FSCOT Agenda
March 2, 2021, 3:30 pm

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**

4.) Committee Reports:

   a. Extended IT Leadership Group – **Brett & Michael**

      i. No Report

   b. IT Policy Review Team – **Don Crawford**, Information Technology Manager, Architecture, Planning & Design, FSCOT Member

      i. Attachment # 1 (page #5) PPM 3433 Data Classification and Security Policy (First Reading)

         1. https://ksuemailprod.sharepoint.com/:w:/s/fscot/EdDRXz5iZthEqJf0YbWQ8BgBHds2wjMqOHyWFsOIUkDetg?e=Wn9Rgb

         2. Action Needed:

            a. Approve or send back more feedback

      ii. Attachment # 2 (page #29) PPM 3470 Technologically Enhanced Classrooms:

         1. https://ksuemailprod.sharepoint.com/:w:/s/fscot/Ea-oMcD-11BDjyRdWp5v_kMBRgZDM6ldMMG12zvHABZ2jg?e=Q4ZGlG

         2. Action Needed:

            a. Approve or send back more feedback

      iii. Attachment # 3 (page #33) PPM 3475 Video Conferencing Policy:

         1. https://ksuemailprod.sharepoint.com/:w:/s/fscot/ESh2KpmxRRpOs-6dZWDaxlMBsHcTQfVixxFAnqYqX9QOZA?e=VBBPXI

         2. Action Needed:

            a. Approve or send back more feedback

   c. Office 365 Governance Group – **Michael**

      i. No Report

d. Project Governance Group – **Brett**

i.

e. Record and Retention Committee – **Lisa Shappee**, Library Director/Associate Professor, K-State Polytechnic, FSCOT Member, and **Ryan Leimkuehler**, CA, DAS, University Records Manager, Assistant Professor Morse Department of Special Collections, Kansas State University Libraries

i. See Attachment # 4 (page #38): Use of University Mobile Devices, Personal Devices, and Accounts

1. https://ksuemailprod.sharepoint.com/:w:/s/fscot/EUkHg3jqFtJKqrDSHfe6RK8BnYUPQ2HnVQagXG3aAeWEig?e=oSksrh

2. Action Needed:

a. Approve or send back more feedback

ii. See Attachment # 5 (page #41): PPM 3090 University Data Storage Guidelines

1. https://ksuemailprod.sharepoint.com/:w:/s/fscot/EaxRs8BzXyZOgAOCPDGuXVoBW5d7UYpgAthtHyWCh8b94Q?e=7sYqSb

2. Action Needed:

a. Approve or send back more feedback

iii. See Attachment # 6 (page #45): PPM 3455 University Email Policy

1. https://ksuemailprod.sharepoint.com/:w:/s/fscot/EaxRs8BzXyZOgAOCPDGuXVoBW5d7UYpgAthtHyWCh8b94Q?e=7sYqSb

2. Action Needed:

a. Approve or send back more feedback

f. University Network Infrastructure Refresh Project – **Michael**

i. No Report

5.) Old Business (Business from Previous Meetings)

a.

6.) New Business

a.

7.) Other Items – **Group**

8.) Adjourn meeting—**Brett**

Future Meetings and Agenda:

- March 16
    - Future, Post COVID, Academic Technology Discussion – Don Saucier, Associate Director, Teaching and Learning Center

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:

- □ Mr. Chad Currier, IT Chief Operations Officer/Deputy CIO for Enterprise Technology, Chief Security Officer
- □ Mr. Ryan Leimkuehler, University Records Manager, University Archives

Attachment # 1:

December 9, 2020

To: Consultant groups

From: IT Policy Review team

Re: PPM 3433 Data Classification and Security Policy

The IT Policy Review Team reviewed PPM 3433 Data Classification and Security Policy and are recommending the changes provided in the proposed revisions. Changes included moving the data protection standards to a knowledge base article, updating roles and responsibilities and governance groups to reflect current nomenclature, updating the data protection standards, changing the name to the Institutional Data and Security policy and verifying the accuracy of all URLs.

The original policy and policy with markup is available below. The draft with limited markup is available here.

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
- Registrar
- HCS
- Business Intelligence, Analytics and Enterprise Applications Leadership Team
- Office of Student Life
- Office of General Counsel
- VP Student Success

The policy team is requesting general comments on the policy as opposed to wordsmithing. Table 1 provides a listing of policies from other universities that were reviewed. Table 2 includes a comparison of the data classification categories. Since the protection standards are more procedural in nature and subject to change, these have been posted in a knowledge base article.

We would appreciate your feedback using this form by February.

Table 1. Policies Reviewed from Other Universities

Universities/dates	URL
KU Jan 2009	Data Classification and Handling Policy - https://policy.ku.edu/IT/data-classification-handling Data Classification and Handling Procedures Guide https://policy.ku.edu/IT/data-classification-handling-procedures

(minor revisions to formatting 2014/2017)	
Auburn May 2018	https://sites.auburn.edu/admin/universitypolicies/Policies/DataClassificationPolicy.pdf
Bowling Green University	
Clemson Nov 2018	Data Classification - https://ccit.clemson.edu/cybersecurity/policy/data-classification/#:~:text=The%20University%2C%20in%20alignment%20with,%2C%20Internal%20Use%2C%20and%20Public.
Colorado State University June 2019	http://policylibrary.colostate.edu/policy.aspx?id=492
Indiana University July 2020	Institutional Data - https://kb.iu.edu/d/avqg
Iowa State University August 2015	Data Classification Policy Data Classification Standards and Guidance - https://www.policy.iastate.edu/policy/dataclassstdguid
NC State	Data Management Framework - https://oit.ncsu.edu/it-security/data-framework/
The Ohio State University 8/15/2014	Institutional Data - https://ocio.osu.edu/sites/default/files/assets/Policies/InstitutionalData.pdf
Stanford University May 2015	Risk based classifications - https://uit.stanford.edu/guide/riskclassifications Use low risk, moderate risk, high risk)
University of Wisconsin System	Information Security: Data Classification - https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification-and-protection/information-security-data-classification/ (Dec 2019)

	Information Security: Data Classification and Protection - https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification-and-protection/ (Dec 2019)
University of Wisconsin (Jan. 2016)	Data Classification - https://kb.wisc.edu/itpolicy/cio-data-classification-policy
Washington State University June 2020	Data Policies - https://policies.wsu.edu/prf/documents/2017/06/ep8-university-data-policies.pdf/

Table 2. Comparison of data classification categories used by other universities

University	Classification	Classification	Classification	Classification
K-State	Public	Internal	Confidential Restricted	Proprietary/Regulated
KU	Level 3 (public)	Level 2	Level 1/2	Level 1
Auburn	Public	Operational	Confidential	
Clemson	Public	Internal Use	Confidential	Restricted
Colorado State University	Public		Restricted	Private
Indiana	Public	University-internal	Restricted	Critical
Iowa State University	Low	Moderate	High	Restricted
Mississippi State University				
NC State (categorized by data element)				
Stanford	Low	Moderate	High	High

University of Wisconsin System	Low	Moderate	High	High
Univ of Wisconsin	Public	Internal	Sensitive	Restricted
Washington State Univ	Public	Internal	Confidential	Regulated

PROPOSED REVISIONS: Institutional Data ~~Classification~~ and Security Policy

Chapter 3433

~~**Issued August 24, 2009**~~

Table of Contents

.010 Purpose

Data and information are important assets of the university and must be classified into categories based on criticality and sensitivity ~~protected from loss of integrity, confidentiality, or availability.~~ Data will be handled in accordance with University Protection Standards in compliance with university policy and guidelines, Board of Regents policy, and state and federal laws and regulations.

.020 Scope

This policy defines classification for University data and provides guidance for classification. 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 information technology resources to create, access, store, or manage University Data to perform their business functions. It also applies to any third-party vendor creating, storing, or maintaining University Data per a contractual agreement.

