
 GUAM WATERWORKS AUTHORITY	STANDARD OPERATING PROCEDURE	No.	SOP-1200-IT-001
	Password Creation & Protection	Effective Date	12/10/2019
		Final Approver	 Miguel C. Bordallo, P.E. General Manager
		Revision Letter	A

1.0 Purpose

This guideline applies to all computer and system users within Guam Waterworks Authority (GWA or Authority). The purpose of this policy is to establish acceptable standards for creation of strong passwords, the protection of those passwords, and the frequency of change. Passwords are an important aspect of computer security. Poor password management or construction may result in unauthorized access and/or exploitation of GWA’s resources. All users, with access to GWA’s systems, are responsible for taking the appropriate steps, as outlined in this policy, to select and secure their passwords.

This is one of GWA’s cybersecurity policies, which informs all users of their responsibilities for the use and protection of technology and information assets. This policy represents the commitment of the Authority to ensuring that system and information integrity policy is appropriately defined and implemented, in order to protect GWA’s assets, systems and data from intentional or unintentional acts that may negatively impact business operations.

2.0 Scope

This policy applies to:

- 2.1. Passwords for user accounts.
- 2.2. Users authenticating access to these accounts.
- 2.3. Users that manage or design systems requiring passwords to access GWA owned or leased systems and applications.

3.0 Policy

Computing accounts shall be protected by strong passwords. Users shall protect the security of those passwords by managing passwords in a responsible fashion. System developers shall develop systems that store or transmit password data responsibly and that use secure authentication and authorization methods to control access to accounts.

4.0 Definitions

- 4.1. **Devices** – Server, Desktop Computer, laptop, tablet, thin client, phone instrument including smart phone, removable storage and any hardware that a User operates to interact with GWA applications and data. This Standard Operating Procedures does not cover peripheral devices such as keyboard and mouse.
- 4.2. **IT Department** – Personnel assigned to the GWA Information Technology (IT) department.

Password Creation & Protection

4.3. **Network Infrastructure** – The distributed hardware and software resources (i.e., cabling, routers, switches, wireless access points, access methods, and protocols), information, and integrating components that allow connectivity, communication, operations and management of an enterprise network.

4.4. **Users** – Are all employees, board members, contractors, consultants, vendors, temporary workers, volunteers, third party, and other persons in a position to know or access information or devices on GWA network.

5.0 Roles and Responsibilities

5.1.	General Manager	Approve all changes in this SOP. Manage and control the overall operations and all properties of GWA.
5.2.	Assistant General Manager of Administration and Support	Oversee development, revision and implementation of this SOP as the Policy Owner. Represent IT Department in the SOP Committee.
5.3.	Information Technology Manager (ITM) and IT Department	Provide oversight and guidance in complying with GWA IT cybersecurity policy (effective date 07/28/2017). Implement IT Standard Operating Procedures and monitor GWA IT systems to ensure compliance thereto. Monitor GWA systems to ensure compliance with regulatory requirements and standards. ITM Represent IT Department in the SOP Subcommittee.
5.4.	Information Security Administrator	Monitor and ensure compliance with this SOP. Provide training for new employees and annual refresher training for existing employees about the requirements of this SOP.
5.5.	Human Resources	Present each new employee, contractor or vendor with the existing GWA IT policies and procedures, upon the first day of commencing work with GWA.

Password Creation & Protection

5.6.	Managers and Supervisors	Ensure that users are informed of appropriate uses of GWA equipment and information technology resources through cybersecurity training and compliance with SOP-1200-IT-004, Acceptable Use of Information Technology (Computer, Software, License, E-mail, Internet, and Standards of Conduct).
5.7.	Users	To know this SOP and to conduct their activities accordingly. When GWA computer and system users are confronted by a situation not covered by this SOP or they do not clearly apply to a situation, users are encouraged to clarify with their respective supervisor or the IT Department.

6.0 Procedure Description

6.1. PASSWORD CREATION

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 GWA's computer systems, data, or the network infrastructure. This guideline provides best practices for creating secure passwords.

6.1.1. **Guideline in creating a password.** The following guideline applies to all passwords including, but not limited to, user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

Passwords should include:

- 6.1.1.1. At least eight (8) alphanumeric characters.
- 6.1.1.2. Both upper and lower-case letters.
- 6.1.1.3. At least one (1) number (for example, 0-9).
- 6.1.1.4. At least one (1) special character (for example, @\$%^&*()_+|~-=\`{}[]:~<>?,/).

Passwords should never:

- 6.1.1.5. Contain less than eight (8) characters.
- 6.1.1.6. Be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.

Password Creation & Protection

- 6.1.1.7. Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- 6.1.1.8. Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- 6.1.1.9. Contain number or letter patterns such as 111111, 123456, 123321, aaabbb, qwerty, zyxwvuts.
- 6.1.1.10. Contain common passwords (for example, Password, Pa\$\$w0rd, & Superman).
- 6.1.1.11. Contain common words spelled backward or preceded or followed by a number (for example, terces, secret1 or 1secret, drowssap1 & PaSSword1)).
- 6.1.1.12. Contain any version of "Welcome123", "Password123" or "Changeme123".
- 6.1.2. **No same password for GWA and non-GWA accounts.** Users must avoid using the same password for GWA and other non-GWA accounts (for example, personal email, Facebook, Instagram or other online accounts).
- 6.1.3. **No same password for various GWA access accounts.** Where possible, users must not use the same password for various GWA access accounts.
- 6.1.4. **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 phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or "Smoke On The Water" could become the password Sm0koNDW@t3R as another variation.
- 6.1.5. **Constructing a password using a passphrase.** It is an acceptable and effective way to remember a strong password. It is a longer version of a password and is, therefore, more secure that provides greater security against "dictionary attacks." A passphrase is typically composed of multiple words.

