WILKES
UNIVERSITY

Security Guidelines for Electronic and Technology Resources

Effective: 05/14/2008
Updated: 05/14/2015
Pages: 15

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 Services (ITS) 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 includes faculty, staff, students, alumni, emeriti, 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, personal computers, mobile devices, external storage devices, output devices (including printers), shared computers, and connecting resources of any kind, including any external networks.

III. Definition of 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, and 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.

IV. 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
- 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.

V. **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”
- 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 online 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 are 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.

VI. **Responsibility**

Users of 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 computers. This includes making regular backups, controlling physical access to the machine, and maintaining virus protection software.
- To be responsible for the security and integrity of University information/data stored on their mobile devices and/or external storage devices.
- To avoid storing passwords or other information that can be used to gain access to other campus computing resources in physical or electronic format.
- To avoid storing any other confidential data or information on their personal computers, mobile devices, or associated external storage devices 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 this 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

Specific Physical and Electronic Security Guidelines

1. Personal Computer Security Guidelines

1.1. Definition

Personal computers are desktop or laptop workstations that, though possibly linked to other computers via a Local Area Network, function as stand-alone units.

1.2. Hardware Security

- Lock offices. Office keys should be registered and monitored to ensure they are returned when the owner leaves the University.
- Secure computers 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.
- Secure external storage devices. External storage devices should be secured against access, tampering, or removal.
- All computers should be clearly marked with a Wilkes University property identification tag.
- Locate computers away from environmental hazards.
- Store critical data backup media in fireproof vaults or in another building.

1.3. Access Security

- Utilize passwords 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 at least three of the following four requirements:

  1. At least one uppercase letter: A-Z
  2. At least one lowercase letter: a-z
  3. At least one number: 0-9
  4. At least one of the following characters: period (.), dash (-), underscore (_) or vertical bar (|)

Your password must also meet the following requirements:

  - Not contain an exact dictionary word or name
  - Not contain your username or any variation
  - Not be an old password

- Passwords will expire after 180 days. Users will be notified of the expiration in their Wilkes University (@wilkes.edu) email account multiple times before expiration.
- Users are responsible for maintaining the security of their password. Passwords should never be stored in any physical or electronic format.
- Users should never:
  - Provide their password in an email. (ITS will *never* ask for an individual's password via email.)
  - Provide their password over the phone or in person unless in the specific instance where they have contacted an ITS support member and that individual needs the password to assist with support. Users should change their password immediately after the support request is complete. Users should be completely sure that they are talking to a member of ITS support by calling the Help Desk or the technician directly or going to see the staff member in person and not give out their password to individuals who call them and simply state they are part of ITS.
  - Share their password with any other individual for any reason except in the specific support scenario defined above.

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 or devices that you don't have a current need to use.
- Delete confidential data from your computer when you finish using it.
- Encrypt any sensitive and confidential information stored on your computer. Notify the Help Desk if you maintain any confidential data so that ITS can provide you with encryption software.
- Monitor printers used to produce sensitive and confidential information.

1.6. Software

Software is protected by copyright law. Unauthorized copying is also a violation of the University Copyright Infringement 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 and Malware/Spyware

Computer viruses are self-propagating programs that infect other programs. Viruses and other harmful software may destroy programs and data as well as using the computer's memory and processing power. Viruses, Malware, and Spyware are of particular concern in networked and shared resource environment because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. If you suspect your computer or device may have a virus or harmful software, immediately contact the ITS Help Desk for assistance.

To decrease the risk of viruses and limit their spread:

- Periodically run Anti-Virus software scans on your system to include "all files."
- Make sure Anti-Virus software, system updates, and other software programs are up to date.
- Do not open emails or attachments from unknown individuals.
- Do not open attachments or click on links in emails that look suspicious, even from known individuals.
- Never login to any University system from a link in an email. Always navigate directly to that resource before logging in. Many "phishing" emails will create fake versions of University websites to obtain login information.
- Immediately report suspicious emails or unusual activity on your computer to the ITS Help Desk.