.030 Effective Date

~~This policy became effective on~~ February 2, 2009

Issued August 24, 2009

Revised 2021

~~All new systems designed and implemented after September 1, 2009, must comply with the security standards in section .054 below. Data stewards must have a compliance plan for all systems with confidential data by January 1, 2011.~~

~~.040 Authority~~

~~The state of Kansas ITEC Information Technology Policy 8000 - Data Administration Program requires state agencies, including Regents' institutions, to "develop, implement, and maintain an Agency Data Administration Program" that incorporates data polices with appropriate security controls.~~

.0~~5~~40 Policy

~~All University Data must be classified according to the K-State Data Classification Schema and protected according to K-State Data Security Standards. This policy applies to data in all formats or media.~~ This policy documents requirements for the protection of Kansas State University's data from unauthorized exposure or access and for relinquishment of data when terminating relationship with the University. All institutional data is assigned a data classification level based on security, compliance, sensitivity, operational use and risk. Institutional data must be protected with security controls and access authorization mechanisms identified within K-State's data protection standards. The level of protection is based on the assigned data classification. Institutional data included, and is not limited to, information in paper, electronic, audio and visual formats.

.0~~5~~42 Data Classification ~~Schema~~

Data and information assets are classified according to the risks associated with data being stored or processed. Data with the highest risk need the greatest level of protection to prevent compromise; data with lower risk require proportionately less protection.

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

Data Classifications are as follows:

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

Examples: K-State's public web site, ~~directory information for students, faculty, and staff except for those who have requested non-disclosure (e.g., per the Family Educational Rights and Privacy Act (FERPA) for students~~), course descriptions, semester course schedules, press releases, etc.

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

Examples: financial accounting data that does not contain confidential information. departmental intranet, information technology transaction logs, employee ID number ("W0..."), student educational records, directory information for students, ~~faculty, and staff~~ employees ~~who have requested non-disclosure (e.g., per FERPA for students.~~

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

Examples: Social Security number, student ID number (if it is the same as the Social Security Number), credit card number, Personal identity information (PII) ~~as defined in 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 one's name in combination with a passport number,~~ Passport number, personnel records, medical records, authentication tokens (personal digital certificates, passwords, biometric data).

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

~~.054 Data Security Standards~~ (This section has moved to a KB article, see https://kstate.service-now.com/kb_view.do?sysparm_article=KB14613)

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

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

~~Security Control Category~~	**~~Data Classification~~**		
	~~Public~~	**~~Internal~~**	**~~Confidential~~**
~~Access Controls~~	~~No restriction for viewing. Authorization by Data Steward or designee required for modification; supervisor approval also required if not a self-service function.~~	~~Viewing and modification restricted to authorized individuals as needed for business-related roles.~~ ~~Data Steward or designee grants permission for access, plus approval from supervisor.~~	~~Viewing and modification restricted to authorized individuals as needed for business-related roles.~~ ~~Data Steward or designee grants permission for access, plus approval from supervisor.~~

		~~Authentication and authorization required for access~~	~~Authentication and authorization required for access.~~ ~~Confidentiality agreement required.~~
~~Copying/Printing (applies to both paper and electronic forms)~~	~~No restrictions.~~	~~Data should only be printed when there is a legitimate need.~~ ~~Copies must be limited to individuals with a need to know.~~ ~~Data should not be left unattended on a printer.~~	~~Data should only be printed when there is a legitimate need.~~ ~~Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement.~~ ~~Data should not be left unattended on a printer.~~ ~~Copies must be labeled "Confidential".~~
~~Network Security~~	~~May reside on a public network.~~ ~~Protection with a firewall recommended.~~ ~~IDS/IPS protection recommended.~~ ~~Protection only with router ACLs acceptable.~~	~~Protection with a network firewall required.~~ ~~IDS/IPS protection required.~~ ~~Protection with router ACLs optional.~~ ~~Servers hosting the data should not be visible to entire Internet.~~ ~~May be in a shared network server subnet with a common firewall ruleset for the set of servers.~~	~~Protection with a network firewall using "default deny" ruleset required.~~ ~~IDS/IPS protection required.~~ ~~Protection with router ACLs optional.~~ ~~Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets like the residence halls and guest wireless networks.~~ ~~Must have a firewall ruleset dedicated to the system.~~ ~~The firewall ruleset should be reviewed periodically by an external auditor.~~
~~System Security~~	~~Must follow general best practices for system management and security.~~	~~Must follow University-specific and OS-specific best practices for system~~	~~Must follow University-specific and OS-specific best practices for system~~

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

	~~Storage in a secure Data Center recommended.~~	~~Storage in a secure Data Center recommended.~~ ~~Should not store on an individual's workstation or a mobile device.~~	~~Storage in Secure Data Center required.~~ ~~Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption.~~ ~~Encryption on backup media required.~~ ~~AES Encryption required with 192-bit or longer key.~~ ~~Paper/hard copy: do not leave unattended where others may see it; store in a secure location.~~
~~Transmission~~	~~No restrictions.~~	~~No requirements~~	~~Encryption required (e.g., via SSL or secure file transfer protocols).~~ ~~Cannot transmit via email unless encrypted and secured with a digital signature.~~
~~Backup/Disaster Recovery~~	~~Backups required; daily backups recommended.~~	~~Daily backups required.~~ ~~Off-site storage recommended.~~	~~Daily backups required.~~ ~~Off-site storage in a secure location required.~~
~~Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper, etc.)~~	~~See K-State's "Draft Media Sanitization and Disposal Policy"~~ ~~Paper: no restrictions.~~	~~See K-State's "Draft Media Sanitization and Disposal Policy".~~ ~~Paper: See K-State's "Draft Media Sanitization and Disposal Policy".~~	~~See K-State's "Draft Media Sanitization and Disposal Policy".~~ ~~Paper: See K-State's "Draft Media Sanitization and Disposal Policy".~~
~~Training~~	~~General security awareness training recommended.~~ ~~System administration training recommended.~~	~~General security awareness training required.~~ ~~System administration training required.~~	~~General security awareness training required.~~ ~~System administration training required.~~

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

~~**Note:** The table above is adapted from the University of Missouri, Information Security, Data Classification System.~~

.0~~56~~43 Contracts with Third Parties

Contracts between the University and third parties involving University Data must include language requiring compliance with all applicable laws, regulations, and University policies related to data and information security; immediate notification of the University if University Data is used or disclosed in any manner other than allowed by the contract; and, to the extent practicable, mitigate any harmful effect of such use or disclosure. Technology Acquisition Review is required for new contracts and contract renewal. See KB 13631.

~~.060 Definitions~~

~~**ACL**~~

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

~~**Authentication**~~

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

~~**Authorization**~~

~~Granting access to resources only to those authorized to use them.~~

~~**Availability**~~

~~Ensures timely and reliable access to and use of information.~~

~~**Classified National Security Information**~~

~~Information that has been determined by the federal government to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. There are three classifications - confidential, secret, and top secret (see White House Press Release: Classified National Security Information).~~

~~**Confidentiality**~~

~~Preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.~~

~~Firewall~~

~~A specialized hardware and/or software system with stateful packet inspection that filters network traffic to control access to a resource, such as a database server, and thereby provide protection and enforce security policies. A router with ACLs is not considered a firewall for the purposes of this document.~~

~~IDS~~

~~Intrusion Detection System; a system that monitors network traffic to detect potential security intrusions. Normally, the suspected intrusions are logged and an alert generated to notify security or system administration personnel.~~

~~Integrity~~

~~Guards against improper modification or destruction of information, and ensures non-repudiation and authenticity.~~

~~IPS~~

~~Intrusion Prevention System; an IDS with the added ability to block malicious network traffic to prevent or stop a security event.~~

~~Local Network~~

~~Any segment of K-State's data network physically located on the Manhattan or Salina campus with an IP address starting with 129.130.X.X or an un-routable private IP address (e.g., 10.X.X.X).~~

~~Remote Access~~

~~Accessing any K-State's local network from any physical location outside the Manhattan or Salina campus. This includes access from off campus using K-State's VPN service.~~

~~Secure Data Center~~

~~A facility managed by full-time IT professionals for hosting computer, data storage, and/or network equipment with 24x7 auditable restricted access, environmental controls, power protection, and network firewall protection.~~

~~Secure Server~~

~~a computer that provides services to other computers, applications, or users; is running a server operating system; and is hardened according to relevant security standards, industry best practices, and K-State security policies.~~

~~Sensitivity~~

~~Indicates the required level of protection from unauthorized disclosure, modification, fraud, waste, or abuse due to potential adverse impact on an individual, group, institution, or affiliate. Adverse impact could be financial, legal, or on one's reputation or competitive position. The more sensitive the data, the greater the need to protect it.~~

~~University Data~~

~~Any data related to Kansas State University ("University") functions that are:~~

1. ~~Stored on University information technology systems.~~
2. ~~Maintained by K-State faculty staff, or students.~~
3. ~~Related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).~~

~~**VPN**~~

~~Virtual Private Network; a VPN provides a secure communication channel over the Internet that requires authentication to set up the channel and encrypts all traffic flowing through the channel.~~

.044 Records Management

Institutional data may reside in university records, be used to produce university records, or constitute university records. University records will be managed in accordance with the Retention of Records policy and the Records Retention Schedule.

