Attachment D

New York State Energy Research and Development Authority
("NYSERDA")

AGREEMENT

1. Agreement Number:

2. Contractor:

3. Project Director:

4. Effective Date:

5. Project Period:

6. Total Award: Cumulative Amount of Task Work Orders Issued

7. Commitment Terms and Conditions

This Agreement consists of this form plus the following documents:

- Exhibit A, Statement of Work;
- Exhibit B, General Contract Provisions, Terms and Conditions;
- Exhibit C, Standard Terms and Conditions;
- Exhibit D, Prompt Payment Policy Statement;
- Exhibit E, Rate Schedule;
- Exhibit F, Employment Policies and Procedures Applicable to Temporary and Leased Employees;
- Exhibit G, Certification for Access to NYSERDA's Internal Networks and Systems;
- Exhibit H, NYSERDA Information Security Policies and Procedures Manual; and
- Exhibit I, Article 15-A Contract Provisions (non-construction contract); and
- Exhibit J, Article 17-B (SDVOB) Contract Provisions (non-construction).

7. ACCEPTANCE. THIS AGREEMENT SHALL NOT BECOME EFFECTIVE UNLESS EXECUTED BELOW BY NYSERDA.

[CONTRACTOR]	**NEW YORK STATE ENERGY RESEARCH AND DEVELOPMENT AUTHORITY**
By:_____	By:_____
Name:_____	Cheryl M. Glanton
Title:_____	Director of Contract Management

STATE OF)
) SS.:
COUNTY OF)

On the day of_____in the year_____, before me, the undersigned, a Notary Public in and for said State, personally appeared_____, personally known to me or proved to me on the basis of satisfactory evidence to be the individual(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their capacity(ies), and that by his/her/their signature(s) on the instrument, the individuals(s), or the person upon behalf of which the individual(s) acted, executed the document.

_____

Notary Public

EXHIBIT A

STATEMENT OF WORK

(Item 1, including Tasks 1-4, is contained in Attachment E and will be reinserted into this Exhibit A, Statement of Work when contracting with awarded proposer(s).)

2. TASK WORK ORDERS

For each assigned initiative, a Task Work Order Template will be developed by the Contractor. A NYSERDA point person will be designated to manage the initiative specific training and work performed under the Task Work Order. Initiative details and specific standard operating procedures will be provided to the Contractor during Task Work Order development.

For each Task Work Order, the Contractor is expected to:

- Develop an approach and budget for review and approval by NYSERDA according to the task(s) assigned.
- Negotiate the scope and cost of the support service.
- Upon agreement by both NYSERDA and the Contractor, provide the required assistance within the agreed upon time frames.
- Submit required deliverables to NYSERDA for review and approval.
- Provide required documentation of expenditures by task based on the approved Task Work Order when seeking payment from NYSERDA.

The Task Work Order must assure that appropriate staff and resources will be available for the services requested as well as general day to day support of the initiative assigned.

If NYSERDA determines that the parties will be unable to reach agreement on the terms of the Task Work Order, NYSERDA may rescind the Task Work Order at its sole discretion.

When NYSERDA finds the terms of the proposed Task Work Order acceptable and has issued a Notice to Proceed on a Task Work Order, the Contractor shall carry out the work pursuant to the requirements of such Task Work Order. The work set forth in the Task Work Order shall, upon its issuance by NYSERDA, constitute Work to be performed by the Contractor under this Agreement.

Task Work Orders may be issued at any time during the Project Period.

The Contractor may submit an invoice for costs when the corresponding Notice to Proceed has been issued by NYSERDA. Should a Notice to Proceed not be issued for a certain Task Work Order, NYSERDA is under no obligation to reimburse the Contractor for any costs or expenses associated with that Task Work Order.

If NYSERDA finds that a Task Work Order must be modified, NYSERDA may issue a Task Work Order modification request. The Contractor shall then prepare a modification to the Task Work Order. If the Contractor's modified Task Work Order is acceptable to NYSERDA, then NYSERDA may issue a Task Work Order Modification.

NYSERDA must be kept informed of milestones, delays or other occurrences in order to participate in any decision or to initiate any necessary action.

NYSERDA will review and approve the finalized tasks to ensure that all items included in the Task Work Order are satisfactorily completed and within the prescribed time frame. The Contractor shall not be accountable for delays caused by NYSERDA, NYSERDA participants, or other potential project co-funders such as a utility.

Task Work Order Template

Date:

Contractor:	
Contract #:	
Task Work Order #:	
Program Area:	
NYSERDA PM:	
Task(s) Assigned:	

Work Assignment:

Staff Assigned:

Tasks:

Deliverables & Schedule:

Budget:

Staff Title	Hourly Rate/Unit Rate	Not to Exceed Total

Grand Total:

Additional Provisions for Contractor Employees Working On-Site at NYSERDA

1. Relationship of the Parties. It is understood and agreed that the personnel furnished by Contractor to perform the services stipulated in this TWO, including personnel who may perform such services at NYSERDA's offices, shall be Contractor's employee(s) or agent(s), and under no circumstances are such employee(s) to be considered NYSERDA's employee(s) or agent(s), and shall remain the employees of Contractor, except to the extent required by section 414(n) of the Internal Revenue Code. Each individual Contractor employee who may perform services at NYSERDA's offices under this TWO must complete the attached Attachment D, NYSERDA - Employment Policies and Procedures Applicable to Temporary and Leased Employees.

The relationship of the parties to this Agreement and TWO is that of independent contractors. Nothing in this TWO shall be construed as creating a partnership, joint venture, employment, agency, legal representation or other relationship between NYSERDA and Contractor for any reason, including but not limited to unemployment, workers' compensation, employee benefits,

expense reimbursement, vicarious liability, professional liability coverage or indemnification. Neither party shall have the right, power or authority to obligate or bind the other in any manner not specified in this TWO.

2. Additional Screening Requirements for Assigned Employees. Provider agrees that it shall perform or have performed, within the two years immediately preceding the placement of any employee, a background check; by virtue of making such placement, Provider certifies that such background check on the employee has been performed. Provider agrees that it will inform Client's Director of Human Resources by phone or email (518.862.1090. ext. 3640; donna.rabito@nyserda.ny.gov), simultaneously with or preceding such placement, if: (1) such background check reveals, with respect to the referred employee, (a) a felony conviction, or (b) any other job-related conviction, or (2) immediately upon its becoming aware that such individual has been convicted of such a crime. Client and Provider will comply with all applicable federal, state and local laws and will consider the nature and gravity of the offense, the amount time that has passed since the conviction and the nature of the duties of the assignment to be performed.

3. No Benefits. Contractor agrees that the personnel furnished by Contractor may be "leased employees" within the meaning of section 414(n) of the Internal Revenue Code. Contractor acknowledges that leased employees are excluded from participation in the employee benefit plans, funds and Programs provided by NYSERDA to its employees including, but not limited to, any group health plan, sickness or accident plan, retirement plan, retirement plan or similar benefit plan provided to employees by NYSERDA, by the terms of such benefit plans, funds or Programs. Contractor agrees to notify NYSERDA if it maintains (or ceases to maintain) a plan described in section 414(n)(5)(B) of the Internal Revenue Code.

4. Insurance. The Contractor, at no additional cost to NYSERDA, shall maintain or cause to be maintained throughout the term of this Agreement, for all personnel, Workers Compensation, Employers Liability, and Disability Benefits as required by New York State.

5. Notification of Claims/Events. Contractor expressly acknowledges NYSERDA's need to be advised, on an immediate basis, of the existence of any claim or event that might result in a claim or claims against NYSERDA, Contractor and/or Contractor's personnel by virtue of any act or omission on the part of NYSERDA or its employees. Accordingly, Contractor expressly covenants and agrees to notify NYSERDA of any such claim or event, including but not limited to, requests for accommodation and allegations of harassment and/or discrimination, immediately upon Contractor's discovery of the same, and to fully and honestly cooperate with NYSERDA in its efforts to investigate and/or address such claims or events, including but not limited to, complying with any reasonable request by NYSERDA for disclosure of information concerning such claim or event even in the event that this TWO should terminate for any reason.

6. Controlling Terms. The terms and conditions set forth in this TWO shall control in the event of any inconsistency between such terms and conditions and matters set forth in the Agreement.

7. NEIS Access. In order for the Contractor's staff to fulfill the requirements of this TWO, access to NEIS is necessary. Each individual Contractor employee who will be completing work under this TWO must complete the Addendum No. 1, Certification for Access to NYSERDA's Internal

Networks and Systems. In addition the Contractor and its employees are subject to Addendum No. 2, NYSERDA Information Security Policies and Procedures Manual as amended and superseded.

8. Additional Employment Policies and Procedures. The Contractor's staff shall sign and agree to abide by such policies and procedures as detailed in Addendum No. 3, NYSERDA-Employment Policies and Procedures Applicable to Temporary and Leased Employees.

3. CONTRACTOR RESPONSIBILITIES

The Contractor shall provide all task management activities necessary for the completion of this Statement of Work, which shall include the following activities:

- Coordinate the work of the Contractor's employees that are undertaking tasks described in this Statement of Work;
- Ensure control over the agreement and/or task work order budgets and adherence to the task schedules;
- Efficiently and effectively manage the project administration process and communications between the various stakeholders (ex. participants, service providers, and contractors); and
- Provide all reporting to NYSERDA as specified in the individual task work orders and this Statement of Work.

The Contractor shall provide recommendations to NYSERDA on potential refinements that will:

- Streamline initiative processes and procedures;
- Streamline project management system(s) and project tracking needs;
- Improve efficiency and participant satisfaction;
- Reduce operational costs; and
- Increase the productivity of Contractor's staff while still effectively achieving initiative goals.

The Contractor shall also:

- Provide staff with excellent verbal and written communication skills using standard U.S. English spelling and vocabulary who are available Monday through Friday, 8am – 5pm Eastern Time (ET).

- Fully understand and be able to explain the variety of NYSERDA market development initiatives they are providing support for.

- Prepare a Task Work Order for review and approval by NYSERDA for each assigned initiative or task.

- Negotiate the scope and cost of the Task Work Order with NYSERDA

- Upon agreement by all parties to the Task Work Order and issuance of a Notice to Proceed by NYSERDA, provide the required services within the required time frame.

- Review applications for compliance with initiative rules and procedures, including eligibility of participants, service providers, projects, and measures; completeness of applications; and compliance with the overall project and funding requested with written program rules.

- Process accepted applications.

- Complete data entry accurately and efficiently.

- Regularly maintain and assure data quality, as well as report general correspondence, application, and incentive metrics to NYSERDA.

- Prepare, review, track, and report out on payment requests.

- Provide NYSERDA with a period and cumulative report by the 10th of each month per Item 2, Task 5 of the Statement of Work.

- Gather insight gained from daily interactions with the public and share it with NYSERDA on a frequent basis.

- Continually provide recommendations to NYSERDA on potential refinements that will streamline and bring consistency in data and project management systems, initiative processes and procedures, improve efficiency and participant satisfaction, reduce operational costs, and increase the productivity of Contractor's staff while still effectively achieving initiative goals.

- Keep NYSERDA informed of each assigned status and confer with NYSERDA on substantive issues.

- Make changes requested by NYSERDA.

- Make timely, accurate, and well documented requests for payment.

- Refer to initiative solicitations for program updates.

4. NYSERDA RESPONSIBILITIES

NYSERDA will maintain overall management and control for all services including the selection, supervision, and coordination of the Contractor. The major responsibilities of NYSERDA are to:

- Assign initiatives/tasks to the Contractors based on expertise, location, and workload to best support NYSERDA and the participants.
- Assist Contractor in developing Task Work Orders.
- Provide Contractor with administrative processes and standard operating procedures for each assigned initiative, subject to improvement with input from shared services provider(s).
- Monitor the progress of the Contractor through ongoing telephone contact, review of status reports and data monitoring activities, etc., identify problems and initiate corrective action.
- Review market trends and insights submitted by the Contractor for potential inclusion in current and future offerings.
- Provide review of deliverables to ensure that the deliverables conform to the Task Work Order and specific initiative requirements.
- Ensure adherence to NYSERDA's established policies and procedures.
- Provide a NYSERDA point person for initiative specific assistance.
- Provide initial and continual training on program/initiative rules & guidelines.
- Provide initial and continual training on program/initiative data management systems.

NYSERDA reserves the right to:

- Incorporate programmatic changes as needed, thus modifying or adding to the services outlined,
- Tailor proposed services within the bounds of the contract based on cost-effectiveness, performance, participation, or other considerations,
- Reallocate funding among the selected providers,
- Add other initiative areas and associated funding to the contract should other initiatives require support.

5. DELIVERABLES

The Contractor shall deliver:

a. A specific Task Work Order for each assignment.

b. Reports as defined in the Task Work Order.

c. Satisfactorily completed tasks and assignments as defined by a NYSERDA approved Task Work Order.

d. Monthly progress reports to NYSERDA no later than the 10th of each month as outlined in Item 2, Task 5 of the Statement of Work.

EXHIBIT B

GENERAL CONTRACT PROVISIONS, TERMS AND CONDITIONS

Article I

Definitions

Section 1.01. Definitions. Unless the context otherwise requires, the terms defined below shall have, for all purposes of this Agreement, the respective meanings set forth below, the following definitions to be equally applicable to both the singular and plural forms of any of the terms defined.

(a) General Definitions:

Agreement: This Agreement shall consist of Page One and Exhibits A, B, C, D, E, and F hereto, all of which are made a part hereof as if set forth here in full.

Budget: Collectively, the budgets set forth in individual Task Work Orders consistent with the rates set forth in Exhibit E hereto.

Cash-based Expenses: Those obligations of Contractor that shall be settled in cash.

Contract Administrator: NYSERDA's Director of Contract Management, Cheryl M. Glanton, or such other person who may be designated, in writing, by NYSERDA.

Contract Information: Recorded information regardless of form or characteristic first produced in the performance of this Agreement, that is specified to be compiled under this Agreement, specified to be delivered under this Agreement, or that is actually delivered in connection with this Agreement, and including the Final Report delivered by Contractor pursuant to Exhibit A, Statement of Work, if applicable.

Contractor: The Contractor identified in Item 2 on the first page of this Agreement.

Customer: An individual, a business, an organization or other entity who is a customer of NYSERDA.

Effective Date: The effective date of this Agreement shall be the date appearing in Item 4 on the first page of this Agreement.

Final Report: The Final Reports as described in Exhibit A.

Notice to Proceed: The Notice described in Section 3 of Exhibit A.

Proprietary Information: Recorded information regardless of form or characteristic, produced or developed outside the scope of this Agreement and without NYSERDA financial support, provided that such information is not generally known or available from other sources

without obligation concerning their confidentiality; has not been made available by the owner to others without obligation concerning its confidentiality; and is not already available to NYSERDA without obligation concerning its confidentiality. Under no circumstances shall any information included in the Final Report delivered by Contractor pursuant to Exhibit A, Statement of Work, if applicable, be considered Proprietary Information.

Person: An individual, a corporation, an association or partnership, an organization, a business or a government or political subdivision thereof, or any governmental agency or instrumentality.

Progress Reports: The Progress Reports as required by the individual Task Work Orders issued pursuant to this Agreement.

Responsible: Responsible or Responsibility means the financial ability, legal capacity, integrity and past performance of Contractor and as such terms have been interpreted relative to public procurements. See NYS Finance Law § 163(1)(c).

Statement of Work: The Statement of Work attached hereto as Exhibit A and the individual Task Work Orders issued pursuant to this Agreement.

Subcontract: An agreement for the performance of Work by a Subcontractor, including any purchase order for the procurement of permanent equipment or expendable supplies in connection with the Work.

Subcontractor: A person who performs Work directly or indirectly for or on behalf of the Contractor (and whether or not in privity of contract with the Contractor) but not including any employees of the Contractor or the Subcontractors.

Task Work Order: A Task Work Order issued by NYSERDA pursuant to Exhibit A of this Agreement, specifically a Task Work Order Plan approved by NYSERDA.

Task Work Order Plan: The statement of work and budget for a project proposed by the Contractor.

Work: The Work described in the Exhibit A and in individual Task Work Orders issued pursuant to this Agreement (including the procurement of equipment and supplies in connection therewith) and the performance of all other requirements imposed upon the Contractor under this Agreement.

Article II

Performance of Work, Project Personnel

Section 2.01. Manner of Performance. Subject to the provisions of Article XII hereof, the Contractor shall perform all work (the "Work") necessary to carry out Task Work Orders issued by NYSERDA for the implementation of the Statement of Work, attached hereto as Exhibit A (including the furnishing of personnel and the procurement of equipment, supplies and other items necessary in connection therewith) and subject to the terms therein. The Work shall

include on-site engineering assistance, training and materials, technical analysis and support, implementation assistance services, and other technical services as requested by NYSERDA. The Work shall be carried out with diligence and skill to the satisfaction of NYSERDA. The Contractor agrees to cooperate with NYSERDA in carrying out the Work, and to review and act upon NYSERDA recommendations, in order to assure the Work's expeditious and satisfactory conduct and completion. The Contractor also agrees to meet with NYSERDA at such times as NYSERDA may reasonably request, and at other times specified in Task Work Orders, to discuss the progress of the Work and any other matters that may arise.

Section 2.02. Project Personnel. It is understood and agreed that the "Contact Person" identified in Item 3 of page one of the Agreement shall serve as Project Director and as such shall have the responsibility of the overall supervision and conduct of the Work on behalf of the Contractor and that the persons described in Task Work Orders shall serve in the capacities described therein for the conduct of the Work described therein. Any changes of Project Director or in persons described in Task Work Orders shall be subject to the prior written approval of NYSERDA. Annexed as Exhibit E is a list of personnel that will be available to perform Work under this Agreement along with the rates that will apply for each such person during the term of this Agreement. If the Contractor wishes to employ personnel not listed on Exhibit E to complete any Task Work Order hereunder, the Contractor must obtain the written approval of NYSERDA. The approvals set forth in this Section shall not be unreasonably withheld, and, in the event that notice of approval or disapproval is not received by the Contractor within thirty (30) days after receipt of request for approval by NYSERDA, the requested change in Project Director or personnel shall be considered approved. In the event that NYSERDA requires additional time for considering approval, NYSERDA shall notify the Contractor within thirty (30) days of receipt of the request for approval that additional time is required and shall specify the additional amount of time necessary up to thirty (30) days.

Section 2.03. Title to Equipment. Title shall vest in NYSERDA to all equipment purchased by the Contractor under this Agreement. Upon the request of NYSERDA, the Contractor shall execute, acknowledge, deliver and perform, or cause to be executed, acknowledged, delivered or performed, all such bills of sale, assignments, conveyances or other documents or acts as NYSERDA may reasonably request in order to assure the better vesting in and confirming to NYSERDA, its successor and assigns, of title to and possession of such equipment.

Article III

Deliverables

Section 3.01. Deliverables. All deliverables shall be provided in accordance with the Exhibit A and the Task Work Orders issued pursuant to this Agreement.

Article IV

Payment

Section 4.01. Payment Terms. Compensation will be based on the Contractor's staff charges and indirect costs plus allowable direct charges (collectively, "Contractor fees"). Contractor fees for a project must be fully described in each Task Work Order Plan budget and must be approved by NYSERDA. The Task Work Order Plan budget must state a not-to-exceed cost cap or ceiling amount for each project. The Contractor shall not accrue billable costs beyond the not-to-exceed cost cap in the Task Work Order Plan without approval in writing by NYSERDA. The Contractor shall not be compensated for time spent in the preparation of any Task Work Order Plan.

The Task Work Order issued by NYSERDA will state NYSERDA's funding obligation. For projects in which NYSERDA is not directly paying 100% of the Contractor's fees, the Contractor itself must negotiate a payment schedule and collect fees from all other parties directly. NYSERDA will be responsible for its share of the project costs only.

(a) Staff Charges: To the extent Cash-based Expenses are incurred by the Contractor, the Contractor shall be reimbursed amounts paid to its employees for the services performed by its employees under the terms of this Agreement at the lesser of the employee's wage rate set forth in each Task Work Order and within the ranges set forth in Exhibit E or the actual wages paid to the employee and applicable at the time the Work is performed. Such billing rates shall be inclusive of actual Cash-based Expenses in the form of wages paid the employee, fringe benefits, overhead, general and administrative (G&A), and other indirect costs. Contractor hereby warrants and guarantees that the billing rates charged herein are Contractor's customary billing rates for performance of work of the type described in the Statement of Work attached hereto. Such billing rates shall not be increased during the term hereof without the written consent of NYSERDA.

(b) Direct Charges: To the extent Cash-based Expenses are incurred by the Contractor, the Contractor shall be reimbursed NYSERDA's pro rata share of reasonable and necessary actual direct costs incurred (e.g., equipment, supplies, travel and other costs directly associated with the performance of the Agreement) to the extent required in the performance of the Work and to the extent such costs are anticipated in the Task Work Order budget. Travel, lodging, meals and incidental expenses shall be reimbursed for reasonable and necessary costs incurred. Costs shall not exceed the daily per diem rates published in the Federal Travel Regulations. Reimbursement for the use of personal vehicles shall be limited to the Internal Revenue Service business standard mileage rate in effect at the time the expense was incurred.

(c) Task Work Order Cost Cap: The Task Work Order budget must state a not-to-exceed cost cap or ceiling amount for each Task Work Order assignment. The Contractor shall not accrue billable costs beyond the not-to-exceed cost cap in the Task Work Order without approval in writing by NYSERDA.

Section 4.02. Progress Payments. Unless otherwise specified in the Notice to Proceed for an individual Task Work Order, the Contractor may submit invoices for progress payment no more than once each month for Work performed. Invoices shall be addressed to NYSERDA, "Attention: Accounts Payable," or submitted electronically to invoices@nyserda.ny.gov. Such invoices shall make reference to the Agreement number shown in Item No. 1 on page one of this Agreement. Invoices shall set forth total project costs incurred. They shall be in a format

consistent with the cost categories set forth in the Task Work Order budget. Invoices shall be itemized and provide reasonable documentation for the above to provide evidence of costs incurred. If a wage rate or billing rate is used, Contractor must certify on its invoice that such rate represents the lesser of: (i) the actual rate at the time the Work was performed, and (ii) the rate listed for each such employee listed in the Task Work Order budget that are within the ranges set forth in Exhibit E. NYSERDA may adjust amounts payable to correlate the proportion of NYSERDA's funding share paid to the proportion of the Work completed.

The Contractor shall be notified by NYSERDA in accordance with Section 5.04.4 (b)(2) of NYSERDA's Prompt Payment Policy Statement, attached hereto as Exhibit D, of any such information or documentation which the Contractor did not include with such invoice.

In accordance with and subject to the provisions of such Exhibit D, NYSERDA shall pay to the Contractor, within the prescribed time after receipt of an invoice for a progress payment, the amount so requested, unless NYSERDA should determine that any such payment or any part thereof is otherwise not properly payable pursuant to the terms of the Agreement or the Budget.

Section 4.03. Release by the Contractor. The acceptance by the Contractor of final payment from NYSERDA under each Task Work Order issued pursuant to this Agreement shall release NYSERDA from all claims and liability that the Contractor, its representatives and assigns might otherwise have relating to the Task Work Order and this Agreement.

Section 4.04. Maintenance of Records. The Contractor shall keep, maintain, and preserve at its principal office throughout the term of the Agreement and for a period of three years after acceptance of the Work, full and detailed books, accounts, and records pertaining to this Agreement, including without limitation, all data, bills, invoices, payrolls, time records, expense reports, subcontracting efforts and other documentation evidencing, or in any material way related to, the direct and indirect costs and expenses incurred by the Contractor in the course of such performance under this Agreement.

Section 4.05. Audit. NYSERDA shall have the right from time to time and at all reasonable times during the term of this Agreement and for the maintenance period set forth in Section 4.04 hereof to inspect and audit any and all books, accounts and records related to this Agreement or reasonably necessary to the performance of an audit at the office or offices of the Contractor where they are then being kept, maintained and preserved pursuant to Section 4.04 hereof. Any payment made under the Agreement shall be subject to retroactive reduction for amounts included therein which are found by NYSERDA on the basis of any audit of the Contractor by NYSERDA, the State of New York or an agency of the United States, not to constitute an allowable charge or cost hereunder.

Article V

Assignments, Subcontracts and Purchase Orders

Section 5.01. General Restrictions. Except as specifically provided otherwise in this Article, the assignment, transfer, conveyance, subcontracting or other disposal of this Agreement or any of the Contractor's rights, obligations, interests or responsibilities hereunder, in whole or

in part, without the express consent in writing of NYSERDA shall be void and of no effect as to NYSERDA.

Section 5.02. Subcontract Procedures. Without relieving it of, or in any way limiting, its obligations to NYSERDA under this Agreement, the Contractor may enter into Subcontracts for the performance of Work or for the purchase of materials or equipment. Except for a subcontractor or supplier specified in a team arrangement with the Contractor in the Contractor's original proposal, and except for any subcontract or order for equipment, supplies or materials from a single subcontractor or supplier totaling less than $50,000, the Contractor shall select all subcontractors or suppliers through a process of competitive bidding or multi-source price review. A team arrangement is one where a subcontractor or supplier specified in the Contractor's proposal is performing a substantial portion of the Work and is making a substantial contribution to the management and/or design of the Project. In the event that a competitive bidding or multi-source price review is not feasible, the Contractor shall document an explanation for, and justification of, a sole source selection. The Contractor shall document the process by which a subcontractor or supplier is selected by making a record summarizing the nature and scope of the work, equipment, supplies or materials sought, the name of each person or organization submitting, or requested to submit, a bid or proposal, the price or fee bid, and the basis for selection of the subcontractor or supplier. An explanation for, and justification of, a sole source selection must identify why the work, equipment, supplies or materials involved are obtainable from or require a subcontractor with unique or exceptionally scarce qualifications or experience, specialized equipment, or facilities not readily available from other sources, or patents, copyrights, or proprietary data. All Subcontracts shall contain provisions comparable to those set forth in this Agreement applicable to a subcontractor or supplier, and those set forth in Exhibit C to the extent required by law, and all other provisions now or hereafter required by law to be contained therein. Each Subcontract shall make express reference to this Agreement, and shall state that in the event of any conflict or inconsistency between any Subcontract and this Agreement, the terms and conditions of this Agreement shall control as between Subcontractor and Contractor. The Contractor shall submit to NYSERDA's Contract Administrator for review and written approval any subcontract(s) specified in a Task Work Order as requiring NYSERDA approval, including any replacements thereof.

Section 5.03. Performance. The Contractor shall promptly and diligently comply with its obligations under each Subcontract and shall take no action that would impair its rights thereunder. The Contractor shall take no action, and shall take all reasonable steps to prevent its Subcontractors from taking any action, that would impair NYSERDA’s rights under this Agreement. The Contractor shall not assign, cancel or terminate any Subcontract without the prior written approval of NYSERDA’s Contract Administrator as long as this Agreement remains in effect. Such approval shall not be unreasonably withheld and, in the event that notice of approval or disapproval is not received by the Contractor within thirty days after receipt of request for approval by NYSERDA, the requested assignment, cancellation, or termination of the Subcontract shall be considered approved by NYSERDA. In the event that NYSERDA requires additional time for considering approval, NYSERDA shall notify the Contractor within thirty (30) days of receipt of the request for approval that additional time is required and shall specify the additional amount of time necessary up to sixty (60) days.

Article VI

Schedule; Acceptance of Work

Section 6.01. Schedule. The Work shall be performed as expeditiously as possible in conformity with the schedule requirements contained herein and in the Statement of Work. It is understood and agreed that the delivery of the draft and final versions of the Final Report by the Contractor shall occur in a timely manner and in accordance with the requirements of the Task Work Order schedule.

Section 6.02. Acceptance of Work. The completion of the Work shall be subject to acceptance by NYSERDA in writing of the Final Report and all other deliverables as defined in the Task Work Order Plan.

Article VII

Force Majeure

Section 7.01. Force Majeure. Neither party hereto shall be liable for any failure or delay in the performance of its respective obligations hereunder if and to the extent that such delay or failure is due to a cause or circumstance beyond the reasonable control of such party, including, without limitation, acts of God or the public enemy, expropriation or confiscation of land or facilities, compliance with any law, order or request of any Federal, State, municipal or local governmental authority, acts of war, rebellion or sabotage or damage resulting therefrom, fires, floods, storms, explosions, accidents, riots, strikes, or the delay or failure to perform by any Subcontractor by reason of any cause or circumstance beyond the reasonable control of such Subcontractor.

Article VIII

Rights in Information; Confidentiality

Section 8.01. Rights in Contract and Proprietary Information.

(a) All Contract Information shall be the property of NYSERDA. The Contractor shall not use Contract Information for any purpose other than to implement its obligations under this Agreement.

(b) All Proprietary Information shall be the property of Contractor.

(c) The use, public performance, reproduction, distribution, or modification of any materials used by Contractor in the performance of this Agreement does not and will not violate the rights of any third parties, including, but not limited to, copyrights, trademarks, service marks, publicity, or privacy. The Contractor shall be responsible for obtaining and paying for any necessary licenses to use any third-party content.

(d) The Contractor agrees that to the extent it receives or is given any information from NYSERDA or a NYSERDA contractor or subcontractor, the Contractor shall treat such data in accordance with any restrictive legend contained thereon, unless another use is specifically authorized by prior written approval of the NYSERDA Project Manager. Contractor

acknowledges that in the performance of the Work under this Agreement, Contractor may come into possession of personal information as that term is defined in Section 92 of the New York State Public Officers Law. Contractor agrees not to disclose any such information without the consent of NYSERDA.

(e) In conjunction with the performance of the work under this Agreement, NYSERDA furnishes the Contractor with certain information concerning that is either non-public, confidential or proprietary in nature (the "Information").

The Information will be kept confidential and will not, without NYSERDA's prior written consent, be disclosed by you, your agents, employees, contractors or professional advisors, in any manner whatsoever, in whole or in part, and will not be used by you, your agents, employees, contractors or professional advisors other than in connection with the Project. You agree to transmit the Information only to your agents, employees, contractors and professional advisors who need to know the Information for that purpose and who are informed by you of the confidential nature of the Information and who will agree in writing to be bound by the terms and conditions of Exhibit B, Article VIII of NYSERDA Agreement XXXXX and this Addendum.

You shall conform to requirements of the New York State Office of Cyber Security Policy P03-002 and any amendments thereto, to maintain the security of and to prevent unauthorized access to Information that is maintained in electronic form on your systems.

You will keep a record of the location of the Information. At the conclusion of the Project, you will return to NYSERDA all the Information and/or provide proof to NYSERDA that the Information was destroyed. You also agree to submit to an audit of its data security/destruction practices by NYSERDA or its representative during the contract term and for up to two years following the expiration of the contract.

Article IX

Warranties and Guarantees

Section 9.01. Warranties and Guarantees. The Contractor warrants and guarantees that:

(a) all information provided and all representations made by Contractor as a part of the proposal, if any, submitted to NYSERDA in order to obtain or in application for this Agreement were, to the best of Contractor's knowledge, complete, true and accurate when provided or made;

(b) as of the Effective Date, it is financially and technically qualified to perform the Work, and is qualified to do business and is in good standing in all jurisdictions necessary for Contractor to perform its obligations under this Agreement;

(c) it is familiar with and will comply with all general and special Federal, State, municipal and local laws, ordinances and regulations, if any, that may in any way affect the performance of this Agreement;

(d) the design, supervision and workmanship furnished with respect to performance of the Work shall be in accordance with sound and currently accepted construction and design standards and best engineering practices;

(e) all materials, equipment and workmanship furnished by it and by Subcontractors in performance of the Work or any portion thereof shall be free of defects in design, material and workmanship, and all such materials and equipment shall be of first-class quality, shall conform with all applicable codes, specifications, standards and ordinances and shall have service lives and maintenance characteristics suitable for their intended purposes in accordance with sound and currently accepted construction and design standards and best engineering practices;

(f) neither the Contractor nor any of its employees, agents, representatives or servants has actual knowledge of any patent issued under the laws of the United States or any other matter which could constitute a basis for any claim that the performance of the Work or any part thereof infringes any patent or otherwise interferes with any other right of any Person;

(g) to the best of Contractor's knowledge, there are no existing undisclosed or threatened legal actions, claims, or encumbrances, or liabilities that may adversely affect the Work or NYSERDA's rights hereunder;

(h) it has no actual knowledge that any information or document or statement furnished by the Contractor in connection with this Agreement contains any untrue statement of a material fact or omits to state a material fact necessary to make the statement not misleading, and that all facts have been disclosed that would materially adversely affect the Work;

(i) all information provided to NYSERDA with respect to State Finance Law Sections 139-j and 139-k is complete, true and accurate;

(j) Contractor is familiar with and will comply with NYSERDA's Code of Conduct for Contractors, Consultants, and Vendors with respect to the performance of this Agreement; [1] and

(k) its rates for the indirect costs charged herein have been determined based on the Contractor's reasonably anticipated indirect costs during the term of the Agreement and calculated consistent with generally accepted accounting principles.

Article X

Indemnification

Section 10.01. Indemnification. The Contractor shall protect, indemnify and hold harmless NYSERDA and the State of New York from and against all liabilities, losses, claims, damages, judgments, penalties, causes of action, costs and expenses (including, without limitation, attorneys' fees and expenses) imposed upon or incurred by or asserted against NYSERDA or the State of New York resulting from, arising out of or relating to the

[1] http://www.nyserda.ny.gov/~/media/Files/About/Board%20Governance/CodeConduct.ashx?sc_database=web

Contractor's or its Subcontractors' performance of this Agreement. The obligations of the Contractor under this Article shall survive any expiration or termination of this Agreement, and shall not be limited by any enumeration herein of required insurance coverage.

Article XI

Insurance

Section 11.01. Maintenance of Insurance; Policy Provisions. The Contractor, at no additional direct cost to NYSERDA, shall maintain or cause to be maintained throughout the term of this Agreement, insurance of the types and in the amounts specified in the Section hereof entitled Types of Insurance. All such insurance shall be evidenced by insurance policies, each of which shall:

(a) name or be endorsed to cover NYSERDA, the State of New York and the Contractor as additional insureds;

(b) provide that such policy may not be cancelled or modified until at least 30 days after receipt by NYSERDA of written notice thereof; and

(c) be reasonably satisfactory to NYSERDA in all other respects.

Section 11.02. Types of Insurance. The types and amounts of insurance required to be maintained under this Article are as follows:

(a) Commercial general liability insurance for bodily injury liability, including death, and property damage liability, incurred in connection with the performance of this Agreement, with minimum limits of $1,000,000 in respect of claims arising out of personal injury or sickness or death of any one person, $1,000,000 in respect of claims arising out of personal injury, sickness or death in any one accident or disaster, and $1,000,000 in respect of claims arising out of property damage in any one accident or disaster; and

(b) Workers Compensation, Employers Liability, and Disability Benefits as required by New York State.

Section 11.03. Delivery of Policies; Insurance Certificates. Prior to commencing the Work, the Contractor shall deliver to NYSERDA certificates of insurance issued by the respective insurers, indicating the Agreement number thereon, evidencing the insurance required by Article XI hereof. In the event any policy furnished or carried pursuant to this Article will expire on a date prior to acceptance of the Work by NYSERDA pursuant to the section hereof entitled Acceptance of Work, the Contractor, not less than 15 days prior to such expiration date, shall deliver to NYSERDA certificates of insurance evidencing the renewal of such policies, and the Contractor shall promptly pay all premiums thereon due. In the event of threatened legal action, claims, encumbrances, or liabilities that may affect NYSERDA hereunder, or if deemed necessary by NYSERDA due to events rendering a review necessary, upon request the Contractor shall deliver to NYSERDA a certified copy of each policy.

Article XII

Stop Work Order; Termination; Non-Responsibility

Section 12.01. Stop Work Order.

(a) NYSERDA may at any time, by written Order to the Contractor, require the Contractor to stop all or any part of the Work called for by this Agreement for a period of up to ninety (90) days after the Stop Work Order is delivered to the Contractor, and for any further period to which the parties may agree. Any such order shall be specifically identified as a Stop Work Order issued pursuant to this Section. Upon receipt of such an Order, the Contractor shall forthwith comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the Work covered by the Order during the period of work stoppage consistent with public health and safety. Within a period of ninety (90) days after a Stop Work Order is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, NYSERDA shall either:

(i) by written notice to the Contractor, cancel the Stop Work Order, which shall be effective as provided in such cancellation notice, or if not specified therein, upon receipt by the Contractor, or

(ii) terminate the Work covered by such order as provided in the Termination Section of this Agreement.

(b) If a Stop Work Order issued under this Section is cancelled or the period of the Order or any extension thereof expires, the Contractor shall resume Work. An equitable adjustment shall be made in the delivery schedule, the estimated cost, the fee, if any, or a combination thereof, and in any other provisions of the Agreement that may be affected, and the Agreement shall be modified in writing accordingly, if:

(i) the Stop Work Order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this Agreement, and

(ii) the Contractor asserts a claim for such adjustments within 30 days after the end of the period of Work stoppage; provided that, if NYSERDA decides the facts justify such action, NYSERDA may receive and act upon any such claim asserted at any time prior to final payment under this Agreement.

(c) If a Stop Work Order is not cancelled and the Work covered by such Order is terminated, the reasonable costs resulting from the Stop Work Order shall be allowed by equitable adjustment or otherwise.

(d) Notwithstanding the provisions of this Section 12.01, the maximum amount payable by NYSERDA to the Contractor pursuant to this Section 12.01 shall not be increased or deemed to be increased except by specific written amendment hereto.

Section 12.02. Termination.

(a) This Agreement may be terminated by NYSERDA at any time during the term of this Agreement with or without cause, upon ten (10) days prior written notice to the Contractor. In such event, payment shall be paid to the Contractor for Work performed and expenses incurred prior to the effective date of termination in accordance with the provisions of the Article hereof entitled Payment and in reimbursement of any amounts required to be paid by the Contractor pursuant to Subcontracts; provided, however, that upon receipt of any such notice of termination, the Contractor shall cease the performance of Work, shall make no further commitments with respect thereto and shall reduce insofar as possible the amount of outstanding commitments (including, to the extent requested by NYSERDA, through termination of subcontracts containing provisions therefor). Articles VIII, IX, and X shall survive any termination of this Agreement, and Article XVI shall survive until the payment obligations pursuant to Article VIII have been met.

(b) NYSERDA specifically reserves the right to terminate this agreement in the event that the certification filed by the Contractor in accordance with State Finance Law Sections 139-j and 139-k is found to have been intentionally false or intentionally incomplete, or that the certification filed by the Contractor in accordance with New York State Tax Law Section 5-a is found to have been intentionally false when made. Terminations under this subsection (b) will be effective upon Notice.

(c) Nothing in this Article shall preclude the Contractor from continuing to carry out the Work called for by the Agreement after receipt of a Stop Work Order or termination notice at its own election, provided that, if the Contractor so elects: (i) any such continuing Work after receipt of the Stop Work Order or termination notice shall be deemed not to be Work pursuant to the Agreement, and (ii) NYSERDA shall have no liability to the Contractor for any costs of the Work continuing after receipt of the Stop Work Order or termination notice.

12.03 Suspension or Termination for Non-Responsibility.

(a) Suspension. NYSERDA, in its sole discretion, reserves the right to suspend any or all activities under this Agreement, at any time, when it discovers information that calls into question the Responsibility of the Contractor. In the event of such suspension, the Contractor will be given written notice outlining the particulars of such suspension. Upon issuance of such notice, the Contractor must comply with the terms of the suspension order. Contract activity may resume at such time as NYSERDA issues a written notice authorizing a resumption of performance under the Contract.

(b) Termination. Upon written notice to the Contractor, and a reasonable opportunity to be heard with appropriate NYSERDA officials or staff, this Agreement may be terminated by NYSERDA at the Contractor's expense where the Contractor is determined by NYSERDA to be non-Responsible. In such event, NYSERDA may complete the contractual requirements in any manner it may deem advisable and pursue available legal or equitable remedies for breach.

Article XIII

Independent Contractor

Section 13.01. Independent Contractor. (a) The status of the Contractor under this Agreement shall be that of an independent contractor and not that of an agent, and in accordance with such status, the Contractor, the Subcontractors, and their respective officers, agents, employees, representatives and servants, including the Project Director, shall at all times during the term of this Agreement conduct themselves in a manner consistent with such status and by reason of this Agreement shall neither hold themselves out as, nor claim to be acting in the capacity of, officers, employees, agents, representatives or servants of NYSERDA nor make any claim, demand or application for any right or privilege applicable to NYSERDA, including, without limitation, vicarious liability, professional liability coverage or indemnification, rights or privileges derived from workers' compensation coverage, unemployment insurance benefits, social security coverage and retirement membership or credit. It is understood and agreed that the personnel furnished by Contractor to perform the Work shall be Contractor's employee(s) or agent(s), and under no circumstances are such employee(s) to be considered NYSERDA's employee(s) or agent(s), and shall remain the employees of Contractor, except to the extent required by section 414(n) of the Internal Revenue Code.

