Contents

Document Review Log

Date Reviewed	Description of Changes
8/17/2023	Initial Draft approved by Senior Leadership Team

Purpose and Scope

This policy defines the IT Security framework for Alvernia University ("AU"). The policy is intended to ensure AU systems and data are protected from threats to their confidentiality, integrity, and availability. It is aligned with industry best practices and standards. AU relies on information technology assets to conduct and support operations, and recognize the risk to the organization and brand posed by a security breach. This policy:

- Defines roles and responsibilities with respect to IT security.
- Identifies the standards and best practices used by the AU IT Security program.
- Lists the related AU IT Security policies which provide more detailed guidance on IT security.
- Categorizes the different kinds of data used by AU.

This policy applies to all AU staff, faculty, contractors, and 3rd party service providers, including student employees. Its scope includes all data stored on systems owned by AU, as well as all AU proprietary data stored on 3rd party systems.

Responsibilities

Title or Role	Definition and What They are Responsible For
Chief Information Officer	Maintains and Enforces this policy.
End User	Any employee, contractor or trustee who accesses the AU network or systems containing AU data, including student employees. End users have specific responsibilities for protecting AU systems and data. These responsibilities are outlined in 9.2000, End User Responsibilities.
IT and Data Professionals	Employees or contractors who have an elevated level of access to AU network or systems. These individuals have responsibility for selecting, purchasing, deploying, maintaining and/or disposing of AU network components, systems, or digital information, and have significant security responsibilities. Examples include network and system administrators, database administrators, and application administrators. These individuals have additional security responsibilities, as outlined in 9.3000, IT Security for IT and Data Professionals.
3rd party service provider	Any entity that provides an information system as a service to AU that is hosted outside AU, or who hosts AU data on their systems. These systems may or may not have direct integration and connectivity to the AU network and systems. These third-party systems and organizations must minimally provide equivalent protection to that provided by the AU network and systems. The specific responsibilities of 3rd party information systems providers are described in 9.4000, IT Security for 3rd Party Partners and Providers.

Policy

The IT Security and Compliance program of AU is based on National Institute of Standards and Technology (NIST) standards and best practices, and also aligns with the Family Educational Rights and Privacy Act of 1974 (FERPA), the Payment Card Industry (PCI) standards, as well as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the Health Information Technology for Economic and Clinical Health Act (HITECH) for electronic Protected Health Information, when applicable. Other standards that apply to Alvernia University's system include the Web Content Accessibility Guidelines (WCAG 2.0) and the Americans with Disabilities Act (ADA). A risk-based approach guides the categorization of AU systems, and the selection of the applicable security and compliance controls for those systems. The AU security and compliance program is focused on the entire systems life cycle, including:

- Enterprise systems, network, and application architecture
- Selection, acquisition, and implementation of third-party software and IT services
- Design, development, testing, and implementation of any internally developed software
- Disposition of IT assets and digital information

Policy Framework

AU's IT policies are broken down into a few main areas. Each area may, in turn, be further broken down into separate policy documents to make it easier to maintain or to make it easier to provide focused guidance for a specific process or group. These areas are:

9.1000, IT Security Framework and Governance (this document)

9.2000, End User Responsibilities

9.3000, IT Security for IT and Data Professionals

9.4000, IT Security for 3rd Party Partners and Providers

9.5000, Web Accessibility

9.6000, IT Governance

Approved versions of these policies will be posted on the AU Portal.

Risk-based Approach

The risk-based approach used by AU is based on the approach in ***NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems***, and the categorization of our systems is guided by **Federal Information Processing Standard** (***FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.*** This publication establishes the security categories for both information and information systems based on three security objectives:

Confidentiality – A loss of Confidentiality is the unauthorized disclosure of information.

Integrity – A loss of Integrity is the unauthorized modification or destruction of information.

Availability – A loss of Availability is the disruption of access to or use of information or an information system.

FIPS 199 also defines three categories of potential impact on organizations and individuals for each of these three security objectives, should there be a breach of security:

Low - The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Moderate - The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

High - The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Based on these guidelines, the categorization of AU systems, whether hosted by AU or third-party providers, varies based on the business function supported. For example, systems that carry personal information, including demographic, financial aid, academic, or credit card information, must have a specific focus on preserving the confidence and integrity of that information. Systems that support daily operations, including point of sale systems, physical security systems, and other systems that must be reliable during events, have higher requirements in terms of availability. The supporting network and other IT infrastructure must support the highest combined categorization of all systems that use the infrastructure. The specific controls applicable to each system are driven by the categorization of that system, and 9.3000 provides customized guidance on the controls required for AU systems based on this categorization.

Data Classification

The confidentiality and integrity categorization of each system is, in turn, driven by the classification of the data maintained in each system. The table below defines the different classes of AU data.