.045 Data Destruction

To prevent unauthorized disclosure, institutional data must be properly disposed of using destruction methods that meet legal, regulatory and/or the University Records Retention schedule. K-State provides guidance for the secure destruction of institutional data. KB article in process for Media Sanitization and Disposal.

.046 Public Records

Release of records in response to a public records request must be made in accordance with the Kansas Open Records Act.

.047 Relinquishing Data

Data users are required to relinquish institutional data upon termination or as required by changes in their roles or relationship with the university, based on arrangements with their supervisor, data steward requirements, and/or requirements of Kansas State University.

.0~~7~~50 Roles and Responsibilities

~~Everyone with any level of access to University Data has responsibility for its security and is expected to observe requirements for privacy and confidentiality, comply with protection and control procedures, and accurately present the data in any type of reporting function.~~ All users authorized to access institutional data are obligated to appropriately use and effectively protect institutional data. The following roles have specific responsibilities for protecting and managing University Data and Data Collections.

1. ~~**Chief Data Steward** - Senior administrative officers of the university responsible for overseeing all information resources (e.g., the Provost and Vice Presidents).~~

Data Owner -

Responsibilities of the data owner are as follows:

- Assigns appropriate classifications to institutional data (public, internal, restricted, or proprietary).
- Ensures appropriate controls and protection are implemented for safeguarding the confidentiality, privacy, integrity and availability of institutional data.
- Establishes the appropriate use and data handling processes and procedures for operational and administrative management of institutional data.
- Establishes and approves appropriate authorization process for granting access to institutional data based on the appropriate level of access, need to know and applicable legal or regulatory requirements; and
- Accepts the information security and privacy risk to the University and individuals from business unit operations.

2. **Data Steward** - ~~Deans, associate vice presidents, and heads of academic, administrative, or affiliated units or their designees with responsibility for overseeing a collection (set) of University Data. They are in effect the owners of the data and therefore ultimately responsible for its proper handling and protection. Data Stewards are responsible for ensuring the proper classification of data and data collections under their control, granting data access permissions, appointing Data Managers for each University Data collection, making sure people in data-related roles are properly trained, and ensuring compliance with all relevant polices and security requirements for all data for which they have responsibility.~~

Data Stewards – designated university officials whose functional areas of responsibility include the origination of university data and have the responsibility for managing and maintaining data.

Responsibilities of the data steward are as follows:

- Identify and document systems containing institutional data within their area of responsibility
- Categorize university information within their area of responsibility according to University information security and privacy policies, standards, procedures and guidelines
- Understand and document how institutional data is generated, collected, stored, processed, transmitted, accessed, released, maintained and disposed of in the systems of record for which they are responsible
- Implement appropriate administrative, physical and technical safeguards to ensure the confidentiality, privacy, integrity, and availability of institutional data
- Review and approve requests for access to institutional data within their area of responsibility; and
- Ensure that business unit policies and procedures are consistent with University policies, standards and procedures.

Data Custodian – individuals authorized by the data steward(s) who have operational responsibility for the administration of the systems and devices that store, process, transmit, or provide access to institutional data.

Institutional and personal responsibilities of data custodians are as follows:

Data User – individuals with access to non-public institutional data to conduct university business.

Institutional and personal responsibilities of data users are as follows:

- Follow appropriate policies, standards, procedures and guidelines governing the use, security and privacy of institutional data; and
- Follow the Retention of Records Policy and Regular Retention Schedule
- Report suspected or actual vulnerabilities pertaining to the confidentiality, integrity, or availability of institutional data.

Data Governance Council

Responsibilities of the committee are as follows: (looking for charter).

Data Standards Committee

Responsibilities of the committee are as follows:

- Establish common definitions and understandings for most frequently used data
- Discuss and resolve certain complex issues related to data definition and structure
- Promote collaborations across units
- Maintain an open and regular communications among data managers and users
- Support the strategic directions set by the higher-level Data Governance Council

3. ~~**Data Stewards Council** - A group of Data Stewards appointed by the Chief Data Stewards and Chief Information Officer to maintain the data classification schema, define University Data collections, assign a Data Steward to each, and resolve data classification or ownership disputes.~~
4. ~~**Data Manager** - Individuals authorized by a Data Steward to provide operational management of a University Data collection. The Data Manager will maintain documentation pertaining to the data collection (including the list of those authorized to access the data and access audit trails where required), manage data access controls, and ensure security requirements are implemented and followed.~~
5. ~~**Data Processor** - Individuals authorized by the Data Steward or designee and enabled by the Data Manager to enter, modify, or delete University Data. Data Processors are accountable for the completeness, accuracy, and timeliness of data assigned to them.~~
6. ~~**Data Viewer** - Anyone in the university community with the capacity to access University Data but is not authorized to enter, modify, or delete it.~~

Chief Information Security Officer - Provides advice and guidance on information and information technology security policies and standards.

7. ~~**Internal Audit Office** - Performs audits for compliance with data classification and security policy and standards.~~

.060 Sanctions

Deliberate disregard of this policy or the protection standards, created to implement this policy is subject to disciplinary action, up to and including dismissal.

.0~~9~~70 Related Laws, Regulations, or Policies

Kansas State University Policies

Collection, Use, and Protection of Social Security Numbers

Retention of Records policy

Records Retention Schedule

University Research Compliance Office for information on export controls, confidential/sensitive research data, human subjects, etc.

Security for Information, Computing, and Network Resources

State of Kansas

K.S.A. § 21-6107: Crimes involving violations of personal rights

State of Kansas, ITEC Information Technology Security Standards 7320A. ~~These do not directly apply to K-State, but offer good guidelines for data security controls and represent minimum standards required of non-Regents state agencies.~~

State of Kansas, ITEC Information Technology Policy 8000: Data Administration Program

Federal Legislation and Guidelines

Family Educational Rights and Privacy Act of 1974 (FERPA)

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Gramm-Leach-Bliley Act (GLBA)

Electronic Communications Privacy Act of 1986 (ECPA)

Kansas Open Records Act

NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization

NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

~~NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations~~

NIST Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories

1. ~~Executive Order 12958: Classified National Security Information, As Amended, March 2003~~

Other

- Payment Card Industry Data Security Standard (PCI DSS)

.~~100~~080 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.

~~054 Data Security Standards~~ (Moved data protection standards to a knowledge base article, see https://kstate.service-now.com/kb_view.do?sysparm_article=KB14613

https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification-and-protection/information-security-data-protections/)

Data Protection Standards

The following table provides ~~required~~ the minimum data protection standards that must be met in managing data and data collections. Data security requirements for Proprietary Data are determined by the contracting agency and are therefore not included in the table below. Definitions for public, internal, and confidential data found in the Institutional Data and Security policy.

