PASSWORD POLICY

Team 00



Security Policies

StormSurge Software

**Password Policy**

1. OVERVIEW

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of <Company Name>'s resources. All users, including contractors and vendors with access to <Company Name>'s Team systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1. 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.

1. 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 <Company Name>'s facility, has access to the <Company Name>'s network, or stores any non-public <Company Name>'s information.

1. POLICY
   1. Password Creation
      1. All user-level and system -level passwords must conform to the Password Construction Guidelines
      2. Users must not use the same password for <Company Name>'s accounts as for other non-<Company Name>'s access (for example, personal ISP account, option trading, benefits, and so on).
      3. Where possible, users must not use the same password for various <Company Name>'s access needs.
      4. User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.

* 1. Password Change
     1. All system-level passwords (for example, root, enable, NT admin, application

administration accounts, and so on) must be changed on at least a quarterly basis.

* + 1. All user-level passwords (for example, em ail, web, desktop computer, and so on) must be

changed at least every six months. The recommended change interval is every four months. 4.2.3

Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team and its delegates. If a password is guessed or cracked during one of these

scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

* 1. Password Protection
     1. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential

<Company Name>'s information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place.

* + 1. Passwords must not be inserted into email messages, Alliance cases or other forms of

electronic communication.

* + 1. Passwords must not be revealed over the phone to anyone.
    2. Do not reveal a password on questionnaires or security forms.
    3. Do not hint at the format of a password (for example, "my family name").
    4. Do not share <Company Name>'s passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
    5. Do not use the "Remember Password" feature of applications (for example, web

browsers).

4.3.9 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

* 1. Use of Passwords

A good password is relatively long and contains a combination of upper and lower case letters and numeric and punctuation characters.

4.4.1 Password Format Policy:

2 special characters, 1 upper case character, 1 lower case character.

10 character minimum

4.4.2 Password Security Rules:

lockout the user after 5 failed password attempts

maximum of 90 days before a users password must be changed

No password hints

All of the rules above that apply to passwords also apply to passphrases.

Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-Compliance

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