Information Security Plan

In compliance with the Gramm Leach Bliley Act of 1999

Table of Contents

Information Security Plan **3**

Identification and Assessment of Risks to Customer Information **3**

Data Classification **4**

Information Security Plan Coordinators **6**

Design and Implementation of Safeguards Program **6**

- **Employee Management and Training** **6**
- **Physical Security** **7**
- **Information Systems** **7**
- **Management of System Failures and Compromises** **7**

Selection of Appropriate Service Providers **7**

Information Technology Division General Security Considerations **8**

- **Computer Labs** **8**
- **Anti-Virus** **9**
- **Network Control and Access** **9**
  - DHCP Guidelines 10
  - DNS Guidelines 10
- **Security Assessment** **11**
- **End-User Devices (Workstations, Laptops, Tablets, Mobile Devices, etc.)** **11**
- **Software Licenses** **11**
- **Physical Access** **11**
- **Servers** **12**
- **Passwords** **13**
- **Physical Assets** **13**
- **Wireless Access** **14**

Destruction and Disposal of Information and Devices 14
Employee Training and Management 14
Sensitive Data Protection 14
Privacy Statement 16
Family Educational Rights and Privacy Act (FERPA) 18
Notification of Rights 18
Incident Reporting 19
Incident Response 19
University Individual Department Procedures 21
ID Center 21
Department of Student Financial Assistance 21
Office of the Bursar 21
Office of Admissions 22
Department of Housing and Residence Life 23
Office of the Registrar 26
Violations 26
Continuing Evaluation and Adjustment 26
Revision History 27
Review Date ..... Error! Bookmark not defined.

Information Security Plan

This Information Security Plan describes Western Kentucky University's safeguards to protect data, information, and resources as required under the Gramm Leach Bliley Act. These safeguards are provided to:

- Make reasonable efforts to ensure the security and confidentiality of covered data, information, and resources;
- protect against anticipated threats or hazards to the security or integrity of such information; and
- protect against unauthorized access to or use of covered data, information, and resources that could result in substantial harm or inconvenience to any customer.

This Information Security Plan also provides for mechanisms to:

- Identify and assess the risks that may threaten covered data, information, and resources maintained by the University;
- manage and control these risks;
- implement and review the plan; and
- adjust the plan to reflect changes in technology, the sensitivity of covered data, information and resources, and internal or external threats to information security.

Identification and Assessment of Risks to Customer Information

The University recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of covered data, information, and resources by someone other than the owner of the covered data, information, and resources;
- compromised system security as a result of system access by an unauthorized person;
- interception of data during transmission;
- loss of data integrity;
- physical loss of data in a disaster;
- errors introduced into the system;
- corruption of data or systems;
- unauthorized access or distribution of covered data, information, and resources by employees, students, affiliates, or other constituencies;
- unauthorized requests for covered data, information, and resources;
- unauthorized access through hardcopy files or reports; and
- unauthorized transfer of covered data, information, and resources through third parties.

The University recognizes that this may not be a complete list of the risks associated with the protection of covered data, information, and resources. Since technology is not static, new risks are created

regularly. Accordingly, IT staff will monitor industry sources and advisory groups such as the Educause Security Institute, the Internet2 Security Working Group, and SANS for identification of new risks.

The University believes current safeguards are reasonable and, in light of current risk assessments, are in line with common practices to provide security and confidentiality to covered data, information, and resources maintained by the University. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information. However, the University cannot guarantee the unequivocal security of covered data, information, and resources given the evolving and ever-changing state of IT environments and threats thereto.

Data Classification

There are varying levels or classifications of data stored at and by WKU. Table 1 below describes these classes.

Table 1: Classes of Data at WKU

Class	Description	Examples
Confidential	University-related information is classified as CONFIDENTIAL if access by unauthorized parties could cause the entity to incur substantial University losses. This includes, in particular: 1. Detailed information that can affect the WKU brand and that is not general knowledge to the public; 2. Sensitive, important information which can eventually develop into "insider" information; and 3. Other information which, for commercial or other reasons, should be kept secret from unauthorized parties. Access to information that is CONFIDENTIAL must be approved by the information owner.	• Documentation for the Board of Regents, Administrative Council or other Executive Board at WKU • Non-published accounting material • Budgets and strategy memoranda • Information about major transactions, University partnerships, or contracts • University-critical agreements • Sensitive personal information • Information about strategic or other long-term developments • Significant innovation projects • University-critical intellectual property • Attorney Work Product • Sensitive University Plans
Regulated	Governed by regulatory restrictions, REGULATED data is only accessible to authorized WKU personnel. Extreme care and special precautions are required before its usage, storage, and transmittal. It is forbidden to show or discuss REGULATED data with unauthorized parties. The unauthorized disclosure of such data could adversely affect WKU, its students, employees, business partners, and/or other constituents and may violate local, state, or federal regulations. Disclosing REGULATED data to the public results in WKU experiencing a significant adverse impact. Such an event may: • Cause WKU or its constituents to incur financial or legal liabilities, • Violate regulatory compliance guidelines, or • Undermine confidence in the University.	Regulated Data is information that is protected by federal law, industry specific regulations or industry specific mandates such as: • Health Insurance Portability and Accountability Act (HIPAA) • Personally Identifiable information (PII) as defined in the Kentucky Data Breach Notification Law, KRS 365.7 • Payment Card Industry Data Security Standard (PCI DSS)
Internal Use Only	This class covers University-related information that is not classified as CONFIDENTIAL, REGULATED or PUBLIC. Access to such information is restricted and shall be accessible only to those who need the information to perform their jobs. Accordingly, most University-related information at WKU will belong to this class.	• Internal letters, memos, e-mails, and reports • Internal policies, instructions and procedures • Information associated with routine University activities (students, business partners, services) • Knowledge Base or Intellectual Property • Non-sensitive personal data