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

Security Control Category	**Data Classification**		
	Public (Minimal Risk)	**Internal (Moderate Risk)**	**Confidential (High Risk)**
Access Controls	• No restriction for viewing. • Access to view does not require authentication. ~~• Authorization by Data Steward or designee required for modification; supervisor approval also required if not a self-service function.~~ Access to modify data must use authentication methods and authorized by the data steward or designee.	~~•~~ Access to view~~ing and~~ or modify~~ication~~ restricted to authorized individuals ~~as needed for business-related roles.~~ And must be approved by Data Steward or designee ~~grants permission for access, plus approval from supervisor.~~ ~~• Authentication and authorization required for access~~ • Access requires authentication and authorization.	~~•~~ Access is limited to individuals who have been designated by the appropriate Data Steward or similar position. ~~Viewing and modification restricted to authorized individuals as needed for business-related roles.~~ ~~• Data Steward or designee grants permission for access, plus approval from supervisor.~~ • Access requires authentication and authorization.

			• Remote access by third party for technical support is limited to authenticated and authorized using secure protocols. ~~required for access.~~ • Multifactor authentication required. Confidentiality agreement established and disseminated to appropriate parties. Data must be encrypted in transit and at rest.
Copying/Printing/Transmission (applies to both paper and electronic forms)	• No ~~restrictions.~~minimum standards.	• ~~Data should only be printed when there is a legitimate need.~~ • ~~Copies must be limited to individuals with a need to know.~~ • ~~Data should not be left unattended on a printer.~~ • Data distribution limited to individuals whose role requires access and who have authorization to the data set.	• ~~Data should only be printed when there is a legitimate need.~~ • ~~Copies~~ Data distribution must be limited to individuals authorized to access the data set and have signed a confidentiality agreement. • ~~Data~~ Hard copies should not be left unattended ~~on a printer.~~ • Copies must be labeled "Confidential".

		- Hard copies must not be left unattended.	- Data must be encrypted in transit and at rest.
Network Security	- May reside on a public network. - Protection with a firewall recommended. - IDS/IPS protection recommended. - Protection only with router ACLs acceptable. University of Wisconsin No minimum standards.	- ~~Protection with a network firewall required.~~ - ~~IDS/IPS protection required.~~ - ~~Protection with router ACLs optional.~~ - ~~Servers hosting the data should not be visible to entire Internet.~~ - ~~May be in a shared network server subnet with a common firewall ruleset for the set of servers.~~ - Defense in depth must be used, including two of the following controls: - 1. Network firewall protection, port restriction, protocol restriction or IP address Access Control Lists (ACL). - 2. Single factor authentication (user name and password).	- ~~Protection with a network firewall using "default deny" ruleset required.~~ - ~~IDS/IPS protection required.~~ - ~~Protection with router ACLs optional.~~ - ~~Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets like the residence halls and guest wireless networks.~~ - ~~Must have a firewall ruleset dedicated to the system.~~ - ~~The firewall ruleset should be reviewed periodically by an external auditor.~~ - In addition to the moderate controls, protection with a network firewall is required. Network access to a system or

		• 3. Comprehensive intrusion detection and intrusion prevention (advanced logging or all attempted access to network resources, or Advanced Threat Protection (ATP).	server hosting the data must be limited to the minimum necessary.
System Security	• ~~Must follow general best practices for system management and security.~~ • ~~Host-based software firewall recommended.~~ No minimum standards.	• ~~Must~~ Follow University-specific and ~~OS~~ operating system specific best practices for system management and security. • Host-based software firewall required. • Host-based software IDS/IPS recommended	• ~~Must~~ Follow University-specific and ~~OS-~~ operating system specific best practices for system management and security. • Host-based software firewall required. • Host-based software IDS/IPS recommended.
Virtual Environments	• May be hosted in a virtual server environment. • All other security controls apply to both the host and the guest virtual machines.	• May be hosted in a virtual server environment. • All other security controls apply to both the host and the guest virtual machines. • Should not share the same virtual host environment with guest virtual servers of other	• May be hosted in a virtual server environment. • All other security controls apply to both the host and the guest virtual machines. • Cannot share the same virtual host environment with guest virtual servers of other security classifications.

		security classifications.	
Physical Security	• ~~System must be locked or logged out when unattended.~~ • ~~Host-based software firewall recommended.~~ No minimum standards.	• System must be locked or logged out when unattended. • Hosted in a secure location required; a Secure Data Center is recommended. • Data masked from view to prevent unauthorized access. Hard copy files appropriately marked and stored in a secure location.	• System must be locked or logged out when unattended. • Hosted in a Secure Data Center required. • Physical access must be monitored, logged, and limited to authorized individuals 24x7.
Remote Access to systems hosting the data	• No minimum restrictions.	• Access restricted to local network or ~~general~~ K-State Virtual Private Network (VPN) service. • Remote access by third party for technical support limited to authenticated, temporary access via ~~direct dial-in modem or~~ secure protocols over the Internet.	• Restricted to local network or secure VPN group. • Unsupervised remote access by third party for technical support not allowed. Or Remote access by third party for technical support must be monitored. • Two-factor authentication recommended.
Data Storage	• Storage on a secure server recommended. • Storage in a secure Data Center recommended.	• ~~Storage on a secure server recommended.~~	• ~~Storage on a secure server required.~~

	• No minimum standards.	• ~~Storage in a secure Data Center recommended.~~ • ~~Should not store on an individual's workstation or a mobile device.~~ •	• ~~Storage in Secure Data Center required.~~ • ~~Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption.~~ • ~~Encryption on backup media required.~~ • ~~AES Encryption required with 192-bit or longer key.~~ • ~~Paper/hard copy: do not leave unattended where others may see it; store in a secure location.~~ Data stored in a provided cloud storage service or data center. If data is stored on work stations or mobile devices, encryption at rest is required. Hard copies must not be left unattended and must be stored in a secure location. All devices that access high risk data must be managed in an

			institution approved manner.
Transmission Include with Access or leave on its own?	• No restrictions.	• No requirements	• Encryption required (e.g., via SSL or secure file transfer protocols). • Cannot transmit via email unless encrypted and secured with a digital signature.
Backup/Disaster Recovery	• ~~Backups required; daily backups recommended.~~ • No minimum standard.	• ~~Daily backups required.~~ • ~~Off-site storage recommended.~~ • Regular backup required and recovery periodically tested. Backup media encrypted and stored in a secure location.	• ~~Daily backups required.~~ • ~~Off-site storage in a secure location required.~~ • Regular backup required and recovery periodically tested. Backup media encrypted and stored in a secure location.
Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper, etc.)	• See K-State's "~~Draft~~ Media Sanitization and Disposal Policy" • Paper: no restrictions.	• See K-State's "~~Draft~~ Media Sanitization and Disposal Policy". • Paper: See K-State's "~~Draft~~ Media Sanitization and Disposal Policy".	• See K-State's "~~Draft~~ Media Sanitization and Disposal Policy". • Paper: See K-State's "~~Draft~~ Media Sanitization and Disposal Policy".
Workstation and mobile devices	No minimum standards.	Password protection and an inactivity	Password protection and an inactivity

(includes personally-owned devices)		auto-lock required. Employees shall remove University data from their personally owned devices before the devices are discarded or replaced or before leaving employment with the University system.	auto-lock required. Employees shall remove University data from their personally owned devices before the devices are discarded or replaced or before leaving employment with the University system.
Training Does this even belong?	~~General~~ University security awareness training ~~recommended~~ required. System administration training recommended.	~~General~~ University security awareness training ~~recommended~~ required. System administration training required. Data security training required.	• ~~General~~ University security awareness training ~~recommended~~ required. • System administration training required. • System administrators hired after Sept. 1, 2008, must pass a criminal background check. • Data security training required. • Applicable policy and regulation training required.
~~Audit Schedule~~ ~~Does this belong~~	~~As needed~~	~~As needed~~	~~Annual~~

Attachment # 2:

December 21, 2020

To: Consultant groups

From: IT Policy Review team

Re: PPM 3470 Technology Enhanced Classrooms

The IT Policy Review Team reviewed PPM 3470 Technologically Enhanced Classrooms and are recommending the changes provided in the proposed revisions that begin on page 2. Changes include substituting "centrally-scheduled" for "technology enhanced", updating the equipment per classroom category, updating links, updating titles, etc., Units consulted on the revisions will include:

- FSCOT
- Classroom Planning Committee
- Office of the Registrar
- Vice President of University Operations, and
- CAPP

The policy team is requesting general comments on the policy as opposed to wordsmithing. Table 1 provides a listing of policies from other universities that were reviewed.

