Data Classification and Security Policy **Issued August 1, 2013**

Purpose

Data and information are important assets of the college and must be protected from loss of integrity, confidentiality, or availability in compliance with college policy and guidelines, SAMC policy, and state and federal laws and regulations.

Scope

This policy applies to all college, departments, administrative units, and affiliated organizations. For the purposes of this policy, affiliated organization refers to any organization associated with the College that uses college information technology resources to create, access, store, or manage College Data to perform their business functions. It also applies to any third party vendor creating, storing, or maintaining College Data per a contractual agreement.

Effective Date

This policy became effective on August 2, 2013

All new systems designed and implemented after March 1, 2012, must comply with the security standards in section. Data stewards must have a compliance plan for all systems with confidential data by August 1, 2013.

Authority

SAMC\ACOM - Data Administration Program requires institutions, to "develop, implement, and maintain an Agency Data Administration Program" that incorporates data polices with appropriate security controls.

Policy

All College Data must be classified according to the ACOM Data Classification Schema and protected according to ACOM Data Security Standards. This policy applies to data in all formats or media.

Data Classification Schema

Data and information assets are classified according to the risks associated with data being stored or processed. Data with the highest risk need the greatest level of protection to prevent compromise; data with lower risk require proportionately less protection. Three levels of data classification will be used to classify College Data based on how the data are used, its sensitivity to unauthorized disclosure, and requirements imposed by external agencies.

Data are typically stored in aggregate form in databases, tables, or files. In most data collections, highly sensitive data elements are not segregated from less sensitive data elements. For example, a student information system will contain a student's directory information as well as their social security number. Consequently, the classification of the most sensitive element in a data collection will determine the data classification of the entire collection.

ACOM Data Classifications:

1. Public - Data explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to the College, affiliates, or individuals. Public data generally have a very low sensitivity since by definition there is no such thing as unauthorized disclosure, but it still warrants protection since the integrity of the data can be important. Examples include:

    - ACOM's public web site
    - Directory information for students, faculty, and staff except for those who have requested non-disclosure (for example, per FERPA (Family Educational Rights and Privacy Act - see for students)
    - Course descriptions
    - Semester course schedules
    - Semester course schedules
    - Press releases

2. Internal - Data intended for internal College business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. Internal data are generally not made available to parties outside the ACOM community. Unauthorized disclosure could adversely impact the Colleges, affiliates, or individuals. Internal data generally have a low to moderate sensitivity. Examples include:

    - Financial accounting data that does not contain confidential information
    - Departmental intranet
    - Information technology transaction logs
    - Employee ID number
    - Student educational records
    - Directory information for students, faculty, and staff who have requested non-disclosure (for example, per FERPA for students)

3. Confidential - Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization by the Data Steward is required for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on the business or research functions of the University or affiliates, the personal privacy of individuals, or on compliance with federal or state laws and regulations or University contracts. Confidential data have a very high level of sensitivity. Examples include:
    - Social Security Number

- Student ID number (if it is the same as the Social Security Number)
- Credit card number
- Personal identity information (PII). An individual's name (first name and last name, or first initial and last name) in combination with one or more of the following: a) Social security number, b) driver's license number or state identification card number, or c) financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account. For ACOM's purposes, PII also includes ones name in combination with a passport number.
- Passport number
- Personnel records
- Medical records
- Authentication tokens (e.g., personal digital certificates, passwords, biometric data)

4. Proprietary Data - Classification of data provided to or created and maintained by ACOM on behalf of a third party, such as a corporation or government agency, will vary depending on contractual agreements and/or relevant laws or regulations. The classification and security standards for proprietary data owned by the third party will be defined by the third party. Proprietary data owned by ACOM must be classified and protected according to ACOM's data classification policy and security standards. Individuals managing or accessing proprietary data are responsible for complying with any additional requirements and security policies and procedures specified by the third party owner. Proprietary data include data classified by the federal government as Classified National Security Information (confidential, secret, top secret).

Data Security Standards

The following table defines required safeguards for protecting data and data collections based on their classification. Data security requirements for Proprietary Data are determined by the contracting agency and are therefore not included in the table below.

