SILICON VALLEY
CLEAN ENERGY

ITP11

Category: INFORMATION TECHNOLOGY

IT THREAT-RISK ASSESSMENT POLICY

I. PURPOSE

SVCE shall regularly evaluate its Information Technology (IT) systems and network for threats and vulnerabilities in order to protect its IT assets and reduce the risk to SVCE

II. SCOPE

This procedure applies to all of SVCE's IT assets, including the IT network.

III. DEFINTIONS

Risk – Possibility of losing availability, integrity, or confidentiality of IT assets due to a specific threat; also, the product of threat level and vulnerability level.

Threat – Expression of intent to inflict injury, damage or potential violation of security.

Threat Assessment – A process by which types of threats an IT network might be vulnerable to and where the network is most vulnerable are identified.

Vulnerability – Flaw or weakness in a system's design, implementation, or operation and management that could be exploited.

IV. POLICY

A. IT THREAT & RISK ASSESSMENT – INTRODUCTION

In order to prepare for Threats to its IT assets and infrastructure, SVCE must be aware of the types of Threats that exist, the likelihood that they will occur, their potential impact, and the Risk these Threats may pose.

Threats may be natural or manmade. Natural Threats include floods, storms, and earthquakes. Manmade Threats may be accidental or intentional. Examples of manmade Threats include use of unauthorized hardware or software and having unauthorized access to SVCE systems

Intentional Threats exist both outside the Agency and within

The Risk posed by any given Threat is a function of the combined likelihood of the Threat occurring and the impact it would have on SVCE's assets (hardware, software, data, network/infrastructure, and personnel) if it were to occur. While Risk to SVCE's IT assets cannot be completely eliminated, the Agency must make all reasonable efforts to minimize Risk. Those efforts should begin with assessing Threats and Risks.

B. IT THREAT ASSESSMENT PREPARATION

In advance of conducting a Threat Assessment of any of SVCE's IT systems, IT Support shall establish a baseline for assessment, identifying systems to be assessed (power supply, HR, marketing, etc.) and determining their interconnectivity with other systems.

IT Support should identify and describe Threats that may target the IT assets and systems under consideration by one or more of the following means:

- Periodically (at least once a month) reviewing Access Control Log for threat occurrences, such as unauthorized system access.

- Reviewing IT incidents for trends and/or patterns.

- Reviewing any system test (test script, test procedures, expected results, etc.) for vulnerabilities testing.

- Conducting penetration testing at irregular intervals, to verify the IT network's ability to withstand intentional attempts at circumventing IT security.

IT Support may acquire additional information for developing the assessment baseline by routinely reviewing Threat alerts and bulletins from vendors, standards organizations, etc. Subscribing to one or more Threat alert mailing lists is recommended.

To determine if SVCE needs to act on any given Threat and to what extent it should act, IT Support shall classify Threats/ Vulnerabilities in the following manner:

The likelihood of Threats occurring, according to information provided by external sources. Threat likelihood may be categorized as:

a. Low – the Threat is unlikely to occur;
b. Medium – the Threat may occur. For example, SVCE is located in an earthquake zone, so an earthquake is likely to have an effect on SVCE; and
c. High – the Threat is likely to occur. For example, if SVCE does not require password access to computers or data stores, the likelihood is high that someone will eventually access and steal or compromise SVCE data.

The impact of Threats, in the absence of protection, and the possible or likely consequences of each. Threat impact may be classified as:

a. Low – the Threat may result in minimal loss of SVCE assets/resources;
b. Medium – the Threat may result in a significant loss of SVCE assets/ resources, harm SVCE's mission or interests, or result in injury to an employee; and
c. High – the Threat may result in a very costly loss of SVCE's assets/resources, significantly harm SVCE's mission, interests, or standing, or result in serious or fatal injury to an employee

An exposure rating or Risk assessment shall be based on likelihood and impact ratings. A Risk matrix is prescribed (Figure 1), with likelihood running from low to high along one axis and impact running from low to high on the other axis. The resulting exposure rating/Risk assessment shall be used to prioritize Threats (Figure 2).

a. High-risk Threats require the highest security levels and present the greatest need for immediate action, if existing security tools and techniques are inadequate.
b. Low-risk Threats may require little or no response on the part of the IT Support.

	Impact	Low	Medium	High
Likelihood	High	Low	Medium	High
	Medium	Low	Medium	Medium
	Low	Low	Low	Low

FIGURE 1 – RISK MATRIX

Risk Level	Description and Actions
High	Preventive actions are required and a preventive action plan shall be developed and implemented as soon as possible.
Medium	Preventive actions are required and a plan to incorporate those actions within a reasonable time frame shall be developed.
Low	IT Support should confer with managers of affected systems to determine if preventive action is required or if risk is acceptable.

FIGURE 2 – THREAT PRIORITY

C. IT THREAT/RISK ASSESSMENT

At regular intervals (at least once every six months), IT Support shall conduct a Threat/Vulnerability scan of the IT network. This scan should be performed using commercially available software designed expressly for the purpose.

IT Support shall review scan results and analyze the findings in order to determine if SVCE needs to act on them and to what extent.

IT Support shall create an IT Threat/Risk Assessment Report summarizing assessment findings and containing the following information, at a minimum:

- Systems reviewed

- Number of Threats found this period and last
- A summary of identified Threats.

D. IT THREAT/RISK MANAGEMENT REVIEW

IT Support shall periodically review the Risk assessment process to ensure its continued timeliness and applicability. Historical data (i.e., number, nature, and severity of Threats over time) shall help determine if Risks are under control.

Any time a significant implementation, revision, etc., takes place, IT Support shall review the Risk assessment process, to ensure existing controls are applicable to such changes or if improved controls are required.

V. ATTACHMENTS

1. Threat-Risk Assessment Report

Category: INFORMATION TECHNOLOGY

THREAT-RISK ASSESSMENT REPORT

Date: __________________

Systems Reviewed: ____

____

Threats found this period: ______________________

Description: ____

____

____

Threats found last period: ______________________

Description: ____

____

____

Threat Summary:

Risk Level	Number	Description
LOW		
MEDIUM		
HIGH		