Post comments here. We would appreciate your feedback by Feb. 5.

Table 1. Policies Reviewed from other universities.

University	URL
Auburn	
Clemson	Technology Classroom (not a policy) - https://ccit.clemson.edu/services/teaching-learning/campus-technology/classroom-technology/
KU	Technology Classroom support (not a policy) https://technology.ku.edu/services/classroom-technology-support Room Reservations - https://registrar.ku.edu/room-reservations
Ohio University 2016	Classroom and Laboratory Scheduling - https://www.ohio.edu/policy/01-024?no_redirect=true
University of Georgia Jan 2018	Centralized Classroom and Event Scheduling - https://provost.uga.edu/policies/academic-affairs-policy-manual/3-04-policy-for-centralized-classroom-and-event-scheduling//

University of Texas March 2011	Minimum Classroom Computing Standards - https://it.utexas.edu/sites/default/files/minimum_classroom_computing_standards.pdf
University of Virginia	Classroom Policies - https://www2.virginia.edu/registrar/hbclasspolicies.html

PROPOSED REVISIONS: ~~Technologically Enhanced~~ Centrally-Scheduled Classrooms

Chapter 3470

Revised September 2, 2010; January 2021

Table of Contents

.010 Purpose

Kansas State University is committed to providing state-of-the art learning environments including ~~technologically-enhanced~~ centrally-scheduled classrooms for our faculty, staff and students.

.020 Scope

~~This policy applies to general use classrooms that have been converted to technology-enhanced classrooms and newly built technologically-enhanced classrooms that receive support from general university funding and are centrally-scheduled. View the General Use Classroom List (that notes the different types of technology classrooms).~~

This policy applies to centrally-scheduled classrooms that receive general university funding. View the Centrally Scheduled Classroom list.

.030 Policy

Common-core technology will be provided in classrooms where appropriate. Faculty needing technology enhancements beyond the common core must work with the K-State ~~Technology~~ Classroom Planning Committee to incorporate these technologies into the classrooms. Basic technology will be included in rooms where common and expanded technology options are not feasible or are cost prohibitive (see definitions below).

Scheduling of ~~technology~~ centrally-scheduled classrooms is subject to the provision of reasonable accommodations for qualified individuals with disabilities, as determined by the University through an individualized interactive process. The following order of priority defines how classes will be scheduled:

A. Priority will be given to classes requiring either the technology or the learning environment.

B. Preference will be given to provide for conditions such as use of artifacts that cannot legally be removed from specific buildings, equipment or other items that cannot be safely and/or reasonably moved, IT licensing restrictions, and other such constraints.

C. Within groupings of classes requiring the technology or learning environment, larger classes will have preference.

D. When classes from various departments have equivalent need for the room, those from the department with previous (historical) "scheduling priority" will be given preference.

All users of the technology in these classrooms must be trained. Personnel in the I~~nformation Technology Assistance Center (iTAC)~~, Division of Information Technology, or at K-State Olathe or K-State Polytechnic will provide the training. Keys to the consoles will be issued only to individuals who have completed the training.

To protect the classroom environment, the consumption of food in technology classrooms is discouraged. ~~All~~ Beverages must be in covered, spill-proof containers such as travel mugs or capped bottles. Instructors are responsible for ensuring that their students follow this policy.

.040 Definitions

Basic Technology Classrooms

Basic Technology Classrooms ~~have a place to plug a laptop~~ are equipped with a computer (with DVD drive), camera, and microphone and an LCD projector or other display device. Video, internet, and audio connections are provided. All cabling is dedicated to the in-room computer.

Common Technology Classrooms

Common Technology Classrooms are equipped with a camera, and microphone, an LCD projector or other display, computer (with DVD drive), sound system, document camera, and internet connection.

Expanded Technology Classrooms

Expanded Technology Classrooms include common technology equipment~~. which have additional capabilities that may include video conferencing equipment and/or video or audio capturing equipment.~~ In addition, these rooms have one or more of the following capabilities: enhanced video conferencing equipment, enhanced video or audio capturing equipment, or enhanced interactive technologies.

Studio Technology Classrooms

Studio Technology Classrooms are computing lab environments equipped with hardware and software that are unique to a discipline or related disciplines. All Studio Technology Classrooms have either Common or Expanded Technology, with the exception of Cardwell 221 & 222, which have no instructional AV equipment.

.050 Roles and Responsibilities

If a department or college purchases and installs equipment and/or software in a ~~general use~~ centrally-scheduled classroom, this equipment must meet or exceed standards established by the ~~Technology~~ Classroom Planning Committee. Any approved user having access to the room will be able to use the equipment. Hardware becomes the property of the university unless other agreements are in place.

Software that is used to display content to or used by students must meet the requirements outlined in Section F, Part 125 of the University Handbook: Course Accessibility Standards Policy.

Faculty needing software installed on the computers in these rooms must have a licensed copy of the software. A minimum of two months' leeway, prior to the beginning of a semester, is recommended ~~before software can be installed on a technology~~ to install software in a centrally scheduled~~-~~classroom ~~machine~~ computer or before any hardware is installed in the classroom. This timeframe is required to ensure that the added software or hardware is compatible with existing systems. More leeway may be needed for more complex systems.

.060 Implementing Procedures

Changes to the physical and technological infrastructure require lead time for planning, testing, renovation and other improvements. Faculty and departments who want to pursue incorporating technology into a ~~general use~~ centrally-scheduled classroom can complete the Technology Installation Request Form. The request will be placed in a priority list and maintained by the ~~Technology~~ Classroom Planning Committee.
Scheduling will be ~~done under the auspices of the Chief Information Officer, using centralized scheduling programs, whenever possible~~ managed by the Office of the Registrar. Only classes and K-State related events may be scheduled in these rooms, and any deviations shall be approved by the Vice President for University Operations. Requestors must use the ~~Facilities Building and Grounds Request Form.~~ ~~–~~Request for University Buildings and Grounds form .

~~When web training is used, a face-to-face certification of faculty by personnel from the Information Technology Assistance Center (ITAC), or at K-State Olathe or K-State Polytechnic is required.~~
Classrooms are checked ~~once a day~~ five days a week for functionality and environmental issues. ~~Each classroom will have a specified block of time once a week when the room is unavailable so that maintenance can be performed.~~ Classrooms are also evaluated on a regular schedule for major upgrading.

.070 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 Director ~~of the Information Technology Assistance Center (ITAC)~~ for Academic and Student Technology.

Attachment # 3:

December 21, 2020

To: IT Policy Review Team

From: IT Communications Team

Re: PPM 3475 Video Conferencing Policy

The Subject Matter Experts (SMEs) reviewed PPM 3475 Video Conferencing Policy and are recommending that the policy be retired. As per comments from the SMEs, video conferencing has changed since the policy was revised in 2010 from proprietary video conferencing equipment to a full range of technology offerings. With Zoom, Microsoft Teams, FaceTime, Webex, and other platforms being compatible with personal mobile devices to complex classroom systems, it would be difficult to write a policy requiring the use of certain types of video/web conferencing equipment.

The suggestion is to focus on the current software supported at K-State and direct users to IT Resources and Services and continue to update best practices. In the updated information, IT would include where to go for assistance with supported software and a link to the Technology Installation Request for assistance with the selection and installation of technology, including equipment to support modern video conferencing software. For security and compatibility purposes, links to security policies for keeping the video conferencing software, operating systems, browsers, and other software up-to-date and secure also would be included.

Table 1 provides a listing of policies from other universities that were reviewed. The majority of the universities do not have a video conferencing policy. The original and a proposed revision is provided below Table 1. A revised version without markup also is included.

Units to be consulted on this policy will include:

- Academic and Student Support Technology Services
- FSCOT
- Division of Communications and Marketing
- Purchasing
- Network and Telecommunications Services
- System Administrators

There is PPM 6310 https://www.k-state.edu/policies/ppm/6300/6310.html#telecom that lists ITS (NTS) as the contact for equipment acquisition. Should we expand to include video conferencing equipment?

