Security Guidelines for Electronic and Technology Resources

I. Purpose

Wilkes University acknowledges an obligation to ensure appropriate security for all Information Technology data, equipment, and processes in its domain of ownership and control. Within this context the University endeavors to balance the need for security against unreasonable risk with the need of students, faculty, and staff to be able to use its systems with the minimum of encumbrance. The obligation for security is shared, to varying degrees, by every member of the University.

Confidentiality of information is mandated by law, formal statute, explicit agreement, professional practice and/or convention. Different classes of information warrant different degrees of confidentiality.

The information stored in its information technology systems represents a sizable monetary investment that must be protected. Some of which may have taken significant resource investments to generate, and some of which can never be reproduced.

- It is recognized that various sections of the University provide services that relate to IT security, both directly and indirectly. It is expected that there will be collaboration between these sections and the Office of Information Technology in generation of standards and implementation of the policy.
II. **Applicability**

This policy applies to all persons accessing Wilkes University’s electronic and technology resources, which include faculty, staff, students, alumni, emeritus, contractors, guests or any other user. All electronic and technology resources of the University are covered by this policy, including without limitation all networks, supported backbones and links, stand-alone computers, output devices, including printers, shared computers, and connecting resources of any kind, including any external networks.

**Confidential Data**

Confidential data is considered to include: Credit Card Numbers, Salary Information (except when considered public record), Social Security Numbers, race/ethnicity or gender, financial information, FERPA and HIPPA protected information (grades, test scores, class schedule, GPA, medical records).

Under FERPA guidelines the following information is not considered confidential (unless a student requests that it be so) and may be released without their consent: Name, Address, phone, place and birth date, school email, photograph, field of study, dates of attendance, degrees, and awards.

III. **Definition of Security**

Security can be defined as “the state of being free from unacceptable risk”. Risk for the University concerns the following categories of losses:

- Confidentiality of Information.
- Integrity of data.
- Assets.
- Efficient and Appropriate Use.
- System Availability.

Confidentiality refers to the privacy of personal or enterprise information. This includes issues of copyright.

Integrity refers to the accuracy of data. Loss of data integrity may be gross and evident, as when a computer disk fails, or subtle, as when a character in a file is inappropriately altered.
The assets that must be protected include:

- Computer and Peripheral Equipment,
- Communications Equipment,
- Computing and Communications Premises,
- Supplies and Data Storage Media,
- System Computer Programs and Documentation,
- Application Computer Programs and Documentation, and
- Information/Data.

Availability is concerned with the full functionality of a system (e.g. finance or payroll) and its components.

The potential causes of these losses are termed “threats”. These threats may be human or non-human, natural, accidental, or deliberate.

IV. **Policy**

All users of Wilkes University technology resources:

- Will operate under the provisions of the “Security Guidelines for Electronic and Technology Resources”
- Will operate under the provisions of the “Acceptable Use Policy for Electronic and Technology Resources”
- Will operate under the provisions of the “Copyright Infringement response Policy”
- Will operate under the provisions of the “Electronic Mail Policy”
- Will operate under the provisions of the “Account Creation and Removal Policy”

The University will endeavor to protect the confidentiality of information and material furnished by constituents and will instruct all personnel to protect the confidentiality of such information and material.

The University will endeavor to safeguard the possibility of loss of information within the University's computing and networking facilities but will not be liable to the user in the event of any such loss. The user is responsible for take all reasonable measures to further safeguard against any loss of information on their local system (i.e. making backup copies of all important documents).

The University, through authorized individuals, reserves the right to periodically check and monitor the computing and networking facilities, and reserves any other rights necessary to protect them.
The University disclaims responsibility and will not be responsible for loss or disclosure of user information or interference with user information resulting from its efforts to maintain the privacy, security, and integrity of the computing, and networking facilities and information.

The University reserves the right to take emergency action to safeguard the integrity and security of the computing and networking facilities. This includes but is not limited to the termination of a program, job, or on-line session, or the temporary alteration of user account names and passwords. The taking of emergency action does not waive the rights of the University to take additional actions, up to and including disciplinary actions, under this policy.

