



WESTERN
KENTUCKY
UNIVERSITY®

**Information Technology
Network Security Plan**

Updated 8/28/07

TABLE OF CONTENTS

1	Introduction.....	3
2	Responsibilities.....	3
3	General Provisions	4
4	Network Control.....	7
5	DHCP and DNS SERVICES.....	8
6	Firewall and VPN Security	9
7	Wireless Network Services	9
8	Destruction and Disposal of Information and Devices	9
9	Computer Labs	10
10	Virus Protection	10
11	Network Access.....	11
12	Security Assessment	11
13	Workstations.....	11
14	Software Licenses	12
15	Physical Access.....	12
16	Servers	13
17	Passwords	14
18	Email Usage	15
19	Employee Training and Management.....	15
20	Incident reporting.....	15
21	Incident Response.....	16
22	Violations	18
23	Privacy.....	18

1 Introduction

The Western Kentucky University Information Technology Network Security Plan serves to create an environment that will help protect all members of the University community from information security threats that could compromise privacy, productivity, reputation, or intellectual property rights. The Plan recognizes the vital role information plays in the University's educational, research, operational, and advancement missions, and the importance of taking the necessary steps to protect information in all forms. As more information is used and shared by students, faculty and staff, both within and outside the University, an effort must be made to protect information. This Plan serves to protect information resources from threats from both within and outside of the University by setting forth responsibilities, guidelines, and practices that will help the University prevent, deter, detect, respond to, and recover from compromises to these resources, and to foster an environment of secure dissemination of information.

2 Responsibilities

- 2.1 Because of the openness of the Internet, the actions of an individual can be seen as a reflection upon the University. As such, each person is expected to use their network access primarily for University-related purposes and to conduct themselves honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others.
- 2.2 Unnecessary or inappropriate network usage can cause network and server congestion, and can interfere with the ability of others to complete work or assignments in a timely manner. This is especially true when communicating with off-campus resources, due to limited bandwidth to the Internet. Unlawful Internet usage may also result in negative publicity and expose the individual or University to significant legal liabilities. Examples of inappropriate network usage that is strictly prohibited include, but are not limited to:
 - The transmission or posting of sexually explicit, racial, harassing or otherwise derogatory messages or images.
 - "Hacking" activities such as those used to attempt to gain access to systems or information to which access permission has not been explicitly granted. This includes unauthorized ping sweeps, port scans, network sniffing, exploiting system vulnerabilities, IP address spoofing, and password guessing.
 - The transmission or sharing of private or copyrighted information for which distribution rights have not been obtained.
- 2.3 The sending of unsolicited mass e-mails unrelated to the function of the University. Examples of this include e-mail chain letters and the advertisement of non-University items or services.

- 2.4 Through the use of chat rooms, newsgroups and e-mail, users have the unprecedented ability to reach tens, hundreds or many thousands of individuals with the click of a mouse. Because this ability allows us to propagate messages and share information in near real-time, special care must be taken to maintain the clarity, consistency and integrity of shared information.
- 2.5 While a connection to Western's network and the Internet offers many potential benefits, it can also open the door to some significant risks, if appropriate security measures are not followed. Security needs to be evaluated in terms of the services and information provided and who needs access to the information. Appropriate security can include a wide variety of physical and logical access controls, including passwords, access control lists, the location of network connections, physical location of computer hardware, firewall protection, data encryption, Virtual Private Networks and other methods of security, including the possibility of NOT connecting certain machines to the University network. Although Network and Computing Support is able to provide suggestions and discuss a variety of options for implementing network and system security, the ultimate responsibility for system and data security, including backups, rests with the system's administrator (or the user in the case of a single user system). It is the responsibility of the system administrator to ensure that appropriate steps are taken to protect machines and University information from malicious attack or loss. The overriding principle is that security must be everyone's first concern.

