UNIVERSITY OF GUAM
UNIBETSEDÅT GUÅHAN

OFFICE OF INFORMATION TECHNOLOGY
Information Security Office

University of Guam Multi-Factor Authentication (MFA) Policy

Introduction

Multi-Factor Authentication (MFA) adds a second layer of verification, beyond just passwords, to better protect UOG systems and data. This aligns with UOG's commitment to secure, reliable technology services and mitigates risks associated with compromised credentials.

Scope

This policy applies to all UOG faculty, staff, students, third-party contractors, and affiliates who access university systems that:

- Host sensitive and/or university-controlled data (student records, finance, HR, email, LMS, etc.), or
- Are classified as Moderate or High risk as per the data classification and handling policy

Policy Statement

MFA Requirement: The university shall enforce MFA on all relevant systems.

Approved Authentication Factors: Acceptable MFA factors include:

- Something you know: password or PIN
- Something you have: smartphone authenticator apps (Microsoft Authenticator, Google Authenticator, Authy) hardware tokens, OTP
- Something you are: biometric methods (where supported)

Enrollment and Implementation

- Enrollment in MFA is mandatory before access to covered systems
- Users may self-enroll following OIT documentation

Exceptions

- Exceptions require formal, documented approval from the Information Security Office and must include a risk assessment

Training and Support: OIT will offer step-by-step guidance and optional training sessions.

Technical support for MFA reset and troubleshooting is available via Help Desk or helpdesk@triton.uog.edu.

Roles & Responsibilities

- CIO - Authorizes and oversees MFA policy implementation
- Information Security Office (ISO) - Defines MFA standards, coordinates rollout, approves exceptions
- OIT - Manages MFA systems, documentation, training, support
- System Owners - Ensure MFA enforcement on managed systems
- End Users - Enroll in MFA, manage authentication devices responsibly

Compliance and Enforcement

Non-compliance may result in system access suspension.

Definitions

MFA: Authentication requiring two or more distinct factors (knowledge, possession, or inherence).

Sensitive Data: Data whose unauthorized disclosure may negatively impact individuals or the university.