(b) Contractor expressly acknowledges NYSERDA's need to be advised, on an immediate basis, of the existence of any claim or event that might result in a claim or claims against NYSERDA, Contractor and/or Contractor's personnel by virtue of any act or omission on the part of NYSERDA or its employees. Accordingly, Contractor expressly covenants and agrees to notify NYSERDA of any such claim or event, including but not limited to, requests for accommodation and allegations of harassment and/or discrimination, immediately upon contractor's discovery of the same, and to fully and honestly cooperate with NYSERDA in its efforts to investigate and/or address such claims or events, including but not limited to, complying with any reasonable request by NYSERDA for disclosure of information concerning such claim or event even in the event that this Agreement should terminate for any reason.

Article XIV

Compliance with Certain Laws

Section 14.01. Laws of the State of New York. The Contractor shall comply with all of the requirements set forth in Exhibit C hereto.

Section 14.02. All Legal Provisions Deemed Included. It is the intent and understanding of the Contractor and NYSERDA that each and every provision of law required by the laws of the State of New York to be contained in this Agreement shall be contained herein, and if, through mistake, oversight or otherwise, any such provision is not contained herein, or is not contained herein in correct form, this Agreement shall, upon the application of either NYSERDA or the Contractor, promptly be amended so as to comply strictly with the laws of the State of New York with respect to the inclusion in this Agreement of all such provisions.

Section 14.03. Other Legal Requirements. The references to particular laws of the State of New York in this Article, in Exhibit C and elsewhere in this Agreement are not intended to be exclusive and nothing contained in such Article, Exhibit and Agreement shall be deemed to modify the obligations of the Contractor to comply with all legal requirements.

Article XV

Notices, Entire Agreement, Amendment, Counterparts

Section 15.01. Notices.

(a) All notices, requests, consents, approvals and other communications which may or are required to be given by either party to the other under this Agreement shall be in writing and shall be transmitted either:

(i) via certified or registered United States mail, return receipt requested;
(ii) by facsimile transmission;
(iii)by personal delivery;
(iv)by expedited delivery service; or
(v) by e-mail, return receipt requested.

Such notices shall be addressed as follows, or to such different addresses as the parties may from time-to-time designate as set forth in paragraph (c) below:

NYSERDA
Name: Cheryl M. Glanton
Title: Director of Contract Management
Address: 17 Columbia Circle, Albany, New York 12203
Facsimile Number: 518-862-1091
E-Mail Address: Cheryl.Glanton@nyserda.ny.gov
Personal Delivery: Reception desk at the above address

[Contractor]
Name:
Title:
Address:
Facsimile Number:
E-Mail Address:

(b) Any such notice shall be deemed to have been given either at the time of personal delivery or, in the case of expedited delivery service or certified or registered United States mail, as of the date of first attempted delivery at the address and in the manner provided herein, or in the case of facsimile transmission or email, upon receipt.

(c) The parties may, from time to time, specify any new or different address in the United States as their address for purpose of receiving notice under this Agreement by giving fifteen (15) days written notice to the other party sent in accordance herewith. The parties agree to mutually designate individuals as their respective representatives for the purposes of receiving notices under this Agreement. Additional individuals may be designated in writing by the parties for purposes of implementation and administration/billing, resolving issues and problems and/or for dispute resolution.

Section 15.02. Entire Agreement; Amendment. This Agreement embodies the entire agreement and understanding between NYSERDA and the Contractor and supersedes all prior

agreements and understandings relating to the subject matter hereof. Except as otherwise expressly provided for herein, this Agreement may be changed, waived, discharged or terminated only by an instrument in writing, signed by the party against which enforcement of such change, waiver, discharge or termination is sought.

Section 15.03. Counterparts. This Agreement may be executed in counterparts each of which shall be deemed an original, but all of which taken together shall constitute one and the same instrument.

Article XVI

Publicity

Section 16.01. Publicity.

(a) The Contractor shall collaborate with NYSERDA's Director of Communications to prepare any press release and to plan for any news conference concerning the Work. In addition the Contractor shall notify NYSERDA's Director of Communications regarding any media interview in which the Work is referred to or discussed.

(b) It is recognized that during the course of the Work under this Agreement, the Contractor or its employees may from time to time desire to publish information regarding scientific or technical developments made or conceived in the course of or under this Agreement. In any such information, the Contractor shall credit NYSERDA's funding participation in the Project, and shall state that "NYSERDA has not reviewed the information contained herein, and the opinions expressed in this report do not necessarily reflect those of NYSERDA or the State of New York." Notwithstanding anything to the contrary contained herein, the Contractor shall have the right to use and freely disseminate project results for educational purposes, if applicable, consistent with the Contractor's policies.

(c) Commercial promotional materials or advertisements produced by the Contractor shall credit NYSERDA, as stated above, and shall be submitted to NYSERDA for review and recommendations to improve their effectiveness prior to use. The wording of such credit can be approved in advance by NYSERDA, and, after initial approval, such credit may be used in subsequent promotional materials or advertisements without additional approvals for the credit, provided, however, that all such promotional materials or advertisements shall be submitted to NYSERDA prior to use for review, as stated above. Such approvals shall not be unreasonably withheld, and, in the event that notice of approval or disapproval is not received by the Contractor within thirty days after receipt of request for approval, the promotional materials or advertisement shall be considered approved. In the event that NYSERDA requires additional time for considering approval, NYSERDA shall notify the Contractor within thirty days of receipt of the request for approval that additional time is required and shall specify the additional amount of time necessary up to 180 days. If NYSERDA and the Contractor do not agree on the wording of such credit in connection with such materials, the Contractor may use such materials, but agrees not to include such credit.

Addendum A

Pursuant to Agreement XXXX, XXXX ("Contractor" or "you") provides services to the New York State Energy Research and Development Authority (NYSERDA" or "we"), as specified in Exhibit A, Statement of Work (the "Project"). In conjunction with Contractor's performance of the Project NYSERDA furnishes Contractor with certain information concerning the Project that is either non-public, confidential or proprietary in nature (the "Information"). Exhibit B, Article VIII of the Agreement governs the handling of confidential or proprietary information. This Addendum supplements Article VIII with regards to Contractor's use of the Information

1. The Information will be kept confidential and will not, without NYSERDA's prior written consent, be disclosed by you, your agents, employees, contractors or professional advisors, in any manner whatsoever, in whole or in part, and will not be used by you, your agents, employees, contractors or professional advisors other than in connection with the Project. You agree to transmit the Information only to your agents, employees, contractors and professional advisors who need to know the Information for that purpose and who are informed by you of the confidential nature of the Information and who will agree in writing to be bound by the terms and conditions of Exhibit B, Article VIII of NYSERDA Agreement XXXX and this Addendum.

2. You shall conform to requirements of the New York State Office of Cyber Security Policy P03-002 v.3.4 and any amendments thereto, to maintain the security of and to prevent unauthorized access to Information that is maintained in electronic form on your systems. Such measures shall include:
   a. Access Control on Servers, Systems, Apps, Databases, i.e., role-based permissions, authentication, authorization, and password policy;
   b. Network Security, i.e., isolation of Information, secure V-LANS, Firewalls;
   c. Patch Management, i.e., formal patch cycles and maintenance process;
   d. Malware Prevention, i.e., anti-virus, anti-spyware, vulnerability assessments, penetration testing, audits;
   e. Encryption of Information in transit and Information in storage on desktops, backups, and removable media;
   f. Change Control to ensure that new and modified system software are authorized, tested, and implemented accurately;
   g. Security Event Logging/Monitoring that provides real time alerting of security events
   h. IDS, WS, Website Monitoring of websites for compromise indicators which indicates website defacements, compromises or inappropriate content (Application/Host/Network IDS and IPS);
   i. Web Application scanning that is performed on code and application in compliance with Open Web Application Security project (OWASP) and SANS (SysAdmin, Audit, Network, and Security) Institute standards.

3. You will keep a record of the location of the Information. At the conclusion of the Project, you will return to NYSERDA all the Information and/or provide proof to NYSERDA that the Information was destroyed. You also agree to submit to an audit of its data security/destruction practices by NYSERDA or its representative during the contract term and for up to two years following the expiration of the contract.

EXHIBIT C

REVISED 5/12

STANDARD TERMS AND CONDITIONS
FOR ALL NYSERDA AGREEMENTS

(Based on Standard Clauses for New York State Contracts and Tax Law Section 5-a)

The parties to the Agreement agree to be bound by the following clauses which are hereby made a part of the Agreement:

1. NON-DISCRIMINATION REQUIREMENTS. To the extent required by Article 15 of the Executive Law (also known as the Human Rights Law) and all other State and Federal statutory and constitutional non-discrimination provisions, the Contractor will not discriminate against any employee or applicant for employment because of race, creed, color, sex, national origin, sexual orientation, age, disability, genetic predisposition or carrier status, or marital status. Furthermore, in accordance with Section 220-e of the Labor Law, if this is an Agreement for the construction, alteration or repair of any public building or public work or for the manufacture, sale or distribution of materials, equipment or supplies, and to the extent that this Agreement shall be performed within the State of New York, Contractor agrees that neither it nor its subcontractors shall, by reason of race, creed, color, disability, sex or national origin: (a) discriminate in hiring against any New York State citizen who is qualified and available to perform the work; or (b) discriminate against or intimidate any employee hired for the performance of work under this Agreement. If this is a building service Agreement as defined in Section 230 of the Labor Law, then, in accordance with Section 239 thereof, Contractor agrees that neither it nor its subcontractors shall, by reason of race, creed, color, national origin, age, sex or disability: (a) discriminate in hiring against any New York State citizen who is qualified and available to perform the work; or (b) discriminate against or intimidate any employee hired for the performance of work under this contract. Contractor is subject to fines of $50.00 per person per day for any violation of Section 220-e or Section 239 as well as possible termination of this Agreement and forfeiture of all moneys due hereunder for a second subsequent violation.

2. WAGE AND HOURS PROVISIONS. If this is a public work Agreement covered by Article 8 of the Labor Law or a building service Agreement covered by Article 9 thereof, neither Contractor's employees nor the employees of its subcontractors may be required or permitted to work more than the number of hours or days stated in said statutes, except as otherwise provided in the Labor Law and as set forth in prevailing wage and supplement schedules issued by the State Labor Department. Furthermore, Contractor and its subcontractors must pay at least the prevailing wage rate and pay or provide the prevailing supplements, including the premium rates for overtime pay, as determined by the State Labor Department in accordance with the Labor Law. Additionally, effective April 28, 2008, if this is a public work contract covered by Article 8 of the Labor Law, the Contractor understands and agrees that the filing of payrolls in a manner consistent with Subdivision 3-a of Section 220 of the Labor Law shall be a condition precedent to payment by NYSERDA of any NYSERDA-approved sums due and owing for work done upon the project.

3. NON-COLLUSIVE BIDDING REQUIREMENT. In accordance with Section 2878 of the Public Authorities Law, if this Agreement was awarded based upon the submission of bids, Contractor warrants, under penalty of perjury, that its bid was arrived at independently and without collusion aimed at restricting competition. Contractor further warrants that, at the time Contractor submitted its bid, an authorized and responsible person executed and delivered to NYSERDA a non-collusive bidding certification on Contractor's behalf.

4. INTERNATIONAL BOYCOTT PROHIBITION. If this Agreement exceeds $5,000, the Contractor agrees, as a material condition of the Agreement, that neither the Contractor nor any substantially owned or affiliated person, firm, partnership or corporation has participated, is participating, or shall participate in an international boycott in violation of the Federal Export Administration Act of 1979 (50 USC App. Sections 2401 et seq.) or regulations thereunder. If such Contractor, or any of the aforesaid affiliates of Contractor, is convicted or is otherwise found to have violated said laws or regulations upon the final determination of the United States Commerce Department or any other appropriate agency of the United States subsequent to the Agreement's execution, such Agreement, amendment or modification thereto shall be rendered forfeit and void. The Contractor shall so notify NYSERDA within five (5) business days of such conviction, determination or disposition of appeal. (See and compare Section 220-f of the Labor Law, Section 139-h of the State Finance Law, and 2 NYCRR 105.4).

5. SET-OFF RIGHTS. NYSERDA shall have all of its common law and statutory rights of set-off. These rights shall include, but not be limited to, NYSERDA's option to withhold for the purposes of set-off any moneys due to the Contractor under this Agreement up to any amounts due and owing to NYSERDA with regard to this Agreement, any other Agreement, including any Agreement for a term commencing prior to the term of this Agreement, plus any amounts due and owing to NYSERDA for any other reason including, without limitation, tax delinquencies, fee delinquencies or monetary penalties relative thereto.

6. PROPRIETARY INFORMATION. Notwithstanding any provisions to the contrary in the Agreement, Contractor and NYSERDA acknowledge and agree that all information, in any format, submitted to NYSERDA shall be subject to and treated in accordance with the NYS Freedom of Information Law ("FOIL," Public Officers Law, Article 6). Pursuant to FOIL, NYSERDA is required to make available to the public, upon request, records or portions thereof which it possesses, unless that information is statutorily exempt from disclosure. Therefore, unless the Agreement specifically requires otherwise, Contractor should submit information to NYSERDA in a non-confidential, non-proprietary format. FOIL does provide that NYSERDA may deny access to records or portions thereof that "are trade secrets or are submitted to an agency by a commercial enterprise or derived from information obtained from a commercial enterprise and which if disclosed would cause substantial injury to the competitive position of the subject enterprise." [See Public Officers Law, § 87(2)(d)]. Accordingly, if the Agreement specifically requires submission of information in a format Contractor considers a proprietary and/or confidential trade secret, Contractor shall fully identify and plainly label the information "confidential" or "proprietary" at the time of disclosure. By so marking such information, Contractor represents that the information has actual or potential specific commercial or competitive value to the competitors of Contractor. Without limitation, information will not be considered confidential or proprietary if it is or has been (i) generally known or available from other sources without obligation concerning its confidentiality; (ii) made available by the owner to others without obligation concerning its confidentiality; or (iii) already available to

NYSERDA without obligation concerning its confidentiality. In the event of a FOIL request, it is NYSERDA's policy to consider records as marked above pursuant to the trade secret exemption procedure set forth in 21 New York Codes Rules & Regulations § 501.6 and any other applicable law or regulation. However, NYSERDA cannot guarantee the confidentiality of any information submitted. More information on FOIL, and the relevant statutory law and regulations, can be found at the website for the Committee on Open Government (http://www.dos.state.ny.us/coog/foil2.html) and NYSERDA's Regulations, Part 501 (http://www.nyserda.ny.gov/en/About/~/media/Files/About/Contact/NYSERDARegulations.ashx).

7. IDENTIFYING INFORMATION AND PRIVACY NOTIFICATION. (a) FEDERAL EMPLOYER IDENTIFICATION NUMBER and/or FEDERAL SOCIAL SECURITY NUMBER. As a condition to NYSERDA's obligation to pay any invoices submitted by Contractor pursuant to this Agreement, Contractor shall provide to NYSERDA its Federal employer identification number or Federal social security number, or both such numbers when the Contractor has both such numbers. Where the Contractor does not have such number or numbers, the Contractor must give the reason or reasons why the payee does not have such number or numbers.

(b) PRIVACY NOTIFICATION**.** The authority to request the above personal information from a seller of goods or services or a lessor of real or personal property, and the authority to maintain such information, is found in Section 5 of the State Tax Law. Disclosure of this information by Contractor to the State is mandatory. The principal purpose for which the information is collected is to enable the State to identify individuals, businesses and others who have been delinquent in filing tax returns or may have understated their tax liabilities and to generally identify persons affected by the taxes administered by the Commissioner of Taxation and Finance. The information will be used for tax administration purposes and for any other purpose authorized by law.

8. CONFLICTING TERMS. In the event of a conflict between the terms of the Agreement (including any and all attachments thereto and amendments thereof) and the terms of this Exhibit C, the terms of this Exhibit C shall control.

9. GOVERNING LAW. This Agreement shall be governed by the laws of the State of New York except where the Federal supremacy clause requires otherwise.

10. NO ARBITRATION. Disputes involving this Agreement, including the breach or alleged breach thereof, may not be submitted to binding arbitration (except where statutorily required) without the NYSERDA's written consent, but must, instead, be heard in a court of competent jurisdiction of the State of New York.

11. SERVICE OF PROCESS. In addition to the methods of service allowed by the State Civil Practice Law and Rules ("CPLR"), Contractor hereby consents to service of process upon it by registered or certified mail, return receipt requested. Service hereunder shall be complete upon Contractor's actual receipt of process or upon NYSERDA's receipt of the return thereof by the United States Postal Service as refused or undeliverable. Contractor must promptly notify NYSERDA, in writing, of each and every change of address to which service of process can be

made. Service by NYSERDA to the last known address shall be sufficient. Contractor will have thirty (30) calendar days after service hereunder is complete in which to respond.

12. CRIMINAL ACTIVITY. If subsequent to the effectiveness of this Agreement, NYSERDA comes to know of any allegation previously unknown to it that the Contractor or any of its principals is under indictment for a felony, or has been, within five (5) years prior to submission of the Contractor's proposal to NYSERDA, convicted of a felony, under the laws of the United States or Territory of the United States, then NYSERDA may exercise its stop work right under this Agreement. If subsequent to the effectiveness of this Agreement, NYSERDA comes to know of the fact, previously unknown to it, that Contractor or any of its principals is under such indictment or has been so convicted, then NYSERDA may exercise its right to terminate this Agreement. If the Contractor knowingly withheld information about such an indictment or conviction, NYSERDA may declare the Agreement null and void and may seek legal remedies against the Contractor and its principals. The Contractor or its principals may also be subject to penalties for any violation of law which may apply in the particular circumstances. For a Contractor which is an association, partnership, corporation, or other organization, the provisions of this paragraph apply to any such indictment or conviction of the organization itself or any of its officers, partners, or directors or members of any similar governing body, as applicable.

13. PERMITS. It is the responsibility of the Contractor to acquire and maintain, at its own cost, any and all permits, licenses, easements, waivers and permissions of every nature necessary to perform the work.

14. PROHIBITION ON PURCHASE OF TROPICAL HARDWOODS. The Contractor certifies and warrants that all wood products to be used under this Agreement will be in accordance with, but not limited to, the specifications and provisions of State Finance Law Section 165 (Use of Tropical Hardwoods), which prohibits purchase and use of tropical hardwoods, unless specifically exempted by NYSERDA.

15. OMNIBUS PROCUREMENT ACT OF 1992. It is the policy of New York State to maximize opportunities for the participation of New York State business enterprises, including minority and women-owned business enterprises as bidders, subcontractors and suppliers on its procurement contracts.

Information on the availability of New York State subcontractors and suppliers is available from:

NYS Department of Economic Development
Division for Small Business
30 South Pearl St -- 7th Floor
Albany, New York 12245
Telephone: 518-292-5220
Fax: 518-292-5884
http://www.esd.ny.gov

A directory of certified minority and women-owned business enterprises is available from:

NYS Department of Economic Development
Division of Minority and Women's Business Development
30 South Pearl St -- 2nd Floor
Albany, New York 12245
Telephone: 518-292-5250
Fax: 518-292-5803
http://www.empire.state.ny.us

The Omnibus Procurement Act of 1992 requires that by signing this Agreement, Contractors certify that whenever the total amount is greater than $1 million:

(a) The Contractor has made reasonable efforts to encourage the participation of New York State Business Enterprises as suppliers and subcontractors, including certified minority and women-owned business enterprises, on this project, and has retained the documentation of these efforts to be provided upon request to the State;

(b) The Contractor has complied with the Federal Equal Opportunity Act of 1972 (P.L. 92-261), as amended;

(c) The Contractor agrees to make reasonable efforts to provide notification to New York State residents of employment opportunities on this project through listing any such positions with the Job Service Division of the New York State Department of Labor, or providing such notification in such manner as is consistent with existing collective bargaining contracts or agreements. The Contractor agrees to document these efforts and to provide said documentation to the State upon request; and

(d) The Contractor acknowledges notice that the State may seek to obtain offset credits from foreign countries as a result of this contract and agrees to cooperate with the State in these efforts.

16. RECIPROCITY AND SANCTIONS PROVISIONS. Bidders are hereby notified that if their principal place of business is located in a country, nation, province, state or political subdivision that penalizes New York State vendors, and if the goods or services they offer will be substantially produced or performed outside New York State, the Omnibus Procurement Act 1994 and 2000 amendments (Chapter 684 and Chapter 383, respectively) require that they be denied contracts which they would otherwise obtain. NOTE: As of May 15, 2002, the list of discriminatory jurisdictions subject to this provision includes the states of South Carolina, Alaska, West Virginia, Wyoming, Louisiana and Hawaii. Contact NYS Department of Economic Development for a current list of jurisdictions subject to this provision.

17. COMPLIANCE WITH NEW YORK STATE INFORMATION SECURITY BREACH AND NOTIFICATION ACT. Contractor shall comply with the provisions of the New York State Information Security Breach and Notification Act (General Business Law Section 899-aa; State Technology Law Section 208).

18. PROCUREMENT LOBBYING. To the extent this Agreement is a "procurement contract" as defined by State Finance Law Sections 139-j and 139-k, by signing this Agreement the Contractor certifies and affirms that all disclosures made in accordance with State Finance

Law Sections 139-j and 139-k are complete, true and accurate. In the event such certification is found to be intentionally false or intentionally incomplete, NYSERDA may terminate the agreement by providing written notification to the Contractor in accordance with the terms of the agreement.

19. COMPLIANCE WITH TAX LAW SECTION 5-a. The following provisions apply to Contractors that have entered into agreements in an amount exceeding $100,000 for the purchase of goods and services:

a) Before such agreement can take effect, the Contractor must have on file with the New York State Department of Taxation and Finance a Contractor Certification form (ST-220-TD).

b) Prior to entering into such an agreement, the Contractor is required to provide NYSERDA with a completed Contractor Certification to Covered Agency form (Form ST-220-CA).

c) Prior to any renewal period (if applicable) under the agreement, the Contractor is required to provide NYSERDA with a completed Form ST-220-CA.

Certifications referenced in paragraphs (b) and (c) above will be maintained by NYSERDA and made a part hereof and incorporated herein by reference.

NYSERDA reserves the right to terminate this agreement in the event it is found that the certification filed by the Contractor in accordance with Tax Law Section 5-a was false when made.

20. IRANIAN ENERGY SECTOR DIVESTMENT. In accordance with Section 2879-c of the Public Authorities Law, by signing this contract, each person and each person signing on behalf of any other party certifies, and in the case of a joint bid or partnership each party thereto certifies as to its own organization, under penalty of perjury, that to the best of its knowledge and belief that each person is not on the list created pursuant to paragraph (b) of subdivision 3 of section 165-a of the State Finance Law (See www.ogs.ny.gov/about/regs/ida.asp).

EXHIBIT D

NYSERDA PROMPT PAYMENT POLICY STATEMENT

504.1. Purpose and Applicability. (a) The purpose of this Exhibit is to provide a description of Part 504 of NYSERDA's regulations, which consists of NYSERDA's policy for making payment promptly on amounts properly due and owing by NYSERDA under this Agreement. The section numbers used in this document correspond to the section numbers appearing in Part 504 of the regulations.[2]

(b) This Exhibit applies generally to payments due and owing by the NYSERDA to the Contractor pursuant to this Agreement. However, this Exhibit does not apply to Payments due and owing when NYSERDA is exercising a Set-Off against all or part of the Payment, or if a State or Federal law, rule or regulation specifically requires otherwise.

504.2. Definitions. Capitalized terms not otherwise defined in this Exhibit shall have the same meaning as set forth earlier in this Agreement. In addition to said terms, the following terms shall have the following meanings, unless the context shall indicate another or different meaning or intent:

(a) "Date of Payment" means the date on which NYSERDA requisitions a check from its statutory fiscal agent, the Department of Taxation and Finance, to make a Payment.

(b) "Designated Payment Office" means the Office of NYSERDA's Controller, located at 17 Columbia Circle, Albany, New York 12203.

(c) "Payment" means payment properly due and owing to Contractor pursuant to Article IV, Exhibit B of this Agreement.

(d) "Prompt Payment" means a Payment within the time periods applicable pursuant to Sections 504.3 through 504.5 of this Exhibit in order for NYSERDA not to be liable for interest pursuant to Section 504.6.

(e) "Payment Due Date" means the date by which the Date of Payment must occur, in accordance with the provisions of Sections 504.3 through 504.5 of this Exhibit, in order for NYSERDA not to be liable for interest pursuant to Section 504.6.

(f) "Proper Invoice" means a written request for Payment that is submitted by a Contractor setting forth the description, price or cost, and quantity of goods, property or services delivered or rendered, in such form, and supported by such other substantiating documentation, as NYSERDA may reasonably require, including but not limited to any requirements set forth in Exhibits A or B to this Agreement; and addressed to NYSERDA's Controller, marked "Attention: Accounts Payable," at the Designated Payment Office.

(g)(1) "Receipt of an Invoice" means:

---

[2] This is only a summary; the full text of Part 504 can be accessed at: http://www.nyserda.ny.gov/en/About/~/media/Files/About/Contact/NYSERDARegulations.ashx)

(i) if the Payment is one for which an invoice is required, the later of:

(a) the date on which a Proper Invoice is actually received in the Designated Payment Office during normal business hours; or

(b) the date by which, during normal business hours, NYSERDA has actually received all the purchased goods, property or services covered by a Proper Invoice previously received in the Designated Payment Office.

(ii) if the Agreement provides that a Payment will be made on a specific date or at a predetermined interval, without having to submit a written invoice the 30th calendar day, excluding legal holidays, before the date so specified or predetermined.

(2) For purposes of this subdivision, if the Agreement requires a multifaceted, completed or working system, or delivery of no less than a specified quantity of goods, property or services and only a portion of such systems or less than the required goods, property or services are working, completed or delivered, even though the Contractor has invoiced NYSERDA for the portion working, completed or delivered, NYSERDA will not be in Receipt of an Invoice until the specified minimum amount of the systems, goods, property or services are working, completed or delivered.

(h) "Set-off" means the reduction by NYSERDA of a payment due a Contractor by an amount equal to the amount of an unpaid legally enforceable debt owed by the Contractor to NYSERDA.

504.3. Prompt Payment Schedule. Except as otherwise provided by law or regulation or in Sections 504.4 and 504.5 of this Exhibit, the Date of Payment by NYSERDA of an amount properly due and owing under this Agreement shall be no later than thirty (30) calendar days, excluding legal holidays, after Receipt of a Proper Invoice.

504.4. Payment Procedures.

(a) Unless otherwise specified in this Agreement, a Proper Invoice submitted by the Contractor to the Designated Payment Office shall be required to initiate payment for goods, property or services. As soon as any invoice is received in the Designated Payment Office during normal business hours, such invoice shall be date-stamped. The invoice shall then promptly be reviewed by NYSERDA.

(b) NYSERDA shall notify the Contractor within fifteen (15) calendar days after Receipt of an Invoice of:

(1) any defects in the delivered goods, property or services;

(2) any defects in the invoice; or

(3) suspected improprieties of any kind.

(c) The existence of any defects or suspected improprieties shall prevent the commencement of the time period specified in Section 504.3 until any such defects or improprieties are corrected or otherwise resolved.

(d) If NYSERDA fails to notify a Contractor of a defect or impropriety within the fifteen (15) calendar day period specified in subdivision (b) of this section, the sole effect shall be that the number of days allowed for Payment shall be reduced by the number of days between the 15th day and the day that notification was transmitted to the Contractor. If NYSERDA fails to provide reasonable grounds for its contention that a defect or impropriety exists, the sole effect shall be that the Payment Due Date shall be calculated using the original date of Receipt of an Invoice.

(e) In the absence of any defect or suspected impropriety, or upon satisfactory correction or resolution of a defect or suspected impropriety, NYSERDA shall make Payment, consistent with any such correction or resolution and the provisions of this Exhibit.

504.5. Exceptions and Extension of Payment Due Date. NYSERDA has determined that, notwithstanding the provisions of Sections 504.3 and 504.4 of this Exhibit, any of the following facts or circumstances, which may occur concurrently or consecutively, reasonably justify extension of the Payment Due Date:

(a) If this Agreement provides Payment will be made on a specific date or at a predetermined interval, without having to submit a written invoice, if any documentation, supporting data, performance verification, or notice specifically required by this Agreement or other State or Federal mandate has not been submitted to NYSERDA on a timely basis, then the Payment Due Date shall be extended by the number of calendar days from the date by which all such matter was to be submitted to NYSERDA and the date when NYSERDA has actually received such matter.

(b) If an inspection or testing period, performance verification, audit or other review or documentation independent of the Contractor is specifically required by this Agreement or by other State or Federal mandate, whether to be performed by or on behalf of NYSERDA or another entity, or is specifically permitted by this Agreement or by other State or Federal provision and NYSERDA or other entity with the right to do so elects to have such activity or documentation undertaken, then the Payment Due Date shall be extended by the number of calendar days from the date of Receipt of an Invoice to the date when any such activity or documentation has been completed, NYSERDA has actually received the results of such activity or documentation conducted by another entity, and any deficiencies identified or issues raised as a result of such activity or documentation have been corrected or otherwise resolved.

(c) If an invoice must be examined by a State or Federal agency, or by another party contributing to the funding of the Contract, prior to Payment, then the Payment Due Date shall be extended by the number of calendar days from the date of Receipt of an Invoice to the date when the State or Federal agency, or other contributing party to the Contract, has completed the inspection, advised NYSERDA of the results of the inspection, and any deficiencies identified or issues raised as a result of such inspection have been corrected or otherwise resolved.

(d) If appropriated funds from which Payment is to be made have not yet been

appropriated or, if appropriated, not yet been made available to NYSERDA, then the Payment Due Date shall be extended by the number of calendar days from the date of Receipt of an Invoice to the date when such funds are made available to NYSERDA.

504.6. Interest Eligibility and Computation. If NYSERDA fails to make Prompt Payment, NYSERDA shall pay interest to the Contractor on the Payment when such interest computed as provided herein is equal to or more than ten dollars ($10.00). Interest shall be computed and accrue at the daily rate in effect on the Date of Payment, as set by the New York State Tax Commission for corporate taxes pursuant to Section 1096(e)(1) of the Tax Law. Interest on such a Payment shall be computed for the period beginning on the day after the Payment Due Date and ending on the Date of Payment.

504.7. Sources of Funds to Pay Interest. Any interest payable by NYSERDA pursuant to Exhibit shall be paid only from the same accounts, funds, or appropriations that are lawfully available to make the related Payment.

504.8. Incorporation of Prompt Payment Policy Statement into Contracts. The provisions of this Exhibit shall apply to all Payments as they become due and owing pursuant to the terms and conditions of this Agreement, notwithstanding that NYSERDA may subsequently amend its Prompt Payment Policy by further rulemaking.

504.9. Notice of Objection. Contractor may object to any action taken by NYSERDA pursuant to this Exhibit that prevents the commencement of the time in which interest will be paid by submitting a written notice of objection to NYSERDA. Such notice shall be signed and dated and concisely and clearly set forth the basis for the objection and be addressed to the Vice President, New York State Energy Research and Development Authority, at the notice address set forth in Exhibit B to this Agreement. The Vice President of NYSERDA, or his or her designee, shall review the objection for purposes of affirming or modifying NYSERDA‘s action. Within fifteen (15) working days of the receipt of the objection, the Vice President, or his or her designee, shall notify the Contractor either that NYSERDA‘s action is affirmed or that it is modified or that, due to the complexity of the issue, additional time is needed to conduct the review; provided, however, in no event shall the extended review period exceed thirty (30) working days.

504.10. Judicial Review. Any determination made by NYSERDA pursuant to this Exhibit that prevents the commencement of the time in which interest will be paid is subject to judicial review in a proceeding pursuant to Article 78 of the Civil Practice Law and Rules. Such proceedings shall only be commenced upon completion of the review procedure specified in Section 504.9 of this Exhibit or any other review procedure that may be specified in this Agreement or by other law, rule, or regulation.

504.11. Court Action or Other Legal Processes.

(a) Notwithstanding any other law to the contrary, the liability of NYSERDA to make an interest payment to a Contractor pursuant to this Exhibit shall not extend beyond the date of a notice of intention to file a claim, the date of a notice of a claim, or the date commencing a legal action for the payment of such interest, whichever occurs first.

(b) With respect to the court action or other legal processes referred to in subdivision (a) of this section, any interest obligation incurred by NYSERDA after the date specified therein pursuant to any provision of law other than Public Authorities Law Section 2880 shall be determined as prescribed by such separate provision of law, shall be paid as directed by the court, and shall be paid from any source of funds available for that purpose.

EXHIBIT E

Rate Sheet

DIRECT PERSONNEL COSTS:

Sample Title Classifications	Not to Exceed Hourly Rate Range (fully burdened)											
	2017		2018		2019		2020		2021		2022	
	Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.
Principal												
Senior Manager												
Project Manager												
Coordinator II												
Coordinator I												
Administrative												

DIRECT NON-PERSONAL SERVICE COSTS:

Direct non-personal service costs will be allowed and reimbursed at cost for project related expenses. Items not listed but necessary to complete the work must be pre-approved by NYSERDA:

Travel Postage Supplies

Exhibit F

Employment Policies and Procedures Applicable to Temporary and Leased Employees

The following policies and procedures are applicable to temporary and/or leased employees while on assignment at NYSERDA. For purposes of this document, the terms "Employee(s)" shall, in each case that it appears, mean the temporary/leased employee identified below. By signing, the temporary/leased employee agrees to abide by such policies and procedures.

EQUAL OPPORTUNITY

POLICY

NYSERDA prohibits discrimination in employment practices – including hiring, firing, promotion, compensation, and other terms, privileges, and conditions of employment against any individual on the basis of race, color, creed, sex, sexual orientation, gender identity, familial status, marital status, age, national origin, disability, pregnancy, childbirth or a related medical condition, military status, predisposing genetic characteristics, domestic violence victim status, prior conviction records, or prior arrests, youthful offender adjudications or sealed records or any other basis prohibited by law. NYSERDA is committed to the principle that employment decisions be based on merit, qualifications and abilities, and expects all employees to act in accordance with this Policy.

As part of the company's Equal Employment Opportunity policy, NYSERDA will also take affirmative action as called for by applicable laws and Executive Orders to ensure that minority group individuals, females, disabled veterans, recently separated veterans, other protected veterans, Armed Forces service medal veterans, and qualified disabled persons are introduced into our workforce and considered for promotional opportunities.

Employees and applicants can raise concerns and make reports and shall not be subjected to harassment, intimidation or any type of retaliation because they have (1) filed a complaint; (2) assisted or participated in an investigation, compliance review, hearing or any other activity related to the administration of any federal, state or local law requiring equal employment opportunity; (3) opposed any act or practice made unlawful by any federal, state or local law requiring equal opportunity; or (4) exercised any other employment right protected by federal, state or local law or its implementing regulations. (See Personnel Handbook Section 2)

Any employee in a position of supervision, leadership or authority who becomes aware of conduct that may constitute a violation of this Policy must report such information to the Affirmative Action Officer Regional Team Leader. This obligation exists regardless of the desire of an individual to keep such information private and regardless of the individual's assessment of the veracity of the claim.

Any employee, whether in a supervisory role or not, who witnesses or is personally subjected to harassment and/or discrimination should: (a) fill out a complaint form, which is available on NYSERDA's SharePoint Intranet, Human Resources Forms Page, and (b) contact an independent

Affirmative Action Officer Regional Team Leader for their Region (Albany, NYC or West Valley & Buffalo):

Regional Team Leaders
Albany Region - OGS Diversity and Equal Employment Office; DEEO@ogs.ny.gov or by fax at (518) 474-9211.

NYC Region - Allison Clavery: (212) 480-7717 or Allison.Clavery@dfs.ny.gov.

West Valley and Buffalo Region - Matthew Chiesa: (518) 408-0071 or Matthew.Chiesa@omig.ny.gov.

The Team Leader can explain the investigative procedure and respond to any questions that you may have.

Complaints shall be investigated and resolved fairly, promptly and thoroughly. The privacy of those involved will be preserved to the extent possible under the law and consistent with a full and fair investigation and appropriate remedial or disciplinary action.

If there is a determination that remedial or disciplinary action is warranted, such action may include oral or written reprimand, transfer, education programs, fines, suspension, demotion or termination.

The Affirmative Action Policy overseeing NYSERDA's employment practices is derived from relevant federal and State law, and from the Chair's and President and CEO's personal commitments.

POLICY REGARDING THE AMERICANS WITH DISABILITIES ACT

The State of New York and NYSERDA are committed to assuring equal employment opportunity for persons with disabilities. To this end, it is the State's policy to provide reasonable accommodation to a qualified person with a disability to enable such person to perform the essential functions of the State government position for which he or she is applying, or in which he or she is employed. This policy is based on the New York State Human Rights Law, Sections 503/504 of the Federal Rehabilitation Act of 1973 as amended, the Americans with Disabilities Act (ADA), and all applicable Executive Orders and Memoranda. The policy applies to all employment practices and actions. It includes, but is not limited to, recruitment, the job application process, examination and testing, hiring, training, disciplinary actions, rates of pay or other compensation, advancement, classification, transfer and reassignment, and promotions. The Director of Human Resources is NYSERDA's Designee for Reasonable Accommodation (DRA).

To request an accommodation, let the employer know that you need an adjustment or change in applying for a positions or at work for a reason related to a medical condition. Current employees may request an accommodation through either their supervisor or the DRA. If an employee makes his or her request through the supervisor, the supervisor may handle and approve the request, but only after consultation with and approval by the DRA. However, since certain determinations may require a more complex analysis, or may involve agency expenditures, the supervisor shall forward the request to the DRA for handling where so directed.

Reasonable Accommodation Request Forms are posted on NYSERDA's SharePoint, Human Resources Forms page.

POLICY REGARDING RELIGIOUS OBSERVANCES OR PRACTICES

The State of New York and NYSERDA are committed to assuring equal employment opportunity for persons who engage in religious observances or practices. To this end, it is the State's policy to provide reasonable accommodation for religious observances or practices. This policy is based on the New York State Human Rights Law, the federal Civil Rights Act of 1964, Title VII, and all applicable Executive Orders and Memoranda. The policy applies to all employment practices and actions. It includes, but is not limited to, recruitment, the job application process, examination and testing, hiring, training, disciplinary actions, rates of pay or other compensation, advancement, classification, transfer and reassignment, promotions, and other terms, condition or privileges of employment. The Director of Human Resources is NYSERDA's Designee for Reasonable Accommodation (DRA).

To request an accommodation, an individual need only let the employer know that s/he needs a change or adjustment related to a religious observance or practice. Current employees may request a religious accommodation through either their supervisor or the DRA. If an employee makes his or her request through the supervisor, the supervisor may handle and approve the request, with consultation with the DRA as needed. When the request cannot be granted, the supervisor shall forward the request to the DRA, to assure that the request is reviewed, documented, and resolved in accordance with policy and governing statutes.

Reasonable Accommodation Request Forms are posted on NYSERDA's SharePoint, Human Resources Forms page.

ANTI-HARASSMENT POLICY AND COMPLAINT PROCEDURE

ANTI- HARASSMENT POLICY

NYSERDA prohibits unlawful harassment in the workplace. Harassment based on race, ethnicity, color, creed, sex, sexual orientation, gender identity, familial status, marital status, age, national origin, disability, military status, predisposing genetic characteristics, domestic violence victim status or any other basis is against the law. Unlawful harassment is a violation of the Federal Civil Rights Act of 1964 and the New York State Human Rights Law and will not be tolerated. In addition, retaliation against an individual who opposes discrimination or participates in a complaint proceeding is also a violation and will not be tolerated. The Anti-Harassment Policy applies to the workplace during all hours, to all work related social functions, whether on or off NYSERDA premises, and to business related travel.

All employees, and particularly employees with supervisory responsibilities, are responsible for ensuring a work environment free from all forms of harassment, including sexual harassment. All employees are expected to avoid any behavior or conduct that could be interpreted as harassment or sexual harassment.

Although NYSERDA recognizes that working relationships often foster social relationships, it strongly discourages sexually or romantically intimate relationships between individuals where a direct supervisory relationship exists. In such cases, NYSERDA may take steps to eliminate such a supervisory relationship.

NYSERDA considers unlawful harassment to be a form of employee misconduct. Employees and managers who violate NYSERDA's Anti-Harassment Policy will be subject to discipline, up to and including termination of employment.

No supervisor shall threaten or insinuate, either explicitly or implicitly, that an employee's submission to or rejection of sexual advances will in any way influence any personnel decision regarding that employee's employment, compensation, advancement, assigned duties, or any other condition of employment or career development.

NYSERDA has and will continue to require periodic training concerning sexual harassment prevention.

If any staff member feels that he or she has witnessed or has been subject to any behavior that constitutes sexual harassment, he or she should file a complaint pursuant to the procedures provided for in Section 5 of this handbook, and below. **If the staff member is in a supervisory role, he or she is obligated to file a complaint pursuant to these stated procedures.**

WHAT IS HARASSMENT?

