PASSWORD POLICY

POLICY# OTECH-POL2021-005

FRANK L.G. LUJAN, JR.
OFFICE OF TECHNOLOGY, GOVERNMENT OF GUAM
Otech.guam.gov

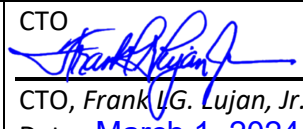
OFFICE OF TECHNOLOGY
GOVERNMENT OF GUAM

SEPTEMBER 6, 2021

Overview

Policy Number:	OTECH-POL2021-005
Title:	Password Policy
Purpose:	To establish adequate controls relating to password requirements of Government of Guam Information Technology (IT) systems.
Authority:	5 GCA Chapter 1 Article 12.106 (e)
Publication Date:	September 6, 2021
Policy Approval:	Frank LG Lujan, Jr Chief Technology Officer
Target Audience:	All OTECH employees, contractors, vendors and third parties. The intended recipients of this policy also include all entities under the authority of the Office of Technology, pursuant to the provisions of Public Law 34-076.
Contact Details:	**Office of Technology** 211 Aspinall Avenue PO Box 884 Hagåtña, Guam 96910 O: 671.635.4500 F: 671.472.9508 https://otech.guam.gov

Revision History

Date of Change	Responsible	Summary of Change
February 2018	OTECH Systems Support	Draft policy
September 2021	OTECH Systems Support	Update policy
September 2021	OTECH CTO and Data Processing Manager	Review, approve and disseminate policy
February 2024	OTECH Systems Support	(a) Add Review & internal audit section
March 2024	CTO  CTO, *Frank G. Lujan, Jr.* Date: March 1, 2024	Review, approve policy updates for dissemination

Introduction

One of the many critical measures of system protection for Government of Guam (GovGuam) Information Systems, users and applications is password-based authentication. This document is intended to provide rules governing the structure and content of the password.

1.0 Policy

The Office of Technology recognizes that passwords are critical to the overall security of systems. It is essential that password guidelines and standards are implemented to ensure security and overall protection of all GovGuam IT systems and devices.

The following guidelines shall be applied:

1.1 Information Systems that Process and Store Sensitive Information.

For the purpose of this document, Sensitive Information pertains to Personally Identifiable Information (PII), Social Security Administration (SSA) provided data, sensitive patient health information protected under HIPPA and Federal Tax Information (FTI).

1.1.1 Password Requirements

The information system must, for password-based authentication:

a. Enforce minimum password complexity of:
    1. Eight characters
    2. At least one numeric and at least one special character
    3. Storing and transmitting only encrypted representations of passwords
b. Enforce password minimum lifetime restriction of one day
c. Enforce non-privileged account passwords to be changed at least every 90 days
d. Enforce privileged account passwords to be changed at least every 60 days
e. Prohibit password reuse for 24 generations
f. Allow the use of a temporary password for system logon requiring an immediate change to a permanent password
g. User profile will be disabled after 3 failed login attempts.

1.1.2 System Use Notification Requirements

The information system must:

a. Before granting access to the system, display to users a warning banner that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
    1. The system contains U.S. Government information
    2. Users actions are monitored and audited
    3. Unauthorized use of the system is prohibited
    4. Unauthorized use of the system is subject to criminal and civil sanctions

The warning banner must be applied at the application, database, operating system, and network device levels.

b. Retain the warning banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

Sample of an Acceptable Warning Banner:

WARNING! BY ACCESSING AND USING THIS GOVERNMENT COMPUTER SYSTEM, YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION AND PENALTIES.

1.2 Other GovGuam Information Systems

GovGuam Information Systems that do not process or store sensitive information shall follow the following guidelines.

1.2.1 Password Requirements

a. Password must be at least 7 characters long, must contain at least 1 capital and 1 lower case letter, and at least 1 number and/or special character(!, @, #, $, etc.)
b. User will need to change their password with their first login.
c. Standard User Passwords will expire every 90 days.
d. User profile will be disabled after 10 failed login attempts.

Procedures

All GovGuam information systems and applications utilizing password-based authentication shall adhere to the minimum rules documented in this policy and system settings shall be established to enforce these rules.

Policy Compliance

Compliance Measurement

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

Exceptions

Any exception to this policy must be approved by the Chief Technology Officer (CTO) in advance and have a written record.

The exception request must document:

- The name of Government of Guam Agency funding application
- The name of the application
    - If applicable, name of vendor and contract details
- Description of application's purpose and function
- Data classification category of application

- The nature of non-compliance
- Why an exception is required
- Assessment of the potential risk posed by non-compliance, i.e., if the exception isgranted
- Plan for managing or mitigating those risks
- Anticipated length of non-compliance
- Any additional information as needed, including any specific conditions or requirements for approval

Non-Compliance

Any Government of Guam application found to have violated this policy may be subject to delays in service until such vulnerabilities are properly assessed and addressed. Responsible parties may be subject to disciplinary action.

Any employee found to have violated this policy may be subject to disciplinary action.

Review and Internal Audit

This policy shall be reviewed and updated annually, on an as needed basis, or if there is a breach in protocol and procedures. OTECH shall initiate the review process on the first day of each Fiscal Year – 1st of October, or next business day. Policy review and updates shall be documented in the policy's Revision History section. The review process shall be completed before the end of the Fiscal Year's first quarter and the updated policy shall be disseminated (via OTECH website, Agency Memo or email) by December 31 of each year.