SILICON VALLEY CLEAN ENERGY

ITP5

Category: INFORMATION TECHNOLOGY

IT SECURITY PLAN POLICY

I. PURPOSE

To provide an overview of the security requirements of SVCE's Information Technology (IT) system and network, to describe the controls in place to meet those requirements, and to delineate responsibilities and expected behavior of all individuals who access the system.

II. SCOPE

This applies to all IT assets and to all SVCE personnel.

III. DEFINTIONS

"Security" refers to the state of being free from danger or injury. The effort to create a secure computing platform, designed so that agents (users or programs) can only perform actions that have been allowed.

IV. POLICY

A. PREPARING IT SECURITY

- IT Support shall begin the planning process with an up-to-date inventory of IT assets.

- IT Support shall continue the planning process with an assessment of the threats and risks to the IT system/network, in accordance with the IT Threat Assessment Checklist.

- IT Support shall conduct a Security assessment of SVCE's IT network.

- IT Support shall evaluate findings and discuss recommendations to correct deficiencies and/or improve Security with the Director of Finance and Administration.

B. DEVELOPING THE IT SECURITY PLAN

IT Support shall develop the Information Technology Security Plan and submit the plan to the SVCE Board of Directors for approval.

C. IMPLEMENTING THE IT SECURITY PLAN

All IT systems shall be identified according to a standard format. Systems identification shall include, but not necessarily be limited to, the following:

- System name and ID
- Responsible organization(s)
- Contact information
- Operational status
- Description & purpose
- Interconnections and information sharing
- Applicable regulations
- Information sensitivity

Management controls for every system shall include, but not necessarily be limited to:

- Risk assessment and management;
- Review of Security controls;
- Security planning throughout the system life cycle; and
- Processing authorization.

Operational controls for each system shall include, but not necessarily be limited to:

- Personnel Security
- Physical/environmental protections
- Production and input/output controls
- Contingency planning
- Hardware/software maintenance controls

- Integrity controls
- System documentation
- Incident response
- Security awareness and training

Technical controls for each system shall include, but not necessarily be limited to:

- Identification and authentication of users
- Access control
- Audit trails

IT Support shall communicate the Information Technology Security Plan to all SVCE staff and will address any questions related to the plan.

IT Support shall coordinate employee Security training with the Administration and Finance Department. Administration and Finance shall train all new users in IT Security within one week of their hiring and retrain all users in accordance with the Information Technology Security Plan at least once every two years.

D. IT SECURITY PLAN REVIEW

Once the Information Technology Security Plan is implemented, IT Support shall conduct a periodic internal review of the plan. This review should take place at least annually and shall include an examination of:

- Current Security conditions
- Changes to the plan, as recommended by IT Support
- User satisfaction Results of any internal or external audits
- Progress of the stated goals of the existing plan.

At least once every three years, SVCE shall participate in an external review (audit), to verify its compliance with the Information Technology Security Plan and help evaluate the plan's effectiveness.

E. IT SECURITY PLAN UPDATE

After any review of the IT Security Plan, IT support shall be responsible for implementing required updates.

Within three months of such updates, IT Support shall verify that the updates have been implemented and are providing the desired results.

V. ATTACHMENTS

1. Information Technology Security Plan
2. IT Security Plan Implementation Schedule

INFORMATION TECHNOLOGY SECURITY PLAN

A. SYSTEM IDENTIFICATION

Date:

System Name/Title

- Unique Identifier and Name Given to the System

Responsible Organization

- List organization responsible for the system

Information Contact(s)

- Name of person(s) knowledgeable about, or the owner of, the system.

Name:

Title

Address:

Phone:

Assignment of Security Responsibility

- Name of person responsible for security of the system.

Name:

Title

Address:

Phone:

System Operational Status

If more than one status is selected, list which part of the system is covered under each status.

- Operational
- Under Development
- Undergoing a major modification

General Description/Purpose

- Describe the function or purpose of the system and the information processed.
- Describe the processing flow of the application from system input to system output.
- List user organizations (internal and external) and type of data and processing provided.
- List all applications supported by the general support system. Describe each application's functions and information processed.

System Environment

- Provide a general description of the technical system. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.)
- Describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources.
- Include any security software protecting the system and information.

System Interconnection/Information Sharing

- List of interconnected systems and system identifiers (if appropriate).
- If connected to an external system not covered by a security plan, provide a short description of any security concerns that need to be considered for protection.
- It is required that written authorization (MOUs, MOAs) be obtained prior to connection with other systems and/or sharing sensitive data/information. It should detail the rules of behavior that must be maintained by the interconnecting systems. A description of these rules must be included with the security plan or discussed in this

section.

