FHSU INFORMATION SECURITY POLICY

1. Purpose. To set forth regulations and procedures to ensure confidentiality, integrity, and availability of the University's electronic information.

2. Definitions.

2.1 "Asset classification" means the process of assigning value to data in order to organize it according to its sensitivity to loss or disclosure.

2.2 "Community" means University Groups, Employees, Students, former Students who continue to have authorized access to University electronic information systems, emeriti, former Employees who continue to have authorized access to FHSU email systems, and authorized Non-University Groups.

2.3 "Data" means electronic information providing support to and meeting needs of the University community. Data includes, but is not limited to:

- Elements supporting financial management;
- Student records;
- Payroll;
- Personnel records;
- Capital equipment inventory; and,
- Any electronic information:
  - Used for planning, managing, reporting, or auditing a major administrative function;
  - Referenced or used by a Department(s) or College to conduct University business;
  - Included in a University administrative report; or,
  - Used to derive a data element meeting any of the criteria above.

2.4 "Data element" means a unit of data that has an identification such as a data element name, a clear definition, a data type such as date/amount/identifier/indicator, and if applicable, enumerated values.

2.5 "Data definition" means a human readable phrase or sentence associated with a data element within a data dictionary that describes the meaning of a data element.

2.6 "Access token" means a protected physical object that contains information about the identity and privileges associated with a user account.

2.7 IST – Information Security Team, a team in Computing and Telecommunications responsible for overseeing security policies, security monitoring, training, and enforcement. The current team: Mark Griffin (co-chair), Cheryl Helget (co-chair), David Schmidt, Derek Johnson (networking), Mike Nease (microcomputing), Viv Zimmerman (training), and Jeff Mayo (server administration).

3. Organizational Security.

3.1 Management Responsibility. The University's electronic information systems management shall provide or recommend resources needed to:

- Ensure confidentiality, integrity, and availability of the University's electronic information;
- Reduce the risk of exposure that would damage the reputation of the University;
- Protect University electronic information assets; and,
- Oversee risk management and compliance with applicable electronic information security-related federal and state laws, regulations, Payment Card Industry requirements, and other contractual requirements.

3.2 Core Security Values. The electronic information security regulations and procedures shall support the following security values:

- The protection of the University's resources, reputation, legal position, and ability to conduct its operations;
- The protection of information privacy;
- The application of cost-effective measures commensurate with the sensitivity and value of resources, and the actual threats to those resources;
- Use requirements consistent with the best practices at institutions of higher education;
- Explicitly stated responsibilities of individual members of the community including, but not limited to, the shared responsibility for protecting University resources;
- Accountability of each member of the Community for access to and use of University resources;
- Mandate regulations, procedures, and practices which are flexible enough to change as circumstances change, and only where necessary to provide adequate protection.
- Regulations and procedures designed to ensure appropriate measures are taken to prepare for possible incidents which threaten the continuity of business; and,
- Continuing reassessment of regulations and procedures.

3.3 Department(s) or College Cooperation. All Department(s) or Colleges providing information technology services shall:

- Work collaboratively to effect security solutions compatible with each other; and,
- Coordinate technical and regulation decisions with the University's security program and with the University's Information Security Team (IST).

3.4 Authorization of Information Processing Facilities. Establishment of electronic information processing facilities, whether comprised of single or multiple servers or services, shall:

- Be reviewed by a member of the Information Security Team (IST) for compliance to electronic information security regulations and procedures; and,
- Not be connected to the network until compliance with security regulations and procedures are met and approved by an IST member.

3.5 Arrangements with Non-University Groups. Any proposed arrangements with a Non-University Group involving electronic data and information shall be submitted to the IST for:

- Reviewing security related issues; and,
- Recommending changes if required.

3.5.1 For protection of the electronic systems and information, arrangements shall require the Non-University Group to agree to comply with:

- All applicable federal and state laws and regulations;
- All University electronic information security regulations; and,
- Industry standards involving, but not limited to, confidentiality, integrity, and availability.

3.5.2 Approved outsourcing arrangements shall be monitored by the IST and other appropriate University administrators.

3.6 Risk Analysis and Assessment. An information risk analysis and assessment is to be performed at the direction of the IST. The results of the risk analysis and assessment will become the basis of Information Security Programs or Initiatives.

4. **Asset Management.** This section provides for the management of and access to University data with the intent being to increase its value and security.

4.1 Data Ownership. Fort Hays State University and the FHSU Foundation are the only known owners of data described in 2.3 above. If other entities own data on the FHSU network, they must notify the IST to ensure proper security measures are taken.

4.2 Management Structure. Each community member is responsible for managing data per University regulations when data is under the control of said member of the community.

4.3.1 Each Vice President, and Presidential designee shall be responsible for:

- All data maintained by the Department(s) or College (s) reporting to them;
- Ensuring data resources are used in ways consistent with the mission of the University;
- Enforcing regulations and procedures concerning the accuracy, privacy and integrity of the data subsets for which they are responsible;
- Interpreting and implementing federal and state laws and regulations relevant to their administrative areas (FERPA, for example), and University regulations;
- Ensuring data quality and data definition standards are met (best efforts at obtaining correct Chinese names, for example);
- Approve broad classification levels for data (see section 4.4 below);
- Approve authorization procedures to facilitate appropriate data access as defined by campus data regulations and ensuring security for that data;
- Assist in resolving issues related to stewardship of data elements crossing multiple Department(s) or Colleges;
- In the case of disagreement, assist in developing standard definitions for data elements, including those that cross multiple units or divisions. For example, there shall either be a single definition of “full-time equivalent employee” or new data elements shall be created for each unique definition; and,
- Working with Institutional Research or the CTC to identify any College or Division-specific data maintained for their Department(s) or College(s).