Harassment is a form of discrimination and includes communicating, sharing or displaying written or visual material, making verbal comments and/or engaging in any other conduct, including physical conduct, which is demeaning or derogatory to an employee, applicant, contractor or visitor because of his or her: gender, race, color, religion, national origin, age, familial status, marital status, sexual orientation, pregnancy, disability, citizenship, veteran status or any other class protected by applicable federal, state or local laws, including material, comments or conduct intended as humor. The use of NYSERDA facilities, property or equipment to disseminate, duplicate or display such materials is prohibited by NYSERDA policy.

EXAMPLES OF HARASSMENT

Prohibited harassment on the basis of gender, race, color, religion, national origin, age, familial status, marital status, sexual orientation, pregnancy, disability, citizenship, veteran status, or any other protected bases, includes behavior similar to sexual harassment such as:

- Verbal conduct such as threats, epithets, derogatory comments/whistles etc, pranks, intimidation, jokes or slurs;
- Visual conduct such as derogatory posters, photographs, videos, cartoons, drawings, or gestures;
- Physical conduct such as assault, unwanted touching, violence or blocking normal movement, and;
- Retaliation for reporting harassment or threatening to report harassment.

WHAT IS SEXUAL HARASSMENT?

Sexual Harassment includes making unwelcome and unwanted sexual advances, unwelcome or inappropriate comments regarding physical appearance, requesting sexual favors in exchange for favorable treatment or continued employment, engaging in verbal or physical conduct of a sexual nature which is made a term or condition of employment, or which is used as the basis for employment decisions. Sexual Harassment also includes any type of unwelcome sexually-oriented conduct, including unwelcome sexual jokes or physical contact that has the purpose or effect of interfering with an employee's work performance or creating a work environment that is intimidating, hostile, offensive or coercive to a reasonable person. Sexual Harassment is not limited to male-female interaction.

EXAMPLES OF SEXUAL HARASSMENT

Depending on the circumstance, sexual harassment may include, but is not limited to, explicit sexual propositions, sexual innuendo, suggestive comments, statements regarding appearance or dress, sexually oriented "kidding" or "teasing," "practical jokes," jokes about gender-specific traits, obscene language or

gestures, display of obscene or sexually suggestive printed or visual material (including emails, images and videos), physical conduct such as any touching, patting, pinching, or brushing against another's body, obscene or sexually oriented computer or phone mail messages, or suggestive or obscene letters, notes, or invitations. These descriptions comprise only a partial list of conduct that may be considered sexual harassment. Any questions about the legal definition of whether some particular behavior constitutes sexual harassment should be referred to the Director of Human Resources or to the Office of Counsel.

HARASSMENT COMPLAINT PROCEDURE

NYSERDA's goal is to discourage inappropriate behavior at the source and as soon as possible. Employees are encouraged to speak directly with persons exhibiting behavior that makes them uncomfortable. Communicate politely, clearly and firmly to the offending party that the conduct is unwelcome, unwanted, offensive, intimidating, or embarrassing and ask that the conduct stop.

Any staff member who believes he/she is being harassed, or who observes harassment or retaliation, should, and in such a case any supervisor *must*:

(a) fill out a complaint form, which is available on NYSERDA's SharePoint Intranet, Human Resources Forms Page [http://intranet.nyserda.org/HR%20Forms/Human%20Resources.aspx], and,

(b) contact an Affirmative Action Officer (AAO) Regional Team Leader for their Region (Albany, NYC or West Valley & Buffalo).

Contact information for AAO's is as follows:

Albany Region - OGS Diversity and Equal Employment Office; DEEO@ogs.ny.gov or by fax at (518) 474-9211.

NYC Region - Allison Clavery: (212) 480-7717 or Allison.Clavery@dfs.ny.gov.

West Valley and Buffalo Region - Matthew Chiesa: (518) 408-0071 or Matthew.Chiesa@omig.ny.gov.

The Team Leader can explain the investigative procedure and respond to any questions that you may have.

Complaints shall be investigated and resolved fairly, promptly and thoroughly. The privacy of those involved will be preserved to the extent possible under the law, and consistent with a full and fair investigation and appropriate remedial or disciplinary action.

If there is a determination that remedial or disciplinary action is warranted, such action may include oral or written reprimand, transfer, education programs, fines, suspension, demotion or termination.

Any employee in a position of supervision, leadership or authority who becomes aware of conduct that may constitute a violation of this Policy must report such information to the Affirmative Action Officer Regional Team Leader for their Region. This obligation exists regardless of the desire of an individual to keep such information private and regardless of the individual's assessment of the veracity of the claim.

WHO CAN BE HELD LIABLE FOR DISCRIMINATION OR HARASSMENT?

Supervisors and employees may be held both individually and jointly liable for acts of discrimination and harassment under anti-discrimination and harassment laws.

EMERGENCY, FIRE SAFETY AND SECURITY

REPORTING AN EMERGENCY

In the event of an emergency situation, press “8” on any office phone, and then dial 911.Give the operator the following information: your name and the exact description and location of the incident you are reporting so proper emergency personnel and equipment can be dispatched to handle the situation.

If it is a fire condition, you should close doors closest to you in an attempt to contain it and leave the area by the nearest safe exit.

EVACUATION PROCEDURE

At the sound of the fire alarm:

1. Immediately terminate all telephone conversation.
2. Close all desk and file cabinet drawers.
3. Secure all monies, checks, etc., and other State funds of instruments.
4. Take your coat and pocketbook and leave. Do not bring coffee cups, soda, etc.
5. Leave office lights on and close the door behind you.
6. Use stairways and not the elevator.
7. Calmly escort all visitors to safety with you.
8. Only disabled persons should use the elevator.
9. Leave the building. Assemble in areas far enough from the building to allow easy access by emergency personnel.
10. You can best assist in the evacuation by not attempting to fight a fire or handle an emergency. Personal safety is paramount. However, in the case of small, manageable fires, there are fire extinguishers located throughout the offices for use by personnel.

Staff must familiarize themselves with the location of fire exits near their workspace in the event of a fire or evacuation. NYSERDA shall conduct periodic evacuation drills, generally not less than semiannually, which shall be coordinated by the Facility Manager.

WEST VALLEY OFFICE

NYSERDA employees performing work at the Western New York Nuclear Service Center must complete worker orientation as provided by either the West Valley Demonstration Project or NYSERDA's West Valley Site Management Program, depending upon the location in which the work will be performed. This worker orientation includes site specific emergency and fire safety information, and should be completed prior to beginning any unescorted work.

BUILDING SECURITY AND ACCESS

Staff are not permitted to introduce, use or possess a firearm or deadly weapon on NYSERDA property or in NYSERDA offices as defined by New York State Penal Law Section 10.00.

Security cameras are installed at some NYSERDA locations for the safety and security of NYSERDA staff.

All staff are provided with a key or keycard for access to NYSERDA offices. Staff should not attempt to copy or duplicate keys or keycards. If keys or keycards are lost or stolen, staff should see the Facility Manager for a replacement. All previous keycards will be deactivated to prevent unlawful access.

Any visitor(s) to NYSERDA should be directed to sign in at the reception desk and indicate to the receptionist who their appointment is with. That employee will be contacted and should escort the visitor(s) to the area where business will be conducted. The visitor should then be escorted back to the reception area for proper exit from the building.

Visitors should not be invited to NYSERDA during off hours. If necessary for a visitor to be on premises during off hours, s/he must be accompanied by a NYSERDA employee at all times and sign in at the reception desk even though a receptionist is not present.

WORKPLACE VIOLENCE PREVENTION PROGRAM

PURPOSE

In accordance with New York State Labor Law, Section 27-b, "Duty of Public Employers to Develop and Implement Programs to Prevent Workplace Violence," public employers are required to perform a workplace evaluation or risk evaluation at each worksite, and to develop and implement programs to prevent, minimize and respond to incidents of Workplace Violence. The law is designed to ensure that the risk of workplace assaults and homicides are regularly evaluated by employers and that workplace violence protection programs are implemented to prevent and minimize the hazard to public employees. The New York State Department of Labor (DOL) has issued regulations designed to implement Section 27-b, at 12 NYCRR Part 800.6. Both Section 27-b and DOL's regulations require agencies and authorities to develop and implement a written workplace violence prevention program. This document constitutes NYSERDA's written program.

POLICY

NYSERDA endeavors to ensure that its workforce is free from violence, threats of violence, harassment, intimidation, and disruption. The Authority will not tolerate any acts of violence in the workplace. NYSERDA is committed to the following:

- Fostering a non-hostile work environment and encouraging positive work relationships
- Reducing the risk of violence in the workplace and ensuring employees' personal safety
- Responding immediately and effectively to threats or acts of violence
- Promoting the resolution of conflict
- Providing regular training for all employees on NYSERDA's workplace violence prevention program

NYSERDA will take action against any conduct that violates employee safety and will support any employee who becomes a target of such behavior while at work.

Offenders may be removed from the premises and employees subjected to appropriate disciplinary action up to and including termination. When necessary, NYSERDA will refer cases to law enforcement authorities for appropriate action. NYSERDA will also endeavor to prohibit domestic violence or abuse from intruding into the workplace and to ensure that our policies and procedures are responsive to the needs of and do not discriminate against the victims of domestic violence.

New York State Department of Labor regulations define workplace violence as: any physical assault or acts of aggressive behavior occurring where a public employee performs any work-related duty in the course of his or her employment including but not limited to:

(i) An attempt or threat, whether verbal or physical, to inflict physical injury upon an employee;
(ii) Any intentional display of force which would give an employee reason to fear or expect bodily harm;
(iii) Intentional and wrongful physical contact with a person without his or her consent that entails some injury;
(iv) Stalking an employee with the intent of causing fear of material harm to the physical safety and health of such employee when such stalking has arisen through and in the course of employment.

PROCEDURES

It is the Authority's goal to minimize the opportunities for violence in the workplace. Accordingly, the Authority has adopted the following procedures:

- **Training -** All employees are expected to attend annual training regarding Workplace Violence Prevention. All employees are expected to be familiar with building alarm systems and the steps to maintain their personal safety.
- **Visitors -** All visitors are to sign in and wear a visitor badge. All visitors are to be escorted by an employee at all times. Employees should be alert to anyone loitering near the office for no apparent reason. Do not allow anyone to follow you into the building without checking with the receptionist - This is called tailgating. Employees should not hesitate to ask a person they do not recognize for her or his name and identification. Employees should report any suspicious persons or activities to your supervisor or manager and the Director of Human Resources.
- **Exterior entrances -** All exterior entrances are to be locked at all times from the outside except for the front door. No doors are to be propped open. No emergency exits are to be blocked.
- **Alarm systems -** Alarm systems will be checked at least every six months to ensure that they are in working order by the Facility Manager.
- **Company vehicles -** Employees are not to pick up strangers, hitchhikers or other individuals not well known to them in a company vehicle.
- **Prosecution -** Any individual engaging in violence against the Authority, its employees or its property will be prosecuted to the full extent of the law.
- **Discipline -** Any employee who engages in workplace violence is subject to discipline including immediate discharge. Employees are expected to cooperate with any investigation. Employees who fail or refuse to cooperate may be disciplined, which may include discharge. Any employee who provides false information or omits information during an investigation is subject to discipline including discharge.

<u>Responsibilities of Employees</u>

All employees are responsible for the following:

- Refraining from engaging in workplace violence
- Reporting to supervisors or managers and the Director of Human Resources any dangerous or threatening situations that occur in the workplace

- Bringing to the supervisor's or manager's and the Director of Human Resources' attention any off-premises circumstances that may affect workplace safety such as any court-issued orders of protection.

NYSERDA employees are required to immediately report any threatening, coercive or violent behavior. This includes instances where an employee is impacted by such conduct or witnesses the abuse of others. The obligation of prompt reporting is each employee's responsibility. It is essential to keeping the workplace safe for all. Under-reporting of threats and incidents of violence hinders efforts to increase safety.

In responding to threatening or violent behavior, no employee, either management or staff, should take any action that will compromise his or her own safety or the safety of others. No person, other than law enforcement personnel, should attempt to restrain, remove or forcibly disarm an armed or dangerous person.

In an emergency or a threatening situation in the workplace, the following guidelines are recommended:

Situation	Action
Emergency - immediate threat to your safety or to the safety of others.	1. Secure your own safety 2. Dial 911 and seek medical care if anyone is injured • Provide exact location information (street address & floor of emergency) • Type of emergency 3. Warn others who may be in danger 4. Notify your supervisor or manager and the Director of Human Resources
Situations that do not represent an immediate threat	Report the situation to your supervisor or manager and the Director of Human Resources
Robbery	In the event of a robbery, all money is to be given to the robber and employees are to cooperate fully with the robber's demands. Once safe, call 911 and notify your supervisor or manager and the Director of Human Resources.
Theft	In the event of theft of personal or company property, please report this immediately to the Director of Human Resources and to the Facilities Manager who will take appropriate action
Person says that s/he intends to cause harm to self and/or others	Report immediately to Human Resources
Bomb threats	1. Immediately notify your supervisor or manager and the Director of Human Resources so everyone can be evacuated safely 2. Evacuate to pre-arranged evacuation points

3. Dial 911 and seek medical care if anyone is injured
    - Note specific characteristics of the caller (such as gender, voice quality, accent, if any, background noise, etc.) and time of call
    - Provide specific information relevant to the bomb threat (such as location if stated, time the threat was received and in what manner; what type of explosive if specified, etc.)
4. Take headcount

Explosive material is extremely hazardous and should be handled by Hazardous Device Unit experts only. <u>Do not attempt to handle.</u> If you see what appears to be an explosive device or suspicious package in the workplace, leave the area and report it to the authorities immediately.

<u>Responsibilities of Human Resources</u>

The Director of Human Resources or designee is the Authority's Workplace Violence Prevention Program Administrator. The Director will investigate and coordinate the Authority's response to any report of prohibited conduct.

Human Resources has the following responsibilities:

1. Decide whether to handle the incident within Human Resources or to call in additional resources such as:
    - NYSERDA's Management
    - NYSERDA's Counsel
    - Employee Assistance Program (EAP)
    - Other applicable resources (e.g. law enforcement)

2. Ensure that the Authority's violence response procedures are followed and take steps to minimize harm and trauma

3. Mobilize all necessary resources including threat assessment experts, conflict resolution specialists, security professionals, mental health professionals and counselors, including consultants from outside the State service

4. Organize crisis aftermath measures including trauma counseling

5. Keep the workforce informed about the WPV policy

6. Arrange for periodic skills training and policy education for all employees

7. Provide advice and guidance to all employees

8. Prepare the ability to respond to incidents

9. Conduct post-incident investigations and follow up with appropriate support strategies

Following a workplace violence incident, Human Resources will:

- Consult with and advise managers/supervisors on appropriate actions throughout the process

- Arrange for temporarily relieving a manager/supervisor of regular duties, if necessary, while he or she is dealing with a critical incident
- Assess the situation, taking statements from the first-line supervisor, witnesses, the threatened employee, and the perpetrator, if possible
- Arrange for and/or participate in counseling sessions
- Prepare any disciplinary/adverse action that may be required
- Ensure that good faith reporting does not become a basis for retaliation
- Determine whether additional measures should be implemented to prevent recurrence of similar behavior
- Identify and address any underlying conditions that may have given rise to the incident

When a threat or act of violence is reported, Human Resources will promptly conduct a thorough fact-finding review, to be compiled into the NYSERDA Workplace Violence Incident Report located on NYSERDA's Human Resources SharePoint Page. Fact-finding is not fault finding. Fact-finding is an effort to determine the causes of an incident, find ways to eliminate systemic factors that may be conducive to violence and to prevent a recurrence.

Human Resources' (or its designate) fact-finding procedures may include the following:
• Visit the scene of the incident
• Interview impacted employees and witnesses
• Photograph any physical damage or injuries
• Maintain comprehensive records of the inquiry
• Conduct an analysis based on the facts and reports
• Recommend a course of action.

Since a threat or act of violence is an inherently traumatic experience, victims and others may suffer psychological after effects that result in a decline in work performance and/or problems in an employee's home life. There may be difficulty concentrating or remembering details, panic attacks and a strain in relations with coworkers and supervisors. Witnesses, victims and others may experience trauma, whose effects sometimes do not appear until months after the crisis.

NYSERDA will utilize the resources of its contracted Employee Assistance Program (EAP) based on an assessment of the needs of individual employees or a group of workers. The services provided will be organized by the EAP using community resources and trained professionals where necessary.

Human Resources will review incidents as well as obtain assistance from professional consultants to ascertain possibly dangerous conditions and recommend corrective action and changes in procedures or training.

NYSERDA Human Resources will arrange for training on the prevention of workplace violence including periodic training to update skills.

Training will cover the following topics:
- Requirements of the regulation
- Review of NYSERDA's policy and guidelines – where it is kept and how to obtain a copy
- Risk factors found and the most common causes of violence
- How employees can protect themselves and review of the work controls, procedures, devices or practices employees can use to protect themselves
- Awareness and recognition of warning signs
- Skills for resolving conflict and monitoring the climate of the workplace

- Procedures for obtaining crisis counseling, use of EAP and other resources

POLICY REGARDING ALCOHOL AND CONTROLLED SUBSTANCES IN THE WORKPLACE

It is the policy of NYSERDA that employees are prohibited from manufacturing, distributing, selling, attempting to sell, possessing or purchasing controlled substances, and from using non-prescribed controlled substances while at the workplace or while performing in a work-related capacity. Employees doing so will be subject to criminal, civil and disciplinary penalties. Such illegal acts, even if engaged in while off duty, may result in disciplinary action. An employee may possess and use a controlled substance which is properly prescribed for him or her by a physician. Employees are also prohibited from the use of or impairment from alcohol or controlled substances while on the job or on the work site at any time.

An employee may be required to undergo a confidential medical examination to ascertain the cause of impairment or disability when there exists a "reasonable suspicion," based on specific, reliable observations, that such impairment or disability is a result of the use of alcohol or a controlled substance. If alcohol or controlled substance use or impairment is found to exist, NYSERDA will determine the appropriate course of action, which may include disciplinary action, referral to the Employee Assistance Program, or the use of disability leave procedures.

The Federal Drug-Free Workplace Act of 1988, amended in 1994, requires that all agencies that have contracts with the United States Government that exceed $100,000, and all agencies that receive Federal grants, maintain a drug-free workplace. If an employee is involved in work on a contract or grant covered by this law, they are required to notify the Director of Human Resources in writing of any criminal drug statute conviction, for a violation occurring in the workplace or at a work site, not less than five days after the conviction. Agencies covered by this law must notify the Federal government of the conviction and must take personnel action against an employee convicted of a drug abuse violation.

<u>Drug Addiction and Alcoholism under the Human Rights Law and Regulations.</u>

An individual who is currently using drugs illegally is not protected under the disability provisions of the Human Rights Law. A test to determine the illegal use of drugs is not considered a medical test that is governed by the Human Rights Law. The law protects individuals who are recovered or recovering drug addicts or alcoholics, and may protect alcoholics if the alcoholism does not interfere with job performance; intoxication or use of alcohol on the job is not protected. Alcoholism or drug dependency may qualify as a disability (see Section 4).

SMOKING POLICY

Smoking is prohibited inside NYSERDA’s offices. Consistent with practices to improve indoor air quality promoted by NYSERDA, employees and guests are encouraged, whenever practicable, to refrain from smoking near any entrance to NYSERDA’s offices.

My signature below indicates that I understand and agree to abide by the policies and procedures listed above. Violation of or failure to abide by these policies and procedures may result in termination of the Employee’s assignment.

Printed Name:_____

Signature/Date:_____

EXHIBIT F

Certification for Access to NYSERDA's Internal Networks and Systems

Pursuant to Agreement _____, (Contractor and Employee) requires access to NYSERDA's internal networks and systems using either NYSERDA issued or their own equipment.

During the term of the Agreement, (Employee and Contractor) shall comply with all of NYSERDA's policies including, but not limited to NYSERDA's Information Security Policies and Procedures Manual which shall include at a minimum the following:

- Ensure that all computer equipment has an antivirus solution, and that this solution is kept to the most current level necessary, as required by NYSERDA's Information Security Policies and Procedures Manual.

- Ensure that all computer equipment patching levels are current and maintained by (Contractor), as required by NYSERDA's Information Security Policies and Procedures Manual.

- (Contractor) must certify in writing on a monthly basis that antivirus and patching levels are current and up to date.

- When the use of password or authentication is required for NYSERDA network access, (Employee) will follow the required guidelines set forth in NYSERDA's Information Security Policies and Procedures Manual under the Password Policy regarding complexity and non-sharing of passwords.

- (Employee) is prohibited from downloading any type of hacking tools, including, but not limited to, network sniffers, vulnerability scanners, or password cracking tools. If at some point it is a requirement of the project to use these products to indentify security issues, NYSERDA shall approve the download in writing.

- Execution of this certification indicates that (Employee) has read and acknowledged NYSERDA's Acceptable Use Policy as set forth in NYSERDA's Information Security Policies and Procedures Manual.

Non-compliance with this Certification may result in lost privileges to NYSERDA's Networks and Systems, as well as potential Agreement termination.

_____

[Contractor]
Name:
Title:
Date:

EXHIBIT G

New York State

Energy Research and Development Authority

Information Security Policies and Procedures Manual

July 2014

NEW YORK STATE ENERGY RESEARCH AND DEVELOPMENT AUTHORITY

INFORMATION SECURITY POLICIES AND PROCEDURES MANUAL

Table of Contents

New York State
Energy Research and Development Authority
Information Security Policies and Procedures Manual

INTRODUCTION

The Information Security Policies and Procedures Manual is a statement of the requirements, ethics, responsibilities, and accepted behaviors NYSERDA requires to establish and maintain a secure computing, reporting, and communications environment and to protect the confidentiality, integrity, and availability of all data/information collected, stored, and communicated or reported by NYSERDA in any format (e.g. digital, hardcopy).

Administration of this Manual balances the measures taken to protect NYSERDA's data/information and computer networks with the ease of access to information/data and the usability of the computer networks. Specific practices and procedures may legitimately differ in different circumstances based upon conclusions regarding the necessary time, training, money, or other resources that impact data/information and computer network security, provided that, at a minmum, NYSERDA remains in compliance with New York State mandatory requirements.

Purpose

The purpose of this policy manual is to define the set of policies and standards that NYSERDA must implement and adhere to once implemented in order to satisfy the mandatory requirements of the New York State Office of Cyber Security (OCS) as set forth in Cyber Security Policy P03-002.

The primary objectives of this Information Security Policy and security program are to:

- Effectively and efficiently manage the risk of security exposure or compromise within NYSERDA systems and information assets;
- Communicate the responsibilities for the protection of NYSERDA information;
- Establish a secure processing base and a stable processing environment;
- Reduce, to the extent reasonably possible, the opportunity for errors to be entered into an electronic system supporting business processes;
- Preserve management's options in the event of an information asset misuse, loss, or unauthorized disclosure; and
- Promote and increase the awareness of information security.

Scope

The scope of this policy includes all personnel who have or are responsible for an account on any system that resides at any NYSERDA facility or has access to the NYSERDA network, including staff, contractors, and other affiliates who access the NYSERDA computer networks, systems, applications, or information.

Enforcement

Any employee found to have violated this policy manual will be required to comply and may be subject to disciplinary action, up to and including termination of employment.

A contractor found to have violated this policy manual will be required to comply and may be determined to have committed a material breach of its contract which could result in contract termination. Other consequences and penalties may also be pursued, as permitted by law.

1.0 INFORMATION CLASSIFICATION AND CONTROL

PURPOSE

The primary objective of this section is to ensure that information entrusted to NYSERDA is uniformly protected.

The purposes of this section are as follows: (1) to define a system for the protection of privacy and security of NYSERDA information assets through a classification scheme for all information by type; (2) to provide standards and supporting procedures for classifying information; and (3) to supply appropriate controls to protect the confidentiality, integrity, and availability of information. Based on its individual business needs and specific legal requirements, NYSERDA may exceed the security requirements put forth in this document but must, at a minimum, achieve the security levels required by this section.

SCOPE

This section applies to all types and forms of information collected or maintained by NYSERDA on its Information Assets. The scope of this section includes information through its entire life cycle (i.e., generation, use, storage, and disposition).

When information is extracted from NYSERDA information assets, the classification and corresponding control requirements in this policy cover that information in any form it may later take including electronic, paper, video, or other physical forms. It also applies to the transfer of information by voice.

This section is applicable to NYSERDA staff and all others, including outsourced third parties, who have access to or manage NYSERDA information. This policy does not change the conditions of employment.

ROLES AND RESPONSIBILITIES

Each NYSERDA department/unit and, in specific, its manager or director is responsible for implementing, reviewing, and monitoring internal policies, practices, etc. to assure compliance with this policy. Those managers designated as data owners are responsible for ensuring that the information they collect on NYSERDA's behalf is compliant with this policy.

Information Classification and Control is established and maintained through the combined efforts of the organization. While the classification of information is a detailed and technical process and will be conducted for departments by trained specialists, the control of information includes responsibilities for all staff and contractors who access NYSERDA's Information Assets as well as all staff and contractors that collect information on behalf of NYSERDA or use NYSERDA information that has not been made public.

1.1 PPSI PRIVACY POLICY

OVERVIEW

NYSERDA is committed to the responsible management and use of personal, private or sensitive information (PPSI) collected from and about its staff, program participants, business partners, and others who provide such information to NYSERDA. This commitment is in accordance with both state and federal regulations concerning the use of such information. Such information includes information that could be used to cause financial harm or reputational harm to any individual or entity.

This policy applies to PPSI and how it is collected. The complete definition of PPSI data is provided in the Glossary.

PURPOSE

The purpose of this policy is to protect the privacy of individuals and entities who have PPSI stored (either in electronic or paper form) on assets owned by NYSERDA or its contractors (where collected in connection with NYSERDA's activities), while at the same time providing NYSERDA the ability to share this information with authorized individuals or entities as required by law or policy.

SCOPE

The PPSI Privacy Policy applies to all staff, contractors, and other affiliates who interact with NYSERDA systems and processes, electronic or otherwise. This policy is not intended to replace or supersede other existing NYSERDA policies and procedures relating to the use or maintenance of PPSI, such as those related to compliance with the Nuclear Regulatory Commission's Safeguards Information standards or HIPAA privacy standards.

POLICY

Limits on Use and Access

Authorized uses of PPSI within NYSERDA are limited to uses which are necessary to a) meet legal and regulatory requirements; b) facilitate access to services, transactions, facilities, and information; or c) support proper evaluation or reporting of NYSERDA results and performance.

Access to PPSI possessed by NYSERDA is limited to:

- the individual whose information is produced or displayed;
- a NYSERDA staff member or agent of NYSERDA with authorized access based upon a legitimate business interest and a need to know;
- an organization or person authorized to receive the information by the individual whose information is produced or displayed;
- a legally authorized government entity other than NYSERDA or its representative;
- other circumstances in which NYSERDA is legally compelled to provide access to information, such as the NY Freedom Of Information Law.

Social Security Numbers (SSN)

Social Security numbers are PPSI, and are therefore subject to the access restrictions described above.

NYSERDA will collect and maintain Social Security numbers in all instances in which that number is required by law for reporting or other uses. This includes, but is not limited to, collecting and maintaining Social Security numbers of all employees of NYSERDA and individuals to whom NYSERDA is making payments. In addition, NYSERDA will continue to use Social Security numbers, as allowed by law, for operational purposes when there is no reasonable substitute.

NYSERDA, its staff, contractors, and other affiliates must abide by all state and federal legal regulations pertaining to Social Security Number protection. Although NYSERDA itself is exempt from the New York State Social Security Number Protection Law, it is NYSERDA's intention to provide privacy protections equivalent to those afforded by this law. All contractors and other affiliates must understand their obligations under this law and comply with it.

Social Security Number (SSN) Removal

Since NYSERDA collects SSNs during its normal course of business over time, it is NYSERDA policy to remove all previously collected SSNs from NYSERDA systems and information assets other than those information assets which meet current control and access requirements. Even within those systems and information assets meeting current control and access requirements, SSNs shall only be retained as long as required and shall otherwise be destroyed using a method approved by the Information Security Officer (ISO).

Legal Requirements and NYSERDA Policies

Due to the increasing threat of identity theft and fraud, state and federal governments have created privacy laws and NYSERDA has adopted internal policies that require ensuring the security and privacy of an individual's Social Security Number.

It is against NYSERDA Policy to...

- Publically post or display the SSN
- Require an individual to transmit his/her SSN unless the connection is secure or the number is encrypted
- Require an individual to use his or her Social Security number to access an Internet site unless a unique password or PIN is also required
- Electronically transmit (e.g. e-mail, FTP, etc.) the SSN of an individual unless the SSN is encrypted (FTC)
- Transmit the SSN in e-mail unless the data is encrypted
- E-mail SSN(s) to outside parties without prior authorization
- Store SSN(s) on computers without protecting it appropriately
- Permit an unauthorized individual access to SSN data
- Require an individual to list his or her SSN on mailed outbound materials (e.g. applications or other forms) unless required by a state or federal agency (must use only approved state or federal forms)

- Collect, store or process SSN data unless there is a need to do so
- Transmit SSN information over public networks without encryption
- Retain SSN data beyond its required life
- Store SSN data without encryption

Partial Social Security Numbers

Although storing and processing partial SSN data (e.g. just the last four digits of a SSN) can reduce the risk of identity theft to an individual, residual risks do remain in instances where partial SSNs are used in conjunction with other identifying information such as address or birthplace. NYSERDA shall treat partial SSNs as if they were full SSNs.

Collecting PPSI on Physical Forms and through the Web

When NYSERDA collects PPSI using a physical form (or other physical document), NYSERDA will give the individual providing the PPSI a copy of the NYSERDA Privacy Disclosure Notice. This Notice describes how NYSERDA may share the collected PPSI with outside entities. The NYSERDA Privacy Disclosure Notice may be found and downloaded from the NYSERDA Intranet site on the Data Governance page in the common links area.

When NYSERDA collects PPSI through a Web based application, NYSERDA will post a link on the PPSI-collecting web page to the NYSERDA Privacy Disclosure Notice. This Notice describes how NYSERDA may share the collected PPSI with outside entities. Any changes to the Notice will be posted on the Web site.

PPSI must only be collected on NYSERDA approved forms/web pages regardless of medium. Proposed forms collecting PPSI must be approved by the Chief Information Officer, General Counsel, Director of Performance Management & Evaluation Systems (PMES) and the Information Security Officer (ISO), or their respective designees, before being put into use or modified. The identities of individuals with official authority and their approved designees may be found on the NYSERDA Intranet site on the Data Governance page in the common links area.

1.2 PPSI INFORMATION ASSET ACCESS POLICY

OVERVIEW

The purpose of this policy is to allow access to personal, private, or sensitive information (PPSI) as required for the proper functioning of NYSERDA while maintaining a level of privacy and security that meet PPSI requirements.

NYSERDA shall control access to data identified as PPSI in order to ensure that access is available only with appropriate authorization, that PPSI is used appropriately, and that authorized access complies with the *NYSERDA PPSI Privacy Policy* and relevant state and federal laws.

PURPOSE

This policy outlines requirements for granting and revoking access to PPSI in the possession of NYSERDA or its contractors.

SCOPE

This policy governs access to data maintained for official purposes by NYSERDA or a party acting on behalf of NYSERDA. Any system containing such data or tangible container of such data in physical form constitutes a NYSERDA Information Asset.

This policy does not apply to data or records that were not obtained through any NYSERDA business practice but are placed onto NYSERDA Information Assets by individual staff, contractors, and other affiliates (non-NYSERDA) for their personal use. NYSERDA staff, contractors, and other affiliates should not store non-NYSERDA PPSI on NYSERDA systems.

Requests for records under NYS Freedom of Information Law and other requests in which NYSERDA is legally compelled to provide access to information are outside of the scope of this policy and shall be addressed under policies and procedures specific to those requests.

POLICY

NYSERDA Data Shall be Classified

NYSERDA Data shall be classified in accordance with the NY State Information Technology Standard: Information Classification.The current standard may be found and downloaded from the NYSERDA Intranet site on the Data Governance page in the common links area.

Data Owners shall notify the PMES department and the Information Security Officer in writing when they have a need to collect new types of data that will be collected or stored on NYSERDA Information Assets to support NYSERDA business functions. PMES and the ISO shall work with the Data Owner to ensure that data is classified before it is collected. If data is classified as PPSI both controls and approvals to access PPSI must be in place before PPSI data is collected.

Approval to Access PPSI

Directors Approve Access to PPSI

Data Owners shall obtain authorization to access PPSI from their department Director (or NYSERDA Officer) using the approved PPSI Authorization form.The Director grants approval for access to PPSI. Directors shall grant access in compliance with the *NYSERDA PPSI Privacy Policy* and all relevant regulations (e.g. HIPAA). Directors shall grant access only to those employees, affiliates, and systems that need access to perform their job duties or mission. The PPSI Access Authorization form as well as the identities of individuals with official authority and their approved designees may be found and downloaded from the NYSERDA Intranet site on the Data Governance page in the common links area.

The PMES department shall maintain a record of Data Owners, who collect or maintain PPSI data, identified according to Data Governance Policy and verified by the Information Security Officer (ISO). If a Data Owner is not clearly designated, the data in question is owned by the Officer or Director of the unit that originates the data.

Officers Review Access to PPSI
Access to PPSI shall be reviewed by the officers on an annual basis. Officer(s) or their designee shall ensure that there is evidence of a completed and signed copy of the PPSI Access Authorization form for any individual having access to PPSI data.

Data Owners are Responsible for Requesting, Seeking Approval or Approving, Auditing, and Revoking Access
Data Owners shall ensure that the approved NYSERDA procedures for requesting and approving access to PPSI are followed. Data Owners shall also implement procedures for regularly auditing access to PPSI and revoking access when it is no longer needed or authorized. All approvals and revocations shall be in writing and shall include sufficient tracking of requests, approvals, and revocations that authorized access to PPSI is auditable in conformance with the Data Governance and Records Retention policies.

Access to PPSI retained in NYSERDA's Information Systems shall only be granted when a properly approved request for access is submitted to the Information Security Officer (ISO). The ISO shall communicate authorizations to IT (the custodian of information assets.)

Only Authorized Data Users Shall Access PPSI
Access to PPSI shall be controlled by measures (i.e., internal controls) that provide reasonable assurance that access by unauthorized users will be prevented.

Authorized Data Users Shall Use PPSI Responsibly
Data Users must use PPSI to which they have access only for its intended purpose. Data Users must maintain the confidentiality of data in accordance with applicable laws, the *NYSERDA PPSI Privacy Policy* and the *NYSERDA Data Classification and Control Policy and Standard*, section 1.3 below. Authorized access to PPSI does not authorize further dissemination of data, including copying or any use(s) other than that for which the Data User was expressly authorized. Upon completion of work or revocation of access the Data User shall return or destroy the PPSI and document such actions.

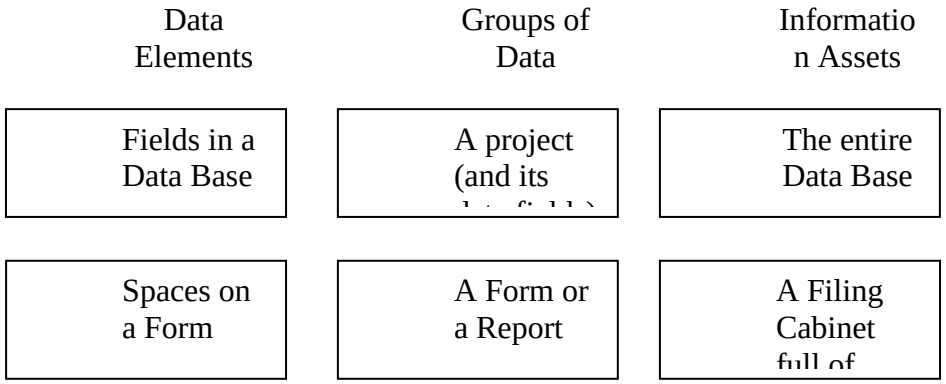
External Third-Party Access to PPSI Shall be Governed by Contractual Agreement
Access to PPSI by external parties shall be governed by individual contractual agreement. Such agreements shall be approved by NYSERDA Counsel's Office and by the appropriate NYSERDA designated Data Owner.

1.3 Data Classification and Control Policy and Standard

OVERVIEW

NYSERDA produces, collects, and uses many different types of data in fulfilling its mission. Laws and institutional policy mandate privacy and protection of certain types of data, and NYSERDA's need to manage risks to its constituents and to its reputation requires the protection of other information. Classifying data is the first step in determining the appropriate level of control required for a given type of data or information asset.

Data classification focuses on the data elements. A data element is the container for a type of data, rather than the data itself (e.g., the data element "NAME" or "STREET ADDRESS" rather than the data contained in that element, such as "John Smith" or "123 Main Street"). During classification, data elements that appear together may be classified in data groupings (e.g., an application form, whether electronic or paper). Data elements collected and maintained together create information assets (e.g., a program database or a file cabinet). Information assets or groups of data with multiple data elements, such as reports, contracts, business data bases, etc., shall be classified based upon the classification level of the most sensitive or restricted individual data element contained therein.



The classification of data is a detailed process with specific technical requirements. This standard is applicable to NYSERDA staff, contractors, and other affiliates, which have access to or manage NYSERDA information. The scope of this section includes information through its entire life cycle (i.e., generation, use, storage, and disposition). It covers information in any form including electronic, paper, video, or other physical forms.

NYSERDA Classification Schema for Confidentiality

While maintaining compliance with the NY State Standard for classification, NYSERDA will apply its own data-classification schema to more specifically describe the restrictions required for data classified as "High Confidentiality". The NYSERDA classification schema shall include both "Confidential – Restricted" and "Confidential – Private" to designate different types of "High confidentiality" based upon identity theft and privacy risk and business need for access.

NYSERDA shall use "Internal Use Only" to designate Moderate Confidentiality and "Public" to designate Low Confidentiality.

Information Classification

Information classification is based on three principles of security: 1) confidentiality, 2) integrity, and 3) availability. For each principle, information can be classified as low, moderate, or high based on the potential impact. Impact levels are defined as limited, serious and severe or catastrophic. For purposes of classification, limited impact shall be deemed to include no impact.

Low = Limited impact that would:

- cause a degradation in mission capability to an extent and duration that NYSERDA is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- result in minor damage to NYSERDA or third party assets;
- result in minor financial loss; or
- result in minor harm to individuals.

Moderate = Serious impact that would:

- cause a significant degradation in mission capability to an extent and duration that NYSERDA is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- result in significant damage to NYSERDA or third party assets;
- result in significant financial loss; or
- result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

High = Severe or catastrophic impact that would:

- cause a degradation in or loss of mission capability to an extent and duration that NYSERDA is not able to perform one or more of its primary functions;
- result in major damage to NYSERDA or third party assets;
- result in major financial loss; or
- result in catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Figure 1 – Information Asset Classification Matrix

	INFORMATION CLASSIFICATION CATEGORIES		
	LOW	**MODERATE**	**HIGH**
CONFIDENTIALITY Consider impact of unauthorized disclosure on factors such as: • Health and Safety • Financial Loss • Mission/Programs • Public Trust	The unauthorized access or disclosure of information would have ***limited or no impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized access or disclosure of information would have ***serious impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized access or disclosure of PPSI or other information would have a ***severe or catastrophic impact*** on the organization, its critical functions, workforce, business partners and/or its customers.
INTEGRITY Consider impact of unauthorized modification or destruction on factors such as: • Health and Safety • Financial Loss • Mission/Programs • Public Trust	The unauthorized modification or destruction of information would have ***limited or no impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized modification or destruction of information would have ***serious impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized modification or destruction of information would have a ***severe or catastrophic impact*** on the organization, its critical functions, workforce, business partners and/or its customers.
AVAILABILITY Consider impact of untimely or unreliable access to information on factors such as: • Health and Safety • Financial Loss • Mission/Programs ▪ Public Trust	The disruption of access to or use of information would have ***limited or no impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The disruption of access to or use of information would have ***serious impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The disruption of access to or use of information would have a ***severe or catastrophic impact*** on the organization, its critical functions, workforce, business partners and/or its customers.

The information classification process includes the following steps:

1. Identifying information assets
2. Classifying information assets by confidentiality, integrity, and availability (CIA)
3. Determining controls based upon the classification

Step 1. Identification of Information Assets

Identification of information assets involves creating an inventory of all information assets in the NYSERDA. The following items need to be considered when constructing this inventory:

1. Determining the information owner (In NYSERDA's data governance system this role shall be called data owner and the terms are used interchangeably.)
2. Determining the information custodian
3. Identifying information assets

Step 1.1 Grouping of Information Assets

In order to facilitate the classification of information assets and allow for a more efficient application of controls, it may be desirable to group information assets together. It is important to establish that the grouping of assets for classification is appropriate. A broad grouping may result in applying controls unnecessarily as the asset must be classified at the highest level necessitated by its individual data elements. For example, if a Human Resources unit decides to classify all of their personnel files as a single information asset and any one of the files contains a name and social security number, the entire grouping would need to be protected with the controls for a confidentiality of high.

A narrow grouping allows for more precise targeting of controls. However, as there are more information assets to classify, this increases the complexity of the classification and the management of controls. Using the previous example, classifying the multitude of personnel files (e.g., appointment letters, timecards, position classifications, holiday waivers) as individual information assets requires specifying the set of controls for each classification.

