

FSCOT Agenda
May 4, 2021

Zoom Connection: <https://ksu.zoom.us/j/7855322637>
Phone Connection: +1 669 900 6833 or +1 646 876 9923

- 1.) Turn on recording and announce disclaimer
- 2.) Call meeting to order – **Brett**
- 3.) Approve agenda (additions) – **Brett**
 - a. Suggest discussing the Response to SGA Resolution on Zoom CC and Live Transcriptions so IT staff can drop off -- see Old Business, 6.a. -- before committee reports.
- 4.) Ask someone to take minutes – **Brett**
- 5.) Committee Reports:
 - a. Extended IT Leadership Group – **Brett & Michael**
 - i. The group is reevaluating its purpose and charge and then will work on the next steps of the IT strategic plan
 - b. IT Policy Review Team – **Don Crawford**, Information Technology Manager, Architecture, Planning & Design, FSCOT Member
 - i. [Attachment # 1 \(page # 4\) PPM 3415 Information Security Plan \(First Reading\)](#)
 - ii. [Attachment # 2 \(page # 10\) PPM 3434 IT Security Incident Reporting and Response Policy \(First Reading\)](#)
 - iii. [Attachment # 3 \(page # 17\) PPM 3495 Collection, Use and Protection of Social Security Numbers \(First Reading\)](#)
 - c. Office 365 Governance Group – **Michael**
 - i. Evaluating some changes with Teams and moving away from Skype
 - d. Project Governance Group – **Brett**
 - i. No Report
 - e. Record and Retention Committee – **Lisa Shappee**, Library Director/Associate Professor, K-State Polytechnic, FSCOT Member
 - f. University Network Infrastructure Refresh Project – **Michael**
 - i. Continuing to discuss a huge infrastructure project if funding is available
- 6.) Old Business (Business from Previous Meetings)

- a. Response to SGA Resolution on Zoom CC and Live Transcriptions Labs – **Scott Finkeldei**, Director of Academic and Student Technology, Information Technology Services and FSCOT Liaison for Chief Information Officer, Shelley Griffin, Supervisor, from Classroom Technology – See Attachment # 4 (page # 23)
 - i. Create an appropriate response to the SGA resolution on Zoom cc and live transcriptions
 - ii. Action:
 - 1. Develop official response that represents IT and FSCOT
- b. Joint meeting with Faculty Affairs about TopHat resolution – 30 minutes – **Michael**
- c.
- 7.) New Business
 - a. IT Strategic Plan Priorities?
 - b.
- 8.) Other Items – **Group**
 - a.
- 9.) Future Meetings and Agenda – **Brett**
 - a. May 18
 - i. Joint meeting with Faculty Affairs about TopHat resolution – 30 minutes
 - ii. Follett Bookstore updates – Do we want an update? -- Brett
 - iii. Replacement FSCOT member on the Record and Retention Committee
 - 1. Action:
 - a. Maybe wait for new membership to decide unless there is a current member who wishes to fill
 - iv. Gartner Rep – Resources available for Faculty and Researchers – Gary
 - b. Decide if we will have a June 1 or June 15 meeting
 - c.
- 10.) Adjourn meeting—**Brett**

Attendance:

- Aryan Tayal, Student Representative
- Be Stoney, Education (18-22)
- Bill Zhang, Engineering (20-23)
- Bob Larson, Veterinary Medicine (18-21)
- Brett DePaola, Arts and Sciences (17-22) Co-Chair
- Colby Moorberg, Agriculture (20-22)
- Don Crawford, Architecture, Planning, and Design (20-22)
- Ignacio Ciampitti, Extension (20-22)
- Jason Maseberg-Tomlinson, General University (20-23)
 - Jim Bach, General University alternate (20-23)
- Lisa Shappee, Technology & Aviation K-State Polytechnic (15-21)
- Martin Seay, Health and Human Sciences (20-21)
- Michael Raine, Business Administration (07-20) Co-Chair
- Ryan Otto, K-State Libraries (17-20)

Non-voting Attendees:

- Gary Pratt, CIO
- Debbie Webb, Liaison for University Support Staff
- Scott Finkeldei, Liaison for Chief Information Officer

Guests:

- Shelley Griffin, Supervisor, Classroom Technology
-
-

Attachment # 1: PPM 3415 Information Security Plan

March 16, 2021

To: IT Policy Review Team

From: IT Communications Team

Re: First review of PPM 3415 **Gramm-Leach-Bliley Act Compliance Plan**

The following is a first review of PPM 3415 Gramm-Leach-Bliley Act Compliance Plan and comparison to policies from peer institutions. Auburn and Iowa State have policies/statements regarding Gramm-Leach-Bliley. Other universities embed security of financial information in privacy policies/notice (Clemson, Iowa State, Oregon State (2018)), compliance (NC State), data policies (Oklahoma State (2019), Univ. Massachusetts – Amherst, WSU) and security policies/programs (Colorado State (2019) and Iowa State). LSU provides a listing of data security laws.

We need further discussion about keeping the policy or including the information in larger IT Security Policy (see [Colorado State University: Information Technology Security](#)). There are at least nine policies at K-State related to IT security, which does not include PPM 3420 Information Technology Usage policy, PPM 3495 Collection, Use and Protection of Social Security Numbers, PPM 3433 Data Classification and Security and PPM 3436 Media Sanitization and Disposal Policy.