Applicable Laws or Regulations Affecting the System

- List any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.

General Description of Information Sensitivity

- Describe, in general terms, the information handled by the system and the need for protective measures. Relate the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability). For each of the three categories, indicate if the requirement is **High**, **Medium**, or **Low**.
- Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.

B. MANAGEMENT CONTROLS

Risk Assessment and Management

- Describe the risk assessment methodology used to identify the threats and vulnerabilities of the system. Include the date the review was conducted. If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.

Review of Security Controls

- List any independent security reviews conducted on the system in the last three years.
- Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

Rules of Behavior

- A set of rules of behavior in writing must be established for each system. The rules of behavior should be made available to every user prior to receiving access to the system. It is recommended that the rules contain a signature page to acknowledge receipt.
- The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. They should state the consequences of inconsistent behavior or noncompliance. They should also include appropriate limits on interconnections to other systems.
- Attach the rules of behavior for the system as an appendix and reference the appendix number in this section or insert the rules into this section.

Planning for Security in the Life Cycle

Determine which phase(s) of the life cycle the system or parts of the system are in. Describe how security has been handled in the life cycle phase(s) that the system is currently in.

Initiation Phase

- Reference the sensitivity assessment which is described in Section 3.7, Sensitivity of Information Handled.

Development/Acquisition Phase

- During the system design, were security requirements identified?
- Were the appropriate security controls with associated evaluation and test procedures developed before the procurement action?
- Did the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?
- Did the requirements permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented?
- If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security

requirements identified and included in the acquisition specifications?

Implementation Phase

- Were design reviews and systems tests run prior to placing the system in production? Were the tests documented? Has the system been certified?
- Have security controls been added since development?
- Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?
- Include the date of the certification and accreditation. If the system is not authorized yet, include date when accreditation request will be made.

Operation/Maintenance Phase

- The security plan documents the security activities required in this phase.

Disposal Phase

- Describe in this section how information is moved to another system, archived, discarded, or destroyed. Discuss controls used to ensure the confidentiality of the information.
- Is sensitive data encrypted?
- How is information cleared and purged from the system?
- Is information or media purged, overwritten, degaussed or destroyed?

Authorize Processing

- Provide the date of authorization, name, and title of management official authorizing processing in the system.
- If not authorized, provide the name and title of manager requesting approval to operate and date of request.

C. OPERATIONAL CONTROLS

Personnel Security

- Have all positions been reviewed for sensitivity level?
- Have individuals received background screenings appropriate for the position to which they are assigned.
- Is user access restricted to the minimum necessary to perform the job?
- Is there a process for requesting, establishing, issuing, and closing user accounts?
- Are critical functions divided among different individuals (separation of duties)?
- What mechanisms are in place for holding users responsible for their actions?
- What are the friendly and unfriendly termination procedures?

Physical and Environmental Protection

- Discuss the physical protection for the system. Describe the area where processing takes place (e.g., locks on terminals, physical barriers around the building and processing area, etc.)
- Factors to address include physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, and mobile and portable systems.

Production, Input/Output Controls

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to, software should be listed. In this section, provide a synopsis of the procedures in place that support the system. Below is a sampling of topics that should be reported in this section.

- User support - Is there a help desk or group that offers advice?
- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information

- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media
- Audit trails for receipt of sensitive inputs/outputs
- Procedures for restricting access to output products
- Procedures and controls used for transporting or mailing media or printed output
- Internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary)
- External labeling with special handling instructions (e.g., log/inventory identifiers, controlled access, special storage instructions, release or destruction dates)
- Audit trails for inventory management
- Media storage vault or library-physical, environmental protection controls/procedures
- Procedures for sanitizing electronic media for reuse (e.g., overwriting or degaussing)
- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse
- Procedures for shredding or other destructive measures for hardcopy media when no longer required

Contingency Planning

Briefly describe the procedures (contingency plan) that would be followed to ensure the system continues to process all critical applications if a disaster were to occur. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan can be attached as an appendix.

- Any agreements of backup processing.
- Documented backup procedures in including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup).
- Location of stored backups and generations of backups kept.
- Are tested contingency/disaster recovery plans in place? How often are they tested?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

Hardware and System Software Maintenance Controls

- Restriction/controls on those who perform maintenance and repair activities.
- Special procedures for performance of emergency repair and maintenance.
- Procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site).
- Procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements.
- Version control that allows association of system components to the appropriate system version.
- Procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production.
- Impact analyses to determine the effect of proposed changes on existing security controls to include the required training for both technical and user communities associated with the change in hardware/software.
- Change identification, approval, and documentation procedures.
- Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes.
- Are test data “live” data or made-up data?
- Are there organizational policies against illegal use of copyrighted software or shareware?