In the case of a system (e.g., database, data warehouse, application server), it may be easier to apply controls if the system is classified as a single entity. However, costs may be reduced by applying controls to individual elements (e.g., field, record, application). Therefore, it is important that NYSERDA evaluate the difference between the two scenarios to identify the most appropriate solution when determining the grouping of information assets for classification.

Step 1.2 Determining the Data Owner[3]

Responsibility for the classification and control of an information asset must be assigned to an individual in a managerial position. If multiple individuals are found to be "owners" of the same information asset, a single owner must be designated by a higher level of management. The data owner is responsible for determining the information's classification and how and by whom the information will be used. Owners must understand the uses and risks associated with the information for which they are responsible. Each owner must exercise due diligence

[3] Information Owner and the Data Owner are equivalent.

with respect to the proper classification of data in order to prevent improper disclosure and improper access.

Step 1.3 Determining the Information Custodian

Information custodians are people, units, or organizations responsible for implementing the authorized controls for information assets based on the classification level. An information asset may have multiple custodians. Based on the data owner's requirements, the custodian secures the information, applying safeguards appropriate to the information's classification level. Information custodians can be from within NYSERDA or from third parties (e.g., another state entity or non-State entity). If the custodian is a third party, a formal, written agreement must specify the responsibilities between the custodian's organization and NYSERDA regarding who owns the information. An information custodian may also be the data owner.

Step 1.4 Identifying Information Assets

For each information asset in their control, the data owner must identify at a minimum:

1. Source of the information asset (e.g., unit, agency)
2. Use of the information asset (i.e., purpose/business function)
3. Business processes dependent on the information asset
4. Users/groups of users of the information asset

Step 2. Classification of Information Assets

Owners must answer the following question to determine the classification of their information assets. It is appropriate to recruit and work with subject matter experts who have specific knowledge about the information asset? The PMES department and Information Security Officer may also be called upon to advise and assist the data owner in determining the classification.

Step 2.1 Information Asset Classification Questions

Information assets are classified according to confidentiality, integrity, and availability. Each of these three principles of security is individually rated as low, moderate, or high. For example, an information asset may have a confidentiality level of "high", an integrity level of "moderate", and an availability level of "low" (i.e., HML).

Below are the state-specified model questions. Unless otherwise indicated, the answers to each question must indicate the impact level (i.e., none or limited (low), serious (moderate) or severe or catastrophic (high).

Confidentiality Questions

Does the information include or contain PPSI (Personal, Private or Sensitive Information)? Y/N
What impact does unauthorized access or disclosure of information have on health and safety?
What is the financial impact of unauthorized access or disclosure of information?
What impact does unauthorized access or disclosure of information have on NYSERDA's mission?
What impact does unauthorized access or disclosure of information have on the public trust?

Is confidentiality mandated by law or regulation? If yes, determine the impact of unauthorized access or disclosure of information.

Is the information intended for limited distribution? If yes, determine the impact of unauthorized access or disclosure of information.

Is the information publicly available? Y/N

If the answer to question 1 above is "Yes" or if any of the other answers are "severe or catastrophic", the confidentiality rating is high. If the answer to question 1 above is "No" and if any of the other answers are "serious" but none are "severe or catastrophic", the confidentiality rating is moderate. If the answer to question 1 above is "No" and if all of the other answers are "limited" or "none", the confidentiality rating is low.

Integrity Questions

[1] Does the information include medical records? Y/N

[2] Is the information (e.g., security logs) relied upon to make critical security decisions? Y/N

[3] What impact does unauthorized modification or destruction of information have on health and safety?

What is the financial impact of unauthorized modification or destruction of information?

What impact does the unauthorized modification or destruction of information have on NYSERDA's mission?

What impact does unauthorized modification or destruction of information have on the public trust?

Is integrity addressed by law or regulation? If yes, determine the impact of unauthorized modification or destruction of information.

Is the information (e.g., financial transactions, performance appraisals) relied upon to make business decisions? If yes, determine the impact of unauthorized modification or destruction of information.

If the answer to question 1 or 2 above is "Yes" or if any of the other answers are "severe or catastrophic", the integrity rating is high. If the answer to question 1 and 2 above is "No" and if any of the other answers are "serious" but none are "severe or catastrophic", the integrity rating is moderate. If the answer to question 1 and 2 above is "No" and if all of the other answers are "limited" or "none", the integrity rating is low.

Availability Questions

[4] Is availability of the information essential for emergency response or disaster recovery? Y/N

[5] This information needs to be provided or available:

As time permits - LOW

Within 1 to 7 days - MODERATE

24 hrs. per day/7 days a week - HIGH

[6] What is the impact to health and safety if information were not available when needed?

[7] What is the financial impact if information were not available when needed?

[8] What is the impact to NYSERDA if information were not available when needed?

[9] What is the impact to the public trust if the information were not available when needed?

If the answer to question 1 is "Yes" or if any of the other answers are "severe or catastrophic" or "high", the availability rating is high. If the answer to question 1 above is "No" and if any

of the other answers are "serious" or "moderate" but none are "severe or catastrophic" or "high", the availability rating is moderate. If the answer to question 1 above is "No" and if all of the other answers are "limited", "low" or "none", the availability rating is low.

Step 3. Determination of Controls

Once the information is classified, the classification can be used to determine baseline controls. A listing of baseline controls for each type of classification can be found in Appendix A - Information Security Control Charts.

Step 4. Additional NYSERDA Steps:

Using the state specified model questions as the minimum standard, NYSERDA shall develop additional NYSERDA specific questions to assist in proper classification and balance required controls and NYSERDA's operational need to have access to specific data. These questions shall be developed by the Director of PMES and approved by the Information Security Officer and Chief Information Officer.

As mentioned above, for data requiring High-Confidentiality, NYSERDA shall further divide the classification into two sub-categories to assist NYSERDA as defined below.

Confidential - Restricted

This relates to data that is NYS High Confidentiality and NYSERDA has determined to tightly restrict access within NYSERDA due to personal privacy, potential for identity theft or legal requirements. Most PPSI will be classified and controlled in this manner. Examples are HIPPA protected health data, Social Security Numbers and Bank Account Numbers.

Confidential - Private

This relates to data that is NYS High Confidentiality and NYSERDA has determined to make it available as required for proper functioning of NYSERDA programs and operations. Examples are the names of participants in low income programs and company proprietary data provided by applicants to receive NYSERDA funding.

CONTROL

NYSERDA shall apply the appropriate level of control to protect data at all times - as data is being collected, once it has been collected, and as data is being transmitted or provided to internal and external stakeholders. In general, control requirements relating to integrity and availability will be applied systemically at the information asset level. By contrast, control requirements relating to confidentiality, expressed in terms of the NYSERDA Classification Schema for Confidentiality, are more likely to be applied at the data user level.

NYSERDA has developed minimum standard control requirements for the protection of each classification of data when being used or handled in a specific context (e.g. Social Security Numbers sent in an email message). Please note that NYSERDA control standards are not intended to supersede any regulatory or contractual requirements for handling data. Some specific data sets such as payroll, insurance or financial account data, may have requirements in addition to the minimum standard requirements.

NYSERDA shall publish a control plan for each identified Information Asset and standard data sharing rules to be applied to each group of data or individual data field that is classified as NYS Medium or High Confidentiality.

Each NYSERDA department/unit is responsible for implementing, reviewing, and monitoring internal policies, practices, etc. to assure compliance with this standard.

All NYSERDA personnel are responsible for maintaining the confidentiality, integrity, and availability of NYSERDA information to facilitate the effective and efficient conduct of NYSERDA business.

In addition, the following responsibility designations identify roles and responsibilities related to information classification at NYSERDA.

The Information Security Officer (ISO) and the Director of Performance Management and Evaluation Systems (PMES) are responsible for the State Entity duties enumerated in the NY State Information Technology Standard: Information Security Controls. The primary function of the ISO is to ensure compliance with the requirements below and to monitor and audit accordingly. The primary function of the Director of PMES is to maintain and improve the system to support compliance including system design, training and development of procedures. Duties which are unique to either the ISO or Director of PMES are labeled as such below:

- Developing, implementing, and maintaining the NYSERDA data classification program in consultation with NYSERDA Executive Management/Stakeholders/Business Units, enabling the data owners, information custodians, and other key individuals to make appropriate decisions regarding the security classification and protection of data (Director of PMES Implements and ISO verifies)
- Building agency-wide compliance with NYSERDA's data-classification program (Director of PMES Implements and ISO verifies)
- Developing, implementing, and maintaining the processes and procedures for properly labeling media (electronic or paper based) commensurate with the classification of the information (Director of PMES Implements and ISO verifies)
- Developing, in conjunction with the NYSERDA Business Units, the necessary controls of access to applications, commensurate with classification of the information processed by the system or application (Director of PMES Implements and ISO verifies)
- Overseeing the development and implementation of a centralized data-classification repository (Director of PMES primary)
- Taking the appropriate actions (e.g., Incident Response Management) if non-public information is lost or disclosed to unauthorized parties — or is suspected of being lost or disclosed to unauthorized parties (ISO determines appropriate actions, Director of PMES will report any violations to ISO)
- Working with the business units to develop mitigating security strategies when exceptions or waivers are deemed necessary (ISO makes determinations, Director of PMES will assist as a technical resource.)

A Data Owner must be identified for each NYSERDA information asset. Data Owners are responsible for maintaining appropriate security measures commensurate with any applicable federal or state statutes or regulations governing the data. Authority for implementing security measures may be delegated (e.g., to the Information Custodian), although accountability and responsibility remain with the identified Data Owner.

The Data Owners are the persons in the Business Unit responsible and accountable for the information asset, are at the manager or executive level, and are non-IT staff.

The Data Owners are responsible and accountable for the following areas (the Data Owners can delegate authority in these areas, but accountability remains with them):

- Assigning the appropriate data classification to information under their jurisdiction
- Determining the means (e.g., a process, event, or date) by which the information can be reclassified
- Determining to whom and under what conditions access is granted
- Identifying and documenting the controls required to maintain the confidentiality, integrity, and availability of the information commensurate with its classification level (e.g., written agreements with IT and end users, procedures, etc.)
- Verifying that the identified security controls are in place and functioning properly
- Verifying that access to the information is based on the "least- access" principle
- Verifying that all legal requirements for access, disclosure, retention, archiving, and expungement of information are satisfied
- Verifying that whenever any data is transferred to another entity (e.g., another state agency or contractor), the entity is educated/informed of the proper handling, storage, disseminating, and disposal of the data via an executed MOU/MOA or other written agreement
- Reviewing periodically, and at a minimum annually, to confirm the classification of, or reclassifying, information assets of which they are the owner
- Reviewing, annually, the master data-classification records for accuracy
- Reviewing for appropriateness the actions of those granted access to information of which they are the owner
- Acting on security violations against their information assets and immediately notifying the Information Security Officer (ISO)
- Notifying the ISO if non-public information is lost or disclosed to unauthorized parties — or is suspected of being lost or disclosed to unauthorized parties

The Information Technology department functions as NYSERDA's Information Custodian. An Information Custodian (IC) must be identified for each NYSERDA information asset. An IC can be a person, a unit, or an organization responsible for implementing the authorized controls for information assets based on the classification level set forth by the Data Owner The IC is able to take the necessary actions to secure the information by applying controls appropriate to the information's classification level. An IC can either be internal to NYSERDA or from a third party (e.g., another state entity or a non-state-entity). It is recommended that a service level agreement exist between the IC and the Data Owner, so the parties understand their respective responsibilities.

Data Users (also referred to as Information End Users) fall into two categories:

1) NYSERDA Data Users –Authority staff, contractors, and other affiliates who, as part of their job responsibilities, are authorized users of NYSERDA information.

2) Business partner Data Users –NYSERDA business partners, who include but are not limited to, various state and local government entities, voluntary agencies, and other business partners, that are authorized users of NYSERDA information.

NYSERDA Data Users are responsible for accessing and using the information only for the intended purpose, as defined by the Data Owner; for maintaining the confidentiality, integrity, and availability of the information, as required by the owner; and for familiarizing themselves and complying with applicable NYSERDA security policies.

Business partner Data Users are governed by agreements specifying their responsibility to handle the information in a secure manner and in compliance with all applicable statutes and regulations.

Data Users are required to report a suspected or actual violation of NYSERDA polices and standards to the ISO in writing.

Data Users are also responsible for notifying the IO and the ISO if non-public information is lost or disclosed to unauthorized parties — or is suspected of being lost or disclosed to unauthorized parties.

1.4 EXEMPTION PROCESS

In limited situations, NYSERDA may determine that a particular electronic or digital control cannot be implemented due to technical constraints or business limitations. NYSERDA must mitigate the risk associated with not implementing that control through the use of compensating controls, which may have to be manual control processes and activities. The decision to mitigate risk in this manner requires documentation that must provide a written description that demonstrates an understanding of the risk and a list of compensating controls that will be implemented. NYSERDA may only consider the use of compensating controls if it has undertaken a risk analysis and has legitimate technological or business constraints.

NYSERDA must complete an Information Classification and Control Standard Exemption Request form (refer to PS08-001, Appendix A) signed by the NYSERDA Information Security Officer, Chief Information Officer, and the Treasurer, or equivalent. This document must be submitted to the Office of Cyber Security (OCS) for review. Exemption requests are valid for a period of one year. After this time, the control must be reevaluated. If the control still cannot be implemented, a new exemption request form must be completed and submitted to OCS.

2.0: PERSONNEL SECURITY

Personnel security is established to reduce the risk of human error and the misuse of NYSERDA information and facilities to an acceptable level.

2.1: INCLUDING SECURITY IN JOB RESPONSIBILITIES

The roles and responsibilities are documented and include general responsibilities for all NYSERDA employees, as well as specific responsibilities for protecting specific information and performing tasks related to security procedures.

Information Security Roles and Responsibilities Include:

Senior Management

Senior Management provides overall guidance and direction for information security. Senior Management has final responsibility for information security functions and activities. Senior Management must allocate resources consistent with the criticality of business functions, systems and roles and responsibilities of all parties including those defined herein and charge the administrators and the Information Security Officer to carry their mission and functions. Senior Management shows security leadership by personal involvement in security issues and functions and by complying with security policies and procedures.

Information Security Officer

The Information Security Officer is the central point of contact for all information security matters. Acting as the internal technical consultant, it is the Information Security Officer's responsibility to create effective information security policies, procedures, guidelines and standards that take into consideration the needs of users, Local Area Network Administrators, Data Owners, and third parties. The Information Security Officer is responsible for overseeing all access control administration activities, monitoring the security of the information systems, and providing information security training and awareness programs. The Information Security Officer is additionally responsible for periodically providing management with information about the current state of coordinating a security incident response team to promptly respond to virus infections, hacker break-ins, system outages, and other information security problems.

The Information Security Officer must provide the direction and technical expertise to ensure that information is properly protected. This includes consideration of the confidentiality, integrity, and availability of both information and the systems that handle it. The Information Security Officer will act as a liaison on information security matters between all organizational units and with all organizations with access to agency information or systems and must be the focal point for all information security activities. The Information Security Officer will perform risk assessments, audits, prepare actions plans, evaluate vendor products, participate on in-house systems development projects, assist with control implementations, investigate information security breaches, and perform other activities which are necessary to assure a secure information handling

environment.

All information security problems must be reported to and handled with the involvement and cooperation of the Information Security Officer.

Internal Audit Department

The Internal Audit Department periodically performs compliance checks and internal audits of the Information Security function and its activities. These reviews provide the Authority with additional assurance that information security policies are consistent with today's information security standards, management expectations, organizational goals, and comply with state agency and public authority requirements.

Supervisor

The Information Security Officer or other IT management does not approve individual access control requests. Employees are automatically provided access to individual network drives and group drives based on their organizational unit. The employee's Supervisor approves a request for any other network system or application access based on job function or other attribute consistent with the requirements defined by the Information Security Officer. When a user leaves employment, it is the responsibility of the Human Resources department to promptly notify the Information Security Officer so the Information Security Officer can initiate the request for the revocation of the privileges associated with the individual's User-ID. User-IDs are specific to individuals, and must not be reassigned to, or used by others. Prior to employee separation, the supervisor is responsible for reassigning the involved duties and files to other users.

Data Owners

Data owners are the people responsible for defining the security rights to an Information Asset. Data Owners work with the Information Security Officer to protect Information Assets.

Information Users

Users play an important role in information security. Now that information and information systems are distributed to the office desktop, and are used in remote locations, the user's role has become an essential part of information security. Information Users are individuals who have been granted explicit authorization to access, modify, delete, and utilize information by the relevant Data Owner. Users must use the information only for the purposes specifically approved by the Data Owner. Users must also comply with all security measures defined by the Data Owner, implemented by the Local Area Network Administrator, and defined by the Information Security Officer. Unless explicitly authorized by existing policy, Users must refrain from disclosing information in their possession without first obtaining permission from the Data Owner. Users must additionally report to the Information Security Officer or Help Desk all situations where they believe an information security vulnerability or violation may exist. Users are required to familiarize themselves with, and act in accordance with all information security policy requirements. Users are also required to participate in information security training and awareness

efforts and to report all suspicious activity and security problems. Users are responsible for all activity performed with their personal User-IDs. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their User-IDs. Similarly, users are forbidden from performing any activity with User- IDs belonging to other users.

Specific information security responsibilities must be incorporated into all user job descriptions if such individuals have access to sensitive information.

Human Resources Department

Non-compliance with information security policies and procedures may result in disciplinary actions.

External Local Area Network Administrators

Each organizational entity connected to the NYSERDA computing environment is responsible for the security of the information that they enter, maintain and access. For external organizations connected to the NYSERDA computing environment, an appropriate Local Area Network Administrator must be designated as the point of contact for access to all systems. Each external organization has responsibility for their information and locally controlled hardware, software and components. The individuals so designated as Local Area Network Administrators do not legally own the information in question; they are instead designated to make decisions on behalf of NYSERDA for the system and information involved and access to the system and information. Working with NYSERDA, each organization is required to make the following decisions and perform the following activities:

- Approve all access control privileges for specific job functions, groups, and classes of users;
- Approve all access control requests which do not fall within the definition of existing security profiles;
- Select a data retention period for their information in conformance with legal, regulatory, State Archive and Records Administration and other applicable requirements;
- Select special controls needed to protect information (such as additional data integrity checks, more frequent back-up procedures or encryption);
- Define acceptable limits on the quality of their information (accuracy, timeliness, time from capture to usage, etc.);
- Approve all acceptable uses and declare the limitations of their information;
- Approve all application systems development or changes that use their information before these systems are moved into production status;
- Review reports about system intrusions and other events which are relevant to their information;
- Periodically review access control privileges to assure conformance with requirements;
- Select a sensitivity classification category relevant to their information and review this classification periodically;
- Determine business criticality of systems and information so that appropriate business continuity planning can be performed; and

- Promptly report any suspected compromises to information systems, including any suspected inappropriate disclosure of sensitive or confidential information, to the NYSERDA Information Security Officer or Help Desk.

The Local Area Network Administrator must designate a back-up person to act if they are absent or unavailable. They may not further delegate ownership responsibilities without approval from the NYSERDA Information Security Officer. Local Area Network Administrators are responsible for authorizing User access to information based on the need-to-know. They must also make decisions about the permissible uses of information including relevant business rules. The Local Area Network Administrator is responsible for choosing relevant controls for information consistent with policies and standards. The Local Area Network Administrator must understand the uses and risks associated with the information for which they are accountable. This means that they are responsible for the consequences associated with improper disclosure, insufficient maintenance, inaccurate classification, and other security related control deficiencies pertaining to the information under their control.

NYSERDA Local Area Network Administrators

Local Area Network Administrators are in physical or logical possession of information or information systems. Local Area Network Administrators follow the instructions of Owners, operate systems on behalf of Owners and serve Users authorized by Owners. Local Area Network Administrators must define the technical options, such as information criticality categories, and then allow Owners to select the appropriate option(s) for their information. Local Area Network Administrators also define information systems architectures and provide technical consulting assistance to Owners so that information systems can be built and run to best meet business objectives. Local Area Network Administrators are responsible for safeguarding the information in their possession as specified in applicable security policies, procedures and standards.

Information Custodians

Typically information custodians include the Information Security Officer and other IT administrators, Security Coordinator, Systems Administrator, Network/Local Area Network Administrator, Database Administrator, etc.

Outsourced Functions

Where business or technical functions, tasks or activities are outsourced to external suppliers, whether other governmental units or non-government organizations, the supplier will be required to meet all the roles and responsibilities and compliance with all policies, procedures, and standards appropriate to the function(s) they perform. Suppliers shall provide documentation of compliance and be subject to periodic audits of their activities.

Separation of Duties

Whenever a computer-based process involves sensitive or critical information, the system must

include controls involving a separation of duties or other compensating control measures. These control measures must ensure that no one individual has exclusive control over these types of Information Assets or functions related to them.

Whenever practical, no person should be responsible for completing a task involving sensitive or critical information from beginning to end. Likewise, a single person must not be responsible for approving their own work. To the extent possible, for every task at least two people must be required to coordinate their information-handling activities.

2.2: USER TRAINING

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organizational security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific training. The philosophy of protection and specific security instructions must be taught to, and reinforced with, computer users. The security awareness and training information needs to be continuously updated and reinforced.

- All new users must attend an approved Security Awareness Training class to ensure they are aware of and understand:
    - information Security policies;
    - their role and responsibility regarding the protection of NYSERDA information and equipment;
    - the proper use of information processing facilities; and
    - typical security threats.
- All users must be provided with sufficient training and supporting reference materials to allow them to properly protect NYSERDA information resources.
- Information Security manuals that describe NYSERDA Information Security Policies and procedures will be made available to all users, either electronically or in hard copy.
- A Security Awareness Training Program will be developed, implemented, and maintained to address the security education of all NYSERDA employees.
- The Security Awareness Training Program will act as a supplement to new employee orientation and will be reinforced annually.
- A communication process will be developed and maintained to communicate new computer security program information, security bulletin information, and security items of interest.

Appropriate records will be kept to document the Security Awareness Training Program.

2.3: SECURITY INCIDENTS OR MALFUNCTIONS

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. By implementing security policies, blocking unnecessary access to networks and computers, improving user security awareness, and providing early detection and

mitigation of security incidents NYSERDA can reduce the risk and drive down the cost of security incidents. Having the appropriate response levels defined for incidents and malfunctions is necessary to mitigate the total cost of the situation and reduce business disruption.

This section describes the responsibilities and the requirements for assessing, managing, and coordinating the appropriate response to security incidents and malfunctions. Incidents and malfunctions are assigned one of five levels of severity and will fall into one of four response levels.

Responsibilities

- The Information Security Officer is responsible for notifying the Director of Information Technology, relevant Information Technology department staff, or OCS, as appropriate, and initiating the appropriate incident management action including restoration as defined in the NYSERDA Information Technology "IT Contingency Plan".
- The Information Security Officer is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The technical resources involved are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The Information Security Officer, working with the Vice President for Operations and Energy Services as appropriate, will determine if a widespread NYSERDA communication is required, the content of the communication, and how best to distribute the communication.
- The technical resources involved are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- The Information Security Officer is responsible for initiating, completing, and documenting the incident investigation with assistance from the other technical resources involved.
- Because viruses and worms can reduce the functionality or otherwise affect NYSERDA's network, individuals and information technology support professionals are expected to:
    - Prevent computer equipment under their control from being infected with malicious software by the use of preventative software and monitoring; and
    - Take immediate action to prevent the spread of any acquired infections from any computers under their control.

Reporting of IT Security Incidents

Individuals should:

- ***Stop*** any IT security incident as it occurs. Power-down the computer or disconnect it from the network to stop any potentially threatening activity.
- ***Report*** IT security incidents to the IT Help Desk or to the Information Security Officer. IT support staff will assess the problem and determine how to proceed.
- ***Comply*** with the directions provided by IT support staff or the Computer Incident Response Team to repair the system, restore service, and preserve evidence of the incident.

IT Staff shall:

- Respond quickly to reports from individuals.
- Take immediate action to stop the incident from continuing or recurring.
- Determine the incident severity and response and take the appropriate actions.
- In the case of an IT department security incident, IT staff will determine if the incident involves the loss of confidential information or has other serious impacts to individuals, and:
    - If not, the IT staff will repair the system, restore service, and preserve evidence of the incident and then continue to the appropriate Response Determination.
    - If so, the IT staff will continue with Response Determination.

Response Determination

IT staff will make two assessments to determine a course of action – assessment of the level of severity and an assessment of the response level.

Assess the Severity Level:

I. Critical Business Impact

Complete loss of service or resources for which no work around exists and staff's work cannot reasonably continue. An example of a Severity Level I issue is the inability of staff to log into an application or to use a mission critical application, such as e-mail or the financial and contracts system.

II. Serious Business Impact

Staff, regardless of the environment or product usage, is experiencing significant or degraded loss of service from an application. An example of a Severity Level II issue would be a major product flaw with a work around, or an application may be running, but with a performance problem.

III. Minor Business Impact

Staff, regardless of the environment or product usage, has experienced a minor loss of service. A minor product flaw with a work around represents this type of issue.

IV. No Business Impact

Systems or software are in full working mode and staff's work is not being impeded at this time. This can be represented as a minor irritant or frustration using specific features of the software or as a result of misunderstanding or inadequate training.

V. Enhancement, Information, or Other

Staff is making enhancement requests or recommendations for consideration in future product releases.

Assess the Response Level:

I. Activation of IT Contingency Plan

There has been a full loss of mission critical computing resources. The plan can only be activated on authority of the NYSERDA President and CEO, the NYSERDA Vice President for Operations and Energy Services, or the NYSERDA's Director of Information Technology.

II. Activation of the NYS OCS Incident Response Team (IRT)

There has been or is an ongoing adverse security incident that threatens the confidentiality, integrity, or accessibility of NYSERDA information resources. These can include hacking attempts, denial of service, or failures that have adverse effects on health, economic security of the State of New York, or safety. It can include assistance with a current security situation that needs additional resources.

Examples of incidents include:

- Unauthorized access of root or administrator accounts on critical servers, routers, firewalls, etc.
- Wide spread damaging virus or worm infection.
- Major outages due to denial of service attacks.
- Mission critical application failures.
- Attacks on mission critical infrastructure services.
- Major reconnaissance scans and probes.
- Attempted denial of service attacks.
- Degradation of service attacks.
- Website defacements.

If the OCS IRT is not activated, a report must still be filed with OCS in accordance with the Cyber Security Policy P03-001, V2.0, "Cyber Incident Reporting Policy", issued June 30, 2004.

III. Notification of NYSERDA Information Security Officer

All security incidents and malfunctions are to be reported to the NYSERDA Information Security Officer.

IV. Activation of NYSERDA Help Desk

Activation of the help desk is used to assign resources to correct incidents and

malfunctions. The IT Operations will maintain a help desk escalation process to be sure appropriate action is taken.

3.0: PHYSICAL SECURITY

Critical or sensitive business information processing and storage facilities must be contained in secure areas protected by a defined security perimeter, with appropriate security barriers and some form of access controls. Physical protection measures will be implemented to protect the facility from unauthorized access, damage and interference. Physical security includes controlling access to the main building and the remote offices.

Periodic threat and risk analysis to determine where additional physical security measures are necessary must be included in the annual update to any business continuity and disaster recovery plan. Appropriate steps will be taken to mitigate the risks.

3.1: PHYSICAL SECURITY PERIMETER

Technical support staff, security administrators, system administrators, and others may have information resource physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to Information Resource facilities is extremely important to an overall security program. Therefore:

- All Information Resource facilities must be physically protected in proportion to the critically or importance of their function at NYSERDA.
- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all Information Resource restricted facilities must be documented and managed by the Information Security Officer and Facility Manager in an Access Control List.
- Card access records and visitor logs for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- The Information Security Officer must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- Upon approval of the Information Security Officer, the Facility Manager will issue and log in the Access Control List card or key access to Information Resource facilities to NYSERDA support personnel, and contractors, whose job responsibilities require access to that facility.
- Access cards or keys must not be shared or loaned to others.
- Access cards or keys that are no longer required must be returned to the Facility Manager who will then update the Access Control List.
- The Facility Manager must remove the card or key access rights of individuals that change roles with NYSERDA or are separated from their relationship with NYSERDA as well as log the update the Access Control List.
- Lost or stolen access cards or keys must be reported to the Facility Manager who will then log it into the Access Control List.

3.2: EQUIPMENT SECURITY PERIMITER

In order to prevent security threats and environmental hazards, all NYSERDA computer equipment and supporting facilities must be physically protected. This will also reduce the risk of unauthorized access to information and to protect against loss or damage.

IT Operations must administer equipment and applications within the scope of this section. With Information Security Officer and Chief Information Officer approval, third party equipment must be deployed:

- Based on value, equipment must be documented in an equipment database. The following information must be entered, but is not limited to:
    - User
    - Equipment type
    - Equipment description
    - Serial number
- Passwords must be maintained in accordance with User Password Management.(see 6.4)
- Sign out of portable devices will follow NYSERDA's guidelines for Portable Devices.(see 4.9)
- Unused equipment not directly assigned to a user will be located in a secure area.
- Immediate access to equipment and system logs must be granted to members of IT upon demand, per the section on Monitoring System Access and Use.(see 6.10)

All computer equipment must be configured to comply with the following:

- Hardware, operating systems, services, and applications must be approved by the Information Security Officer as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards.
- All patches and hot-fixes recommended by the equipment vendor and Information Security Officer must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches and hot-fixes.
- Services and applications not serving business requirements must be disabled.
- Non-secure services or protocols (as determined by the Information Security Officer) must be replaced with more secure equivalents whenever such exist.
- Security-related events for devices identified by the Information Security Officer must be logged and audit trails saved to Information Security Officer approved logs. Security-related events include, but are not limited to, the following:
    - User login failures.
    - Failure to obtain privileged access.
    - Access violations.
- The Information Security Officer will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

All computer equipment will be physically protected and secure:

- All information processing resources will be located away from hazardous processes or

materials.

- Air-conditioning units will be sufficient to support the equipment in all computing facilities.
- Adequate protection will be provided to information and information processing resources against damage from exposure to water, smoke, dust, chemicals, electrical supply interference, etc.
- Manually activated and optionally automatically activated fire suppression equipment will be installed.
    - Power to the computer room will be automatically shut off prior to water release.
    - If present the automatically activated fire suppression system should be inspected and tested annually.
    - Self-contained portable fire extinguishers will be conveniently located, well marked, and inspected and tested annually.
- Computer hardware will be protected from electrical surges.
- Power and communication lines will be underground were possible or subject to adequate protection. Networking cabling will be protected from unauthorized interception or damage.
- Two levels of access are required for entry to the computer room facility.

3.3: SECURE DISPOSAL OF MEDIA AND EQUIPMENT

If it is determined that computer equipment cannot be reused or recycled, then it should be disposed of in compliance with State of New York and federal laws for environmentally responsible disposition and in accordance with NYSERDA equipment disposal procedures.

Computers will be considered obsolete when they can no longer provide a "basic level of service" or have exceeded their useful life. Prior to disposition, the following must be met:

- Department of Defense (DoD) approved forensic software eraser method will be used to erase all NYSERDA storage devices to be disposed of or reused.
- Any storage media that cannot be forensically erased will be physically destroyed.
- Any optical media, such as CD or DVD, will be shredded.
- Any tape media will be physically destroyed or degaussed.
- A signed record of the destruction of any hard drive, whether forensically erased or physically destroyed, will be given to the Information Security Officer prior to removal or reuse.

3.4: CLEAR SCREEN

Computers are most vulnerable when the user is logged into the network and then leaves it unattended, where it is possible for unauthorized access to applications to occur, which may result in a breach in security of NYSERDA information.

Users will comply with the following:

- When leaving a computer unattended, even if only for a few minutes, users should log off or lock their computer with a password.
- Terminate active sessions when finished, unless these sessions can be secured by an appropriate lock.
- Log off all systems and networks as sessions are finished.
- Any computers whose primary function is to process data while unattended will be moved to a secure area.
- Desktop computers will be shutdown and turned off at the end of the workday.
- When possible, desktop computers will be locked or shutdown automatically by an automated process. Process according to the following schedule:

  After 10 minutes – Monitor enters power save state
  After 15 minutes –Secure screen saver (password enabled) is activated
  After 20 minutes – Computer goes into suspend mode

4.0: NETWORK

Measures will be put into place to mitigate any new security risks created by connecting NYSERDA's network to any third party network. All such connections must be authorized by the Information Security Officer. Additions or changes to network configurations must also be reviewed and approved through a change management process.

Where a server or application has been outsourced to a third party service, the Information Security Officer must perform periodic security reviews of the outsourced environment to ensure the security and availability of the information and applications.

4.1: SHARING INFORMATION EXTERNALLY

To facilitate the secure sharing of information, appropriate security measures must be in place commensurate with the sensitivity and confidentiality of the information being shared. In most cases, the security confidentiality requirements of the data being shared will determine the level of security required when sharing data.

Non-public information can only be shared outside of NYSERDA with the documented authorization of the Data Owner (unless authorized by Counsels office, including a current, signed Non Disclosure Agreement - NDA).

The documented authorization the Data Owner must provide will:

- evaluate the sensitivity of the information to be released;
- identify the responsibilities of each party for protecting the information;
- define the minimum controls required to transmit and use the information;
- record the measures each party has in place to protect the information;
- define a method for compliance measurement;
- provide a signoff procedure for each party to accept responsibilities; and
- establish a schedule and procedure for reviewing the controls.

A copy of the authorization shall be provided to the Information Security Officer.

4.2: NETWORK MANAGEMENT

Network controls maintain security of the trusted internal network and ensures the protection of connected services and networks. These controls help prevent unauthorized access and use of the NYSERDA private network. The components of network management for this section include separation of duties, remote access, and data safeguards.

This section covers:

- Any Internet Protocol (IP) networks to which NYSERDA network equipment is connected;
- All NYSERDA equipment connected to the networks;
- Any IP networks across which NYSERDA data travels;
- Data in transit over any of the networks;
- Network administrators managing the equipment; and,
- All users utilizing equipment that is connected to the network.

This includes, but is not limited to:

- the 15 Columbia Local Area Network
- the 210 Washington Avenue Local Area Network
- the Malta Local Area Network
- the Buffalo Local Area Network
- the NYC Local Area Network
- the WV User Local Area Network
- the Alb Local Area Network infrastructure
- the 17 Columbia Local Area Network (first floor)
- the 17 Columbia Local Area Network (second floor)
- the DMZ Local Area Network
- the NYSERDA Class C domain
- the NYSERDA Class B domain

Classification

This section is based on other policies, principles, and guidelines described in the NYSERDA Information Security Policies manuals. All NYSERDA network equipment (routers, switches, servers, workstations, etc.) shall be classified according to NYSERDA's classification scheme and placed in a network segment appropriate to its level of classification. Access to these segments is controlled in an appropriate manner. Whenever data travels over a network segmentation of a lower security classification than the data, it shall be protected in manner appropriate to its classification level.

All users, hosts, and data must be classified as:

- Security Level 1 "Unclassified"
- Security Level 2 "Shared"
- Security Level 3 "NYSERDA Only"
- Security Level 4 "Confidential"

All physical network segments, IP subnets, and other IP traffic carriers must be classified in the same way. All data traveling on an IP network must be classified, and all users using network equipment or requesting data over the network must be assigned a level of clearance according to the same system.

Network Segmentation

Unless otherwise stated here, all network segments are classified "Security Level 1 - Unclassified."

A network segment can only be classified as another security level with a written request to and approval from the Information Security Officer. The new level of classification must be recorded in this document.

Wherever a network segment connects to another network segment with a different security level, then the connection between the two networks must be controlled by an approved trusted point. A trusted point is equipment capable of regulating the flow of traffic between two network segments in a manner appropriate to the classification of the networks. Trusted points are covered in further detail within this section.

No network equipment may be connected to a network segment that is not of the same security level as the equipment itself.

The Information Security Officer may choose to segment two networks of the same security level.

Trusted Points

A trusted point that is used to segment two networks shall be appropriate for the network with the highest security level.

The default behavior of a trusted point is to deny all IP traffic between the network segments it protects.

At the discretion of the Information Security Officer, the default behavior of the trusted point may be to allow all traffic out from the network with the higher security level while denying all inbound traffic.

At the discretion of the Information Security Officer, the trusted point may be configured to allow specific traffic into the network with the higher security level.

All trusted points must be completely under the control of the Information Security Officer. Access to any trusted point shall only be granted with the explicit written permission of the Information Security Officer and under close supervision.

There are a number of technologies that can act as trusted points. They are divided into the following categories:

- Network Level Control such as TCP wrappers, host. allow lists, filter routers, network-level firewalls , and VIRTUAL LOCAL AREA NETWORK switches;
- User Level Control: such as application proxies, user-level firewalls ; and
- Strong User-Level Control: such as token-based user authentication systems and certificates.

Whenever there is a connection that skips over one security level the stronger user level control must be used. Even if strong user control is used, a connection may never skip more than one security level.

Control of traffic must be exercised in the manner listed below:

For connections into **SECURITY LEVEL 1** Unclassified segments		
From	**Control Type**	**Comment**
Unclassified	None	
Shared	None	
NYSERDA Only	None	Except for Internet
Confidential	None	

For connections into **SECURITY LEVEL 2** Shared segments		
From	**Control Type**	**Comment**
Unclassified	None	
Shared	None	
NYSERDA Only	None	
Confidential	None	

For connections into **SECURITY LEVEL 3** NYSERDA Only segments		
From	**Control Type**	**Comment**
Unclassified	Strong user-level Control	I.e. SMTP
Shared	Network Level Control	
NYSERDA Only	None	
Confidential	None	

For connections into **SECURITY LEVEL 4** Confidential segments		
From	**Control Type**	**Comment**
Unclassified	Not Allowed	
Shared	Not Allowed	
NYSERDA Only	Strong user-level Control	
Confidential	No Control	

Data in Transit

Data moving on the network between any two network-components is considered to be "data in transit". This also includes all control and management sessions.

All network technologies are regarded as either "safe" or "unsafe" in their native state (i.e. without any encryption). The only networks regarded as safe by NYSERDA are switched Ethernet Local Area Networks. All other network types are regarded unsafe.

All data in transit over an unsafe network segment that has a classification lower than the classification of the data must be protected by data encryption. Data in transit over a safe network segment may be encrypted at the discretion of the Information Security Officer.

Encryption of data in transit may take any of the following forms:

- Network Encryption: in which data is encrypted at the IP layer (for example, with IPSec); Session Encryption: in which data is encrypted at a TCP layer (for example, with SSL);
- Message Encryption: in which blocks of data are encrypted before they are sent (for example, with SMIME); and,
- Data Encryption: in which the entire data package is encrypted before it is transmitted (for example, with file encryption).

Encryption systems used must offer strong encryption and use internationally recognized encryption algorithms. The choice of the crypto-algorithm is the responsibility of the Information Security Officer and is laid out in NYSERDA's Cryptographic Controls. (See section 6.4)

Access to the Internet

Access to the Internet from NYSERDA networks is considered a special case. Two trusted points are used, including the Border Router and the Firewall. Encryption is accomplished by session encryption within the browser. Since user actions can override security, separate policies cover acceptable use and security awareness. Automated monitoring systems (such as network based Internet content filters) and desktop controls (such as antivirus, anti-malware, and local software firewall systems) are deployed to increase network security.

Classification of Users

Every user of the NYSERDA network is designated as “Security Level 1 - Unclassified” until their classification is explicitly changed by the Information Security Officer. NYSERDA staff will be granted “Security Level 2 - Shared” once they are assigned to a NYSERDA work group. It is the responsibility of an employee's manager to justify any requested higher levels of clearance. For example, the appropriate department head may request that an employee in the Finance Unit be granted “Security Level 3 - NYSERDA Only,” to be able to work in the Financial Management System.

The Information Security Officer is responsible for the management and control of the clearance levels for all personnel and for oversight for the System Administrators who will actually implement the security level changes.

It is the responsibility of all System Owners (the functional owner of a computer-based application can also be responsible for establishing the rules for appropriate use and protection of the data),

and System Administrators (any individual authorized by the Chief Information Officer to administer a particular information technology hardware system software) to determine the Security Level of a given user before granting that user access to any system.

It is the responsibility of the User to know his or her own clearance level and to understand the rights and limitations associated with that clearance.

Classification of Equipment

All computing equipment must be given a classification by the Information Security Officer.

Classifications for existing NYSERDA equipment are as follows:

- Security Level 1 - Unclassified, NONE.
- Security Level 2 - Shared, all equipment that is not located on NYSERDA premises; all equipment used in the transfer of data to and from the Internet;
- Security Level 3 - NYSERDA Only, all user workstations, file-servers, print-servers, etc.; and,
- Security Level 4 - Confidential, all Local Area Network servers and other hosts used in the management of the NYSERDA infrastructure or NYSERDA internal network infrastructure.

The Information Security Officer must maintain a complete list of the classifications of all computing equipment at NYSERDA.

