

NOVA SOUTHEASTERN UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGIES

**INFORMATION SECURITY POLICY
AND PROCEDURE
COMPILATION**

March 2005

(revision of April 2007)

Index

Index.....	2
Rationale.....	4
Review and Approval	4
Purpose.....	5
Goal.....	5
Policy.....	5
Scope.....	5
Related Policies.....	6
Technology Policy Web Site	6

Acceptable Use of Computing Resources	7
Access to Systems:	
Authorized Users.....	7
Administrative Systems Access (Banner, etc.)	7
NSU Email Account.....	8
WebStar	8
Backup and Recovery.....	9
Contracts and Agreements.....	10
Data:	
Aggregate Data.....	10
Critical Data	10
Employee Information.....	10
FERPA.....	10
GLBA	11
HIPAA.....	11
Identify Theft	11
Ownership, Data Management and Accountability	12
Sensitive Data.....	12
Delegation of Responsibility – Networks.....	12
Delegation of Responsibility - Systems	12
Disposal of Stored Data/Documents	13
Disposal of Technology Equipment and Media Equipment..	13
Documentation: Systems, Network, and Software	13
Executable Web Content Management	14
Mass Distribution of Email.....	14
Networks -Video Over IP.....	14
Networks – Wireless	14
Physical Security of Equipment:	
DataCenter	15
Data Closets	15
Desktops, Laptops, Peripherals	15
Desktops/Workstations	15
Purchase Requests.....	16

Risk Management	16
Sanctions.....	16
Security Breaches or Suspicious Activity	17
SPAM and Virus Filters (Network)	17
Subpoenas.....	17
Vendors.....	18
- - - - -	
Appendix A - Relevant Links	19
Appendix B - Sample Policy Template.....	20
Acknowledgements	21

Rationale

Nova Southeastern University (NSU or the University) is responsible for developing, implementing, maintaining, and enforcing appropriate security procedures to ensure the integrity of institutional information, and for imposing appropriate penalties for substantiated violations.

The University maintains and periodically reviews the collection of technology policies that define acceptable information security policies and practices. Collectively, these policies specify security procedures for information processing and distribution, information storage and retrieval, and computing and networking systems throughout the University. A formal process is in place for the review and approval of all technology policies by the Office of the President; once approved, the policy is forwarded to and retained by the Office of the Vice President for Research, Planning and Governmental Affairs.

The Information Security Policy and Procedure Compilation serves as a comprehensive reference document of all University technology policies and procedures.

Review and Approval of the NSU Information Security Policy and Procedure Compilation:

ITPC Policy Subcommittee, Chair

Vice President for Information Technologies Approved s/ Virginia McLain 3/10/05
Virginia McLain Date

Vice President for Academic Affairs Approved s/ Frank DePiano 4/26/05
Frank DePiano, Ph.D. Date

Executive Vice President for Administration Approved s/ George Hanbury 4/26/05
George Hanbury, Ph.D. Date

President Approved s/ Ray Ferrero, Jr. 4/27/05
Ray Ferrero, Jr., J.D. Date

Purpose

To support the University mission of teaching, learning, and research, regardless of geographic location, NSU is committed to providing secure, yet open networks and systems that protect the integrity and confidentiality of information and data. The NSU Office of Information Technologies and Digital Media (OIT) is charged with providing the University community with the technological resources to deliver and support these commitments.

Goal

The goal in establishing NSU's Information Security Policy and Procedure Compilation is to ensure that the confidentiality, integrity, and availability of each piece of information owned by, or entrusted to NSU is protected in a manner consistent with the value attributed to it by the University as determined by appropriate risk management strategies.

Policy

Each member of the NSU community is responsible for the security and protection of electronic information resources. Resources to be protected include networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized incursions, malicious use, or inadvertent compromise. Electronic information activities outsourced by contract to non-NSU entities must comply with the same security requirements as the University.