Units to be consulted on policy changes include (highlight means that group has been consulted):

- FSCOT
- Data Governance Group
- Office of Risk and Compliance
- IT Security
- Division of Financial Services
- HCS
- Business Intelligence, Analytics and Enterprise Applications Leadership Team
- Office of General Counsel

Table 1. Links to policies from peer and other institutions

Universities	Policies
K-State	Gramm Leach Bliley Compliance Plan - https://www.k-state.edu/policies/ppm/3400/3415.html (1/9/2012)
Auburn	Policy Regarding Privacy Rights/Gramm-Leach-Bliley https://sites.auburn.edu/admin/universitypolicies/Policies/PolicyRegardingPrivacyRightsGrammLeachBlileyAct.pdf

Clemson	Family Privacy Protection Act - https://www.clemson.edu/privacypolicy.html
Colorado State University	Information Technology Security - http://policylibrary.colostate.edu/policy.aspx?id=492 (6/5/2019) Information Collection and Personal Records Privacy - http://policylibrary.colostate.edu/policy.aspx?id=493 (2/10/2019)
Iowa State University	Electronic Privacy - https://www.policy.iastate.edu/electronicprivacy (11/8/2012) Financial Services Information Security Program https://iastate.servicenow.com/it?id=kb_article&sysparm_article=KB0011955&sys_kb_id=a29089201b006490a28e7445cc4bcb9f (10/22/2020)
Louisiana State University	Data Security Laws - https://www.lsu.edu/it_services/its_security/data-security-laws/index.php Security of Data https://www.lsu.edu/policies/ps/ps_6.20.pdf (5/20/2009)
North Carolina State University	Information Security Risk and Assurance (compliance with external requirements) - https://oit.ncsu.edu/about/units/sc/isra/programs/
Oklahoma State University	Data Stewardship – Data Classification policy, responsibilities and guidelines: https://adminfinance.okstate.edu/site-files/documents/policies/data-stewardship-data-classification-policy-responsibilities-and-guidelines.pdf (10/2019) NOTE: See chart in the policy on managing data. State and Federal Regulations - https://it.okstate.edu/policies-procedures-and-guidelines/index.html
Oregon State University	None found referencing Gramm-Leach-Bliley – Privacy Notice - https://uit.oregonstate.edu/ois/privacy-notice-oregon-state-university (7/20/2018)
University of Massachusetts - Amherst	Data classification (Gramm Leach Bliley mentioned) - https://www.umass.edu/it/support/security/data-classification-umass-amherst
Washington State University	WSU Guideline Cloud Computing - https://its.wsu.edu/documents/2018/06/wsu-cloud-computing-guideline.pdf/ (3/15/2017) University Data Policies - https://policies.wsu.edu/prf/index/manuals/executive-policy-manual-contents/ep8-university-data-policies/#Security (6/8/2020)

PPM 3415 Gramm-Leach-Bliley Act Compliance Plan

Chapter 3415

Revised January 9, 2012



Table of Contents

- [.010 Purpose](#)
- [.020 Scope](#)
- [.030 Effective Date](#)
- [.040 Authority](#)
- [.050 Policy](#)
- [.060 Definitions](#)
- [.070 Roles and Responsibilities](#)
- [.080 Information Security Program Elements](#)
- [.090 Related Laws, Regulations, or Policies](#)
- [.100 Questions/Waivers](#)



.010 Purpose

This compliance plan ("Plan") describes K-State's safeguards to protect non-public, financial-related personal information ("covered information") in accordance with the requirements of the Gramm-Leach-Bliley Act of 1999 (GLBA). The Safeguards Rule of the GLBA, as defined by the Federal Trade Commission (FTC), requires financial institutions, which the FTC explicitly indicated includes higher education institutions, to have an information security program to protect the confidentiality and integrity of personal information.

These safeguards are provided to:

1. Ensure the security and confidentiality of covered information.
2. Protect against anticipated threats or hazards to the security or integrity of such information.
3. Protect against unauthorized access to or use of covered information that could result in substantial harm or inconvenience to any customer.

This Information Security Plan also provides for mechanisms to:

1. Designate an employee or employees to coordinate the information security program.
2. Identify and assess the internal and external risks that may threaten covered information maintained by K-State.
3. Design and implement safeguards to control the identified risks.
4. Oversee service providers, including third party contractors, to ensure appropriate safeguards for covered information are maintained.
5. Periodically evaluate and adjust the information security program as circumstances change.

.020 Scope

This policy applies to all K-State colleges, departments, administrative units, affiliated organizations and third party contractors that create, access, store or manage covered information.

.030 Effective Date

Approved November 2004; revised November 2011.

.040 Authority

This plan responds to the Gramm-Leach-Bliley Act of 1999 that mandates protection of customer information, which for universities is primarily student financial information. See section [.060 Definitions](#) for a definition of information covered by this policy.

.050 Policy

The University will develop, implement and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards to protect covered information.

.060 Definitions

Covered Information

Information that K-State has obtained from a customer (e.g., a student) in the process of offering a financial product or service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

Information Security Program

The administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle covered information.

Service Providers

Any person or entity that receives, maintains, processes, or otherwise is permitted access to covered information through its direct provision of services to the University.

.070 Roles and Responsibilities

Chief Information Security Officer (CISO)

The CISO is responsible for coordinating and overseeing all elements of K-State's information security program. The CISO will work with appropriate personnel from other offices as needed (such as the Registrar's Office, Internal Audit, and the Division of Financial Services) to ensure protection of covered information.