".100 Telecommunications Equipment Acquisition

The acquisition of telecommunications hardware, services, software, supplies, etc. may require prior approval from Information Technology Services regardless of cost. Telecommunications equipment includes telephone, answering machines, radio equipment including base stations, mobile or portable units and pagers. Contact Information Technology Services, (785) 532-7001, for assistance."

Post comments here. We would appreciate your feedback by Feb. 5 .

Table 1. Policies Reviewed from Other Institutions

Universities/dates	URL
KU	Resource/service (not a policy) - https://technology.ku.edu/services/web-video-conferencing#:~:text=Zoom%20at%20KU%20allows%20for,systems%20(e.g.%2C%20Polycom).&text=Host%2FSchedule%20Meetings%20%E2%80%94%20A%20KU,required%20to%20host%2Fschedule%20meetings.
Auburn	None found
Clemson	Resource/service (not a policy) - https://ccit.clemson.edu/services/teaching-learning/video-conferencing/
Colorado State University	Resource/service (not a policy) - https://www.acns.colostate.edu/video-conferencing/
Indiana University	None found
Iowa State University	None found - https://www.policy.iastate.edu/policy/information-technology
NC State	None found - https://policies.ncsu.edu/category/information-technology/
Stanford University	None found – resource/service - https://uit.stanford.edu/videoconferencing/best-practices
Washington State University	None found – video conferencing services - https://its.wsu.edu/wsu-video-conferencing-services/

PROPOSED REVISIONS: Video Conference Policy

Chapter 3475

~~Revised September 2, 2010~~

Table of Contents

.010 Purpose

Provide guidance on the acquisition and deployment of video conferencing equipment ~~by all~~ for K-State units. Provide standards for acquisition and use to insure support services can be provided by the university.

.020 Scope

This policy applies to all users of existing K-State video conferencing services as well as individuals or units who desire to establish video conferencing capabilities regardless of physical location. Exceptions can only be granted by the Chief Information Officer (CIO).

All K-State information technology policies apply to the use of K-State video conferencing services, as do all other applicable K-State policies and procedures and all federal, state and local laws.

The K-State Video and Audio Conferencing Services will be the Single Point of Contact (SPOC) for all video services at Kansas State University. This unit will also serve as the SPOC for strategic initiatives for expansion of video services.

.030 Policy

Authority, Standards and Access

The ~~ITS~~ Division of Information Technology (IT) or designee is responsible for establishing and enforcing ~~all~~ video conferencing standards and any variation from these standards must be approved by the IT~~S~~. Acquisition of video conferencing devices should be compatible with the existing university video conferencing systems. Information on current university systems can be obtained from the Single Point Of Contact (SPOC) (or is available from?).

Units that acquire video conferencing equipment or systems including software that are not compatible with the university systems will do so with the understanding that these acquisitions will not be centrally supported.

Assistance for acquisition of video conferencing equipment can be obtained from the K-State Video and Audio Conferencing Services serving as the SPOC to coordinate with and refer to other providers of video conferencing services at K-State as applicable. Units are strongly encouraged to register video conferencing equipment/locations with the SPOC and indicate if the video site is available for general university use. Individual desktop units must meet standards, but are not required to register the video equipment.

K-State video conference providers will meet annually to review and provide recommendations to the IT~~S~~ on the video conferencing standards. Those providers include, but are not limited to, ~~Telecommunications, Educational Communications Center (ECC), Information Technology Assistance Center (iTAC), TELENET 2, K-State Research and Extension/Information and Educational Technology (KSRE/IET), Office of Mediated Education (OME) and the College of Technology and Aviation. The Director of TELENET 2 will be responsible for convening and facilitating the annual meeting and providing a report to the ITS.~~ Academic and Student Technology Services, Division of Communications and Marketing, K-State Olathe and K-State Polytechnic.

.040 Effective date

Revised September 2010

Revised 2021

.050 Exclusions

Scheduling of video conferencing systems is the responsibility of the organization that owns the video conferencing system. Assistance for scheduling ~~the university~~ video conferencing systems can be obtained from the SPOC.

~~.050 Definitions~~

~~Codec (Coder/DECoder)~~

~~Device to convert analog audio or video signals to digital for transmission and reconvert at the receiving site.~~

~~Desktop video conferencing~~

~~Video conferencing on a personal computer.~~

~~H.264~~

~~Video compression standard that brings higher quality with lower bandwidth.~~

~~H.320~~

~~A widely used video compression standard that allows a wide variety of video conferencing systems to communicate.~~

~~H.323~~

~~A set of protocols that facilitate multimedia communication over IP packets.~~

~~ISDN (Integrated Services Digital Network)~~

~~A set of transmission standards designed to ensure compatibility among digital telecommunications services, worldwide.~~

~~IP (Internet Protocol)~~

~~Videoconferencing: point-to-point or multipoint video conferencing over an IP connection.~~

~~Multipoint Bridge (Multipoint Control Unit)~~

~~A set of integrated software controlled data components that enable more than two video conferencing sites to participate in a video conference.~~

~~Multipoint video conferencing~~

~~Video conferencing in which more that two sites can participate.~~

~~Point-to-Point~~

~~Video conference or other transmission between two locations.~~

~~Room-based video~~

~~Video conferencing using a system appropriate for groups.~~

~~Single Point Of Contact (SPOC)~~

~~Initial contact for information and referral for video conferencing and related video services.~~

~~Video conferencing~~

~~Two-way, interactive audio and video connecting two or more locations.~~

~~Video streaming~~

~~As a component of interactive video conferencing is the transfer of the interactive synchronous video activity to a web-based location for asynchronous use on the Internet.~~

.060 See the Video Conferencing Services website for additional information, including providers, locations and contacts.

.070 Questions

Questions regarding this policy should be sent to the Chief Information Officer (CIO).

Attachment #4:

Use of University Mobile Devices, Personal Devices, and Accounts Policy Draft:

Policy Statement:

The purpose of this policy is to define the controls when using mobile devices. It mitigates the following risks:

- Loss or theft of mobile devices, including the data on them
- Compromise of protected information such as: CUI, FERPA, or KORA through observation by the public
- Introduction of viruses and malware to the network
- Damage to reputation

It is important that the controls set out in this policy are observed at all times in the use and transport of mobile devices.

Scope and Applicability

This policy applies to the University Community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the University's information assets, and protects the interest of the University, its customers, personnel, and business partners.

Policy

Mobile computing is an increasing part of everyday life, as devices become smaller and more powerful, the number and complexity of tasks that can be achieved away from the office grows. As the capabilities increase so, too, do the risks. Security controls that have evolved to protect the static desktop environment are easily bypassed when using a mobile device outside of the confines of a building.

Mobile devices include, but not limited to items such as:

- Laptops
- Notebooks
- Tablet devices
- Smart phones
- Smart watches

Unless specifically authorized, only mobile devices provided by Kansas State University may be used to hold or process University records. Use of personal devices may open the device/account to litigation in the case of a Kansas Open Records Request (See PPM 3060)

Note: Access vs. storage on personal devices – for example accessing and viewing records through a cell phone app or web browser such as Outlook client, OneDrive client, Microsoft Teams client, etc. would not be a violation of this policy as no data is actually 'living' on the device. Downloading/storing data and/or records to devices or unapproved systems would be a violation of this policy.

Risks, Liabilities, Disclaimers

Employees who elect to participate in the use of personal devices and accounts accept the following risks, liabilities, and disclaimers:

- At no time does the University accept liability for the maintenance, backup, or loss of data on a personal device. It is the responsibility of the equipment owner to backup all software and data to other appropriate backup storage systems before requesting assistance from IT. (see PPM 3090 and PPM 3433)

- Persons violating this policy may also be held personally liable for resulting damages and civil or criminal charges. Kansas State University will comply with any applicable laws regarding data loss or breach notification and may also refer suspected violations of applicable laws to appropriate law enforcement agencies.
- The University shall not be liable for the loss, theft, or damage of personal devices. This includes, but is not limited to, when the device is being used for University business, on University time, or during business travel.
- Kansas State University Information Technology reserves the right to implement technology such as mobile device management to enable the removal of Kansas State University owned data.
- Personal devices are not a University maintained space for storage and does open up personal accounts to review to determine whether those accounts contain documents subject to the Kansas Open Records Act.

