GUAM POWER AUTHORITY STANDARD OPERATING PROCEDURE	Prepared/Revised by: Rudolph Manibusan / 6-10-2022 Signature / Print Title:
TITLE: Password Creation and Protection Policy	Reviewed by: / 6/11/2022 Signature / Print **Chief Information Technology Officer**
NO: 163 Supersedes: SOP-163 Dated: 05/07/18	Concurred by: / 6/13/2022 Signature / Print **Assistant General Manager, Engineering & Technical Services**
Page 1 of 5	Approved: / 6/17/22 **John M. Benavente (P.E) General Manager** / Date

1.0 OVERVIEW & PURPOSE

This guideline applies to all users which includes: employees, contractors, and consultants, temporary and other workers at Guam power Authority (GPA, # Authority), including all personnel affiliated with third parties both that log-in to GPA Network Infrastructure either on-site and/or off-site (remote access). The purpose of this standard operating procedure is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change.

 # All users are responsible for the safeguard of their system access login and password credentials and must comply with the standards identified in this policy.

Password are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of GPA's resources. All users, with access to GPA's systems, are responsible for taking the appropriate steps, as outlines in this policy, to select and secure their passwords.

2.0 SCOPE

The scope of this standard operating procedure includes all users who have or are responsible for an account (or any form of access that supports or requires a password) on any of GPA owned system that resides at any GPA facility, has access to GPA's network, or stores any nonpublic GPA information.

3.0 RESPONSIBILITY

The Information Security section within the Information Technology (IT) Division is responsible for implementing, monitoring, and ensuring compliance with this policy.

4.0 POLICY

4.1 # Account Security Controls

4.1.1 # Account Lockout Threshold: 3 invalid logon attempts lockout a user account.

4.1.2 # Account Lockout Duration: Amount of time an account remains locked out. Locked accounts will remain locked out until an authorized IT Support staff unlocks the account or resets user password.

4.1.3 # Reset Account Lockout Counter After: Locked out account requires an IT Support staff to unlock the account

4.1.4 # Password History: 24 passwords. Number of unique new passwords used by a user before an old password can be reused again.

4.2 Password Creation

4.2.1 All user-level and system level passwords must conform to the Password Construction Guidelines (see Section 5.0)

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

4.2.3 Where possible, users must not use the same password for various GPA access accounts.

4.2.4 User accounts that have system level privileges granted through group members, programs or operating systems must have a unique password from all other accounts held by that user to access systems level privileges.

4.3 Password Protection

4.3.1 Passwords shall not be shared with anyone. All passwords shall be treated as sensitive, confidential GPA information.

4.3.2 Passwords shall not be written down or inserted into an email message or other forms of electronic communication.

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

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

4.3.5 Do not share GPA passwords with anyone, including administrative assistants, secretaries, managers, co-workers, consultants, contractors and family members.

4.3.6 Do not write passwords down and store them anywhere in your office.

4.3.7 Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

4.3.8 Do not use "Remember Password" feature of applications (for example, "Web browsers").

4.3.9 Any user suspecting that his/her passwords may have been compromised must immediately report the incident to the IT Information Security section and change all passwords immediately.

5.0 PASSWORD CONSTRUCTION GUIDELINES

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 GPA's computer systems, data, or the network infrastructure. This guideline provides best practices for creating * complexed and secured passwords.

The following guideline applies to all passwords including, but not limited to user-level accounts, system-level accounts, web accounts, email accounts, screen saver protection, voicemail, and local router logins.

5.1 Password Creation

5.1.1 All passwords ***** must be complexed and must meet or exceed the following characteristics and guidelines.

5.1.1.1 ***** Minimal of 8 characters and maximum of at least 64 characters

5.1.1.2 Contain both upper and lower case letters

5.1.1.3 Contain at least one number (for example, 0-9)

5.1.1.4 Contain at least one special character (for example, !@#$%^&*()_-+={[}]:;"'<>,.?/).

5.1.2 Poor or weak passwords:

5.1.2.1 Contains personal information such as: birthdays, addresses, phone numbers, or names of family members, pets, friends and or fantasy characters

5.1.2.2 Contains work-related information such as building names, system commands, sites *(locations), companies, hardware and or software

5.1.2.3 * Can be found in dictionaries, including foreign language, or exists in a language slang, dialect or jargon

5.1.2.4 # Do not use common passwords such as: Password1, Pa$$w0rd1, Password1$, Superman1!, PaSSword!, Power!23, Password!23, weLCome12@, Admin!23, Admin12$, ChangeMe!23, ***** or similar versions

5.1.2.5 # Do not write down a password and store password.

5.1.3 A strong, # complexed password is one that's either not commonly used or not easily compromised. To test how strong your password is, you may visit the site:

https://www.my1login.com/resources/password-strength-test

This # web link is a password strength meter that checks the strength of a password or passphrase. It uses common password dictionaries, common dictionaries first name dictionaries and last name dictionaries and other reference materials for comparison.

5.2 Use of Password and Passphrases

A passphrase is similar to a password in use, however, it is relatively long and constructed with multiple words. It is a longer version of a password and is therefore, provides greater security against "dictionary attacks".

 # Dictionary Attack: An attempted illegal entry to a computer system that uses a dictionary headword list to generate possible passwords.

*****A passphrase is a string of words that is used to gain access to a computer system or services, example: MyDogHasFleas = MyD0gH@5F!3Az, ***** GuamIsHot = Gu@M!zh0T

5.3 Create Passwords Easily Remembered

Create passwords that you can remember easily.

One way to do this is to create a password based on a song title, affirmation, or other phrases. For example, the phrase; "This May Be One Way To Remember" = "TsmB1wy2Rmr! Or "Smoke On The Water" = Sm0koNDW@t3R as another variation.

6.0 STANDARD OPERATING PREOCEDURE COMPLIANCE

6.1 Compliance Measurement

It is the user's responsibility to ensure that he/he follows this policy with best practice recommendations and guidelines with the highest of professional conduct and ethical standards.

6.2 Exceptions

Any exception to this policy must be approved in writing by the IT Division's Chief Information Technology Officer (CITO) or designee in advance.

6.3 Non-Compliance

An individual found to have violated this policy shall be subject to progressive disciplinary action as outlined in GPA's Code of Conduct or dismissal depending on the severity and/or adverse effect(s) of the infraction on GPA's Operations and Security.

6.4 Severity is determined by the IT Division under the CITO, Assistant General Manager, Engineering and Technical Services (AGMETS), and approved by the Cybersecurity Steering Committee with the concurrence of the General Manager.