Reviewed: 2022/06/06
Updated: 2022/06/06

EKU
Information Technology
Information Security Plan

Contents

This page is intentionally left blank.

Information Security Plan

This Information Security Plan describes Eastern 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.

Scope

This plan applies to the entire Eastern Kentucky University (EKU) community, including the President, Vice Presidents, Provost, Deans, Directors, and Department Heads, students, faculty, staff, alumni, trustees, temporary employees, contractors, volunteers, and guests who have access to EKU information technology services. Such assets include data, images, text, or software, used on hardware, paper, or other storage media.

Definitions

Confidentiality- "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" A loss of confidentiality is the unauthorized disclosure of information.

Integrity- "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" A loss of integrity is the unauthorized modification or destruction of information.

Availability- “Ensuring timely and reliable access to and use of information…” A loss of availability is the disruption of access to or use of information or an information system.

Risk Assessment is a process which determines what information technology resources exist that require protection, and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability.

Control Activities are the policies, procedures, techniques, and mechanisms that help ensure that management's response to reduce risks identified during the risk assessment process is carried out.

Access Control refers to the process of controlling access to systems, networks, and information based on business and security requirements.

ISO (International Organization for Standardization) - An international-standard-setting body composed of representatives from various national standards organizations.

NIST (National Institute of Standards and Technology) - A non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

VPN (Virtual Private Network) - A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to the University’s network. VPN’s use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

IDS (Intrusion Detection System) - A device (or application) that monitors network and/or system activities for malicious activities or policy violations.

IPS (Intrusion Prevention System) - A device (or application) that identifies malicious activity, logs information about said activity, attempts to block/stop activity, and reports activity.

Encryption- Process of converting information so that it is humanly unreadable except by someone who knows how to decrypt it.

Confidential Data - A generalized term that typically represents data classified as Restricted. This term is often used interchangeably with sensitive data.

Sensitive Data - A generalized term that typically represents data classified as Restricted. This term is often used interchangeably with confidential data.

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 threats are created regularly. Accordingly, IT staff will monitor industry sources and advisory groups for the identification of new risks.

The University believes current safeguards are reasonable and, in light of ongoing risk assessments, are in line with standard 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 definite security of covered data, information, and resources given the evolving and ever-changing state of IT environments and threats to it.

Information Security Plan Coordinators

The CIO and the Director of Information Security and Application Systems 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 or conducting audits of this plan periodically.

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 allowed to possess keys or combinations to them. Paper documents that contain covered data and information are to be shredded at the time of disposal per the University Records Management policy.

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 the application of appropriate patches and updates in a timely fashion. Authentication is also required of users before they can access University-protected data. Also, security systems have been implemented to assist with the 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 a real or attempted unauthorized access to covered data, information, and resources. Incident 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 required to provide services the University determines it will not offer 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 acknowledgment 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 sensitive 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 available for use by EKU students, faculty, and staff. Departmental and IT computer labs require login authentication, and 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 when access has been requested by an authorized faculty or staff member and approved by the Director of Information Security and Application Systems or Chief Information Officer. 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 EKU 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. Lab machines are prohibited from engaging in port scanning, traffic spamming/flooding, and other similar activities that negatively impact the University network 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 EKU IT Division.

Anti-Virus

1. All EKU PC-based computers must have EKU'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 or distribute malicious programs into EKU'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 appropriately 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. EKU 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 plan.
5. Expansion or manipulation of network hardware or software, except by designated individuals within the IT Division, without prior approval from the IT Division, is strictly prohibited.
6. Before connecting any server to the University network, approval must be obtained via a support ticket from the EKU IT Division.
7. The following devices should not be attached to the campus network and are strictly prohibited, other than those provided or approved by the IT Division:
    - 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. 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.
10. 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 new 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 IPv4, IPv6, and DHCP.
- 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 before the 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 before the 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 EKU'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 EKU.edu are made available upon request at no charge for University approved services.
- DNS names for domains other than EKU.edu and which are to be hosted on University systems must be requested from the IT Division. Any charges for the 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 EKU.edu domain, will not be approved for use without justification. For any other domain name to be approved for EKU purposes, it must be demonstrated that equivalent functionality cannot be provided under the existing EKU.edu domain.

Default Accounts

- The passwords for default accounts must be changed before deploying a device or system on the network.
- Default accounts should be disabled if the account is unnecessary.

Security Assessment

1. Network and system security will be assessed periodically.
2. Security testing and audits will be conducted periodically.
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 policies.
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. Unauthorized access to areas where personally identifiable information (PII) is stored is prohibited.
3. Supervisors must ensure that staff who (voluntarily) terminate their employment with the department return their physical access keys and fobs on their last day of work in that unit.
4. 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.
5. If an employee does not return his/her keys, areas controlled by the outstanding keys must be rekeyed.

6. University information or records may not be removed (or copied) from the office where it is kept except in the performance of job responsibilities.
7. Access to EKU IT Infrastructure operations areas shall be restricted to those responsible for operation and maintenance.
8. Access to EKU's Information Technology data center by non-IT personnel is not permitted unless an authorized IT staff member escorts them.
9. 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 allow the physical keys to be a shared resource but under auditable conditions.
10. Computer installations should provide reasonable security measures to protect the computer system against natural disasters, accidents, loss or fluctuation of electrical power, and sabotage.
11. 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 EKU must be approved by IT. Server maintenance plans must be established and maintained by each operational group and approved by the IT Division.
4. All new servers physically located on campus, including extended campuses, must have a default deny rule for inbound and outbound traffic. IT Security must approve any exceptions.
5. 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;
    - data types that are housed on the server;
    - main functions and applications, if applicable; and
    - MAC address
6. IT Systems personnel should be kept up-to-date with any changes to server information pertaining to number 5 above.
7. Operating system configuration should be in accordance with approved security best practices.
8. Services, protocols, daemons, and applications that will not be used must be disabled where possible.
9. Each server should be implemented with only one primary function to prevent functions that require different security levels from co-existing on the same server.