Classification of Networks

The Information Security Officer must classify every network segment that constitutes part of the NYSERDA infrastructure. A complete list of the classifications of all network segments in the NYSERDA network is maintained by the Information Security Officer. Classifications for existing NYSERDA network segments are as follows:

- The NYSERDA VIRTUAL LOCAL AREA NETWORKs are classified as “NYSERDA only.”
- The Albany Server Local Area Network is classified as "Confidential".
- The NYC IP Circuit is classified as "Shared".
- The Buffalo IP Circuit is classified as "Shared".
- The West Valley T1 Circuit is classified as "NYSERDA only."

Classification of Data

Any NYSERDA user with legitimate access to NYSERDA data may, with sufficient justification, change the classification of the data. The user may only change the classification of data if there is sufficient, justifiable reason to do so. Users will be held strictly responsible for these decisions.

All newly created data must be classified "NYSERDA Only" until it is reclassified by a user, who does so on his or her own prerogative. Users are held solely responsible for any data whose

classification they change. Initial classifications for existing NYSERDA data are as:

- Security Level 1 – Unclassified: E-mail between NYSERDA employees and non-NYSERDA employees;
- Security Level 2 – Shared: Published information (pamphlets, performance reports, marketing material, etc.);
- Security Level 3 - NYSERDA Only: NYSERDA business information (memos, financial documents, planning documents, etc.);
- Security Level 3 - NYSERDA Only: NYSERDA customer data (contact details, contracts, billing information, etc.);
- Security Level 3 - NYSERDA Only: E-mail between NYSERDA employees;
- Security Level 4 – Confidential: Network management data (IP addresses, passwords, configuration files, etc.); and,
- Security Level 4 – Confidential: Human Resources information (employment contracts, salary information, etc.).

CLASSIFICATIONS: ROLES AND RESPONSIBILITIES

It is the responsibility of the user to:

- know his or her own clearance level and to understand the rights and limitations associated with that clearance;
- ensure all the data he or she works with is correctly classified;
- ensure that he or she understands the restrictions associated with the data he or she is working with; and
- ensure all the data he or she works with is housed and protected appropriately.

It is the responsibility of all System Owners and System Administrators to:

- determine the Security Level of a given user before granting that user access to any system;
- verify the classification of the equipment they manage; and
- verify that the equipment is installed and protected in accordance with its classification.

It is the responsibility of each Program Director (or administrative department head) to:

- obtain clearance for employees in their program;
- clarify the classification of data on systems under their control;
- clarify the classification of equipment under their control and to ensure that those systems are correctly installed; and
- ensure all employees in that Program understand and implement the security policy.

It is the responsibility of the Information Security Officer to:

- approve all classifications;
- maintain a list of all classifications;

- approve the final layout of the NYSERDA network;
- control and manage all trusted points; and
- determine the type of cryptographic protection to be used for data in transit.

4.3: VUNERABILITY SCANNING

Technical support staff, Security Administrators, System Administrators, and others may request the Information Technology staff or Information Security Officer to provide physical facility access to be able to perform scans.

When requested, and for the purpose of performing a vulnerability scan, consent may be provided to authorized NYSERDA IT or ISO staff or to an authorized external party by the Information Security Officer. Approved external parties sign a contract containing non-disclosure terms or sign a separate NDA with NYSERDA prior to being provided access for a vulnerability scan. By this policy section, NYSERDA provides its consent to allow the approved individual to access its networks and firewalls to the extent necessary to allow them to perform the scans authorized in this policy.

NYSERDA will provide protocols, addressing information, and network connections sufficient for the authorized party to utilize the software to perform network scanning.

Also by this policy section, NYSERDA grants the OCS the right to scan NYSERDA's network environment at their discretion or upon NYSERDA's request.

This access includes, but is not limited to:

- User Level and System Level access to any computing device;
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on NYSERDA equipment or premises;
- Access to work areas (offices, cubicles, storage areas, etc.); and
- Access to interactively monitor and log traffic on NYSERDA networks.

Network Control

If NYSERDA does not control parts of the network or services are provided via a second or third party, NYSERDA will obtain approval to perform a scan from the third party hosting the server(s). Under this section, all involved parties must acknowledge that they authorize in writing the designated NYSERDA staff and the independent auditors or OCS to use their service networks as a gateway for the conduct of these tests during the agreed to dates and times.

Service Degradation and Interruption

Network performance and availability may be affected by the network scanning. Therefore all scans will be performed with the knowledge of the NYSERDA Information Security Officer. At the direction of the NYSERDA Information Security Officer, scans shall be terminated if the

NYSERDA Information Security Officer determines that there is an unacceptable adverse impact.

NYSERDA recognizes the inherent risk and releases the OCS scanning team of any and all liability for damages that may arise from network availability restrictions caused by the network scanning, unless such damages are the result of gross negligence or intentional misconduct.

Client Point of Contact During the Scanning Period

If the Information Security Officer is not available, NYSERDA shall identify a person to be available if the authorized party conducting the vulnerability scan has questions regarding data discovered or requires assistance.

Scanning Period

NYSERDA and the authorized party shall identify the allowable dates for the scan to take place.

4.4: PENETRATION & INTRUSION TESTING

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems some type of assurance is needed that the systems and network are secure. Penetration and intrusion testing can provide part of that assurance.

The penetration and intrusion testing program will comply with the following:

- All NYSERDA computing systems that provide information through a public network will be subjected to NYSERDA penetration analysis and intrusion testing. Analysis and testing will be used to determine if:
    - An individual can make an unauthorized change to an application.
    - A user may access the application and cause it to perform unauthorized tasks.
    - An unauthorized individual may access, destroy or change any data.
    - An unauthorized individual may access the application and cause it to take actions unintended by the application designer(s).
- Only authorized NYSERDA staff or a qualified third party will perform penetration or intrusion testing.
- NYSERDA's Information Security Officer must approve each test.
- OCS must be notified 24 hours prior to each test.
- Operating system, user accounting, and application software audit logging processes must be enabled on all tested host and server systems whenever possible.
- Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
- Audit logging of any firewalls and other network perimeter access control system must be

enabled.

- Audit logs from the perimeter access control systems must be monitored and reviewed daily by the System Administrator.
- Host based intrusion tools will be checked on a routine basis.
- All trouble reports should be reviewed for symptoms that might indicate intrusive activity.
- Users shall be trained to report any anomalies in system performance and signs of wrongdoing to Information Technology (IT) or the Information Security Officer.
- All IP addresses of any systems used to perform penetration or intrusion testing will be provided to NYSERDA's Information Security Officer.

4.5: INTERNET AND E-MAIL ACCEPTABLE USE

Internet and e-mail are to be used for business purposes serving the interests of NYSERDA in the course of normal operations. Effective security is a team effort involving the participation and support of every NYSERDA employee and affiliate who deals with information and information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Access to Internet and E-mail Services

Internet and e-mail services are provided to all NYSERDA full time and part time employees and to all NYSERDA interns. Generally speaking, anyone who has a computer account on the NYSERDA computing facilities will have Internet access and an e-mail account as well. NYSERDA business systems may extend to remotely based e-mail (sent through laptops, home or other computers) and any Internet usage or e-mail sent through a remote system is also subject to this policy section.

Internet

- Internet access is provided to all NYSERDA full time and part time employees, and to all NYSERDA interns. Generally, anyone who has a computer account on the NYSERDA LOCAL AREA NETWORK will have Internet access.
- Users may not post classified, sensitive, confidential, or trade secret information on an open Internet website. If a User is posting classified, sensitive, confidential, or trade secret information as part of a collaboration using a password protected website such as Google Docs or Microsoft NetMeeting, the User must be aware that these websites are not necessarily secure.
- A User may not post confidential information, or information the disclosure of which is an unwarranted invasion of a person's personal privacy.
- All software used to access the Internet must be part of the NYSERDA standard software suite or approved by the NYSERDA Information Security Officer. This software must incorporate all vendor provided security patches.
- Unless authorized by the Information Security Officer, users may not download or install any executable programs on any NYSERDA owned desktops, laptops, or other electronic devices.

- Users may not download anything that would violate copyright restrictions.
- Non-business purchases made over the Internet are prohibited. Business related purchases are subject to NYSERDA procurement procedures.
- All sites accessed must comply with this section.
- User Internet activity may be subject to logging and review.
- NYSERDA will deploy content filtering software to block certain websites.
- NYSERDA websites shall be Americans with Disabilities Act ("ADA") compliant.
- NYSERDA websites shall comply with New York State mandated policies, guidelines, and standards.

E-Mail

Use of e-mail

E-mail services, like other means of communication, are to be used to support NYSERDA business. Staff may use e-mail to communicate informally with others within the NYSERDA network, so long as the communication meets professional standards of conduct. Staff may use e-mail to communicate outside of NYSERDA when such communications are related to legitimate business activities and are within their job assignments or responsibilities. Certain personal use is not prohibited when it is incidental and necessary and is limited in number and duration, such as the reasonable personal use of telephones and incidental personal electronic mail, and does not conflict with the proper exercise of the employee's duties.

Staff will not use e-mail for illegal, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interests of NYSERDA or the State of New York. Additionally, e-mail may not be used for any of the following purposes:

- to represent yourself as someone else;
- to send e-mail that is intimidating or harassing;
- to use e-mail for conducting personal business;
- to use e-mail for the purpose of political lobbying or campaigning;
- to violate copyright laws by inappropriately distributing protected works;
- for spamming;
- for unauthorized attempts to break into any computing system whether NYSERDA's or another organization's;
- for theft or unauthorized copying of electronic files;
- for posting sensitive NYSERDA information without authorization;
- for any activity which creates a Denial of Service; or
- for passing on chain letters, jokes, hoaxes or similar messages.

Staff must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of NYSERDA unless appropriately authorized to do so. An explicit disclaimer will be included, unless it is clear from the context that the author is not representing NYSERDA.

All e-mail users should:

- Be courteous and professional and follow accepted standards of etiquette.
- Protect NYSERDA and others' privacy and confidentiality. Remember messages you send are often permanent and may be republished in other media.
- Consider organizational access before sending, filing, or destroying e-mail messages.
- Protect their passwords.
- Remove personal messages, transient records, and reference copies in a timely manner.
- Comply with NYSERDA policies, procedures, and standards.

Privacy and Access

E-mail messages are not personal or private and staff does not have any reasonable expectation of privacy. E-mail System Administrators will not routinely monitor individual staff members' e-mail and will take reasonable precautions to protect the privacy of e-mail. However, senior management or system administrators with Chief Information Officer or Information Security Officer's approval may access an employee's e-mail:

- for a legitimate business purpose (e.g., the need to access information when an employee is absent for a period of time);
- to diagnose and resolve technical problems involving system hardware, software, or communications; or
- to investigate possible misuse of e-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation. This requires Senior Management, Program Directors, or Administrative Department Head Approval.

A User is prohibited from accessing another User's e-mail without his or her permission.

All e-mail messages sent or received in conjunction with NYSERDA business may be releasable to the public under the Freedom of Information Law (FOIL). Additionally special protection will be afforded to all e-mail messages that contain information protected by the Personal Privacy Protection Law. All e-mail messages, including personal communications, may be subject to discovery proceedings in legal actions.

Security

E-mail security is a joint responsibility of technical staff and e-mail users. Users must take all reasonable precautions, including safeguarding and changing passwords (in accordance with the "User Password Management" (see section 6.4), to prevent the use of the account by unauthorized individuals.

Viruses

It is possible that attachments to e-mail may be infected by a virus. To protect NYSERDA's computing facilities, never open attachments received anonymously or from unknown individuals. With increasing frequency, e-mail return addresses are faked to appear to be from a known person.

It is advised that only e-mail attachments that are expected and with a known attachment name be accepted by a user.

The NYSERDA antivirus systems, antispam systems, and other protective systems are authorized to delete any e-mail messages deemed to pose a threat to the NYSERDA computing facilities.

Records Retention

The NYSERDA e-mail system is not a records management system. The on-line system exists to facilitate communications, much as a phone system or a fax system. The off-line system, or "backup" system, exists to facilitate disaster recovery and is not intended to be a records retention system. Records communicated using e-mail need to be identified, managed, protected, and retained, as long as they are needed to meet operational, legal, audit, research, or other requirements. Records needed to support program functions shall be retained, managed, and accessible an existing filing system outside the e-mail system in accordance with the appropriate Program unit's standard practices under the direction of the NYSERDA Records Management Officer.

Records communicated via e-mail will be disposed of within the record keeping system in which they have been filed in accordance with a Records Disposition Authorization (RDA) approved by the State Archives and Records Administration (SARA). Program Managers should consult with the NYSERDA Records Management Officer concerning RDAs applicable to their program's records.

Users should dispose of copies of records in e-mail after they have been filed in a record keeping system and delete records of transitory or little value that are not normally retained in record keeping systems as evidence of Authority activity.

Management and Retention of E-mail Communications

This section applies to all e-mail messages and attachments.

Since e-mail is a communications system, messages should not be retained for extended periods of time. Users should remove all e-mail communications in a timely fashion. If a user needs to retain information in an e-mail message for an extended period, he or she should transfer it from the e-mail system to an appropriate electronic or other filing system. E-mail administrators are authorized to remove any information retained in an e-mail system that is more than 180 days old.

Management and Retention of E-mail Communications

This section applies to records communicated via e-mail

E-mail created in the normal course of official business and retained as evidence of official policies, actions, decisions or transactions are records subject to records management requirements under the New York Arts and Cultural Affairs Law and specific program requirements.

Examples of messages sent by e-mail that typically are records include:

- policies and directives;
- correspondence or memoranda related to official business;
- work schedules and assignments;
- agendas and minutes of meetings;
- drafts of documents that are circulated for comment or approval;
- any document that initiates, authorizes, or completes a business transaction; and
- final reports or recommendations.

Some examples of messages that typically do not constitute records are:

- personal messages and announcements,
- copies or extracts of documents distributed for convenience or reference,
- phone message slips; and
- announcements of social events.

Records Management Responsibilities

NYSERDA Senior Management will insure that policies are implemented by Program unit management and unit supervisors. Program unit managers and supervisors will develop and publicize record keeping practices in their area of responsibility including the routing, format, and filing of records communicated via e-mail. They will train staff in appropriate use and be responsible for ensuring the security of physical devices, passwords, and proper usage.
NYSERDA network administrators are responsible for e-mail security, backup, and disaster recovery.

4.6: EXTERNAL CONNECTIONS

External connections to network systems administered by outside parties increase the risk or security exposures to NYSERDA's Information Resources. This section works in conjunction with NYSERDA's "Network Access Control" (see Section 6.5) and "External Connections" (see Section 6.6)

External connections will comply with the following:

- Dial-up access will be in accordance with NYSERDA's "Modem Usage"(see Section 4.12)
- All connections from the NYSERDA network to external networks must be approved in writing by the Information Security Officer.
- Connections to external networks will only be allowed if found to have acceptable security controls and procedures, or appropriate security measures have been implemented by the Information Security Officer to protect NYSERDA network resources.
- A risk assessment will be performed for any connection to an external network to ensure that

the connection will not compromise NYSERDA's private network.

- Additional controls may be used between the third party and NYSERDA such as firewalls or a demilitarized zone. These controls must be periodically reviewed to ensure:
    - The business case for the connection is still valid and required.
    - The security controls in place are current and functioning correctly.

- Connection to the NYSERDA network will be done in a secure manner to preserve the integrity of the network, data transmitted over the network, and the availability of the network.
- Security requirements for each connection will be assessed individually by the Information Security Officer.
- Only authorized NYSERDA staff will be permitted to use technology on the network to monitor operational data and security events.
- The Information Security Officer will regularly review audit trails and system logs of external network connections for abuses and abnormalities where available.
- Third party network or workstation connection to the NYSERDA network must have an internal NYSERDA sponsor develop a business case for the network connection.
- All third party organizations will have an authorized representative sign a NYSERDA NDA when appropriate.
- All third party equipment must conform to New York State's security policies and standards and be approved for connection by NYSERDA's Information Security Officer.
- Encryption will be used whenever possible for any connection between NYSERDA firewalls and the external network.

4.7: SECURITY OF ELECTRONIC MAIL

Electronic mail provides an expedient method of creating and distributing messages both within NYSERDA and outside of NYSERDA. Use of e-mail systems must take into account security measures taken to protect the NYSERDA computing environment from malicious or fraudulent e-mail messages.

Users of the NYSERDA e-mail system are a visible representative of the State of New York and of NYSERDA and must use the systems in a legal, professional, and responsible manner.

Users of the NYSERDA e-mail systems must comply with “Internet and E-Mail Acceptable Use” (see Section 4.5)

The NYSERDA Information Security Officer must assure steps are taken to protect the NYSERDA computing environment from vulnerabilities created by having access to e-mail.

To assure maximum security precautions are taken, NYSERDA staff shall not connect to commercial e-mail systems from any workstation or NYSERDA system (i.e., AOL, Yahoo, MSN, Hotmail, university or college systems, etc.). Access to commercial e-mail systems via the Internet facilities or by other means will have the effect of bypassing the security systems established to

protect the NYSERDA computing environment by bringing e-mail directly into NYSERDA. The bypassed systems include an antispam server, antifraud server, and an e-mail attachment antivirus server.

The only exception to the prohibition shall be any access granted by the Information Security Officer after an analysis of the need has been conducted. The request must demonstrate why alternative means, incorporating the existing NYSERDA e-mail systems, will not meet the stated need (i.e., can mail be forwarded from the external account to the NYSERDA account, where it will be processed through appropriate security systems). Both the request and approval both must be in writing, and the approval will only be granted if it can be demonstrated that the external e-mail system has equal or greater security measures in place than NYSERDA has in place.

4.8: INSTANT MESSAGING, COLLABORATION & CONFERENCING

There are a wide variety of tools and technologies available today that allow for increased communications between employees. These services have become increasingly popular as they allow for alternative means of communication that prove to be convenient and useful. However, these tools and services may increase the risk of any security exposures to NYSERDA.

For any system that is not internal to NYSERDA:

- All instant messaging programs and services are prohibited from use at NYSERDA.
- Only NYSERDA IT conferencing applications can be used for video conferencing and web conferences.
    - Video conferencing is available and allowed from designated locations.
    - Video conferencing applications will only be used to exchange public information unless authorized by NYSERDA management and security controls are implemented to the satisfaction of the Information Security Officer.
    - Web conferencing is allowed only for systems created and run by IT Operations. (see iLinc service on NYSERDA SharePoint IT Computer training)
- Collaboration programs and services are prohibited from use at NYSERDA.

    In special cases where collaboration services are necessary to facilitate communications of Non-Confidential Information between NYSERDA and a large number of external members of a project, a request should be made to IT descri*b*ing the business need, intended use and parties involved. A review of the security of service will be performed by the Information Security Officer.

4.9: PORTABLE DEVICES

Portable devices shall be secured to prevent compromise of confidentiality or integrity.

Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number or applications. However, the portability offered by these devices creates greater risks of loss or theft.

This section establishes the rules necessary to preserve the integrity, availability, and confidentiality of NYSERDA information stored on notebook computers, handheld computers, PDAs, pagers, cell phones and other portable devices that store or transmit non-public information (data).

The following will apply:

- Only NYSERDA approved portable computing devices maybe used to access NYSERDA Information Resources.
- Portable devices shall be password protected.
- Portable devices shall be encrypted.
- NYSERDA data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
- All remote access (dial in services) to NYSERDA must be either through an approved modem pool or via an Internet Service Provider (ISP).
- Non-NYSERDA computer systems that require network connectivity must conform to NYSERDA standards and must be approved in writing by the Information Security Officer.
- Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.
- When in public places, care must be taken to avoid the risk of unauthorized persons viewing information on-screen.
- When traveling, portable laptop, notebook, palmtop, and other transportable computers must not be checked through airline luggage systems. All portable computers must remain in possession of the traveler as hand luggage.
- Because of increased risk of loss, all portable computers will routinely be backed up and the backups will comply with NYSERDA's "Information Back Up" Policy (see Section 5.6)
- The Information Security Officer or designee will periodically audit NYSERDA issued portable devices to ensure all facets of security are active and maintained at proper levels.

4.10: TELEPHONES AND FAX EQUIPMENT

The use of telephones outside NYSERDA for business reasons is sometimes necessary. However, this can create potential security exposures. Actions must be taken to decrease the possibility of any such risk.

The following are precautions that should be taken while discussing or sending sensitive material:

- When sending sensitive or confidential documents via fax, verify the phone number of the destination fax.
- Do not use third party fax services to send or receive sensitive or confidential information.
- Do not send sensitive or confidential documents via wireless fax devices.
- Do not send teleconference call-in numbers and passwords to a pager, if sensitive or

confidential information will be discussed during the conference.

- Take care that conversations are not overheard when discussing sensitive or confidential matters.
- Avoid the use of any wireless or cellular phones when discussing sensitive or confidential NYSERDA information.
- Avoid leaving sensitive or confidential messages on voice-mail systems.
- If sending sensitive or confidential documents via fax, contact the recipient to ensure protection of the fax, either by having it picked up quickly or by ensuring that the fax output is in a secure area.
- When chairing a sensitive or confidential teleconference, confirm that all participants are authorized to participate, before stating any discussion.

4.11: WIRELESS NETWORKS

Wireless technology has become increasingly popular, bringing fundamental changes to data networking and telecommunications. However, with these changes comes the risk of security exposures to NYSERDA's network. Wireless is a shared medium and everything that is transmitted goes over the radio transmitters. This represents a potential security issue for wireless Local Area Networks (LAN's).

Suitable controls such as Media Access Control (MAC) address restriction; authentication and encryption must be implemented to ensure that a wireless network or access point cannot be exploited.

Additionally:

- A risk assessment and written approval from Information Security Officer is required for the installation of a wireless network or wireless access point.
- 802.11x wireless network security features will be available and implemented from the beginning of deployment.
- Nonpublic information is not permitted via a wireless network unless appropriate measures (authentication, authorization, access controls, logging) have been implemented and approved by the Information Security Officer.
- All wireless Local Area Networks access must use Information Security Officer-approved vendor products and security configurations.
- Register Access Points and Cards
    - All wireless Access Points/Base Stations connected to the corporate network must be registered and approved by the Information Security Officer. These Access Points/Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with the Information Security Officer.
- VPN Encryption and Authentication
    - All computers with wireless Local Area Networks devices must utilize an Information Security Officer-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this section,

wireless implementations must maintain point-to-point hardware encryption of at least 128 bits. All implementations must support a hardware address that can be registered and tracked, (i.e., a MAC address.) All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

- Setting the SSID
    - The Service Set Identifier (SSID) shall be configured so that it does not contain any identifying information about NYSERDA, such as the company name, division title, employee name, or product identifier.
- All segments of the NYSERDA network incorporating wireless devices will reside on a separate Virtual Local Area Network or network.

4.12: MODEM USAGE

Modem use provides a means of access to NYSERDA's corporate network. Special precautions must be in place to avoid the compromise of NYSERDA information.

Connecting dial-up modems to computer systems connected to NYSERDA's Local Area Network or to another internal communication network is prohibited unless a business case is justified and approved by NYSERDA's Information Security Officer.

An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and NYSERDA are literal extensions of NYSERDA's corporate network, and that they provide a potential path to the company's most sensitive information. The employee and authorized third party individual must take every reasonable measure to protect NYSERDA's assets.

- For Outbound service (configured for outgoing calls only):
    - Modems must not be left in auto-answer mode, such that they are able to receive in coming dial-up calls.
    - Communication systems must not be established that accept incoming dialup calls.
    - Under no circumstances will a user attempt to add a remote access server to the network.

- For Inbound service (configured for modem to accept incoming calls only):
    - All dial-up modem phone numbers are confidential and must not to be posted or divulge to unauthorized individuals.
    - Under no circumstances will users add remote control software.
    - Dial-up modem must be configured not to answer calls before the fourth ring.
    - System configuration is set up to disconnect after three unsuccessful password attempts.
    - When not in use lines will be disconnected.

4.13: PUBLIC WEBSITE CONTENT APPROVAL

The World Wide Web provides an opportunity for NYSERDA to disseminate information and to provide government services quickly and cost effectively. Because anything posted on a public web server is globally available and each server is a potential connection path to NYSERDA, care must be exercised in the deployment of publicly accessible servers.

This section will clarify the roles and responsibilities with respect to the content, organizational structure, and design of NYSERDA's public-facing web servers. Additionally, this section will clarify what material may be posted and the security requirements for the web server(s).

This section covers all public facing web servers owned or operated by NYSERDA. This section also covers all public-facing web servers that are present on the Internet, but which may not be owned or operated by NYSERDA, but which make information available to the Internet on behalf of NYSERDA.

There are three major considerations applying to this section including review and approval of content, protection over confidential information, and security of the server. Development of the web site must also comply with the "Systems Development and Maintenance".

Review and approval

The content of each public site must be reviewed and additions or changes to the public site must be authorized. Web site content falls into one of the following categories:

1. Major Changes. Major changes include, but are not limited to: menu changes, news releases, reports, and significant updates (significant updates include adding new content, maps, photos, links to new material, adding new pages, and redevelopment of existing web pages). Requests for changes and content posting must comply with NYSERDA's Accessibility, Branding, Copyright and Fair Use Policy and Procedure.

2. Minor Changes. Minor changes include, but are not limited to: corrections which include factual updates, changes in address or phone numbers, adding a name, adding a link to previously approved material, spelling corrections, and corrections to formatting. As a result of processes in place for multiple staff to review and approve content, the following changes are also considered minor: job postings, public solicitations, and Board materials. Requests for changes and content posting must comply with NYSERDA's Accessibility, Branding, Copyright and Fair Use Policy and Procedure.

3. Responses to the Public. Responses included acknowledgments of e-mail by either an automated reply or by a designated information contact person. Responses should be sent within two working days. If responses require research, information should be sent with five to fifteen working days.

Consideration for data

When content is reviewed, consideration must include:

1. Copyright issues. Copyright issues include both the potential publication of copyright material and the appropriate protection of NYSERDA copyright material.

2. Type of information. Types of information being made available should be considered. This includes confidentiality, privacy, and sensitivity of the information.

3. Accuracy. Accuracy of the information avoids potential legal implications of providing the information.

Sensitive or confidential New York State information must not be made available through a public-facing server unless appropriate safeguards are in place. The safeguards must ensure user authentication, data confidentiality and integrity, access control; data protection and logging mechanisms are in place. Definition of sensitive information includes, but is not limited to the following:

- structures, individuals and services essential to the security, government, or economy of the State of New York, including telecommunications (including voice and data transmission and the Internet);
- electrical power, gas and oil storage and transportation;
- banking and finance;
- transportation;
- water supply;
- emergency services (including medical, fire, and police services); and
- the continuity of government operations.

Examples of sensitive information include, but are not limited to:

- critical infrastructure assets which are so vital that their infiltration, incapacitation, destruction, or misuse would have a debilitating impact on the health, welfare or economic security of the citizens and businesses of New York State;
- data that identifies specific structural, operational, or technical information, such as maps, mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities;
- training and security procedures at sensitive facilities and locations;
- descriptions of technical processes and technical architecture;
- plans for disaster recovery and business continuity;
- inventory, depictions, photographs, or locations of physical equipment, assets and infrastructure;
- reports, surveys, or audits that contain sensitive information; and
- other subjects and areas of relevant concern as determined by the Information Security Officer.

Security of hosting services

The design of a hosting service must be reviewed and approved by the Information Security Officer to ensure the security of the web server, protection of NYSERDA's network, performance of the site, and integrity and availability considerations are adequately addressed. The hosting service is subject to the "Vulnerability Scanning". (see section 4.3)

Consideration for Design

1. No personal commercial advertising may be made available via NYSERDA websites.
2. NYSERDA websites shall have an approved disclaimer and privacy policy statement. The privacy policy statement will comply with the Office for Technology (OFT) Guidelines for Internet Privacy Policies, G02-001.
3. NYSERDA websites shall comply with the OFT State of New York Common Web Banner, NYS Mandatory Technology Standard S05-001.
4. NYSERDA websites shall have an approved contacts page that complies with OFT contact Web Pages, NYS Mandatory Technology Standard S05-002.
5. NYSERDA websites shall conform to the OFT requirements for Web Accessibility, including Accessibility of State of New York Agency Web-based Intranet and Internet Information and Applications, Statewide Technology Standard S04-001, and Best Practice Guideline G06-001.

Approvals for major changes

1. The web author assembles the content.
2. The Program Director (or senior manager) approves the content.
3. Marketing, along with the content owner, will decide if the content needs to be reviewed by Legal or by Executive, and if so, their approval will be added. Marketing reviews the content in accordance with the provisions contained within this section, with emphasis on the "Considerations for Data".
4. Content is provided to the IT Technical Services Supervisor, who schedules a web administrator to upload and test the changes.
5. The web administrator notifies the web author that the content was posted.
6. The web author confirms the web content was correctly implemented.

Approvals for minor changes

1. The web author assembles the content.
2. Content is provided to the IT Technical Services Supervisor, who schedules a web administrator to upload and test the changes.
3. The web administrator notifies the web author that the content was posted.
4. The web author confirms the web content was correctly implemented.

Responses to the public

1. E-mail requests are automatically routed to the designated Subject Matter Expert.

2. Depending on the content of the request, the Subject Matter Expert either sends a response, or forwards the message to the relevant person or department, or to the Director of Communications to be treated as a FOIL request.
3. The Subject Matter Expert follows up on all referred requests to assure timely response.
4. If a response is not forthcoming within the acceptable time frame, the Subject Matter Expert sends a follow-up e-mail message to the requester as a courtesy.
5. The Subject Matter Expert maintains appropriate records of the transactions.

4.14: ELECTRONIC SIGNATURES

A signature policy is a set of rules for the creation and validation of an electronic signature, under which the validity of signature can be determined. A given legal/contractual context may recognize a particular signature policy as meeting its requirements.

The New York State Electronic Signatures and Records Act (ESRA) (9 NYCRR Part 540) created a statutory structure in New York State that supports the use of electronic signatures in everyday public and business undertakings.

At NYSERDA:

- Electronic signatures may be used in electronic transactions where there is a need for a signature.
- NYSERDA will comply with the ESRA, which states that electronic signatures are equivalent to hand-written signatures, as well as any associated rules and regulations.
- NYSERDA will comply with Chief Information Officer / Office For Technology NYS Best Practices Guidelines G04-001.

4.15: PUBLIC KEY INFRASTRUCTURE

This section will apply should NYSERDA choose to use public key technology as the preferred means of electronically authenticating the identity of individuals and of documents. Public key infrastructures, based on principles associated with public key cryptography permit, the encryption of data and the use of digital signatures to enable and facilitate secure electronic business.

To secure both internal and external electronic communications, NYSERDA plans to implement an Enterprise Certification Authority using Public Key Infrastructure (PKI) technology and an Enterprise Directory Service using Lightweight Directory Access Protocol (LDAP) technology.

The full PKI implementation is a combination of Technology, Policies and Procedures, which supports digital signatures, encryption and other inherent PKI-Enabled security services.

A PKI enables users of a basically unsecured public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and a directory service that can store the certificates.

PKI technology provides the mechanism for ensuring that electronic transactions are more secure than their paper counterparts. A PKI offers the security services of confidentiality, authenticity, integrity, and technical non-repudiation.

Essential components of the PKI are:

- A Certification Authority (CA) that issues and verifies digital certificates,
- A Registration Authority (RA) that acts as the verifier for the CA before a digital certificate is issued to a requestor,
- One or more directories where the certificate (with their public keys) are held,
- A Certification Practice Statement and Certification Policy, and
- Revocation Authority.

An Enterprise PKI using LDAP will strengthen internal and external security and NYSERDA will realize significant ease of operation and deployment through implementation of a single Organizational Certification Authority hierarchy and Directory rather than multiple ones in the various NYSERDA program areas with potentially incompatible Certification Authorities and Directories. The implementation will govern external organizations with which NYSERDA program areas may work where secure communications are required.

It is NYSERDA's goal to promote and manage the use of public key cryptography, as a component of NYSERDA's common information management and information technology infrastructure, in order to:

1. Support Government objectives with respect to service transformation and improvement;
2. Facilitate and promote, for the business of NYSERDA, the implementation and use of Public Key Infrastructures as the preferred means of authenticating the identity of individuals and documents;
3. Promote and enable the use of Common Certification Authorities;
4. Enable and encourage co-operation and collaboration between State of New York Certification Authorities; and
5. Encourage the development and use of open standards for commercial products that use public key cryptography.

NYSERDA, before it issues any Public Key Certificates (including cross-certificates), must:

1. Establish a Certification Authority.
2. Ensure that it's Certification Authority;

Manages the Public Key Certificates and Certificate Revocation Lists it issues by,

1. Implementing one or more Certificate Policies and a Certification Practice Statement with respect to the operation of that Certification Authority; and
2. Ensuring compliance with its Certificate Policy (ies) and Certification Practice Statement(s) by any individual or Entity acting on its behalf.

In applicable Certificate Policies, acceptable use policies or subscriber agreements advises Subscribers and Employees as to the respective rights and obligations of the Certification Authority, Subscribers and Employees.

NYSERDA will designate one or more officials as the Operational Authority for each Certification Authority NYSERDA operates or employs, who will provide information and/or documentation to the Information Security Officer, when requested to do so, as to any aspect of the operation of the Certification Authority.

NYSERDA's Standards

All NYSERDA deployments of a PKI shall meet FIPS 140-1 Standards (FIPS 140-1, Security Requirements for Cryptographic Modules of January 1994).

NYSERDA PKI Architecture

The NYSERDA PKI architecture shall be that of a Hierarchical Root CA (which could be either an NYSERDA Root CA system or a trusted third party). Deployments within NYSERDA shall formulate a Subordinate Certification Authority to operate under the root Certificate Policy (CP). The NYSERDA's root CA will issue certificates to the subordinate CAs. This will result in a single trust domain composed of subordinate CAs operating within the NYSERDA hierarchy.

The Subordinate CAs shall operate in accordance with the policies and procedures established by the NYSERDA Root Certification Authority.

Trust between CAs flows down from the root. Relying parties shall only directly trust other users whose CA is a member of the same hierarchy. In a hierarchy, the level of trust for a CA is a function of the level of trust associated with the CA at the root of the hierarchy.

The NYSERDA PKI architecture shall interoperate with any established State of New York Bridge Certification Authority, should one be formed as a result of the NYS Enterprise Architecture or of the NYS Strategic Plan.

Relying Party

Any subsequent NYSERDA deployments shall be considered Relying Parties.

Relying parties are obliged to use the certificate for the purpose for which it was issued in accordance with the corresponding CP and the current Certificate Practice Statement (CPS).

Prior to its use, relying parties are obliged to check each certificate for its validity, revocation, or suspension before use.

Relying parties are obliged to verify the digital signature of a received digitally signed message and to verify the digital signature of the CA that issued the certificate.

Enrollment/Registration Process

All subsequent NYSERDA deployments (under the CA) shall follow an enrollment/registration process.

The PKI user enrollment process shall minimally contain the following steps:

1. Initial Application
2. In person identity proofing
3. Key pair generation and Certificate request
4. Certificate Issuance

The NYSERDA Chief Information Officer is responsible for approving any implementation of PKI (and any subsequent deployments) at NYSERDA. The NYSERDA Chief Information Officer shall be responsible for appointing a CA PKI Manager.

The NYSERDA CA PKI Manager is responsible for:

1. Developing, maintaining currency, and publication of the Certification Practice Statement.
2. Establishing and monitoring PKI security procedures.
3. Oversight of PKI operations.
4. Identifying and investigating areas for PKI improvement.
5. Reviewing Certification Authority operations and activity.
6. All technical, hardware and software aspects of the PKI.
7. Reviewing PKI functional, technical, staffing, and budgetary plans.

5.0: OPERATIONAL MANAGEMENT

Computing hardware, software or system configurations must not be altered or added to in any way unless exempted by documented procedures or by specific written approval of NYSERDA management. Where NYSERDA provides a server, application or network service to another New York State Entity, operational and management responsibilities must be coordinated by both New York State Entities.

The roles and responsibilities of individuals who operate or use NYSERDA information processing facilities will be controlled by documented operating instructions, management processes and formal incident management procedures related to information security matters.

5.1: SEGREGATION OF SECURITY DUTIES

This section reduces the risk of accidental or deliberate system misuse.

To reduce the risk of accidental or deliberate system misuse, separation of security duties or areas of responsibility must be established. Whenever separation of security duties is difficult to achieve, other compensatory controls, such as audit trails and management supervision, must be implemented. At a minimum the audit of security must remain independent and segregated from the security function.

Transaction Authorization

Transaction authorization is the responsibility of the user department. Authorization is delegated to the degree that it relates to the particular level of responsibility of the authorized individual in the department. Periodic checks must be performed by management and audit to detect the unauthorized entry of transactions.

Custody of Assets

Custody of corporate assets must be determined and assigned appropriately. The data owner usually is assigned to a particular user department, and their duties should be specific and in writing. The data owner has responsibility for determining authorization levels required to provide adequate security, while the administration group is responsible for implementing and enforcing the security system.

Access to Data

Controls over access to data are provided by a combination of physical, system, and application security in the user area and the information processing facility. The physical environment must be secured to prevent unauthorized personnel from accessing the various tangible devices connected to the central processing unit and, thereby, permitting access to data. System and application securities are additional layers of security that may prevent unauthorized individuals from gaining access to corporate data. Access to data from external connections is a growing

concern since the advent of the Internet. Therefore, IT management has added responsibilities to protect Information Assets from unauthorized access.

Access control decisions are based on organizational policy and on two generally accepted standards of practice (1) separation of duties and (2) least privilege. Controls for effective use must not disrupt the usual work flow more than necessary or place too much burden on administrators, auditors, or authorized users. Further access must not be unconditional, and access controls must adequately protect all of the organization's resources. To ensure these, it may be necessary to first categorize the resources.

Policies establish levels of sensitivity, such as top secret, secret, confidential and unclassified, for data and other resources. These levels should be used for guidance on the proper procedures for handling information resources. They may be used as a basis for access control decisions as well. Individuals are granted access to only those resources at or below a specific level of sensitivity. Labels are used to indicate the sensitivity level of electronically stored documents. Policy-based controls may be characterized as either mandatory or discretionary.

Authorization Forms

Supervisors must provide IT with authorization forms (either hard copy or electronic) that define the access rights of their employees. This can be found on the NYSERDA Employee Orientation Form under the Rights to Network Folders and Other Information sections. Program Directors shall be responsible for determining their respective department's employee accessibility. Authorization forms must be evidenced properly with management-level approval. Generally, all users should be authorized with specific system access via written request of management.

User Authorization Tables

IT should use the data from the authorization forms to build and maintain user authorization tables. These will define who is authorized to update, modify, delete and/or view data. These privileges are provided at the system, transaction or field level. In effect, these are user access control lists. These authorization tables must be secured against unauthorized access by additional password protection or data encryption. A control log should record all user activity, and appropriate management should review this log. Access privileges should be reviewed, at least annually, to ensure that they are current and appropriate to the user's job functions. This will be done by the Information Security Officer in coordination with IT.
All exception items should be investigated.

Compensating Controls for Lack of Segregation of Duties

NYSERDA is a small business where the IT department is limited, so compensating control measures must exist to mitigate the risk resulting from a lack of segregation of duties. Compensating controls would include:

- "**Audit trails**" Audit trails are an essential component of all well-designed systems. They

help the IT and user departments, as well as, independent auditors, and IT by providing a map to retrace the flow of a transaction. They enable the user and independent auditors to recreate the actual transaction flow from the point of origination to its existence on an updated file. In the absence of adequate segregation of duties, good audit trails may be an acceptable compensating control. The independent auditor should be able to determine who initiated the transaction, the time of day and date of entry, the type of entry, what fields of information it contained, and what files it updated.

- "**Reconciliation**" Reconciliation is ultimately the responsibility of the user. In some organizations, limited reconciliation of applications may be performed by the data control group with the use of control totals and balancing sheets. This type of independent verification increases the level of confidence that the application ran successfully and that the data are in proper balance.

- "**Exception reporting**" Exception reporting should be handled at the supervisory level and should require evidence, such as initials on a report, noting that the exception has been handled properly. Management should also ensure that exceptions are resolved in a timely manner.

- "**Transaction logs**" A transaction log may be manual or automated. An example of a manual log is a record of transactions (grouped or batched) before they are submitted for processing. An automated transaction log or journal provides a record of all transactions processed, and it is maintained by the computer system.

- "**Supervisory reviews**" Supervisory reviews may be performed through observation and inquiry or remotely.

- "**Independent reviews**" Independent reviews are carried out to compensate for mistakes or intentional failures in following prescribed procedures. These are particularly important when duties in a small organization cannot be appropriately segregated. Such reviews will help detect errors or irregularities.

5.2: SEPARATION OF COMPUTING ENVIRONMENTS

This section defines the separation of the development, test and production environments for business critical development and production facilities. This reduces the risk of accidental changes and unauthorized access to production software and business data.

Since development and testing activities can cause unintended changes to software and data if sharing the same computing environment, the environments will be segregated. Separation of the development, test, and production environments can be done either logically or physically. The degree of separation must be considered by each application to ensure adequate protection of the production environment.

