UNIVERSITY OF GUAM
UNIBETSEDÅT GUÅHAN
Board of Regents

Resolution No. 26-02

RELATIVE TO ADOPTING THE UNIVERSITY OF GUAM'S INFORMATION TECHNOLOGY CYBERSECURITY POLICIES AND WRITTEN INFORMATION SECURITY PROGRAM

WHEREAS, the University of Guam (UOG) is the primary U.S. Land Grant and Sea Grant institution accredited by the Western Association of Schools and Colleges Senior College and University Commission serving the post-secondary needs of the people of Guam and the Western Pacific region;

WHEREAS, UOG governance and well-being are vested in the Board of Regents (BOR);

WHEREAS, the University has been undergoing a review of its Rules, Regulations and Procedures Manual (RRPM), which is being changed to the University Policy Manual (UPM), and in line with that review, the University Information Technology (IT) Cybersecurity Policies and written Information Security Program (ISP) attached were reviewed and revised;

WHEREAS, the University has determined that the revisions to the IT policies and ISP should go into effect immediately and not wait for the full UPM to be approved;

WHEREAS, the revised IT policies and written ISP have been through the University's shared governance process and are now being brought to the BOR for review and approval; and

WHEREAS, the President and the Physical Facilities Committee have reviewed and recommend the revised IT policies and ISP attached to the BOR for approval.

NOW, THEREFORE, BE IT RESOLVED, that the BOR hereby adopts the revised UOG IT policies and ISP to be effective immediately.

Adopted this 14th day of January, 2026

Agapito "Pete" A. Diaz, Chairperson

ATTESTED:

Anita Borja Enriquez, D.B.A., Executive Secretary

University of Guam Incident Response Policy

Purpose

The purpose of this policy is to establish a structured and effective approach for identifying, managing, and resolving cybersecurity incidents that may impact the University of Guam's information systems, data assets, and operational integrity. This policy supports the university's commitment to safeguarding institutional resources and ensuring continuity of academic, administrative, and research functions.

Scope

This policy applies to all University of Guam faculty, staff, students, contractors, and third-party affiliates who access or manage university-owned systems, networks, or data. It encompasses incidents affecting on-premises infrastructure, cloud services, and mobile or remote environments.

Policy Statement

The University of Guam shall maintain a formal incident response capability under the Office of Information Technology (OIT) to detect, analyze, contain, and recover from cybersecurity incidents in a timely and coordinated manner. All confirmed incidents must be reported immediately to OIT through designated channels.

Incident Categories

Incidents may include, but are not limited to:

- Unauthorized access to systems or data
- Malware infections or ransomware attacks
- Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks
- Data breaches or data loss
- Misuse of university resources or violations of the responsible use policy
- Physical theft or loss of devices containing sensitive information

The severity of each incident shall be evaluated in accordance with the University's Data Classification Policy, which defines the sensitivity and criticality of affected information assets.

Response Procedures

OIT shall follow a standardized incident response lifecycle consisting of the following phases:

- Phase 1: Planning
  1. Preparation: Ensure that users are aware of their responsibilities in the incident response lifecycle
  2. Prevention: Ensure proper safety controls are implemented to safeguard system
- Phase 2: Incident Handling
  3. Detection: Detect an incident through monitoring tools, user reports, or automated alerts.
  4. Analysis: Assess what has been affected and the scope
  5. Containment and Eradication– Isolate affected systems to prevent further damage or spread.
  6. Recovery – Restore systems to normal operation and verify integrity of data and services.
  7. Post-Incident Activity – Document findings, assess root causes, and recommend improvements to prevent recurrence.

Roles and Responsibilities

- Office of Information Technology (OIT): Leads incident response efforts, maintains documentation, and coordinates with external agencies as needed.
- System Owners and Administrators: Assist in containment and recovery efforts, and ensure systems are patched and secured.
- University Personnel: Must report incidents promptly and cooperate with investigation procedures.

