SILICON VALLEY CLEAN ENERGY

ITP6

Category: INFORMATION TECHNOLOGY

IT ACCESS CONTROL POLICY

I. PURPOSE

To prevent unauthorized access to or use of SVCE information, to ensure its security, integrity, and availability to appropriate parties.

II. SCOPE

This applies to all SVCE information and to all storage and access methods.

III. DEFINTIONS

"Access Control**"** refers to enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access (or, providing access to authorized users while denying access to unauthorized users).

IV. POLICY

A. BUSINESS REQUIREMENTS FOR REGULATING ACCESS

Every Information Technology (IT) user shall have a unique identifier and a system password assigned.

There shall be a system in place for authenticating and authorizing users beyond the login point. Access to applications, databases, etc., once a person is in the system must be controlled.

Each user shall be given access to IT resources based on position and department. Users shall be given the fewest privileges needed to perform their duties, as listed in their job descriptions.

User activity shall be monitored frequently and reviewed for unusual, unauthorized or illegal activity, current periods of inactivity, etc.

User access may be suspended for:

- A number of consecutive failed log-on attempts;
- Unauthorized or illegal activity; or
- An extended period of account inactivity.

B. MANAGEMENT OF USER ACCESS

Users shall be formally registered at the time of their employment with SVCE. Users shall be reregistered upon changing jobs within SVCE and deleted/unregistered upon leaving SVCE or after a specific period (e.g., 30 days) of inactivity.

Access to SVCE information shall be granted on a need-to-know basis. Users shall be authorized according to minimum access requirements for their duties. Access may be "read only", "read/write", or "full access" and users may or may not be given administrative privileges for their computers and for certain data.

Password Control – see Password Protection Policy.

- Accounts shall be automatically suspended upon three consecutive failed logon attempts. Users shall request a password reset from IT Support.
- Systems shall identify and authenticate users before granting access.

IT Support shall review all users' access rights/privileges on a regular basis (every 90 days, at a minimum).

C. USER RESPONSIBILITIES

Users must secure their equipment if it is to be unattended for any length of time. Screen locks should automatically activate after 15 minutes of inactivity (users may set screen locks to activate sooner and they should be allowed to activate screen locks immediately, if desired).

Users shall have direct access only to services and information that they have been specifically authorized to use. Unless expressly authorized, access to all resources and services is denied. IT Support shall maintain an Access Control database for that purpose.

All communications to external (i.e., Internet-based) resources by way of SVCE's IT network shall be restricted to authorized users. Users shall apply for permission to access external resources and access shall be authorized on a case-by-case basis.

D. OPERATING SYSTEM ACCESS CONTROL

- Access to operating systems shall be limited to trusted, authorized users (for example, IT Support staff).
- Only authorized support personnel shall be authorized to access operating systems and utilities outside of normal business hours.
- Access to operating systems and related utilities shall be logged and such logs shall be reviewed periodically (weekly, at a minimum) by IT Support.
- Operating systems connections shall be terminated after 15 minutes of inactivity.

E. APPLICATION ACCESS CONTROL

- Access to applications shall be limited to authorized users.
- Access to applications shall be limited to normal business hours, with reasonable exceptions.
- Application access shall be logged and those logs shall be reviewed by IT Support who is responsible for developing, installing, and maintaining the applications.
- Connections to applications should be terminated after a predetermined period of inactivity (15 minutes).

F. MONITORING SYSTEM ACCESS USE

- Instances of access and use of any IT resource shall be automatically logged.
- Access control logs shall be retained in accordance with legal and regulatory requirements.

V. POLICY COMPLIANCE

A. COMPLIANCE

The IT Department will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

B. NON-COMPLIANCE

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