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,

- 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**

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

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

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:

  -

1.6. Software

- Use (wh

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.

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

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

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

- 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.
- Unauthn.1 Tf [(om) 0.2 () 0.2 (s)]TJET 0 0.24 0 04 39.26 cmBT 50 0 0 50 0 0 50 0 0 50 0 0

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

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