October 2011

8.105 Information Security Policy

Type of Policy ■ ***University*** □ ***Campus*** □ ***Department/Unit*** □ **Interim**	**Information Security Policy** **Policy 8. 105**
Information Technology Policies	**Effective date: June 12, 2010**

Policy History:	**Approved by:**	**Resolution #**	**Date**
Approved	**Board of Governors**	**6.12.10:9**	**June 12, 2010**
Revised (Non-substantive)	**Office of University Counsel**	**N/A**	**May 31, 2017**
Revised	**Chancellor**	**N/A**	**December 1, 2022**
Responsible Office	**Responsible Administrator:**	**Contact information**	**Applies to:**
University Chief Financial Officer	**University Chief Financial Officer**	**937-769-1304**	**All Antioch University employees, academic and administrative units, foundations, vendors, contractors, third-party systems vendors, and integrators, and agencies which handle or process Antioch University data.**

I. Purpose

This policy is established to implement, maintain and continually improve the Antioch University Information Security Program. This policy lays the foundation for a common understanding of information security at Antioch University based on the generally accepted information security principles of confidentiality, integrity and availability.

II. Introduction

Information is a resource of great value to Antioch University as are the information systems, resources and processes that facilitate creation, collection, use, sharing, and storage of information throughout University operations. Therefore, it is important to adequately preserve the confidentiality, integrity and availability of the important data assets and data management

resources that the University relies upon to achieve its strategic and operational objectives, including the preservation of open information sharing that forms the basis of the University's academic culture.

Information Security is the ongoing process of identifying, evaluating, and treating risks to the confidentiality, integrity and availability of information, information systems, and other business information processing resources and activities (collectively known as "Information Assets").

Antioch University is committed to implementing and continually improving Information Security controls, policies and practices that:

1. Provide clear responsibilities for Information Security across the University;

2. Implement safeguards to manage risk factors to mitigate, transfer or avoid risks that may adversely impact the confidentiality, integrity, and availability of Information Assets;

3. Comply with applicable law, regulatory and industry requirements, and contractual obligations; and

4. Provide assurance to Antioch University stakeholders that Information Security risks are responsibly managed.

III. Key Definitions

1. ***Information*** refers to the body of knowledge, collection of information, or data obtained, produced, organized, shared, or managed by Antioch University or authorized Third Parties over the course of its business operations. Information may be shared or stored in a physical or electronic manner, or may take the form of the spoken word. Information includes, but is not limited to, any document, record, file, data, data set, or definable unit of information from any source that is created, processed, shared, or stored by Antioch University or authorized Third Parties in any manner. Information is not easily replaced without funding, skill, knowledge, resources, time, or any combination of these factors. Therefore, Information is considered a critical resource from the standpoint that it is used to build knowledge, accomplish business objectives, and sustain or create organizational value.

2. ***Information Asset*** refers to Information, Information Systems, wholly-owned or leased facilities, and other resources or activities related to processing or storage of Information. The value of an Information Asset is determined not only by its financial value, but also the impact it has in supporting organizational activities and achieving business objectives.

3. ***Information Systems*** refers to wholly-owned or leased computing hardware, software and media components for collecting, processing, storing, or delivering Information, or performing operational tasks that involve Information, and the infrastructure that supports those components. Examples of information systems include, for example, computers, laptops, tablets, and smartphones.

4. ***Information Security (or "Information Security")*** refers to the ongoing process of identifying, evaluating, and treating risks to the confidentiality, integrity and availability of Information Assets.

5. ***Information Security Program (or "Information Security Program" or "Program")*** refers to the Information Security objectives, requirements, controls, and processes prescribed in this Policy as well as its framework of supporting standards, procedures, and guidelines.

6. ***Risk Owners*** are those individuals responsible for identifying and managing risk factors that may adversely impact the confidentiality, integrity, and availability of Information Assets within their business function or span of organizational control.