Public	University-related information can only be classified as PUBLIC if the information has been quality controlled and approved for publication by a department manager or WKU 's division of Public Affairs. Information can only be classified as PUBLIC by being reclassified from INTERNAL USE ONLY or CONFIDENTIAL or following the expiration or repeal of all applicable regulations.	• Information posted on the Internet or published in other types of media • Manuscripts and files for presentations (after they are approved for external use) • Marketing, e.g. campaign material

Information Security Plan Coordinators

The Registrar and the VP for Information Technology have been appointed as the coordinators of this plan. They are responsible for assessing the risks associated with unauthorized transfers of covered data, information, and resources. They are also responsible for implementing procedures to minimize those risks to the University and/or conducting audits of this plan on a periodic basis.

Design and Implementation of Safeguards Program

Employee Management and Training

References of new employees working in areas that regularly work with covered data, information, and resources (e.g., Information Technology, Office of Bursar, and Admissions) are checked. Additionally, criminal background checks are conducted on all employees of the University hired after July 12, 2006. Other checks could include identity verification, education verification, moving violation record, credit report, and professional licenses.

During employee orientation, each new employee in departments that regularly work with covered data, information, and resources will receive proper training on the importance of confidentiality of student records, student financial information, and other types of covered data, information, and resources. Each new employee is also trained in the proper use of computer information and passwords. Training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including "pretext calling"[1] and how to properly dispose of documents that contain covered data, information, and resources.

Each department responsible for maintaining covered data, information, and resources is instructed to take steps to protect the information from destruction, loss, or damage due to environmental hazards, such as fire and water damage or technical failures. Further, each department responsible for maintaining covered data, information, and resources should coordinate with the plan coordinators on an annual basis for the review of additional privacy training appropriate to the department. These

[1] "Pretext calling" occurs when an individual improperly obtains personal information of University customers so as to be able to commit identity theft. It is accomplished by contacting the University, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit, convincing an employee of the University to release customer identifying information.

training efforts should help minimize risk and safeguard covered data, information, and resources security.

Physical Security

The University has addressed physical security by placing access restrictions at buildings, computer facilities, and records storage facilities containing covered data, information, and resources to permit access only to authorized individuals. These locations are to be locked, and only authorized employees are permitted to possess keys or combinations to them. Paper documents that contain covered data and information are to be shredded at time of disposal.

Information Systems

Access to covered data, information, and resources via the University's IT Infrastructure is limited to those employees who have a business reason to know such information. Each employee is assigned a set of unique credentials. Databases containing personal covered data, information, and resources including, but not limited to, accounts, balances, and transactional information are available only to University employees in appropriate departments and positions.

The University will take reasonable and appropriate steps consistent with current technological developments to make sure that all covered data, information, and resources are secure and to safeguard the integrity of records in storage and transmission. The University requires that all servers must be registered before being implemented in a University data center or before access to them is allowed through data center firewalls, thereby allowing verification that the system meets necessary security requirements as defined by the IT Division. These requirements include maintaining the operating system and applications, including application of appropriate patches, and updates in a timely fashion. Authentication is also required of users before they can access University-protected data. In addition, security systems have been implemented to assist with detection and mitigation of threats, along with procedures to handle security incidents when they do occur.

When reasonable, encryption technology will be utilized for both storage and transmission. All covered data, information, and resources will be maintained on servers that are behind a firewall.

Management of System Failures and Compromises

The University has developed written plans and procedures to detect actual or attempted attacks on University systems and has Incidence Response plans in place which outline procedures for responding to an actual or attempted unauthorized access to covered data, information, and resources. Incidence Response and Reporting procedures are detailed later in this document.

