Information Technology Security Program

Purpose and Scope

- The purpose of this policy is to describe the objectives and components of the Information Technology (IT) security program
- This policy is applicable to all College students, faculty and staff, as well as all others granted use of Wofford College information resources.
- This policy is applicable to all IT information resources, including but not limited to, all computer and communication facilities owned, leased, operated, or contracted by the College. This includes servers, network storage, networking devices and infrastructure, classroom technology, personal computers, workstations, telephones, wireless devices, cable TV, and any associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes.
- This is an overall security policy that relies on and incorporates portions of other IT security policies. All IT policies are available at the following URL: http://www.wofford.edu/technology/

Objectives of the IT Security Program[1]

- The primary objectives of the IT security program are to protect:
    - **Confidentiality of information**. Preserve the privacy of personal or college information for authorized uses only.
    - **Integrity of data**. Assure the reliability of data
    - **Availability of resources**. Ensure timely and reliable access to and use of data
    - **Authorized use of resources**. Limit the use of information resources to authorized users

Components of the IT Security Program[2]

- Risk management
    - Risk assessment and mitigation
    - Vulnerability and activity monitoring
    - Malware protection
    - Change management
- Protection of assets and data
    - Asset identification and documentation
    - Data classification, protection and retention
    - Full disk encryption on laptops
- Incident response
- Authorized use of resources
- Availability of resources
- IT staff training
- Awareness programs
- Disaster recovery and business continuity

[1] Bowdoin College Information Security Policy. 15 Dec 2007. <http://www.bowdoin.edu/it/contact/inf-sec.shtml>
[2] Kathy Bergsma. "Building an IT Security Program." 20 Jan 2008 <http://net-services.ufl.edu/~kathya/faeds.ppt>

Risk Management: Risk Assessment and Mitigation[3]

- Risk assessment and mitigation provides a routine process by which IT staff will help keep Wofford College information resources free from unacceptable risk.
- The process of risk assessment and mitigation identifies and deals with the most crucial potential risks. It involves the following steps:
    - Identify critical assets
    - Identify potential threats and vulnerabilities for different assets
    - Identify resources that are available to mitigate the risks
    - Assign priorities to risks so that available resources can be used to mitigate risk in a cost-effective and efficient manner
- IT risk assessment and mitigation at Wofford will rely on the following
    - An IT security audit conducted by an outside source every four years
        - The first IT security audit was conducted by Stalwart Systems. The report from this audit was received in April, 2006
    - The EDUCAUSE *IT Security Guide*[4]
- After each risk assessment, the IT staff will develop a plan to mitigate the risks identified in the assessment. This plan will include the following:
    - Safeguards designed to mitigate risks as thoroughly as possible within the limits of available resources
    - A timeline for implementation of each step in the plan
    - IT staff responsibilities for each step in the plan
    - Metrics that will help measure progress in mitigating risks

Risk Management: Vulnerability and Activity Monitoring

- The IT Security Coordinator will routinely monitor the vulnerability of components of our network with vulnerability assessment applications, such as eEye REM.
    - Vulnerability analyses will be conducted weekly
    - Reports on potential vulnerabilities will be sent to the staff member(s) responsible for the hardware or software involved, and to the Vice-President of Technology
    - Unless approved by the Vice-President of Technology, vulnerabilities will be removed within two weeks of their report
        - The staff member(s) involved will report the vulnerability removal to the Security Coordinator and Vice-President of Technology when completed
- The IT Network Administrator will use network intrusion detection device(s) to monitor for suspicious activity to and from the Internet.
- The IT Security Coordinator will collaborate with server managers on monitoring individual devices with host-based intrusion detection applications.
- The IT Security Coordinator will collaborate with network and server managers on the use of a security monitoring, analysis and response system to identify, manage, and counter security threats.
    - We plan on implementing this system in FY08-09

---

[3] "Technology Risks." IT Security. Virginia Tech. 19 Oct 2007. Fall 2007. http://www.security.vt.edu/ITrisks.html

[4] a) EDUCAUSE Computer and Network Security Taskforce. "Risk Analysis of Critical Areas and Processes." *IT Security Guide*. 19 Oct 2007. 16 Aug 2006. https://wiki.internet2.edu/confluence/display/secguide/Risk+Analysis+of+Critical+Areas+and+Processes

- The limits on permissible monitoring of system activity and computers on the Wofford College campus are described in the *Monitoring Policy*.