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters: (for example, MyDogHasFleas = MyD0gH@sF!eAz).
- 6.1.6. **Unique password for accounts for users with system-level privileges.** Accounts for users with system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access system-level privileges. Users that manage or design systems are typically granted accounts with system-level privileges.
- 6.1.7. **Test of password strength.** A strong password is not easily guessed and not easily deduced by a computer program brute force attack. To test how strong your password is, you may visit the my1login website at

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

This website uses a computer program to test the strength of a password by comparing it to common password dictionaries, regular dictionaries, first name and last name dictionaries as well as other commonly used algorithms.

6.2. PASSWORD CHANGE

- 6.2.1. **90-day rule for system-level passwords.** All system-level passwords (for example, root, enable, admin, application administration accounts, and so on) must be changed every ninety (90) days.
- 6.2.2. **90-day rule for user-level passwords.** All user-level passwords (for example, email, web, desktop/laptop computer, and tablet) must be changed every ninety (90) days.
- 6.2.3. **Password penetration test.** The IT Department Information Security Team or its delegates shall conduct planned penetration testing for the use of weak passwords. If a password fails a penetration test, the user will be required to change it immediately to conform with the Password Construction Guidelines.

6.3. PASSWORD PROTECTION

- 6.3.1. Passwords must never be shared with anyone. All passwords are to be treated as sensitive, confidential GWA information.
- 6.3.2. Passwords must never be written down or inserted into email messages or other forms of electronic communication.
- 6.3.3. Never reveal a password on questionnaires or security forms.
- 6.3.4. Never hint at the format of a password (for example, "my family name").
- 6.3.5. Never share GWA passwords with anyone, including administrative assistants, secretaries, managers, co-workers, consultants, contractors, and family members.
- 6.3.6. Never write passwords down and store them anywhere in your office that is unsecured or store passwords in a file on a computer system or mobile device (i.e., phone or tablet) without encryption.
- 6.3.7. Never use "Remember Password" feature of applications (for example, "Web browsers").
- 6.3.8. If a User suspects that his/her password has been compromised in any way, they must immediately report the incident to the IT Department Information Security Team and reset their password(s).
- 6.3.9. System administrators shall not use default user ID and passwords for administrative accounts.

6.4. ACCOUNT LOCKOUT

A user account will lockout after five (5) invalid password attempts in fifteen (15) minutes. Accounts will remain locked for a duration of thirty (30) minutes, unless the IT Help Desk is contacted, and the user's identity is verified for the account to be unlocked sooner.

6.5. STANDARD OPERATING PROCEDURE COMPLIANCE

- 6.5.1. **Compliance Measurement.** The IT Department Information Security team shall verify compliance with this policy through various monitoring and audit methods/tools. Practicable measures shall be put in place to log successful and failed system login attempts. Users are expected to report suspected violations of this policy to the Information Technology Division; their supervisor or manager; or the Internal Audit Office.
- 6.5.2. **Exceptions.** Any exception to the policy must be approved, in writing, by the IT Department, Information Technology Manager in advance.
- 6.5.3. **Non-Compliance.** Any user violating this policy may be subject to progressive disciplinary action ranging from a verbal warning, dismissal or as outlined in GWA Codes of Conduct depending on the severity and/or adverse effect(s) of the infraction(s) on the Authorities' operation and security.

7.0 Document Approvals

Role	Position	Name of Approver	Approval Signature	Date Approved
Author		GPWA IT departments	Approval on File	12/03/2019
Policy Owner	Assistant General Manager for Administration and Support	Christopher M. Budasi	Approval on File	12/03/2019
Final Approver	General Manager	Miguel C. Bordallo, P.E.	Page 1	12/10/2019

8.0 Records of Revisions

All suggestions for improvement shall be directed to the Policy Owner indicated below. The Policy Owner will consider input received, develop recommendations on how to address the suggestions, and obtain authorization to make the recommended changes. Updates, revisions, corrections and waivers to this SOP shall be made in writing and be approved by the GM.

8.1. Policy Owner: Assistant General Manager for Administration and Support

8.2. Authorization: General Manager

Effective Date	Revision Letter	Document Author	Description of Change
12/10/2019	A	GPWA IT departments	Initial Release of Policy/Procedure

9.0 References

- 9.1. GPA Password Creation and Protection Policy 7.09.18
- 9.2. GPA SOP-163 – Password Policy and Creation Policy
- 9.3. Notes provided by AGM for Administration & Support
- 9.4. CCU Resolution on Cybersecurity Policies and Procedures:
 - GPA Resolution No. 2018-14
 - GWA Resolution No. 38-FY2018