4.3.2 The Director of the Computing and Telecommunications Center (Director of CTC) shall additionally be responsible for ensuring an adequate and appropriate technical infrastructure is in place to support University data needs.

4.3.3 Each Dean or Director overseeing data for a subject area shall be responsible for:

- Operational management of the data activities related to the collection, maintenance, protection, and dissemination of data in their Department(s) or College(s);
- Determining whether the data is collected or maintained directly by the Department(s) or College(s), members of the community in other Department(s) or College(s), or Non-University Group sources;
- Reviewing and approving requests for access by members of the community;
- In consultation with the IST, determining the level of access given to a member of the community;
- Ensuring compliance with federal and state laws and regulations, University regulations, and contractual obligations regarding the release, responsible use of, and access to data;
- Informing members of the community of applicable regulations and proper understanding of data;
- Assist in providing data definitions for each data element within the domain of the applicable Department(s) or College(s) (in some cases the Departments and Divisions will work with Institutional Research staff to define the meanings of key terms);
- Ensuring the accuracy, privacy, and integrity of the data which the Dean or Director oversees.

4.3.4 Each member of the community who is authorized to access data by the Dean or the Director shall be responsible for:

- Accessing the data solely for the conduct of and only as required to conduct University business;
- Following regulations and procedures established for responsible use of the data;
- Ensuring the privacy of data by viewing, storing, and deriving information from it under secure conditions
- Ensuring accuracy and timeliness of any data entered or updated; and,
- Collecting, preparing, entering or maintaining data for the authorized Department(s) or College(s), if authorized by a Dean or Directors.

4.4 Data Classification. Data assets shall be classified in a manner consistent with its value and sensitivity to loss or disclosure. All data shall be designated as internal, and thus solely for use within the University, or designated as available for meeting reporting requirements to the Kansas Board of Regents, state government, federal government, or other external agencies. Except as required by law or as designated by executive staff, data shall not be open to the general public.

4.4.1 Permission to view or query data for legitimate University purposes shall normally be granted to Employees. See below 4.5 Requesting Data Access.

4.4.2 Each data element and data view of University data will be assigned one of the following three classifications by the Deans and Directors, in consultation with the executive staff member to whom they report

- Unrestricted Data – data elements having no access restrictions and therefore available to the general public;

- Sensitive data – data elements for which members of the community must obtain specific authorization to access since the data's unauthorized disclosure, alteration, or destruction could cause damage to the University. The specification of data as sensitive shall include:
  - Reference to the legal or externally imposed constraint requiring this classification;
  - The categories of users typically given access to the data; and,
  - The conditions or limitations under which access is typically given.
- Confidential Data – data elements for which the highest levels of restriction shall apply based on risk or potential of harm resulting from disclosure or inappropriate use. This includes, but is not limited to, information:
  - Which when improperly used or disclosed could adversely affect the ability of the University to accomplish its mission
  - Required to be kept private or confidential by the Family Educational Rights and Privacy Act of 1974 (FERPA) or other state or federal law requiring the nondisclosure of information and,
  - Data protected from disclosure under the Open Records Act or other applicable laws or regulations.

4.4.3 Data originating from the central administrative systems shall be classified as sensitive unless otherwise indicated.

4.5 Requesting Data Access

4.5.1 Requests for access to data shall**:**
- Be submitted in writing or electronically to the appropriate executive staff member, Dean, or Director;
- Include written or electronic approval of the requestor's Dean or Director; and,
- Specify the data needed and the purpose for accessing the data.

4.5.2 The executive staff member, Dean or Director shall reject or approve the request and if approved, shall:
- Specify the access right as read only, write, modify, or delete;
- Forward the request to CTC for technical implementation, and,
- Retain a copy (paper or electronic) for audit purposes.

4.6 Documenting Data Access. The documentation maintained by the executive staff members or the Dean or Director shall include, but not be limited to:
- Name
- Description
- Sensitivity of Classification
- Location
- Retention

4.6.1 The Institutional Research Office also has responsibility for documenting and defining data for official university reporting purposes. This Office works with the Deans and Directors of the applicable Department(s) or College(s) data so members of the community are aware of the definitions, restrictions, or interpretations, as well as other issues ensuring the correct use of data.

5. **Personnel Security.** Appropriate practices, technologies, and/or services shall be utilized for the purpose of ensuring personnel security safeguards are applied. Appropriate practices, technologies, or services shall include, but not be limited to:
   - Granting or withdrawing physical and system access privileges upon:
     - Initial employment of an individual;
     - The transfer of an employee to another Department or College;
     - Change in an employee's job duties, or;
     - The termination or resignation of an employee
   - Granting, modifying, or revoking of an employee's physical or system access privileges by an employee's supervisor.
   - Maintaining confidentiality of University data by:
     - Keeping all passwords private and confidential and protecting them from disclosure to any person or entity;
     - Allowing no person or entity to use any password or account not assigned to them; and,
     - Accessing and/or disclosing to others confidential information only as may be required in the performance of job duties;
   - Training to reinforce the University's security standards within 30 days of a new hire; and,
   - Background checks of individuals per University regulations.

   5.1 Security in Employee Handbook. The Employee Handbook for all employees shall clearly state the employee's responsibility for protecting relevant information assets accessed on or off campus.

