FSCOT Agenda
September 21, 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.) Introductions – **Brett**

5.) Discuss taking minutes – **Brett**

6.) Committee Reports:

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

  b. IT Policy Review Team – **Don Crawford**, Information Technology Manager, Architecture, Planning & Design, FSCOT Member & **Chad Currier**, Division of IT, Chief Operations Officer, Deputy CIO for Enterprise Technology, Chief Information Security Officer

  c. Office 365 Governance Group – **Michael & Chad Currier**, Division of IT, Chief Operations Officer, Deputy CIO for Enterprise Technology, Chief Information Security Officer

    i. Teams Retention Policy – implementation date not yet determined

    ii. Attachment # 1 (page 5): Retention schedule for Microsoft Teams | IT News (k-state.edu)

  d. Project Governance Group – **Brett**

  e. Record and Retention Committee – **Brett**

    i. Replacement FSCOT member on the Record and Retention Committee

  f. University Network Infrastructure Refresh Project – **Michael & Chad Currier**, Division of IT, Chief Operations Officer, Deputy CIO for Enterprise Technology, Chief Information Security Officer

7.) Old Business (Business from Previous Meetings)

  a. Update on Academic Tools Committee – **Brett**

    i. Email from Lynn Carlin:

ii. We are hoping to have the committee charge completed by the end of the month. It is tied to some other work we are considering related to innovation as well. Unfortunately, we had two key staff members for our Office leave in August – Emily Lehning and Mandy Cole – and we are stretched right now with the beginning of the school year. That said, we should have something ready to go and share with you by the end of September.

b. Emeritus faculty to K-State technology resources – **Brett & Chad Currier**, Division of IT, Chief Operations Officer, Deputy CIO for Enterprise Technology, Chief Information Security Officer

i. What is the specific process

ii. Attachment # 2 (page 6): Review of Leaving K-State page: Leaving K-State: https://www.k-state.edu/it/leaving

iii. Attachment # 3 (page 8): eID with Extended Access form: https://kstate.service-now.com/it?id=sc_cat_item&sys_id=2c81ae271d483c00d31f875c04fc296f

8.) New Business

a. Password Lockout Policy Update – **Brett & Chad Currier**, Division of IT, Chief Operations Officer, Deputy CIO for Enterprise Technology, Chief Information Security Officer

b. Explain the Legislative Post Audit – **Michael & Chad Currier**, Division of IT, Chief Operations Officer, Deputy CIO for Enterprise Technology, Chief Information Security Officer

i. Kansas Legislative Division of Post Audit – Kansas State Auditors (kslpa.org)

ii. itec-7230a.pdf (ks.gov)

c. Security Technologies and Equipment Policy – **Michael & Chad Currier**, Division of IT, Chief Operations Officer, Deputy CIO for Enterprise Technology, Chief Information Security Officer

i. Attachment # 4 (page 9): Security Technologies and Equipment Policy

9.) Other Items – **Group**

10.) Future Meetings and Agenda – **Brett**

a. Generally scheduled for the first and third Tuesdays, 3:30 to 5:00 pm

b. Will generally keep first meeting but might cancel second meeting of the month if there is not enough business.

c. Next meeting: October 5

i. Open/Alternative Textbook Initiative

ii. TopHat Resolution

iii. Non-Technical Update on the Data Center

iv. Agenda requests?

11.) Adjourn meeting—**Brett**

Attendance:

- □ Brett DePaola, Arts and Sciences (17-22) Co-Chair
- □ Colby Moorberg, Agriculture (20-22)
- □ Don Crawford, Architecture, Planning, and Design (20-22)
- □ Jason Maseberg-Tomlinson, General University (20-23)
  - □ Jim Bach, General University alternate (20-23)
- □ Jennifer Wilson, Extension (21-22)
- □ Justin Thomason, Veterinary Medicine (21-24)
- □ Katherine Jones, Technology & Aviation K-State Polytechnic (21-24)
- □ Kevin Wanklyn, Engineering (21-23)
- □ Lisa Rubin, Education (21-22)
- □ Michael Raine, Business Administration (07-22) Co-Chair
- □ Nathan Vontz, Student Representative (21-22)
- □ Phil Vardiman, Health and Human Sciences (21-24)
- □ Ryan Otto, K-State Libraries (17-23)

Non-voting Attendees:

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

Guests:

- □ Chad Currier, Division of IT Chief Operations Officer, Deputy CIO for Enterprise Technology, Chief Information Security Officer.
- □

Attachment # 1:

https://blogs.k-state.edu/it-news/2020/08/07/retention-schedule-for-microsoft-teams/

Retention schedule for Microsoft Teams

Posted on August 7, 2020 by Information Technology

With the move to Microsoft Teams there have been questions about the length of time chats, messages, etc are retained. The records retention schedule for Teams is now available online and provided below. The schedule becomes effective Aug. 24.

The Microsoft Teams Message Retention Schedule

Function	**Timeframe**	**Description**
Person to person chat	30 Days	Chats between two or more parties. Chats over the retention time will be silently dropped.
Teams Channel Messages	365 Days*	Channel messages inside of Team sites. Conversations over the retention time will be silently dropped.
Recover Team Sites Timeouts	30 Days	The time from when a Team's site is deleted and when it can be safely recovered.
Video Calls	Not Saved	Recordings from video calls are not saved unless configured on a per-call basis.
Voice Calls	Not Saved	Recordings from voice calls are not saved unless configured on a per-call basis.