7. ***Third Party Service Providers (or "Third Parties")*** are entities with whom Antioch University enters into a Third Party agreement. Third Parties include employees, contractors, agents and subcontractors of Third Parties who have access to, store, or process Information. Third Parties may also have access to, or may manage, Information Systems.

IV. Roles and Responsibilities

All Antioch University employees, and third parties such as contractors and/or vendors are responsible for supporting and complying with the Information Security Program requirements outlined in this policy. However, certain individuals and groups are in a position to safeguard information security in specific ways, based on access to and usage of various aspects of the University's information systems. The following Information Security Program roles and responsibilities shall be allocated and maintained to contribute to and control the implementation of Information Security across the University:

A. **University Leadership** shall be responsible for:

1. Implementing and regularly improving the Information Security Program so as to be compatible with organizational strategy and operational objectives;

2. Providing adequate resources, training, and appropriately integrating the Information Security Program across Antioch University business units and organizational processes; and

3. Promoting and supporting the Information Security Program by communicating with relevant stakeholders about the importance of achieving and complying with Information Security Program objectives and requirements.

B. The **Chief Information Officer (CIO)** shall be responsible for:

1. Allocating budgetary resources for management, oversight, and continuous improvement of the Information Security Program;

2. Reporting on the performance and effectiveness of the Information Security Program to Senior Management for review at regular intervals; and

3. Providing direction and support to the Information Security Officer (ISO), as necessary.

C. The **Information Security Officer (ISO)** shall direct and manage implementation and continuous improvement of the Information Security Program, including:

1. Establishment of a process for identifying objectives for, and governance of, the Information Security Program that is scoped across relevant Antioch University business units and organizational processes;

2. Maintenance of this Policy and its supporting framework of standards, procedures, and guidelines;

3. Design and implementation of an Information Security risk assessment process that identifies and evaluates Information Security risks against relevant risk criteria;

4. Design and implementation of an Information Security risk treatment process to drive formulation, implementation, and monitoring of Information Security risk treatment plans by relevant Risk Owners;

5. Providing for Antioch University employee awareness and necessary competence to understand the implications of noncompliance with Information Security Program requirements and contributing to Information Security Program effectiveness; and

6. Monitoring and reporting on performance and effectiveness of the Information Security Program.

D. **Risk Owners** are responsible for allocating or managing resources to address risk factors identified by the ISO or other relevant Information Security Program stakeholders that may adversely impact the confidentiality, integrity, and

availability of Information Assets within their business function or span of organizational control.

V. Information Security Principles

All components of the Information Security Program and requirements of this policy are designed to address risks to Information Assets. Risks to Information Assets shall be evaluated and managed according to the following fundamental security criteria, or principles:

A. **Data Confidentiality.** Antioch University stores and generates sensitive Information Assets that must be protected from unauthorized access or exposure. The University adheres to the principle of Data Confidentiality by restricting access to Information Assets to only those individuals or processes with a legitimate business need for the information.

B. **Data Integrity.** Antioch University relies on Information Assets to deliver services to students and as a basis for making business decisions. The University adheres to the principle of Data Integrity by developing and maintaining Information Assets using methods that ensure the accuracy and completeness of information.

C. **Data Availability.** Antioch University expects Information Assets to be available when needed to support educational activity and business operations. The University adheres to the principle of Data Availability by maintaining reliable and prompt access to Information Assets.

VI. Information Security Risk Management Plan

A. General Overview

Antioch University shall create a Data Security Plan document that will define and implement a framework for identification and management of Information Security risks across the University. The Data Security Plan shall address the following areas of data security:

1. A risk assessment process that is applied to identify, evaluate, treat, and report Information Security risks to applicable Risk Owners and Senior Management;

2. Policies and implementation standards that outline mandatory Information Security control categories, objectives, and requirements that must be achieved across the University;

3. An awareness program to make Antioch University employees and relevant external parties aware of Information Security policies, standards and expected practices as well as the implications of non-compliance;

4. A management process to oversee the performance and evaluate the effectiveness of the Information Security Program across Antioch University at regular intervals.