   5.2 Security Awareness Training. Each employee shall complete ongoing information security awareness training. Security awareness training shall include:
   - A formal process which includes information security training, prior to access to data or information systems being granted (for example, for grade entry or access to CICS data);
   - Periodic reminders of both general security topics and specific issues of relevance to the University;
   - Other appropriate efforts to raise and maintain awareness of security issues.

   5.3 Discipline for Violations. Any existing policy or procedure of FHSU for discipline of students and employees applies to any breach of this policy.

5. **Termination or Change of Employment.**

   5.4.1 Changes of responsibilities and duties within the University shall be, for information security purposes, processed as a termination of old responsibilities and re-assignment to new responsibilities using established CTC controls for those processes unless otherwise indicated.

   5.4.2 The terminating Employee shall return all of the University's information assets in the Employee's possession (examples include flash drives, external hard drives, and information stored on smart phones).

   5.4.3 Employee access to information and information systems shall be severed upon termination of employment or a contractual relationship, and Employee rights shall be disabled or removed.

6. **Physical and Environmental Security.** Security measures intended to prevent unauthorized physical access, damage, or interference with the University's information systems shall be established. Security measures appropriate to the identified risks and the value of the protected information assets shall be used.

6.1 Securing Work and Asset Location Areas.

6.1.1 Physical Security Perimeters to protect areas containing servers, multi-user systems, or other non-personal computer systems shall consist of, but not be limited to, the following:

- Walls;
- Controlled entry doors;
- Staffed reception desks.

6.1.2 Secure areas shall be protected by appropriate entry controls including, but not limited to:

Key cards or personal identification numbers (PIN);
Requiring Non-CTC individuals or groups to be monitored while present in restricted areas;
Requiring formal authorization of Non-University Groups before entry is permitted; and,
Requiring Non-University Groups to be monitored while working or while present in restricted areas.

6.1.3 Physical protection against damage from natural or man-made risks, shall be implemented including, but not limited to:

- Appropriate fire suppression equipment effectively located on site.
- Uninterruptible Power Supplies (A.K.A. UPS or battery backup) for sustaining power to computing systems for an acceptable length of time.
- Appropriate placement of backup facilities and data copies in a suitable location at least one mile from data source.

6.2 Equipment and Cabling Security on Premises. Each Department or College shall establish controls to protect equipment and cabling from loss, damage, theft, or compromise of information assets or interruption of the University's activities.

6.2.1 Equipment shall be located and protected to reduce the risks from environmental threats and hazards, and to:

- Reduce the opportunities for unauthorized access;
- Minimize unnecessary risks to equipment; and,
- Eliminate the possibility for unauthorized access to sensitive areas.

6.2.2 Power and telecommunications cabling carrying sensitive data or supporting information services shall be protected from interception or damage.

6.2.3 Equipment shall be correctly maintained to ensure its continued availability and integrity

6.2.4 Sensitive or confidential information shall be protected by either locking the screen or logging out when leaving the computer unattended.

6.3 Equipment Security Off-premises. Appropriate security measures shall be applied to any portable computer device, including mobile devices such as laptops or PDAs taken off-site, with consideration given to the variable risks of working outside the University's premises.

6.3.1 Employees shall exercise due care of any computer device in their possession to prevent damage to or loss of the device, including but not limited to:

- Not leaving the device unattended in public places;
- Not displaying sensitive information displayed on the screen in public;
- Storing the device in a secure location when it has to be left unattended; and,
- Carrying the device as hand luggage while traveling.

6.3.2 Employees shall report loss or theft of the device to local law enforcement, the University Police Department, and the CTC.

6.3.3 Employees shall prevent unauthorized use of or access to the mobile device by:

- Protecting the display with a password if it is unattended; and,
- Creating a password that is reasonably secure. See website http://www.fhsu.edu/ctc/helpdesk/securepassword.shtml for guidelines.

6.3.4 Access to or use of data stored on the device shall be prevented by methods including, but not limited to:

- The use of software encryption for any files to be stored on local disk drives on laptops not having hardware encryption or the use of an encrypted USB Key;
- Backing up sensitive or confidential data only to secure media. No copies of files shall be moved to unencrypted portable drives;
- Saving all sensitive or confidential data on University network servers whenever possible rather than saving on the local disk.

6.3.5 Only software licensed to the University or free software shall be installed on the devices assigned. Due care shall be exercised to protect against installation of any malicious or unlicensed software on the device. *Sophos* and other security companies have updated lists of malicious software. The university reserves the right to block installation and use of applications that have been shown to be malicious.

6.3.6 Any device shall be used in compliance with applicable laws and regulations, including, but not limited to:

- Copyright and trademark laws;
- License agreements of software installed on the device; and,
- All University policies and regulations applicable to the use of the University computer information systems.

6.3.7 Data as described in Section 2.3 must be encrypted if stored off campus or stored and removed from campus. Such storage shall be approved in advance by the appropriate Dean or Director.

6.4 Secure Disposal or Re-use of Equipment. Prior to disposal, all equipment containing storage media shall be checked by the CTC to ensure sensitive data and licensed software have been removed or securely overwritten.

7. Communications and Operations Management.

7.1 Operational Procedures and Responsibilities. Operational procedures and Employee responsibilities shall be enforced by Deans and Directors to ensure correct and secure operation of information processing.

7.1.1 Operating procedures shall be documented, maintained, and made available to Employees as needed.

7.1.2 Appropriate change management procedures shall govern changes to information processing facilities and systems.

7.1.3 Duties and areas of responsibility shall be pragmatically segregated to reduce opportunities for unauthorized or unintentional modifications or misuse of the University's information assets.