The Office of Information Technologies maintains procedures to support security policies when alleged violations from internal or external threats, unauthorized incursions, malicious use, or inadvertent compromise are suspected. OIT responds to written requests for information only from the President's Office, the office of Human Resources and the department of Public Safety. Information gathered by OIT in response to an authorized request is provided by OIT only to those authorized units. OIT does not report or provide information to any external agency unless authorized to do so by appropriate University representatives. In the event of a subpoena, OIT will respond at the direction of Legal Affairs.

Scope

The NSU Information Security Policy and Procedure Compilation provides guidelines for the use of the University's computing resources. The policies apply to all users of the University's computing resources, including students, faculty, staff, alumni, and authorized guests. Computing resources include all computers, related equipment, software, data, and local area networks for which the University is

responsible, as well as networks throughout the world to which the University provides computer access.

Academic units of NSU may have in place unit-level information policies, procedures, and technology plans, designed to address their units' particular issues. The NSU Information Security Policy and Procedures Compilation provides that such units may develop their own unit-specific policies and procedures. However, all unit-level policies and procedures are subordinate to the main University policies and procedures contained in the NSU Information Security Policy and Procedures Compilation.

Related Policies

In addition to the policies contained in the NSU Information Security Policy and Procedure Compilation, usage and access to all NSU systems and networks must be in accordance with all other NSU policies and applicable state and federal laws. Among the more important laws are the Florida Computer Crimes Act, the Federal Computer Fraud and Abuse Act of 1984 (revised in 1994), the Federal Electronic Communications Privacy Act (1986), the U.S. Copyright Act, the Technology, Education, and Copyright Harmonization Act enacted in 2002. Copies of these laws and the NSU Copyright Policy may be examined in the Office of the Vice President for Academic Affairs.

Additional and/or modified policies and procedures that address early childhood, preschool, and K-12 concerns are in place for the students, parents, faculty, and staff of the University School of Nova Southeastern University and the Mailman Segal Institute for Early Childhood Studies. However, these policies and procedures are subordinate to the main University policies and procedures contained in the NSU Information Security Policy and Procedures Compilation.

Technology Policy Website

The Information Security Policy and Procedures Compilation is posted on the NSU web at <http://www.nova.edu/common-lib/policies/>. The Compilation is dynamic in nature; as new policies and procedures are approved and existing policies are revised, they will be posted on the Compilation website.

Acceptable Use of Computing Resources

The NSU policy on Acceptable Use of Computing Resources is comprehensive, yet dynamic in nature, and covers such activities as violation of copyright laws, denial of service attacks, decoding access control information, attempts to circumvent security, IP spoofing, unauthorized monitoring of electronic communications, creating and propagating viruses, spamming, port scanning, disrupting services, damaging files, and intentional destruction of or damage to equipment, software, or data. The NSU policy on Acceptable Use of Computing Resources clearly states that “the computing resources of Nova Southeastern University are intended to be used for its programs of instruction and research and to conduct the legitimate business of the University.”

Access to Systems:

Authorized Users

Authorized user access to NSU networks and systems is a privilege, not a right. Authorized users include current students, faculty, staff, alumni and guests of the University; individuals connecting to public information services; others whose access furthers the mission of the University, and whose usage does not interfere with other authorized users’ access to resources. A user must be specifically authorized to use a particular computing or network resource. Access to networks and computer systems owned or operated by NSU require certain user responsibilities and obligations and, is subject to University policies and local, state, and federal laws. See specifically the NSU *Policy on Acceptable Use of Computing Resources*.

The University administrative system, SunGard SCT Banner (Banner), maintains official status codes for all students and employees. As long as the Banner system recognizes a student or employee as having an “active” status, their access to NSU computing resources remains enabled. Examples of NSU computing resources requiring secure access include electronic mail, academic computing applications, electronic library, library patron services, NSU campus card, campus parking, and pay-for-print allocation.

Administrative Systems Access – (Banner, etc.)