Selection of Appropriate Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, external resources may be needed to provide services the University determines it will not provide on its own. In the process of choosing a service provider that will maintain or regularly access covered data, information, and resources, the evaluation process shall include the ability of the service provider to

safeguard confidential financial information. Contracts with service providers may include the following provisions:

- An explicit acknowledgement that the contract allows the contract partner access to confidential information;
- a specific definition or description of the confidential information being provided;
- a stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- an assurance from the contract partner that the partner will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information;
- a provision providing for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract;
- an agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles the University to terminate the contract without penalty; and
- a provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.

Information Technology Division General Security Considerations

Computer Labs

1. Computing labs are provided for use by WKU students, faculty, and staff. In cases that a computer lab does not have logon authentication, 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.
2. Guests are allowed to use computer labs for a limited period of time when access has been requested by an authorized faculty or staff member and approved by the Coordinator of Student Technology. Guest accounts are password protected.
3. Lab managers are responsible for the security of their labs and their labs' impact on the University IT infrastructure.
4. Lab managers are responsible for the lab's compliance with all WKU security policies.
5. The IT Division reserves the right to disable lab connections that negatively impact the University network or pose a security risk.
6. Labs machines are prohibited from engaging in port scanning, traffic spamming/flooding, and other similar activities that negatively impact the University network and/or non-University networks.
7. Labs must not advertise network services that may compromise University network integrity or put lab information at risk.
8. Network equipment such as hubs, switches, routers, and wireless access points may not be placed in University labs without written authorization from the WKU IT Division.

Anti-Virus

1. All WKU PC-based computers must have WKU's standard, supported anti-virus software installed.
2. The anti-virus software and the virus definitions must be kept up-to-date.
3. Virus-infected computers may be removed from the network until they are verified as virus-free.
4. Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is in place, operating correctly, and computers are virus-free.
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.

Network Control and Access

1. Anyone who uses the campus computing environment must be properly authorized.
2. Users must not
    - perform acts that negatively impact the operation of computers, peripherals, or networks or that impedes the ability of someone else to do his/her work;
    - attempt to circumvent protection schemes for access to data or systems; or
    - gain or grant unauthorized access to computers, devices, software, or data.
3. Users may be held legally and financially responsible for actions resulting from unauthorized use of University network and system accounts.
4. WKU has installed various network security devices, including account passwords and firewalls, to help ensure 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.
5. Expansion or manipulation of network hardware and/or software, except by designated individuals within the IT Division, without prior approval from the IT Division, is strictly prohibited.
6. Prior to connecting any server to the University network, approval must be obtained in writing from the WKU IT Division.
7. Attachment of any the following devices to the campus network, other than those provided or approved by the IT Division, is strictly prohibited:
    - DHCP servers
    - DNS servers
    - NAT routers
    - Packet capturing technology
    - Any device that disrupts or negatively impacts network operations
8. Static assignment of IP addresses not approved and obtained through the IT Division is not permitted.
9. Only IT Division staff or authorized agents may move University-owned networking and communications equipment.

10. 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.
11. Only authorized merchants may use university networks, wired or wireless, to accept credit card payments. Use of WKU networks by these merchants must comply with WKU policy 3.3101, Policy & Procedures for Credit Card Merchants, which describes the process of becoming an authorized merchant. Merchants must also notify and receive approval from the Office of IT Security and Identity Management before using WKU networks to accept payments and must comply with current Payment Card Industry Data Security Standards (PCI DSS).
12. DHCP and DNS Services – the IT Division 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

- By default, 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.
- 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 changed.
- Reserved IP addresses needed for devices functioning as servers must be requested from the IT Division. Once assigned, the IP address must be obtained by the machine via DHCP. The MAC address for any reserved IP address must be provided prior to assignment.
- Static IP addresses to be hard-coded for specialized equipment incapable of using DHCP may be requested from the IT Division. The MAC address for any statically assigned IP address must be provided prior to assignment.
- The IT Division must be informed of any changes to equipment utilizing reserved or static IP addresses.

DNS Guidelines

- Any domain that is to be associated with WKU's class-B IP network must be registered with the IT Division.
- Requests for assignment of DNS names must be for valid University purposes.
- DNS names ending in wku.edu are made available upon request at no charge for University approved services.
- DNS names for domains other than wku.edu and which are to be hosted on University systems, must be requested from the IT Division. Any charges for initial or ongoing registration of the requested name are the responsibility of the requestor.

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

Security Assessment

1. Network and system security will be assessed on a periodic basis.
2. Security testing and audits will be conducted on a periodic basis.
3. If a security concern is found, the responsible party will be notified so the problem can be addressed. Depending on the severity of the concern the device may be removed from the network.

End-User Devices (Workstations, Laptops, Tablets, Mobile Devices, etc.)