7.1.4 Development and test environments will be functionally independently of production environments to prevent development or testing in production environments.

7.2 System Planning and Acceptance.

7.2.1 The CTC shall engage in capacity planning by appropriately monitoring and making projections of future capacity requirements to ensure adequate system performance.

7.2.2 Acceptance criteria for new information systems, upgrades, and new versions shall be established, and suitable system testing will be carried out during development and prior to acceptance.

7.3 Protection from Malicious Software and Mobile Code. The integrity of software and information shall be protected by implementation of appropriate measures for prevention and detection of, and response to, malicious code. This includes, but is not limited to:

- Appropriate employee awareness;
- Forbidding execution of unlicensed or unapproved software;
- Timely updating of anti-virus and anti-spyware software; and,
- Periodic reviews/scans of computer systems to identify and, where possible, remove any unlicensed software.

7.4 Housekeeping. In accordance with back-up schedules approved by the Director of the CTC or the responsible Dean or Director, back-up copies of data and software shall be made and periodically tested, including but not limited to:

- A definition of the level of backup required for each system (scope of data to be imaged, frequency of imaging, duration retention) on the basis of legal, regulatory, certificatory standards, and/or business requirements;
- Maintenance records of back-up copies, including content and current location;
- Complete documentation of restoration procedures for each system;
- Storage of back-up copies in a remote location, at least one mile from the primary site;
- Appropriate physical and environmental controls for back-up copies wherever located;
- Appropriate technical controls for back-up copies of sensitive or confidential information;
- Regular testing of back-up media; and,
- Regular testing of restoration procedures.

7.5 Network Security Management. Regulations and procedures shall be established and maintained by the Director of CTC in coordination with the Networking Supervisor which protect the information and networks and maintain security for the systems and applications using the network, which includes data in transit. These regulations and procedures shall include, but are not limited to:

- Ensuring the availability of network services and information services using the network;
- Establishing responsibilities and procedures for management of equipment on the network;
- Implementing controls to safeguard the confidentiality and integrity of sensitive data passing over the University's network and to or from public networks; and,
- Appropriate logging and monitoring of network activities, including security-relevant actions.

7.6 Electronic Media Handling. Deans and Directors shall establish procedures to prevent unauthorized disclosure, modification, removal, or destruction of sensitive or confidential information assets, or interruptions to business activities encompassing the following:

7.6.1 Procedures shall be established for management of removable media containing sensitive or confidential data which shall include, but not be limited to, requiring authorization by the responsible Dean or Director prior to removal or relocation.

7.6.2 When media is no longer needed it shall be disposed of in a secure manner.

7.6.3 Data shall be protected from unauthorized disclosure or misuse by procedures appropriate for the sensitivity level.

7.6.4 System documentation shall be appropriately protected against unauthorized access.

7.7 Exchange of Data. The security of data and software exchanged within the University and with Non-University Groups shall be maintained by the applicable Dean or Director.

7.7.1 Formal procedures shall be developed and implemented to protect the exchange of data, covering the use of all types of communications and data storage media including, but not limited to:

- Procedures for the protection of wireless communications (example, do not transmit proprietary information over open wireless networks);
- Use of cryptographic methods where appropriate to achieve sufficient protection (example, when transmitting proposals to the federal government the use of public key, private key cryptology is commonly used);
- Guidelines about acceptable and unacceptable uses of communication facilities and media. Examples include using secure ftp and secure telnet to prevent the intercepting and/or logging of plain text data over the network.
- Retention and disposal guidelines for business data; and,
- Compliance with all relevant legal, regulatory, and/or certificatory requirements for information exchange as needed.

7.7.2 Information involved in electronic messaging shall be appropriately protected to the extent possible. Users should be very careful about what information and attachments are sent via e-mail and instant messaging, for example.

7.7.3 Business processes shall be developed and implemented to protect data associated with the interconnection of business systems.

7.7.4 Data involved in electronic commerce passing over public networks shall be appropriately protected from fraudulent activity and unauthorized disclosure and modification.

7.7.5 Data involved in on-line transactions shall be appropriately protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, and unauthorized disclosure and modification.

7.7.6 The integrity of data being made available on a publicly available system, such as a Web server, shall be appropriately protected to prevent unauthorized modification.

7.8 Monitoring for Security Incidents and Malfunctions.

7.8.1 Audit logs recording individual activities, exceptions, and information security events shall be produced, and kept for an agreed-upon time period specified by the Director of the CTC to assist future investigations and access control monitoring.

7.8.2 Procedures for monitoring use of information processing facilities shall be established and the results of monitoring activities and utilization will be regularly reviewed.

7.8.3 Logging facilities and log information shall be appropriately protected against tampering and unauthorized access.

7.8.4 System administration and system operation activities shall be appropriately logged, as part of the general audit trail process.

7.8.5 System malfunctions shall be appropriately logged and analyzed, and appropriate actions taken to correct and prevent future occurrences.

7.8.6 The clocks of all relevant processing systems within the University or security domain shall be appropriately synchronized. This is important for obtaining accurate computer logs, forensic information, MAC times, and other security matters.

8. Access Control. Department Heads shall control access to data, information processing facilities, and business processes in partnership with the CTC.