Risk Management: Malware Protection

- IT will furnish and manage a variety of tools, both hardware and software based, to counter threats from viruses, Trojans, spyware, spam and other malware. This process is described in our *Anti-Virus Policy*.
- Computers will be managed as described in the *Computer Management Policy*, which includes standard security precautions, such as antivirus software, password-protected screensavers, routine patch management and IT management of multi-use computers.

Risk Management: Change Management

- Changes to the College's technology environment will be made only after they have been communicated in advance to College staff members responsible for technology here. This process, which will allow risks to be analyzed in advance, is described in the *Change Management Policy*.

Protection of Assets and Data: Asset Identification and Documentation

- IT assets will be identified and classified as critical or non-critical.
- Hardware and software documentation for critical assets, such as servers and network equipment, will be stored as described in the *IT Documentation Policy*.

Protection of Assets and Data: Data Classification, Protection and Retention

- Measures to be taken to help preserve the integrity of administrative data are described in the *Banner Data Standards Policy* and *Banner Batch Loading Policy*
- Measures to be taken to protect administrative data are described in the *Banner Data Security Policy*.
- The routine creation and off-site storage of backup files for Wofford information assets are described in the *Data Backup Policy*.
- The College's policy for the retention and preservation of electronic data is described in the *Electronic Data Retention and Preservation Policy*.

Protection of Assets and Data: Full Disk Encryption for Laptops

- IT will furnish application software that will encrypt data stored on the hard drives of laptop computers used by administrative staff
- This program is under development and should be completed in FY08-09.

Incident Response

- The process for dealing with security events and weaknesses associated with information systems is described in the *Security Incident Response Policy*.

Authorized Use of Resources

- User responsibilities are described in the *Policy on Responsible and Ethical Use of Wofford College Technology Resource.*
- The creation, maintenance, use, and termination of digital identities at Wofford College is described in the *Identity Management Policy*.
    - This policy includes requirements for strong domain and Banner passwords.
    - Passwords are transmitted and stored using secure protocols and algorithms
- Access privileges for authorized users are described in the *Privilege Management Policy*.
- Network access privileges and requirements are described in the *Network Access Policy*.

Availability of Resources

- Wofford technology resources available to users are described in three documents
    - *Access to Technology Resources Policy;*
    - *Network Access Policy;* and
    - *IT Hardware, Software, and Services* report.
- The level of service that the college community can and should expect from IT for critical and basic services is described in the *IT Service Level Agreement.*
- When possible, IT staff will work on server and software maintenance outside of normal working hours to avoid interruptions in service.
- The process for communicating about events that either may lead or have led to an interruption in the use of technology resources is described in the *Campus Notification Policy*

IT Staff Training

- When appropriate, IT staff will be given the opportunity to receive security-related training

Awareness Programs

- All users are required to read and agree with the *Policy on Responsible and Ethical Use of Wofford College Technology Resources* before being issued a network account
- All Banner users are required to read and agree with the *Banner Confidentiality Agreement* before being issued a Banner user name and password. When users sign this agreement, they agree to the following:
    - Comply with the Wofford College Banner Data Security Policy
    - Comply with the provisions of FERPA and College policies pertaining thereto in their handling of the information to which they have access.
    - Restrict their retrieval and other computer activities to information related to their assigned duties
    - Not to share their user name and password with others
    - Not to leave a computer unattended when it is logged onto the Banner database
    - To report any security violation as soon as they become aware of it.

- The IT Help Center maintains a security web page on IT section of the official Wofford web site
    - IT has posters around campus directing users to the IT security web page
- The IT Help Center routinely notifies the campus community of suspicious and dangerous email messages.

Disaster Recovery and Business Continuity

- IT's Disaster Recovery (DR) plan is based on the possibility of a disaster in which the primary data center (DC1) in the Olin Building is damaged or destroyed, but most of the campus remains intact
- In case of such a disaster, IT's goal is to restore critical services for everyone on campus as soon as possible, in most cases within 24 – 48 hours
    - Banner and Banner Web
    - Electronic Mail
    - Internet connection
    - Telephone system
        - Critical locations within 24 hours
        - Entire campus within 10 working days
    - Network storage
- IT has built a secondary data center (DC2) in another location on campus some distance away from DC1
    - DC2 will house the servers necessary for critical services. In most cases these will be redundant servers that duplicate servers in DC1.
    - DC2 will house network equipment necessary to maintain critical services at an adequate level of security
- We will install a secondary fiber infrastructure centered on DC2 using existing conduits
- This project will be completed as part of our next network upgrade by November, 2009.

Responsibility

- The responsibility for enforcing this policy lies with the Vice President of Technology, 597-4294.