Reporting and Notification

All incidents must be reported to the OIT Information Security Office or designated security contact. In cases involving potential data breaches, OIT will coordinate with university leadership and legal counsel to determine notification obligations under applicable laws and regulations, including Guam Breach Notification Law (9 G.C.A. § 48.10–.80).

Compliance and Enforcement

Faculty, staff, and student employees who willfully and/or repeatedly violate this policy may face disciplinary action pursuant to the applicable administrative process. OIT shall maintain logs and records of all incidents for audit and compliance purposes.

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.

University of Guam Physical Security Policy

Purpose

The purpose of this policy is to establish physical security controls to protect University of Guam information systems, infrastructure, and data assets from unauthorized physical access, damage, or disruption. This policy supports the University's commitment to safeguarding institutional data and ensuring the confidentiality, integrity, and availability of its information resources.

Scope

This policy applies to all University-owned facilities, data centers, server rooms, and any location where University information systems or sensitive data are stored or accessed. It applies to all employees, contractors, vendors, and authorized third parties.

Policy Statement

The University of Guam shall implement and maintain reasonable physical safeguards to prevent unauthorized access to systems and data. These safeguards shall include, but are not limited to:

- **Access Control Measures**
  - Restricted access to server rooms, data centers, and telecommunications closets shall be enforced using keycard systems, biometric authentication, or physical locks.
  - Only authorized personnel shall be granted access to secure areas.
  - Visitor access shall be logged and escorted.

- **Device Protection**
  - Workstations, laptops, and mobile devices shall be physically secured when unattended when applicable.
  - Portable storage devices containing sensitive data shall be stored in locked containers or safes when not in use.

- **Incident Response**
    - Any physical breach or unauthorized access shall be reported immediately to the OIT Information Security Office and documented in accordance with the University's incident response procedures.

Compliance and Enforcement

Faculty, staff, and student employees who willfully and/or repeatedly violate this policy may face disciplinary action pursuant to the applicable administrative process. The office of Information Technology shall conduct periodic reviews and audits to ensure adherence to physical security standards.

University of Guam Security Awareness and Training Policy

Purpose:

Security awareness training equips UOG faculty, staff, students, contractors, and affiliates with the knowledge to recognize and prevent cyber threats, such as phishing, social engineering, ransomware, and other attacks, helping fulfill UOG's mission to provide secure, reliable IT services

Scope:

Applies to all individuals accessing UOG-managed systems, networks, or resources, including central and departmental systems, as part of their employment, academic endeavor, or affiliation

Definitions:

Security Awareness Training: Educational lessons designed to increase knowledge of cybersecurity risks and best practices.

Acknowledgment: A user's formal confirmation of understanding and commitment to comply.

Sensitive Data: Any data classified as Level 2 or higher under UOG Data Classification Standards

Policy:

Mandatory Training

- All employees must complete mandatory security awareness training upon initial system access and annually thereafter.
- Training content includes phishing recognition, safe handling of sensitive data, password management, MFA, and incident reporting

Training Delivery Methods

- Delivered through interactive online platforms (e.g., KnowBe4) and in-person/virtual workshops coordinated by ISO, for example, sessions like "Cybersecurity Awareness Training" and "MFA setup"
- Supplemental materials and periodic "tips" disseminated during Cybersecurity Awareness Month (October) via OIT channels

Recordkeeping & Reminders

- ISO/OIT shall log training completions in IT systems.
- Automated reminders will notify individuals prior to training deadlines.
- Non-compliance may result in system access restrictions.

Additional & Role-Based Training

- Certain roles (e.g., system admins, finance) may be required to complete specialized training modules.
- Training is updated to reflect emerging threats and technologies in collaboration with partners.

Compliance and Enforcement

Faculty, staff, and student employees who willfully and/or repeatedly violate this policy may face disciplinary action pursuant to the applicable administrative process. OIT shall maintain logs and records of all security awareness training results for audit and compliance purposes.

University of Guam System Change Management Policy And Procedure

Purpose:
Change Management seeks to ensure IT system changes are planned, communicated, coordinated, monitored, and documented to minimize risks, prevent disruptions, maintain compliance, and ensure IT services continuity.