Formal application processes are in place for access to all University mission critical administrative systems. Access is based on a need-to-know basis and must be directly related to a user’s defined job description. Access Request Forms require multiple sign-offs: the individual applicant requesting access; the applicant's immediate supervisor; the account coordinator for the department, school, college or center; followed by the signature of the coordinator for the functional-user department who assigns required permissions. Once the process is complete, the

signed form is forwarded to an OIT Security Administrator who verifies the request and activates access to the requested system.

Employee administrative accounts remain active until an OIT Security Administrator is notified in writing by the Office of Human Resources to terminate and/or suspend an employee's accounts.

University Computer Account (NSU Email Account)

The University requires all students, faculty, and staff to hold and regularly maintain one official University-assigned computer account that is used to access major computing resources, including electronic mail. This University-assigned computer account corresponds directly to an NSU email addresses.

New students and employees are directed to use a web-based application to create their own accounts electronically. In order for an account to be activated, all students and employees are required to accept the terms and conditions set forth in the NSU Computing Account Security Policy Agreement. The new user accepts the agreement by clicking on the "submit" button indicating that the user has read and understood the rules for using NSU's computing systems and agrees to abide by them.

All official electronic mail communications directed to NSU students, faculty, and staff will be sent exclusively to NSU-assigned computer accounts to ensure timely and accurate delivery of information. NSU students may forward their NSU generated email to external locations, but do so at their own risk.

Student computer accounts, except under extenuating circumstances when access may be limited or suspended, remain active from the time of acceptance in an academic program to the time the student leaves the University. Employee computer accounts remain active until OIT is notified in writing by the Office of Human Resources to terminate and/or suspend an employee's account. In all cases, student and/or employee, the contents of University computer accounts are electronically archived before being deactivated.

Requests for an online guest account must be submitted for approval using the NSU Guest Account Request Form, signed off by an appropriate official representative of a school, college, center or program, and forwarded to OIT for activation. The guest accounts are activated for a predetermined period of time, and are established with restricted and limited access to NSU services.

Access to WebStar

Web for Student access is based on active student status in the Banner system. Students are assigned a Personal Identification Number (PIN) to use for access to

WebStar for services such as online course registration, credit card payments, financial aid status, Bursar information, unofficial transcripts, grades, and other student online services.

Web for Employee access is based on employee status in the Banner. Employees can access personnel records including salary information, vacation, personal leave, etc., using the assigned PIN for WebStar. If an employee also has student status, any required student permissions are added to the single PIN access.

Web for Faculty access is based on faculty status in Banner and course assignments. Faculty access is expanded from Web for Employee access to include class schedules, rosters, and grades. Access is obtained with the assigned PIN used for access to WebStar. If the faculty member is also a student, any required student permissions are added to the single PIN access.

Backup and Recovery

As outlined in specific operating procedures manuals, backup procedures for systems and data housed in the University DataCenter must be performed according to the schedule and the processes defined by the OIT System Administrators responsible for the NSU administrative and academic mission critical systems. In the event of an emergency, such as a hurricane, University procedures will be followed as defined in the NSU Public Safety Emergency Operations Procedures for Hurricanes and Other Severe Weather Conditions (contact NSU Public Safety Department to obtain a copy). OIT is charged with protecting the integrity of NSU data, and is responsible for all final decisions concerning emergency procedures, processes, safety, and security for systems, networks, and data. OIT works collaboratively with NSU Public Safety and NSU Facilities Management in the decision making process.

OIT facilitates backup services for NSU schools, colleges, centers, and departments requiring backup assistance, including the use of secure off-site storage facilities that provide courier service with pickup and delivery. Service is available by contacting OIT Technical Support Services (954) 262-4900.

Remote backup “host” sites are maintained by NSU with OIT having the responsibility for networks, systems, and personnel assigned to maintain and administer the remote site systems. During regularly scheduled backups, access to the NSU Banner system is not available. In the event of a major disaster that would necessitate taking down the main NSU DataCenter systems, the remote site would be activated. Real-time service and access could possibly take up to two weeks to restore from the backup site, depending on the extent of damage incurred.