Additionally, processes are documented and implemented to govern the transfer of software from the development environment to the production platform.

Consideration of separation between development and test functions must also be given. In high availability production environments, the use of a stable quality assurance environment where user acceptance testing can be conducted and changes cannot be accidentally made to the programs being tested is very important. In these situations, separation must also be implemented between development and test environments.

Good design of environments will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions.

Finally, the department which requests and authorizes a computer application (the owner) must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired for, computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the information custodian.

Development Environment

- Whenever possible, the development and test staff must not be permitted to have access to production systems.
- Development and production applications will run on different servers and occasionally in separate domains.
- Development and test work will be separated at a logical level.
- Different user-IDs will be used by developers for development/test systems versus production systems.
- The system must clearly identify which environment the user is currently logged into.
- Development software and tools must be maintained on computer systems isolated from the production environment.
- Testing of all security patches and system and software configuration changes will be completed before deployment to production.
- To the highest degree, there will be a separation of duties between development/test and production environments.
- There will be a review of custom code prior to release to production to identify any potential coding vulnerability.
- Software will be adequately documented and tested before it is used for critical information.
- Production data are not used for testing or development – all production software testing must utilize sanitized information.

Production Environment

- Development and production applications will run on different servers and occasionally in separate domains.
- Rules governing the transfer of software from development to production will be established.
- Software version controls will be employed.
- Access to compilers, editors and other system utilities will be removed from production systems.

- Logon procedures and environmental identification must be sufficiently unique for production testing and development.
- Controls must be in place to issue short-term access to development staff to correct problems with production systems allowing only necessary access.
- All production systems must have designated owners for the critical information they process.
- All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to users. A designated access control administrator (who is not a regular user on the system in question) must be assigned for all production systems.
- All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.
- All test data and accounts must be removed before production systems become active.
- All custom application accounts, usernames, and passwords must be removed before applications become active.
-

Change Control

A formal change control process will be deployed. At a minimum, the change control process will include:

- Documentation of impact of the change.
- Management sign-off by appropriate parties.
- Proof of testing that verifies operational functionality.
- Back-out procedures.

5.3: SYSTEM PLANNING AND ACCEPTANCE

Planning for system capacity and availability must be addressed by the IT department. Guidelines for the acceptance of new information technology deployment must be made within the constraints set by the computing environment.

It is the responsibility of the IT department to ensure that information technology investments are justified by sound business cases and linked to NYSERDA business plans, that they align with NYSERDA's and the State of New York's enterprise information technology strategies and are leveraged to the maximum extent reasonable for the benefit of the enterprise, and that necessary information about such investments is available for information sharing, reporting, and planning purposes.

The IT department is also responsible for recommending and developing IT-related administrative rules, policies, standards, practices and guidelines for NYSERDA in support of making those information technology investments. Policy development duties will be conducted by the Chief Information Officer who will:

- serve as a resource for IT-related rule and policy interpretation;
- seek broad based input and collaborative rule and policy development with authority stakeholders;
- track and coordinate IT-related rule and policymaking;
- review, evaluate and report the effectiveness of policy implementation; and
- conduct research on "best practices" and industry trends.

Because system and data availability is a security concern, advance planning and preparation will be performed to ensure the availability of adequate capacity and resources. Storage and memory capacity demands will be monitored and future capacity requirements projected to ensure adequate processing and storage capability is available when needed.

IT system capacity upgrade projects, security projects, and other IT projects will be interrelated with implementation planning for new initiatives via a governance group to assure proper planning and control over system development and growth. Control includes:

- identification of capacity requirements for each new and ongoing system/service;
- projection of future capacity requirements, taking into account current use, projected trends, and anticipated changes in business requirements; and
- system monitoring and tuning to ensure and, where possible, improve availability and effectiveness of current systems.

All NYSERDA staff will seek approval from the Chief Information Officer in advance of information technology investments, whether directly or by the contracting process, that will be deployed at NYSERDA, including Commercial Off The Shelf software, custom software, hardware, custom developed databases, and custom developed web sites. IT investment review and approvals will seek to:

- Assure purchases and initiatives conform to system capacity planning.
- Align authority spending with the Governor's priorities and initiatives, the State of New York Chief Information Officer / Office For Technology Enterprise Architecture (EA) Strategy, and other related statewide plans, initiatives, goals and objectives.
- Ensure that the information technology investment is linked with authority business plans;
- Facilitate risk assessment of information technology projects and investments;
- Ensure that information technology investments are justified on the basis of sound business cases;
- Facilitate development and review of information technology performance related to business operations;
- Ensure that NYSERDA thoroughly analyzes (and reengineers, if appropriate) authority business processes prior to the automation of those processes through investments in technology.
- Ensure that projects are effectively and efficiently run utilizing appropriate system development lifecycle, project management, and quality assurance methodologies.
- Identify projects, and ensure that NYSERDA explores opportunities to partner with others on projects, that can cross agency and program lines to leverage resources.

- Via the Chief Information Officer Council, and other State of New York organizations, assist in state government-wide planning for common, shared information technology infrastructure.

Acceptance criteria must be developed and documented for new information systems, upgrades and new versions of existing systems. Acceptance testing will be performed by the system owner to ensure requirements are met prior to the system being migrated to the production environment. Authority managers will ensure that the security requirements and criteria for acceptance are clearly defined, agreed, documented and tested. Control includes:

- clear definition of, agreement on, testing of, and documentation of compliance with requirements for system acceptance; and
- consultation with affected persons, or representatives of affected groups, at all phases of the process.

5.4: PROTECTION AGAINST MALICIOUS SOFTWARE

Information Resources are those pieces of data and the systems they reside on that are recognized as valuable to an organization. They are not easily replaceable without cost, skill, time, resources or a combination. They form a part of a corporation's corporate identity. Information security identifies the threats against the risks and the associated potential damage to, and the safeguarding of Information Resources.

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Anti Virus

- All workstations whether connected to the NYSERDA network, or standalone, shall use the IT approved virus protection software and configuration.
- The virus protection software shall not be disabled or bypassed.
- The settings for the virus protection software shall not be altered in a manner that will reduce the effectiveness of the software.
- The automatic update frequency of the virus protection software shall not be altered to reduce the frequency of updates.
- Each file server attached to the NYSERDA network shall utilize NYSERDA approved virus protection software and setup to detect and clean viruses that may infect file shares.
- Each e-mail gateway shall utilize IT approved e-mail virus protection software and must adhere to the IT rules for the setup and use of this software.
- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Information Security Officer.

Anti Malware

- An antispam gateway will be deployed to stop e-mail from being delivered which contains links to websites which may attempt to download malware.
- Patch levels of windows will be maintained at current versions, or as close to current versions as possible, to keep the Microsoft Malicious Software Removal Tool at current revision levels.
- A web content filter will be deployed to restrict access from websites which may attempt to download malware.
- IT security and the Information Security Officer will cooperate with external security organizations to coordinate firewall rules to block known harmful Internet websites.

5.5: SOFTWARE MAINTENANCE

Maintaining software at current versions is a method of identifying and removing weaknesses that can be used to compromise the confidentiality, integrity, or availability of a computer information asset. Regularly installing updates is a preventative information security practice that removes weaknesses before they can be used to compromise a computer information asset.

For production systems:

- All system software must be maintained at a vendor-supported level to ensure software accuracy and integrity, unless the Information Security Officer approves otherwise in writing.
- A change management system or process will be used to ensure changes are appropriately authorized, tested and accepted.
- All known security patches must be reviewed, evaluated and appropriately applied in a timely manner to reduce the risk of security incidents that could affect the confidentiality, integrity, and availability of business data or software integrity.

5.6: INFORMATION BACKUP

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system failures, malicious attacks, data entry errors, or system operation errors.

For information backup of data center systems at NYSERDA:

Information backed up

- A risk assessment will be performed to determine the criticality of the business systems the time frame required for recovery, and the frequency of backup.
- All NYSERDA business units will work in cooperation with the Information Security Officer to develop approaches that can meet the IT backup and recovery requirements of NYSERDA.

- Backups of critical NYSERDA data and software will be performed in accordance with the requirements of the NYSERDA disaster recovery plan.
- Restoration will be performed in accordance with the requirements of any, to be created, NYSERDA disaster recovery plan.

Backup Processes

- NYSERDA's IT operations must document and periodically review the backup and recovery process for each system.
- Backups must be periodically tested to ensure that they are recoverable. A log of such activity will be maintained.
- Backup media will be stored off site
- Backup media must have at minimum the following identifying criteria that can be readily identified by labels or a bar-coding system:
    - System Name
    - Creation Date
- A log book will be kept detailing the transport of media, both to and from the offsite storage facility.
- An inventory of all backup media will be maintained.
- Backup media will be encrypted whenever possible.
- Any loss of backup media constitutes a security incident and must be reported to the Information Security Officer and must be handled in accordance with the Cyber Security Citizens' Notification Policy (see Section 8)

5.7: RISK ASSESSMENT

Risk analysis is a method of identifying vulnerabilities, threats, the likelihood of loss and its impacts, theoretical effectiveness of security measures and the possible damage in order to justify security safeguards. It is used to ensure that security is cost effective, relevant, timely, and responsive to threats. Therefore:

- An assessment of the critical services provided and the sensitivity of the information held on all servers (including all installed software and operating system versions, firewalls, switches, routers, and other communication equipment operating systems) will be maintained.
- A periodic assessment of a representative sample of portable devices or desktops will be conducted to ensure compliance with NYS, OCS, and NYSERDA policies. The assessment may include, but is not limited to, configuration, patching, and antivirus signatures are at appropriate levels and information or data is appropriately stored.

- The execution, development and implementation of remediation programs are the joint responsibility of the Information Security Officer and the departments responsible for the systems are being assessed.

- Employees will fully cooperate with any risk assessment being conducted on systems for

which they are held accountable.

Risk Assessment Guidelines

- Assign value to information and assets.
- Estimate potential loss per risk.
- Perform a threat analysis.
- Derive the overall loss potential per threat.
- Reduce, assign, or accept the risk.

5.8: SYSTEM SECURITY CHECKING

Systems and services that process or store Personal, Private, and Sensitive Information (PPSI) or provide support for critical processes will undergo technical security reviews to ensure compliance with implementation standards and for vulnerabilities to subsequently discovered threats. Reviews of systems and services that are essential to supporting a critical authority function must be conducted at least once every year. Reviews of a representative sample of all other systems and services must be conducted at least once every 24 months.

Any deviations from expected or required results that are detected by the technical security review process must be reported to the NYSERDA Information Security Officer and corrected immediately. In addition, the NYSERDA application owner must be advised of the deviations and must initiate investigation of the deviations (including the review of system activity log records if necessary).

A formal certification and accreditation (C&A) process will be used. This is the process by which an information system is assessed to determine that the system meets the security requirements for the mission function and the sensitivity of information handled.

The C&A process will consist of four phases: Initiation, Certification, Accreditation, and Continuous Monitoring:

1. ***Initiation*** is the phase in which the System Owner prepares for certification activities. This includes preparing the required documentation, notifying the Information Security Officer that the system is ready for C&A, and ensuring that a System Security Plan (SSP) is created and is up-to-date.

2. ***Certification*** is the phase in which a certification team performs a comprehensive evaluation of the information system's technical and non-technical security features and other safeguards to establish the extent to which the information system meets the specified security requirements. When the information system passes certification, the System Owner assembles the accreditation package. The accreditation package includes the Security Agreement Report (SAR), the updated SSP, and the Plan of Action & Milestones (POA&M).

3. ***Accreditation*** is the phase in which the System Owner submits the accreditation package to management (or their designee) who will act as a Designated Approving Authority (DAA). The DAA decides whether or not the system will be authorized to operate. The DAA issues the decision in a letter, and transmits the decision letter and the accreditation package back to the System Owner. The System Owner either deploys the information system to production (via NYSERDA IT policies) or further modifies it as needed to receive an authorization to operate.

4. ***Continuous monitoring*** is the phase that occurs after the information system receives authorization to operate, in which the System Owner monitors and tracks changes to the information system's security controls over time. Reaccreditations must be performed when a significant change occurs to the information system or every three years. The system may require recertification if a significant change requires testing by the certification team. Reaccreditations may also be required if a new authorizing official is assigned to the information system.

A major component of the process will depend on a risk assessment. As needed, for this section, NYSERDA will follow the guidance of the National Institute of Standards and Technology (NIST), Special Publication 800-30, "Risk Management Guide for Information Technology Systems", July 2002.

6.0: ACCESS CONTROL

NYSERDA Information Assets will be protected by logical and physical access control mechanisms commensurate with the value, sensitivity, consequences of loss or compromise, legal requirements, and ease of recovery of these assets.

6.1: USER REGISTRATION AND MANAGEMENT

This section defines the process to control the creation, deletion, and modification of user accounts, other than administrative and privileged accounts, which are discussed in Section 6.3.

Information access owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges will be. These privileges will be granted in accordance with the user's job responsibilities. The user management process defines the generation, distribution, modification and deletion of user accounts for access to resources.

The appropriate Data Owner or other authorized party will make requests for the registration and granting of access rights for NYSERDA employees. For purposes of this section, notice must come from Human Resources for new or exiting employees and notice from the employee's supervisor or the Data Owner for the changing of access rights.

For applications that interact with individuals that are not employed by NYSERDA, the Data Owner is responsible for ensuring an appropriate user management process is implemented. The Data Owner must define standards for the registration of such external users including the credentials that must be provided to prove the identity of the user requesting registration, validation of the request, and the scope of access that may be provided.

ENROLLING NEW USERS

1. Notice shall be provided to the IT Operations Support Manager by a representative of Human Resources whenever a new employee is to be given access rights to any of NYSERDA's computing facilities.

2. Human Resources shall initiate the process by providing the starting date, user's full name (including at least a middle initial), office location, phone extension, title, department, gender, and name of user's direct supervisor or other information as needed.

3. An IT operations staff member will then be authorized to create the account and create temporary passwords that the user must change. The User will be granted access to their department group folder.

4. IT Operations will complete and submit a "NYSERDA Orientation Form" to the Information Security Officer. The new user signs the document indicating, at a minimum, that they have changed their passwords, they know how to reach the IT help desk, they have a basic understanding of core applications (such as e-mail), and that they have taken

the Cyber Security Awareness Training.

REMOVING USER-IDs

1. Notice shall be provided to the IT Operations Support Manager by a representative of Human Resources whenever an employee will be terminating employment with NYSERDA (usually 2-week notice).

2. Human Resources shall initiate the process by providing the date the resignation was received, the exit date, the user's full name, and name of user's direct supervisor to the IT Operations Manager or other information as needed.

3. The IT Operations Manager will initiate the IT Technical Services exit process and the Information Security Officer exit process.

4. An IT Operations staff member will be authorized to initiate the exit process steps which can be completed prior to the user's exit date (such as establishing automated e-mail notices).

5. On the user's exit date, Human Resources require an "Employee Exit Clearance Form" to be signed by the Director of Information Technology or designee. The user's accounts can then be disabled.

6. IT Operations will complete and submit a "NYSERDA Employee Exit Checklist" to the Information Security Officer.

PERIODIC REVIEWING OF USERS ENROLLED TO ANY SYSTEM

On a periodic basis, the Data Owner is responsible for ensuring that appropriate reviews of the individuals that are employed by NYSERDA are valid users.

ASSIGNING A NEW AUTHENTICATION TOKEN

All personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any NYSERDA facility, has access to the NYSERDA network, or stores any non-public NYSERDA information must adhere to “User Password Management”, including password strength and password aging.

Any user, who requires a password reset, will contact the IT Help Desk. A temporary password will be assigned, which must be changed by the user.

6.2: LOGON BANNER

Logon banners must be implemented to give users fair notice of what NYSERDA considers acceptable use of the computer systems. They also provide fair notice of expectations.

Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for business or other approved use consistent with NYSERDA policy, and that user activities may be monitored, and the user should have no expectation of privacy. Logon banners are usually presented during the authentication process.

All computer systems, including but not limited to computer equipment, work product and data software, storage media, and network accounts providing e-mail, web browsing, and desktop applications are the property of NYSERDA. These systems are to be used for business purposes in serving the interests of NYSERDA and of our clients and customers in the course of normal operations.

Prior to authentication to the NYSERDA network, the following logon banner will be displayed:

NOTICE

> This system and all data on it are the property of NYSERDA. Unauthorized use or attempted unauthorized use of this system is not permitted and may constitute a crime. Such use may subject you to appropriate disciplinary and/or criminal prosecution. Use of this system is only permitted under the auspices of NYSERDA. Use is limited to conducting the official business of NYSERDA. Use for incidental and necessary personal purposes is permitted, provided that such use is in a limited amount and duration and does not conflict with the proper exercise of the duties of the employee. Any use, whether authorized or not, may be monitored, intercepted, recorded, read, copied, accessed, or captured in any manner, and used or disclosed in any manner, by authorized personnel without additional prior notice to users. Users have no legitimate expectation of privacy during any use of this system or in any data on this system. Use whether authorized or unauthorized, constitutes express consent for NYSERDA to monitor, intercept, record, read, copy, access or capture and use or discloses such information.
>
> By clicking OK, you certify that you have read and accept the above terms and conditions.

6.3: PRIVILEGED ACCOUNT MANAGEMENT

The use of privileged accounts will be restricted and controlled.
Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program. Inappropriate use of system account privileges is often found to be a major contributing factor to the failure of systems that have been breached. Therefore:

- All users of administrative or special access accounts must have account management instructions, documentation, training, and authorization when necessary.

- Each individual that uses administrative or special access accounts must refrain from abuse of privilege and shall only do investigations under the direction of the Information Security Officer.

- Each individual that uses administrative or special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).

- Each account used for administrative or special access must meet the NYSERDA User Password Management Policy. (See 6.4)

- When special access accounts are needed for internal or external audit, software development, software installation, or other defined need, they:

  - must be authorized by the Information Security Officer;
  - must be created with a specific expiration date; and
  - must be removed when work is complete.

6.4: USER PASSWORD MANAGEMENT

This section controls password integrity to authenticate a user's identity and will be automated whenever possible.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of NYSERDA's entire corporate network. As such, all NYSERDA employees (including contractors and other affiliates with access to NYSERDA systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Guidelines:

- All system-level passwords (e.g., root, admin, application administration accounts, etc.) must be changed on a quarterly basis.
- All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed quarterly basis.
- The minimum password age will be 7 days. Password age is the length of time users need to wait before a password can be changed again.
- The password uniqueness (history) will be 12 passwords. Uniqueness is the number of new passwords that must be used before an old password can be reused.
- The account will be locked out after 6 failed logon attempts.

- The account lockout duration will be forever (until reset by an authorized person).
- All user-level and system-level passwords must conform to the guidelines described below.

"**Password Construction**" Passwords are used for various purposes at NYSERDA. Some of the more common uses include: user level accounts, web accounts, e-mail accounts, screen saver protection, and voice-mail password. Since very few systems have support for one-time tokens (i.e.) dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Strong passwords will:

- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Have numeric digits and punctuation characters as well as letters.
- Be at least eight alphanumeric characters long.
- Not be a word in any language, slang, dialect, jargon, etc.
- Not be based on personal information, names of family, etc.
- Not be the same as the user's ID.

"**Password Protection Standards**" Strong passwords need to be protected from discovery. The following standards will help protect passwords from discovery:

- Do not use the same password for NYSERDA accounts as for other non-NYSERDA access (e.g., personal ISP account, option trading, benefits, etc.).
- Do not use the "Remember Password" feature of Windows applications.
- Do not share NYSERDA passwords with anyone, including administrative assistants. All passwords are to be treated as sensitive, confidential NYSERDA information.
- Do not reveal a password over the phone to anyone and never reveal a password in an e-mail message unless it is a single use password.
- Do not talk about a password in front of others and don't hint at the format of a password (e.g., "my family name").
- Do not share a password with family members and don't reveal a password to co-workers while on vacation.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on any computer system (including PDAs, cell phones, or similar devices) without encryption.

If someone demands a password, refer the individual to this section or call the Information Security Officer.

If an account or password is suspected to have been compromised, report the incident to the Information Security Officer and change all passwords.

The Information Security Officer, IT managers or their designees may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

6.5: NETWORK ACCESS CONTROL

The NYSERDA network infrastructure is provided as a central utility for all users of NYSERDA information resources. It is important that the infrastructure, which includes cabling and the associated active equipment, continues to develop with sufficient flexibility to meet NYSERDA demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Network access will consist of:

- Access to NYSERDA's network requires a User-ID and an authentication mechanism (password, token, and smart card, digital certificate) to validate all authorized users.
- Users are responsible for all activity performed with their personal User-IDs. User-IDs may not be used by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their User-IDs. Similarly, Users are forbidden from performing any activity with User-IDs belonging to other users.
- Network controls will ensure that users are permitted to use only those network addresses issued to them by the NYSERDA IT department.
- Users must not extend or re-transmit network services in any way. This means users must not install a router, switch, hub, or wireless access point to the NYSERDA network without Information Security Officer approval.
- Users must not install network hardware or software that provides network services without Information Security Officer approval.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, NYSERDA users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the NYSERDA network infrastructure.
- Users are not permitted to alter network hardware in any manner.

6.6: EXTERNAL CONNECTIONS (REMOTE ACCESS CONTROL)

To maintain information security, NYSERDA requires that individual accountability be maintained at all times, including during remote access.

Connection to NYSERDA's networks must be done in a secure manner to preserve the integrity of the network, data transmitted over that network, and the availability of the network. Security mechanisms must be in place to control access to NYSERDA systems and networks remotely from fixed or mobile locations. (see "External Connections" Section 4.6).

Advance approval for any such connection must be obtained from NYSERDA Senior Management and the Information Security Officer. An assessment must be performed and documented to determine the scope and method of access, the risks involved and the contractual, process and technical controls required for such connection to take place.

Because of the level of risk inherent with remote access, use of two-factor authentication, such as a security token, is required prior to connecting to any NYSERDA network. All sessions are subject to periodic and random monitoring.

When accessing a NYSERDA network remotely, identification and authentication of the entity requesting access must be performed in such a manner as to not disclose the password or other authentication information that could be intercepted and used by a third party.

Use of a common access point is required where all remote connections to a computer must be made through managed central points-of-entry. Using this type of entry system to access a NYSERDA computer provides many benefits, including simplified and cost effective security, maintenance, and support.

For a vendor to access NYSERDA computers or software, individual accountability is also required. For those systems (hardware or software) for which there is a built-in User-ID for periodic maintenance, the account must be disabled until the User-ID is needed. The activity performed while this vendor User-ID is in use must be logged. Since these accounts are not regularly used, the vendor User-ID must be disabled, the password changed or other controls implemented to prevent or monitor unauthorized use of these privileged accounts during periods of inactivity.

In the special case where servers, storage devices, or other computer equipment has the capability to automatically connect to a vendor to report problems or suspected problems, the Information Security Officer must review any such connection and process to ensure that connectivity does not compromise the NYSERDA or other third party connections.

Working from a remote location must be authorized by NYSERDA Senior Management and appropriate arrangements made for this activity through written policy and procedure, to ensure the work environment at the remote location provides adequate security for NYSERDA data and computing resources. Appropriate protection mechanisms commensurate with risk and exposure must be in place to protect against theft of NYSERDA equipment, unauthorized disclosure of

NYSERDA information, misuse of NYSERDA equipment or unauthorized access to the NYSERDA internal network or other facilities by anyone including family and friends. To ensure the proper security controls are in place and all NYSERDA security standards are followed, the following must be considered:

- the physical security of the remote location including using a laptop at any location other than an employee's work station;
- the accessing mechanism given the sensitivity of NYSERDA's internal system the sensitivity of and method of transmitting information; and
- Appropriate business continuity procedures including backing up critical information.

The following controls must be considered and appropriately implemented. If implemented, they must be monitored and audited:

- a definition of the classification of the information and the systems and services that the remote user is authorized to access;
- documented procedures and necessary tools allowing for secure remote access such as security tokens and passwords, including procedures for revocation of authorization and return of equipment;
- hardware and software support and maintenance procedures including anti-virus software and maintenance of current signature files;
- implementation of suitable network boundary controls to prevent unauthorized information exchange between NYSERDA networks connected to remote computers and externally connected networks, such as the Internet. Such measures include firewalls and intrusion detection techniques at the remote location; and
- physical security of the equipment used for remote access (e.g. such as cable locking device, or locking computer cabinet or secure storage area).

For encryption requirements, refer to "Cryptographic Controls" (see Section 7.4).

6.7: SEGREGATION OF NETWORKS

This section protects NYSERDA's network from other connected networks.

A cornerstone in the foundation of information security is controlling how resources are accessed so they can be protected from unauthorized modification or disclosure. The controls that enforce access control can be technical, physical, or administrative in nature. The segregation of networks takes advantage of all three mechanisms by placing a physical control with embedded technologies that must be maintained at a high security level by application of administrative controls governing maintenance.
When the NYSERDA network is connected to another network, or becomes a segment on a larger network, controls must be in place to prevent users from other connected networks access to sensitive areas of NYSERDA's network. Routers or other technologies will be implemented to control access to secured resources on the trusted NYSERDA network.

6.8: OPERATING SYSTEM ACCESS CONTROL

Access to operating system code, services and commands must be restricted to only those individuals necessary in the normal performance of their job responsibilities. All individuals (systems programmers, database administrators, network and security administrators, etc.) will have a unique privileged account (User-ID) for their personal and sole use so that activities can be traced to the responsible person. User-IDs will not give any indication of the user's privilege level, e.g., supervisor, manager, administrator. These individuals should also have a second User-ID when performing normal business transactions, such as when accessing the NYSERDA email system.

In certain circumstances, where there is a clear business requirement or system limitation, the use of a shared User-ID/password for a group of users or a specific job can be used. Approval by the Information Security Officer and Senior Management must be documented in these cases. Additional compensatory controls must be implemented to ensure accountability is maintained.

Where technically feasible, default administrator accounts will be renamed, removed, or disabled. The default passwords for these accounts will be changed if the account is retained, even if the account is renamed or disabled.

6.9: APPLICATION ACCESS CONTROL

The dissemination and manipulation of information resources across large-scale networks of computers is increasingly prevalent. As a result, common concern is drawn to the security of resources in distributed systems, which deals with many aspects, such as identification and authentication of users, encryption of resources and access control.

To prevent unauthorized access to information held in information systems, access to NYSERDA business and systems applications is restricted to those individuals who have a business need to access those applications or systems in the performance of their job responsibilities. Access to source code for applications and systems is restricted. Only authorized NYSERDA staff, contractors, and other affiliates can access source code and only for those applications and systems they directly support.

Access control will normally be accomplished with system account access privileges. Internal access controls will be used where available and may include authentication with roll based controls. For high availability, mission critical, or PPSI, additional security tools will be deployed in accordance with suitable risk mitigation from a formal risk assessment.

6.10: MONITORING SYSTEM ACCESS AND USE

Systems and applications must be monitored and analyzed to detect deviation from the "Access

Control" and record events to provide evidence and to reconstruct lost or damaged data. Audit logs recording exceptions and other security-relevant events must be produced and kept consistent with record retention schedules developed in cooperation with the New York State Archives and Records Administration (SARA) and NYSERDA requirements to assist in future investigations and access control monitoring. IT, in consultation with Functional Users, will define, create, review and protect the audit logs.

7.0: SYSTEMS DEVELOPMENT AND MAINTENANCE

This section assures accurate data, to protect software applications from unauthorized access, and to provide for application security.

Software applications store, manipulate, retrieve and display information. NYSERDA becomes dependent on the applications and it is essential the data processed be accurate and protected from unauthorized access or tampering.

To ensure that security is built into all information systems, all security requirements, including the need for rollback arrangements, must be identified during the requirements phase of a project. The Information Security Officer must be involved in all phases of the System Development Life Cycle (SDLC) which is a formal process of developing information systems through investigation, analysis, design, implementation and maintenance. SDLC is also known as information systems development or application development.

Security requirements and controls must reflect the business value of the information involved, and the potential business damage that might result from a failure or absence of security measures. This is especially critical for Internet web and other online applications.

Controls in systems and applications can be placed in many places and serve a variety of purposes. The specific control mechanisms must be documented at the application level, in the System Development Methodology, and in security standards documents. The security measures that are implemented must be based on the threat and risk assessments of the information being processed and cost/benefit analysis.

7.1: INPUT DATA VALIDATION

An application's input data must be validated to ensure it is correct and appropriate including the detection of data input errors. Personnel must be clearly identified to perform these functions. The checks that are performed on the client side must also be performed at the server to ensure data integrity. Checks will be performed on the input of business transactions, static data (names, addresses, employee numbers, etc.) and parameter tables. Set up a process to verify and correct fields, characters, completeness of data and range/volume limits.

Data validation also ensures that a program operates on clean, correct and useful data. It uses routines, often called validation rules that check for correctness or meaningfulness of data that are input to the system. The rules may be implemented through the automated facilities of a data dictionary, or by the inclusion of explicit application program validation logic.

The simplest data validation verifies that the characters provided come from a valid set. For example, telephone numbers should include the digits and possibly the characters +, -, (and) (plus, minus and the parentheses). A more sophisticated data validation routine would check to see the

user has entered a valid country code; the number of digits entered matches the convention for the country or area specified, etc.

Incorrect data validation can lead to data corruption or security vulnerability. Data validation checks that the data are valid and sensible/reasonable before they are processed. Some methods used for data validation are:

- *Format or picture check* Checks that the data is in a specified format (template), e.g., dates have to be in the format DD/MM/YYYY.
- *Data type checks* Check the data type of the input and give an error message if the input data does not match with the chosen data type, e.g., In an input box accepting numeric data, if the letter 'O' was typed instead of the number zero, an error message would appear.
- *Range check* Checks that the data lie within a specified range of values, e.g., the month of a person's date of birth should lie between 1 and 12.
- *Limit check* Unlike range checks, data is checked for one limit only, upper OR lower, e.g., data should not be greater than 2 (>2).
- *Presence check* Checks that important data are actually present and have not been missed out, e.g., customers may be required to have their telephone numbers listed.
- *Check digits* Used for numerical data. An extra digit is added to a number which is calculated from the digits. The computer checks this calculation when data are entered, e.g., The ISBN for a book. The last digit is a check digit calculated using a modulus 11 method.
- *Batch totals* Checks for missing records. Numerical fields may be added together for all records in a batch. The batch total is entered and the computer checks that the total is correct, e.g., add the 'Total Cost' field of a number of transactions together.
- *Hash totals* This is just a batch total done on one or more numeric fields which appears in every record, e.g., add the Telephone Numbers together for a number of Customers.
- *Spelling check* Looks for spelling and grammar errors.
- *Consistency Checks* Checks fields to ensure data in these fields corresponds, e.g., If Title = "Mr.", then Gender = "M".
- *Typical Data* Data that is usually entered into a system. This is to check that normal information can be entered into the system.
- *Extreme data* This is data that is used only in certain rare occasions. For instance, a birth date extreme data type would be 29/02/1910, which are the 29th of February (being a leap year date) and an unlikely birth date for a currently living person.
- *Invalid Data* Data that should not be accepted into the system, for instance in a Telephone Number, inputting symbols and letters should then be stopped.

Typical controls to put in place to safeguard a production system should include:

- validation checks of data entered at the database level;
- roll back at the database if transactions are not fully completed;
- use of replication or two-phase commit mechanisms;
- validation of changes, additions and deletions to web content for critical or sensitive web sites;
- encryption of passwords at all times;

- remove the ability to make any changes or additions and deletions to data held in a database made by any other means than the appropriate business application; e.g. the use of end-user tools to directly modify databases must be limited to authorized support and administrative personnel;
- checking hard copy input documents for unauthorized changes prior to input;
- have a processes for appropriate action if validation errors occur;
- define the responsibilities of those involved in data input;
- maintain audit trails (logs);
- perform integrity verification programs such as consistency and reasonableness checks to look for evidence of data tampering, errors, and omissions;
- where possible, conduct system performance monitoring to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes, and
- encryption of data fields that contain PPSI.

7.2: CONTROL OF INTERNAL PROCESSING

Data that has been entered correctly can be corrupted by processing errors or through deliberate acts. Checks and balances must be incorporated into systems to prevent or stop an incorrect program from running. Application design must ensure that controls are implemented to minimize the risk of processing failures, leading to a loss of data or system integrity. Whenever possible use correction programs to recover from failures, provide the ability to make changes to application data, and to ensure the correct processing of data.

Validation checks should be incorporated into applications to detect the corruption of information through processing errors or deliberate acts.

Responsibilities should be defined along with processes for responding to detected errors.

7.3: MESSAGE INTEGRITY

Traditional paper-based communications accompanied by handwritten signatures provide three essential security characteristics: message integrity, originator authentication, and non-repudiation. Depending on the nature of the communication, an additional security characteristic, confidentiality, may be desired. The effectiveness of the various techniques used to ensure the desired level of security in turn depends on the adequacy of the administrative controls associated with their use.

The communication components defined are:

- *Message integrity* the assurance that the content of a communication is complete and has not been changed prior to receipt.
- *Originator authentication* provides assurance that the communication originated from the

named source.

- *Non-repudiation* is a stronger form of authentication which relates to the ability of a disinterested third party to reasonably conclude that the identified originator intended to be bound by the substance of the communication.
- *Confidentiality* is the ability to limit access to the information contained in a communication.

Electronic messages need to achieve the same level of effectiveness as the paper counterpart. The validity of an electronic message deals with methods that ensure that the contents of a message have not been tampered with and altered. The most common approach is to use a one-way hash function that combines all the bytes in the message with a secret key and produces a message digest that is impossible to reverse.

For any PPSI electronic message transmitted by NYSERDA, it is necessary to put into place a method to detect unauthorized changes to the content of the transmitted electronic message.

Message integrity must also be considered for applications where there is a security requirement to protect the message or data content, such as electronic funds transfer, EDI transactions, etc.

An assessment of threats and risks will be performed to determine if message integrity is required and to identify the most appropriate method of implementation. It should also be noted that message integrity will not protect against unauthorized disclosure.

7.4: CRYPTOGRAPHIC CONTROLS

This section provides a means of protecting the authenticity and integrity of electronic documents.

As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. The art of protecting information by transforming, or encrypting it, into an unreadable format is commonly used today to protect e-mail messages, credit card information and corporate data. Encryption is a technique that can be used to protect the confidentiality of information.
Based on a risk assessment, the required level of protection will be identified taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys employed. To the extent possible, consideration must also be given to the regulations and national restrictions that may apply to the use of cryptographic techniques in different parts of the world. In addition, and to the extent possible, consideration must be given to controls that apply to the export and import of cryptographic technology.

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric cryptosystem keys must be of a length that yields equivalent strength. NYSERDA's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by

qualified experts outside of the vendor in question and approved by (OCS). The export of encryption technologies is restricted by the federal government.

7.5: KEY MANAGEMENT

The proper management of cryptographic keys is essential to the effective use of cryptography for security. Keys are analogous to the combination of a safe. If a safe combination becomes known to an adversary, the strongest safe provides no security against penetration. Similarly, poor key management may easily compromise strong algorithms. Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded to the keys. All keys need to be protected against modification, and secret and private keys need to be protected against unauthorized disclosure. Key management provides the foundation for the secure generation, storage, distribution, and destruction of keys.

A secured environment must be established to protect the cryptographic keys used to encrypt and decrypt information. Keys must be securely distributed and stored. Access to these keys must be restricted to only those individuals who have a business need to access the keys. Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted.

As needed for this section, NYSERDA will follow and adhere to the recommendations published by the National Institute of Standards and Technology (NIST) in NIST Special Publication 800-57, March, 2007, "Key Management – Part 1: General (Revised)". This recommendation provides cryptographic key management guidance. It consists of three parts: Part 1 provides general guidance and best practices for the management of cryptographic keying material; Part 2 provides guidance on policy and security planning requirements for U.S. government agencies; and Part 3 provides guidance when using the cryptographic features of current systems.

Additionally, as needed for this section, NYSERDA will follow and adhere to the recommendations published in NIST Special Publication 800-57, DRAFT (April, 2005), "Recommendation for Key Management – Part 2: Best Practices for Key Management Organizations". Part 2 of the Recommendation for Key Management is intended primarily to address the needs of system owners and managers. It provides context, principles, and implementation guidelines to assist in implementation and management of institutional key management systems. It identifies applicable laws and directives concerning security planning and management, and suggests approaches to satisfying those laws and directives with a view to minimizing the impact of management overhead on organizational resources and efficiency.

7.6: PROTECTION OF SYSTEM TEST DATA

Test data is intended to test the expected behavior of software, systems and applications. Test data is developed to test a comprehensive set of conditions and outcomes, including exception

processing and error conditions, to demonstrate accurate processing and handling of information and the stability of the software, system, or application.

Once test data is developed, it must be protected and controlled for the life of the testing. In those cases where test data is reused, whenever modifications are made to the software, system or application then the test data must be protected and controlled during the entire useful life. This protection mechanism is essential to ensuring a valid and controlled simulation with predictable outcomes.

Production data may be used for testing only if the following controls are applied:

- a business case is documented; approved in writing by the Data Owner; and access controls, system configurations, and logging requirements for the production data are applied to the test environment; or
- a business case is documented, approved in writing by the Data Owner, and PPSI will be masked or overwritten with fictional information and the data will be deleted as soon as the testing in completed.

7.7: CHANGE CONTROL

This section minimizes the possibility of corruption of information systems.

The Information Resources infrastructure at NYSERDA is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong change management process is essential.

From time to time each Information Resource element requires an outage for planned upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure. Therefore:

- every change to a NYSERDA Information Resource such as operating systems, computing hardware, networks, and applications are subject to the Change Control Procedures;
- support programmers only have access to those parts of a system necessary to perform their job;
- access to source code libraries for both NYSERDA applications and operating systems will be tightly controlled;
- access to source code libraries by authorized individuals will be logged and monitored when possible; and
- where possible, change control tracking and reporting will be automated.

Change Control Procedures, in General (changes to certain computer applications have specific

processes used to document these procedures):

- Request for a change to take place
    - Requests should be presented to the Technical Services Manager who is responsible for approving changes and overseeing the activities of change that take place within an environment.
- Approval of the change
    - The individual requesting the change must justify the reasons and clearly show the benefits and possible pitfalls of the change. Sometimes the requester is asked to conduct more research and provide more information before the change is approved.
- Documentation of the change
    - Once the change is approved, it should be entered into the Change Log. The Change Log should be updated as the process continues toward completion.
- Tested and presented
    - The change must be fully tested to uncover any unforeseen results. Depending on the severity of the change, the change and implementation may need to be presented to the Chief Information Officer. This helps show different signs to the purpose and outcome of the change and the possible ramifications.
- Implementation
    - Once the change is fully tested and approved, the Technical Services Manager may need to develop a schedule that outlines the projected phases of the change being implemented and the necessary milestones. These steps should be fully documented and progress should be monitored where necessary.
- Report changes to management
    - A full report should be submitted to the Chief Information Officer summarizing the change. This report can be submitted on a periodic basis to keep the Chief Information Officer up to date and ensure continual support.

8.0: CYBER SECURITY CITIZENS NOTIFICATION

This section covers unauthorized acquisition of private information.

Policy

If NYSERDA owned or licensed computerized data that includes private information is acquired, or is reasonably believed to have been acquired, by a person, without valid authorization, due to a breach of the security of the system, NYSERDA will disclose such breach to residents of New York State whose private information was, or is reasonably believed to have been, acquired.

Procedure for Reporting Breaches

If NYSERDA determines there has been, or reasonably believes there may have been, a breach of the security of private information, it will consult with the Office of Cyber Security (OCS) to determine the scope of the breach and restoration measures.

After consultation with OCS and with respect to the private information that may have been disclosed, the Information Security Officer will implement the following procedures:

NYSERDA-Owned or Licensed Data. If NYSERDA computerized data that includes private information, is acquired by a person, without valid authorization, due to a breach of the security of the system, the Information Security Officer will immediately notify the Treasurer and the General Counsel of such breach and will disclose such breach to residents of New York whose private information was, or is reasonably believed to have been, acquired, in accordance with the Notice Requirements section below.

Disclosure will be made in the most expedient time possible, without unreasonable delay, but consistent with: (a) the legitimate needs of law enforcement (e.g., immediate disclosure would impede a criminal investigation, in which case notification would be made after the law enforcement agency determines that disclosure would not compromise such investigation), and (b) any other measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Additional Requirements for Private Information Not Owned by NYSERDA. If NYSERDA does not own the computerized data that includes the private information that is acquired, or reasonably believed to be acquired, by a person, without valid authorization, due to a breach of the security of the system, the Information Security Officer will immediately notify the Treasurer and the General Counsel of such breach. The Information Security Officer will also notify the owner or licensee of the information of the breach of the security of the system immediately following discovery.