8.1 Access Control Regulation. In the development of these regulations, consideration has been given to:

- Security issues for particular information systems, given business needs, anticipated threats and vulnerabilities;
- All relevant legislative, regulatory, certificatory, and program requirements;
- Relevant contractual obligations or service level agreements;
- Other University regulations regarding electronic information access, use, and disclosure,
- Consistency among such regulations across the University's systems and networks;
- Clearly stated rules and rights based on user profiles;
- Consistent management of access rights across a networked environment;
- An appropriate mix of logical (technical) and physical access controls;
- Segregation of access control roles including, but not limited to: access request, access authorization, and access administration;
- Requirements for formal authorization of access requests (provisioning); and,
- Requirements for authorization and timely removal of access rights (de-provisioning)

8.2 Identity Management. The Director of the CTC and CTC staff shall ensure authorized user access, and prevent unauthorized access to data and information systems by:

- Implementing formal procedures to control the allocation of access rights;
- Creating procedures to cover all stages in the life-cycle of user access, from provisioning to de-provisioning;
- Giving special attention to control of privileged or administrative access rights; and,
- Implementing appropriate technical measures for identification and authentication to ensure compliance with defined access rights.

8.2.1 Formal user registration and de-registration procedures shall be implemented by the Director of the CTC for granting and revoking access to all information systems and services including, but not limited to:

- Assignment of a unique identifier (user-ID) to each user;
- Confirmation by supervisor or other personnel that each user's access is consistent with business purposes and other security regulation controls;
- Documentation of approval from data custodian for each user's access;
- Ensuring service providers do not grant access until all authorization procedures are completed;
- Maintaining a current record of all user authorized access to a particular system or service;
- Upon notification, changing or eliminating access rights for users who have changed positions, whose duties have changed, or show employment with the University has terminated; and,
- Checking for and removing redundant or apparently unused user-IDs.

8.2.2 Allocation and use of access privileges shall be restricted and controlled by, but not limited to:

- Development of privilege profiles for each system, based on user profiles and system resources;
- Granting of privileges based on these standard profiles when possible;
- A formal authorization process for all privileges; and,
- Maintaining a current record of privileges granted.

8.2.3 Allocation of passwords shall be controlled through a formal management process including, but not limited to:

- Secure methods for creating and distributing temporary, initial-use passwords;
- Forcing users to change any initial-use password;
- Development of procedures to verify a user's identity prior to providing a replacement password;
- Prohibiting loaning of passwords;
- Prohibiting storage of passwords on computer systems in unprotected form; and,
- Prohibiting use of default vendor passwords, where applicable.

8.2.4 Allocation of access tokens, such as key-cards, shall be controlled through a formal management process including, but not limited to:

- Secure methods for creating and distributing tokens;
- Use of two-factor tokens (token plus PIN) where appropriate and technically feasible;
- Development of procedures to verify a user's identity prior to providing a replacement token; and,
- Prohibiting loaning of tokens.

8.2.5 Using a formal process, each user's access rights shall be reviewed at regular intervals, and after any promotion, demotion, transfer, termination or change of duties of a user.

8.3 User Responsibilities. The user is responsible for preventing unauthorized access, compromise, or theft of data and information systems by:

- Maintaining authentication security, particularly regarding password and token safety; and,
- Securing computers and other office equipment.

8.3.1 Users shall follow good security practices in the selection and use of passwords. Good security practices include but are not limited to:

- Keeping passwords confidential and not sharing them;
- Not keeping a paper or electronic record of passwords unless done so securely;
- Changing a password when there is any suspicion it has been compromised, then reporting the suspicion.
- Selecting passwords which are resistant to standard security attacks.
- Changing passwords periodically;
- Changing a temporary password on first log-on;
- Avoiding the storage of passwords in automated log-on processes;
- Not using the same password for business and non-business purposes; and,
- Using the same password for multiple systems or services only where a reasonable level of security can be assured for each.

8.3.2 In the use of access tokens users shall follow good security practices including, but not limited to :

- Keeping tokens secure and not sharing them;
- Avoiding keeping a paper or electronic record of PIN associated with a two-factor token or keeping such records in a secure location; and,
- Reporting when a token is lost or there is any suspicion it has been compromised.

8.3.3 Users shall monitor password and token activity history where available including, but not limited to:

- Observing and reporting discrepancies in the last successful login and last unsuccessful login information, when it is available; and,
- Observing and reporting discrepancies in the date and time information for all other activities which have timestamps, such as file accesses or modification.

8.3.4 With respect to the equipment assigned to them, users shall observe appropriate physical and technical practices including, but not limited to:

- Limiting use to performing appropriate functions in an appropriate manner; and,
- Learning appropriate functions and use.

8.3.5 Users shall ensure unattended computing equipment has appropriate protection including, but not limited to:

- Terminating logged-in sessions before a device is left unattended, unless it can be securely locked with a password-protected screensaver; and,
- Physically securing devices, or the area in which a device is located, with a key-lock or equivalent if a device will be unattended.

8.3.6 Users shall ensure desks and other work areas are kept cleared of sensitive and confidential data and any storage media when unattended. Computer screens shall be kept clear of sensitive and confidential data when unattended.

8.3.7 Users shall ensure photocopiers, fax machines, and other office equipment are kept cleared of sensitive and confidential data and any storage media when unattended.

8.4 Network Access Control. The Data Communication Coordinator shall prevent unauthorized access to network services.

8.4.1 Users shall be restricted to access those services that they have been specifically authorized to use by implementation of:

- Authorization procedures for determining who is allowed to access which networks and network services consistent with other access rights; and,
- Regulations governing deployment of technical controls limiting network connections.

8.4.2 Appropriate authentication methods shall be used to control remote access to the network

8.4.3 Access to the network shall be limited to identified devices or locations where appropriate and technically feasible.

