PASSWORD PROTECTION POLICY

I. PURPOSE

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

II. SCOPE

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any SVCE facility, has access to the SVCE network, resides on third party servers (BOX, Office 365, etc), or stores any non-public SVCE information.

III. POLICY

A. PASSWORD CREATION

All user-level and system-level passwords must conform to the Password Construction Guidelines in Attachment 1.

Where possible, users must not use the same password for various SVCE access needs.

Users must not use the same password for SVCE accounts as for other non-SVCE access (for example, personal ISP account, benefits, and so on).

B. PASSWORD CHANGE

All system-level passwords (for example application administration accounts, and so on) must be changed on at least a quarterly basis.

All user-level passwords (for example, email, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

Password cracking or guessing may be performed on a periodic or random basis by the IT Support Team. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. PASSWORD PROTECTION

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential SVCE information.
- Passwords must not be inserted into email messages, or other forms of electronic communications.
- Passwords must not be revealed over the phone to anyone.
- Do not share SVCE passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Do not reveal a password on questionnaires or security forms.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile device (phone, tablet) without encryption.
- Do not use the “Remember Password” feature of applications (for example, web browsers).
- Any user suspecting that their password may have been compromised must report the incident and change all passwords.

IV. 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.

V. ATTACHMENTS

1. Password Construction Guidelines

PASSWORD CONSTRUCTION GUIDELINES

I. OVERVIEW

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data or the SVCE network. This guideline provides best practices for creating secure passwords.

II. SCOPE

This guideline applies to employees, contractors, consultants, temporary and other workers at SVCE. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection and voicemail.

III. STATEMENT OF GUIDELINES

All passwords should meet or exceed the following guidelines:

STRONG PASSWORDS HAVE THE FOLLOWING CHARACTERISTICS:

- Contain at least 12 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, #$?!).

POOR, OR WEAK, PASSWORDS HAVE THE FOLLOWING CHARACTERISTICS:

- Contain at least eight characters.
- Can be found in a dictionary or exists in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone number, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.

- Contain number patterns such as aaabbb, 123321, etc.
- Are some version of “Welcome123”, “Password123”, etc.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).

PASSPHRASES

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines and include upper and lower case letters, number, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).