B. Specific Components of the Information Security Risk Management Plan

The following processes, practices and controls shall be part of the University's Information Security Risk Management Plan:

1. Information Security Policy. This Information Security Policy 8.105 defines the University's objectives and support for Information Security. This Policy shall be reviewed at least annually, or at more frequent intervals if significant changes to the scope of the Information Security Program or business have occurred to evaluate the Policy's suitability, adequacy and effectiveness.

2. Personnel Security. Controls associated with Personnel Security shall be implemented to confirm that Antioch University employees and Third Parties understand and fulfill their Information Security responsibilities. Personnel Security includes the following control objectives:

a. Screening of employees and Third Parties;

b. Communication to, and agreement by, employees and Third Parties on their Information Security responsibilities prior to employment or prior to providing services to Antioch University, including requirements for confidentiality and non-disclosure of Information;

c. Information Security awareness, education or training of employees and relevant Third Parties, along with procedures for documenting that education and training;

d. A disciplinary process to sanction employees or Third Parties for failure to comply with Information Security policy; and;

e. A process for managing employee separation and Third Party off-boarding that includes revocation of access to, and recovery of, Information Assets.

3. Information Asset Management. Information Asset Management controls shall be implemented to identify, classify and assign responsibilities for protecting

Information Assets, as practicable. Information Asset Management includes the following objectives:

a. Identifying and maintaining an inventory of Information Assets and the Risk Owners responsible for their protection;

b. Classifying Information Assets in a manner consistent with their value or business criticality; and

c. Defined acceptable use, management, transfer, storage and disposal practices associated with Information Assets in accordance with University information classification.

4. Access Control. The objective of Access Control is to restrict access to Information Assets or to Information Systems. Only employees and Third Parties with a legitimate business need and authorized by management shall have access to Information Assets or Information Systems. Access Control shall be achieved through implementation of the following:

a. Processes for managing employee and Third Party access to Information or Information Systems that include access provisioning, review of access rights at regular intervals, and modification or termination of access rights;

b. Controls and mechanisms to authenticate employee and Third Party access to Information Assets or Information Systems; and

c. Controls to monitor and prevent unauthorized access to Information and Information Systems.

5. Segregation of Duties. Conflicting or overlapping Information Security control responsibilities shall be segregated to confirm that consistent Information Security governance and risk management is implemented across the organization. Segregation of duties shall be defined based on risk factors determined and evaluated by Information Security.

6. Physical and Environmental Security. Physical and Environmental Security controls shall be implemented to prevent unauthorized physical access, damage, loss, theft, or disruption to tangible Information Assets, including Antioch University office locations or facilities. Physical and Environmental Security objectives shall be achieved through implementation of the following:

a. Maintaining secure perimeters and entry controls to protect and authorize physical access to Antioch University office locations and facilities;

b. Protecting supporting utilities and computer equipment from environmental threats, power failures, or other disruption, based on applicable risk factors;

c. Protecting computer equipment and other tangible Information Assets from theft or unauthorized removal; and

d. Processes to dispose of computer equipment or other tangible Information Assets to securely remove Information prior to re-use, or destroyed prior to final disposition.

7. Operations Security. Operations Security controls shall be implemented to protect and provide for the confidentiality, integrity and availability of Information and Information Systems. Operations Security controls shall include:

a. Maintaining adequate documentation related to the design and operational performance of Information Systems;

b. Maintaining a change management process to control planned and unplanned changes to Information Systems;

c. Physical and/or logical separation of Information System development, test and production environments, or applicable controls to safeguard the use of Information in development, test and production environments;

d. Security measures to detect threats, safeguard computing services, protect Information, or control access or changes to Information Systems;

e. Protecting against Information loss by backing up Information and Information Systems and testing backups at regular intervals to allow Antioch University to recover Information and Information Systems in timeframes sufficient to meet business requirements;

f. Identifying and preventing against exploitation of technical vulnerabilities;

g. Protecting against malware threats by employing solutions or processes to detect and recover from malware-based attacks; and

h. Monitoring Information Systems to record and regularly review security events to identify unintended or unauthorized activity.