Users of the computing and networking facilities do so subject to applicable laws and University policies. Wilkes University disclaims any responsibility and/or warranties for information and materials residing on non-University computer systems or available over publicly accessible networks, except where such responsibility is formally expressed. Such materials do not necessarily reflect the attitudes, opinions, or values of Wilkes University, its staff, or students.

V. **Responsibilities**

Users of the Wilkes University electronic and technology resources accept the following specific responsibilities:

- To safeguard their data, personal information, passwords and authorization codes, and confidential data;
- To be responsible for the security and integrity of University information/data stored on their personal desktop system. This includes making regular backups; controlling physical access to the machine, and maintaining virus protection software.
- To avoid storing passwords or other information that can be used to gain access to other campus computing resources.
- To avoid storing any other confidential data or information on their laptop PC or associated floppy disks or CD’s unless required to perform their job. All such information should be secured using approved encryption technologies.
- To respect the intended usage of resources; for example, to use only the account name and password, funds, transactions, data, and processes assigned by service providers, unit heads, or project directors for the purposes specified, and not to access or use other account names and passwords, funds, transactions, data, or processes unless explicitly authorized to do so by the appropriate authority.
To report any information concerning instances in which the University IT Security Policy or any of its standards and codes of practice has been or is being violated, to the ITS Help Desk which will redirect the incident to the appropriate person(s) for action or will handle it directly.
Appendix A

Security Guidelines for
Electronic and Technology Resources
1. Desktop/Laptop Computer Security Guidelines

1.1. Definition

Desktop/Laptop computers are personal workstations that, though possibly linked to other computers via a Local Area Network, function as stand-alone units.

1.2. Hardware Security

1. Lock offices. Office keys should be registered and monitored to ensure they are returned when the owner leaves the University.

2. Secure Desktop/Laptops in public areas. Equipment located in publicly accessible areas or rooms that cannot be locked should be fastened down by a cable lock system or enclosed in a lockable computer equipment unit or case.

3. Secure hard disks. External hard disks should be secured against access, tampering, or removal.

4. Mark personal computers clearly with the Wilkes University property tag.

5. Locate computers away from environmental hazards.

6. Store critical data backup media in fireproof vaults or in another building.
1.3. **Access Security.**

- Utilize password facilities to ensure that only authorized users can access the system.

- Users will be assigned accounts on the appropriate domains in accordance with industry wide security standards.

- Password guidelines:
  - Each password must be at least eight characters in length and contain all of the following:
    - At least one lowercase letter: a-z
    - At least one uppercase letter: A-Z
    - At least one digit: 0-9
  - Passwords may not be the same as your user ID
  - Passwords will expire every 180 days
  - Passwords may not be the same as the past five passwords (password history 5 previous passwords)
  - Accounts will be locked after five failed login attempts

- Users are responsible for maintaining the security of their password.
  - Passwords should never be written down or stored on-line. Users should create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Good Way To Remember," and the password could be: "TmB1gw2R" or some other variation
  - Users must not:
    - reveal their password in an email message
    - talk about their password in front of others
    - hint at the format of their password
    - reveal their password on questionnaires or security forms
    - share their password with family members
    - reveal their password to co-workers while away from campus
1.4. **Data and Software Availability**

- Ensure that important records and programs are backed up on a regular schedule.
- Check data and software integrity.
- Request assistance from Help Desk personnel to repair software problems.

1.5. **Confidential Information**

- Don’t store confidential information on your computer that you don’t have a current need to use.
- Delete confidential data from your computer when you finished using it.
- Encrypt any sensitive and confidential information stored on your computer. Notify the Help Desk if you maintain any confidential information (e.g. SSN, Credit Card, Grades on your system) so that IT can provide you with an encryption device.
- Monitor printers used to produce sensitive and confidential information.

1.6. **Software**

Software is protected by copyright law. Unauthorized copying is a violation of University Copyright policy. Anyone who uses software should understand and comply with the license requirements of the software. The University is subject to random license audits by software vendors.

1.7. **Viruses**

Computer viruses are self-propagating programs that infect other programs. Viruses and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. Fixes to infected software should be made as soon as a problem is found.