Contracts and Agreements --Technology

All contracts and agreements for technology, including hardware, software and/or consulting services, negotiated by the University are submitted by OIT to the NSU Vice President for Legal Affairs for review and approval.

Data:

Aggregate Data

The University authorizes users to analyze and aggregate institutional data. However, official University published reports that include such aggregate data may only be used with the review and approval of the appropriate information provider, specifically the NSU Office of Research, Planning and Governmental Affairs and/or the NSU Executive Office. In addition, the University prohibits sharing aggregate institutional data with individuals or organizations for which the reports are not primarily intended and requires the permission of the NSU Executive Office and/or the individual or office primarily responsible for the generation of the report.

Critical Data

NSU defines critical data as information that is vital to the mission and function of the University, the loss of which would have an unacceptable impact. The data deemed critical are: student records including all instances of Banner; EPS imaging; academic history; legacy; athletics; financial aid; finance and accounting records; human resources and personnel records; payroll and budget records; clinic patient information; and all academic online coursework.

Employee Information

University policy provides that all external requests for information, status, or recommendations concerning current or former employees must be referred to the NSU Office of Human Resources.

Family and Educational Rights and Privacy Act - FERPA

Policies concerning public disclosure of information regarding students and former students are defined by the Family and Educational Rights and Privacy Act (FERPA). Restrictions imposed on the release of information include requests by telephone, email, in writing, or direct disclosure to a third party. While FERPA generally prohibits disclosure of information regarding current and former students, FERPA does allow for the public disclosure of certain "directory information" that may be shared with the general public. Questions regarding NSU policies concerning release of such information, and all questions pertaining to clarification

of disclosure of student or former student information must be referred to the Office of Student Financial Services and Registration or to the Office of the Vice President for Academic Affairs prior to the release or disclosure of any student information.

Gramm, Leach-Bliley Act – GLBA

NSU has a written information security program in place to comply with The Financial Services Modernization Act of 1999 also known as the Gramm Leach-Bliley Act (GLBA). The security program is designed to (i) ensure the security, integrity and confidentiality of Non-public Personal Information (as defined in GLBA), (ii) protect against any anticipated threats or hazards to the security or integrity of such information; and, (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to the person that is the subject of such information. All questions regarding GLBA should be referred to the Associate Vice President for Student Financial Services and Registration, the coordinator of the University’s GLBA program.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

NSU is committed to complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regarding the security of electronic protected health information (EPHI). These regulations are commonly known as the HIPAA Security Regulations. “Protected health information” is any information that (a) is created or received by a provider and relates to the past, present or future physical or mental health condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; and (b) either identifies the individual or could reasonably be used to identify an individual. Specific information is contained in the University’s HIPAA Security Policies and Procedures document. Any questions, requests for information, clarification, or reporting of alleged violations should be directed to the University’s Corporate Compliance Department by calling the HIPAA Hotline (954) 262-4302.

“Identity Theft”

Recognizing that “Identify Theft” is a serious and growing problem, NSU requires that extra precautions be taken when collecting, using, and storing non-public “personally identifiable” information, such as: Social Security Number; date of birth; place of birth; mother’s maiden name; credit card numbers; bank account numbers; income tax records; and driver’s license numbers. Collection of this identifying information must be limited to situations where there is a legitimate business need and there is no reasonable alternative available. Access to such information will only be granted to authorized University staff on-a need-to-know basis.

Ownership, Data Management, and Accountability

NSU is the legal owner of all University data, and the University retains the exclusive right to and use of all computer assets, including data content.

Sensitive Data

Much of the data collected and managed at NSU is sensitive or confidential. Sensitive information is confidential by law and requires protection from unauthorized access. OIT security procedures ensure that computer files are accessed only by authorized personnel as required in the performance of their duties. In the case of computer generated reports or other hardcopy documents that contain sensitive information, all departments must develop procedures to provide an auditable chain of custody. Extreme care must be exercised in the disposition of printed materials containing sensitive data. Data must not be released to persons unaffiliated with NSU without proper University written authorization.