3 General Provisions

- 3.1 The communications network at Western Kentucky University is designed to provide students, faculty and staff with the infrastructure necessary to communicate with others, exchange ideas, promote learning and conduct the business necessary to support the mission of the University.
- 3.2 User accounts and passwords are implemented to maintain individual accountability for network resource usage. Any user who obtains an account and password for accessing a University provided resource, is required to keep that information confidential. Users of these systems may only use the accounts and passwords for which they have been assigned and authorized to use, and are prohibited from using the network to access these systems through any other means. This plan also prohibits the sharing of personal user accounts or passwords for accessing University or Internet computing resources. In the interest of maintaining account security, passwords should be changed on a regular basis or anytime the integrity of the account is in question.
- 3.3 All users of the University network shall identify themselves accurately and completely (including University affiliation and function where requested) when participating in chats or newsgroups, or setting up accounts on outside computer systems.

- 3.4 Communications-intensive operations such as large file transfers, video downloads, mass e-mailings and similar activities, should be scheduled for off-peak times when possible.
- 3.5 Any file that is downloaded must be scanned for viruses before it is run or accessed.
- 3.6 Employees with Internet access may download only software with direct business use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license.
- 3.7 Download or distribution of copyrighted materials without the express written consent of the owner (pirated software or data), including audio and video files, is expressly prohibited.
- 3.8 Western Kentucky University retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any employee in the course of his or her duties.
- 3.9 Users are reminded that chats and newsgroups are public forums where it is inappropriate, and in some cases illegal, to reveal confidential or personal information.
- 3.10 Users may not upload or redistribute any software licensed to the University or data owned by the University without the express authorization of the manager responsible for the software or data.
- 3.11 Sensitive information, or files containing sensitive University data which must be transferred across the network, should be considered vulnerable to interception by an unauthorized 3rd party and should be encrypted during transmission.
- 3.12 Western Kentucky University's network or computing resources may not be used for commercial purposes, for personal profit or to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of University resources for any illegal activity may result in loss of network access privileges, official reprimand, suspension or dismissal, and Network Services will cooperate with any legitimate law enforcement agency or inquiry in the investigation and prosecution of any alleged wrongful activity.
- 3.13 Users may be held legally and financially responsible for actions resulting from unauthorized use of University network and system accounts for which they are responsible.

- 3.14 The University's network and Internet facilities may not be used to intentionally propagate any virus, worm, Trojan horse, back-door program code or similar content.
- 3.15 The University's network or Internet facilities may not be used to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
- 3.16 Western Kentucky University has installed various network security devices, including account passwords and firewalls, to help assure the safety and security of University information. Any attempt to disable, defeat or circumvent any security facility is considered inappropriate activity and is a violation of this network policy.
- 3.17 The display of any kind of sexually explicit image or document on any University system, except possibly for Department approved research or instructional purposes, may be considered a violation of the University's policy on sexual harassment. In addition, because a wide variety of materials may be considered offensive by colleagues, students or contacts outside the University, sexually explicit material not required for an official program at the University, may not be archived, stored, distributed, edited or recorded using the University's network or Network Computing resources.
- 3.18 Reconfiguration of network hardware or software, except by designated individuals within Network and Computing Support, without prior approval by the Director, is strictly prohibited.
- 3.19 Prior to connecting any server, network communication or monitoring device to the University Network, approval must be obtained from Network Services.
- 3.20 Attachment of any the following devices to the campus network, other than those provided or approved by Network and Computing Support, is strictly prohibited:
 - DHCP servers.
 - DNS servers.
 - NAT routers.
 - Network Gateways.
 - Packet capturing or network monitoring devices.
 - Any device that disrupts or negatively impacts network operations.
- 3.21 Static assignment of IP addresses not approved and obtained through Network and Computing Support is not permitted.
- 3.22 University owned networking and communications equipment, may only be moved by Network and Computing Support staff, or authorized agents.

- 3.23 The owners of data stored on network accessible systems are responsible for managing and determining the appropriateness of information stored on these systems. This includes both private storage areas and “shared” folder areas.