To decrease the risk of viruses and limit their spread:

- Periodically run Anti-Virus software scans on your system to include “all files”.
- Check all software before installing it.
• Use software tools to detect and remove viruses.

1.8. **Computer Networks.**

Networked computers may require more stringent security than stand-alone computers because they are access points to computer networks.

While ITS has responsibility for setting up and maintaining appropriate security procedures on the network, each individual is responsible for operating their own computer with ethical regard for others in the shared environment.

The following considerations and procedures must be emphasized in a network environment:

• Check all files downloaded from the Internet. Avoid downloading shareware files.

• Test all software before it is installed to make sure it doesn't contain a virus/worm that could have serious consequences for other personal computers and servers on University networks.

• Use (where appropriate) encrypting/decrypting and authentication services to send confidential information over the Internet.
2. **Enterprise System Platforms**

2.1. **Definition of ‘Enterprise’**

An *enterprise* system is one that meets *several* of the following criteria:

1. Is critical to the mission of the University.
2. Affects large parts of the University.
3. Yields University-wide benefits.

2.2. **Management of Enterprise Systems**

The following policies apply in the management of enterprise systems:

1. Enterprise platforms will be managed and operated by ITS.
2. The designated custodian of the application will manage enterprise Applications.

2.3. **Physical Security**

The following standards of physical security of enterprise platforms must be met:

- Premises must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc.
- Air temperature and humidity must be controlled to within acceptable limits.
- Platforms must be electrically powered via UPS and generator to provide the following:
  - Minimum of 2 days operation in the event of a power blackout.
  - Adequate protection from surges and sags.

2.4. **Physical Access**

- Access will be limited to designated staff via card or key access.
- External doors will remain locked, preferably with electronic locks.
2.5. **Fire Detection and Control**

- There will be smoke and thermal detectors on the premises.
- Under floor areas will have smoke and water detectors.

2.6. **Account Creation and Removal**

- See Account Creation and Removal Policy

2.7. **Administrative System (Banner) Access Control**

- **Granting of Access:**
  Access to the Banner administrative computing system will only be granted to users through approval of a designated banner module Data Manager. Data Managers hold the following organizational positions:

  - Finance – Controller
  - Accounts Receivable – Controller
  - Payroll – Controller
  - Advancement – Advancement Data Services Manager
  - Financial Aid – Director of Financial Aid
  - Student – Registrar
  - General – ITS Banner Security Administrator

  The Data Managers may appoint someone with appropriate authority as a proxy agent who approves access in their absence. Access will be granted only with receipt of a formal request from a data manager or their proxy via electronic mail (email) of a signed and dated request form.

- **Monitoring of Access:**
  IT Services will conduct a quarterly audit of employees with Banner access. Data Managers will receive electronic copies of all users within their modules who have access to objects, processes, and forms. Data Managers will determine the appropriateness of the Banner access within their designated modules. Data Managers will notify the ITS Banner Security Administrator of the affirmation that the access data is correct AND any changes to a Banner user’s security at this time. Copies of these audits and responses will be retained on a secured ITS share drive. **Data Managers are responsible for notifying IT Services**
of any errant security at any time that this information becomes known to them.

- Termination of Access:
  Human Resources will notify IT Services of separation of employees. Upon the employee’s termination date, Banner access will be locked, and Banner classes will be removed from their Banner ID.

2.8. **Data Integrity**

- Security backups of all data will be made daily.

- The backup regime must meet the following criteria:
  
  - Enable recovery to at least the start of business on any weekday of a failure.
  
  - Provide at least one more level of backup to a previous time, to cover the case of the failure of the primary backup media.

- There must be offsite storage of security backup media to enable a full data recovery to no earlier than one working week.

- There must be a validation of security backup media at least once every six months.

- There should be a separation of responsibilities of persons conducting backups from personnel conducting system restores.

2.9. **Disaster Recovery Plan**

There will be a Disaster Recovery Plan for every enterprise system.
3. Software Change Control

3.1. Definition

Software Change Control covers the control of all aspects of enterprise systems software including the operating system, its associated packages and utilities, third party and University developed applications, together with any command procedures and documentation to support and run them.