Notice Requirements

In consultation with the Treasurer and the General Counsel, the Information Security Officer will provide notice directly to the affected New York residents by one of the following methods:

(a) written notice;

(b) electronic notice, if the person has expressly consented to receiving said notice in electronic form (and a log of each such notification is be kept by the office of the Information Security Officer);

(c) telephone notification (and a log of each such notification is kept by the office of the Information Security Officer); or

(d) if a determination is made that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or NYSERDA does not have sufficient contact information, the Information Security Officer will notify the State Attorney General of this determination, and if the State Attorney General concurs with such determination, notice will be given by the Information Security Officer by:

(1) e-mail notice, when an e-mail address is available for the affected New York resident;

(2) conspicuous posting of the notice on NYSERDA's web page; and

(3) notification to major Statewide media.

The notice will include contact information at NYSERDA and a description of the categories of information that were, or are reasonably believed to have been, acquired, including specification of which of the elements of personal information and private information were, or reasonably have been, acquired.

The ISO shall promptly file a New York State Security Breach Reporting Form with the State Attorney General, the Consumer Protection Board, and OCS. The form is located on NYSERDA’s Sharepoint intranet site.

In the event that more than five thousand New York residents are to be notified at one time, NYSERDA will also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. This notice will be made without delaying notice to affected New York residents.

9.0: COMPLIANCE

This section provides for audit and control over information systems security.

NYSERDA managers and supervisors will ensure that all security processes and procedures with their areas of responsibility are followed. Their compliance may be subjected to reviews the Information Security Officer to ensure compliance with security policies and standards.

OCS is the owner of Cyber Security Policy P03-002 “Information Security Policy”. The policy is a statement of the minimum requirements, ethics, responsibilities and accepted behaviors required to establish and maintain a secure environment and achieve the state's information security objectives. NYSERDA is a New York State entity and as such, NYSERDA's compliance with P03-002 is mandatory.

Consistent with P03-002, OCS may perform periodic reviews of NYSERDA's security programs for compliance with this and other security policies and standards. OCS establishes and monitors effectiveness of information security policy, standards, and controls within the State of New York. In addition to its compliance monitoring capacity, OCS also acts as the security consultant to the Information Security Officer.

The policies in this section are put into place to provide for audit and control over NYSERDA's, Information Security Policies and Procedures Manual.

9.1: MONITORING

This section provides for NYSERDA's rights to monitor and control information systems.

Consistent with applicable law, employee contracts and NYSERDA policies, NYSERDA reserves the right to monitor, inspect and search at any time all NYSERDA information systems.

The Chief Information Officer, Information Security Officer, and Executive Management shall have the right to inspect at anytime, any or all of NYSERDA’s computers and systems.

NYSERDA’s computers and networks are provided for business purposes. Staff shall have no expectation of privacy in the information stored in or sent through these information systems.

NYSERDA’s Chief Information Officer, Information Security Officer, and Executive Management retains the right to remove from its information systems any unauthorized material.

Please refer to Section 6.2 “Logon Banner” for NYSERDA’s fair notice of expectations.

9.2: COMPLIANCE

This section provides for audit, control, and review.

NYSERDA will take every step necessary, including legal and administrative measures, to protect its assets and has established the post of the Information Security Officer to monitor compliance with policy matters.

NYSERDA managers and supervisors will ensure that all security processes and procedures within their areas of responsibility are followed and their compliance may be subject to reviews by the Information Security Officer to ensure compliance with security policies and standards.

OCS

OCS may periodically review NYSERDA's compliance with P03-002. Such reviews may include, but are not limited to, reviews of the technical and business analyses required to be developed pursuant to P03-002, and other project documentation, technologies or systems which are the subject of the published policy or standard.

Compliance with P03-002 is mandatory. Each user must understand their role and responsibilities regarding information security issues and protecting NYSERDA's information.

The failure to comply with P03-002 or any other security policy that results in the compromise of NYSERDA's information confidentiality, integrity, privacy, and/or availability may result in appropriate action as permitted by law, rule, regulation, policy or negotiated agreement.

As part of NYSERDA’s Internal Controls, NYSERDA will annually determine the level of compliance with P03-002. Areas where compliance with the policy requirements is not met will be documented and reported to Chief Information Officer and to OCS. The Chief Executive Officer will certify NYSERDA’s Level of Compliance with this policy in writing to OCS by December 31st of each year. For each area of non-compliance, a plan will be developed to address the deficiencies, and if requested, forwarded to OCS. A risk assessment of the area of noncompliance may be required by the Information Security Officer.

Audit

When requested, and for the purpose of performing an audit, the Information Security Officer may consent to grant access to NYSERDA information systems to: authorized NYSERDA staff, NYSERDA’s independent auditors, or consultants retained by NYSERDA’s Internal Audit department. The Information Security Officer may also grant access to other authorized government organizations (such as Office of the State Comptroller, Inspector General, Attorney General) when that access is required to support authorized audits or investigations. The approved individual(s) will be granted access to networks, hardware or documentation to the extent necessary to allow them to perform the audit.

Any release of security information or confidential materials is subject to Information Security Officer's approval.

No security information or confidential materials shall be released to any auditor unless an appropriate Non Disclosure Agreement or contract with NDA or Confidentiality language is in place.

9.3: ENFORCEMENT AND VIOLATION HANDLING

The enforcement of NYSERDA's security policies are intended to effectively manage the risk of security exposure or compromise within NYSERDA systems. The policies communicate the responsibilities for the protection of NYSERDA information, establish a secure and stable processing environment, and attempt to reduce the chance for errors to be introduced into an electronic system supporting a business process. The policies preserve management's options in the event of an information asset misuse, loss or unauthorized disclosure and they promote and increase the awareness of information security.

Any compromise or suspected compromise of any of NYSERDA's technology systems must be handled in accordance with "Security Incidents or Malfunctions Management" Section 2.3. Any violations of NYSERDA's security policies may be subject to disciplinary or other appropriate action in accordance with law, rule, regulation, policy, or negotiated agreement.

Access authorization for user accounts involved in a compromise may be suspended during the time when a suspected violation in under investigation. Upon request, automated violation reports generated by the various security systems may be forwarded by the Information Security Officer to the Director of Human Resources or a member of executive management or senior management for use in such an investigation.

Any employee found to have violated NYSERDA's information security police will be required to comply and may be subject to disciplinary action, up to and including termination of employment.

10.0: GENERAL SECURITY

The policies in this section are specific to NYSERDA and are in addition to the mandatory requirements of the New York State Office of Cyber Security (OCS) as set forth in Cyber Security Policy P03-002.

10.1: COMPUTER AND LAPTOP ASSIGNMENT

This section ensures that NYSERDA desktop and laptop computers are used for purposes appropriate to its mission; are used in compliance with policies; are used cost effectively; comply with permissible data storage use and network security standards; and, prevent misuse of computers and network services.

NYSERDA's Information Technology Department maintains an inventory of hardware and software for use by employees in conducting normal daily business activities. The IT Department issues these desktop and laptop computers to staff for the purpose of conducting NYSERDA business.

Assignment

- All NYSERDA employees are assigned a desktop computer at or near their start date. NYSERDA's daily business needs will generally include word processing; Internet based research and information gathering, and communication via electronic mail. A computer is considered essential for NYSERDA employees and is a standard office appliance.
- All NYSERDA computers are normally assigned on a three- year cycle and typically become eligible for upgrades upon completion of the fixed asset depreciation.
- Certain personal use of NYSERDA computers is not prohibited when it is incidental and necessary and is limited in number and duration, such as the incidental personal electronic mail, and does not conflict with the proper exercise of the employee's duties. Information security is a high priority and therefore all use of NYSERDA assigned computers are subject to the policies found in the "NYSERDA Information Security Policies and Procedures Manual, which governs usage, passwords, virus protection and many other factors.
- IT Operations are responsible for administration of desktop and laptop computers, including activities such as procurement, inventory control, configuration, troubleshooting, operation, decommissioning, and disposal.
- IT Operations is responsible for the determination of the assignment of desktop computers.
- Assignment of laptop computers is based on evaluation of individual job responsibilities and functions:
    - Executive Management: The President and CEO, the vice President, the Treasurer, General Counsel, and other officers are eligible for a laptop via notice to the Director of IT.
    - Directors: Supported by a justification sent to the Director of IT and with approval of an Officer and with concurrence of the Chief Information Officer, Directors are eligible for a laptop in lieu of a desktop computer.

    - Staff: In very specific situations of value or need to NYSERDA, staff are eligible for assignment of a laptop. These circumstances must be documented and the additional approval of their Director must be supplied along with approval of an officer and the concurrence of the CIO. The laptop will be assigned in lieu of a desktop computer.
    - Function: A laptop may be temporarily assigned to a staff member via a sign out pool managed by IT Operations. Use is restricted to travel, presentations, work level needs outside of business hours, or other needs deemed appropriate by the Manager of IT Operations. These temporary assignments are on a first-come first-serve basis, are expected to be short term in duration, and a log must be kept of the assignment, as well as, the condition of the laptop upon assignment and return.
- Employees are responsible for all IT equipment assigned to them and if there is any problem, the employee must contact the IT Helpdesk to arrange for correction as soon as possible.
- Computers are property of NYSERDA. Upon separation from NYSERDA, employees must return all equipment in good working condition. IT Operations will confirm, by use of an inventory tracking system, that all assigned equipment has been returned.
- NYSERDA requires all computers to run data encryption software. In the event of loss or theft of computers, the employee must immediately report the incident to the Information Security Officer for appropriate handling. Theft will be reported to the police.

10.2: BORROWING HARDWARE AND SOFTWARE

NYSERDA maintains an inventory of hardware and software for use by employees in conducting normal daily business activities. At times, the need may exist for employees to conduct business activities outside of the normal business hours or away from NYSERDA's official offices. At such times, employees may be allowed to take NYSERDA equipment into their possession for a limited time for business purposes.

Process

- Employees may borrow certain hardware or software for use outside of NYSERDA for a finite length of time.
- Available hardware includes laptop computers, projectors, memory sticks, modems, cables, or other items now in the sign-out pool and which are approved by the Director of IT
- Employees may request the use of software packages. The employee must agree to comply with applicable laws, copyright and license agreements and to fully uninstall the software prior to its return.
- To request the hardware or software, employees must submit a signed, written request to the Director of IT or his or her designee.
- The Director of IT or his or her designee must issue a signed approval to the employee, which details the equipment being signed out, the duration of the loan and the statement of agreement. The detail will include the description, serial number, and other necessary identifying information to uniquely identify the equipment.

- In the statement of agreement, the employee will agree that equipment remains the property of NYSERDA, that it may need to be returned prior to the agreed upon date, that they accept the responsibility for taking reasonable precautions to assure the equipment is returned in good working order, and that the equipment will be returned by the agreed upon date. In the case of software, the employee will agree that they will uninstall the software prior to returning it to NYSERDA.

Employee Sign Out

- Equipment may be reserved using the electronic resource reservations system or by calling or e mailing the Help Desk. An expected return date is required.
- Upon pick up, a signature is required on the equipment sign out form, indicating acceptance for responsibility of the equipment and peripheral components (power cables, mouse, and external drives). A small card will be distributed containing the user name and logon password. It is important that the password card is kept separate from the equipment.
- A laminated page will be placed in each equipment bag listing the contents of the bag and how each item should be returned (i.e. cables should be coiled). When the equipment is returned contents will be compared to the page. This will help IT to ensure that the next person using the equipment has a working unit and they have all the items they may need.
- Equipment must be returned directly to an IT staff member. Items should not be left in IT offices or the equipment sign out areas.
- Upon return, the equipment will be inspected by IT to ensure that it is in good working order and that all components have also been returned. IT will sign the equipment sign out form indicating that all equipment has been returned properly and is in good working order. Any discrepancies will be reported and submitted for repair/replacement.
- Any difficulties with equipment while in possession should be relayed to IT.
- On a monthly basis, the following maintenance procedure will be performed by IT on all NYSERDA sign out pool portable computers:

  - Antivirus updates
  - Change power-on password
  - Change log-on password
  - Apply Windows critical Operating System updates
  - Modem dialer updates
  - Remove any unused data from hard drive and desktop

10.3: SOFTWARE DISTRIBUTION

Ensures that NYSERDA desktop and laptop computers are configured for a baseline purpose.

The IT Department prepares computers for use by employees to facilitate their ability to conduct normal daily business activities. Basic software is installed on all computers prior to their distribution to employees.

IT Operations will provide certain software that is commonly used by the majority of employees, including but not limited to word processing, spreadsheet, and presentation software (such as Microsoft Office), anti-virus software (such as Symantec), PDF reader (such as Adobe Acrobat), email and calendar software (such as Microsoft Outlook), and a web browser (such as Microsoft Internet Explorer). Other applications may become part of this baseline install.

Employees may not install software on NYSERDA computers including downloaded software, free software, or purchased software owned by an individual. Employees wishing to have a software application installed on their computer must request it using the "Software Request" form. Software found not to be in compliance with copyright laws or with this policy will be removed. IT staff are authorized to remove software with or without the employees knowledge or consent.

Software installed on NYSERDA computers may not be used for non business purposes, including for personal purposes or for outside activities of any kind. Certain software, such as Internet Explorer, may be used for incidental and necessary personal purposes providing that such use is in a limited amount and duration and does not conflict with the proper exercise of the duties of the employee.

Information security is a high priority and therefore all use of NYSERDA assigned computers and software is subject to the policies found in the "NYSERDA, Information Security Policies and procedures manual".

IT Operations are responsible for administration of baseline desktop and laptop software, including activities such as procurement, inventory control, configuration, troubleshooting, operation, decommissioning, and disposal.

Employees are responsible for all IT installed software assigned to them and if there is any problem, the employee must contact the IT Helpdesk to arrange for correction as soon as possible.

Software licenses are the property of NYSERDA. Upon separation from NYSERDA, employees must relinquish access to all copies of software. IT Operations will confirm, by use of an inventory tracking system, that all returned licenses are available for redeployment as needed and that NYSERDA is in compliance with owned versus deployed licenses.

No employee shall copy or distribute software that violates copyright laws. All employees shall be aware that software and the accompanying documentation are generally owned by the manufacturer and the license only grants the user the right to use the software. Unlicensed software installations, also known as software piracy, are unacceptable at NYSERDA.

10.4: SOCIAL MEDIA

Purpose and Applicability

This policy establishes the policies and procedures for the use of any Social Media through NYSERDA's computer network systems, or the use of a NYSERDA-affiliated account on a Social Media Site, including use by NYSERDA employees, and use by approved contractors on NYSERDA's behalf.

Policy

It is NYSERDA's policy to establish, maintain, and enforce the highest standards of integrity and fairness in all business dealings, including the use of social media technologies. In the discharge of related duties, each employee shall observe the highest standards of business and personal ethics, while promoting NYSERDA's objectives and interests, and conduct themselves in a manner that will withstand public, media, legal, and organizational scrutiny. Due to the mass communication aspects of Social Media Sites, NYSERDA employees, and contractors working on NYSERDA's behalf, must be particularly attentive and self-vigilant of the potential implications of their communications in these forums.

Guiding Principles and Procedures

Only specific NYSERDA employees, based on their job responsibilities, and authorized contractor employees, will be granted access to a NYSERDA-affiliated account on a Social Media Site in order to administer such account on behalf of NYSERDA. Such employees will be approved by the Director of External Affairs and documented in writing to the Information Security Officer and Chief Information Officer. Documentation will specify the employee's roles (read, post, edit) for accessing the Social Media Site account. In accordance with Guiding Principle and Procedure B, if the request is for access to a Social Media Site for which NYSERDA has not previously approved access, the Information Security Officer shall consult with Counsel's Office to determine if the requested Social Media Site's Terms of Service is acceptable.

A) Approved employees shall use such sites only for official, authorized purposes.

1. An employee may request access to a Social Media Site by submitting a written request to the employee's immediate supervisor, which shall include a description of the purpose for accessing the Social Media Site and the benefits to NYSERDA from providing such access to the employee's immediate supervisor for approval.

2. If the immediate supervisor is below the Program Manager (or Administrative Department Head) level, the request shall also be approved by the Program Manager/Administrative Department Head.

3. Once approved, the completed request shall be submitted to the Information Security Officer for approval. In accordance with Guiding Principle and Procedure B, if the request is for access to a Social Media Site for which NYSERDA has not previously approved access, the Information Security Officer shall consult with Counsel's Office to determine if the requested Social Media Site's Terms of Service policy is acceptable.

B) Use of Social Media Sites shall be subject to the Terms of Service for each individual site. When possible, NYSERDA shall be subject to specially developed terms for state governments.

    1. Counsel's Office shall review the Terms of Service and evaluate the risks and capabilities of NYSERDA, or its employees, to agree to certain terms, including: the site's conditions of use and access privileges; NYSERDA's ownership of the data and ability to retrieve it, including guidelines for records management; conflict of laws, jurisdictional and venue provisions; liability and indemnification provisions; and any other applicable New York State laws and practices. Counsel's Office shall approve whether NYSERDA shall agree to use any Social Media Site, either through a NYSERDA-affiliated account or through an individual employee account, based upon its Terms of Service and whether the terms are acceptable to NYSERDA's interests.

    2. If approved by Counsel's Office, the Information Security Officer shall determine if there are any significant information security issues associated with providing access to the Social Media Site through NYSERDA's computer network. The Information Security Officer shall also consult with the Chief Information Officer to determine if there are any computer network system operational issues or costs associated with providing access to such Social Media Site.
    3. If approved, access to such Social Media Site shall be provided as soon as practicable. If denied, the reason for denial shall be communicated by the Information Security Officer to the requestor in writing.

C) Each NYSERDA employee or contractor, that has been authorized to access a NYSERDA-affiliated account on a Social Media Site, or authorized to access a Social Media Site from within NYSERDA's computer network, shall comply with the following:

    1. Only authorized and designated individuals shall have permission to publish content through a NYSERDA-affiliated account on a Social Media Site.

    2. Will conduct themselves in accordance with NYSERDA's policies and procedures, including, but not limited to, the Internal Control Manual and the Employee Code of Conduct.

    3. Will not use social media sites to look up or screen applicants. Such action could violate principles of Affirmative Action &/or anti-discrimination laws if certain identifying information is gained.

4. Will record all contacts that a reasonable person would infer was an attempt to influence a procurement in accordance with Section 4.9 of the Operations and Procedures Manual.

5. Will not post classified, sensitive, confidential, or trade secret information.

6. Will replace error with fact, not argument.

7. Must note the use of incorrect information or misstatements.

8. Must use best judgment for all activities.

9. Will not post offensive content, defined as content which is obscene, pornographic, threatening, defamatory, discriminatory or harassing.

10. Will, as soon as practical, remove offensive content posted by other parties on any NYSERDA-affiliated account on a Social Media Site, but shall maintain a copy of such content prior to removal as part of records management requirements.

11. Will respect copyright, fair use and financial disclosure laws.

12. Will not publish or report on conversations or information that is has not been released as final NYSERDA policy or internal to NYSERDA unless given permission by management.

13. Will not post confidential information, or information the disclosure of which is an unwarranted invasion of a person's personal privacy.

14. NYSERDA-affiliated accounts on a Social Media Site shall be created using an official NYSERDA email account.

15. Any NYSERDA account on a Social Media Site shall contain visible elements that identify them as an official NYSERDA site. Among other items, this includes displaying the official NYSERDA logo and providing contact information and link(s) to official websites.

16. An individual shall be appointed to be responsible for periodically monitoring and maintaining content on each NYSERDA-affiliated account on any Social Media Site.

17. Use of NYSERDA-affiliated accounts on any Social Media Site that is not Americans with Disabilities Act Section 508 ("ADA") web accessible shall contain "simple" text links to identical material on a compliant website or other social media network. The Information Security Officer will be responsible for running an ADA scan on all NYSERDA-affiliated accounts to ensure their compliance.

18. Any NYSERDA-affiliated account on a Social Media Site shall prominently display, or provide a link to, NYSERDA's Disclaimer, Privacy Policy, Contact Information, and

Citizen Conduct Guidelines.

Citizen Conduct Guidelines for NYSERDA Social Media Venues

The New York State Energy Research and Development Authority (“NYSERDA”) encourages the public, as well as members of NYSERDA, to participate in and contribute content to NYSERDA Branded Social Media Venues ("Website"). Contributors (hereinafter referred to as “Participants”) are encouraged to take advantage of the many opportunities to provide input that the Website(s) afford, and in so doing contribute to a fair and respectful dialogue among the general public and NYSERDA.

To promote open and productive dialogue, and in the spirit of fair and transparent access to NYSERDA’s Website(s), Participants are hereby advised that all postings, including any links to 3rd-party sites, shall be subject to limited monitoring for appropriateness. For purposes herein, appropriateness is defined as postings that are relevant to NYSERDA’s official governmental business, responsive to the issue(s) being discussed, and phrased in respectful and appropriate language for the general public.

The following types of content are considered inappropriate for posting on NYSERDA Website(s):
commercial; self-promotional; campaign-related; prurient; abusive; discriminatory speech, including but not limited to, hate speech based on race, gender, sex, national origin, age, sexual orientation, religion or disability; offensive content including but not limited to, items that are obscene, pornographic, threatening, defamatory, or harassing; in certain contexts personal contact information.

If content is determined to be inappropriate, such content either will not be posted or will be removed from the Website by a NYSERDA External Affairs staff member designated for such review (“the Reviewer”). Such action will be taken in order to maintain the effective operation of the Website(s) as a forum for civil, constructive and thoughtful discourse. If a Participant notices that his or her content is not posted within 48 hours of submission, and he or she wishes to dispute the determination by the Reviewer, such Participant may request an explanation of rejection by the Reviewer at http://www.nyserda.org/ContactInformation/Default.asp.

Participants should note the following prior to posting content on this site:

(a) Regarding community-moderated content, a participant may flag content he or she believes to be in violation of this Citizen Conduct Guideline. He or she may not

19. NYSERDA-affiliated Social Media Site account administrators shall review site activity and content for exploitation or misuse.

20. Supervisors of employees granted access to Social Media Sites shall be responsible for monitoring employee use of those Social Media Sites.

21. Perceived or known compromises to NYSERDA-affiliated accounts on any Social Media Site shall be promptly reported to the Information Security Officer.

D) An employee is not permitted to use Social Media Sites for personal use in the workplace.

E) Content posted to a NYSERDA-affiliated account on a Social Media Site that is considered an electronic record, is subject to disclosure under the Freedom of Information Law (New York State Public Officers Law, Article 6). For these reasons, NYSERDA shall maintain copies of postings that are vital to the transaction of public business and that evidence NYSERDA's public functions, decisions and operations. Where such materials are in the custody of a third party provider, NYSERDA shall make reasonable efforts to obtain a copy of such when needed for public access or record preservation purposes.

In addition, content posted to a NYSERDA-affiliated account on a Social Media Site is subject to record retention and disposition requirements of the New York State Arts and Cultural Affairs Law. Therefore, NYSERDA must maintain a copy of all content posted to a Social Media Site that is considered a record in accordance with NYSERDA's General Retention Schedule.

F) Social Media Security considerations.

1. Staff shall use unique user accounts with strong passwords, in accordance with NYSERDA's password policy, wherever possible. For sites which do not allow unique usernames/passwords for site administration and posting, additional care should be exercised by staff to protect the shared username and password being used by multiple authorized staff. For both unique accounts and shared accounts, users shall comply with NYSERDA's password change policy.

2. In instances where access to NYSERDA accounts has been provided to NYSERDA contractors to administer accounts or post content on NYSERDA's behalf, additional care shall be exercised to periodically monitor the work of such contactors, and contractual language shall exist specifying the contractor's authorization for posting content on NYSERDA's behalf. Once a contractor has completed work or the contract has ended, the password on all NYSERDA accounts accessed by the contractor must be changed.

3. Staff responsible for posting content shall adhere to expectations for acting within their level of authority and shall be responsible for consulting with supervisory and management staff prior to posting or responding to sensitive matters.

H) A NYSERDA employee who has access to Social Media Sites at work may only use it for official, authorized purposes. Any employee who has access to Social Media Sites at work may not use them for personal use.

I) If the employee is acting in an approved official capacity, but states his or her own opinion, then the employee must include the following disclaimer when posting information: "The postings on this site are my own and don't necessarily represent NYSERDA positions, strategies or opinions."

J) Social Media Sites which are approved for use shall be reviewed not less than annually by Counsel's Office, the Information Security Officer, and the Chief Information Officer to ensure that no unacceptable changes to the site's Terms of Service policies or significant information security issues should result in the discontinued use of such sites by NYSERDA.

10.5: AMERICANS WITH DISABILITIES ACT

This section establishes the process regarding the Americans with Disabilities Act (ADA). The policy calls for all reasonable accommodations to be made to qualified individuals.

The purpose of this section is to address several accommodations being made by the Information Technology Department (IT) and to provide information on obtaining further services.

The accommodations outlined may apply in a variety of situations and are intended to include employees, contractors, and guests and visitors to varying degrees.

Contact information is provided to help guide individuals seeking assistance.

The process for employees seeking ADA accommodations at NYSERDA is interactive, involving the employee and their supervisor as well as the Director of Human Resources and any others as needed. Employees should begin with their direct supervisor or with the Human Resources Department. Once qualification is established, employees may request the purchase of information technology based assistive technologies from the Information Technology Department. Contractors, guests and visitors may need to contact various NYSERDA staff for assistance or to take advantage of the services offered by IT.

Contact Information: Employees, contractors, guests and visitors should contact any of the following as needed:

- For all employees wishing assistance or for general ADA assistance, contact the Human Resources Department, Donna Rabito, (518) 862-1090 x3640, Donna.Rabito@nyserda.ny.gov.
- For assistance with Facilities, contact Stan Brownell, Facilities Manager, (518) 862-1090 x3211, Stanley.Brownell@nyserda.ny.gov.
- For assistance with NYSERDA websites, contact the web accessibility coordinator, Robert McKeon, (518) 862-1090 x3538, Robert.McKeon@nyserda.ny.gov.
- For assistance with planning or acquiring accommodations for using IT systems, hardware, or software, contact David Young, CIO and Director of Information Technology, (518) 862-1090 x3204, David.Young@nyserda.ny.gov.
- To take advantage of, or to configure systems already provided by the Information Technology Department, contact the IT Help Desk, (518) 862-1090 x4357, HelpDesk@nyserda.ny.gov.

Services: The Information Technology Department is prepared to assist with the configuration of personal computers (PCs) including display schemes for high contrast, large fonts, screen

magnifier, on-screen keyboard, configuration for alternative input devices, and other optimizations related to mobility, vision and hearing.
The IT maintains a PC workstation for general use which is configured with Dragon NaturallySpeaking, ZoomText and JAWS. These provide the following services:

- Dragon NaturallySpeaking provides speech recognition to create text documents or to input voice commands. It is intended to provide continuous speech recognition with adaptive technology to learn voice patterns and characteristics to achieve high accuracy. Dragon supports voice commands, dictation playback and supports almost any Windows application.
- ZoomText provides a large array of features to configure visual settings for the PC and does have screen magnification and screen reading features. ZoomText allows users to see and hear everything on the computer screen, providing complete access to applications, documents, email and the Internet using a variety of customizable tools and features.
- JAWS is a screen reader using a voice synthesizer. It works with Windows to provide audio access to software applications and the Internet.

In addition to the IT workstation, which anyone may use, all of these products are also available to qualified employees and will be purchased upon request to the CIO and Director of Information Technology.

Staff requiring ergonomic accommodations or alternate furniture configurations, lighting, or other physical accommodations are encouraged to work with both the Human Resources and Facilities Departments.
Information Resources: The following may be of use for further information:

- Microsoft http://www.microsoft.com/enable/
- Dragon http://www.SpeechTechnology.com/dragon/index.html
- ZoomText http://www.AIsquared.com/zoomtext/
- JAWS http://www.FreedomScientific.com/products/fs/jaws-product-page.asp
- ADA http://www.ADA.gov/
- Web ADA http://Section508.gov/index.cfm
- ADA Board http://www.Access-Board.gov/

GLOSSARY

Authentication: The process to establish and prove the validity of a claimed identity.

Authorization: The granting of rights, which includes the granting of access based on an authenticated identity.

Authorizing Authority: An Official with authority to formally approve the Information Technology staff to make appropriate changes.

Availability: The extent to which information is operational, accessible, functional and usable upon demand by an authorized entity (e.g., a system or user).

Biometric Data: Unique physical or behavioral characteristics, such as fingerprints or voice patterns, used as a means of verifying personal identity.

Breach of the security of the system**:** unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by NYSERDA. Good faith acquisition of personal information by an employee or agent of NYSERDA for NYSERDA purposes is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, NYSERDA may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Business Risk: This is the combination of sensitivity, threat and vulnerability.

CIO: Chief Information Officer.

Classification: The designation given to information from a defined category on the basis of its sensitivity.

Compensating Controls: Alternative safeguards or countermeasures that accomplish the intent of the original security control.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Consumer Reporting Agency: Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the State Attorney General and furnished upon request to State Entities required to make a notification under this Policy.

Controls: Countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.

Copyright: A property right in an original work of authorship fixed in any tangible medium of expression, giving the holder the exclusive right to reproduce, adapt, distribute, perform and display the work (Black's Law Dictionary, 7th ed. 1999).

CPE: Continuing Professional Education.

Cracking: Breaking into or attempting to break into another system in excess of one's access rights or authorization with or without malicious intent.

Cryptographic: Relating to a method of storing and transmitting data in a form that only those it is intended for can read and process.

Cryptographic Key: A binary number used by an encryption algorithm to perform calculations.

OCS**:** The New York State Office of Cyber Security

Data: See Information.

Decryption**:** The reversal of a corresponding reversible encryption to render information intelligible using the appropriate algorithm and key.

Denial of Service: An attack that takes up so much of the company's business resource that it results in degradation of performance or loss of access to the company's business services or resources.

Disaster: A condition in which information is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of NYSERDA's business objectives as determined by NYSERDA's management.

DMZ: Demilitarized zone; a semi-secured buffer or region between two networks such as between the public Internet and the trusted private State network.

DSL**:** Digital Subscriber Line (DSL): a data communications link to the local telephone company using copper telephone wiring. DSL and cable (broadband) have become popular means of delivering always-connected Internet access at speeds much faster than dial-up.

Electronic Storage Media: Media used to record and store data, including, but not limited to hard drives, tapes, removable drives of any kind, flash drives or other USB storage media, CDs, diskettes, etc..

Encryption: The cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

Extranet**:** The expanded use and logical connection of various local and wide area networks beyond their traditional Internet configuration that uses the standard Internet protocol, TCP/IP, to communicate and conduct E-commerce functions.

Field Level Encryption: Protects data by encrypting data in certain fields of a database.

File Level Encryption: Protects data by encrypting data on a file by file basis.

Firewall: A security mechanism that creates a barrier between an internal network and an external network.

Folder Level Encryption: Protects data by encrypting data on a folder by folder basis.

Full Disk Encryption: Protects data by encrypting the entire drive no matter how many partitions it holds. This can be either hardware or software based.

Host: A system or computer that contains business and/or operational software and/or data

HTTP**:** The protocol that delivers hypertext documents, via the World Wide Web, is called the Hypertext Transfer Protocol (http).

Identity: A set of attributes for a person.

Incident: Any adverse event that threatens the confidentiality, integrity or availability of information resources.

Incident Response: The manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.

Information: Any representation of facts, concepts or instructions created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media. This may include, but is not limited to the data contained in reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Information Assets: Any category of information (automated and non-automated) that has value NYSERDA. This data may be considered in records, files, or databases, and represents facts concepts, or instructions that are stored, filed, produced or reproduced (regardless of the form or media) including the data contained in reports, folders, manuals, memoranda, statements, examinations, transcripts, images, communications – in electronic or hard copy. In some situations it may include the hardware, software, data, system documentation or storage media. See Information.

Information Custodian: An individual, organizational unit (e.g., IT, Operations, Systems, Network) or entity (e.g., Office for Technology) acting as caretaker of information on behalf of its owner.

Information Owner: An individual or a group of individuals that has responsibility for making classification and control decisions regarding use of information. See Part 2 of Information Security Policy P03-002, Organizational and Functional Responsibilities. (In NYSERDA's data governance system this role shall be called Data Owner and the terms are used interchangeably.)

Information Security: The concepts, techniques and measures used to protect information from accidental or intentional unauthorized access, modification, destruction, disclosure or temporary or permanent loss (See Availability).

Information Security Architecture: A framework designed to ensure information security. Principles are defined and integrated into business and IT processes in a consistent manner.

Information Technology Equipment: Includes, but is not limited to, personal computer workstations, laptops, PDAs, mainframes, servers, fax machines, copiers, printers and other electronic devices used to input, store, process and output information.

Integrity: The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.

Intranet: An internal (i.e., non-public) network that uses the same technology and protocols as the Internet.

Internet: A system of linked computer networks, international in scope, that facilitate data transmission and exchange, which all use the standard Internet protocol, TCP/IP, to communicate and share data with each other.

Intrusion Detection: The monitoring of network activities, primarily through automated measures, to detect, log and report upon actual or suspected authorized access and events for investigation and resolution.

IRM**:** Incident Response Manager as defined in the NYSERDA Business Continuity Plan and the Disaster Recovery Plan.

Least Privilege: User, program or process is granted only the access they specifically need to perform their business task and no more.
Malicious Code: Malicious code refers to code that is written intentionally to carry out annoying, harmful actions or use up the resources of a target host. They sometime masquerade as useful software or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include Trojan horses and viruses.

Media Access Control (MAC) address: A hardware address that uniquely identifies each node of a network.

Merging: The process of combining different sources of information into a new source of information.

MIME**:** Multipurpose Internet Mail Extension. The format for Internet mail that includes objects other than just text.

Multi-User System: Refers to computer systems that support two or more simultaneous users. All mainframes, servers and microcomputers are multi-user systems, but most personal computers, laptops and workstations are not.

Need to Know/Need to Do: see Least Privilege.

NNTP**:** The protocol, which delivers USENET news documents, via the Internet, to USENET news group servers, is called the Netnews Transport Protocol.

Packet Sniffers**:** Software programs that can see the traffic passing over a network or part of a network. As data streams travel back and forth over the network, the program captures each packet and eventually decodes its content.

Passphrase: A sequence of words or other text used to control access to a computer system, program or data, similar to a password in usage, but generally longer for added security (e.g., betty was smoking tires and playing tuna fish).

PDA: see Personal Digital Assistant.

Penetration Testing: The portion of security testing in which evaluators attempt to exploit physical, network, system or application weaknesses to prove whether these weaknesses can be exploited by gaining extended, unauthorized or elevated privileged access to protected resources.

Personal Digital Assistant (PDA): A small portable device, such as a Palm Pilot or Blackberry, which combines computing, telephone/fax and networking features. Also called palmtop, handheld and pocket PC.

Personal, Private, or Sensitive Information (PPSI): Any information where unauthorized access, disclosure, modification, destruction or disruption of access to or use of such information could severely impact NYSERDA, its critical functions, its employees, its customers, third parties, or

citizens of New York . This term shall be deemed to include, but is not limited to, the information encompassed in existing statutory definitions.

PPSI includes:

- Information concerning a person which, because of name, number, personal mark or other identifier, can be used to identify that person, in combination with:
    - Social Security Number;
    - driver's license number or non-driver identification card number;
    - mother's maiden name; or
    - financial account identifier(s) or other information which would permit access to a person's financial resources or credit.

- Information used to authenticate the identity of a person or process (e.g., PIN, password, passphrase, and biometric data). This does not include distribution of one-time use PINs, passwords, or passphrases.

- Information that identifies specific structural, operational, or technical information, such as maps, mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities, including, but not limited to:
    - training and security procedures at sensitive facilities and locations as determined by the Office of Homeland Security (OHS);
    - descriptions of technical processes and technical architecture;
    - plans for disaster recovery and business continuity; and
    - reports, logs, surveys, or audits that contain sensitive information.

- Security related information (e.g., vulnerability reports, risk assessments, security logs).

Physical Security: The protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

PPSI: See Personal, Private, or Sensitive Information.

Privacy: The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Privileged Account: The user-ID or account of an individual whose job responsibilities require special system authorization, such as a network administrator, security administrator, etc. Special authorizations are allocated to this account such as RACF Administrator, auditor, Special, UNIX root or Microsoft Administrator.

Procedures: Specific operational steps that individuals must take to achieve goals stated in this Policy.

Proprietary Encryption**:** An algorithm that has not been made public and/or has not with stood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Remote Access: Any access coming into NYSERDA's network from off NYSERDA's private trusted network. This includes, but is not limited to, dialing in from another location over public lines by an employee or other authorized individual.

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.

Risk Assessment: The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.

Risk Management: The process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

Role-Based Access Control: An approach to restricting system access where permissions to perform certain operations are assigned to specific job functions.

SE: See State Entity (ies).

Security Administration: The actions and responsibility for administering the security mechanisms including identification and authentication establishment and authorization maintenance.
Security Management: The responsibility and actions required to manage the security environment including the security policies and mechanisms.

Security Policy: The set of criteria for the provision of security services based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

Security Zone**:** An area or grouping within which a defined set of security policies and measures are applied to achieve a specific level of security. Zones are used to group together those entities with similar security requirements and levels of risk and ensure each zone is adequately segregated from another zone.

Sensitivity: The measurable, harmful impact resulting from disclosure, modification, or destruction of information.

SMTP-Simple Mail Transfer Protocol**:** A TCP/IP based protocol for the transmission of electronic mail. (See definition for Internet e-mail.)

Sniffing: Monitoring network traffic.

Social Engineering: Manipulation of people to obtain security critical assets that allow security perils to take place.

Social Media: An umbrella term that defines the various activities that integrate technology, social interaction, and content creation. Through Social Media, individuals can create, organize, edit, comment on, or share content on a Social Media Site.

Social Media Site: A World Wide Web site that uses Social Media. These sites include, but are not limited to: You Tube, Facebook, Wikipedia, Twitter, and various forums and message boards.

Spamming: Blindly posting something to a large number of groups.

Spoofing: Representing you as someone else.

Standard: Sets of rules for implementing policy. Standards make specific mention of technologies, methodologies, implementation procedures and other detail factors.

State: The State of New York.

State Entity (ies): State Entity for the purpose of this Policy, shall include all State agencies, departments, offices, divisions, boards, bureaus, commissions and other entities over which the Governor has executive power, the State University of New York Central Administration, the City University of New York Central Administration and all public benefit corporations the heads of which are appointed by the Governor.

Symmetric Cryptosystem**:** A method of encryption in which the same key is used for both encryption and decryption of the data.

System(s): An interconnected set of information resources under the same direct management control that shares common functionality. A system may include hardware, software, information, applications or communications infrastructure.

Technical Security Review: A technical security review would consist of reviewing the controls built into a system or application to ensure they still perform as designed and are in compliance with documented security policies and procedures. It would also include reviewing security patches to ensure they have been installed and are operational, reviewing security rules such as access control lists for currency, testing of firewall rules, etc. This type of testing includes intrusion and/or penetration testing of controls.

TELNET**:** The protocol, which allows users to use Internet services to remotely log onto a computer and run a program across the Internet. A TCP/IP based protocol used for remote terminal access to a server or network device. Telnet is inherently unsecured, being that all data, including username/password authentication are transmitted in clear-text.

Third Party: Any non-NYSERDA employee such as a contractor, vendor, consultant, intern, another SE (e.g., Office for Technology), etc.

Threat: A force, organization or person, which seeks to gain access to, or compromise, information. A threat can be assessed in terms of the probability of an attack. Looking at the nature of the threat, its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in risk assessment.

Trojan Horse: Malicious code hidden in a legitimate program that when executed performs some unauthorized activity or function.

Unauthorized Access or privileges: Insider or outsider who gains access to network or information technology equipment resources without permission or without valid authorization.

USENET news group**:** A USENET news group is a bulletin board where people can read or post Netnews messages on specific topics. There are many specialized business news groups. Many news groups are subscribed to by experts in the given topic and these individuals can provide valuable information and will sometimes respond to direct queries.

User: Any State Entity(ies), federal government entity(ies), political subdivision(s), their employees or third party contractor(s) or business associates, or any other individual(s) who are authorized by such entities to access a system for a legitimate government purpose.
Value: A measure of worth which can be expressed in monetary terms or in terms of importance to NYSERDA.

Virus: A program that replicates itself on computer systems by incorporating itself into other programs that are shared among computer systems. Once in the new host, a virus may damage data in the host's memory, display unwanted messages, crash the host or, in some cases, simply lie dormant until a specified event occurs (e.g., the birth date of a historical figure).

Volume Level Encryption: Protects data by encrypting the entire partition of a disk or, in the case of a single partition hard drive, the entire drive.

VPN**:** Virtual Private Network. Internet protocol (IP) virtual private networks (VPNs) are a collection of technologies that ensure the privacy of data over a shared unsecured IP network infrastructure. The two key points as to what constitutes an IP VPN are privacy and an IP network.

Vulnerability: A weakness of a system or facility holding information which can be exploited to gain access or violate system integrity. Vulnerability can be assessed in terms of the means by which the attack would be successful.

Vulnerability Scanning: The portion of security testing in which evaluators attempt to identify physical, network, system or application weaknesses to discover whether these weaknesses may be exploited by persons or machines seeking to gain either unauthorized or elevated privileged access to otherwise protected resources.

Workforce: State employees, and other persons whose conduct, in the performance of work for NYSERDA, is under direct control of NYSERDA, whether or not they are paid by NYSERDA.

