Policy Title	Incident Response Policy
Responsible AIU Office (Higher Management/Directorate)	Chief Information Officer (CIO)
Policy Owner (Executive Department/Office)	~~Information Technology Department~~Information Technology Department Information Security Office (ISO)
Pertinent Dates	July 2022

I. SCOPE OF POLICY

The purpose of this policy is to clearly define IT roles and responsibilities for the investigation and response of computer security incidents and data breaches.
This policy applies to information systems, regardless of ownership or location, used to store, process, transmit or access AIU data as well as all personnel including employees, students, temporary workers, contractors, those employed by contracted entities and others authorized to access AIU enterprise assets and information resources.

This policy applies globally to anyone with access to AIU's information and information technology assets, including permanent, temporary or contracted employees, consultants, volunteers or third-party organizations irrespective of the time of day, means of access, or location of the person.

II. DEFINITIONS

Incident: An event, whether electronic, physical or social that adversely impacts the confidentiality, integrity or availability of AIU data or information systems; or a real or suspected action, inconsistent with AIU Privacy or Acceptable Use policies.
Data Breach: Unauthorized access, acquisition, use or disclosure of Restricted Data. Data breach notifications are subject to regulatory requirements following a privacy investigation and risk assessment.
Asset: An asset is any tangible or intangible thing or characteristic that has value to AIU. An asset (owned, leased or licensed) may include, but is not limited to, data in any form, hardware, software and application systems applicable to information systems.
Evidence: is Information that proves or disproves a stated event.
Incident Response: is a response to a disaster or other significant event that may significantly affect the enterprise its people, or its ability to function productively.

Formatted: Font: Not Bold, Complex Script Font: 11 pt

III. POLICY STATEMENT

Any individual who suspects that a theft, breach, or exposure of AIU restricted or sensitive data has occurred must immediately provide a description of what happened to the Information Security Office (ISO) which handles the incident response process.

All members of the ISO must participate in a training program is to sustain and refine the university's ability to handle incidents following the procedures described in this policy.

IV. RESPONSIBILITIES

- The Information Security Office (ISO) detects and investigates security events to determine whether an incident has occurred, and the extent, cause and damage of incidents.
- The ISO directs the recovery, containment and remediation of security incidents and may authorize and expedite changes to information systems necessary to do so. The ISO coordinates response with external parties when existing agreements place responsibility for incident investigations on the external party.
- During the conduct of security incident investigations, the ISO is authorized to monitor relevant AIU IT resources and retrieve communications and other relevant records of specific users of AIU IT resources, including login session data and the content of individual communications without notice or further approval and in compliance with the Securing Technology Resources and Services Policy.
- Any external disclosure of information regarding information security incidents must be reviewed and approved by the CIO in consultation with other university stakeholders as appropriate.
- The ISO should maintain appropriate contacts with authorities, external interest groups, or forums that handle the issues related to information security incidents and coordinate with law enforcement, government agencies, peer ISOs and relevant Information Sharing and Analysis Centers (ISACs) in the identification and investigation of security incidents. The ISO is authorized to share external threat and incident information with these organizations that does not identify any member of the AIU Constituency.

V. POLICY STANDARDS AND PROCEDURES

Any individual who suspects that a theft, breach, or exposure of AIU restricted or sensitive data has occurred must follow the following steps:

- **Evaluate severity level**. Any security incident involving an information system used to store, transmit or process AIU restricted data or a security incident that results in degraded performance of a AIU IT asset, which represents more than a minor impact on operations, is considered a high-severity incident. High-severity incidents should be reported immediately.
- **Report high-severity incidents to the AIU Information Security Office**. Include a brief description of the incident and who should be contacted for more information.
- **Protect the evidence**
- **Do not access (logon) or alter the affected IT asset**
- **Do not power off or logoff the affected IT asset**
- **Unplug the network cable** from the affected IT asset, network port or wall-jack
- **Physically label the IT asset**, directing others to not touch or use the IT asset
- **Document the following,** provide as much specificity as possible:
    - When and how the incident was detected?
    - What actions have been taken so far? Include the date/time, location, person(s) involved and actions taken for each step.
    - The type of data the affected IT asset is used to store, transmit or process
    - Anticipate that the AIU Information Security Office (ISO) will collect all related system or service logs and ancillary electronic evidence

- Be prepared to assist the AIU ISO as they investigate the incident
- All reported high-severity security events and/or incidents shall be promptly investigated and documented by the AIU Information Security Office (ISO) in accordance with AIU's Information Security Incident Response Plan. The AIU ISO is authorized to direct all incident response activities including, when necessary, containment and remediation tasks necessary to protect AIU's IT resources.

For any incident, a point of contact for security incidents' detection and reporting is maintained; and an incident investigator from ISO team is assigned the responsibility of investigating the incident, identifying the root causes and responding to the incident.

VI. FORMS/INSTRUCTIONS (if applicable)

~~N/A~~N/A

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Justified

VII. APPENDICES (if applicable)

N/A

VIII. RELATED POLICIES

Risk Management Policy

VIV. CONTACT INFORMATION

Triggered by:	Name	Date	Sig.
Created by:	Name	Date	Sig.
Revised by:	Name	Date	Sig.
Approved by:	Name	Date	Sig.