.080 Information Security Program Elements

1. Risk Assessment

Under the oversight of the CISO, risk and privacy assessments are performed for all information systems that house or access covered information. These risk and privacy assessments shall address unauthorized access, use, disclosure, disruption, modification and/or destruction of information or the information system itself. Further, the assessments shall identify known potential threats, the likelihood of their occurrence and the magnitude of the impact of those threats should they occur.

Internal and external risks at K-State include, but are not limited to:

1. Unauthorized access of covered information by persons within or outside the University
2. Compromised system security as a result of human error, vulnerabilities, infection by malicious software, or unauthorized system access
3. Interception of data during transmission
4. Loss of data integrity
5. Physical loss of data in a disaster
6. Errors introduced into the system
7. Corruption of data or systems
8. Unauthorized access through hardcopy files or reports
9. Unauthorized disclosure of covered information through third parties

Risk and privacy assessments are used to determine the likelihood and magnitude of harm that could come to an information system, the affected individual(s), and ultimately the University itself in the event of a security breach. By determining the amount of risk that exists, the University shall determine how much of the risk should be mitigated and what controls should be used to achieve that mitigation.

Both risk and privacy assessments shall be performed prior to, or if not practical, immediately after acquisition of an information system (in the event that the information system is owned/operated by the University) or prior to initial establishment of service agreements (in the event that the information system is owned/operated by a third party on behalf of the University). Further, the risk and privacy assessments shall be reviewed and, where required, updated after three years or whenever a significant change is made to the information system, whichever comes first.

Risk assessment should include consideration of risks in each of the following operational areas, in accordance with the requirements of the GLBA:

10. **Employee training and management**

Prior to being granted access to covered information, new employees in positions that require access to covered information (e.g., position in the Division of Financial Services, Registrar, and Student Financial Assistance) will receive training on the importance of confidentiality of student records, student financial information, and other types of covered information, and the risks of not providing appropriate protection. Furthermore, all employees receive annual training in general information technology security. Training also covers controls and procedures to prevent employees from providing confidential information to an unauthorized individual through social engineering or improper disposal of documents that contain covered information. All training will be reviewed and, where needed, updated at least annually.

All new employees with access to covered information must pass a criminal background check as a condition of employment.

Each department responsible for maintaining covered information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

11. **Information systems**

Including network and software design, as well as information processing, storage, transmission, and disposal. See section [.090 Related Laws, Regulations, or Policies](#) for the policy framework that manages the risk related to information systems associated with covered information.

12. **Incident management**

Including detecting, preventing and responding to attacks, intrusions, or other systems failures. K-State's strategy for managing IT security incidents, including assessing risks, is described in the [IT Security Incident Reporting and Response Policy](#) and associated [IT Security Incident Management](#).

2. **Designing and Implementing Safeguards**

Safeguards are necessary to mitigate and control the risks identified through risk assessment. Furthermore, the effectiveness of safeguards' key controls, systems, and procedures should be regular tested to ensure continued protection of covered information. The policy framework for K-State's information security program that governs the design, implementation, and maintenance of these safeguards is provided in section [.090 Related Laws, Regulations, or Policies](#). Protection of covered information is explicitly encompassed by K-State's comprehensive information security program that protects all K-State information and technology assets, commensurate with size and complexity of the institution, the nature and scope of activities, and the sensitivity of information assets.

3. **Overseeing Service Providers**

In the process of choosing a service provider that will maintain or regularly access covered information, the selection and retention processes shall ensure the ability of the service provider to implement and maintain appropriate safeguards for covered information. Contracts with service providers may include the following provisions:

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

4. **Program Evaluation and Adjustment**

The CISO will periodically review and adjust the information security program as it relates to the GLBA requirements, with input from the University's Security Incident Response Team ([SIRT](#)) and relevant stakeholders. Program evaluation should be based on results of testing and monitoring of security safeguard effectiveness and reflect changes in technology and/or operations, evolving internal and external threats, and any other

circumstances that have a material impact on the information security program. The Office of General Counsel and the Chief Information Officer must review any recommended adjustments.

.090 Related Laws, Regulations, or Policies

- [Operations and Management Security Policy](#)
- [Collection, Use and Protection of Social Security Numbers](#)
- [Identity Theft Prevention per the Federal Trade Commission's Red Flag Rules](#)
- [System Development and Maintenance Security Policy](#)
- [Physical and Environmental Security Policy](#)
- [Access Controls Security Policy](#)
- [IT Security Incident Reporting and Response Policy](#)
- [IT Security Incident Management](#)
- [Data Classification and Security Policy](#)
- [Media Sanitization and Disposal Policy](#)

.100 Questions/Waivers

The [Chief Information Officer](#) is responsible for this plan. The CIO or designee must approve any exception to this plan. Questions relating to this plan should be directed to K-State's [Chief Information Security Officer](#).

Attachment # 2: PPM 3434 IT Security Incident Reporting and Response Policy

March 14, 2021

To: IT Policy Review Team

From: IT Communications Team

Re: PPM 3434 IT Security Incident Reporting and Response Policy

PPM 3434 IT Security Incident Reporting and Response Policy was reviewed and compared to policies from peer institutions (links provided below). In comparing peer institutions: separate policies were found for Auburn (2018), and Iowa State (2016). At Colorado State (2019) and the University of Massachusetts at Amherst (2018) the information is posted in the IT Security policy. At Oregon State the information is included in the data management policy (2017). LSU posted reporting information in the computer use policy (2016) and documents an abbreviated version of the response in the security of computing resources policy (2016). Universities that provide procedures and not policies are NC State (reporting and communication procedures), and Oklahoma State. WSU requires a login.