In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

Security Control Category	*Data Classification*		
	Public	***Internal***	***Confidential***
Access Controls	• No restriction for viewing • Authorization by Data Steward or designee required for modification; supervisor approval also required if not a self-service function	• Viewing and modification restricted to authorized individuals as needed for business-related roles • Data Steward or designee grants permission for access, plus approval from supervisor • Authentication and authorization required for access	• Viewing and modification restricted to authorized individuals as needed for business-related roles • Data Steward or designee grants permission for access, plus approval from supervisor • Authentication and authorization required for access • Confidentiality agreement required
Copying/Printing (applies to both paper and electronic forms)	• No restrictions	• Data should only be printed when there is a legitimate need • Copies must be limited to individuals with a need to know • Data should not be left unattended on a printer	• Data should only be printed when there is a legitimate need • Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement • Data should not be left unattended on a printer • Copies must be labeled "Confidential"
Network Security	• May reside on a public network • Protection with a firewall recommended • IDS/IPS protection recommended • Protection only with router ACLs acceptable	• Protection with a network firewall required • IDS/IPS protection required • Protection with router ACLs optional • Servers hosting the data should not be visible to entire Internet • May be in a shared network server subnet with a common firewall ruleset for the set of servers	• Protection with a network firewall using "default deny" ruleset required • IDS/IPS protection required • Protection with router ACLs optional • Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets like the residence halls and guest wireless networks • Must have a firewall ruleset dedicated to the system

System Security	• Must follow general best practices for system management and security • Host-based software firewall recommended	• Must follow University-specific and OS-specific best practices for system management and security • Host-based software firewall required • Host-based software IDS/IPS recommended	• Must follow University-specific and OS-specific best practices for system management and security • Host-based software firewall required • Host-based software IDS/IPS recommended
Virtual Environments	• May be hosted in a virtual server environment • All other security controls apply to both the host and the guest virtual machines	• May be hosted in a virtual server environment • All other security controls apply to both the host and the guest virtual machines • Should not share the same virtual host environment with guest virtual servers of other security classifications	• May be hosted in a virtual server environment • All other security controls apply to both the host and the guest virtual machines • Cannot share the same virtual host environment with guest virtual servers of other security classifications
Physical Security	• System must be locked or logged out when unattended • Host-based software firewall recommended	• System must be locked or logged out when unattended • Hosted in a secure location required; a Secure Data Center is recommended	• System must be locked or logged out when unattended • Hosted in a Secure Data Center required • Physical access must be monitored, logged, and limited to authorized individuals 24x7
Remote Access to systems hosting the data	• No restrictions	• Access restricted to local network or general K-State Virtual Private Network (VPN) service • Remote access by third party for technical support limited to authenticated, temporary access via direct dial-in modem or secure protocols over the Internet	• Restricted to local network or secure VPN group • Unsupervised remote access by third party for technical support not allowed • Two-factor authentication recommended

Data Storage	• Storage on a secure server recommended • Storage in a secure Data Center recommended	• Storage on a secure server recommended • Storage in a secure Data Center recommended • Should not store on an individual's workstation or a mobile device	• Storage on a secure server required • Storage in Secure Data Center required • Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption • Encryption on backup media required • AES Encryption required with 192-bit or longer key • Paper/hard copy: do not leave unattended where others may see it; store in a secure location
Transmission	• No restrictions	• No requirements	• Encryption required (for example, via SSL or secure file transfer protocols) • Cannot transmit via e-mail unless encrypted and secured with a digital signature
Backup/Disaster Recovery	• Backups required; daily backups recommended	• Daily backups required • Off-site storage recommended	• Daily backups required • Off-site storage in a secure location required

Training	• General security awareness training recommended • System administration training recommended	• General security awareness training required • System administration training required • Data security training required	• General security awareness training required • System administration training required • System administrators hired after Sept. 1, 2008, must pass a criminal background check • Data security training required • Applicable policy and regulation training required
Audit Schedule	• As needed	• As needed	• Annual

Note: the table above is adapted from the University of Missouri-Columbia Information & Access Technology Services data classification system:http://iatservices.missouri.edu/security/data-classification/

Contracts with Third Parties

Contracts between the College and third parties involving College Data must include language requiring compliance with all applicable laws, regulations, and College policies related to data and information security; immediate notification of the College if College Data is used or disclosed in any manner other than allowed by the contract; and, to the extent practicable, mitigate any harmful effect of such use or disclosure.

Definitions

1. ACL - Access Control List; a set of rules in a network device, such as a router, that controls access to segments of the network. A router with ACLs can filter inbound and/or outbound network traffic similar to a firewall but with less functionality.

2. Authentication - Process of verifying one's digital identity. For example, when someone logs into Webmail, the password verifies that the person logging in is the owner of the User ID. The verification process is called authentication.