8.4.4 Physical and logical access to diagnostic and configuration ports shall be appropriately controlled by:

- Providing physical security for on-site diagnostic and configuration ports;
- Providing technical security for remote diagnostic and configuration ports; and,
- Disabling ports, services, and similar facilities not required for business functionality.

8.4.5 Groups of information services, users, and services shall be segregated on networks where appropriate and technically feasible by:

- Separation into logical domains, which each protected by a defined security perimeter; and,
- Secure gateways between or among logical domains.

8.4.6 Capabilities of users to connect to the network shall be appropriately restricted by filtering the connection using methods consistent with access control regulations and applications requirements. Connection types include, but are not limited to:

- Messaging;
- Email;
- File transfer;
- Interactive access; and,
- Applications access.

8.4.7 Routing controls shall be implemented to ensure computer connections and information flows do not breach the access control regulations of the business applications. Routing controls include, but are not limited to:

- Positive source and destination address checking; and,
- Routing limitations based on the access control regulations.

8.5 Operating System Access Control. The Director of the CTC and Server Administrators shall implement controls to restrict data system access to authorized users by requiring authentication of authorized users in accordance with the defined access control regulations including, but not limited to:

- Providing mechanisms for authentication by knowledge-token and or biometric-factor methods as appropriate;
- Recording successful and failed system authentication attempts; and,
- Recording the use of special system privileges.

8.5.1 Access to systems shall be controlled by secure log-on procedures including, but not limited to:

- Display of general notice warning about authorized and unauthorized use;
- Forbidding display of system or application identifiers before successful log-on;
- Forbidding display of help messages prior to successful log-on that could aid unauthorized users;
- Validation or rejection of log-on only upon completion of both user-ID and password;
- Display passwords as symbols and not as characters or spaces as entered;
- Forbidding transmission of passwords in clear text;
- Limiting the number of unsuccessful log-on attempts in total or for a given time period;
- Logging of successful and unsuccessful log-on attempts; and,
- On successful log-on, display date and time of last successful log-on and any unsuccessful attempts.

8.5.2 All information system users shall have a user-ID for their personal use only.
A suitable authentication technique, knowledge-token and/or biometric-based, shall be chosen to authenticate the user incorporating such methods as, but not limited to:

- Prohibiting the sharing of user IDs except for monitored email accounts approved by the Director of the CTC and the University Attorney;
- Allowing guest user-IDs only with required paper audit trail and only when limited access privileges justify the practice;
- The use of multiple identification and authentication factors suitable to the sensitivity of the information being accessed; and,
- The prevention of regular user activities being performed from privileged accounts.

8.5.3 Systems for managing passwords designed to ensure the quality of adopted authentication methods shall include, but not be limited to:

- Log-on methods which enforce the use of individual user-IDs and associated passwords;
- Set or change password methods which enforce choice of strong passwords;
- Forcing change of temporary password on first log-on;
- Enforcing password change thereafter at reasonable intervals;
- Storing passwords separately from application data; and,
- Storing and transmitting passwords in encrypted form only.

8.5.4 Systems for managing access tokens shall be designed to ensure the quality of adopted authentication methods.

8.5.5. Use of system utilities capable of overriding other controls shall be restricted and appropriately monitored.

8.5.6 Interactive sessions shall be designed to shut down and lock out the user after a defined period of inactivity. Resumption of interactive sessions shall require re-authentication. The inactivity time periods shall be based on:

- Time-out periods that reflect risks associated with type of user, setting of use, and sensitivity of the applications and data being accessed;
- Waiver or relaxation of time-out requirement when it is incompatible with a business process, provided other steps are taken to reduce vulnerabilities including, but not limited to remove of:
  - Sensitive data;
  - Confidential data;
  - Network connection capabilities; and,
  - Compliance with the PCI-DSS 15 minutes timeout requirements.

8.5.7 To provide additional security for high-risk applications or remote communications capabilities, restrictions on connections times and from specific internet protocol (IP) address ranges will be in place.

8.6 Application and Information Access Control. The following application and information access controls shall be established by the Director of CTC.

8.6.1 Access to information and application system functions by users and support personnel shall be restricted in accordance with defined access control regulations consistent with the University's access regulations.

8.6.2 Sensitive systems shall have a dedicated computing environment including, but not limited to, explicit identification and:

- Documentation of sensitivity by each system or application; and,
- Acceptance of risks when shared facilities and/or resources must be used.

8.7 Mobile Computing and Teleworking. The Director of the CTC and the IST shall recommend policies for and implement controls for use of mobile computing and teleworking facilities which are commensurate with:

- Type of user(s);
- Setting(s) of mobile or teleworking use; and,
- Sensitivity of the applications and data being accessed from mobile or teleworking settings.

8.7.1 For mobile computing and communications activities, all regulations in this section 8. and other sections apply. This includes all forms of portable computing devices, mobile phones and smart phone-PDAs, and portable storage devices and media. Relevant sections include:

- Physical protection (Section 6);
- Data storage minimization (Section 7);
- Access controls (Section 8);
- Cryptographic techniques (Section 7);
- Data backups (Section 7.4);
- Anti-virus and other protective software (Section 7);
- Operating systems and other software updating (Sections 9 and 10);
- Secure communication (Virtual Private Network) (Section 7);
- Sanitization prior to transfer or disposal (Section 7).

8.7.2 For teleworking activities in off-premises locations, all regulations in this and other sections apply. Relevant sections include, but are not limited to:

- Physical security measures at the off-premises site (Section 6);
- Appropriate controls to prevent access by others at the site (Section 8);
- Cryptographic techniques for data storage at the site and communications to or from the site (Sections 7 and 9);
- Data backup processes and security measures for those backup copies (Section 7);
- Security measures for wired and wireless network configurations at the site (Sections 6 and 7);
- Appropriate software licensing (Section 6);
- Use of University computing hardware at the site (Section 6); and,
- Use of teleworkers' computing hardware at the site (Section 6).