If an employee is required to make use of mobile equipment, the employee is provided with an appropriate device which is configured to comply with the University's policies. Support provided by the IT Department may at times require access to the university issued device for problem resolution and maintenance purposes. Kansas State University has implemented security measures to protect its critical information during mobile device usages. The acceptable use policy for all university owned devices can be found: https://www.k-state.edu/policies/ppm/3400/3420.html.

Definitions

The following are the definitions relevant to the policy:

- Computing resources: All University information processing resources including all University owned, licensed, or managed computing services, hardware, software, and use of the University network via physical or wireless connection regardless of the ownership of the computer or device connected to the network.
- Institutional Data: All data owned or licensed by the University.
- University Community: Includes faculty, administrators, staff, student workers, graduate/technical assistants, alumni, interns, guests or agents of the administration, external individuals and organizations accessing University network services, and other authorized users.

Compliance

The University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. Instances of non-compliance must be presented and reviewed and approved by the Director of Information Security, or equivalent officer.

All breaches of information security, actual or suspected, must be reported to and investigated by the Director of Information Security, or equivalent officer.

Those who violate security policies, standards, or security procedures are subject to disciplinary action up to and including loss of computer access and appropriate disciplinary actions as determined by the University.

Related Policies, Standards, and Regulations:

- PPM 3030
- PPM 3060

- PPM 3090
- PPM 3420

Attachment # 5:

University Data Storage Guidelines

General Records Management Statement:

Kansas State University, as an agency of the State of Kansas, is governed by state statutes defining records retention requirements. State law provides that all government records are public property and shall not be destroyed or otherwise disposed of except as authorized by law or applicable retention and disposition schedules (see Kansas Statutes Annotated (K.S.A.) 45-403). The University Archives is designated as the official repository for the preservation of all Kansas State University non-current government records with enduring value. The University Archives also has responsibility for advising on the management of current records, primarily through the efforts of the University Records Manager. The University Records Manager serves as the liaison between the University Archives and Kansas State University offices to develop and maintain records retention and disposition schedules. The University Records Manager also provides training on records management topics and acts as an advisor on policies.

Retention of Records Policy: PPM 3090

Key Concepts to Keep in Mind:

Office 365 tools are acceptable repositories for retaining university records if they are deployed properly and actively managed, taking into consideration the following points:

- University records and information must be managed no matter where they are kept. Do not allow any system or repository to become a dumping ground for files.
- The University's records retention schedules must be applied to all university records regardless of where they are maintained no matter the format. Premature or otherwise inappropriate destruction of university records is unacceptable and violates State statute.
- When using Office 365 tools, access must be actively managed and reviewed on an ongoing basis. Updating access when changes to unit staffing occur is critical.
- DO NOT USE: Dropbox, Google Drive, etc. is not a University maintained space for storage and does open up personal accounts to review to determine whether those accounts contain documents subject to the Kansas Open Records Act.

Office 365 and University Data Storage Guidelines:

Chat/Instant Messaging: A private, synchronous exchange of messages between parties over a computer network. All messages should be short-term conversational communication. All policy or business function communication should be conducted through a more permanent medium such as email. (link to routine and policy correspondence) See also Data Classification and Security Policy 3433

Managed Network Drive Formerly Catfiles/W:Drive: This drive is for information that needs to be shared across the unit/organization.

- Depending on your unit or department this space may be limited or unavailable. Check with your IT administrator for specific guidance.

Y: Drive: These are created for each user and accessible only to the user. Types of files that could exist in this environment would be working documents/drafts, meeting notes, personnel records, etc.

- Depending on your unit or department this space may be limited or unavailable. Check with your IT administrator for specific guidance.

Microsoft Teams: Teams are cloud-based virtual workspaces that can be created by faculty and staff to facilitate collaborative work. Team sites can be made using a variety of Office 365 applications including Outlook, Teams, Yammer, and Planner. Team sites are intended to be accessed by a group of people who are working on a common project or task where rapid, remote, or simultaneous access is anticipated or desired.

When the project or task has been completed, the team site owners should determine which files, if any, are to be retained and transferred to longer term record storage or the University Archives. Once the files have been transferred, the owner should delete them from the Team site to prevent duplication and potential over-retention. ITS will keep a Team one year past the date it becomes dormant/inactive. Before a Team is deleted permanently, all archival/permanent/long term records will be migrated out of the Team structure to longer term storage or transfer to archives. [See KSU retention schedule website for guidance]

OneDrive: OneDrive is a cloud-based storage provided to individual faculty, staff, or departments/units to store university information and materials related to your work at Kansas State University. This space is not intended for personal, non-university-related files. If OneDrive is utilized users should implement a file and folder structure to ensure public records important to the University are stored in a way that makes it easy for long-term storage and retrieval, transfer to University archives, or permanent storage by the department or unit. ***Note*** OneDrive is a secure environment for storage of University records.

SharePoint Online Communication Sites: Communication sites when deployed and properly configured, are cloud-based repositories intended for storage and sharing of university records and information. Communication sites are intended to be accessed by a group of people who need the unit's documents and where rapid, remote, or simultaneous access is beneficial. Communication sites can act as a unit's long-term records repository for digital files because they are not subject to the same expiration rules as Team sites or OneDrive for Business document libraries, and they avoid creating silos of university information and records. Note that the university records with a final deposition of Archives need to be transferred to the Kansas State University Archives once their period of retention has been met; it is not appropriate to retain these files in your unit's records repository indefinitely.

Department Intranets: A computer network that is restricted to users within a specific organization, especially network services intended for disseminating information within the organization through the use of web technology. An intranet is distinguished from the internet, in that it is not generally accessible to the public. These areas can be used to store longer term records as they are more secure, but it should be noted this is not a preservation environment. Permanent or Archival records should be managed in a system that will check the authenticity, integrity, and accessibility of the record over time.

Department-Specific Record Systems: This could apply to a variety of vendor or homegrown systems used at the university. These record systems may be designed specifically for certain types of records such as financial, flight data, or research data. Plans should be in place to monitor and manage records in these environments and that the records are destroyed or transferred as appropriate for the system. Note that some systems create additional records that you may want to track and manage such as critical metadata associated with records in the system.

Email: **Email is a record**. Whenever an email message is sent in the course of University business that email becomes an official record of the University. Such records can be subject to disclosure in response to an open records request or subject to subpoena by courts. So it is important that you take care when sending emails for a business. [See Also PPM 3455]

In today's world, we all have multiple email accounts. Some are personal (such as Gmail, etc.), and some will be institutional (such as your KSU employee account). Always use your KSU employee email account for University business. Also, try to avoid using your KSU employee email account for personal communication; that is best for personal accounts.

If you use a non-KSU employee account to create, respond to, or store work-related information you are increasing the risk of causing an inadvertent privacy breach by using a non-authorized service provider. In addition, those emails are still subject to open records requests and subpoena so you run the risk that your own personal emails will be drawn into an open records request. For these reasons, it is important that you keep your personal and work-related correspondence separate.

Be sure to keep and file email records appropriately. Retain messages that are sent and received only if they relate to University business; all other messages can be treated as transitory and deleted. (See also Email Records Management FAQ)

- When retaining a series of replies or forwards, keep only the last message as long as the thread is complete and has not been changed in the course of the exchange.
- Make sure to retain information in the header regarding the sender, recipients, date and time; this helps preserve the context of the message.
- *Note* The email system is not a recordkeeping system. A recordkeeping system organizes records according to a file plan, provides shared access to those who need it, and applies retention and disposition rules. So, it is best practice to implement a file/folder structure for your email account.

Use of Personal Devices and Accounts Policy: [see attached document]

Glossary of Terms:

Long term: the length of time needed to retain a record to satisfy the minimum retention period of a record. Retention periods can range from one year to several decades.

Record:

1. A written or printed work of a legal or official nature that may be used as evidence or proof; a document.

2. Data or information that has been fixed on some medium; that has content, context, and structure; and that is used as an extension of human memory or to demonstrate accountability.