Why is this policy necessary? Could we use a KB article instead that is behind an eID/password to access how we respond to an incident. OR Put the reporting process in the KB.

Units to be consulted on the changes to the policy include (highlight means that group has been consulted):

- FSCOT
- Office of Risk and Compliance
- System Admins
- IT Security
- Office of General Counsel

Table 1. Links to policies from peer and other institutions

Universities	Policies
K-State	IT Security and Incident Reporting Policy – https://www.k-state.edu/policies/ppm/3400/3434.html (4/15/2009) KB14577 https://kstate.servicenow.com/it?id=kb_article&sys_id=c83bc4f1db7c6cd0047d3cae7c9619f9
Auburn	https://sites.auburn.edu/admin/universitypolicies/Policies/InformationSecurityIncidentReportingPolicy.pdf (9/10/2018) Information Security Incident Response Team - https://sites.auburn.edu/admin/oit/CyberSecurityCenter/Pages/isirt.aspx
Clemson	Security Incident Response - https://ccit.clemson.edu/services/security/incident-response/#
Colorado State University	Information Technology Security - http://policylibrary.colostate.edu/policy.aspx?id=492#responses (6/5/2019)
Iowa State University	IT Security Incident Reporting - https://www.policy.iastate.edu/sites/default/files/resources/111/IT%20Security%20Incident%20Reporting%202006-02-02%20SECURED.pdf (2/2/2006) IT Security https://www.policy.iastate.edu/policy/it/security/ (11/8/2012)

Louisiana State University	Reporting: Computer Users' Responsibilities - https://www.lsu.edu/policies/ps/ps_107.pdf (1/1/2016) Incident Response: Security of Computing Resources - https://www.lsu.edu/policies/ps/ps_114.pdf (1/1/2016) Data template - https://www.lsu.edu/it_services/its_security/files/item849.pdf
North Carolina State University	Reporting an IT Security Incident: https://oit.ncsu.edu/it-security/reporting/ Incident Communications Procedures: https://oit.ncsu.edu/it-security/incident-communications-procedures/
Oklahoma State University	Incident handling: https://it.okstate.edu/services/incident-handling/index.html General policy listing - https://it.okstate.edu/policies-procedures-and-guidelines/index.html
Oregon State University	University Data Management, Classification and Incident Response - https://policy.oregonstate.edu/UPSM/08-015_university_data_management_policy (6/27/2017)
University of Massachusetts - Amherst	Data Security Incidents: Prevention and Response Procedures at UMass Amherst https://www.umass.edu/it/security/incident-reporting Information Security - https://www.umass.edu/it/policies/informationsecuritypolicy (3/15/2018)
Washington State University	Welcome to Information Security Services - https://its.wsu.edu/information-security

Proposed Revisions: PPM 3434 IT Security Incident Reporting and Response Policy

Chapter 3434

Issued April 15, 2009



Table of Contents

- [.010 Purpose](#)
- [.020 Scope](#)
- [.030 Effective Date](#)
- [.040 Authority](#)
- [.050 Policy](#)
- [.060 Definitions](#)
- [.070 Roles and Responsibilities](#)
- [.080 Implementing Procedures](#)
- [.090 Related Laws, Regulations, or Policies](#)
- [.100 Questions/Waivers](#)



.010 Purpose

This policy governs the actions required for reporting or responding to security incidents involving K-State information and/or information technology resources to ensure effective and consistent reporting and handling of such events.

.020 Scope

This policy applies to all members of the University community, including students, personnel, units, and affiliates using University information technology resources or data.

.030 Effective Date

January 8, 2009

Revised 2021

.040 Authority

For major incidents, which include a breach of personal identity information (PII), Kansas Regents IT Council (RITC) policy requires escalation to the top administration on campus and prompt notification of the Board of Regents office. Likewise, Kansas Senate bill 196 that went into effect in January 2007 requires a prompt investigation and notification of potential victims in response to a security incident involving a breach of PII.

.050 Policy

All members of the University community are responsible for reporting known or suspected information or information technology security incidents. All security incidents at K-State must be promptly reported to K-State's Chief Information Security Officer (CISO) and other appropriate authority(ies) as outlined below in [Section .080: Implementing Procedures](#).

Incident response will be handled appropriately based on the type and severity of the incident in accordance with the Incident Response Summary Table below in [Section .080: B.2](#) and [K-State's IT Security Incident Management Procedures](#). Handling of security incidents involving confidential data will be overseen by an Executive Incident Management Team.

All individuals involved in investigating a security incident should maintain confidentiality, unless the Chief Information Officer authorizes information disclosure in advance.

.060 Definitions

Security incident

Any real or suspected event that may adversely affect the security of K-State information or the systems that process, store, or transmit that information. Examples include:

- Unauthorized access to data, especially confidential data like a person's name and social security number
- Computer infected with malware such as a worm, virus, Trojan Horse, or botnet

- Reconnaissance activities such as scanning the network for security vulnerabilities
- Denial of Service attack
- Web site defacement
- Violation of a K-State security policy
- Security weakness such as an un-patched vulnerability

Personal identity information (PII)

[K.S.A. § 21-6107: Crimes involving violations of personal rights](#) defines PII as including, but not limited to: an individual's name; date of birth; address; telephone number; driver's license number or card or nondriver's identification number or card; social security number or card; place of employment; employee identification numbers or other personal identification numbers or cards; mother's maiden name; birth, death or marriage certificates; electronic identification numbers; electronic signatures; and any financial number, or password that can be used to access a person's financial resources, including, but not limited to, checking or savings accounts, credit or debit card information, demand deposit or medical information. For K-State's purposes, PII also includes ones name in combination with a passport number.

