NETWORK AND DATA SECURITY POLICY

07.300

Authority:	Board of Trustees
History:	Approved by the Board of Trustees August 3, 2007; revised July 18, 2007; reformatted May 25, 2005; approved by the Board of Trustees October 28, 2004; effective October 28, 2004.
Source of Authority:	Consolidated University of North Carolina Netstudy – Security Subcommittee Baseline Recommendations (Feb. 16, 2003); International Standard ISO17799
Related Links:	
Responsible Office:	Information Technology Systems Division

I. Introduction/Purpose

This document provides the guidelines to establish a security framework to protect the university networks, computing systems and data. Through this policy, the university will encourage the application of industry-wide best practices to assure that:

A. Confidentiality, availability and integrity of university institutional data will be maintained at all times.

B. Stewardship and custodial responsibility of all university institutional data will be defined and that data owners and custodians identify and protect such data in accordance with State and Federal laws and regulations.

C. The level of security applied to networks, systems and data is appropriate for the level of risk associated with disclosure, corruption, improper modification or loss of university institutional data.

II. Scope/Coverage

This policy applies to each administrator or user of the university's networks and computers (enterprise servers, departmental servers, desktops and mobile computing devices). Administrators of servers that process institutional data are expected to apply industry best practices to ensure appropriate security of that data. Network administrators are expected to apply best practices to ensure that the network is protected, available and secure from breach. Users of university information technology resources are expected to apply best practices to prevent corruption or

unauthorized disclosure of university institutional data, disruption of university networks or loss of university business continuity.

III. Policy Statement

A. Roles and Responsibilities

1. Information Technology Security Officer

   The university's Information Technology Security Officer has responsibility for development, practice and enforcement of the information security policy of the university. The IT Security Officer will also coordinate security efforts for other departments within the university. This position reports to and is supervised by the Vice-Chancellor of Information Technology Systems Division.

2. University Institutional Data

   University institutional data is data that is relevant to planning or managing an administrative or academic function of the university. Responsibility for the integrity and accuracy of that data is the data owner. Responsibility of application of the protections necessary to insure confidentiality and availability of that data is the function of the custodians of that data.

3. Data Owner

   The Data Owner is the entity, department, or administrative workgroup that is responsible for entering that data into university information systems and is responsible for assurance that the data is accurate and complete. The Data Owner, due to legal, legislative, or ethical constraints, may also, after consultation with others, make the determination that access to certain elements of the data is limited.

4. Data/Network Custodian

   The custodial responsibilities of university institutional data generally comprise the following areas within the university: managers and administrators of computer systems and servers where institutional data resides; managers and applications programmers of software systems and web applications that store, modify or provide access to that data; and managers of networks that provide internal and external access to that data. Each of these groups share a custodial responsibility to assure that the confidentiality, integrity and accessibility of university institutional data is maintained at all times within the parameters defined by the data owner, university policy, and State and Federal requirements.

B. Data Classification/Public Records

All data residing on university computers, or on backup media retained for the purpose of business continuity and disaster recovery, is subject to the N.C. Public Records Act with the following exceptions: data subject to the exclusion of N.C. G.S. 132-6.1(c) and other subsections; certain police records and criminal investigative information; data subject to protection from disclosure by State or Federal Legislation (e.g. N.C. Personnel Records Act, FERPA, etc.); transactional data subject to Federal legislation (e.g. ECPA); and incidental communication not related to performance of an employee's assigned duties. It is the responsibility of the data owner to identify elements of all data records for which the data owner has responsibility of stewardship to determine the level of protection that the data element requires. If a data element requires protection from access or disclosure, it is the incumbent responsibility of the data owner to inform the appropriate data custodians of that requirement.

C. Non-disclosure

As a condition of employment, data users are expected to access institutional data only in the performance of their assigned duties, to respect and adhere to the confidentiality and privacy of individuals whose records they access and to abide by all applicable laws or policies with respect to access, use or disclosure of information. Institutional data may not be disclosed or distributed in any medium unless required by an employee's assigned duties. University institutional data may not be accessed or used for personal gain or to satisfy personal curiosity. Certain employees may be exposed to confidential information in normal performance of their assigned duties. The exposure could either be incidental to or material in performance of their duties. Therefore, the university may, based upon the likelihood of exposure to confidential information, require that certain employees also sign a confidentiality statement.

