NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 110**
	Section: 100 General
	Page 1 of 4
	Responsible office: Comptroller
	Origination date: 01/01/2000
Subject: Information Security Plan for Northern Arizona University	Effective date: 05/23/2003
	Revision date: 12/1/15

PURPOSE

To document the University Information Security Plan as required by the FTC for the administrative, technical, and physical safeguarding of customer information.

SOURCE

University policy

NACUBO Data Security Resources

Federal Trade Commission, Regulation of Commercial Practices

BACKGROUND

Financial institutions, including colleges and universities, must meet a general standard in order to comply with the requirements of the Gramm-Leach-Bliley Act "to develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards" appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of any customer information at issue. The information security program developed should be flexible, designed to address the needs of the individual institution.

The final rules indicate that the objectives of the information security program should be:

- to ensure the security and confidentiality of customer information;
- to protect against any anticipated threats to the security or integrity of such information; and
- to guard against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 110**
	Section: 100 General
	Page 2 of 4
	Responsible office: Comptroller
	Origination date: 01/01/2000
Subject: Information Security Plan for Northern Arizona University	Effective date: 05/23/2003
	Revision date: 12/1/15

CMP 110: Information Security Plan for Northern Arizona University

I. The designated group for the coordination and execution of the Information Security Plan is the Information Security Committee of Northern Arizona University. All correspondence and inquiries should be directed to the Committee.

II. The following have been identified as relevant areas to be considered when assessing the risks to customer information (this list is meant to be as inclusive as possible but the policy is applicable to all university departments and their affiliates which collect financial information from their customers whether listed below or not):

- Academic Departments (which collect financial data during payment of fees for affiliated programs)
- Accounts Payable
- Admissions
- Alumni Association
- Aquatic Center
- Athletics (including Summer Sports Camps)
- Bookstore
- Central Ticket Office
- Cline Library
- Dental Hygiene
- Dining Services
- Distance Learning
- Financial Aid Office
- Campus Health Services
- Information Technology Services
- KNAU
- JacksCard Office
- Student and Departmental Account Services (includes Accounts Receivable and Student Loans)
- Parking and Shuttle Services
- Performing Arts (Including Summer Camps)
- Postal Services
- Property Administration
- Contracting and Purchasing Services
- Recreation Center
- Registrar's Office

NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 110**
	Section: 100 General
	Page 3 of 4
	Responsible office: Comptroller
	Origination date: 01/01/2000
Subject: Information Security Plan for Northern Arizona University	Effective date: 05/23/2003
	Revision date: 12/1/15

CMP 110: Information Security Plan for Northern Arizona University

- Housing and Residence Life
- Skydome
- Transportation Services
- University Advancement

III. The Information Security Committee will coordinate with various University Offices to maintain the information security program. The Information Security Committee will provide guidance in complying with all privacy regulations. Each relevant area is responsible to secure customer information in accordance with all privacy guidelines. A written security policy that details the information security policies and processes will be maintained by each relevant area and will be made available to the Information Security Committee or Internal Auditor's office upon request. Such a policy would include procedures to physically and electronically protect both hard copy and electronic data. In addition, ITS will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic customer information and that guard against the unauthorized use of such information for the information systems they operate.

IV. The University's Contracting and Purchasing Services will be responsible for selecting which service providers will be given access to customer information in the normal course of business. All contracts with such service providers shall require that the service provider implement and maintain adequate safeguards for customer information. Contracts with service providers shall include the following provisions:

- An explicit acknowledgement that the contract allows the contract partner access to confidential information.
- A specific definition of the confidential information being provided.
- A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract.
- A guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract.
- A guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customer's confidential information.
- A provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract
- A stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract.

NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 110**
	Section: 100 General
	Page 4 of 4
	Responsible office: Comptroller
	Origination date: 01/01/2000
Subject: Information Security Plan for Northern Arizona University	Effective date: 05/23/2003
	Revision date: 12/1/2015

CMP 110: Information Security Plan for Northern Arizona University

- A stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles the University to immediately terminate the contract without penalty.
- A provision allowing auditing of the contract partners' compliance with the contract safeguard requirements.
- A provision ensuring that the contract's protective requirements shall survive any termination of the agreement.

V. The Human Resources Office will be responsible for a component to all new employee training sessions which cover employee responsibilities to protect personal financial data. This training can be added to the existing training given on FERPA.

VI. This information security plan shall be evaluated and adjusted in light of relevant circumstances, including changes in the University's business arrangements or operations, or as a result of testing and monitoring the safeguards. Periodic auditing of each relevant area's compliance shall be done per the internal auditing schedule. Annual risk assessment will be done through the Internal Auditor's Office. Evaluation of risk of new or changed business arrangements will be done through the legal counsel's office.

CROSS-REFERENCES

NACUBO - Complying with Domestic Security Legislation

FTC Regulations on Commercial Practices

FERPA Web Site at NAU

FTC Gramm-Leach-Bliley Act web site