October 2011

8.105 Information Security Policy

ANTIOCH UNIVERSITY

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
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. Introduction

A. Purpose

The purpose of this policy is to protect Antioch University's information resources from accidental or intentional unauthorized access or damage, while also preserving the open information sharing requirements of its academic culture. This policy lays the foundation for a common understanding of information security at Antioch University based on the generally accepted information security principals of confidentiality, integrity and availability. Confidentiality limits information security access to authorized users. Integrity

protects information against unauthorized modification. Availability ensures that information is accessible when needed.

The information assets of Antioch University must be available to the Antioch community, protected commensurate with their value, and must be administered in conformance with federal and state law. This will include digital, analogue, and non-technical information used in the court of conducting university business.

Reasonable measure shall be taken to protect these assets against accidental or unauthorized access, disclosure, modification or destruction, as well as to assure the confidentiality, integrity, availability and authenticity of information. Reasonable measures shall also be taken to assure availability, integrity and utility of information systems and the supporting infrastructure, in order to protect the productivity of its members.

II. Definitions

A. Lifecycle Protection – Information systems and supporting infrastructure have a lifecycle that begins with evaluation and selection, and advances through planning, development / acquisition, and operations through to disposal or retirement. Information safeguards are needed at all phases of the lifecycle. Lifecycles could also include records retention guidelines.

B. Information Assets – Information assets is any mode of information including but not limited to E-mails, electronic reports and documents, paper copies of documents, information shared over telephone or voicemails, information used in publications and presentations.

C. Information Safeguards – Administrative, technical and physical controls that support the confidentiality, integrity, availability and authenticity of information.

D. Operating Framework & Guidelines – Procedures and guidelines that the Antioch community will follow to ensure complete implementation of all policies and safeguards associated with Information Security.

E. Information Systems and Supporting Infrastructure – Information in its analog and digital forms and the software, network, computers, tokens and storage devices that support the use of information.

F. Controls – Depends on the system, its capabilities, and expected usage, as well as anticipated threats against the information.

G. Preventive Controls – Preventative controls include use of encryption, information integrity measures, security configuration, media reuse, and use of antivirus and physical protection.

H. Detective Controls – Detective controls include network and information access monitoring, and intrusion detection (host based or network based), manual or automated review of security logs

I. Corrective Controls – Corrective controls include recovery plans for handling isolated information safeguard failure incidents to business continuity plans.

J. Antioch Community – 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.