D. Application of Best Practices to Create a Secure Computing and Network Environment

1. Network Management

a. Network administrators will apply current industry standard best practices to provide appropriate firewall protection to the university network perimeter and to associated network segments as appropriate.

b. Installation of network operating systems and applications will be crafted to provide network protection equivalent to the current industry standard.

c. Unnecessary open ports and services to servers will be shut off. All open ports must be approved by the Director of Computing Services of the Information Technology Systems Division and documented.

d. Open mail relays not administered by Information Technology Systems Division will be eliminated.

e. Encrypted sessions will be used for remote administration.

f. Regular vulnerability assessments will be performed to ensure that network security components perform as expected.

g. Network Time Protocol (NTP) or other authorized time synchronization will be used to assure that all university network time stamping is consistent and accurate.

h. Network logging will be performed consistent with university policy and logs will be reviewed regularly.

i. Retention of log data will conform to university policy for log data retention.

j. Intrusion Detection Systems (IDS) will be employed where appropriate and feasible.

2. Server Management

a. Administrators responsible for management of central or departmental servers will incorporate anti-virus protective measures and will keep such software current.

b. Administrators responsible for management of central or departmental servers will incorporate an operating environment patch strategy to address security issues as required.

c. Administrators responsible for management of central or departmental servers will institute a procedure to require strong passwords of user accounts.

d. Administrators responsible for management of central or departmental servers will use university approved software where appropriate to audit passwords and effect remediation of weak passwords.

e. Administrators responsible for management of central or departmental servers will employ and monitor Intrusion Detection sensors (IDS) and host based firewalls where appropriate.

f. Administrators responsible for management of central or departmental servers will use NTP or other authorized time synchronization to ensure

that all university computer activity time stamping is consistent and accurate.

g. System activity logging should be performed consistent with university policy and logs will be reviewed regularly. Retention of log data will conform to university policy for data retention.

h. Some email may be considered official university institutional data. Such email will be retained by the owner of the email in accordance with N.C. records retention requirements.

i. Where feasible, login or "first page banners" as provided by the U.S. Department of Justice, or as approved by the university, will accompany all login screens or entry pages to applications that allow access to data other than public inquiry.

3. Individual Computers, Laptops, Personal Digital Assistants (PDAs), and other Mobile Computing Devices

a. Users of portable computing devices are responsible for the security of the device and its content.

b. Confidential or protected information on portable computers should be protected using encryption.

c. Confidential or protected information must not be transmitted to or from a portable computing device unless secure connection and transmission protocols are used.

d. Users of university-owned computers or computers that access university computers or networks will use university-approved anti-virus protective measures and will keep such software current.

e. Users of university-owned computers or computers that access university computers or networks will ensure that the computers are kept up to date with all security patches.

f. Remote access to university networks will use university-approved encrypted VPN. Such VPN access will conform to university defined methodology to ensure that unauthorized access to university networks is prevented. When a unique situation exists that requires another type of access (e.g. vendor support), access will be granted only for the duration of the session and will be monitored by the server administrator.

g. Laptop computers, PDAs, and other mobile computing devices offer a challenge to the security of the university systems and networks. While

they provide convenience and portability, they also create a unique material risk to university data security. Loss or theft of a university laptop computer can result in disclosure of data that is protected by State or Federal regulation, or data that should be protected as proprietary for other reasons. Loss or theft or a university laptop computer can allow uncontrolled access to university systems through stored information such as passwords, cookies, etc. The university may, as a result of risk analysis, determine that certain individual computers constitute an elevated risk to the university through loss, and require that the computer be "hardened" through the use of internal recovery software and internal data encryption.

h. Users of university computers will configure those systems to conform to university computer security standards. Users of personally owned computers that access university computers or networks should configure those systems to conform to university computer security standards.

i. Users of any PDA or mobile computing device that accesses the university network, whether owned by the university or otherwise, will use VPN and university specified encryption when connecting to university networks.

4. Physical Security

a. Central Servers, Departmental Servers and Network Appliances

1) Physical Access Controls will be implemented to prohibit access to these facilities by unauthorized personnel.

2) Visitors and maintenance personnel should be escorted and monitored while they are in a secure area.

3) All facilities housing central servers, departmental servers, and network appliances will have, where appropriate, fire sensing/extinguishing devices present.

4) Where feasible, all facilities housing central servers, departmental servers and network appliances will utilize cipher locks or controlled access card entry systems.

b. Desktop, Laptop and PDAs

1) Users should log off computers when the user is not in the vicinity of the computer.

2) All spaces housing personal computers and desktop equipment should be kept locked when not occupied by the employee(s) in order to reduce the occurrence of unauthorized entry and opportunity for theft.