1.8. 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.
- Contact the ITS Help Desk before installing any program on your computer.

- Use (where appropriate) encryption and authentication services to send confidential information over the Internet.
- Do not store personal information on Network resources.

2. Enterprise System Platforms

2.1. Definition of Enterprise System

An enterprise system is one that meets 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 to the management of enterprise systems:

- Enterprise platforms will be managed and operated by ITS.
- 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 two days operation in the event of a power outage.
    - 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. Sub-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 email of a signed and dated request form.

Monitoring of Access:

- ITS 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 ITS 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 off-site 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 system software, associated packages and utilities, application 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 system 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

3.5.1 Change Control Procedures

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

3.5.2 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.

3.5.3 Technical, Operations, and End User Documentation

Appropriate documentation in respect to 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 two major areas:

1. Campus Local Area Network
2. External Access via Internet

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

1. Total control over the campus LAN and Inter-campus Network, given that ITS staff is in control of planning, installation, management, and maintenance of these systems.
2. No control over Internet 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 for 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 UPS to provide the following:

  1. Minimum of 15 minutes' operation in the event of a power outage.
  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 management.

4.1.3 Data Integrity: Intrusion Protection

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

- Non-University individuals from indiscriminately plugging laptop computers into any access port on the campus network.
- Unauthorized access of staff, faculty, and students to the University's enterprise systems.
- Proliferation of viruses and other harmful software.

Only those computers belonging to staff, faculty, 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.

Appendix B

Identity Authentication for Remote Resources

1. Identity Authentication in Online Courses

The University and students share a joint responsibility to ensure that each student's contribution in online course activity comes from that student alone. For the student, this responsibility has two parts:

1. Students are responsible for positively ensuring that every contribution to an online course created with the student's Wilkes University computer account is made by that student alone. Contributions covered under this policy include: written assignments, quiz and exam submissions, discussion forum postings, live participation in text-based chat sessions, phone conferences, and video conferences. If a student allows another person to write or make any kind of submission to an online activity in the student's name, then this constitutes cheating and will be treated as a violation of academic honesty.
2. Students are responsible for ensuring the integrity of their Wilkes University computer account security by following the actions required of them by the University's Security Guidelines for Electronic and Technology Resources Policy and the Acceptable Use Policy. These actions include keeping passcodes private, updating passcodes when required by the University, and reporting breaches of the security policy to the ITS Help Desk.

2. Remote Account Support Requests

Members of the University (users) who require support involving their University account and cannot come physically to the ITS Help Desk must call in for support. ITS will not accept email requests for account support.

An individual must call in themselves for support on their account. No proxy will be accepted for the user unless express written permission has been provided to ITS and approved by the University.

When contacting the Help Desk, users must confirm their identity by providing two of the following four pieces of personal information:

1. Wilkes Identification Number (WIN)
2. Date of birth
3. Last four digits of their SSN
4. Current home address of record

Failure to provide this proof of identification will result in a denial of support.

ITS Help Desk staff will use the following procedure to assist users in resetting their account password:

1. Attempt to walk the user through a self-reset on the University Password Manager website (http://password.wilkes.edu). Students can self-enroll on this website and reset or unlock their own password by entering a series of personally-identifying questions based on data stored in Banner or by creating their own security questions from a list of pre-approved question options.
2. If the self-reset fails, staff will manually reset the password using a tool only available to ITS Help Desk staff. They will then provide the user with a new temporary password and verify that the password now works for the user's account. Once verification is complete, the staff will walk the user through the self-reset process on the Password Manager website. This ensures that the ITS Help Desk staff only have access to the user's account for the duration of the support call.

Users are responsible for the integrity of their own password by following the guidelines set forth in Appendix A, Section 1.3 of the above policy.