UNG
UNIVERSITY of NORTH GEORGIA™

University of North Georgia

2013

Information Security Program Policy

Division of Information Technology

Version 1.0

Unrestricted

Revision & Sign-off Sheet

Change Record

Date	Author	Version	Change Reference

Reviewers

Name	Version Approved	Position	Date
Alfred Barker	1.0 - Approved	CISO	11/26/2012
Brandon Haag	1.0 - Approved	CIO	11/30/2012
Brian Murray	1.0 - Approved	ISO	12/04/2012
Steven McLeod	1.0 - Approved	Assoc. CIO	12/12/2012
Jenna Colvin	1.0 - Approved	Legal Representative	02/02/2013
IT Leadership	1.0 - Approved	Governance Review	02/06/2013
Jill Holman	1.0 - Approved	Internal Audit	02/26/2013

Distribution

Name	Location
Backup Copy	Dunlap Mathis Building, Rm. 132 (Fire Rated Safe)
Original Copy	D/M, Rm. 129 (CISO's Office)
Electronic Copy	https://my.ung.edu/departments/InfoSec/ (Secure Portal)

Document Properties

Item	Details
Document Title	Information Security Program Policy
Document Type	Policy – Internal/Operational
Author	Alfred Barker
Document Manager	Alfred Barker
Creation Date	11/26/2012
Last Updated	12/12/2012
Document Classification	Unrestricted

1.0 Executive Summary

As the Board of Regents of the University System of Georgia begins to standardize and guide the colleges and universities of the system to a more secure computing environment, the need of standardized documentation for the purpose of qualitative and quantitative assessments becomes ever apparent. In support of this effort, the University of North Georgia (the "University") shall strive to develop and maintain a comprehensive information security program to protect the confidentiality, integrity, and availability of information resources and to meet security requirements defined by USG/BOR policy, state and federal laws, and relevant contractual obligations.

In accordance with *Board of Regents Policy Manual Section, 11.3.1*, the University recognizes that information resources including confidential data are valuable assets that must be reasonably protected from unauthorized disclosure, modification, or destruction. The degree of protection needed is influenced by the nature of the resource, its intended use, and the associated risks. The University shall strive to create and maintain an internal information security technology infrastructure consisting of an information security organization and program that ensures confidentiality, availability, and integrity of the university system information assets.

This policy will outline the guidelines adopted by the Division of Information Technology (the "IT") to secure the computer and network resources of the University, recognize the requirements of the Board of Regents to standardize documentation, and establish the need for the existence of the *Information Security Program Plan* and all associated documents. This policy also establishes the understanding that it is appropriate for the IT to conduct risk assessments for establishing the existence of the required security documentation.

2.0 Governance / Compliance / Authority

To set the foundation for governance, the *Board of Regents Policy Manual, Section 11.3.3 Institutional Responsibilities* states the President of each institution shall be responsible for ensuring that appropriate and auditable information security controls are in place. In addition, the President and cabinet of each institution shall be responsible for defining institutional risk tolerance, security directives, and subsequent objectives; providing resources to meet defined security objectives; assigning and delegating information security management responsibilities; and shaping institutional culture in relation to defined security objectives. In addition, Section 5 of the Board of Regents *Information Technology Handbook* states that each USG institution must:

1. *Build an information security program;*
2. *Assign management responsibilities for information security program, including the appointment of an Information Security Officer (ISO);*
3. *Develop and maintain a computer/data incident management component;*
4. *Develop and maintain an information security and privacy policy and compliance management process;*
5. *Build, test, and maintain a "Continuity of Operations Plan" (C.O.O.P.) including:*
    - *Backup and Recovery Plan*
    - *Incident Management Plan*
        - *Note: It is our future intention to require that the C.O.O.P. include a "Disaster Recovery Plan" and a "Business Continuity Plan."*
6. *Establish and maintain an information technology and information security risk management program, including a risk assessment, analysis, planning mitigation, and monitoring process;*
7. *Maintain an annual information security awareness, and training component for all employees and contractors; and,*

8. Comply with USG reporting requirements."

In support of these requirements, the Chief Information Officer ("CIO") of the University shall be responsible for reviewing and providing initial approval of the information security plan; overseeing enforcement of institutional information security policies, standards, and baselines; and communicating to the President and presidential cabinet through the approved channels all reasonable information security risks, needs, deficiencies, as well as the overall state of campus information security controls.

