SILICON VALLEY CLEAN ENERGY

ITP1

Category: INFORMATION TECHNOLOGY

INFORMATION SYSTEMS USE POLICY

I. PURPOSE

The purpose of this policy is to outline the acceptable use of information systems and resources at SVCE. Inappropriate use exposes SVCE to risks including malware, compromise of network systems and services, and legal issues. Therefore, this policy has been put into place to protect users and SVCE.

II. SCOPE

All users of SVCE's computers or network infrastructure.

III. DEFINTIONS

"Data" is any and all information stored or transmitted over SVCE Resources.

"Information Systems" refers to all Resources that store, transmit or present information related to SVCE business.

"Resources" refers to all SVCE-owned hardware and software including, but not limited to:

- Computers, laptops, tablets, desk phones
- Network storage, network infrastructure, servers
- All software applications licensed by SVCE
- Accounts such as email account or other accounts used to access SVCE applications
- Data plans, subscription services

"Sensitive Information" includes all Data, in its original and duplicate form, which contains personal information, protected health information, customer record information, card holder Data, confidential personal Data, or information that is deemed to be confidential or is otherwise exempt from disclosure under state law.

"User" is anyone using SVCE computing Resources including, but not limited to: employees, contractors, limited-term employees, and interns.

Adopted: 6/14/2017
Revised: 9/13/2017

IV. POLICY

A. ACCEPTABLE USE

Use of SVCE's Information Systems is limited to SVCE business.

You may access, use or share SVCE proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

B. STRICTLY PROHIBITED USE

Use of SVCE Information Systems to send messages of a threatening, harassing, or obscene nature, or any behavior found to be inconsistent with the SVCE Employee Handbook, is prohibited. Inappropriate use may include, but is not limited to: the display or transmission of sexually explicit images, messages or cartoons, any transmission that contains ethnic slurs, racial epithets, or anything that constitutes harassment or disparagement of others based on their race, national origin, color, sex, sexual orientation, age, disability, religious or political beliefs.

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SVCE.

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from

magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which SVCE or the end user does not have an active license is strictly prohibited.

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

C. SECURITY AND PERSONAL INFORMATION

- All software applications and subscription services are to be secured with a password sufficient to protect SVCE information.
- Users who are granted access to any part of SVCE's Information Systems are provisioned with an account.
- Users are to use their assigned account and no other.
- Users are prohibited from using another User's account to access any part of an Information System.
- Users are prohibited from sharing their passwords or passphrases.
- Authorized staff may reset passwords as required for business purposes.
- Users who are provisioned with SVCE Resources are not allowed to change permissions, modify hardware, or modify code and configuration on any SVCE Resource, unless directed to do so by authorized personnel.

- All Users are responsible for safeguarding Sensitive Information.
- Users may access, use or share Sensitive Information held by SVCE only to the extent it is authorized and necessary to fulfill their assigned job duties.
- Users must immediately notify IT Support if Sensitive Information is inappropriately shared or exposed.
- Users must immediately report to IT Support any suspicious e-mail or other computer activity.

D. NO EXPECTATION OF PRIVACY

SVCE owns all Data stored on Agency Resources and reserves the right to access anything the User has viewed or created using those Resources.

Users shall have no expectation of privacy. Authorized SVCE staff may view any and all activities and Data created, stored or transmitted using SVCE Resources. They may access any electronic Data or files at any time without consent from or notification to the User.

SVCE may monitor, record and review any Data or websites a User may have accessed through an SVCE internet connection.

SVCE strongly discourages the storage of personal files and messages (pictures, personal email, texts, instant messages, music, spreadsheets, etc.) on SVCE-provided computers. All such Data may be accessed and reviewed at the Agency's discretion and may be deleted without notice.

V. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

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.