10. Access to services should be logged or protected through access-control methods if possible.
11. The most recent patches must be installed on the system as soon as practical.
12. Do not use accounts with elevated privileges (such as administrator or root) access when a non- privileged account can be used.
13. Privileged access must be performed via an encrypted network protocol (such as SSH, HTTPS, RDP) and/or over an encrypted VPN tunnel).
14. All security-related events on critical or sensitive systems must be logged and audit trails saved for a minimum of 30 days.
15. Security-related events will be reported to IT Security, 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.
16. Audits may be performed on any device utilizing EKU Network resources at the discretion of the CIO and IT Security.

Passwords

1. Passwords are designed to prevent unauthorized access to information. Users are responsible for safeguarding passwords along with other authentication mechanisms (such as usernames, PINs, etc.) and are accountable for negligent disclosure of passwords.
2. Passwords should be a minimum of 10 characters long and meet the complexity requirements.
3. Password changes are required every 90 days or immediately if compromised. Systems should automatically expire passwords at regular intervals and require the user to reset the password by 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 "autocomplete" types of features available in browsers and other software. These password "memorization" functions should be disabled and never utilized. IT may approve password managers on a case-by-case basis.
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 EKU accounts as for other non-EKU access (e.g., personal ISP account, option trading, benefits, etc.).
9. EKU 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 EKU network resources via open, unsecured wireless communication mechanisms except for the following:
    - "EKU_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.
    - "EKU_BYOD" wireless network provided by the University IT Divisions for devices that are unable to connect to EKU's secure wireless network. This network will have restricted access to non-confidential resources.
2. Wireless access points not sanctioned by the EKU IT Division are prohibited.

Destruction and Disposal of Information and Devices

1. Confidential information must be disposed of in such a manner as to ensure it cannot be retrieved and recovered by unauthorized persons. Physical documents must be shredded.
2. When donating, selling, transferring, surplus, 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 destroyed thoroughly. In general, it is insufficient to "delete" the information, as it may remain on the medium. The data should be adequately removed from the drive in a manner that meets the U.S.

Department of Defense specifications, or the drive may be physically destroyed.

Employee Training and Management

1. Employees who have access to University Banner information must sign an agreement to follow EKU'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 complete an interactive online training program regarding the handling of sensitive data and applicable laws or policies once every 3 years. Notice of this requirement will be communicated directly with these employees or their supervisor(s). Failure to complete the 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 the appropriate department or law enforcement agencies; and
    - reviewing all IT Policies.

Sensitive Data Protection

Special care and awareness are required concerning "sensitive data." Sensitive data are any data that the unwarranted or unauthorized disclosure of such would harm 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 or store SSNs unless a federal or state agency requires it 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 it.security@eku.edu explaining why the SSNs must be utilized and how and where they are being collected/stored.
2. Use the EKUID assigned to all individuals as the unique identifier for all EKU entities. If EKUID is not available or does not exist for specific 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 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. Individuals responsible for maintaining web site content must be particularly aware 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 promptly to minimize risk.
7. Do not store sensitive data on or copy it to mobile, external, 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 or ensure that only authorized individuals have access.
9. Do not use shared network drives to share or exchange data unless you are confident that access to those shared drive resources is restricted to individuals authorized to handle such data.
10. Know and understand your environment technically. Understand who has access to areas to which you send, receive, store, or transmit data. Participate in EKU 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 EKU Data to 3rd Parties - Do not release EKU data of any kind to 3rd party, non-EKU 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 EKU department or unit enlisting the services of the 3rd party entity. Any EKU department or unit releasing data to a non-EKU 3rd party entity is responsible for how the data are used (misused). The 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. Exceptions to be made for encrypted email when email is the only viable choice, never for credit card numbers.
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 keeping such numbers on paper or in electronic files for periodic processing is bad practice and insecure. Unprotected primary account numbers must not be sent via any end user-messaging technologies. If you need help processing credit cards securely, contact the IT service desk.
15. Report any breaches, compromises, or unauthorized/unexplained access of sensitive data immediately to IT Security.

Privacy Statement

1. Eastern 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 the 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' names, mailing addresses, telephone numbers, email addresses, 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 (PII) 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.
7. The University strongly discourages the use or storage (electronic/paper) of SSNs in the course of daily academic or administrative business. All EKU employees and students are assigned a 9 digit EKUID that is the key to all personal, academic, and administrative information. This EKUID is more secure than the SSN as it has no meaning outside the University and unlikely to aid in identity theft.
8. EKU assumes that failure on the part of any student or employee to request the withholding of categories of information indicates explicitly individual approval for disclosure.
9. Personal information may only be released or provided to others as follows:
    - To employees 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.

Incident Reporting

EKU employees must immediately report the following to their managers, unless a conflict exists, and IT Security:

- Any actual or suspected security incident that involves unauthorized access to electronic systems owned or operated by EKU;
- 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

IT Security is the primary point of contact for responding to and investigating incidents related to misuse or abuse of Eastern 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. IT Security;
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 the 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 actions 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.
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 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 the incident;
    - a detailed list of the system(s) and data which were

compromised;
- corrective actions are taken to prevent future occurrences;
- identity of those responsible for the incident (if available).

The CIO 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.

EKU will act per the Kentucky data breach notification law, KRS 365.732.