1. Users are responsible for the security and integrity of University information stored on their end-user devices, which includes controlling physical and network access to the equipment. This includes personally owned devices to the extent they access University IT services or contain University data of any kind. Storage of sensitive or personal covered data on mobile devices is strictly prohibited.
2. Users may not run or otherwise configure software or hardware that may allow access by unauthorized users.
3. Employees must not access University-owned end-user devices that have not been provided to them for their work without the express permission of their department head.
4. Employees accessing University IT services and systems with their own personal devices must adhere to all IT polices
5. Anti-virus software must be installed on all workstations/laptops that connect to the University network.

Software Licenses

1. Virtually all commercially developed software is copyrighted; and the users may use it only according to the terms of the license the University obtains.
2. Duplicating such software with the intent to redistribute or installing multiple instances of such software without authorization is prohibited.
3. All users are legally liable to the license issuer or copyright holder.
4. Placing unlicensed or illegally obtained software, music, movies, or documents on University computers is strictly prohibited.

Physical Access

1. Access should only be granted to any person with proper authorization to access the corresponding area.

2. We comply with the University's least required access for distribution of keys.
3. Unauthorized access to areas where personally identifiable information is stored is prohibited.
4. Supervisors must ensure that staff who (voluntarily) terminate their employment with the department return their physical access keys and cards on their last day of work in that unit.
5. Employees who are (involuntarily) dismissed from the institution must return their keys and other access control devices/cards at the time they are notified of their dismissal. Any access granted to access control devices/cards must be removed immediately.
6. If an employee does not return his/her keys, areas controlled by the outstanding keys must be rekeyed.
7. University information or records may not be removed (or copied) from the office where it is kept except in performance of job responsibilities.
8. Access to WKU IT Infrastructure operations areas shall be restricted to those responsible for operation and maintenance.
9. 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.
10. Key access is granted on an individual basis and in no case should be lent or given to others. Some units leverage electronic key cabinets to allows the physical keys to be a shared resource but under auditable conditions.
11. Computer installations should provide reasonable security measures to protect the computer system against natural disasters, accidents, loss or fluctuation of electrical power, and sabotage.
12. Adequate disaster recovery plans and procedures are required for critical systems data.

Servers

1. Administrative access to servers containing or processing protected data must be password protected.
2. Servers should be physically located in an access-controlled environment.
3. All servers deployed at WKU must be approved by the IT Division. Server maintenance plans must be established and maintained by each operational group and approved by the IT Division.
4. All servers must be registered with the IT Division. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location;
    - hardware and operating system/version;
    - main functions and applications, if applicable; and
    - MAC address
5. Network Services should be kept up-to-date with any changes to server information.
6. Operating system configuration should be in accordance with approved security best practices.
7. Services and applications that will not be used must be disabled where possible.
8. Access to services should be logged and/or protected through access-control methods if possible.
9. The most recent patches must be installed on the system as soon as practical.
10. Do not use accounts with elevated privileges (such as administrator or root) access when a non-privileged account can be used.

11. Privileged access must be performed via an encrypted network protocol (such as SSH, HTTPS, RDP) and/or over an encrypted VPN tunnel).
12. All security-related events on critical or sensitive systems must be logged and audit trails saved for a minimum of 30 days.
13. Security-related events will be reported to the Office of IT Security and Identity Management, who will review logs and prescribe corrective measures as needed. Security-related events include, but are not limited to:
    - Port-scanning or Distributed Denial of Service attacks.
    - 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.
14. Audits may be performed on any device utilizing WKU Network resources at the discretion of the Office of IT Security and Identity Management.

Passwords

1. Passwords are designed to prevent unauthorized access to information. Users are responsible for safeguarding passwords along with other authentication mechanisms (such as user names, PINs, etc.) and are accountable for negligent disclosure of passwords.
2. Passwords should be a minimum of 8 characters long and constructed of a combination of alpha and numeric characters.
3. Passwords changes are required every 180 days at a minimum or immediately if compromised. Systems should automatically expire passwords at regular intervals and require the user to reset the password in accordance with the requirements for that system.
4. Passwords should be memorized and never written down.
5. Passwords should not be stored in electronic form – in computer files or on portable devices such as USB memory keys unless strongly encrypted.
6. Passwords should not be stored in browser caches or other "auto complete" types of features available in browsers and other software. These password "memorization" functions should be disabled and never utilized.
7. Passwords must not be inserted into email messages or other forms of electronic communication without the use of strong encryption.
8. Do not use the same password for WKU accounts as for other non-WKU access (e.g., personal ISP account, option trading, benefits, etc.).
9. WKU accounts or passwords should not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
10. Password "lockout" features should be enabled on any systems where it is available and reasonable to implement. Users will be locked out of systems after X number of unsuccessful attempts in Y period of time to log in and will require Helpdesk intervention to regain access.

Physical Assets

1. Networking and computing hardware should be placed in a secure environment and space shall be dedicated to the functions whenever possible.

2. Employees must know where the fire suppression equipment is located and how to use it.
3. Materials should not be stored on top of or directly next to equipment; proper airflow and environmental conditions must be maintained.