Scope:
This policy applies to all staff and contractors involved in IT applications or system changes, updates, or patches both operational and project based.

Policy Statement
This policy ensures that all changes to IT infrastructure and Colleague ERP application are communicated, reviewed, and approved before implementation to prevent disruptions and conflicts.

Change Management Requirements:

- Users must be informed of upcoming changes affecting system availability or operations.
- Emergency changes or unplanned outages must be communicated immediately, with regular updates until resolution.
- Device configurations must be backed up before implementation.
- All changes, both scheduled and unscheduled, require a formal request via the UOG Colleague Change Approval Form

Policy Procedures

<u>UOG Colleague Change Approval Form</u>

1. Consult with Ellucian Colleague support to schedule the earliest available dates for updating the Test and Live environments, ensuring updates occur with minimal service disruptions.
2. Request system and workstation requirements documentation for the target version from Ellucian Colleague support. Assess current system and workstation settings and make necessary adjustments to meet the target version's requirements.
3. Schedule a meeting with Colleague super users to plan and schedule testing of the new version.
4. Request each involved department to complete testing and submit their signed section of the UOG Colleague Change Approval Form along with a testing document signed by their administrator.
5. Compile all submitted Testing Documents.

6. Request approval from the OIT CIO to proceed with the Live environment upgrade using the **UOG System Change Approval Form**
7. Notify all users of the scheduled Live environment upgrade or patch via a memo.
8. Upon completing the Live upgrade, request the OIT CIO to acknowledge completion by signing the SYSTEM Upgrade Approval Form for the Live Environment.

UNIVERSITY OF GUAM
UNIBETSEDÅT GUÅHAN

OFFICE OF INFORMATION TECHNOLOGY
Information Security Office

University of Guam System User Management Policy

Purpose:

This policy sets standards for administering computing accounts that grant access to the University of Guam's ERP Colleague System. It establishes guidelines for issuing, managing, and monitoring accounts to ensure the university's data security.

Scope:
All University of Guam employees (e.g., faculty, staff, student employees) and authorized users accessing the University's data resources.

Policy Statement:

This policy ensures the proper recording and maintenance of the **UOG Data Security Request Form**, which serves as documentation for requesting the creation, modification, or disabling of system accounts.

The following precautions serve as a guide for account management and provisioning.

- Unused accounts must be locked or disabled.
- User affiliation must be verified before account creation.
- Accounts are strictly for individual use—no sharing allowed.
- Access privileges must be limited to necessary functions as per users' daily tasks and duties.
- Account setup/modifications require a completed and signed **UOG Data Security Request Form**
- OIT must issue unique accounts and promptly deactivate them when no longer needed.
- User identity must be verified before account and password issuance.
- Passwords for new accounts should not be emailed unless encrypted.
- Department Heads must review accounts bi-annually to ensure appropriate access and privileges.
- Privileged account managers must sign a Confidentiality Agreement, stored with HR.
- Guest accounts must have an expiration date (max one year or upon work completion) and require sponsorship from an authorized administrator.

A completed and signed **UOG Data Security Request Form** is required to create, modify and disable a system account.

UOG Data Security Request Form Instructions

1. Complete the **UOG Data Security Request Form**
2. Obtain approval from your Department Head (e.g., Deans, Directors).
3. Obtain approval from the Data Approver/Overseer.
    - **For ST- Academic Student Records** – Associate Dean and Registrar, Arline E. Leon Guerrero, M.Ed.
    - **For Financial Aid** – Director of Financial Aid, Mark A. Duarte, MPA
    - **For CF – Finance / Payroll/ Bursar** – Business Office Comptroller, Abigail Martin or Associate Comptroller/Bursar, Elsa Flores
    - **For HR- Human Resource** - Chief Human Resources Officer, Joseph Gumataotao
    - **For Nuventive** - Vice Provost for Institutional Effectiveness, Marlena Pangelinan
4. Ensure all approvals are finalized.
5. Submit the completed form to the Office of Information Technology via the helpdesk (helpdesk.uog.edu) to process account requests.