.070 Roles and Responsibilities

1. The **incident manager** is responsible for managing the response to a security incident as defined in the incident response summary table in Section .080.B.2 below.
2. The **Executive Incident Management Team** oversees the handling of security incidents involving confidential data (e.g., personal identity information). This team has authority to make decisions related to the incident and to notify appropriate parties. The team consists of:
 - Senior administrator for the affected unit
 - Chief Information Officer
 - Chief Information Security Officer
 - Representative from the Office of General Counsel
 - Assistant Vice President for Media Relations
 - Others as needed (for example, K-State Police for criminal incidents)

.080 Implementing Procedures

1. Reporting Security incidents

Any member of the K-State community who suspects the occurrence of a security incident must report incidents through the following channels:

1. All suspected high severity events as defined in Section .080.B.1 below , including those involving possible breaches of personal identity information, must be reported directly to the [Chief Information Security Officer \(CISO\)](#) as quickly as possible by phone (preferred), email, or in person. If the CISO cannot be reached, contact the [Chief Information Officer \(CIO\)](#).
2. All other suspected incidents must also be reported to the CISO. These incidents may be first reported to departmental IT support personnel, the unit's [Security Incident Response Team \(SIRT\) representative](#), or the unit head who can then contact the CISO. Reports should be made by sending email to abuse@k-state.edu (preferred) or by notifying the CISO by phone, email, or in person.
3. For detailed information about reporting IT security incidents, see the [K-State IT Security Incident Management Procedures](#).

2. Responding to Security Incidents

1. Incident Severity

Incident response will be managed based on the level of severity of the incident. The level of severity is a measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response. Four levels of incident severity will be used to guide incident response: high, medium, low, and NA (Not Applicable).

1. High

The severity of a security incident will be considered "high " if any of the following conditions exist:

1. Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire institution is affected)

2. Poses a potential large financial risk or legal liability to the University
3. Threatens confidential data (for example, the compromise of a server that contains or names with social security numbers or credit card information)
4. Adversely impacts an enterprise system or service critical to the operation of a major portion of the university (for example, email, student information system, financial information system, human resources information system, learning management system, Internet service, or a major portion of the campus network)
5. Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.
6. Has a high probability of propagating to many other systems on campus and/or off campus and causing significant damage or disruption

2. Medium

The severity of a security incident will be considered "medium" if any of the following conditions exist:

1. Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building
2. Adversely impacts a non-critical enterprise system or service
3. Adversely impacts a departmental system or service, such as a departmental file server
4. Disrupts a building or departmental network
5. Has a moderate probability of propagating to other systems on campus and/or off campus and causing moderate damage or disruption

3. Low

Low severity incidents have the following characteristics:

1. Adversely impacts a very small number of systems or individuals
2. Disrupts a very small number of network devices or segments
3. Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate

4. NA (Not Applicable)

This is used for events reported as a suspected IT security incident but upon investigation of the suspicious activity, no evidence of a security incident is found.

2. Incident Response Summary Table

The following table summarizes the handling of IT security incidents based on incident severity, including response time, the responsible incident managers, and notification and reporting requirements. Detailed procedures for incident response and management are further defined in the K-State IT Security Incident Management Procedures.

Incident Severity	Characteristics (one or more condition present determines the severity)	Response Time	Incident Manager	Who to Notify	Post-Incident Report Required*
High	<ol style="list-style-type: none"> 1. Significant adverse impact on a large number of systems and/or people 2. Potential large financial risk or legal liability to the University 3. Threatens confidential data 	Immediate	Chief Information Security Officer or an Executive Incident Management Team	<ol style="list-style-type: none"> 1. Chief Information Security Officer 2. Chief Information Officer 3. Unit administrator (VP, Provost, Dean, etc.) 4. Unit head 	Yes

	<ul style="list-style-type: none"> 4. Adversely impacts a critical enterprise system or service 5. Significant and immediate threat to human safety 6. High probability of propagating to a large number of other systems on or off campus and causing significant disruption 			<ul style="list-style-type: none"> 5. SIRT representative 6. Departmental security contact 7. Technical support for affected device 8. If breach of PII, see K-State IT Security Incident Management Procedures for additional notification requirements 	
Medium	<ul style="list-style-type: none"> 1. Adversely impacts a moderate number of systems and/or people 2. Adversely impacts a non-critical enterprise system or service 3. Adversely impacts a departmental scale system or service 4. Disrupts a building or departmental network 5. Moderate risk of propagating and causing further disruption 	4 hours	Appointed by unit head	<ul style="list-style-type: none"> 1. Chief Information Security Officer 2. Unit head 3. SIRT representative 4. Departmental security contact 5. Technical support for affected device 	No, unless requested by the Chief Information Officer or other appropriate administrator
Low	<ul style="list-style-type: none"> 1. Adversely impacts a very small number of non-critical individual systems, services, or people 2. Disrupts a very small number of network devices or segments 3. Little risk of propagation and further disruption 	Next business day	Technical support for affected device	<ul style="list-style-type: none"> 1. Chief Information Security Officer 2. SIRT representative 3. Departmental security contact 	No
N/A	"Not Applicable" - used for suspicious activities which upon investigation are determined not to be an IT security incident.				