8. Communications Security. Communications Security controls shall be implemented to provide for the security of electronic communications networks

and to protect Information. Communications Security shall be achieved through implementation of the following controls:

a. Network segregation achieved by grouping Information Systems on segmented networks according to inherent risk factors;

b. Controlling access between users and Information Systems on segmented networks;

c. Deploying mechanisms for network security monitoring according to inherent risk factors; and

d. Maintaining requirements for secure exchange and storage of electronic Information, including the use of encryption.

9. Information Systems Development and Maintenance. Information Systems Development and Maintenance controls are associated with integrating Information Security requirements across the entire Information System lifecycle. Security controls in this category shall include:

a. Analysis of Information Security requirements for modifications to existing or new Information Systems;

b. Implementing protections for applications that transmit, process, or store Information to safeguard against unauthorized disclosure, modification, duplication, interference, replay, misrouting, or fraudulent activity;

c. Applying secure software and systems engineering principles to Information System development and maintenance efforts;

d. Maintaining a change management process to control planned and unplanned changes to software and applications;

e. Securing development environments used for software engineering and systems integration activities;

f. Security review and testing of Information Systems, including review and testing of software and applications; and

g. Using carefully selected and protected data during software integration and quality assurance activities.

10. Third Party Security. Controls shall be implemented to protect Information Assets that are shared with, accessible to, or stored by Third Parties. Security controls shall include:

a. A process to identify risks to Information Assets and incorporate Information Security and relevant risk treatment requirements into business agreements with Third Parties;

b. Processes to monitor Third Party performance toward Information Security requirements.

11. Information Security Incident Management. Controls shall be implemented to provide for consistent and effective management of Information Security incidents. Information Security Incident Management controls shall include:

a. A defined process for Information Security incident management that includes management responsibilities, requirements for reporting potential security incidents by staff, incident assessment or classification criteria, and documented response guidelines;

b. Communication to and awareness by relevant individuals of their role in the Information Security incident management process; and

c. A defined process to capture and apply knowledge gained from Information Security incidents to address and reduce the impact or likelihood of future occurrences.

12. Business Continuity Management. Controls shall be implemented to provide continued confidentiality, integrity and availability of Information Assets, as well as to provide for the continuity of applicable Information security controls or processes, during unplanned, adverse events. Business Continuity Management controls include:

a. A process to scope, document, and enact requirements for continuity of access to, availability, or recovery of, Antioch University Information Assets; and

b. A process implemented at regular intervals to evaluate the effectiveness of business continuity activities.

13. Compliance and Audit. Compliance and Audit objectives are associated with the need to monitor business, legal, regulatory, or contractual requirements and confirm that Information Security controls and requirements are implemented consistently. Such security controls shall include:

a. Monitoring, identification and review of applicable legal, regulatory, or contractual requirements as they relate to Information Security, including security and privacy of personal information; and

b. Auditing compliance with Information Security policies, standards, controls, processes or requirements at regular intervals.

VII. Policy Review Schedule

This policy shall be reviewed at least annually by the Information Security Officer (ISO).

VIII. Compliance and Enforcement

The ISO is responsible for monitoring compliance with this Policy and reporting instances of non-compliance to Antioch University Senior Management stakeholders. Violations of University Information Security policies, procedures and directives will be evaluated and handled in accordance with Antioch's Corrective Action and Discipline Policy 4.617.

Policy Cross Reference

Corrective Action and Discipline	Policy #4.617