Wireless Access

1. This policy strictly prohibits access to WKU network resources via open, unsecured wireless communication mechanisms except for the “WKU-GUEST” wireless network provided by the University IT Division for the convenience of visiting constituencies. This guest network will have restricted access to non-confidential resources.
2. Wireless access points not sanctioned by the WKU IT Division are prohibited.

Destruction and Disposal of Information and Devices

1. Confidential information must be disposed of in such manner as to ensure it cannot be retrieved and recovered by unauthorized persons. Physical documents must be shredded.
2. When donating, selling, transferring, surplusing, or disposing of computers or removable media, care must be taken to ensure that confidential data is rendered unreadable. Any restricted information that is stored must be thoroughly destroyed. 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 U.S. Department of Defense specifications or the drive may be physically or destroyed.

Employee Training and Management

1. Employees who have access to University Banner information must sign an agreement to follow WKU’s confidentiality and security standards.
2. Employees and affiliate users who have access to systems or data that IT considers to be of a sensitive nature must annually complete an interactive online training program regarding the handling of sensitive data and applicable laws and/or policies. Notice of this requirement will be communicated directly with these employees and/or their supervisor(s). Failure to complete the annual training by the deadline contained within the notice will result in the revocation of access to the data or application.
3. 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; and
    - reviewing all IT Policies.

Sensitive Data Protection

Special care and awareness is required with regard to “sensitive data.” Sensitive data are any data that the unwarranted and/or unauthorized disclosure of such would have an adverse effect on the institution or individuals to which it pertains. Unauthorized disclosure or mishandling of sensitive data can be a

violation of federal and state law and the institution and its employees can be held personally liable for damages or remediation costs.

Data related to identity theft such as social security number (SSN), credit card numbers, bank account information, driver's license, name, address, birthdate, passwords, Personal Identification Numbers (PINs), and ID pictures are of particular concern as all or most of this information is collected in the course of University business. Other types of data such as medical information, tax returns, donor information, mailing lists, scholarship information, financial information, and bidding information are examples of data that could require confidential handling or restricted access. These examples are not exhaustive or all inclusive. It is the responsibility of University employees handling any University data to understand what data are sensitive and confidential and to adhere to the following guidelines and any applicable regulations.

1. Do not collect and/or store SSNs unless it is required by a federal or state agency and there is no other option in terms of unique identifier. If collection and storage of SSNs are required for operations in a given unit, register this by sending an email to ITSecurity@wku.edu explaining why the SSNs must be utilized and how and where they are being collected/stored.
2. Use the WKUID assigned to all individuals as the unique identifier for all WKU entities. If WKUID is not available or does not exist for certain populations, use a non-SSN type of ID.
3. Data should be stored in as few places as possible and duplicated only when necessary. Unless absolutely necessary, data should be stored on central administrative systems only.
4. Avoid storing data on departmental servers or creating "silo" databases that duplicate data on central administrative systems.
5. Never upload, post, or otherwise make available any kind of sensitive data on a web server even for short periods of time. Individuals responsible for maintaining web site content must be particularly cognizant and vigilant regarding this matter.
6. Inventory and identify the data under your control that is external to central administrative systems. Know where you have data and in what form (electronic, paper, etc.). Purge or delete data files in a timely manner to minimize risk.
7. Do not store sensitive data on or copy it to mobile, external, and/or removable storage devices. This may include smartphones, tablets, or any other device that could easily be lost, stolen or compromised.
8. Do not store sensitive data on or copy it to local workstations or network drives unless such data is not available on centralized systems. If you must store data on workstations or network drives, it is your responsibility to secure your workstation and/or ensure that only authorized individuals have access.
9. Do not use shared network drives to share or exchange data unless you are certain that access to those shared drive resources is restricted to individuals authorized to handle such data. For example, do not put anything sensitive or confidential on the S: Drive under S:\UNIVERSITY-WIDE-SHARED. All employees can access this shared folder.