3. Data or information in a fixed form that is created or received in the course of individual or institutional activity and set aside (preserved) as evidence of that activity for future reference.

4. An instrument filed for public notice (constructive notice); see recordation.

5. Audiovisual Records: A phonograph record.

6. Computing: A collection of related data elements treated as a unit, such as the fields in a row in a database table.

7. Description: An entry describing a work in a catalog; a catalog record.

Retention schedule: A document that identifies and describes an organization's records, usually at the series level, and provides instructions for the disposition of records throughout their life cycle.

Short term: the length of time needed to retain a record to complete a task or project. Lasting from days to years.

Transitory record: a record that has little to no documentary or evidential value and that need not be set aside for future use. Examples of transitory records include correspondence that requires no administrative action, policy decision, or special handling; and non-record copies of quasi-official notices, such as memoranda, that are not used as the basis of an administrative or program action or decision.

Attachment # 6:

University Email Policy 3455

Kansas State University Email Policy

Every KSU employee is individually responsible for handling and maintaining records (including University email and other electronic records) in accordance with University policy and requirements. Emails are records which may contain evidence of official University actions, decisions, approvals, or transactions. Email is subject to statutes of the State of Kansas, KSA 45-401 through 45-414, which applies to the preservation and destruction of records.

Email Records FAQ

1: How Long Do I Keep Email Messages I Have Received and Sent?

Email You Can Delete

Most received and sent emails have a very transitory value. They have no administrative, legal, fiscal, or archival retention requirements and can therefore be deleted as soon as they have fulfilled their reference purpose. Examples of such email messages include:

- Preliminary drafts
- Routine replies/requests for information
- Emails sent as reference or for informational distribution
- Emails used to set-up or accept meetings
- Announcements
- Acknowledgements

Email You Must Keep

All other email messages, both sent and received, must be retained for a designated amount of time (retention period). Retention periods are listed on a Records Retention Schedule. The retention period is based on the content of each individual email.

Emails that contain the following types of information have specific retention periods:

- Policy and procedure directives
- Substantive decisions regarding matters of University business
- Legal, discipline, or audit issues
- Approvals for purchases, HR decisions, and other actions to be taken
- Financial records including invoices and receipts
- Final reports or recommendations
- Student advising files
- Documentation of departmental/office actions, decisions, operations and responsibilities

2: How Do I Delete My Email Messages?

Deleting an email is the first step toward eliminating information that does not require further retention.

Delete emails in your Inbox, Sent Mail, and other folders that are not required to be retained or have passed their retention periods.

If you save a message that is the last in a thread of emails, you may be inadvertently saving content that you do not want or need as part of the previous messages in the string. Try to save only the information that is pertinent to a subject and not parts of a string that are unrelated.

Each email system has its unique way of storing email. You need to know how your system works to ensure all email messages that should be deleted actually are deleted.

3: When Creating a Message, What Can I Do to Help Ensure It Will Be Properly Managed?

Do You Need It?

Before creating an email message, consider whether it needs to be created:

- Can other modes of communication be used more efficiently or effectively?
- Is it necessary to create and send “information only” emails?
- Could this information be shared on a collaborative workspace such as SharePoint or Slack?
- Is it necessary to CC all of the listed recipients?
- Do you need to reply? Avoid replying to messages you receive unless a reply is actually required.

Be Objective

Be objective in the content of your email. Remember that email is subject to public information requests and may be accessed during litigation or audits. Create each email as if it were being published on the front page of the local newspaper.

One Subject Per Message

Try to limit the content in each email message to one subject. If there are several unrelated subjects to discuss, send individual emails for each subject. The messages will be easier to track, find, use, and eventually delete.

Subject Line

It is important to be objective and accurate in choosing the subject heading. Subject lines should be clear, concise, and closely articulate the purpose or action requested in your email.

Stick to the Subject When Forwarding

When forwarding email, review the original subject line and ensure it applies to your response. Too often, people continue to use a string of email messages with the same subject line, even though the topic of the messages has changed. This makes it difficult to properly categorize email messages for deletion.

When replying or forwarding messages, you can choose to not include the original message. At the top of your email inbox click File > Options > Mail > Replies and Forwards to see options. (Outlook 2016)

4: What Do I Do with All My Email?

Once you open an email message, decide what you are going to do with it before you close it.

Delete It

Can the information be found elsewhere, such as on an internal/external website, collaborative web tool, or network drive? Is it a newsletter, acknowledgement, notification, or alert? Does the email request or provide routine information? All of these types of emails can be deleted as soon as you no longer need it for reference. For most KSU employees, 70-80% of emails meet these criteria and do not need to be kept beyond reference purpose.

Do It

If you can respond or take specific action in two minutes or less – do it. File it in a folder, respond, make a call, etc.

Delegate It

Email messages requesting information or an action are not always directed to the appropriate person. After reading a message, determine whether you need to respond to it or whether you should delegate it to someone who is better placed to respond to it.

Defer It

If a response or specific action will take more than two minutes of dedicated time – defer it. If you use Outlook, you have the ability to flag emails for follow-up, label them, and add them to your Tasks list. These tools can help you find them later so that you can determine whether action is still required.

File It

Create folders that are logically aligned with the way in which business is conducted for your office such as projects, transactions, standing meetings, budgets, and employees.

5: How Do I Manage the Email I Have to Keep?

Manage Emails by Folders

Email folder titles should be clear, concise, and relate directly to the emails that will reside in the folder. Once the project or function is completed, you may add the retention period to the folder title for easy future cleanup.

Create a folder for each project or standing meeting:

- Make a folder for each project and/or standing meeting and put all email related to this project into this single folder. Use your email client's search function to check both your inbox and sent mail folder for these emails. When the project is complete, note the date of the termination of the records retention period and retain the entire folder until that time.

Create a folder for specific functions or transactions:

- Create a folder for specific functions, transactions, or processes. For example, if you approve purchases for your office, you can create an Approvals folder for each fiscal year.

Use subfolders:

- Creating subfolders is a very useful way to easily find information. For example, a Budget Files folder can have subfolders named for each budget with which you work.

Create a folder for archival emails:

- Archive folders can be created for groups of emails related to the same topic or function that have been designated archival on the General Records Retention Schedule. Archival emails should be transferred to the University Archivist at the end of their retention period.

Separate Transitory Email

In order to keep your inbox clean, delete transitory messages as soon as you no longer need them for reference. Any transitory emails you may need to keep for a limited amount of time can be moved to a folder that is purged regularly.

Use Search and Sort Functions

Search and sort functions are useful for locating and grouping specific messages that have characteristics in common. You can search for emails to or from an individual, by date, subject, and keywords in the body.

To search in Outlook, click on the folder you would like to search, enter the search term in the search box and press Enter. Outlook’s search options also allow you to search all folders and include the Deleted Items folder in your search. You can access more options by clicking the Search tab at the top of your screen.

Don't Use Email - Collaborate Via the Web

Consider utilizing an online collaboration tool such as Microsoft Teams, Groups, or OneDrive for projects/meetings rather than using email. These tools compile all the information, written and received, by its users in one location. All notes, drafts, conversation, and meeting minutes may be stored on the tool. Remember that information stored on web collaboration tools are subject to public records requests, audits, and litigation and must be retained and later deleted as per an approved retention schedule.

6: What are My Responsibilities as a Manager?

If You Are a Manager:

- Schedule a quarterly or yearly records cleanup time for your office.
- Include records management responsibilities in your office's new employee checklist.
- Establish an office procedure for setting up email accounts that allows access to email by other(s) in the office in case of absence.
- Establish general email protocols which ensure that everyone in the office is managing their email in the same way.

When an Employee Separates from Employment:

In accordance with KSU policy, managers and/or administrators are responsible for managing records associated with separated employees - this includes email.

- The employee and their manager or administrator should develop a plan for determining which emails must be kept and which may be deleted.
- Email that must be kept should be transferred to another employee or stored in a centralized location, such a network drive or SharePoint site.

To allow time for the department to appropriately transfer ownership or dispose of the records, systems administrators must ensure that email and other electronic records associated with a separated employee are not automatically deleted until at least one year after separation.