SILICON VALLEY
CLEAN ENERGY

ITP9

Category: INFORMATION TECHNOLOGY

IT SECURITY AUDIT POLICY

I. PURPOSE

To ensure that SVCE's Information Technology (IT) security system conforms to legal, regulatory and SVCE requirements, that the system is effectively implemented and maintained, and that it performs as expected.

II. SCOPE

This applies to all IT systems and assets.

III. DEFINTIONS

"Audit Criteria" -- Policies, practices, procedures, or requirements against which the auditor compares collected audit evidence about the subject matter.

"Auditee" – Party or parties whose processes, procedures, etc., are the subject of the audit.

"Security Audit" – An examination of a computer system for security problems and vulnerabilities.

IV. POLICY

A. IT SECURITY AUDIT PLANNING

SVCE shall conduct internal audits of its security management system at planned intervals (annually, at a minimum) to determine if its control objectives, controls, processes, and procedures conform to legal/regulatory requirements, and that SVCE information security requirements are effectively implemented, maintained and perform as expected.

IT Support shall conduct an assessment of the existing IT security system, in order to establish a baseline for auditing.

IT Support shall acquire and review additional pertinent information for IT Security Auditing, including industry standards and practices.

The plan shall serve as the basis for internal audits of IT Security.

IT Support shall develop the IT Security Audit Plan and submit the Plan to management.

B. IT SECURITY AUDIT PLAN

Prior to conducting the audit, IT Support shall define the objectives, scope and criteria of the audit and determine if the audit is feasible.

IT Support shall from an audit team, which can include internal as well as external resources. The audit team shall prepare for onsite audit activity by preparing the audit plan and assigning tasks to members of the audit team.

Audit team members shall prepare work documents, such as audit checklists, sampling plans and forms for recording information (minutes of meetings, supporting evidence, audit findings, etc).

Communication during the audit:

- The audit team should meet periodically to exchange information, access the progress of the audit and reassign work between members, if needed.
- Evidence that suggests an immediate and significant risk should be reported to the Director of Administration and Finance immediately.
- Audit team members shall collect, record and verify information relevant to the objectives, scope and criteria of the audit. Information may be acquired through interviews, observations of activities and document reviews.
- Audit team members' concerns about issues outside the audit scope should be reported to the audit team leader for possible communication to IT Support.
- The audit team shall meet as needed for review their findings.
- The audit team shall prepare, approve and distribute its IT Security Audit Report.

C. IT SECURITY AUDIT REVIEW

If it has been decided to take corrective action, the Director of Administration and Finance shall submit a corrective action plan, including objectives, actions, and deadlines, to the audit team leader. If it has been decided not to take corrective action, the Director of Administration and Finance shall inform the audit team leader of this decision, with explanation.

D. IT SECURITY AUDIT – CORRECTIVE ACTION

IT Support shall be responsible for taking corrective actions, if required. Corrective actions shall be taken within the period prescribed in the audit and as agreed to by the Director of Administration and Finance.

IT Support shall notify the audit team when corrective actions have been completed. The audit team shall verify that corrective actions have been taken and that they are having the desired effect.

V. ATTACHMENTS

1. IT Security Audit Report

IT SECURITY AUDIT REPORT

A. Audit Objectives

B. Audit Scope

C. Audit Client

D. Audit Team (leader and members)

(NOTE: Auditors cannot audit their own work)

E. Dates of Onsite Audit

F. Audit Criteria

G. Audit Findings/Observations

H. Audit Conclusions

IT Support: ________________________________ Date: ____________

Admin & Finance: ___________________________ Date: ____________