World Wide Web (WWW): A hypertext-based system designed to allow access to information in such a way that the information may physically reside on locally or geographically different servers. This access was greatly improved through the introduction of a graphical interface to the World Wide Web called a web browser. Netscape and Internet Explorer are two of the most popular web browsers.

Worm: A program similar to a virus that can consume large quantities of network bandwidth and spread from one network to another.

APPENDIX A

Information Control Charts Classification Rating Menu

Page #	Classification Rating	Confidentiality	Integrity	Availability
A-1	LLL	Low	Low	Low
A-2	LLM	Low	Low	Moderate
A-3	LLH	Low	Low	High
A-4	LML	Low	Moderate	Low
A-5	LMM	Low	Moderate	Moderate
A-6	LMH	Low	Moderate	High
A-7	LHL	Low	High	Low
A-8	LHM	Low	High	Moderate
A-9	LHH	Low	High	High
A-10	MLL	Moderate	Low	Low
A-11	MLM	Moderate	Low	Moderate
A-12	MLH	Moderate	Low	High
A-13	MML	Moderate	Moderate	Low
A-14	MMM	Moderate	Moderate	Moderate
A-15	MMH	Moderate	Moderate	High
A-16	MHL	Moderate	High	Low
A-17	MHM	Moderate	High	Moderate
A-18	MHH	Moderate	High	High
A-19	HLL	High	Low	Low
A-20	HLM	High	Low	Moderate
A-21	HLH	High	Low	High
A-22	HML	High	Moderate	Low
A-23	HMM	High	Moderate	Moderate
A-24	HMH	High	Moderate	High
A-25	HHL	High	High	Low
A-26	HHM	High	High	Moderate
A-27	HHH	High	High	High
A-28	Confidentiality Controls			
A-29	Integrity Controls			
A-30	Availability Controls			

CONFIDENTIALITY (C): LOW	INTEGRITY (I): LOW	AVAILABILITY (A): LOW

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
	INFORMATION OWNER CONTROLS	
3	R Access authorized by information owner	C
43	R Review access lists	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
12	R Basic input data validation	I
22	R Erase re-writeable media prior to reuse	C
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
31	O Label: "NYS CONFIDENTIALITY-LOW"	C
54	R Use disposal method for paper or write-once media	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
46	R Review security procedures and controls	CIA

CONFIDENTIALITY (C): LOW	INTEGRITY (I): LOW	AVAILABILITY (A): MODERATE

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
	INFORMATION OWNER CONTROLS	
3	R Access authorized by information owner	C
6	R Access provided to more than one person	A
43	R Review access lists	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
20	R Environmental protection measures	IA
22	R Erase re-writeable media prior to reuse	C
39	R Regular backup	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
31	O Label: "NYS CONFIDENTIALITY-LOW"	C
54	R Use disposal method for paper or write-once media	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
46	R Review security procedures and controls	CIA

CONFIDENTIALITY (C): LOW	INTEGRITY (I): LOW	AVAILABILITY (A): HIGH

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan	A
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
	INFORMATION OWNER CONTROLS	
3	R Access authorized by information owner	C
6	R Access provided to more than one person	A
43	R Review access lists	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
8	R Alternate means of availability	A
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
37	R Off-site backup	A
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
31	O Label: "NYS CONFIDENTIALITY-LOW"	C
54	R Use disposal method for paper or write-once media	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): LOW	INTEGRITY (I): MODERATE	AVAILABILITY (A): LOW

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
	INFORMATION OWNER CONTROLS	
3	R Access authorized by information owner	C
43	R Review access lists	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
22	R Erase re-writeable media prior to reuse	C
39	R Regular backup	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
31	O Label: "NYS CONFIDENTIALITY-LOW"	C
49	R Secure area	CI
54	R Use disposal method for paper or write-once media	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
46	R Review security procedures and controls	CIA

CONFIDENTIALITY (C): LOW	INTEGRITY (I): MODERATE	AVAILABILITY (A): MODERATE

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
	INFORMATION OWNER CONTROLS	
3	R Access authorized by information owner	C
6	R Access provided to more than one person	A
43	R Review access lists	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
22	R Erase re-writeable media prior to reuse	C
39	R Regular backup	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
31	O Label: "NYS CONFIDENTIALITY-LOW"	C
49	R Secure area	CI
54	R Use disposal method for paper or write-once media	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
46	R Review security procedures and controls	CIA

CONFIDENTIALITY (C): LOW	INTEGRITY (I): MODERATE	AVAILABILITY (A): HIGH

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan	A
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
	INFORMATION OWNER CONTROLS	
3	R Access authorized by information owner	C
6	R Access provided to more than one person	A
43	R Review access lists	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
8	R Alternate means of availability	A
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
37	R Off-site backup	A
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
31	O Label: "NYS CONFIDENTIALITY-LOW"	C
49	R Secure area	CI
54	R Use disposal method for paper or write-once media	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): LOW	INTEGRITY (I): HIGH	AVAILABILITY (A): LOW

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
10	R Approved storage facility	CI
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
48	R Review system and application security logs	CI
	INFORMATION OWNER CONTROLS	
3	R Access authorized by information owner	C
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
34	R Message integrity	I
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
31	O Label: "NYS CONFIDENTIALITY-LOW"	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
54	R Use disposal method for paper or write-once media	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): LOW	INTEGRITY (I): HIGH	AVAILABILITY (A): MODERATE

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
10	R Approved storage facility	CI
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
48	R Review system and application security logs	CI
	INFORMATION OWNER CONTROLS	
3	R Access authorized by information owner	C
6	R Access provided to more than one person	A
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
34	R Message integrity	I
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
31	O Label: "NYS CONFIDENTIALITY-LOW"	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
54	R Use disposal method for paper or write-once media	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): LOW	INTEGRITY (I): HIGH	AVAILABILITY (A): HIGH

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan	A
10	R Approved storage facility	CI
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
48	R Review system and application security logs	CI
	INFORMATION OWNER CONTROLS	
3	R Access authorized by information owner	C
6	R Access provided to more than one person	A
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
8	R Alternate means of availability	A
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
34	R Message integrity	I
37	R Off-site backup	A
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
31	O Label: "NYS CONFIDENTIALITY-LOW"	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
54	R Use disposal method for paper or write-once media	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): MODERATE	INTEGRITY (I): LOW	AVAILABILITY (A): LOW

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
17	R Destroy when no longer needed	C
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
	INFORMATION OWNER CONTROLS	
4	R Access authorized by information owner (written)	C
43	R Review access lists	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
12	R Basic input data validation	I
22	R Erase re-writeable media prior to reuse	C
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
14	R Conceal physical media	C
15	R Confirmation of identity and access rights of requester	C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"	C
42	R Retrieval when printing/faxing (timely)	C
49	R Secure area	CI
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
46	R Review security procedures and controls	CIA

CONFIDENTIALITY (C): MODERATE	INTEGRITY (I): LOW	AVAILABILITY (A): MODERATE

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
17	R Destroy when no longer needed	C
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
	INFORMATION OWNER CONTROLS	
4	R Access authorized by information owner (written)	C
6	R Access provided to more than one person	A
43	R Review access lists	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
20	R Environmental protection measures	IA
22	R Erase re-writeable media prior to reuse	C
39	R Regular backup	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
14	R Conceal physical media	C
15	R Confirmation of identity and access rights of requester	C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"	C
42	R Retrieval when printing/faxing (timely)	C
49	R Secure area	CI
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
46	R Review security procedures and controls	CIA

CONFIDENTIALITY (C): MODERATE	INTEGRITY (I): LOW	AVAILABILITY (A): HIGH

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan	A
17	R Destroy when no longer needed	C
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
	INFORMATION OWNER CONTROLS	
4	R Access authorized by information owner (written)	C
6	R Access provided to more than one person	A
43	R Review access lists	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
8	R Alternate means of availability	A
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
37	R Off-site backup	A
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
14	R Conceal physical media	C
15	R Confirmation of identity and access rights of requester	C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"	C
42	R Retrieval when printing/faxing (timely)	C
49	R Secure area	CI
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): MODERATE	INTEGRITY (I): MODERATE	AVAILABILITY (A): LOW

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
17	R Destroy when no longer needed	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
	INFORMATION OWNER CONTROLS	
4	R Access authorized by information owner (written)	C
43	R Review access lists	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
22	R Erase re-writeable media prior to reuse	C
39	R Regular backup	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
14	R Conceal physical media	C
15	R Confirmation of identity and access rights of requester	C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"	C
42	R Retrieval when printing/faxing (timely)	C
49	R Secure area	CI
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
46	R Review security procedures and controls	CIA

CONFIDENTIALITY (C): MODERATE	INTEGRITY (I): MODERATE	AVAILABILITY (A): MODERATE

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
17	R Destroy when no longer needed	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
	INFORMATION OWNER CONTROLS	
4	R Access authorized by information owner (written)	C
6	R Access provided to more than one person	A
43	R Review access lists	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
22	R Erase re-writeable media prior to reuse	C
39	R Regular backup	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
14	R Conceal physical media	C
15	R Confirmation of identity and access rights of requester	C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"	C
42	R Retrieval when printing/faxing (timely)	C
49	R Secure area	CI
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
46	R Review security procedures and controls	CIA

CONFIDENTIALITY (C): MODERATE	INTEGRITY (I): MODERATE	AVAILABILITY (A): HIGH

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan	A
17	R Destroy when no longer needed	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
	INFORMATION OWNER CONTROLS	
4	R Access authorized by information owner (written)	C
6	R Access provided to more than one person	A
43	R Review access lists	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
8	R Alternate means of availability	A
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
37	R Off-site backup	A
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
14	R Conceal physical media	C
15	R Confirmation of identity and access rights of requester	C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"	C
42	R Retrieval when printing/faxing (timely)	C
49	R Secure area	CI
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): MODERATE	INTEGRITY (I): HIGH	AVAILABILITY (A): LOW

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
10	R Approved storage facility	CI
17	R Destroy when no longer needed	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
48	R Review system and application security logs	CI
	INFORMATION OWNER CONTROLS	
4	R Access authorized by information owner (written)	C
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
34	R Message integrity	I
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
15	R Confirmation of identity and access rights of requester	C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"	C
42	R Retrieval when printing/faxing (timely)	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): MODERATE	INTEGRITY (I): HIGH	AVAILABILITY (A): MODERATE

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
10	R Approved storage facility	CI
17	R Destroy when no longer needed	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
48	R Review system and application security logs	CI
	INFORMATION OWNER CONTROLS	
4	R Access authorized by information owner (written)	C
6	R Access provided to more than one person	A
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
34	R Message integrity	I
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
15	R Confirmation of identity and access rights of requester	C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"	C
42	R Retrieval when printing/faxing (timely)	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): MODERATE	INTEGRITY (I): HIGH	AVAILABILITY (A): HIGH

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan	A
10	R Approved storage facility	CI
17	R Destroy when no longer needed	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
38	R Privacy disclaimer on e-mail and fax cover sheets	C
48	R Review system and application security logs	CI
	INFORMATION OWNER CONTROLS	
4	R Access authorized by information owner (written)	C
6	R Access provided to more than one person	A
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
8	R Alternate means of availability	A
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
34	R Message integrity	I
37	R Off-site backup	A
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
15	R Confirmation of identity and access rights of requester	C
32	O Label: "NYS CONFIDENTIALITY-MODERATE"	C
42	R Retrieval when printing/faxing (timely)	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): HIGH	INTEGRITY (I): LOW	AVAILABILITY (A): LOW

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
9	R Approved electronic storage media and devices	C
10	R Approved storage facility	CI
13	R Chain of custody for physical media	C
17	R Destroy when no longer needed	C
29	R Information classification and inventory	CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	C
38	R Privacy disclaimer on e-mail and fax cover sheets	C
40	R Reproduction authorized by information owner	C
48	R Review system and application security logs	CI
56	R Written approval for Transmission, Transportation and Storage (TTS)	C
	INFORMATION OWNER CONTROLS	
5	R Access authorized by information owner (written & cc: exec)	C
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
12	R Basic input data validation	I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	C
19	R Encryption/hashing of electronic authentication information	C
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
15	R Confirmation of identity and access rights of requester	C
30	O Label: "NYS CONFIDENTIALITY-HIGH"	C
35	R No confidential information in e-mail subject line	C
41	R Retrieval when printing/faxing (immediate)	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
51	R Situational awareness during verbal communications	C
53	R Transportation handling controls for paper	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
1	R Access approval/removal process (audit)	C
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): HIGH	INTEGRITY (I): LOW	AVAILABILITY (A): MODERATE

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
9	R Approved electronic storage media and devices	C
10	R Approved storage facility	CI
13	R Chain of custody for physical media	C
17	R Destroy when no longer needed	C
29	R Information classification and inventory	CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	C
38	R Privacy disclaimer on e-mail and fax cover sheets	C
40	R Reproduction authorized by information owner	C
48	R Review system and application security logs	CI
56	R Written approval for Transmission, Transportation and Storage (TTS)	C
	INFORMATION OWNER CONTROLS	
5	R Access authorized by information owner (written & cc: exec)	C
6	R Access provided to more than one person	A
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	C
19	R Encryption/hashing of electronic authentication information	C
20	R Environmental protection measures	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
39	R Regular backup	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
15	R Confirmation of identity and access rights of requester	C
30	O Label: "NYS CONFIDENTIALITY-HIGH"	C
35	R No confidential information in e-mail subject line	C
41	R Retrieval when printing/faxing (immediate)	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
51	R Situational awareness during verbal communications	C
53	R Transportation handling controls for paper	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
1	R Access approval/removal process (audit)	C
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): HIGH	INTEGRITY (I): LOW	AVAILABILITY (A): HIGH

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan	A
9	R Approved electronic storage media and devices	C
10	R Approved storage facility	CI
13	R Chain of custody for physical media	C
17	R Destroy when no longer needed	C
29	R Information classification and inventory	CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	C
38	R Privacy disclaimer on e-mail and fax cover sheets	C
40	R Reproduction authorized by information owner	C
48	R Review system and application security logs	CI
56	R Written approval for Transmission, Transportation and Storage (TTS)	C
	INFORMATION OWNER CONTROLS	
5	R Access authorized by information owner (written & cc: exec)	C
6	R Access provided to more than one person	A
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
8	R Alternate means of availability	A
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	C
19	R Encryption/hashing of electronic authentication information	C
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
37	R Off-site backup	A
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
15	R Confirmation of identity and access rights of requester	C
30	O Label: "NYS CONFIDENTIALITY-HIGH"	C
35	R No confidential information in e-mail subject line	C
41	R Retrieval when printing/faxing (immediate)	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
51	R Situational awareness during verbal communications	C
53	R Transportation handling controls for paper	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
1	R Access approval/removal process (audit)	C
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): HIGH	INTEGRITY (I): MODERATE	AVAILABILITY (A): LOW

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
9	R Approved electronic storage media and devices	C
10	R Approved storage facility	CI
13	R Chain of custody for physical media	C
17	R Destroy when no longer needed	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	C
38	R Privacy disclaimer on e-mail and fax cover sheets	C
40	R Reproduction authorized by information owner	C
48	R Review system and application security logs	CI
56	R Written approval for Transmission, Transportation and Storage (TTS)	C
	INFORMATION OWNER CONTROLS	
5	R Access authorized by information owner (written & cc: exec)	C
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	C
19	R Encryption/hashing of electronic authentication information	C
20	R Environmental protection measures	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
39	R Regular backup	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
15	R Confirmation of identity and access rights of requester	C
30	O Label: "NYS CONFIDENTIALITY-HIGH"	C
35	R No confidential information in e-mail subject line	C
41	R Retrieval when printing/faxing (immediate)	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
51	R Situational awareness during verbal communications	C
53	R Transportation handling controls for paper	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
1	R Access approval/removal process (audit)	C
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): HIGH	INTEGRITY (I): MODERATE	AVAILABILITY (A): MODERATE

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
9	R Approved electronic storage media and devices	C
10	R Approved storage facility	CI
13	R Chain of custody for physical media	C
17	R Destroy when no longer needed	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	C
38	R Privacy disclaimer on e-mail and fax cover sheets	C
40	R Reproduction authorized by information owner	C
48	R Review system and application security logs	CI
56	R Written approval for Transmission, Transportation and Storage (TTS)	C
	INFORMATION OWNER CONTROLS	
5	R Access authorized by information owner (written & cc: exec)	C
6	R Access provided to more than one person	A
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	C
19	R Encryption/hashing of electronic authentication information	C
20	R Environmental protection measures	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
39	R Regular backup	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
15	R Confirmation of identity and access rights of requester	C
30	O Label: "NYS CONFIDENTIALITY-HIGH"	C
35	R No confidential information in e-mail subject line	C
41	R Retrieval when printing/faxing (immediate)	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
51	R Situational awareness during verbal communications	C
53	R Transportation handling controls for paper	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
1	R Access approval/removal process (audit)	C
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): HIGH	INTEGRITY (I): MODERATE	AVAILABILITY (A): HIGH

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan	A
9	R Approved electronic storage media and devices	C
10	R Approved storage facility	CI
13	R Chain of custody for physical media	C
17	R Destroy when no longer needed	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	C
38	R Privacy disclaimer on e-mail and fax cover sheets	C
40	R Reproduction authorized by information owner	C
48	R Review system and application security logs	CI
56	R Written approval for Transmission, Transportation and Storage (TTS)	C
	INFORMATION OWNER CONTROLS	
5	R Access authorized by information owner (written & cc: exec)	C
6	R Access provided to more than one person	A
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
8	R Alternate means of availability	A
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	C
19	R Encryption/hashing of electronic authentication information	C
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
37	R Off-site backup	A
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
15	R Confirmation of identity and access rights of requester	C
30	O Label: "NYS CONFIDENTIALITY-HIGH"	C
35	R No confidential information in e-mail subject line	C
41	R Retrieval when printing/faxing (immediate)	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
51	R Situational awareness during verbal communications	C
53	R Transportation handling controls for paper	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
1	R Access approval/removal process (audit)	C
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): HIGH	INTEGRITY (I): HIGH	AVAILABILITY (A): LOW

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
9	R Approved electronic storage media and devices	C
10	R Approved storage facility	CI
13	R Chain of custody for physical media	C
17	R Destroy when no longer needed	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	C
38	R Privacy disclaimer on e-mail and fax cover sheets	C
40	R Reproduction authorized by information owner	C
48	R Review system and application security logs	CI
56	R Written approval for Transmission, Transportation and Storage (TTS)	C
	INFORMATION OWNER CONTROLS	
5	R Access authorized by information owner (written & cc: exec)	C
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	C
19	R Encryption/hashing of electronic authentication information	C
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
34	R Message integrity	I
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
15	R Confirmation of identity and access rights of requester	C
30	O Label: "NYS CONFIDENTIALITY-HIGH"	C
35	R No confidential information in e-mail subject line	C
41	R Retrieval when printing/faxing (immediate)	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
51	R Situational awareness during verbal communications	C
53	R Transportation handling controls for paper	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
1	R Access approval/removal process (audit)	C
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): HIGH	INTEGRITY (I): HIGH	AVAILABILITY (A): MODERATE

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
9	R Approved electronic storage media and devices	C
10	R Approved storage facility	CI
13	R Chain of custody for physical media	C
17	R Destroy when no longer needed	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	C
38	R Privacy disclaimer on e-mail and fax cover sheets	C
40	R Reproduction authorized by information owner	C
48	R Review system and application security logs	CI
56	R Written approval for Transmission, Transportation and Storage (TTS)	C
	INFORMATION OWNER CONTROLS	
5	R Access authorized by information owner (written & cc: exec)	C
6	R Access provided to more than one person	A
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	C
19	R Encryption/hashing of electronic authentication information	C
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
34	R Message integrity	I
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
15	R Confirmation of identity and access rights of requester	C
30	O Label: "NYS CONFIDENTIALITY-HIGH"	C
35	R No confidential information in e-mail subject line	C
41	R Retrieval when printing/faxing (immediate)	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
51	R Situational awareness during verbal communications	C
53	R Transportation handling controls for paper	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
1	R Access approval/removal process (audit)	C
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY (C): HIGH	INTEGRITY (I): HIGH	AVAILABILITY (A): HIGH

Glossary X-Ref #	R=Required O=Optional	CIA
	STATE ENTITY (SE) CONTROLS	
2	R Access approval/removal process in place	C
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan	A
9	R Approved electronic storage media and devices	C
10	R Approved storage facility	CI
13	R Chain of custody for physical media	C
17	R Destroy when no longer needed	C
23	R Formal change control procedures for information systems	I
24	R Formal test plans and documented results for information systems	I
29	R Information classification and inventory	CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties	C
38	R Privacy disclaimer on e-mail and fax cover sheets	C
40	R Reproduction authorized by information owner	C
48	R Review system and application security logs	CI
56	R Written approval for Transmission, Transportation and Storage (TTS)	C
	INFORMATION OWNER CONTROLS	
5	R Access authorized by information owner (written & cc: exec)	C
6	R Access provided to more than one person	A
44	R Review access lists (annually)	CI
45	R Review and reclassify information	CIA
	INFORMATION CUSTODIAN CONTROLS	
8	R Alternate means of availability	A
11	R Backup recovery procedures	IA
12	R Basic input data validation	I
16	R Data plausibility and field comparison edits	I
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE	C
19	R Encryption/hashing of electronic authentication information	C
20	R Environmental protection measures	IA
21	R Environmental protection measures monitoring	IA
22	R Erase re-writeable media prior to reuse	C
33	R Limit access to secure areas	CI
34	R Message integrity	I
37	R Off-site backup	A
39	R Regular backup	IA
52	R Test recovery of backup data	IA
55	R Use disposal method for re-writeable media	C
	SE WORKFORCE (INFORMATION USER) CONTROLS	
15	R Confirmation of identity and access rights of requester	C
30	O Label: "NYS CONFIDENTIALITY-HIGH"	C
35	R No confidential information in e-mail subject line	C
41	R Retrieval when printing/faxing (immediate)	C
49	R Secure area	CI
50	R Secure physical media when unattended	CI
51	R Situational awareness during verbal communications	C
53	R Transportation handling controls for paper	C
	INFORMATION SECURITY OFFICER (ISO) CONTROLS	
1	R Access approval/removal process (audit)	C
47	R Review security procedures and controls (annually)	CIA

CONFIDENTIALITY CONTROLS

Glossary X-Ref #	R=Required O=Optional
	LOW CONTROLS
2	R Access approval/removal process in place
3	R Access authorized by information owner
22	R Erase re-writeable media prior to reuse
29	R Information classification and inventory
31	O Label: "NYS CONFIDENTIALITY-LOW"
38	R Privacy disclaimer on e-mail and fax cover sheets
43	R Review access lists
45	R Review and reclassify information
46	R Review security procedures and controls
54	R Use disposal method for paper or write-once media
55	R Use disposal method for re-writeable media
	MODERATE CONTROLS
4	R Access authorized by information owner (written)
14	R Conceal physical media
15	R Confirmation of identity and access rights of requester
17	R Destroy when no longer needed
32	O Label: "NYS CONFIDENTIALITY-MODERATE"
42	R Retrieval when printing/faxing (timely)
49	R Secure area
	HIGH CONTROLS
1	R Access approval/removal process (audit)
5	R Access authorized by information owner (written & cc: exec)
9	R Approved electronic storage media and devices
10	R Approved storage facility
13	R Chain of custody for physical media
18	R Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE
19	R Encryption/hashing of electronic authentication information
30	O Label: "NYS CONFIDENTIALITY-HIGH"
33	R Limit access to secure areas
35	R No confidential information in e-mail subject line
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties
40	R Reproduction authorized by information owner
41	R Retrieval when printing/faxing (immediate)
44	R Review access lists (annually)
47	R Review security procedures and controls (annually)
48	R Review system and application security logs
50	R Secure physical media when unattended
51	R Situational awareness during verbal communications
53	R Transportation handling controls for paper
56	R Written approval for Transmission, Transportation and Storage (TTS)

INTEGRITY CONTROLS

Glossary X-Ref #	R=Required O=Optional
	LOW CONTROLS
12	R Basic input data validation
29	R Information classification and inventory
43	R Review access lists
45	R Review and reclassify information
46	R Review security procedures and controls
	MODERATE CONTROLS
11	R Backup recovery procedures
16	R Data plausibility and field comparison edits
20	R Environmental protection measures
23	R Formal change control procedures for information systems
24	R Formal test plans and documented results for information systems
39	R Regular backup
49	R Secure area
	HIGH CONTROLS
10	R Approved storage facility
21	R Environmental protection measures monitoring
33	R Limit access to secure areas
34	R Message integrity
44	R Review access lists (annually)
47	R Review security procedures and controls (annually)
48	R Review system and application security logs
50	R Secure physical media when unattended
52	R Test recovery of backup data

AVAILABILITY CONTROLS

Glossary X-Ref #	R=Required O=Optional
	LOW CONTROLS
29	R Information classification and inventory
45	R Review and reclassify information
46	R Review security procedures and controls
	MODERATE CONTROLS
6	R Access provided to more than one person
11	R Backup recovery procedures
20	R Environmental protection measures
39	R Regular backup
	HIGH CONTROLS
7	R Address recovery in SE Business Continuity/Disaster Recovery Plan
8	R Alternate means of availability
21	R Environmental protection measures monitoring
37	R Off-site backup
47	R Review security procedures and controls (annually)
52	R Test recovery of backup data

Exhibit I
Article 15-A Contract Provisions (non-construction contract)

1. General Provisions.

(a) NYSERDA is required to implement the provisions of New York State Executive Law Article 15-A and 5 NYCRR Parts 140-144 ("Regulations") for all State contracts as defined therein, with a value (1) in excess of $25,000 for labor, services, equipment, materials, or any combination of the foregoing or (2) in excess of $100,000 for real property renovations and construction.

(b) The Contractor to the subject contract (the "Contractor" and the "Contract," respectively) agrees, in addition to any other nondiscrimination provision of the Contract and at no additional cost to NYSERDA, to fully comply and cooperate with NYSERDA in the implementation of New York State Executive Law Article 15-A. These requirements include equal employment opportunities for minority group members and women ("EEO") and contracting opportunities for certified minority and women-owned business enterprises ("MWBEs"). Contractor's demonstration of "good faith efforts" pursuant to 5 NYCRR §142.8 shall be a part of these requirements. These provisions shall be deemed supplementary to, and not in lieu of, the nondiscrimination provisions required by New York State Executive Law Article 15 (the "Human Rights Law") or other applicable federal, state, or local laws.

(c) Failure to comply with all of the requirements herein may result in a finding of non-responsiveness, non-responsibility and/or a breach of contract, leading to the withholding of funds or such other actions, liquidated damages pursuant to Section 9 of these provisions or enforcement proceedings as allowed by the Contract.

(d) The Contractor further agrees to fully cooperate with NYSERDA in the implementation of such additional reporting requirements as may be required by the Division of Minority and Women's Business Development during the duration of this Agreement.

2. Equal Employment Opportunities.

(a) The Contractor shall submit an EEO policy statement to NYSERDA within seventy two (72) hours after the date of the notice by NYSERDA to award the Contract to the Contractor. If Contractor or Subcontractor does not have an existing EEO policy statement, Contractor or Subcontractor may adopt the model statement provided as **Attachment 1** – Minority- and Women-Owned Business Enterprises And Equal Employment Opportunity Policy Statement. Contractor hereby agrees that this policy shall remain in full force and effect during the performance of this Agreement.

(b) During the performance of this Agreement, Contractor agrees to the following:

(i) Contractor will not discriminate against any employee or applicant for employment because of race, creed, color, national origin, sex, age, disability or marital status, will undertake or continue existing programs of affirmative action to ensure that minority group members and women are afforded equal employment opportunities without discrimination, and shall make and document Contractor's conscientious and active efforts to employ and utilize minority group members and women in its work force on this Agreement. For these purposes, affirmative action shall apply in the areas of recruitment, employment, job assignment, promotion, upgrading, demotion, transfer, layoff, or termination and rates of pay or other forms of compensation.

(ii) At the request of NYSERDA, Contractor shall request each employment agency, labor union, or authorized representative of workers with which it has a collective bargaining or other agreement or understanding, to furnish a written statement that such employment agency, labor union, or representative will not discriminate on the basis of race, creed, color, national origin, sex, age, disability or marital status; and that such union or representative will affirmatively cooperate in the implementation of the contractor's obligations herein.

(iii) Contractor shall state in all solicitations or advertisements for employees that, in the performance of the State contract, all qualified applicants will be afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex, age, disability or marital status.

(iv) Contractor shall comply with the provisions of the Human Rights Law, all other State and Federal statutory and constitutional non-discrimination provisions. Contractor and subcontractors shall not discriminate against any employee or applicant for employment because of race, creed (religion), color, sex, national origin, sexual orientation, military status, age, disability, predisposing genetic characteristic, marital status, or domestic violence victim status, and shall also follow the requirements of the Human Rights Law with regard to non-discrimination on the basis of prior criminal conviction and prior arrest.

(c) Contractor shall include, in all subcontracts related to its performance of its obligations in this Agreement, the requirements set forth in Section 2(b) above, in such a manner that the provisions will be binding upon each subcontractor as to work in connection with this Agreement.

(d) The provisions of this Section shall not be binding upon Contractors or its subcontractors in the performance of work or the provision of services or any other activity that are unrelated, separate, or distinct from this Agreement, as expressed by its terms.

(e) The requirements of this Section shall not apply to any employment outside New York State or application for employment outside New York State or solicitations or advertisements therefor, or any existing programs of affirmative action regarding employment outside New York State.

3. Contract Goals. For purposes of this procurement, NYSERDA hereby establishes the following goals for MWBE participation: ___% for Minority-Owned Business Enterprises ("MBE") participation and ___% for Women-Owned Business Enterprises ("WBE") participation.

4. Participation Goals. The Contractor represents that it has reviewed and familiarized itself with the regulations related to Article 15-A found at 5 NYCRR Parts 140-144 (see http://www.empire.state.ny.us/MWBE/Data/122210_MWBE15-ARegs.pdf), which regulations (the "Regulations") are hereby incorporated herein by this reference. Any conflicts between this Agreement and the Regulations shall be resolved in favor of the Regulations. Contractor shall, in accordance with the Regulations, make good faith efforts and, in a manner that can be established in documentary form, solicit active participation by certified MWBE businesses as identified in the applicable state directory maintained by the NYS Empire State Development's Division of Minority and Women Business Development (see http://www.empire.state.ny.us/MWBE/directorySearch.html). Additionally, Contractor is encouraged to contact the Division of Minority and Woman Business Development ((518) 292-5250; (212) 803-2414; or (716) 846-8200) to discuss additional methods of maximizing participation by MWBEs on the Contract. In furtherance thereof, the Contractor has submitted the following information to NYSERDA, which information sets forth NYSERDA's and Contractor's agreed upon participation goals during the performance of this Agreement:

(a) A completed MWBE Utilization Plan Form (see **Attachment 2**) and/or a NYSERDA-approved Waiver Form (see **Attachment 6**); and

(b) A staffing plan of the anticipated workforce to be utilized by the Contractor during this Agreement, or in the case where the workforce to be utilized in the performance of this Agreement cannot be separated out from the Contractor's and/or its subcontractor workforce, information on the Contractor's and/or subcontractor's total workforce. The staffing plan or workforce data, as applicable, is broken down by ethnic background, gender and Federal occupational categories, or other appropriate categories specified by NYSERDA (see **Attachment 3**).

5. Compliance Reporting Requirements. In order to demonstrate compliance with the stated participation and staffing goals as set forth above, Contractor shall be required to submit compliance reports as follows:

(a) Unless NYSERDA has granted a total waiver or Contractor is a certified MWBE with the Division and is responsible for one hundred percent (100%) of the performance of this Agreement, the Contractor shall submit to NYSERDA an MWBE Compliance Report on a quarterly basis in the form attached hereto as **Attachment 4**; and

(b) Where the workforce to be utilized during the performance of this Agreement can be separated out from the Contractor's total workforce, the Contractor shall submit to NYSERDA on a quarterly basis, in the form attached hereto as **Attachment 5** (Workforce Employment Utilization Report): 1) the total number of employees performing work on the State contract, and 2) the Contractor's and all subcontractor's work force on the State contract broken down by specified ethnic background, gender, and Federal occupational categories or other appropriate categories specified by NYSERDA; or

(c) In the circumstances where the workforce cannot be separated out from the Contractor's and/or subcontractor's total workforce, the Contractor shall submit to NYSERDA information related to the Contractor's total workforce data broken down by ethnic background, gender and Federal occupational categories on a semi-annual basis, or other appropriate categories specified by NYSERDA.

The Contractor's failure to follow the applicable reporting requirements or failure to comply with the stated participation goals in the previous Section set forth above may result in NYSERDA's submission of a complaint to the NYS Empire State Development's Division of Minority and Women Business Development (the "Division") in accordance with the Article 15-A Disqualification and Dispute Resolution Procedures set forth herein.

6. Waiver of participation goal requirements. In accordance with the Regulations § 142.7(c), Contractor may submit, at any time prior to its request for final payment, a request to NYSERDA for partial or total waiver of the MWBE participation goals set forth above. Upon Contractor's submission of a waiver form, NYSERDA may grant a partial or total waiver of the requirements of the participation goals established hereunder. Prior to granting or denying a waiver, NYSERDA shall evaluate the Contractor's "good faith efforts" and may consider the factors set forth in the Regulations §142.8. If NYSERDA, upon review of the MWBE Utilization Plan and updated Quarterly MWBE Contractor Compliance Reports determines that Contractor is failing or refusing to comply with the Contract goals and no waiver has been issued in regards to such non-compliance, NYSERDA may issue a notice of deficiency to the Contractor. The Contractor must respond to the notice

of deficiency within seven (7) business days of receipt. Such response may include a request for partial or total waiver of MWBE Contract Goals. In the event NYSERDA refuses to grant Contractor a waiver, Contractor may file a complaint with the Division in accordance with the Article 15-A Disqualification and Dispute Resolution Procedures set forth herein. A waiver form is provided in **Attachment 6**.

7. **Article 15-A Compliance Monitoring**. NYSERDA is responsible for monitoring Contractor's compliance with the applicable regulations. In that regard, NYSERDA may, at its discretion, notify the Contractor in writing of NYSERDA's intent to inspect relevant records and documents related to Article 15-A compliance. NYSERDA shall analyze and consider such records, documents and other data to determine whether the Contractor has made conscientious and active efforts to employ and utilize minority group members and women on the State contract.

8. **Article Disqualification and Dispute Resolution Procedures**. NYSERDA and Contractor hereby agree to be subject to and bound by the disqualification and dispute resolution procedures contained in Article 15-A of the Executive Law (including, without limitation, Sections 312(5), 313(8), 313(9) and 316), and in relevant sections of the Regulations (including, without limitation, Sections 142.12 and 143.6), as and where applicable.

9. **Penalties.** In accordance with the Regulations §142.13, Contractor hereby agrees that its willful and intentional failure to comply with the M/WBE requirements of Article 15-A as set forth in this Agreement shall create liability to NYSERDA for damages in an amount equal to NYSERDA's actual cost related to its expenses for personnel, supplies and overhead related to establishing, monitoring and reviewing certified minority- and women-owned business enterprise programmatic goals and Affirmative Action and Equal Opportunity compliance.

Exhibit J

Article 17-B (SDVOB) Contract Provisions (non-construction)

1. **General Provisions**

   a. NYSERDA is required to implement the provisions of New York State Executive Law Article 17-B and Title 9, Subtitle G Part 252 of the New York Codes, Rules and Regulations (the "Regulations") for all State contracts as defined therein, with a value (1) in excess of $25,000 for labor, services, equipment, materials, or any combination of the foregoing or (2) in excess of $100,000 for real property renovations and construction.

   b. The Contractor to the subject contract ("Contractor" and "Contract" or "Agreement" respectively, agrees to fully comply and cooperate with NYSERDA in the implementation of New York State Executive Law Article 17-B and the Regulations. These requirements include the promotion of opportunities for maximum feasible participation of certified service-disabled veteran-owned business enterprises (SDVOB) in the performance of NYSERDA contracts and among other things, that NYSERDA establish goals for maximum feasible participation of New York State Certified SDVOBs in the performance of New York State contracts. Contractor's demonstration of "good faith efforts" pursuant to the Regulations shall be a part of these requirements.

   c. Failure to comply with all of the requirements herein may result in a breach of contract, leading to the withholding of funds or other such actions as allowed by the Contract.

   d. The Contractor further fully agrees to cooperate with NYSERDA in the implementation of such additional requirements as may be required by the Division of Service-Disabled Veterans' Business Development located within OGS.

2. **Contract Goals by SDVOBs** NYSERDA's participation goals for this procurement are ___ for SDVOBs. This is in addition to required MWBE participation goals which are discussed in Attachments ___.

3. **Participation Goals** The Contractor represents that it has reviewed and familiarized itself with the Regulations (see http://ogs.ny.gov/About/Regs/docs/part252.pdf) which are incorporated herein by this reference. Any conflicts between this Agreement and the Regulations shall be resolved in favor of the Regulations. The Contractor shall, in accordance with the Regulations, make good faith efforts and, in a manner that can be established in documentary form, solicit active participation by certified SDVOBs, as identified in the applicable state directory maintained by OGS (see http://ogs.ny.gov/core/docs/CertifiedNYS_SDVOB.pdf). Additionally, the Contractor is encouraged to contact the Division of Service-Disabled Veterans' Business Development at 844-579-7570 or VeteransDevelopment@ogs.ny.gov to discuss additional methods of maximizing SDVOBs on the contract. In furtherance thereof, the Contractor has submitted a completed SDVOB Utilization Plan (see **Attachment 8**) and/or a NYSERDA approved Waiver Form (see **Attachment 10**), which information sets forth NYSERDA's and Contractor's agreed upon participation goals during the performance of this Agreement.

4. **Compliance Reporting** In order to demonstrate compliance with the stated Contract goals set forth above, Contractor shall be required to submit compliance reports. Unless NYSERDA has granted a total waiver or Contractor is a certified SDVOB with OGS and is responsible for 100% of the performance of this Agreement, the Contractor shall submit to NYSERDA an SDVOB Compliance Report on a quarterly basis in the form attached hereto as **Attachment 9**. The Contractor's failure to follow the applicable reporting requirements or failure to comply with the stated participation goals in the previous Section set forth above may result in NYSERDA's submission of a complaint to OGS Division of Service-Disabled Veterans' Business Development

5. **Waiver Requests** In Accordance with the Regulations, Contractor may submit, at any time prior to its request for final payment, a request to NYSERDA for total or partial waiver of the requirements of the SDVOB contract goal. NYSERDA may grant a partial or total waiver of the requirements of the Contract goals established hereunder. Prior to granting or denying a waiver, NYSERDA shall evaluate the Contractor's good faith efforts and may consider the factors set forth in the Regulations. If NYSERDA, upon review of the SDVOB Utilization Plan and updated Quarterly SDVOB Contractor Compliance Reports determines that Contractor is failing or refusing to comply with the Contract goals and no waiver has been issued in regards to such non-compliance, NYSERDA may issue a notice of deficiency to the Contractor. The Contractor must respond to the notice of deficiency within seven business days. Such response may include a request for a partial or total wavier of SDVOB Contract goals. In the event NYSERDA refuses to grant a waiver, the proposer may file a complaint with NYSERDA in accordance with the Regulations and as stated below.

6. **Contractor and NYSREDA Complaints** If the Contractor becomes deficient with regard to its Utilization Plan as provided above, the Contractor may file a complaint with NYSERDA. The complaint should state the reasons for the complaint, together with a demand for relief and include the following information: (1) the Contractor's receipt of a written determination by NYSERDA that the contractor is not entitled to a partial or full waiver of the SDVOB goals; or (2) the Contractor's receipt of a written determination by NYSERDA that the Contractor has not acted in good faith, has failed, is failing, or is refusing to comply with goals. NYSERDA shall provide the Contractor with an opportunity to be heard and shall conduct a review and shall render a determination regarding the merits of the complaint. Within 20 days of NYSERDAs determination that the Contractor has not acted in good faith, has failed, is failing, or is refusing to comply with the SDVOB goals, NYSERDA may, after giving the Contractor an opportunity to be heard, make a determination that the Contractor has failed to meet the contract goals and assess such other damages as were identified in the Contract.

7. **Article 17-B Compliance Monitoring** NYSERDA is responsible for monitoring Contractor's compliance with the applicable Regulations. In that regard, NYSERDA may, at its discretion, notify the Contractor in writing of NYSERDA's intent to inspect relevant records and documents related to Article 17-B compliance. NYSERRDA shall analyze and consider such records, documents and other data to determine whether the Contractor has made conscientious and active efforts to employ and utilize SDVOBs on the State contract.

8. **Violations** Any Contractor who willfully and intentionally fails to comply with the SDVOB contract goals and requirements contained in the Agreement and Regulations shall be liable to NYSERDA for damages as otherwise specified in the Agreement. Damages shall be calculated based on the actual cost incurred by NYSERDA related to NYSERDA's expenses for personnel, supplies and overhead related to establishing, monitoring and reviewing SDVOB programmatic goals.