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.