4 Network Control

- 4.1 Network and Computing Support has software and systems in place that have the ability to monitor and record network, Internet and computer system usage. This includes monitoring and security systems that are capable of recording all network traffic, including traffic to World Wide Web sites, chat rooms, newsgroups and e-mail messages, file servers, telnet sessions and file transfers into and out of our internal networks. This capability is necessary in order to maintain normal network operations and diagnose network related problems. Network and Computing Support reserves the right to perform network monitoring at any time, and as such, individuals should have no expectation of privacy as to his or her network usage. Information derived in this manner may be used internally or provided to third-party vendors for diagnostic purposes. The information collected may be used by technicians and management to assess network utilization and trends, and may also be provided to upper management or other authorities as evidence in any investigation of alleged policy violations.
- 4.2 Network and Computing Support reserves the right to inspect files stored in private areas of the network for troubleshooting purposes or as part of an investigation into alleged policy violations.
- 4.3 Network and Computing Support reserves the right to perform periodic port scans and segment sweeps on all network segments.
- 4.4 Network services, functions and resources, which are not required as part of the normal and approved operation of the University, may be bandwidth limited or blocked by network control devices.
- 4.5 Network and Computing Support may suspend network access to any location or system that disrupts normal network operations or systems that violate university policy. In this event, an attempt will be made to contact the responsible individual to resolve the problem.

5 DHCP and DNS SERVICES

Network and Computing Support provides centralized and redundant DHCP and DNS services for the University. Due to the nature of these services, and because of the potential disruption of service and possible security breaches resulting from incorrect

setup of additional systems, attachment of unauthorized DHCP or DNS servers is prohibited. The following guidelines must be followed when requesting or using any DHCP or DNS services.

DHCP Guidelines

- 5.1 Systems requiring an IP address must support DHCP and be capable of obtaining DHCP address information from one of the centrally administered University DHCP servers.
- 5.2 Using DHCP, devices requesting an IP address will be assigned a dynamic pool address from the subnet to which the device is attached. Devices with dynamically assigned IP addresses may have their address change.
- 5.3 Static IP addresses needed for server class machines must be requested from Network and Computing Support. Once assigned, the IP address can be obtained by the machine via DHCP. The MAC address for any statically assigned IP address must be provided prior to assignment.
- 5.4 Static IP addresses for specialized equipment or machines incapable of using DHCP may be requested from Network and Computing Support. The MAC address for any statically assigned IP address must be provided prior to assignment.

DNS Guidelines

- 5.5 User workstations, which have been assigned a dynamic pool IP address, will have an associated DNS name of IPxxx-yy.bldg.wku.edu, where xxx is the IP host address assigned within the class-C subnet of yy associated with building bldg.
- 5.6 Any DNS name or domain name that is to be associated with Western's class-B IP network, must be requested from and/or registered through Network Services, and may not be separately registered outside the University.
- 5.7 Requests for assignment of DNS names must be for valid University purposes.
- 5.8 DNS names ending in wku.edu are made available upon request at no charge for University approved services.
- 5.9 DNS names for domains other than wku.edu, and which are to be hosted on University systems, must be requested from Network and Computing Support. Any charges for initial or ongoing registration of the requested name are the responsibility of the requestor.

- 5.10 Network and Computing Support will work with any user requesting a domain name to identify an appropriate and available name, however Network and Computing Support has final approval for all DNS name assignments.
- 5.11 DNS names, not in the wku.edu domain, will not be approved for use without compelling justification. For other domain names to be approved for use, it must be demonstrated that equivalent functionality cannot be provided under the existing wku.edu domain.

6 Firewall and VPN Security

- 6.1 Firewall security, including VPN access, is maintained by Network and Computing Support. Approval for access to any protected resource must be provided in writing from the appropriate system administrator before access will be granted.

7 Wireless Network Services

- 7.1 Because wireless networks can be used to provide access to the same resources and services as wired network systems, the same basic procedures that are used in a wired network environment can also be applied in a wireless network environment. However, due to the nature of wireless networks, additional security and control mechanisms are needed in order to maintain the security, operation and inter-operability of both traditional and wireless systems.
- 7.2 Please refer to Western Kentucky University Wireless Network Policy for more information about campus wireless technology, definitions, security, usage requirements, and general usage policy.