Delegation of Responsibility - Networks

Oversight for network security, wired or wireless, is assigned to the NSU Information Systems Security Officer (the Vice President for Information Technologies) who serves by appointment of the President of the University.

University network policy provides that all requests for NSU network services must be directed to OIT for evaluation, approval, design, and implementation. Network services encompass all forms of electronic data-flow within the University local-area networks, within the University wide-area network (WAN), and between the University WAN and all external networks (e.g. the Internet). The responsibility for the equipment, systems, and the security necessary to ensure the reliable flow of data, resides with OIT Network Operations. Written requests must be submitted to OIT for any change to existing services. These changes include, but are not limited to, adding new data lines, connecting or disconnecting equipment to the network, changes in network security, and changes to/from network protocol services.

Delegation of Responsibility - Systems

Responsibility for oversight of information technology security policies is assigned to the NSU Information Systems Security Officer. In addition, security officers within OIT, with appropriately defined job descriptions, include System Administrators, Database Administrators, Computer Operators, Network Security Technicians, Quality Assurance Administrators, Security Administrators, and the managers and directors of these units.

OIT System Administrators have custodial responsibility for all academic and administrative systems. OIT Database Administrators have custodial responsibility for all production and development data contained within OIT database management systems, including the University's centralized Banner database management system. OIT Computer Operators have custodial responsibility for implementing, monitoring, and coordinating procedures for accessing all test data files and production manager processing.

Disposal of Stored Data/Documents

The University requires that hard-copies or physical documents containing information that is considered by the University and/or by government FERPA, HIPAA, and GLBA as "sensitive" and/or "critical" must be shredded using a University-approved device or the services of an approved contract shredding facilitator prior to being discarded.

Disposal of Technology and Media Equipment

The University Surplus Property and Equipment Policy requires that the Office of Financial Operations, Fixed Assets department, must approve and process the disposal and/or resale of all University property, including furniture, fixtures, and technology equipment. Disposal and/or resale will be carried out according to the procedures as outlined in the current Property Control Manual. (See Fixed Assets' department website: [Surplus Property and Equipment Policy](#))

In addition, NSU requires that any computer hard drive or removable magnetic medium, such as a diskette, magnetic tape, Zip drive, flash memory, etc. that has been used to store any kind of critical, sensitive or confidential information, as defined in previous paragraphs, must be electronically "cleaned." An OIT approved cleaning process must be used prior to the item being discarded or transferred to another system or to any individual or entity not authorized to receive or view such information. Any non-erasable medium, such as a CD, optical disk, etc. used to hold critical, sensitive or confidential information must be physically destroyed before being discarded.

Documentation - System, Network, and Software

It is the responsibility of OIT to maintain and update all documentation for University academic and administrative systems and networks through the life-cycle of the systems and networks. Documentation of critical and sensitive administrative and academic systems includes: the process; system description, design, architecture; data, database design and dictionary; programming logic, programmer notes; operational procedures and help. Network diagrams and schematics must be

documented for both wired and wireless networks with specific network architecture and configuration.

Executable Web Content Management

The NSU Executable Web Content Policy provides that all requests for installation of web-based programs containing executable content, such as Common Gateway Interface programs, must be directed to OIT for evaluation, approval, installation and implementation. Once approved, requests will be implemented and maintained by OIT.

Mass Distribution of Email

The University maintains a means for mass distribution of email; all requests for mass distribution of electronic mail messages to NSU students, faculty, or staff must be submitted in electronic format to the Office of the President for approval. The Office of Public Affairs has been assigned the responsibility for coordinating such requests with OIT. Approved messages will be distributed to the recipient group(s) by OIT in a timely manner. Message distribution requests must include the text of the message, an appropriate email subject line, and a list of the intended recipients and/or group(s).

NSU schools, colleges, and centers, using students' University-assigned accounts, may distribute mass electronic mail without submitting the request to the Office of the President. However, the distribution is limited to students attending that particular school, college, or center. In addition, the schools, colleges, and centers must work collaboratively with OIT in distributing the email to ensure the proper load balancing of systems and networks during the distribution.