* See [K-State IT Security Incident Management Procedures](#) for details about the Post-Incident Report.

.090 Related Laws, Regulations, or Policies

1. [K-State IT Security Incident Management Procedures](#)
2. [K-State IT security team](#)
3. [K-State Security Incident Response Team \(SIRT\)](#)
4. [Kansas Regents IT Council \(RITC\) Security Incident Policy and Procedure \(PDF\)](#) – April 2005
5. [Enterprise IT Security Reporting Protocols \(PDF\)](#), State of Kansas IT Security Council, October 2007
6. [State of Kansas, ITEC Information Technology Policy 7230, Revision1: General Information Technology Enterprise Security Policy](#)
7. [K.S.A. § 21-6107: Crimes involving violations of personal rights](#)

.100 Questions/Waivers

The [Chief Information Officer](#) (CIO) is responsible for this policy. The CIO or designee must approve any exception to this policy or related procedures. Questions should be directed to the [Chief Information Security Officer](#).

Attachment # 3: PPM 3495 Collection, Use and Protection of Social Security Numbers

March 14, 2021

To: IT Policy Review Team

From: IT Communications Team

Re: PPM 3495 Collection, Use and Protection of Social Security Numbers

PPM 3495 Collection, Use and Protection of Social Security Numbers was reviewed and compared to policies from peer institutions (links provided below). Six of our peer institutions have a policy (Colorado State (2014), Iowa State (2019), LSU (2006), NC State (2005), Oklahoma State (2008) or statement (Oregon State) on the use of SSNs. Clemson and Oregon incorporate their use of SSN in a privacy statement. The University of Massachusetts at Amherst includes SSNs in the data classification policy. Auburn summarizes the use of the SSN in a data protection policy. WSU places their information on the use of SSNs in the data security policy. In summary, six out of the ten of our peer institutions have a policy or statement on the use of SSNs.

The first draft of proposed changes are below. There needs to be discussion about keeping the policy or including the information in larger statement regarding data security.

Units to be consulted on the changes to the policy include (highlight means that group has been consulted):

- FSCOT
- Data Governance Group
- Office of Risk and Compliance
- IT Security
- Division of Financial Services
- HCS
- Business Intelligence, Analytics and Enterprise Applications Leadership Team
- Office of General Counsel

Table 1. Links to policies from peer and other institutions

Universities	Policies
K-State	Collection, Use and Protection of Social Security Numbers - https://www.k-state.edu/policies/ppm/3400/3495.html (9/10/2010)
Auburn	Best practices for protecting data within the typical university office environment - https://www.auburn.edu/administration/oacp/ICQ-DataSecurity.php Sensitive Personally Identifying Information Protection Policy - https://sites.auburn.edu/admin/universypolicies/Policies/SensitivePersonallyIdentifyingInformationProtectionPolicy.pdf (1/30/2019)
Clemson	Family Privacy Protection Act Policy - https://www.clemson.edu/privacypolicy.html

Colorado State University	Social Security Numbers - http://policylibrary.colostate.edu/policy.aspx?id=544 (12/23/2014) Information Technology Security - http://policylibrary.colostate.edu/policy.aspx?id=492 (6/5/2019)
Iowa State University	Social Security Number Protection - https://www.policy.iastate.edu/policy/ssn#:~:text=Policy%20Statement&text=The%20university%20will%20discontinue%20the,limited%20as%20permitted%20by%20law.&text=Employees%20and%20students%20shall%20not,to%20unauthorized%20persons%20or%20entities . (5/1/2019)
Louisiana State University	Social Security Number Policy - https://www.lsu.edu/it_services/its_security/files/item603.pdf (7/13/2006)
North Carolina State University	Process for Requesting Access to Social Security Numbers - https://policies.ncsu.edu/regulation/reg-01-25-11/ (8/9/2005)
Oklahoma State University	Electronic Use of Social Security Numbers https://adminfinance.okstate.edu/site-files/documents/policies/electronic-use-of-social-security-numbers.pdf (7/2008)
Oregon State University	Student Records Right to Privacy - https://catalog.oregonstate.edu/grades-regulations-records/right-to-privacy/ Privacy notice - https://uit.oregonstate.edu/ois/privacy-notice-oregon-state-university Data classification by data element - https://uit.oregonstate.edu/ois/data-classification-data-element
University of Massachusetts - Amherst	Data classification (Social Security Number is mentioned) - https://www.umass.edu/it/support/security/data-classification-umass-amherst Information Security - https://www.umass.edu/it/policies/informationsecuritypolicy (3/15/2018)
Washington State University	University Data Policies - https://policies.wsu.edu/prf/index/manuals/executive-policy-manual-contents/ep8-university-data-policies/#Security (4/8/2020)

State Univ ersit y	Use of social security numbers on forms - https://policies.wsu.edu/prf/index/manuals/90-00-records/90-78-use-social-security-number-forms/
-----------------------------	---

Proposed Revisions - Collection, Use and Protection of Social Security Numbers

Chapter 3495

Revised September 2, 2010

Table of Contents

[.010 Purpose](#)

[.020 Scope](#)

[.030 Objectives](#)

[.040 Policy](#)

[.050 Implementation and Timeframe](#)

[.060 Legacy Data](#)

[.070 Related Laws, Regulations and Policies](#)

[.080 Questions](#)

Appendixes:

[.100 Appendix A](#)

[.110 Appendix B](#)

.010 Purpose

Kansas State University ("the University") is committed to protecting the privacy and confidentiality of personal information related to students, faculty, staff, and other individuals associated with the University. This policy governs the collection, storage, use, and disclosure of Social Security Numbers (SSNs) at the University, consistent with federal and state laws and regulations and the increasing need to protect personal identity data. This policy also authorizes the creation of alternative methods of identification that will reduce reliance on the SSN, allow for easy identification of a person for University transactions, and provide for linking an individual's personal information and records in various university information systems. Kansas State University acknowledges the assistance of the University of Maryland in preparation of this policy. Additional policies consulted include University of Minnesota, 3/17/2005; Georgia Southern University, undated; and Baylor University, undated.