In support of the CIO, the Chief Information Security Officer ("CISO") of the University shall:

- Oversee information resource risk assessment, review, and planning.
- Report identified risks and potential cost-viable solutions to the CIO.
- Develop the university's information security plan.
- Ensure the development of policies, procedures, and baselines in accord with security plan and executive directives.
- Oversee the management of enterprise technical security controls.
- Develop a security awareness program.
- Develop a security compliance program.
- Maintain awareness of emerging threats and vulnerabilities.
- Manage security incident response and review activities.
- Develop security metrics.

The University shall strive to conduct all business in accordance and compliance with all relevant Board of Regents policies, state laws, federal laws, and contractual obligations pertaining to the management and protection of information resources. These obligations shall include but not be limited to:

- Board of Regents Policy *BOR Policy Manual, Section 11 Information Technology(IT)*
- Board of Regents *Business Procedures Manual, Section 12 Protection and Security of Records*
- *PeachNet Acceptable Usage Policy*
- State of Georgia *Electronic Equipment Disposal Policy*
- Georgia Computer System Protection Act (O.C.G.A. § 16-9-90 & H.B. 1630)
- Electronic Communications Privacy Act (ECPA -18 U.S.C § 2510)
- Federal Family Educational Rights and Privacy Act (FERPA-20 U.S.C. § 1232g; 34 CFR Part 99)
- Gramm-Leach-Bliley Act Safeguards Rule (16 CFR 314)
- Health Insurance Portability and Accountability Act Security Rule (45 CFR Parts 160 and 165)
- Payment Card Industry Data Security Standard

IT developed this Plan/Policy/Program and is responsible for its management and administration. This Plan/Policy/Program has been approved by the President and Cabinet of the University.

Moreover, under this Plan/Policy/Program, IT is authorized to log computer and network usage, and to conduct risk assessments for creating the required security related documentation in support of protecting the University's computer and network resources.

3.0 Continuance

This policy may be reasonably modified at any time by the CIO/CISO of IT or the President and/or the cabinet of the University. This document replaces the *Information Security Program Policy* v1.1 (NGCSU-Revised 2008) and the *System Security Policy* v2.0 (GSC-Revised 2009).

4.0 Scope

This policy is binding and applies to all University employees, students, or affiliates located on but not limited to the facilities at Cumming, Dahlonega, Gainesville, and Oconee.

5.0 Requirements

5.0.1 - Standards and Best Practices

The development and maintenance of the University's information security infrastructure will be guided and informed by industry best practices and recognized standards. These shall include but not be limited to the National Institute of Standards and Technology (NIST) 800 Series. http://csrc.nist.gov/publications/PubsSPs.html .

5.0.2 - Security Principles/Roles

The responsibility to appropriately manage and protect information resources is shared by all members of the University community. To better communicate this responsibility, the University will strive to define security roles based on data access and management capabilities that a position or relationship may reasonably require, for example data owners, data stewards, and data custodians. Each security role shall have a set of specific requirements and expectations, which relate to the individual or organization. Additional training, agreements, or legal contracts shall be extended where applicable to ensure common understanding of these expectations and responsibilities.

It is recommended that the personnel responsible for the security of the computer and network resources as described by this policy be categorized in three roles: the Primary Contact, the Secondary Contact, and the Documents Manager – the assignment may be located within the *Communications Plan* and Information Technology's *Contact List.*

5.0.3 - Information Security Program Plan

In accordance with *Board of Regents Policy Manual, Section 11.3.3* and the *USG Institution Information Security Plan Reporting Standard*, the University shall develop, implement, and maintain an overall information security plan that is consistent with the requirements and guidelines provided by the University System of Georgia's Office of Information Security & ePrivacy. The University's responsibilities are to compile for submission to the CISO of USG's Office of Information Security & ePrivacy, the *Information Security Program Report ("ISPR").* This report is due on March 31 annually, and specific instructions for creating and submitting the report can be at located at the following website: http://www.usg.edu/infosec .

5.0.4 - Risk Management

Because it is financially and technically impossible to achieve complete security of information resources, information security is fundamentally a risk management activity by which an acceptable/reasonable balance of preventive controls resulting in residual risk is sought. To facilitate the review and implementation of balanced and cost-effective controls to protect information resources, it is recommended that the University undertake a formal iterative risk management process that includes at minimum the following steps:

- Identification and inventory of institutional information resources and assets;
- Classification of resources according to projected or empirically derived losses associated with frequency, exposure, alteration, loss, or impact;
- Defining threats that are relevant to individual assets or classes of assets; and
- Recommending and implementing controls to protect UNG's information assets from identified threats.

It is recommended that information assets of higher value have more preventive controls deployed to protect them; whereas, information assets of lesser value have fewer attached security controls.

