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 (2.10).
- 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.