8 Destruction and Disposal of Information and Devices

- 8.1 Confidential information must be disposed of in such manner as to ensure it cannot be retrieved and recovered by unauthorized persons. For physical documents, shredders are highly recommended.
- 8.2 When donating, selling, transferring, surplus or disposing of computers or removable media (such as diskettes), care must be taken to ensure that confidential data is rendered unreadable. Any restricted information that is stored on the machines must be thoroughly erased. In general, it is insufficient to "delete" the information, as it may remain on the medium. The data should be properly removed from the drive either by software that meets US Department of Defense specifications by overwriting data on the medium at least 3 times, or the drive may be physically or electromagnetically destroyed.

9 Computer Labs

- 9.1 Computing Labs are provided for use by WKU students, faculty and staff only. Individuals should have a valid University Photo ID at all times while using the labs. Lab staff have the right to deny access to the Labs to anyone without proper identification.
- 9.2 Lab managers are responsible for the security of their labs and the lab's impact on the university network and any other networks.
- 9.3 Lab managers bear first line responsibility for the lab's compliance with all WKU security policies. The following are particularly important: Password Policy, Anti-Virus Policy, Wireless Security, and Physical Access.
- 9.4 Network and Computing Support reserves the right to disable lab connections that negatively impact the university network or pose a security risk.
- 9.5 All user passwords must comply with WKU's Password Policy. Individual user accounts on any lab device must be deleted once access is no longer authorized.
- 9.6 Lab machines are prohibited from engaging in port scanning, traffic spamming/flooding, or other similar activities that negatively impact the University network and/or non-university networks.
- 9.7 Network equipment such as hubs, switches, routers, and wireless access points may not be placed in university labs without authorization from Network Services.

10 Virus Protection

- 10.1 All University owned computers must run University supported anti-virus software. Network and Computing Support provides virus protection software for University owned machines.
- 10.2 The anti-virus software and the virus pattern files must be kept up-to-date.
- 10.3 Virus-infected computers must be removed from the network until they are verified as virus-free.
- 10.4 Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are virus-free.
- 10.5 Any activities with the intention to create and/or distribute malicious programs into WKU's networks (e.g., viruses, worms, Trojan horses, etc.) are prohibited.

11 Network Access

11.1 Anyone who uses the campus computing environment must have appropriate status (e.g. staff, faculty and current students) and must be properly authenticated when required.

11.2 Users must not:

- Perform acts that negatively impact the operation of computers, peripherals or network, or that impedes the ability of someone else to do his/her work.
- Attempt to circumvent protection schemes for access to data or systems.
- Gain or grant unauthorized access to computers, devices, software or data.

12 Security Assessment

12.1 Network and system security will be assessed on a periodic basis.

12.2 When a security concern is identified, the responsible party will be notified, at which point the problem must be addressed in a timely manner.

13 Workstations

13.1 Users are responsible for the security and integrity of University information stored on their workstation, which includes controlling physical and network access to the equipment.

13.2 Users may not run or otherwise configure software or hardware that may allow access by unauthorized users.

13.3 Employees must not access workstations which have not been provided to them for their work without the express permission of their department head.

13.4 Anti-virus software must be installed on all workstations that connect to the University Network.

13.5 To protect data integrity, computer equipment may not be removed from the office area without the department head's prior approval.

13.6 University Computers may not be used to copy, distribute, share, download, or upload any copyrighted material without the permission of the copyright owner.

14 Software Licenses

- 14.1 Virtually all software, music, movies, books and other intellectual property is protected by copyright law. As such, users may use it only according to the terms of the license the agreement, often referred to as EULA (End User License Agreement). Copying or transfer of copyrighted materials without authorization is prohibited.
- 14.2 All users are legally liable to the license issuer or copyright holder.
- 14.3 Placing unlicensed or illegally obtained software, music, movies, or documents on University computers is strictly prohibited.

15 Physical Access

- 15.1 Access should only be granted to persons with proper authorization to access the corresponding area.
- 15.2 Access to areas where administrative information is stored without prior authorization is prohibited.
- 15.3 Supervisors must ensure that employees separating from employment with the University or transferring to another department return their physical access keys and cards.
- 15.4 If an employee does not return their access key, areas accessible by the outstanding keys need to be re-keyed.
- 15.5 University information or records may not be removed (or copied) from the office where it is kept except in performance of job responsibilities.
- 15.6 Access to WKU's computer operations areas should be restricted to those responsible for operation and maintenance.
- 15.7 Access to WKU's Information Technology Data Center by non-IT personnel is not permitted unless they are escorted by an authorized IT staff member.
- 15.8 Key access is granted on an individual basis and in no case should be lent or given to others.
- 15.9 Computer installations should provide reasonable security measures to protect the computer system against natural disasters, accidents, loss or fluctuation of electrical power, and sabotage.