5.0.5 - Policies, Procedures, and Baselines

As part of the information security infrastructure, it is recommended that the University develop, maintain, enact, and enforce institutional policies, procedures, and baselines that address key areas relevant to the management and security of information resources. These areas shall include but not be limited to information systems usage, antivirus, data management and access, electronic information sanitization,

firewall and network filtering, incident response, minimum security for networked devices, password management, risk management, and secure wireless access.

5.0.6 – Data Protection

It is preferred that selected files (such as records containing social security numbers, credit card numbers and other sensitive information) be encrypted in storage and in transit in accordance with security best practices. In addition, a preferred control furthering the protection of data is a reasonable backup and recovery strategy to mitigate loss or disaster. The University strives to develop and manage such policies and plans.

5.0.7 - Access Control

Maintaining and controlling access to systems, services, and other information resources is a critical component of the overall information security plan. To ensure that access control objectives are met, the University will develop reasonable policies and procedures to address the following areas at minimum including data classification, user management, authentication, event logging, and intrusion detection/prevention.

5.0.8 - Network Security

The condition and configuration of network devices such as servers, workstations, routers, switches, access points, and firewalls can play a pivotal role in the overall protection of information resources. For this reason, the University shall strive to develop, maintain and mature reasonable configuration standards and network security controls to safeguard information resources from internal and external network mediated threats.

5.0.9 - Physical Security

The condition and monitoring of the physical environment in which information assets are stored or transmitted (i.e. a server room or switching closet) is foundationally important in the overall protection of information resources. Recognizing this, it is recommended that the University develop reasonable policies, procedures, and guidelines to address the following key areas at minimum include environmental conditioning and monitoring; fire prevention, detection, and suppression, keys and locking systems; physical intrusion detection and alarms; and oversight of third party access.

5.0.10 - Information Disposition

In support of the State of Georgia's DOAS *Electronic Equipment Disposal Policy*, the University acknowledges the importance of sanitizing and removing information from media when storage is no longer required. To accomplish this, the University shall develop and maintain reasonable policies, procedures, and guidelines concerning the disposition of information storage mediums.

5.0.11 - Incident Response

In accordance with *Board of Regents Policy Manual, Section 11.3.3*, the University shall follow clear procedures for handling and reporting information security incidents. These procedures shall include reporting of incidents to the CISO, USG System Office in a timely manner. The procedures shall be documented within the information security plan. In addition, in accordance with Section 5 of the Board of Regents *Information Technology Handbook*, each institution is responsible for the development and implementation of a reasonable incident response management plan. The University shall strive to develop and maintain such a plan in support of this requirement.

5.0.12 - Disaster Recovery

The University recognizes the importance of contingency planning and preparedness concerning actualized threats to information resources as referenced in Section 5 of the Board of Regents *Information Technology Handbook*. In such occurrences, the safety of University students and faculty/staff are of primary concern followed by objectives for the resumption of business and minimization of loss. To support this requirement, the University has made efforts to reasonably compile and publish internally an Information Technology *Disaster Recovery Plan* and an Information Technology *Business Continuity Plan*.

5.0.13 - Personnel Security/Awareness and Education

Personnel security's foundation hinges on having qualified and trustworthy employees who are empowered to access and manage information resources. To accomplish this, the University's Human Resources Department has policies in place to address the following key areas to include pre-employment background checks and user de-provisioning. In accordance with *Board of Regents Policy Manual, Section 11.3.3*, the University recognizes that user education is a vital part of information security. Therefore, the University shall include in its information security plan methods for ensuring that information regarding applicable laws, regulations, guidelines, and policies is distributed and readily available to our employees, students, and affiliates.

6.0 Enforcement/Sanctions

It is recommended that employees, students and affiliates be informed of what constitutes appropriate use of the university's information technology resources. To support this recommendation, the *Appropriate Usage Policy* strives to define the standards of appropriate conduct.

Failure to comply with this and all other IT policies may result in revocation of privileges and/or actions as specified in the University's Human Resources *Progressive Disciplinary Policy*. IT is not responsible for issuance of sanctions.

7.0 Responsibilities/Review

All compliance, documentation, enforcement and maintenance of this policy are the responsibility of IT and are stored within IT's fire-rated safe, online within the University's secure portal, and in working form within the office of the CISO. This policy is to be used to establish the need of and the authority to create and manage the *Information Systems Security Plan* and all associated plans, policies, and procedure documents, as well as conduct risk assessments for the purpose of the security documentation.

It is recommended that the content and execution of this policy be audited at a minimum by the CISO annually, at which time this policy may be updated as appropriate.