10. Know and understand your environment technically. Understand who has access to areas to which you send, receive, store, or transmit data. Attend any WKU Sensitive Data Protection course offerings.
11. Transmission of any sensitive data should be encrypted. Websites should use HTTPS (TLS 1.2 or greater) encryption if they collect data. Unencrypted protocols should be abandoned in favor of their encrypted counterparts (i.e. abandon Telnet in favor of SSH, or abandon FTP in favor of SFTP). When in doubt, contact the IT Helpdesk.
12. Release of WKU Data to 3rd Parties - Do not release WKU data of any kind to 3rd party, non-WKU entities for any reason, unless such entities have agreed in writing to restrict the use of such data to the specific and intended purposes authorized by the WKU department or unit enlisting the services of the 3rd party entity. Any WKU department or unit releasing data to a non-WKU 3rd party entity is responsible for how the data are used (misused). Release of highly sensitive and confidential data (beyond FERPA allowed "directory information") is prohibited.
13. Do not send, receive, or store any sensitive data using email under any circumstances. Email is not secure.
14. Under no circumstances should credit card numbers be collected and stored on standalone devices, digital media, or paper media. Processing credit card numbers should be done via secure methods that authorize or deny the transaction in real time but do not retain or store the credit card number. Collecting credit card numbers via phone calls, websites, or email and retaining such numbers on paper or in electronic files for periodic processing is bad practice and insecure. If you need help processing credit cards securely, contact the IT Helpdesk. All merchants accepting credit card payments on the WKU campus must comply with WKU policy 3.3101, Policy & Procedures for Credit Card Merchants, and to current Payment Card Industry Data Security Standards (PCI DSS).
15. Report any breaches, compromises, or unauthorized/unexplained access of sensitive data immediately to the Office of IT Security and Identity Management via the “Report an Incident” link at www.wku.edu/it/security, by calling the IT Helpdesk at (270) 745-7000, or by submitting an online request at www.wku.edu/it/contact.

Privacy Statement

1. 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.
2. 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.
3. The University does not intend to sell, 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.

4. 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.
5. 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, and personnel or student records.
6. Some data items are considered directory information and will be released to the public unless a request is filed to prevent disclosure of the information, except for any other reason than 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.
7. The University strongly discourages the use or storage (electronic/paper) of SSNs in the course of daily academic or administrative business. All WKU employees and students are assigned a 9 digit WKUID that is the key to all personal, academic, and administrative information. This WKUID is more secure than the SSN as it has no meaning outside the University and unlikely to aid in identity theft.
8. WKU 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.
9. Personal information may only be released or provided to others as follows:
    - To employees and/or officers of the University on an authorized need-to-know basis;
    - only to those individuals who are authorized to use such information as part of their official University duties; and
    - with the following requirements:
        a) 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
        b) they do not further disclose or provide that information to others.
10. 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 unless special circumstances exist in which such notification interferes with the purpose of the request.
11. Student information may be released for health and emergency reasons.
12. 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.

13. 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's 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 that inaccurate or misleading information in the student's record be amended. 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
   400 Maryland Avenue, S.W.
   Washington, DC 20202-5920

Questions pertaining to the Family Educational Rights and Privacy Act may be directed to the University Registrar, 216 Potter Hall, (270) 745-3351.

Incident Reporting

WKU employees must immediately report the following to their managers, unless a conflict exists, and the Office of IT Security and Identity Management:

- Any 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; and
- unauthorized disclosure or modification of electronic institutional or personal information.

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

Incident Response

The Office of IT Security and Identity Management 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.

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

1. The Office of IT Security and Identity Management;
2. the affected system's owner (administrative responsibility for the system);
3. the System Administrator (technical support responsibility for the system); and
4. other individuals as required by the circumstances.
    a. This group will comprise the Incident Response Team for a specific incident. After initial notification, they will provide information updates as appropriate throughout the incident response process.
    b. 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.
    c. Create a log of all actions taken and maintain this log consistently throughout the response process.
    d. 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.
    e. 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.
    f. 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.
    g. 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.
    h. 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. Attempt to 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.
    i. Correct any identifiable system or application vulnerabilities that allowed the intrusion to occur.
    j. Verify system and data integrity.
    k. Restore service once the integrity of the system and/or information has been verified.
    l. 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; and
- identity of those responsible for the incident (if available).

The VP for Information Technology 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.

WKU will act in accordance with the Kentucky data breach notification law, KRS 365.732.

University Individual Department Procedures

ID Center

The student information stored at the ID Center is kept in two locations on one computer, the image directory and the VSC database. Both of these areas are password protected to prevent unauthorized entry. All paper-based information presented by students for the purpose of issuing an ID is shredded on a daily basis. All paper-based information presented by faculty/staff is filed in the appropriate location.

Department of Student Financial Assistance

Confidential information is any information pertaining to the students' financial aid eligibility. This includes information submitted on the FAFSA, IRS tax forms, and other financial documents as well as any information pertaining to the students' financial aid award, grades, and any professional judgment documents that are collected.

Only authorized school officials have access to financial aid information. The information is located on the Banner Student Financial Aid system. The Director of Financial Aid authorizes access to individuals on an as-needed basis. Said individuals must log on with credentials assigned to them for their sole use. Hard copy information is filed by social security number and is kept in filing cabinets in the back of the office. The office is locked during non-office hours.

The Department of Education requires that safeguard procedures are in place in order for the institution to be eligible for Federal Financial Aid. For additional information, call the Student Financial Assistance office at (270) 745-2755.

Office of the Bursar

The Office of the Bursar maintains financial records for the Cashiers, Billings and Receivables, and Perkins Loan functions of the University. These records include both electronic and paper records. The

Bursar's Office is in a secure, locked environment with video surveillance and an intrusion detection system. Electronic records are maintained via Banner, the University's information system. Prior to receiving access to the Banner System, each employee is required to sign an agreement to comply with federal law and University policy regarding the protection of and correct use of information related to students and records privacy.