Networks -Video over IP

NSU schools, colleges, and centers, must coordinate all initiatives to deliver video over IP with OIT to pre-determine and validate the impact of distributed video over the NSU network infrastructure. OIT Network Operations must conduct tests and evaluate the use of resources in order to provide the equitable and proper load balancing of University systems and networks.

Networks - Wireless

The University wireless policy provides that no wireless access points are to be installed on the NSU network, or within any NSU facility, without the express written permission of OIT Network Operations, and all wireless access points operating on the NSU network are to be installed, configured, and maintained by OIT Network Operations. The testing of new or emerging wireless technologies, or the demonstration of wireless products, must be coordinated through OIT Network

Operations. The University wireless policy provides OIT the right to remove or disable any device that is in violation of the wireless policy.

Physical Security of Equipment:

DataCenter

The NSU DataCenter is located in a restricted area with access to such DataCenter and to the adjacent areas controlled by NSU secure card access. (Visitors to the DataCenter are allowed with an appropriate OIT-escort after they receive clearance at the OIT reception area.) Camera views provide visual identification of all visitors to the OIT reception area. All construction, fire suppression systems, air conditioning, uninterrupted power sources, emergency generators, and power requirements are designed, evaluated, and purchased through collaborative review by Facilities Management and the appropriate OIT teams.

Data Closets

Data closets are located in most University facilities; at student educational centers, leased locations, and wherever connectivity to the NSU infrastructure is required. The data network and telecommunication equipment housed in the data closets are considered mission critical and require a high level of security; access to all data closets is restricted to NSU Telecommunication staff and OIT staff. OIT and Telecommunications work collaboratively with Facilities Management to ensure that proper construction of and security standards for all data closets are met.

Desktops, Laptops, Peripherals

NSU requires the use of physical locking devices as recommended by the Public Safety Department for desktop, laptop and peripheral devices. For desktop computers and printers, OIT's standard locking cable (Secure-It) is recommended. For laptop computers, a cable lock is to be used to secure the laptop and "docking station" (port replicate base) to the office desk to prevent theft. This lock can be secured to OIT's standard locking cable (Secure-It). As part of the above locking method, it is recommended that using the docking station or laptop port that includes a "metal shroud" is the preferred method of locking the laptop.

Desktops/Workstations

All individuals with access to a University-owned desktop or workstation must establish and use an appropriate username and password to log in to his or her workstation. Each University-owned workstation should have a screensaver enabled that will automatically activate and require a password before further use if the workstation is idle for more than 15 minutes. To prevent the loss of work in progress, users are encouraged to activate timed-backup features (set for less than 10

minutes) where available so that such work is automatically saved before any automatic log-off can occur.

Additionally, OIT operates several system-level applications including antivirus software, spyware/pop-up blocker software, and software update utilities designed to protect the workstation from computer viruses and malicious attacks from the Internet. Users should not disable or interfere in any way with the operation of these applications. OIT provides access to the system-level applications through the technical support units located at individual schools, colleges, and centers throughout the University.

Purchase Requests

All requests and/or purchase orders for technology purchases, including hardware, software, and peripherals, must be submitted to OIT for approval prior to a purchase order being issued by the Purchasing Department. OIT does not control the budget dollars nor authorize the expenditure of funds; it works with the functional users to determine and define appropriate technology to meet a stated purpose. OIT verifies the compatibility, configuration, and data storage requirements, and to ensure that all requirements for security and compatibility with the University's technology infrastructure are met in a cost-effective and appropriate manner.

Software licenses must be purchased before software is installed, copied, or used on University computer resources. The number of concurrent users must be in accordance with software license agreements and strictly adhered. OIT purchases University-wide licenses in some cases, and arranges appropriate distribution of the licensed materials.