3. Authorization - Granting access to resources only to those authorized to use them.

4. Availability - Ensures timely and reliable access to and use of information.
5. Classified National Security Information - Information that has been determined by the federal government to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. There are three classifications - confidential, secret, and top secret (see http://www.fas.org/irp/offdocs/eo12958.htm).
6. Confidentiality - Preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
7. Firewall - A specialized hardware and/or software system with stateful packet inspection that filters network traffic to control access to a resource, such as a database server, and thereby provide protection and enforce security policies. A router with ACLs is not considered a firewall for the purposes of this document.
8. IDS - Intrusion Detection System; a system that monitors network traffic to detect potential security intrusions. Normally, the suspected intrusions are logged and an alert generated to notify security or system administration personnel.
9. Integrity - Guards against improper modification or destruction of information, and ensures non-repudiation and authenticity.
10. IPS - Intrusion Prevention System; an IDS with the added ability to block malicious network traffic to prevent or stop a security event.
11. Local Network - Any segment of K-State's data network physically located on the Manhattan or Salina campus with an IP address starting with 129.130.X.X or an un-routable private IP address (e.g., 10.X.X.X).
12. Remote Access - Accessing any K-State's local network from any physical location outside the Dothan, Alabama campus. This includes access from off campus using ACOM's VPN service.
13. Secure Data Center - A facility managed by full-time IT professionals for hosting computer, data storage, and/or network equipment with 24x7 auditable restricted access, environmental controls, power protection, and network firewall protection.
14. Secure Server - a computer that provides services to other computers, applications, or users; is running a server operating system; and is hardened according to relevant security standards, industry best practices, and ACOM security policies.
15. Sensitivity - Indicates the required level of protection from unauthorized disclosure, modification, fraud, waste, or abuse due to potential adverse impact on an individual, group, institution, or affiliate. Adverse impact could be financial, legal, or on one's reputation or competitive position. The more sensitive the data, the greater the need to protect it.
16. College Data - Any data related to Alabama College of Osteopathic Medicine ("College") functions that are a) stored on College information technology systems, b) maintained by ACOM faculty staff, or students, or c) related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).
17. VPN - Virtual Private Network; a VPN provides a secure communication channel over the Internet that requires authentication to set up the channel and encrypts all traffic flowing through the channel.

Roles and Responsibilities

Everyone with any level of access to College Data has responsibility for its security and is expected to observe requirements for privacy and confidentiality, comply with protection and control procedures, and accurately present the data in any type of reporting function. The following roles have specific responsibilities for protecting and managing College Data and Data Collections.

1. Chief Data Steward - Senior administrative officers of the college responsible for overseeing all information resources (e.g., the Dean and Vice Presidents).
2. Data Steward - Deans, associate vice presidents, and heads of academic, administrative, or affiliated units or their designees with responsibility for overseeing a collection (set) of College Data. They are in effect the owners of the data and therefore ultimately responsible for its proper handling and protection. Data Stewards are responsible for ensuring the proper classification of data and data collections under their control, granting data access permissions, appointing Data Managers for each College Data collection, making sure people in data-related roles are properly trained, and ensuring compliance with all relevant polices and security requirements for all data for which they have responsibility.
3. Data Stewards Council - A group of Data Stewards appointed by the Chief Data Stewards and Manager of Information Systems - ACOM to maintain the data classification schema, define College Data collections, assign a Data Steward to each, and resolve data classification or ownership disputes.
4. Data Manager - Individuals authorized by a Data Steward to provide operational management of a College Data collection. The Data Manager will maintain documentation pertaining to the data collection (including the list of those authorized to access the data and access audit trails where required), manage data access controls, and ensure security requirements are implemented and followed.
5. Data Processor - Individuals authorized by the Data Steward or designee and enabled by the Data Manager to enter, modify, or delete College Data. Data Processors are accountable for the completeness, accuracy, and timeliness of data assigned to them.
6. Data Viewer - Anyone in the college community with the capacity to access College Data but is not authorized to enter, modify, or delete it.
7. Manager, Information Systems - ACOM - Provides advice and guidance on information and information technology security policies and standards.
8. Internal Audit Office - Performs audits for compliance with data classification and security policy and standards.

Related Laws, Regulations, or Policies

1. Family Educational Rights and Privacy Act of 1974 (FERPA - /registrar/ferpa/index.html
2. Health Insurance Portability and Accountability Act of 1996 (HIPAA)http://www.hhs.gov/ocr/hipaa/
3. Gramm-Leach-Bliley Act (GLBA) http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

4. Electronic Communications Privacy Act of 1986 (ECPA) http://www.usiia.org/legis/ecpa.html
5. NIST Publication 800-88 "Guidelines for Media Sanitization" http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf
6. NIST Publication 800-53 "Recommended Security Controls for Federal Information Systems" http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
7. NIST Publication 800-60 "Guide for Mapping Types of Information and Information Systems to Security Categories"http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf
8. Executive Order 12958, Classified National Security Information, As Amended, March 2003 http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html
9. Payment Card Industry Data Security Standard (PCI DSS) https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Questions/Waivers

The Manager of Information Systems - ACOM is responsible for this policy and is responsible for maintaining the ACOM Data Security Standards.

Questions related to the policy or standards should be directed to the Manager, Information Systems - ACOM.

The Dean of the Alabama College of Osteopathic Medicine or designee must approve any exception to this policy. The Dean must approve any exceptions to the Data Security Standards.