Data Classification	Definition
Public	Information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to disclosure rules, is available to all employees and all individuals or entities external to the corporation. Examples include: •Publicly posted press releases •Publicly available marketing materials, including the AU website •Publicly posted job announcements •Social Media
Internal	Information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Internal Data is information that is restricted to personnel who have a legitimate reason to access it. Examples include: •General academic or employment data (information on employees or the AU organization not covered in the Confidential classification below) •Business partner information where no more restrictive confidentiality agreement exists •Contracts Student data that would be categorized by FERPA as “Directory” information also falls in this category.
Confidential	Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization is required for access because of legal, contractual, privacy, or other constraints. Confidential data have a very high level of sensitivity. Examples include: •Payment Card Industry (PCI) data (credit or debit card data) •University business strategy, forecasts and other sensitive financial information •Personally Identifiable Information. Medical information or social security numbers in combination with other personal data that could be used for identity theft or that are protected by regulation (such as PHI information protected by HIPAA). This also includes other HR information, such as salary. All student data that would be categorized by FERPA as “Protected” data also falls into this category. •Information related to the physical security of AU employees, students, or facilities

The confidentiality and integrity categorization of a system carrying only public or internal data will be **Low**, while the confidentiality and integrity categorization of a system carrying Confidential information will be **Moderate.**

System Categorization

The matrix below shows how different types of AU systems are categorized, and should be used as a guideline by management, IT professionals and 3rd party service providers in defining the specific controls required for a system, based on the guidance in ***NIST 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations*** and ***NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.*** If a system doesn't fit neatly into one of these definitions, the definitions of system categorization and data classification should be used to determine the appropriate categorization for the system. AU will also categorize systems not controlled by AU that reside on the AU network (e.g. Ticketmaster and NBA), and work with the owners of those systems to evaluate their controls and assess the level of risk to compromise of AU systems and data.

Type of System	Confidentiality	Integrity	Availability	Reason for the categorization
Point of sale, student information systems, student financial aid, and other financial transaction systems	M	M	M	These systems carry Confidential data (student protected information or credit card information), and must be available for university operations.
HR systems	M	M	L	These systems carry Confidential data (personal information), but short outages will have minimal impact on operations
Finance systems (general ledger, accounts receivable/payable, etc)	L	L	L	These systems generally only carry Internal data, and short outages will have minimal impact on university operations
Physical security systems	L	M	M	These systems may not carry Confidential data, but compromise of their integrity or availability could present a significant physical risk to employees or students
Building management systems	L	L	M	These systems do not carry Confidential data or carry internal data where this is significant integrity risk, but they have the same availability requirements as all other university operational systems.
General office productivity, e-mail and other back office support, file storage systems	M	M	L	These systems may contain Confidential data, but short outages will have minimal impact on operations
Systems or Applications carrying ePHI	M	M	L	These systems would by definition carry Confidential data, but given the University is not a health care provider, short outages would have minimal impact on operations.
Network and security infrastructure	M	M	M	The underlying infrastructure must meet the high water mark of all systems supported by it.

Legend
H=High M=Medium L=Low

Exceptions to Policy

Exceptions to any of the security policies, e.g. because a specific technology cannot support it or it would be prohibitive to implement the control, will be evaluated based on risk, and must be approved by the Chief Information Officer. Documentation of these exceptions and their rationale will be captured using Exhibit A of 9.3000, "Approval of IT Security Exception".

PCI Compliance

The AU IT Security Policies also addresses Payment Card Industry (PCI) Compliance. The table below provides a cross-reference between the PCI Data Security Standard (DSS) Requirements and the specific sections of the AU IT Security policies where they are addressed.

PCI DSS Security Goal	PCI DSS Requirement	IT Policy Reference
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data	9.3000, section 3.13.1 Requirement 1.1.7 is addressed in 9.3400, Monitor As-Built Against Baseline.
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	9.3000, section 3.13.2
Protect Cardholder Data	3. Protect stored cardholder data	9.3000, section 3.13.11
	4. Encrypt transmission of cardholder data across open, public networks	9.3000, section 3.13.8
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs	9.3000, section 3.14.3
	6. Develop and maintain secure systems and applications	9.3400 and 9.4000
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know	9.3000, section 3.1.3
	8. Assign a unique ID to each person with computer access	9.3000, section 3.5.1
	9. Restrict physical access to cardholder data	9.3000, section 3.8.1
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data	9.3000, sections 3.3.2 and 3.13.1
	11. Regularly test security systems and processes	9.3000, section 3.12.3
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel	9.1000, 2.0, 3.0 and 4.0 together address this requirement.

