Policy-Password

Passwords are an important aspect of computer security and are the front line of protection for user accounts. A poorly chosen password may result in the compromise or expose of company’s entire corporate network. As such, all company employees including contractors and vendors with access to systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

# 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 Link3 facility, has access to the Link3 network, or stores any nonpublic Link3 information.

# Policy

The Chief Security Officer (CSO) shall ensure:

* Policies and procedures manage the process of creating, changing, and safeguarding passwords.
* Policies and procedures prevent staff from sharing passwords with others.
* Procedures that advises staff to commit their passwords to memory and not allow them to be written down. Policies and procedures govern the password change frequency.

A. General

Passwords must be changed and maintain a change log on a regular basis according to the following schedule:

* All system-level passwords (e.g., admin, root) must be changed every 30 days.
* All user-level passwords (e.g. Active Directory Domain Passwords, E-mail, Web, desktop computer, etc.) must be changed at least every 60 days.
* User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
* Passwords must not be inserted into e-mail messages or other forms of electronic communication.
* Passwords must not be stored or transmitted in clear (unencrypted) text in web or any electronic form.
* Users are not permitted to submit a new password/phrase that is the same as any of the last **four** passwords/phrases he or she has used.

All user-level and system-level passwords must conform to the guidelines described below.

B. Guidelines

Passwords are used to restrict access to systems, software applications, and data. When selecting a password, Staff should remember that the longer and stronger the password, the more likely it will help keep safe Information Systems, and the data contained with the systems, secure.

Where possible, company recommends that the passwords:

* Contain both upper and lower case characters (e.g., a-z, A-Z).
* Include both numbers and special characters (e.g. <, >, @, #, $, \*).
* Have a minimum of at least 8 characters and preferably ten alphanumeric characters long and is a passphrase.
* Don’t contain personal information such as a relative or pet’s name, social security or driver's license number, street address or phone number, etc.
* Avoid sequences or repeated characters. For example, 1234, 3333, etc.
* Not be common words such as those found in a dictionary.

Please remember:

* Do not reveal a password over the phone to ANYONE.
* Do not reveal a password in an email message.
* Do not reveal a password to the boss.
* Do not talk about a password in front of others.
* Do not hint at the format of a password (e.g., "my family name").
* Do not reveal a password on questionnaires or security forms.
* Do not share a password with family members.
* Do not reveal a password to co-workers while on vacation.
* Be careful when using social media so that you don’t compromise your password.

If someone demands a password, refer them to this document or have them call someone in the IT Department. Do not use the "Remember Password" feature (e.g. browsers, software applications).

Passwords must not be written down. Do not store passwords in a file on ANY computer system or handheld devices without encryption; suggested widely used devices that supports encryption are: Apple, Android and Microsoft. If an account or password is suspected to have been compromised, report the incident to the IT Department and change all or domain password.

C. Application Development

Application developers must ensure their programs contain the following security precautions:

* Support authentication of individual users, not groups.
* Do not transmit or store passwords in clear text or in any easily reversible form.
* Ensure role management that allows one user to take over the functions of another without having to know the other's password.

# Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# Distribution

This policy is to be distributed to all Staff members with access to Company’s Information Resources.