Integrity Controls

- Is virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?
- Are reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Are password crackers/checkers used?
- Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?
- Are intrusion detection tools installed on the system?

- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?
- Is penetration testing performed on the system? If so, what procedures are in place to ensure they are conducted appropriately?
- Is message authentication used in the system to ensure that the sender of a message is known and that the message has not been altered during transmission?

Documentation

Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security of the system to include backup and contingency activities, as well as descriptions of user and operator procedures.

- List the documentation maintained for the system (vendor documentation of hardware/software, functional requirements, security plan, program manuals, test results documents, standard operating procedures, emergency procedures, contingency plans, user rules/procedures, risk assessment, authorization for processing, verification reviews/site inspections).

Security Awareness & Training

- The awareness program for the system (posters, booklets, and trinkets)
- Type and frequency of general support system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the job training)
- The procedures for assuring that employees and contractor personnel have been provided adequate training

Incident Response Capability

- Are there procedures for reporting incidents handled either by system personnel or externally?

- Are there procedures for recognizing and handling incidents, i.e., what files and logs should be kept, who to contact, and when?
- Who receives and responds to alerts/advisories (e.g., vendor patches, exploited vulnerabilities)?
- What preventive measures are in place (i.e., intrusion detection tools, automated audit logs, penetration testing)?

D. TECHNICAL CONTROLS

Identification and Authentication

- Describe the method of user authentication (password, token, and biometrics).
- If a password system is used, provide the following specific information:
- Allowable character set;
- Password length (minimum, maximum);
- Password aging time frames and enforcement approach;
- Number of generations of expired passwords disallowed for use;
- Procedures for password changes;
- Procedures for handling lost passwords, and
- Procedures for handling password compromise.
- Procedures for training users and the materials covered.
- Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).
- Describe any biometrics controls used. Include a description of how the biometrics controls are implemented on the system.
- Describe any token controls used on this system and how they are implemented.
- Describe the level of enforcement of the access control mechanism (network, operating system, and application).
- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).
- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are transmitted and stored with one-way encryption to prevent anyone [including the System Administrator]

from reading the clear-text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords).

- State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.
- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.
- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).
- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.
- If digital signatures are used, the technology must conform to FIPS 186*, Digital Signature Standard* and FIPS 180-1, *Secure Hash Standard* issued by NIST, unless a waiver has been granted. Describe any use of digital or electronic signatures.

Logical Access Controls

- Discuss the controls in place to authorize or restrict the activities of users and system personnel within the system. Describe hardware or software features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists (ACLs).
- How are access rights granted? Are privileges granted based on job function?
- Describe the system’s capability to establish an ACL or register.
- Describe how users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent user from accessing the system or applications outside of normal work hours or on weekends.

- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.
- Indicate if encryption is used to prevent access to sensitive files as part of the system or application access control procedures.
- Describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Dept. of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

Audit Trails

- Does the audit trail support accountability by providing a trace of user actions?
- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection?
- Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them? (Type of event, when the event occurred, user id associated with the event, program or command used to initiate the event, etc.)
- Is access to online audit logs strictly enforced?
- Is the confidentiality of audit trail information protected if, for example, it records personal information about users?
- Describe how frequently audit trails are reviewed and whether there are guidelines.
- Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem?

IT SECURITY PLAN IMPLEMENTATION SCHEDULE

Task — Completion Date

1. Draft Security Plan ____________
2. Submit Plan for review by other managers ____________
3. Edit Security Plan ____________
4. Finalize Security Plan ____________
5. Submit Plan to Board of Directors ____________
6. Revise as necessary ____________
7. Distribute Security Plan Memo to all personnel ____________
8. Distribute Security Plan to Management Staff ____________
9. Meet with Managers ____________
10. Establish means to accomplish security tasks and activities ____________
11. Establish Security Breach Committee ____________
12. Establish Proactive Security Committee ____________
13. Obtain and install required equipment ____________
14. Implement specific programs ____________
15. Evaluate Security Plan implementation ____________
16. Evaluate Security Program
    - Internal review ____________
    - External audit ____________
17. Modify Security Program and Plan
    - Schedule Security Plan update ____________

IT Support: ________________________________ Date: ____________

Dir. of Admin. and Finance: ____________________ Date: ____________