3) Laptops and PDAs used in openly accessible areas should be locked in secure cabinets when not in use. Offices containing laptops and PDAs should be locked when not occupied.

c. General Physical Security Awareness

1) Certain information relating to the campus network and information security infrastructure is protected from disclosure under the N.C. Public records exclusion N.C. 132-6.1(c). Information pertaining to network structure, password management, wireless access, etc. can be extremely useful to outside hackers and should not be divulged. Report any attempts by strangers trying to gain such information immediately to your supervisor or to IT Security. Supervisors receiving such reports will immediately notify the Office of IT Security of the event.

2) Employees are expected to report any unauthorized access, entry or suspicious activity to supervisors and/or campus police immediately.

3) Users will dispose of confidential waste carefully and securely to maintain confidentiality.

5. Business Continuity

a. Administrators responsible for management of central or departmental servers will create a functional disaster recovery plan containing sufficient information to allow a third-party person to access backup media and restore the system to operational status. The plan should consider not only critical IT resources, but also personnel necessary to effect a successful recovery of the system(s) and data. Critical information assets must be identified so that essential business activities are restored quickly to functional levels. This plan should be reviewed and tested manually and modified as necessary.

b. Administrators responsible for management of central or departmental servers or data will create multi-generational backups of systems and data on a regular predefined schedule.

c. Administrators responsible for management of central or departmental servers will secure the current system and data backup in a secure, protected off-site location. Included with that backup will be a hard-copy listing of the contents of the backup, the current version and hardware of the system from which the backup was obtained and a copy of the disaster

recovery plan needed to restore the contents of the backup to operational status.

6. Privacy Issues

   The university will not release personal information to parties outside the university without prior consent unless that disclosure is permitted by applicable law or university policy. Individuals within the university will only be granted access to personal information if there is a demonstrated and legitimate need to know, based upon normal job duties, and falling within the purpose and scope for which the data were collected.

   The university may permit the inspection, monitoring, or disclosure of university data when access or disclosure is allowed or required by applicable law. This data can include transaction logs, communication logs, pertinent email subject to disclosure, or other records developed in the course of server, systems and network management.

7. Incident Response

   A security incident is an event that causes disruption to normal business activity and that is precipitated by malicious or accidental actions. Examples of incidents include denial of service attacks, computer intrusions or suspected intrusions, hacker episodes, misuse, unauthorized access to IT resources or information, reports of violations of university IT policy, State or Federal laws and computer viruses or worms.

   a. Viruses and worms

      1) It is the responsibility of the owner or administrator of university computers to detect, isolate and repair any incidence of infection by virus, Trojan, or worm.

      2) In the event of infection the owner or administrator should first shut down the affected computer and review the Technology Assistance Center virus web page for assistance. Users may also contact the Technology Assistance Center for further assistance if needed.

   b. Computer intrusions or system compromise

      1) Incidents of computer intrusion or system compromise will be reported to the university Information Technology Security Office or to the Technology Assistance Center which will forward the information to the Information Technology Security Office.

2) Incidents of computer intrusion or system compromise will be investigated in coordination with the Information Security Office.

3) A written incident log of the event will be maintained (dates and times, persons contacted, systems involved) for all events under investigation. This is a critical component, particularly in situations where a criminal investigation may result.

4) The severity of the compromise will be assessed. If the incident is affecting other systems, damaging data, or involving a known root compromise, the incident will be considered critical.

5) If the compromise is critical, the system will be disconnected from the campus network and the owner or administrator of the affected computer will be notified of the disconnection.

6) The compromised system will be backed up forensically to create a system snapshot in the compromised state. This backup will be considered evidentiary in nature and will be handled and stored using forensic best practices for evidence handling.

7) The system will be restored to an operational state before reconnection to the University network.

c. Other incidents

1) Other security incidents will be reported to the Information Security Office.

2) The Information Security Office will conduct an investigation of the incident and coordinate resolution of the incident with Human Resources, the Dean of Students, Campus Police, or other campus entity as appropriate.

8. Wireless access

a. All wireless access points will be centrally managed and subject to periodic audits and penetration testing.

b. Wireless infrastructure will be segmented from the campus network using a firewall, VPN appliance, router access control list, or similar technology.

c. Users of the wireless network must be authenticated with unique IDs and passwords.

d. Confidential data will not be transmitted over a wireless connection unless over an encrypted session.

9. Modem Access and Standards

Modems should only be connected to systems as required to perform system administration, vendor support, or as a part of an administrated application. Modems should only be active during times of use or as needed by an application. The responsibility for periodic audits and penetration testing of modems is the responsibility of the system administrator or application support personnel for the system to which the modem is connected. Periodic audits and/or penetration testing of modems may also be done by Information Technology Systems Division personnel.

