Password Guidelines for Systems Administrators

Document Information

Version Number	1.0
Last Update	12/12/2022
Author	Matthew Coutts
File Name	Password Guidelines for Systems Administrators
Document Title	Password Guidelines for Systems Administrators
Document Owner (Role Position)	Global Head of Enterprise Technology, Risk and Cyber Security
Responsible Executive (Role Position)	Chief Technology Officer

Document Revision History

Version	Issue Date	Author	Comments	Approved By
1.0	12/12/2022	Matthew Coutts		Matthew Coutts

Document Approval and Authorisation by Senior Management

Version	Issued Date	Date Last Reviewed	Approver
1.0	12/12/2022	12/12/2022	Matthew Coutts

1.0 Introduction

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of TEG's enterprise network. As such, all TEG staff (including contractors and vendors with access to TEG systems) with System Administrator account(s) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. System Administrators at TEG include members of any/all Windows Domain Administrators group or local administrators group, and/or users with root level access on UNIX devices. These password settings and procedures are designed to meet or exceed standards outlined in the NIST800-63 Electronic Authentication Guideline document.

- NIST800-63 Electronic Authentication Guideline document
- IT Security Checklists and Implementation Guides from the National Institute of Standards and Technology
- Security Configuration Guides from the National Security Agency
- Shibboleth Installation Guide

2.0 Purpose

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

3.0 Policy Statements

3.1 General Guidelines

All system-level passwords (e.g., root, enable, domain admin, application administration accounts, etc.) must be changed at least every 90-days. All production Service accounts must use the same specifications as domain administration accounts for their passwords. Passwords must not be inserted into email messages or other forms of electronic communication. Where 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. A keyed hash must be used where available (e.g., SNMPv3). All domain administration-level and system-level passwords must conform to the guidelines described below.

3.2 Guidelines

3.2.1 General Password Construction Guidelines

Passwords are used for various purposes at TEG. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain both upper- and lower-case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least 12 alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
- Poor, weak passwords have the following characteristics:
    - The password contains less than eight characters.
    - The password is a word found in a dictionary (English or foreign)
    - The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

NOTE: Do not use any of these examples as passwords

3.2.2 Password Protection Standards

Do not use the same password for TEG accounts as for other non-TEG access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various TEG access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for a Windows account and a UNIX account.

Do not share TEG passwords with anyone. All passwords are to be treated as sensitive, confidential TEG information.

Here is a list of dont's:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- Don't use the "Remember Password" feature of applications.
- If someone demands a password, refer them to this document or have them call someone in the Enterprise Technology Cyber Security area.

- Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including mobile devices) without encryption.
- Change passwords at least once every 60 days.
- If an account or password is suspected to be compromised, report the incident to the Enterprise Technology team IMMEDIATELY.
- Password cracking or guessing may be performed on a periodic or random basis by Information Security or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

3.2.3 Application Development Standards

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

Applications:

1. should support authentication of individual users, not groups.
2. should not store passwords in clear text or in any easily reversible form.
3. should 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. should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible. (Definition Section 5.0)

3.2.4 Use of Passwords and Passphrases for Remote Access Users

Access to the TEG Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

3.2.5 Passphrase

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

4.0 Enforcement

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

5.0 Definitions

Application Administration Account: Any account that is for the administration of an application (e.g., Oracle database administrator, Active Directory administrator).

TACACS+: Terminal Access Controller Access Control System

RADIUS: Remote Authentication Dial In User Service

X.509: Standard for public key infrastructure

LDAP: Lightweight Directory Access Protocol

Status and Details

Status	Current
Effective Date	1 October 2022
Review Date	15 October 2022
Approval Authority	Global Head of Enterprise Technology, Risk and Cyber Security
Approval Date	15 October 2022
Expiry Date	Not Applicable
Responsible Executive	Chief Technology Officer
Enquiries Contact	Enterprise Technology Team