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

Formatted: Font: Font color: Auto, Complex Script Font: Times New Roman, 10 pt

Formatted: Font color: Auto

I. SCOPE OF POLICY

University information, including third party information that may be accessed or stored by the AIU, is a valuable asset to the university and requires appropriate protection.
Unauthorized use or disclosure of data could have adverse consequences for the individuals involved and could subject the university to fines, lawsuits, and government sanctions.

This policy is intended to:

- help the University and its community members comply with legal and contractual requirements to protect information;
- help safeguard University information from accidental or intentional damage, alteration or theft; and
- designate the appropriate level of security requirements for securing information.

This policy applies to everyone (including, but not limited to, all university faculty, researchers, staff, students, visitors, vendors, contractors, volunteers, and employees of an affiliated entity) who accesses data or university networks or who stores data through the use of university credentials or under the authority of and pursuant to university contracts. This policy also applies to such access and storage whether the data is accessed, stored or otherwise resides on university owned or controlled devices, personally owned or controlled devices, or devices owned or controlled by a third party under contract with the university.

Also, this policy applies globally to all assets, information resources and related infrastructure owned, managed or administered by AIU or owned and operated by a third party on behalf of AIU.

II. DEFINITIONS

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.

IT resources - Includes AIU systems that hold AIU information and ICT assets owned or licensed by AIU, or on behalf of AIU by a third party.

III. POLICY STATEMENT

Individuals who manage or use IT resources required by the university to carry out its mission must take reasonable steps to protect them from unauthorized modification, disclosure, and destruction.

Data and software are to be protected, regardless of the form, medium, or storage location of the information.
The level of protection shall be commensurate with the risk of exposure and with the value of the information and of the IT resources.

Some information has additional legal protection, like certain medical information, education records, certain financial records, and specific categories of personal and sensitive information.
Departments that regularly use specified categories of personal information should have written procedures on protecting that data and should also implement specific procedures concerning how that data is destroyed when no longer needed.

In order to manage information security risks, AIU members must ensure that their actions with respect to data and IT resources and their electronic devices and other resources that store, transmit, or process data meet the Information Security Standards, and all applicable laws, university policies, and university contractual obligations.

Individuals must report known non-compliance with this policy to the IT Security Office.

Failure to comply with this policy may result in denied access to IT Resources and disciplinary action, up to and including termination or dismissal.

IV. RESPONSIBILITIES

- Each person has an access to AIU computing resources is responsible for their appropriate use and by their use agrees to comply with all AIU policies.

- University members shall:
  - complete required privacy and information security training;
  - notify administrative and technical staff of high risk or sensitive data that is stored on computers and other electronic devices;
  - work with their local IT staff or unit liaison through the exception request process if needed; and
  - report non-compliance with this policy to the University IT Security Office

- University members with compliance responsibilities shall in addition to the duties of a University Community Member:
    - monitor data security compliance;
    - investigate allegations and incidents of non-compliance;
    - recommend appropriate corrective and disciplinary actions;
    - develop and maintain policies related to the compliance requirements; and
    - participate in breach notification processes.

- University members with Information Technology responsibilities shall in addition to the duties of a university member:
    - Take reasonable action to secure data and IT resources
    - Participate in university system technical and security groups and forums, as appropriate; and
    - Respond to technical questions from university members related to securing IT resources

- Unit administrators shall in addition to the duties of a university member:
    - assign the responsibility of managing the information security risk and identifying specific security requirements associated within the relevant unit;
    - create, disseminate, and enforce local information security requirements to comply with university policies and standards for data and IT resources under their control;
    - provide oversight and manage the security of data created, stored, or accessed by university members as applicable for their units;
    - manage the security gap analysis for data and IT resources for security control requirements as applicable for their units;
    - request exceptions to this policy or Information Security Standards, if needed; and
    - exercise delegated authority and responsibility for unit Information Technology security, unit Data, and unit IT Resources, including designating unit individuals as appropriate.

- Security Officer or Designate shall in addition to the duties of a university member:

    - exercise delegated authority and responsibility for privacy and information security from the CIO;
    - establish information security policies and standards to protect Data and IT Resources;
    - review and approve final information security standards;
    - establish a process to review exception requests to this policy and related standards;
    - review and approve exceptions to information security policies and standards; and
    - review and manage university information security incidents.