15.10 Adequate disaster recovery plans and procedures are required for critical systems data.

15.11 Networking and computing hardware should be placed in a secure environment.

16 Servers

16.1 All servers are subject to a security audit and evaluation before they are placed into production.

16.2 Administrative access to servers must be password protected.

16.3 Servers should be physically located in an access-controlled environment.

16.4 All internal servers deployed at WKU must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group.

16.5 Servers must be registered with the IT department. At a minimum, the following information is required to positively identify the point of contact:

- Server owner contact(s) and location.
- Hardware and Operating System/Version
- Main functions and applications
- MAC address

16.6 Network and Computing Support should be kept up-to-date with any changes to Server information.

16.7 Operating System configuration should be in accordance with approved security guidelines.

16.8 Services and applications that will not be used must be disabled where practical.

16.9 Access to services should be logged and/or protected through access-control methods to the extent possible.

16.10 The most recent security patches must be installed on the system as soon as practical.

16.11 Do not use administrator or root access when a non-privileged account can be used.

16.12 Privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

- 16.13 All security-related events on critical or sensitive systems must be logged and audit trails saved.
- 16.14 Security-related events should be reported to the IT HelpDesk. Security-related events include, but are not limited to:
- Evidence of unauthorized access to privileged accounts
 - Evidence of access to information by an unauthorized viewer.
 - Anomalous occurrences that are not related to specific applications on the host.
 - Audits may be performed on university and departmental servers periodically without prior notice.

17 Passwords

- 17.1 Passwords are designed to prevent unauthorized access to information. Users are responsible for safeguarding passwords and are accountable for negligent disclosure of passwords.
- 17.2 Passwords should be complex and difficult to guess which would include:
- The use of both letters, numbers and special characters
 - The use of upper and lower case
 - A minimum of 6 characters in length
- 17.3 Passwords should be changed every 3 to 6 months or immediately if compromised.
- 17.4 Passwords should never be a persons name or a dictionary word.
- 17.5 Passwords should be memorized and never written down.
- 17.6 When possible, passwords should not be inserted into email messages or other forms of electronic communication.
- 17.7 Do not use the same password for WKU accounts as for other personal accounts.
- 17.8 WKU accounts or passwords should not be shared. All passwords are to be treated as sensitive, confidential information.

18 Email Usage

- 18.1 Email is not a secure medium and therefore employees should have no expectation of privacy associated with Email transmissions. However, electronic mail is kept as private as possible. Attempts to read another person's electronic mail will be treated with the utmost seriousness.
- 18.2 No e-mail may be sent or forwarded through a University system or network for purposes that violate University guidelines or for an illegal or criminal purpose.
- 18.3 Nuisance e-mail or other online messages such as chain letters, obscene, harassing, or other inappropriate messages are prohibited.
- 18.4 Unsolicited e-mail messages to multiple users are prohibited unless explicitly approved by the appropriate University authority. All messages must show accurately from where and from whom the message originated.
- 18.5 The University reserves the right to reject mail and other connections from outside hosts that send unsolicited, mass or commercial messages (spam), or messages that appear to contain viruses.
- 18.6 The University and its administrators of central e-mail systems will not read mail unless necessary in the course of their duties.

19 Employee Training and Management

- 19.1 Each department is responsible for ensuring its employees are trained to take steps to maintain security, confidentiality and integrity of personal information, such as:
 - Securing rooms and cabinets where records are kept;
 - Using strong passwords and not posting, sharing, or releasing passwords;
 - Recognizing any fraudulent attempt to obtain student information and reporting it to appropriate department or law enforcement agencies.