.020 Scope

This policy applies to all university colleges, departments, administrative units, and affiliated organizations. For the purposes of this policy, affiliated organization refers to any organization associated with the University that uses university computer network resources to create, maintain, or store data to perform their business functions.

.030 Objectives

In issuing this policy, the University is guided by the following objectives.

1. Broader awareness of the confidential nature of the SSN and the risk of identity theft related to unauthorized disclosure.
2. Reduced collection of SSNs except where authorized by law.
3. Reduced use of the SSN in records and information systems, including display screens and printed reports.
4. Reduced electronic storage of SSNs to a minimum number of locations with the goal being one location when that is possible.
5. Consistent policies regarding the collection, storage, use, and disclosure of SSNs throughout the University.
6. Increased confidence by students, employees, and affiliates/guests that their SSNs are handled in a confidential manner.

.040 Policy

Use of the SSN as an identifier will be discontinued, except where authorized for employment, IRS reporting, federal student financial aid processing, state and federal reporting requirements, and a limited number of other business transactions. (See [Appendix A](#) below for a list of currently approved uses of the SSN.) While the SSN will continue to be collected and retained as authorized by law, it will not be used for routine identification or authentication purposes. A unique nine-digit university identification number called the Wildcat ID Number (WID)

will be permanently assigned to each individual associated with the University as a personal identifier alternative to the SSN. The WID will begin with an "8" to prevent confusion with an SSN. For computer access, individuals will also have a unique electronic identification (eID) to be used in combination with a password.

.050 Implementation and Timeframe

Traditionally, the University, like many universities, has used the SSN as a common "person" identifier and as the key to university records and information systems maintaining personal information. The University recognizes that many of its major systems use the SSN or the SSN as the Student ID Number as the primary key. Conversion of systems will take time and resources. The expectation is that there will be steady and purposeful movement away from dependency on the SSN. A multi-year plan will be developed in coordination with university entities for meeting the requirements of this policy. Appropriate interim measures may be developed until such time as the conversion to alternative personal identifiers is complete.

Implementing Requirements

1. Kansas State University prohibits the use of a person's SSN as a publicly visible identification number for University-related transactions, unless specifically required by law or business necessity.
2. Each member of the University community will be assigned a unique identification number that will not be the same as nor derived from the individual's SSN. This number is called the Wildcat ID Number (WID). The WID will be printed on University photo ID cards.
3. For computer access or sign-in purposes, University students, faculty, staff, and others will create an electronic identifier (eID) to be used in combination with a password. The eID will be used as the standard identifier for all computer resource authentication purposes.
4. SSNs will not be used for identification purposes unless required by law or internal university business necessity. For business processes that require an SSN, the last four digits of the SSN may be used to confirm the identity of an individual.
5. Academic records, such as grades, and other pieces of personal information will not be publicly posted or displayed with the SSN or any portion of the SSN.
6. Any University office that requests an SSN from an individual must indicate if it is voluntary or required. The request should include or be accompanied by a disclosure statement approved by the **University Data Administrator**. Disclosure statements should state under what authority and why the SSN is being requested, how the number will be used, and to whom it can be disclosed. Sample disclosure notifications for students, employees, and affiliates/guests are provided in [Appendix B](#).
7. An SSN can only be used for the purpose it was collected.
8. Systems developed or purchased **by** the University ~~after the effective date of this policy~~ shall comply with the provisions of this policy. Such systems will not collect SSNs, or display SSNs visually, whether on monitors, printed forms, hardcopy reports, or other system output, unless required by law or business necessity. See [Appendix A](#) for further information.
9. In the transition to one location for the SSN, university systems may use the SSN as a data element, but not as a key for access to databases. In exceptional circumstances, it may be necessary to use the SSN as an alternative search field. All such cases shall be approved by the **University Data Administrator**, who shall seek recommendations from the **Data Resource Stewards Committee**.
10. When a business process requires the SSN, it must be stored in a secure manner. The SSN shall not be stored on devices that are not secured (e.g., laptops, PDAs, CDs). Any transmission of data containing SSNs must be encrypted over any communication network. Encryption policy is specified in the [Information Technology Security Plan, section .040](#).
11. Any University department or office that collects and/or maintains an individual's SSN in either paper or electronic media must: 1) ensure that the number is stored in a secure and confidential environment; 2) eliminate using the number for any purpose except those specifically addressed in this policy; 3) **begin a steady and purposeful movement away from dependency on the SSN in performing its functions and processes**; 4) properly control and restrict access to SSNs to prevent unauthorized disclosure; and 5) properly erase or destroy the storage devices or printed documents that contain SSNs to ensure the information cannot be recovered or reconstructed.