- Technology Services – Privacy and Information Security personnel shall in addition to the duties
- of a university member:
    - oversee the information security policy and standards and related exception process;
    - provide guidance on information technology security issues;
    - monitor and notify regarding potential information security intrusions;
    - review information security incidents;
    - establish and publish the criteria upon which a server is determined to be a “critical server” and provide oversight for the vulnerability scan process;
    - exercise operational responsibility to remove non-compliant electronic devices from the university network and, as appropriate, retrieve IT Resources and Data as part of an investigation;
    - coordinate with the unit administrative and technical/security staff to assure that actions are taken as necessary to protect IT resources and data; and

- coordinate with law enforcement, compliance offices, and university counsel.

V. POLICY STANDARDS AND PROCEDURES

University members must review and comply with the following Information Security Standards:

University data: Protect the confidentiality, integrity, and availability of data.

- Data must be properly classified, labeled, and handled.
- Authorized access to and possession, use, and modification of Data must be provided.

Program Management: Develop and maintain a program management strategy focusing on information risk management, information security, security assessment, and business continuity.

- A risk management strategy, which includes but is not limited to periodic risk assessments and reporting, must be developed and maintained.
- An information security plan, which includes but is not limited to assigning appropriate security roles and resources, must be developed and maintained.
- Periodic security assessments must be performed to comply with this policy and all pertinent laws and university policies and contractual obligations
- Business continuity and disaster recovery plan(s) must be developed, maintained, and periodically reviewed to limit the negative impact of a disruptive event upon university operations.

Legal: Identify laws and regulations applicable to data and IT resources as they become known in order to foster compliance.

Business: Verify segregation of duties in applicable university financial systems and processes to minimize financial fraud.

Purchasing: Include contractual obligations on vendors of third party software products and computer services to satisfy the university's information security requirements.

Personnel Security: Manage the risk presented by each university member throughout the lifecycle of the individual's relationship with the university. Such management includes but is not limited to:

- Reviewing the background and needs of university members before they are placed in positions with access to data in order to match permitted access with the needs of both the university members and the university.
- Establishing and maintaining a process to authorize, revoke, and audit access to data and IT resources by university members.
- Establishing and maintaining a process to retrieve data and IT resources from university members as appropriate when they are transferred within or leave the university.

Facilities: Equip university locations and workspaces with physical access controls to prevent the theft of, tampering with, or destruction of Data and IT Resources.

Information Technology:

- Training and Awareness
  - University members must complete the appropriate privacy and information security training.
  - University members must be made aware of their obligation to know and follow the acceptable use of Information Technology resources and policy for acceptable use of network resources.

- Security Incidents – There must be prompt, effective response and management of information security incidents.

- Identity Management – There must be secure use and management of digital identities and use of secure authentication processes in order for university members to access data or IT resources as appropriate.

- System, Network, and Communication Protection — There must be secure operation and timely access of:
  - Network devices.
  - Server systems
  - Client systems and applications.
  - Mobile devices and applications
  - Digital Communications.
- Malicious Software – Maximize reasonable protection of data and IT resources from exploitation by malicious software, which includes, but is not limited to, malware, viruses, and spyware.
- System Development Life Cycle – Establish a comprehensive approach to manage risks to IT resources and to provide the appropriate levels of information security based on the levels of risk as IT resources are being developed, modified, used, and retired. This approach must include the following:
  - Development Process – Reasonably maximize the production of secure applications and software in the software development process.
  - Application Development – Reasonably maximize the secure operation of applications so that they produce the correct results and perform only authorized transactions and so that Data is not inadvertently exposed during processing.
- Secure Use and Disposal of Information and Equipment – Require that University storage media, which includes but is not limited to optical media (CDs or DVDs), magnetic media (tapes or diskettes), disk drives (external, portable, or removed from information systems), flash memory storage devices (SSDs or UBS flash drives) and documents (paper documents, paper output, or photographic media), are used and disposed of securely.
- Equipment and Software Inventory Management – Require that IT resources, including information assets and software, are identified so they can be managed securely and in compliance with appropriate license agreements and copyright laws.

VI. FORMS/INSTRUCTIONS (if applicable)

N/A

VII. APPENDICES (if applicable)

N/A

VIII. RELATED POLICIES

Securing Technology Resources and Services Policy

VIV. CONTACT INFORMATION

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