Risk Management

NSU, being mindful of the expanding use of computers, increasing software sophistication, the explosive growth of the Internet, World Wide Web, and web-oriented applications, mandates that appropriate controls must be employed to protect physical access to resources commensurate with the identified level of acceptable risk. Risk management, the process of analyzing exposure to risk and determining how to best handle such exposure, necessitates that risk analysis and security measures must be applied to all administrative and academic systems residing in the NSU DataCenter as well as to distributed data locations.

Sanctions

NSU may impose sanctions and punishments on those who violate the policies of the University regarding the use of computer and network resources. Inappropriate conduct and violations of University policies will be addressed by the appropriate procedures and University officials. In cases where a user violates any of the terms

of a policy, the University may, in addition to other remedies, temporarily or permanently deny access to any and all NSU computing resources, and appropriate disciplinary actions may be taken, up to and including dismissal or termination.

Security Breaches or Suspicious Activity

Any member of the University community who comes across any evidence of information, data, systems, or a business process being compromised or who detects any suspicious activity that could potentially expose, corrupt or destroy information, systems, or networks, must immediately report such information to the Office of Public Safety and/or the Office of Human Resources. It is emphasized that no one should take on the responsibility of investigating the matter further without the authorization of an appropriate University administrator. In the event of an alleged business process being compromised, the Office of Human Resources may include the Internal Auditing Department in the investigation process.

Spam and Virus Filters (Network)

NSU is concerned with the negative impact of Spam, electronic “junk” mail, on networks and systems. OIT actively addresses the problem on a multi-level basis, including Network Operations’ central management online Email Scanning System (<http://splog.nova.edu>). Students, faculty, and staff are provided this site to modify their user preferences to decrease the amount of Spam delivered to their accounts or to review their spam or virus filter log files. The spam filter deletes any message with a spam rank higher than the user defined “maximum hits” threshold.

In addition, Network Operations provides and maintains a dynamic virus identification system website for University technical support personnel to use for the purpose of identifying infected or compromised systems. By identifying locations, technicians can quickly remedy the situation. If infected systems are not cleaned and restored in a timely manner, Network Operations removes the compromised systems from the University’s network.

Subpoenas

Data collection of information for any individual including students, faculty, staff, alumni, parents, guardians, spouses, children, donors, beneficiaries, etc., may be subpoenaed and entered into the public record of a court case. Appropriate discretion should therefore be exercised in the creation or the drafting of any document or data that will be stored in any University file. Employees who receive investigative subpoenas, court orders or other compulsory requests from law enforcement agencies requiring the disclosure of University-held information, should immediately contact the Office of Human Resources before responding or taking any action. The Office of Human Resources will notify University legal counsel if necessary.

Vendors

Agreements to provide third party vendors access to NSU systems and data must ensure that such vendors are subject to the same obligations of confidentiality as the University. Agreements with vendors must enable the University to comply with its obligations under all applicable privacy laws, and the vendors must be contractually obligated to implement data protection and security measures that are in compliance with all University practices. NSU employees must adhere to non-disclosure agreements with third party providers, and must refrain from disclosing information entrusted to the NSU employees by the third party providers.

It is the practice of the University to prohibit the transfer and storage of University data by or to third party vendors or to conduct the business of the University on third party servers. Wherever possible, all NSU systems and data will be housed, operated, managed, and supported internally by the University. OIT evaluates all requests for the use of third party vendors or applications service provider systems. Except in extenuating circumstances and when it will not compromise the integrity of the data, systems will remain in-house.

Systems that are recommended for purchase to facilitate the business and/or academic functions of NSU must have the capacity and capability to interface with the University's central administrative and/or academic systems, i.e. Banner, WebCT, TouchNet, etc. The interfaces can be developed either in-house by OIT staff, or developed by an outside vendor. The vendor must execute a non-disclosure agreement with the licensed system provider, i.e., Banner, WebCT, TouchNet, etc. NSU will not release information containing the data dictionary of a licensed administrative or academic system to a third party without written permission from the owner of the license.