Paper records are maintained in filing cabinets. Perkins loan records are maintained in locked filing cabinets within the secure area of the Bursar's Office. The Perkins Loan Office maintains compliance with federal regulations including the use of fireproof filing cabinets for required records.

The University receives credit card information for payment of tuition and fees and uses a lockbox company for credit card processing. The hard copy information is maintained in a filing cabinet and then shredded after a specified period of retention. When a student pays with a credit card via our secured website, the credit card number is masked on their student account.

The University uses service providers for collection agency and student loan service. We oversee service providers by taking steps to select and retain providers that are capable of maintaining appropriate safeguards for customer information. Additional safeguards in place include:

- The Office of the Bursar checks references prior to hiring employees who will have access to customer information;
- records are disposed after the designated period of retention either via shredding or burning; and
- computers are password protected.

For additional information, call the Office of the Bursar at (270) 745-6381.

Office of Admissions

The Office of Admissions obtains and collects a variety of different information for prospective University students through a variety of stages and in different formats. The types of data that are collected include, but are not limited to:

1. Prospect Stage:
    - Purchased information of high school graduates; and
    - solicited information from community colleges of transfer students.
2. Inquiry Stage:
    - General inquiries from prospective students.
3. Applicant Stage:
    - Applications from prospective students;
    - advanced placement examination information;
    - standardized test results for prospective students;
    - immigration documentation of prospective international students; and
    - high school and college transcripts of prospective students.

4. Admission Stage:
    - Applications from re-admit students.

All student records that are stored within the Office of Admissions are covered under the Family Educational Rights and Privacy Act of 1974 (FERPA) and those guidelines establish release of student information. In addition to FERPA regulations, the Office of Admissions has the following policies and procedures in practice to protect information:

1. Electronic data - All data are received on media or received electronically (downloaded) using industry standard privacy software. Enterprise Systems (ES) and Enterprise Applications and Programming (EAP) staff members are responsible for transferring data to the Banner student information system. Media are returned to the Office of Admissions from ES or EAP staff members after their data is loaded into Banner. Banner student information system security is maintained by Enterprise Systems. All electronic data that is received on media that is subject to a disposal requirement is destroyed within the office prior to disposal making the media unreadable; no such media is to be recycled for re-use.
2. Hard copy - Records are maintained within the office until the student is enrolled at Western Kentucky University, at which time the records are moved to the Registrar's Office. Records of students who do not matriculate are held for three years or until they do matriculate. If the student does not matriculate, the records are destroyed after three years. All hard copy documentation that is considered for disposal is shredded using a third party shredder company. All information that is to be disposed of that contains student information is shredded within the office. All bulk record shredding is reported to University Archives. An estimate of the amount of records to be shredded and the general type of records are reported to University Archives.

All personnel are required to read and abide by office procedures on student record information including FERPA regulations. Training agendas include a component on information security.

For additional information call the Office of Admissions at (270) 745-2551

Department of Housing and Residence Life

The following information about students is maintained in the Department of Housing and Residence Life:

- Records related to disciplinary actions originating in the residence halls;
- records related to room assignment, room registration, room occupancy, and applications to live on campus; and
- records related to financial obligations, billing, and payment information for damages to residence hall rooms and facilities.

Records are maintained in both electronic format and hard copy. Specific storage and security measures are in place as follows:

- Records related to disciplinary matters are maintained in hard copy form. Records stored in the main office area are kept in locked file cabinets. Records more than two years old are stored in a locked storage area adjacent to the main office area.
- An electronic file is created summarizing pertinent information related to disciplinary matters. This database is maintained on a secure server accessible via TopNet. Only those individuals with authorized access to the Student Conduct System may access the database through TopNet login procedures.
- Records related to the assignment process are maintained on Banner and in hard copy. The hard copies are held for five years and are stored in a locked storage area adjacent to the main office area.

The Association for Student Judicial Affairs contains the following language pursuant to confidentiality in the Statement of Ethical Principles and Standards of Conduct:

- Confidentiality - Members ensure that confidentiality is maintained with respect to all privileged communications and to educational and professional records considered confidential. They inform all parties of the nature and/or limits of confidentiality. Members share information only in accordance with institutional policies and relevant statutes, when given informed consent, or when required to prevent personal harm to themselves or others.

The Association for College and University Housing Officers - International contains the following language in the Ethical Principles and Standards for College and University Student Housing related to Technology:

- Technology resources used in administration and operations are regularly evaluated for determining whether current and projected needs and opportunities are met.
- Staff have access to adequate technology resources in the performance of their job responsibilities.
- Technology resources are used to create and sustain cost reduction and efficiency improvement measures initiated by professional staff.
- Technology resources are properly maintained and serviced.