.060 Legacy Data

The University recognizes that the SSN must be retained and used as a person identifier in information systems containing older "legacy" data pertaining to ex-students, ex-faculty or staff, or others formerly associated with the university. It is impractical to assign WID numbers to these individuals. In addition, SSNs will continue to be assigned as Student ID numbers to students and used in university mainframe applications until the implementation of the new student information system.

.070 Related Laws, Regulations and Policies

A variety of federal and state laws and regulations address the use of the SSN. These include the Privacy Act of 1974, the Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act (HIPAA), and Kansas Statutes Annotated, 76-768.

.080 Questions

The [Chief Information Officer](#) (CIO) is responsible for this policy.

.100 Appendix A: Approved Uses for Social Security Numbers (SSN)

Appendix A is considered to be part of this policy (Collection, Use, and Protection of Social Security Numbers, Chapter 3495).

The SSN is required for certain legal and business activities and to ensure the accuracy of inter-institutional data exchanges and communications between institutions involved in those activities. Approved uses of the SSN by the University are listed below.

1. **Employment:** The SSN is required for a variety of employment matters; such as proof of citizenship, tax withholding, FICA, or Medicare.
2. **Application and Receipt of Financial Aid:** Students applying for student aid using the federal Free Application for Student Assistance (FAFSA) are required to provide SSNs. Students are also required to provide SSNs when applying for student education loans.
3. **Tuition Remission:** The SSN is required for state reporting of taxable tuition remission benefits received by employees, their spouses and dependents, and by graduate assistants.
4. **Benefits Administration:** The SSN is often required for verifying enrollment, processing, and reporting on various benefit programs, such as medical benefits, health insurance claims and veterans' programs.
5. **Insurance:** SSN will be needed to file insurance claims through Lafene Health Center.
6. **IRS Reporting:** The SSN is used for federally required reporting to the IRS. For example, the University reports the value of all taxable and non-taxable scholarships and grants awarded to non-resident aliens to the IRS.
7. **Student Information Exchange:** Many institutions, including postsecondary educational institutions, use the SSN as a student identifier. The SSN may be used for the exchange of information from student academic records between appropriate institutions, including other colleges and universities or certification and licensure programs.

.110 Appendix B: Sample Disclosure Statements

1. Student Notification - Voluntary SSN Disclosure
(optional) Solicited per K.S.A. 76-725. Used as a student identifier for records and accounts. Required if applying for federal or state financial aid (using FAFSA) and/or educational tax credit/incentives.
2. Employee Notification - Required SSN Disclosure
(mandatory) Solicited per K.S.A. 76-725. Used for tax withholding, record keeping, and government reporting.
3. Affiliates Notification - Voluntary SSN Disclosure
(optional) Solicited per K.S.A. 76-725. Used as an identifier and for record keeping.

Attachment # 4: SGA Resolution on Zoom CC and Live Transcriptions Labs

CERTIFIED LEGISLATION • CERTIFIED LEGISLATION • CERTIFIED LEGISLATION • CERTIFIED LEGISLATION

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45

RESOLUTION 20/21/59

**RESOLUTION FOR ACCESSIBILITY VIA
CLOSED CAPTIONING ON "ZOOM"
COMMUNICATIONS**

BY: Payton Lynn, Nick Saia, and Natalia Rodriguez

WHEREAS, The Kansas State University Accessibility Statement reads that "Kansas State University is committed to making its electronic and information technologies accessible to all individuals, including those with disabilities;"

WHEREAS, An online or hybrid modality is used for some courses, organizations, and events that are offered during the 2020-2021 academic year;

WHEREAS, The video communication platform Zoom is used for many courses' lessons and other university-related meetings;

WHEREAS, Zoom provides an option for meeting hosts to enable closed captioning and live transcriptions for meetings hosted on the platform;

WHEREAS, K-State students, staff, and faculty each have the option to enable this setting for all meetings they host via Zoom; and

WHEREAS, Students who are deaf, hard-of-hearing, have auditory-processing difficulties, or have trouble hearing and understanding others on internet-based communication would greatly benefit from having a live transcription of their meetings or classes.

BE IT RESOLVED THAT:


SECTION 1. In order to uphold its commitment to accessibility, the Kansas State University Student Governing Association requests that closed captioning and live transcriptions should be enabled on Zoom for all K-State classes and university-affiliated events or meetings.

SECTION 2. Upon passage by the Student Senate and Signature of the Student Body President, a copy of this resolution shall be sent to Vice President for Student Life and Dean of Students Thomas Lane; College of Agriculture Dean and Director of K-State Research and Extension Ernie Minton; College of Architecture, Planning and Design Dean Tim de Noble; College of Arts and Sciences Dean Amit Chakrabarti; College of Business Administration Dean Kevin Gwinner; College of Education Dean Debbie Mercer; Carl R. Ice College of Engineering Dean Matthew O'Keefe; College of Health and Human Sciences Dean John Buckwalter; College of Veterinary Medicine Dean Bonnie Rush; Vice Provost for Graduate Education and Dean of the Graduate School Claudia Petrescu; Information Technology Services Chief Information Officer Gary Pratt; University Provost Charles Taber; and University President Richard B. Myers.

RESOLUTION 20/21/59 WAS APPROVED 45-0-0 ON MARCH 18TH, 2021.

I certify this resolution is true and correct

I hereby approve this resolution.


Nathan Bothwell, Speaker of the Student Senate Date 3/24/2021




Tel Wittmer, Student Body President Date 03/26/2021