9. Systems Development and Maintenance. The intent of these regulations is to ensure security is an integral part of the University's information systems, and of the business processes associated with those systems.

9.1 Security Requirements of Information Systems. Statements of business requirements for new information systems, or enhancements to existing information systems shall include specification of the requirements for security controls, including but not limited to:

- Consideration of the business value of information assets affected by the new or changed system(s);
- Consideration of the legal, regulatory, certificatory, and program standards for information assets affected by the new or changed system(s);
- Consideration of administrative, technical and physical controls available to support security for the system(s);
- Integration of controls early in system design and requirements specification; and,
- A plan for testing and acceptance.

9.2 Security in Applications. Security in applications shall be designed to prevent errors, loss, unauthorized modification, or misuse of information in applications.

9.2.1 Data input in applications shall be validated to ensure the data is correct and appropriate.

9.2.2 Validation checks shall be incorporated into applications to detect the corruption of data through processing errors or deliberate acts.

9.2.3 Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.

9.2.4. Data output from applications shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

9.3 Cryptographic Controls. Where appropriate, the confidentiality, integrity, and authenticity of data will be protected by cryptographic means. The application developer shall:

- Create specifications based on a thorough risk assessment, which considers appropriate algorithm selections, encryption key management, and other core features of cryptographic implementations; and,
- Use encryption as appropriate for data:
  - On disk drives;
  - Transported by mobile or removable media and embedded in mobile devices; and,
  - Transmitted over communication links.

9.3.1 Encryption key management and processes shall support the University's use of cryptographic techniques. The Director of CTC shall specify roles and responsibilities for implementation of and the monitoring of compliance with regulations.

9.4 Security of System Files.

9.4.1 Installation of software on operational systems shall be implemented to minimize the risk of interruptions in or corruption of information services. The application developer or administrator shall:

- Update only with appropriate management authorization;
- Appropriately test and certify software deployed to operational systems;
- Use appropriate change management and configuration control processes for stages of updating;
- Maintain appropriate documentation of the nature of the change and the processes used to implement it;
- Have a rollback strategy in place, including retention of prior versions as a contingency measure; and,
- Maintain appropriate audit logs to track changes made to the application or its configuration.

9.4.2 Test data shall be selected carefully and appropriately logged, protected, and controlled.

9.4.3 Access to program source code shall be restricted by providing:

- Appropriate physical and technical safeguards for program source libraries, documentation, designs, specifications, verification and validation plans; and,
- Strict change management and other controls of the maintenance and copying of these materials.

9.5 Security in Development and Support Processes. The Director of CTC shall implement security in development and support processes.

9.5.1 Change control procedures shall include, but not be limited to:

- A formal process of documentation, specification, testing, quality control and managed implementation;
- A risk assessment, analysis of actual and potential impacts of changes, and specification of any security controls required;
- A budgetary or other financial analysis to assess adequacy of resources;
- Formal agreement to and approval of changes by appropriate management;
- Appropriate notification of all affected parties prior to implementation on the nature, timing, and likely impacts of the changes; and,
- Scheduling of changes to minimize the adverse impact on business processes.

9.5.2 When operation systems and processes are changed, critical business processes shall be reviewed and tested to ensure there has been no adverse impact.

9.5.3 Modifications or additions to source codes of purchased applications shall be strictly limited to those assigned by the purchased application's project committee.

9.5.4 Opportunities for data leakage shall be appropriately minimized or prevented.

9.5.5 Outsourced software development shall be appropriately supervised and monitored by the Director of CTC or designee.

9.5.6 The Information Security Team shall provide timely information about technical vulnerabilities of information systems used by the University. The Director of CTC and the IST shall implement controls to limit technical vulnerabilities, including but not limited to:

- A complete inventory of information assets sufficient to identify systems that are at risk for being affected by a particular technical vulnerability;
- Procedures to allow timely response to identification of technical vulnerabilities that present a risk to any of the University's information assets, including a timeline based on the level of risk; and,
- Defined roles and responsibilities for implementation of countermeasures and other mitigation procedures.

10. Business Continuity Management. The Administration's plans for protecting the University from interruptions of business activities or to ensure timely resumption from interruption shall include the continuity of electronic business and information processes.

10.1 Information Security in Business Continuity Management. The electronic information security plans for supporting business continuity or for ensuring timely resumption from interruption caused by failures of information systems, shall include, but not be limited to:

- Identification of information assets involved in critical business processes;
- A risk assessment addressing likely causes and consequences of information system failures;
- Identification and consideration of preventive and mitigating controls in light of these risks;
- Identification of sufficient financial, technical and human resources to address the preventive or mitigating control requirements;
- Development and documentation of business continuity plans and processes, including assignment of responsibilities and incorporation into the organization's general processes and structure; and,
- Regular testing and updating of business continuity plans and processes.

10.2 Identifying Business Interruption Risks. Deans and Directors shall identify events which can cause interruptions to business processes, along with the probability and impact of such interruptions, and their consequences for electronic information security. This process includes, but is not limited to:

- Identification of all significant risks, including the probable impact on operations in terms of scale, likely damage and recovery period;
- Full involvement of owners of significant organizational assets in the assessment process;
- Identification of acceptable and unacceptable losses and interruptions; and,
- Formal documentation of the assessment's results and a plan for regular updating to ensure that it is current and complete.

