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 Gemporia's resources. All users, including contractors and vendors with access to Gemporia systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.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.

3.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 Gemporia facility, has access to the Gemporia network, or stores any non-public Gemporia information.

4.Policy

4.1.Password Creation

4.1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines.

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

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

4.1.4 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.

4.1.5 Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

4.2 Password Change

4.2.1 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.

4.2.2.All user-level passwords (for example, email, 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 or 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.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential Gemporia information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

4.3.2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.

4.3.3 Passwords must not be revealed over the phone to anyone.

4.3.4 Do not reveal a password on questionnaires or security forms.

4.3.5 Do not hint at the format of a password (for example, “my family name”).

4.3.6 Do not share Gemporia passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

4.3.7 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 devices (phone, tablet) without encryption.

4.3.8 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.

4.4 Application Development

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

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.4.3 Applications must not transmit passwords in clear text over the network.

4.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to “unlock” the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against “dictionary attacks.”

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

```
The*?#>*@TrafficOnThe101Was*&#!#ThisMorning
```

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

4.5 Implementation Guidlines

1. Passwords must be kept in an unreadable format (e.g. encrypted) whenever stored or transmitted
2. Initial passwords for each new user account and reset passwords shall be unique to that account
3. Passwords for new user accounts shall be changed at first login
4. Users shall change their passwords every 90 days
5. New passwords shall not be the same as the previous four passwords used
6. Passwords shall be at least 7 characters long. Password lengths to highly privileged roles are recommended set a minimum of 15 characters
7. Passwords shall contain at least one character from at least three of the following groups[1)]
    - Alphabetic lower case (abcdefghijklmnopqrstuvwxyz)
    - Alphabetic upper case (ABCDEFGHIJKLMNOPQRSTUVWXYZ)
    - Numeric (0123456789)
    - Special Characters (`¬¦!“£$%^&*()_+-={}~@:<>?-=[]#';,./\|)
8. Default passwords shall be changed before a new system is brought into production
9. Passwords for special accounts (e.g. administrative accounts) shall be stored in a secure location for retrieval in case of emergency
10. Accounts shall time out or sessions terminate after 15 minutes of inactivity
11. A user’s account shall lock out following five failed login attempts
12. Locked out accounts shall remain locked for 30 minutes, or until unlocked by an administrator
13. Users who have forgotten their passwords shall verify their identity before their password is reset -

5.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.

6.Related Standards, Policies and Processes

See Password Construction Guidelines for further details

For implementing in Amber see Generate Password

7.Definitions and Terms

The following definition and terms can be found in the SANS Glossary located:

Here

- Simple Network Management Protocol (SNMP)

8.Revision History

Date of Change	Responsible	Summary of Change
December 2015	Andrew Smith	Initial document
15th June 2016	Andrew Smith	Review - no change
24th October 2016	Andrew Smith	Replaced TGGC with Gemporia
1st November 2016	Andrew Smith	Renamed document from `Password Protection Policy` to `Password Policy`
3rd November 2016	Andrew Smith	Clarified password requirement from different character sets

[1] for practical reasons it is acceptable to remove similar looking symbols, e.g. `l` and `I`