Consequences:

Faculty, staff, and student employees violating this policy may face disciplinary action under the applicable administrative process. Violators may lose access to specified IT services.

UNIVERSITY OF GUAM
UNIBETSEDÅT GUÅHAN

OFFICE OF INFORMATION TECHNOLOGY
Information Security Office

UOG User Account Management Policy and Procedures
Office of Information Technology only

INSTRUCTIONS:

1. Access the UOG Helpdesk: https://helpdesk.uog.edu
2. Open the ticket requesting access to any of the following application: Colleague Uiwebs, Softdocs, Nuventive or Informer etc…
3. Verify if the user exists in the requested application. If new, verify all information required to be filled in and all proper approvals are completed.
4. Save the completed **UOG Data Security Request Form** in the NAS network drive in the Data Security Request folder using the following *FileName layout*:

   HD_ticket#_LASTNAME, FIRSTNAME_ UOG Applications Request

   Example: HD_31333_SMITH, JOHN_UOG Applications Request

NOTE: If in the future, the user submits another **UOG Data Security Request Form** for the same work location but requesting for additional access to the same application or requesting to be added in a new application, add the letter "_B" after the word "request "on the FileName.
Example: HD_31334_ SMITH, JOHN_UOG Applications Request_B

When a user transfers from one department to another, the department information will be updated to the new department. However, all roles assigned to them previously will be removed. A new **UOG Data Security Request Form** will need to be submitted reflecting their access request in the department.

University of Guam User Access Review Policy

Purpose:

To minimize security risks by regularly assessing and adjusting employee access levels to systems and data, ensuring only authorized individuals have access to information necessary for their role and function, reducing the potential for data breaches from unauthorized access or insider threats.

Scope:

This policy applies to all University of Guam employees, student employees, interns, vendors, and contractors with access to the University's ERP Colleague System. Department heads, deans, and directors are responsible for reviewing and confirming or revoking access for their respective employees. This review process will be conducted twice a year to ensure appropriate access control.

Policy Statement:

This policy establishes the procedures for regularly reviewing and managing employee access levels to university systems and data. The goal is to ensure that access is appropriate, aligned with job responsibilities, and revoked when no longer needed, thereby maintaining data security and compliance.

Consequences:

Violations of this policy may result in suspension of user access.

Access Review Procedures - Office of Information Technology

1. Create a memo regarding the UOG Colleague User Audit for the current Fiscal Year for the coming quarter.

2. The UOG Office of Information Technology shall perform user access review procedures for Colleague modules and security group via the UOG User Access Review Form. Report shall be saved in a secure folder.

3. Send the memo and the output files to the Deans and Directors for review, evaluation, and approval of their current UOG Colleague system users.

Access Review Verification - Department Directors/ College Deans

1. Evaluate and complete UOG User Access Review Form provided by the Office of Information Technology. Failure to submit a completed and signed User Access Review form to the Office of Information Technology may result in revoking access to specified IT services.

2. Access the UOG Helpdesk: helpdesk.uog.edu to process/respond to the UOG Colleague User Audit form tickets submitted by the departments.

UNIVERSITY OF GUAM
UNIBETSEDÅT GUÅHAN

OFFICE OF INFORMATION TECHNOLOGY
Information Security Office

UOG User Access Review Form

Please follow the instructions below:

1. Validate the current list of users and their access in the attached report. The columns list access to specific Colleague Applications.