10. Lifecycle replacement and Data Destruction

a. All university computers will be examined prior to disposal to assure that no institutional or protected data, proprietary software, or software not licensed to be transferred with the computer resides on media attached to the computer.

b. Removal of institutional or protected data, proprietary software, or software not licensed to be transferred with the computer will be accomplished by use of university-approved data destruction software or by physical destruction of the media.

c. All university computers that contain, or have contained protected data, proprietary software, or software not licensed to be transferred with the computer will be certified as "sanitized" prior to disposal or transfer to another department or work unit.

11. Data Retention

Retention of data on backup media should be determined by the type of data that is being stored:

a. Research data retention must conform to the requirements of the grant agency (NIH, NIST, NIMH, DOD, etc.).

b. Users (faculty, staff and students) are responsible for the security and back-up of all data stored on their individual desktops/laptops (including, but not limited to, e-mail and office files). Data is to be backed-up on media separate from the internal hard drive (such as USB drive, external hard drive, or other removable media). The user is responsible for the safe and secure storage of all external back-up media. Data stored on centrally managed servers is automatically backed up.

c. Institutional data governed by Federal regulation must conform to the requirements of the agency that regulates that data (N.C. State Personnel Act, FERPA, etc.).

d. Data related to student coursework will be retained in conformance with the university policy on student data retention.

e. Other institutional data will be retained in accordance with State records retention requirements of N.C.G.S. 132 and N.C.G.S. 121 or other applicable State legislation, or university record retention policy.

12. Employee termination and exit procedures

a. Upon notification that an employee intends to voluntarily separate from the university, the employee's supervisor will take the steps necessary to ensure that:

b. No unauthorized transfer of university institutional data is made from university servers or other computers to any personal computer, mobile computer, storage device or portable media.

c. No unauthorized transfer of university institutional data is made from university servers or other computers to any other computers via the network.

d. No software licensed by the university is copied or transferred to the employee unless the employee has a license to personally possess that software or the software is in the public domain.

e. Any transfer of personal data or information from a computer owned by the university shall be made under supervision at all times.

f. Upon involuntary termination of an employee, the employee's supervisor will take the steps necessary to ensure that all access to university computers, including desktops and mobile computing devices, is denied.

13. Non-affiliate access

There are business needs for the university to provide vendors and other non-affiliated third parties access to the university's information technology resources and networks. For example, vendors assist in support of information technology resources; contractors may need network access to support major project development; and adjunct faculty may assist in important university research. Non-affiliate access is subject to the following restrictions:

a. Non-affiliate access to university IT resources must be authorized by an appropriate Dean, Department Chair, or higher position within the university.

b. The level of access granted will be limited to those IT resources that are required to carry out the specified business or research need of the university.

c. The access must be enabled for specified tasks and functions, and limited to specific individuals and only for the time period required to accomplish approved tasks.

d. Non-affiliate access must be uniquely identifiable, and password management must conform to university policies.

e. The non-affiliate must agree to comply with all applicable Federal and State statues and university policies concerning acceptable use of university IT resources and policies concerning the preservation of the confidentiality of the information to which they have access.

f. The university may, based upon the likelihood of exposure to confidential information, require that the non-affiliate agrees to an instrument of confidentiality.

IV. Enforcement Penalties

The university reserves the right to place restrictions on the use of its electronic resources in response to complaints that present evidence of violations of university policies, rules, regulations or codes, or local, State or Federal laws and regulations. Actions that violate these policies can result in immediate disabling, suspension and/or revocation of the account owner's privileges pending review for further action. Such unauthorized or illegitimate use of electronic resources including computer accounts, resources or facilities may subject the violators to appropriate disciplinary, criminal and/or legal action by the university and/or the State. If evidence is established, the university authorities responsible for overseeing these policies and codes will be consulted on the appropriateness of specific actions.

Individuals who have concerns about the conduct of a member of the university community or the propriety of a given situation or activity should notify their department chair, dean, director, or an administrator in their supervisory chain at a level sufficient to allow objectivity in evaluating the subject of concern. If action is deemed warranted by this official, the matter shall be referred to the appropriate Vice Chancellor or Senior Officer. If disciplinary action is considered, the Vice Chancellor or Senior Officer will consult with Human Resources. Prior to taking action, the Vice Chancellor or Senior Officer responsible for the situation or activity at issue shall

consult with the Vice Chancellor for Information Technology Systems Division, who shall, as appropriate, consult with the university's General Counsel. The responsible official shall then respond to university community members who express concerns about such activities or incidents.

When concern about a given situation or activity involves an imminent threat to individuals, systems, or facilities, users should immediately communicate the concern directly to the Office of the Vice Chancellor of Information Technology Systems, the University Police and to the Information Technology Security office.