Appendix A

Links to Individual NSU Technology Policies:

<http://www.nova.edu/common-lib/policies/>

- [Acceptable Use of Computing Resources](#)
- [Assuring Prompt Assignment of UNIX Accounts](#)
- [Computer Systems Data Access](#)
- [Computing Account Security](#)
- [Copyright and Patent](#)
- [Electronic Mail Communications](#)
- [Executable Web Content Management](#)
- [Mass Electronic Mail Distribution](#)
- [Network Connectivity Management](#)
- [NSU Web Style Resources](#)
- [NSU Wireless Information Network and Global Services \(NSU WINGS\)](#)
- [Obtaining Internet Access](#)
- [NSU Campus Card - Pay-for-Print](#)
- [Responsibility for University Web Site](#)
- [Use of Material in Web Pages](#)
- [World Wide Web Pages](#)

Links to NSU Guides and Agreements

- [NSU's CWIS Information Provider Agreement](#)
- [NSU's Mass Email Information Provider Agreement](#)

Links to Social Security Number Information

- [Computer Professional for Social Responsibility- FAQ](#)
- [Social Security Administration - Your Number And Card](#)
- [Social Security Administration - Identity Theft](#)
- [Privacy Rights - Your Social Security Number](#)
- [Network USA - Social Security Number FAQ](#)

Link to the Privacy Act of 1974

- [Text of Privacy Act of 1974 \(Department of Justice Site\)](#)

Links to Family and Educational Rights and Privacy Act of 1974 (FERPA)

- [Text and Regulations \(Department of Education Site on FERPA\)](#)
- [Electronic Privacy Information Center - Privacy of Education Records](#)

Links to Identity Theft Information

- [US Government's identity theft website](#)
- [A variety of resources pertaining to identity theft](#)
- [Gryphon Foundation newsletter on identity theft](#)

Appendix B Nova Southeastern University

University Policy

Administrative Area(s): Administration/Academic Centers/Technology

Applicability: University-wide

Scope: NSU Wireless Information Network and Global Services (NSUWINGS)

Rationale: Nova Southeastern University through the Office of Information Technologies (OIT) manages a wireless network infrastructure that is compliant with the IEEE 802.11b wireless Ethernet standard, and, is intended to remain current with all future wireless Ethernet standards upgrades. The purpose of the wireless infrastructure is to provide students and faculty with dependable, high-speed mobile computing while on the campuses and Student Centers of the university. The NSU wireless systems uses the unlicensed 2.4GHz frequency spectrum reserved for industrial, scientific, and medical use. To ensure the security, integrity and performance of the NSU wireless network, the following policy must be observed:

Information Technology Policy: March 18, 2002

No wireless access points are to be installed on the NSU network or within any NSU facility without the express written permission of the Office of Information Technologies (OIT) Network Services. All wireless access points operating on the NSU network are to be installed, configured, and maintained by OIT Network Services. Unauthorized wireless devices using the same frequency spectrum as 802.11b (2.4 GHz) or 802.11a (5 GHz) should not be used within any NSU facility. Private 802.11b wireless networks (ad-hoc mode) are not permitted within any NSU facility. The testing of new or emerging wireless technologies or the demonstration of wireless products must be coordinated through OIT Network Services. Request for special wireless installations or suspension of the MAC address authentication system should be submitted in writing to OIT Network Services (nunet@nova.edu) for approval. OIT retains the right to remove or disable any device that is in violation of this policy.

Review by ITPC Policy Subcommittee: Approved _____

Vice President for Academic Affairs: Approved _____

Executive Vice President for Administration: Approved _____

President: Approved _____

Ray Ferrero, Jr.,

Acknowledgements

Nova Southeastern University HIPAA Security Manual

Nova Southeastern University GLB Information Security Program

Princeton University, Information Security Policy, May 21, 2004

University of California-Berkeley, IT Campus Information Technology Security Policy, revision of 2004-01-09

Georgia Institute of Technology, Information Security Policy, June 6, 2001

Florida State University, revision of June 14, 2002

Purdue University, July 12, 2004