2. To deactivate a user, place a strikethrough mark on the username Ex. ~~Username~~

3. To remove a user's specific access to a Colleague Application, place a strikethrough mark on the process. Ex. ~~REQM Requisition Maintenance~~

4. To add a new user(s) or add/modify access to a specific Colleague Application for a current user, complete a **UOG Data Security Request Form** and submit to OIT Helpdesk Link: **https://www.uog.edu/it/helpdesk-ticket.php**

5. No changes in the user listing, still requires the submission of a signed and dated UOG User Access Review form.

Applications:	**Example Process:**
ST – Student	RGN - Registration
CF- Finance	REQM - Requisitions
HR- Human Resources	POSD – Position Definition
UT	
CORE	

*****This form should ONLY be signed by the College Dean or Department Head*****

Department Head/ College Dean Signature: _____

Date: _____

University of Guam GLBA Written Information Security Program

1. Purpose

The Gramm-Leach-Bliley Act ("GLBA") (Public Law 106-102) and its implementing regulations at 16 CFR Part 313 & 314 requires Financial Institutions to protect, to the extent reasonably possible, the security, privacy, and confidentiality of personally identifiable financial records and information, also known as "Covered Information." Because the University of Guam ("University") engages in Financial Services, such as student financial aid, the Federal Trade Commission ("FTC") considers the University a Financial Institution for GLBA purposes.

This program establishes the University of Guam's commitment to protecting the security, confidentiality, and integrity of nonpublic financial information in compliance with the Gramm-Leach-Bliley Act (GLBA) and the FTC Safeguards Rule (16 CFR Part 314).

2. Scope

This policy applies to all University departments and personnel who access, process, store, or transmit Covered Information, including but not limited to:

- Financial Aid Office

- Bursar's Office

- Office of Information Technology (OIT)

- Third-party service providers

3. Definitions

Covered Information: Nonpublic personal financial information obtained in connection with providing a financial product or service.

Customer Information: Information about students or others who receive financial services from the University.

Qualified Individual: The designated person responsible for implementing and overseeing the Information Security Program (ISP).

Service Provider: Any third party with access to Covered Information through a contractual relationship with the University.

4. Governance

The Chief Information Officer (CIO) is designated as the Qualified Individual responsible for the ISP. The CIO may delegate responsibilities to appropriate personnel within OIT, other departments, and/or a contracted virtual Chief Information Security Officer (VCISO).

5. Program Elements

5.1 Risk Assessment

UOG intends, as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information.

The University will:

- Identify internal and external risks to Covered Information
- Assess the effectiveness of current safeguards
- Evaluate risks in areas including:
    - Employee training and management
    - Information systems and data lifecycle
    - Incident detection and response

5.2 Safeguards Implementation

- Implement and periodically review access controls such as Role-based access to systems containing Covered Information.

- Asset inventory - Know what you have and where you have it.

- Encryption: Encrypt data at rest and in transit.

- Multi-Factor Authentication (MFA): Required for all systems accessing Covered Information.

- Secure Disposal: Procedures for securely disposing of paper and electronic records.

- System Monitoring: Logging and monitoring of user activity and system access.

5.3 Employee Training

Annual training for all employees with access to Covered Information, including data handling, phishing awareness, and incident reporting.

5.4 Oversight of Service Providers

- Contracts must require service providers to implement appropriate safeguards.

- The Office of Procurement and Legal Affairs will ensure GLBA compliance in vendor agreements.

- Periodic reviews of vendor compliance will be conducted.

5.5 Incident Response

The University will maintain an incident response plan to detect, respond to, and recover from security incidents. All incidents involving Covered Information must be reported to the CIO and the Office of Information Technology – Information Security Section.

5.6 Program Review and Adjustment

The ISP will be reviewed annually or upon significant changes in operations or threats. Adjustments will be made based on risk assessments, audit findings, and regulatory updates.

6. Enforcement

- Any employee, contractor, or other third-party performing duties on behalf of the University with knowledge of an alleged violation of this Policy shall notify the Office of Information Technology as soon as practicable.
- Any employee, contractor, or other third-party performing duties on behalf of the University who willfully and/or repeatedly violates this Policy may have their access to University Information Resources suspended or revoked. Disciplinary actions for employees will follow the University's standard administrative processes and applicable policies. For contractors and third-party vendors, remedies will be enforced

in accordance with the terms and conditions of their contract, which may include termination of services or other contractual remedies.