3.2. General Obligations

When changes are required to systems software, associated packages and utilities, applications software, command procedures, or documentation, it is essential that the changes are:

- appropriately authorized and approved
- thoroughly tested
- sufficiently documented
- implemented at an appropriate time.

Any change must only be transferred into the production environment when approved by the appropriate System Custodian.

Sound software security management requires the procedures to manage the change control for applications and systems changes are clearly defined. There must be a set of Software Change Control Procedures to assist the process.

All operational software relating to enterprise systems should be placed under appropriate Configuration Management.

3.3. Change Control Responsibilities

Specific personnel will be given the responsibility for the implementation of changes by undertaking appropriate testing in the test environment, and, subject to the appropriate approvals, moving the changes to the production environment. All elements of the system will be subject to Software Change Control Procedures.

There should be a separation of responsibilities in the transfer of software from test into the production environment.
3.4. **Change Control Environment**

Where possible, three separate environments should be maintained for each enterprise system:

- development
- testing
- production

Migration of software between environments should only be undertaken after obtaining the appropriate sign-offs as specified in the Software Change Control Procedures.

New software and changes to existing software should be prepared in the *Development Environment* by appropriately authorized development or applications support staff. Applications should be specified, designed and coded according to the University’s systems development methodology.

Once assessed as satisfactory, the new or modified software should be transferred to the *Testing Environment* for systems and acceptance testing by an appropriate testing group, according to an agreed test procedure. Changes to software are not permitted in the testing environment.

Following successful completion of testing and approval by the appropriate systems custodian, the new or modified software should be transferred to the *Production Environment* for implementation under the control of ITS Operations staff. A contingency plan to enable the software to be restored to its previous version in the event that the implementation is unsuccessful should be prepared where appropriate.

3.5. **Documentation**

- **Change Control Procedures**

  Procedures reflecting these policies must be documented in the ITS Software Change Control Procedures.

- **Software Change Request**

  No software change is to be undertaken without an appropriately authorized software Service Request. The Service Request is also the principal documentation to be completed for the software change management process.
• Technical, Operations and End User Documentation

Appropriate documentation in respect of each software change must be completed in sufficient detail and accepted before the change is implemented in the production environment.

4. Communications

Network access can be categorized into four major areas:

1. Campus Local Area Network
2. External Access via Internet
3. External Access via Internet2
4. Wireless Access via Wire Free Wilkes-Barre

The University has varying degrees of control decisions affecting security management of these areas:

1. Total control over the campus LAN Modem links, and Intercampus Network, given that ITS staff plan, install, manage, and maintain these systems.

2. No control over the Internet, Internet2 or Wire Free Wilkes-Barre systems as they are managed and maintained by outside organizations.

4.1 Campus Local Area Networks

4.1.1. Physical Security

The following standards of physical security campus local area networks must be met:

• Premises housing network control equipment must be physically strong and free from unacceptable risk from flooding, vibration, dust, etc.

• External building ducts must conform to University standards of service reticulation.

• Internal building distribution of cables within ceiling, wall or floor cavities must be reticulated within protective conduits.

• Air temperature and humidity must be controlled to within equipment defined limits.
- Network electronics must be powered via Un-interruptible Power Supplies to provide the following:
  
  1. Minimum of 15 minutes’ operation in the event of a power blackout.
  
  2. Adequate protection from surges and sags.

4.1.2. Physical Access

- Access to areas housing network electronics will be controlled by designated ITS staff.

- Doors to areas housing network electronics will be locked with a unique key, the distribution of which will be determined by ITS staff and the CIO.

4.1.3 Data Integrity

4.1.3.1. Intrusion Protection

Within the boundaries of the LAN, intrusion protection is required to prevent:

1. non-University staff or students from indiscriminately plugging laptop computers into any access port of the campus network

2. unauthorized access of staff and students to the University’s enterprise systems

3. viruses, adware, and malware

- Only those computers belonging to staff and students will be allowed to function when connected to the University network. Visiting personnel wishing to access the network must have authorization from a management team member, who must apply to ITS for temporary access rights.

- Only authorized personnel will be allowed Telnet or FTP access to enterprise computing systems.