HIPAA and HITECH Compliance

HIPAA outlines privacy and security safeguards required for covered entities and business associates to protect individual's identifiable health information, including demographic data and information that relates to the individual's past, present, or future physical or mental health condition, or related to the provision or payment for healthcare for an individual. This information is collectively called Protected Health Information (PHI), and when stored electronically, ePHI. The Health Information Technology for Economic and Clinical Health Act (HITECH) added specific incentives (and enforcement) of the general HIPAA guidelines, including an increase of the civil penalties for willful neglect, and extended certain conditions of HIPAA's civil and criminal penalties to business associates of healthcare providers.

Most of the information handled by Alvernia University is explicitly excluded from HIPAA, such as employment records or student information protected by FERPA. As a result, most or all information carried by university systems will not store, process or access ePHI. However, because of the relationships between the university and community health care organizations, it is possible that ePHI for non-students could be processed, stored or accessed using University systems or by university staff. In those situations, those systems must follow HIPAA and HITECH rules for protecting ePHI. The table below provides a cross-reference between the HIPAA and HITECH requirements and the specific sections of the AU IT Security policies where they are addressed.

HIPAA or HITECH Requirement	IT Policy Reference
HIPAA Privacy Rule	9.2000, End User Responsibilities
HIPAA Breach Notification	**9.3600, Incident Response**
HIPAA Security Rules	
Administrative Safeguards	
(a)(1) Security management process	9.1000, IT Security and Compliance Framework and Governance
(a)(2) Assigned security responsibility	9.1000, IT Security and Compliance Framework and Governance
(a)(3) Workforce security	9.3000, Section 3.1
(a)(4) Information access management	9.3000, Section 3.1
(a)(5) Security awareness and training	IT 30, Section 3.2
(a)(6) Security incident procedures	9.3600, Incident Response
(a)(7) Contingency Plan	9.6000 will address disaster recovery and business continuity upon completion.
(a)(8) Evaluation	9.1000, IT Security and Compliance Framework and Governance, 9.3000, Section 3.11 also addresses the Risk Assessment controls
(b) Business Associate contracts and other arrangements	9.4000, IT Security for 3rd Party Partners and Providers
Physical Safeguards	
(a) Facility Access Controls	Contingency operations will be addressed in 9.6000. 9.3000, Section 3.10 addresses physical protections to facilities where ePHI or other confidential information is kept.
(b) Workstation Use	9.2000, End User Responsibilities addresses the responsibility of non-IT staff with respect to workstation use. 9.3000,
(c) Workstation Security	9.3000, section 3.8 addresses protection of media and systems accessing confidential data
(d) Device and Media Controls	9.3000, section 3.8 addresses protection of media and systems accessing confidential data

Technical Safeguards	
(a) Access Control	9.3000, Section 3.1 addresses Access Control
(b) Audit Controls	9.3000, Section 3.3 addresses audit and accountability controls
(c) Integrity	9.3000, Section 3.14 addresses system and information integrity controls
(d) Person or Entity Authentication	9.3000, Section 3.5 addresses Identity and Authentication controls
(e) Transmission Security	9.3000, Section 3.13 addresses System and Communication Protection controls
HITECH Breach Notification	9.3600, Incident Response
HITECH Electronic Health Record Access	This is not explicitly addressed elsewhere in the policy framework. Alvernia University will comply with HITECH requirements for providing individuals with access to their electronic health records, should the need arise.
HITECH Business Associates and Business Associate Agreements	9.4000, IT Security for 3rd Party Partners & Providers addresses this.

Policy Review

The IT Security policies should be reviewed at least annually and updated when business objectives or the risk environment change.

Note: This addresses PCI requirement 12.11.

References and Related Policies

This section contains any 3rd party standards, guidelines, or other policies referenced by this policy.

1. **NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems,** National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
2. **FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems**, Federal Information Processing Standards Publication, Computer Security Division, National Institute of Standards and Technology, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
3. **NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations,** National Institute of Standards and Technology, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
4. **NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,** National Institute of Standards and Technology, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
5. Payment Card Industry (PCI) Data Security Standard, v3.2
6. PCI DSS Quick Reference Guide, Understanding the Payment Card Industry Data Security Standard version 2.0, https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf
7. Family Educational Rights and Privacy Act, 1974 (FERPA), https://ed.gov/policy/gen/guid/fpco/ferpa/index.html

8. Health Insurance Portability and Privacy Act of 1996 (HIPAA), https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996
9. HIPAA for Professionals, https://www.hhs.gov/hipaa/for-professionals/index.html
10. HITECH Act Enforcement Interim Final Rule, https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

Related Policies

11. 9.2000, End User Responsibilities
12. 9.3000, IT Security for IT Professionals
13. 9.4000, IT Security for 3rd Party Partners and Providers
14. 9.5000, Web Accessibility
15. 9.6000, Disaster Recovery and Business Continuity *(not yet available)*

Exhibits

No exhibits.