10.3 Developing and Implementing Continuity Plans. Deans and Directors shall develop and maintain business continuity plans to maintain or restore operations and ensure availability of information at the required level and in the required time, following interruptions to or failures of business processes, including but not limited to:

- Identification of and agreement on all responsibilities and operational procedures;
- Specification of the disaster recovery/business continuity procedures to affect recovery and restoration of business processes;
- A backup plan to ensure recovery of all data following process restoration, including the ability to replicate exact copies of data in its state prior to disruption of operations;
- Specification of alternative operational procedures to follow pending completion of recovery and restoration, including methods for accessing all critical data;
- Documentation of the above plan elements;
- Appropriate education and awareness for staff regarding plan elements; and,
- Testing and updating of the plan.

10.4 Business Continuity Planning Framework. A single framework of business continuity plans shall be maintained to ensure all plans are consistent, information security requirements are consistently assessed, and priorities are identified for testing and maintenance of the plan.

10.5 Testing, Maintaining and Re-assessing Business Continuity Plans. Business continuity plans shall be tested and updated regularly to ensure they are up to date and effective. The testing and updating shall include, but not be limited to:

- Testing which assures all persons with significant responsibilities under the plan(s) are aware of them and competent to carry out the plan(s);
- A range and frequency of testing exercises, performed as necessary to ensure awareness and competence; and,
- Regular reviews and updating of the plan(s) based on testing results.

11. Compliance. Each Dean or Director shall be responsible for compliance with all regulations including University, statutory, regulatory, and contractual obligations; other legal requirements; and technical standards affecting electronic information processing within the Dean's or Director's area of responsibility.

11.1 Legal Requirements.

11.1.1 All legal requirements shall be identified. The College's or Department's approach to meeting these requirements shall be explicitly defined, documented, and kept up to date. Colleges and Departments should work with the University General Counsel on identifying these requirements.

11.1.2 The procedure of each College or Department shall ensure:

- Protection of confidentiality of personal information;
- Protection of all materials for which there may be intellectual property rights (IPR);
- Protection of University records by:
  - Categorization of data, consistent with legal and business requirements;
  - Creation of data protection procedures consistent with this categorization;
  - Creation of data retention and data destruction procedure consistent with this categorization;
  - Implementation of data retention and destruction schedule;
  - Appropriate controls to protect records from loss, destruction or falsification during their retention period;
  - Appropriate controls to ensure appropriate destruction at the end of their retention period; and,
  - Prohibiting access or disclosure to unauthorized individuals.
    - Cryptographic methods and controls are used in accordance with all applicable legal requirements

11.1.3 The CTC shall implement methods to prevent the misuse of data and information processing facilities by members of the community by methods of, including but not limited to:

- Promoting awareness of the precise scope of their permitted access;
- Promoting awareness of the monitoring in place to detect unauthorized access;
- Providing a log-on warning message reminding of access policies and monitoring; and,
- Intrusion detection and prevention, content inspection, and other monitoring activities as appropriate.

11.2 University Security Regulations and Technical Standards.

11.2.1 Each Dean and Director shall periodically review all security processes within his or her area of responsibility to ensure compliance with relevant security regulations.

11.2.2 Data systems shall be regularly checked for compliance with security implementation standards, including but not limited to, penetration tests and vulnerability assessments.

12. Incident Management. Incident management is governed by the University's Critical Incident Management Team. All serious incidents are reviewed by the Information Security Team. Whenever a potentially serious incident is discovered, the incident should be reported to the Coordinator of the Critical Incident Management Team. An information security incident is any real or suspected adverse event relative to the security of computer systems, networks, or electronic data.

12.1 Incident Documentation. The incident shall be fully documented, including but not limited to:

- How the incident was discovered;
- The category of the incident;
- How the incident occurred;
- From where the attack came;
- The derived response plan;
- The response action; and,
- The effectiveness of the response (if knowable).

12.2 Incident Categories. There shall be 6 categories of incidents as follows:

- Employee fraud;
- Impersonation;
- Loss;
- Alteration of significant data;
- Penetration;
  Theft; and,
- Unauthorized disclosure.

12.3 Retention of Evidence. Evidence gathered during the response shall be retained as long as necessary to complete resolution of the incident and subsequent action by the University or law enforcement. The evidence to be retained shall include copies of all documents, records, logs, emails, and other documentable communication, including but not limited to:

- Activities performed; and,
- Individuals interviewed.

12.4 Reporting to Law Enforcement, Kansas Board of Regents, State of Kansas CITO, and State of Kansas IT Security Officer. Serious incidents will be reported to University law enforcement authorities. The University President will determine whether to contact the President and CEO of KBOR and the CIO of KBOR. For purposes of determining whether to contact KBOR a "major incident" is defined as a breach of data involving credit cards, social security information, or other personally identifiable information that could cause detriment or financial harm to individuals or the institution. Also, major security incident updates should be provided to the Kansas Board of Regents, Executive CITO, and State IT Security Officer.

12.5 Damage Assessment. An assessment of damage to the University shall be made and reported by the data custodian of the affected data including but not limited to:

- An estimate of damage cost; and,
- Cost of containment efforts.

12.6 Response Review. A thorough review of the response shall be made by the Crisis Management Team to determine:

- Appropriateness;
- Efficiency; and,
- Effectiveness.

12.7 Reoccurrence Prevention Plan. A plan shall be developed and implemented for prevention of reoccurrence of such an incident.

Adopted by President's Cabinet 12/02/09