20 Incident reporting

- 20.1 WKU employees must immediately report the following to their managers and the IT Network Security Specialist:
 - An actual or suspected security incident that involves unauthorized access to electronic systems owned or operated by WKU
 - Malicious alteration or destruction of data, information, or communications; unauthorized interception or monitoring of communications;

- Any deliberate and unauthorized destruction or damage of IT resources.
- Unauthorized disclosure or modification of electronic institutional or personal information

20.2 Incidents will be treated as confidential unless there is a need to release specific information.

21 Incident Response

21.1 The IT Network Security Specialist is the primary point of contact for responding to and investigating incidents related to misuse or abuse of Western Kentucky University information technology resources. This includes computer and network security breaches and unauthorized disclosure or modification of electronic institutional or personal information.

21.2 Upon discovery of a security breach, provide initial notification of the breach to:

- The Network Security Specialist
- The affected system's owner (administrative responsibility for the system)
- System Administrator (technical support responsibility for the system)
- Other individuals as required by the circumstances

This group will comprise the Incident Response Team for a specific incident. After initial notification, provide information updates as appropriate throughout the incident response process.

21.3 Communications with the media and public should be restricted to University Public Relations and the University's General Counsel. University employees involved in the incident or the incident's response and investigation should refer all media and other public inquiries to Public Relations or General Counsel.

21.4 Create a log of all actions taken and maintain this log consistently throughout the response process.

21.5 Secure the affected area(s). Electronic evidence can be easily destroyed, resulting in the inability to determine if confidential information has been compromised, or to provide evidence for future prosecution. Identify potential evidence, both conventional (physical) and electronic, and determine if perishable evidence exists. For example, do not alter the condition of any electronic device by either turning it on, off or rebooting it until it is determined that it is safe to do so. Inventory and evaluate the scene.

21.6 Assess the need for forensic information, such as that gathered from packet traces and system monitoring utilities, which can aid in understanding the nature and scope of the incident and provide evidence for any potential criminal

- investigation. During this process, consider both the potential value of forensic information vs. the immediate need to protect and restore University resources and services. Document the decision process.
- 21.7 Collect and save any forensic information identified in the previous two steps. This may include video records, access logs, system logs, network traces, IP addresses, MAC addresses, data backups, system images or affected computer hardware.
 - 21.8 Regain control of the compromised system. This may include network disconnection, process termination, system shutdown, or other action as indicated to prevent further compromise of protected information.
 - 21.9 Analyze the intrusion. Document the nature of the intrusion and its impact on information and process integrity. Determine if unauthorized individuals may have acquired restricted information. Determine the identity of those whose data may have been acquired. Estimate the potential cost, in time, money and resources, of the intrusion to the University.
 - 21.10 Correct any identifiable system or application vulnerabilities that allowed the intrusion to occur.
 - 21.11 Verify system and data integrity.
 - 21.12 Restore service once the integrity of the system and/or information has been verified.
 - 21.13 The incident response team shall create an incident report with all relevant information. The report should include:
 - Date and time the incident occurred
 - Description of incident
 - Detailed list of system(s) and data which were compromised
 - Identifiable risks to other systems or information
 - Corrective actions taken to prevent future occurrences
 - Estimated costs of incident and any corrective actions
 - Identity of those responsible for the incident (if available)
 - 21.14 The VP/IT and University Counsel, with input from the Incident Response Team and other appropriate individuals, shall determine if disciplinary action should be taken, criminal charges filed against those involved, and which individuals should be notified.

22 Violations

Any violation of these rules may lead to suspension of access to Information Technology resources, with the possibility of revocation of privileges, or other action as provided by disciplinary provisions applicable to faculty, staff, or student. Cases of suspected violations of local, state or federal laws will be turned over to the University Attorney and/or the appropriate law enforcement agency.

23 Privacy

Western Kentucky University endeavors to ensure that its treatment, custodial practices, and uses of "Personal Information" are in full compliance with all related federal and state statutes and regulations.

The University commits to take reasonable precautions to maintain privacy and security of students' and employees' personal information. The University cannot guarantee that these efforts will always be successful; therefore, users must assume the risk of a breach of University privacy and security systems.