ACUHO-I recommends the use of the procedures developed and published by the National Association of College and University Business Officers (NACUBO), the Canadian Association of University Business Officers (CAUBO), or other similar national professional associations with regard to financial reporting and accounting.

Staff members shall treat confidential information appropriately.

The Council for Advancement of Standards contains the following language pursuant to records and privacy:

- Judicial program staff members must maintain the highest principles of ethical behavior in the use of technology.

- Information disclosed in individual counseling sessions must remain confidential, unless written permission to divulge the information is given by the student. However, all staff members must disclose to appropriate authorities information judged to be of an emergency nature, especially when the safety of the individual or others is involved. Information contained in students' educational records must not be disclosed to extra-institutional third parties without appropriate consent, unless classified as “Directory” information or when the information is subpoenaed by law. Judicial programs must apply a similar dedication to privacy and confidentiality to research data concerning individuals.
- Judicial program staff members must ensure that confidentiality is maintained with respect to all communications and records considered confidential unless exempted by law.
- Housing staff members must ensure that confidentiality is maintained with respect to all communications and records considered confidential unless exempted by law. Information disclosed in individual counseling sessions must remain confidential, unless written permission to divulge the information is given by the student. However, all staff members must disclose to appropriate authorities information judged to be of an emergency nature, especially when the safety of the individual or others is involved. Information contained in students' educational records must not be disclosed to non-institutional third parties without appropriate consent, unless classified as "Directory" information or when the information is subpoenaed by law. Programs and services must apply a similar dedication to privacy and confidentiality to research data concerning individuals. All staff members must be aware of and comply with the provisions contained in the institution's human subjects research policy and in other relevant institutional policies addressing ethical practices.

The American College Personnel Association contains the following language regarding confidentiality in the Statement of Ethical Principles and Standards:

- Inform students of the nature and/or limits of confidentiality. They will share information about the students only in accordance with institutional policies and applicable laws, when given their permission, or when required to prevent personal harm to themselves or others.
- Use records and electronically stored information only to accomplish legitimate, institutional purposes and to benefit students.

The National Association of Student Personnel Administrators contains the following language regarding confidentiality in the association’s Standards of Professional Practice:

- Members ensure that confidentiality is maintained with respect to all privileged communications and to educational and professional records considered confidential. They inform all parties of the nature and/or limits of confidentiality. Members share information only in accordance with institutional policies and relevant statutes when given the informed consent or when required to prevent personal harm to themselves or others.

For additional information, call the Department of Housing and Residence Life at (270) 745-4359.

Office of the Registrar

The Office of the Registrar maintains a variety of student academic records that are in both electronic and paper format. Employees in this office are trained to protect the privacy of students' records and are well versed in the Family Educational Rights and Privacy Act (FERPA), the federal law that protects the privacy of educational records and defines proper release of that information.

Electronic records are maintained in the Banner student information system, and changes to those records are made only by authorized personnel. Access to the Banner system is via a password, and each employee must be trained in the proper use of the system before access to the system is granted.

The Office of the Registrar also maintains a variety of confidential paper records. Student transcripts date back to 1906, the founding date of the institution, and are stored in filing cabinets in secure vaults. Permanent student record folders are also stored in filing cabinets and are under the daily supervision of two employees. These folders are destroyed following students' five-year absence from the University. Work papers and other documents containing private information are shredded following their use. The office is locked during non-business hours.

For additional information, call the Office of the Registrar at (270) 745-3351.

Violations

Any violation of the rules, regulations, policies, and procedures in this Information Security Plan 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 students. Confirmed or suspected violations of local, state or federal laws will be turned over to the University General Counsel and/or the appropriate law enforcement agency.

Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment. The most frequent of these reviews will occur within the IT Division where constantly changing technology and evolving risks mandate increased vigilance. Continued administration of the development, implementation, and maintenance of the plan will be the responsibility of the designated Information Security Plan Coordinators who will assign specific responsibility for implementation and administration as appropriate. The Coordinators, in consultation with the Office of General Counsel, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security. The VP for Information Technology will be responsible for maintaining the most current version of this policy and keeping it updated both in print and online.

Revision History

- May 23, 2003: created and approved.
- August 3, 2006: revised.
- June 20, 2007: revised per recommendations of the Office of Internal Audit.
- September 15, 2013: revised per IT Policy Update initiative.
- November 3, 2014: revised "Authorized by:" entry changed to reflect current IT Division executive management – Chief Information Technology Officer.
- September 14, 2015: revised per recommendations of the Office of Internal Audit.
- April 12, 2016: revised to add information about the KY breach notification law, KRS 365.732.
- July 1, 2016: revised to make minor changes as part of an annual review process.
- April 17, 2017: revised to add annual training requirement for employees handling sensitive data. Added section for review date.

This document was last reviewed on June 28, 2018.