The University does not intend to sell, swap, rent, or otherwise disclose for commercial purposes, outside the scope of ordinary University functions, students' and employees' name, mailing address, telephone number, e-mail address, or other information. While the University makes reasonable efforts to protect information provided to us, we cannot guarantee that this information will remain secure and are not responsible for any loss or theft.

Personally identifiable information is defined as data or other information which is tied to, or which otherwise identifies, an individual or provides information about an individual in a way that is reasonably likely to enable identification of a specific person and make personal information known about them.

Personal information includes, but is not limited to, information regarding a person's social security number, driver's license, marital status, financial information, credit card numbers, bank accounts, parental status, gender, race, religion, political affiliation, personal assets, medical conditions, medical records or test results, personnel or student records.

Local and home address and telephone numbers are considered directory information and will be released to the public unless a request is filed to prevent disclosure of the information, except for official university business. Employees who request confidentiality of that information should contact the Department of Human Resources, and students should contact the Office of the Registrar within the first five days of the term.

Western assumes that failure on the part of any student or employee to specifically request the withholding of categories of information indicates individual approval for disclosure.

Personal information may only be released or provided to others as follows:

To employees and/or officers of the University or an authorized need-to-know basis, and only to those individuals who are authorized to use such information as part of their official university duties, and with the requirements: (1) that they keep that information confidential and use it only for, and to the extent required by, the official university business purposes that they are authorized to perform; and, (2) that they do not further disclose or provide that information to others.

A student's record may be released in compliance with a court order or subpoena. The University General Counsel will make a reasonable effort to notify the student in advance of compliance.

Student information may be released for health and emergency reasons.

The scope of individuals covered by this policy includes all individuals on whom the University, or any part of the university, or any employee, student, volunteer or contractor etc. of the university, has or maintains personal information. This includes students, employees, donors, patients, alumni, referring physicians, research subjects, individuals identified in research files, volunteers and others.

The University is bound by the Family Educational rights and Privacy Act (FERPA) regarding the release of student education records, and in the event of a conflict with University policies, FERPA will govern. A guide to understanding FERPA is available from the Office of the Registrar. The Notification of Rights is printed in each term's schedule bulletin, the catalog, and is available on the Office of the Registrar website.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA) NOTIFICATION OF RIGHTS

The Family Educational Rights and Privacy Act (FERPA) affords students certain rights with respect to their education records, including:

(1) The right to inspect and review the student's education records within 45 days of the day the University receives a request for access. Students should submit to the registrar, dean, head of the academic department, or other appropriate official, a written request that identifies the record(s) they wish to inspect. The University official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the University official to whom the request was submitted,

that official shall advise the student of the correct official to whom the request should be addressed.

(2) The right to request the amendment of the student's education records that the student believes are inaccurate or misleading. Students may ask the University to amend a record that they believe is inaccurate or misleading. They should write the University official responsible for the record, clearly identify the part of the record they want changed, and specify why it is inaccurate or misleading.

If the University decides not to amend the record as requested by the student, the University will notify the student of the decision and advise the student of his or her right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.

(3) The right to consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent, including:

(a) Disclosure without the student's consent is permissible to school officials with legitimate educational interests. A school official is a person employed by the University in an administrative, supervisory, academic, research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the University has contracted (such as an attorney, auditor, or collection agent); a person serving on the Board of Regents; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

(b) FERPA allows the institution to routinely release information defined as "directory information." The following student information is included in the definition: the student's name, address, e-mail address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, enrollment status (including full-time, part-time, not enrolled, withdrawn and date of withdrawal), degree and awards received and the most recent previous education agency or institution attended by the student. When a student wants any part of the directory information to remain confidential, an official request form must be completed in the Office of the Registrar within the first five days of class of each school term.

(4) The right to file a complaint with the U.S. Department of Education concerning alleged failures by Western Kentucky University to comply with the requirements of FERPA. The name and address of the Office that administers FERPA is:

Family Policy Compliance Office
U.S. Department of Education
600 Independence Avenue, SW
Washington, DC 20202-4605

Questions pertaining to the Family Educational Rights and Privacy Act may be directed to Freida K. Eggleton, Registrar, 238 Potter Hall, 745-5432.