*Shorter retention can be set for individuals, offices, etc. upon request and approval by IT.

NOTE: Files shared in chat are stored in One Drive, however, as per the retention schedule, the links will no longer be available.

Posted in Data management, Microsoft Teams

Attachment # 2:

Leaving K-State: https://www.k-state/it/leaving

Leaving K-State

Leaving K-State? There are several tasks you will need to complete before leaving K-State, such as deleting unwanted mailing lists, and more. See the Student and Employee Checklists for more information.

Access to IT Resources

See below for more information about what each group retains and loses access to when leaving K-State:

Students who leave K-State

NOTE: Students must have taken a credit course.

Retain* access to:	**Lose access to:**
Email and calendar account eProfile Student records in KSIS Personnel records in HRIS Employee Self Service Lafene Health Center Patient Portal	Online library journals and databases Unix file system Canvas (1 year after leaving) OneDrive (1 year after leaving) Office Online web apps (1 year after leaving) Office ProPlus (1 year after leaving) Duo Two-Factor Authentication

* As long as the password is current and not compromised, the services associated with each role continues. However, continued access is subject to changes in university resources and policies.

Employees who leave K-State

Retain* access to:	**Lose access to:**
eProfile Personnel records in HRIS Employee Self Service Lafene Health Center Patient Portal	Online library journals and databases Unix file system OneDrive (240 days after leaving) Office 365 (email, forwarded email, MS Office suite, etc.) (240 days after leaving). Files stored on central file servers and Active Directory systems KSIS Canvas Duo Two-Factor Authentication Zoom (30 days after leaving)

* As long as the password is current and not compromised the services associated with each role continues. However, continued access is subject to changes in university resources and policies.

NOTES:

- At the request of the appropriate university administrator, and with the approval of the Chief Information Officer, email may be terminated immediately for cause. This requires a formal email or letter by the requesting administrator to the Chief Information Officer.
- Before leaving K-State, employees should share business-related files with their supervisor, as appropriate.
- Computers (desktop and laptop) are inventoried and owned at the unit level. The unit controls the reuse and disposal of the computer and should follow K-State's Media Sanitization and Disposal Policy (PPM 3436). The Division of Information Technology provides reuse and disposal service to units who do not have IT staff that provides this service. See the Computer Deployment Request form to request this service.
- **IMPORTANT:** See the University Retention Schedule for information about retention requirements for university documents and data.

Emeritus faculty and staff

Retain* access to:	**Lose access to:**
Email account MS Office Suite Office 365 apps, including OneDrive. NOTE: Access granted following completion of eID with extended access form by department representative on behalf of the faculty or staff member. Business reason must be given for access to be granted. Online library journals and databases from campus computers. Requests for remote access to continue research activities will be considered on an individual basis Canvas Zoom	KSIS Duo Two-Factor Authentication

* As long as the password is current and not compromised, the services associated with each role continues. However, continued access is subject to changes in university resources and policies.

Retirees

Retain* access to:	**Lose access to:**
Email account Online library journals and databases from campus computers. Requests for remote access to continue research activities will be considered on an individual basis Canvas Zoom	MS Office Suite Office 365 apps, including OneDrive (3 weeks after retirement date). NOTE: Access can be extended by having the department representative complete the eID with extended access form on behalf of the faculty or staff member. Business reason must be given for access to be granted. KSIS Duo Two-Factor Authentication

* As long as the password is current and not compromised, the services associated with each role continues. However, continued access is subject to changes in university resources and policies.

eID with Extended Access

Use this form to request extended access for eligible individuals affiliated with the university

Individuals who are affiliated with the university with a legitimate need for access to University IT resources in order to fulfill their obligations ... Show more

Information about person submitting request

Your K-State eID

Preview this record maraine

maraine

Your name:

Your phone number

Your unit name

Your unit head's email address

Information about the person(s) needing extended access

Enter or paste in the eID(s) needing special access or type "See attachment":

Extended access expiration date (maximum of 12 months from now):

Required -Extended access expiration date (maximum of 12 months from now):

○ At the end of the current semester (incomplete students only)

○ Specific date (general requests)

Relationship to K-State

Specific reason for extended access / Coursework being completed

Specific IT resources requested

□ Non IT Staff (cnsvpn)

□ Contractors (contractor-vpn)Contractor VPN is

□ IT Staff (ITS-vpn)

□ Email services

□ K-State Canvas access

□ University Computing Labs / Wireless Access

□ Library checkout

□ Remote (off-campus) library access

□ O365 Apps (OneDrive, Teams, etc)

□ Zoom access

□ Other IT Resources

Terms of Service

Terms of Service

□

I have read and understand the K-State eID Policy.

Add attachments

Delivery Time: 2 Days

Submit

Required information

Your unit nameYour name:Your unit head's email addressYour phone numberEnter or paste in the eID(s) needing special access or type "See attachment":Extended access expiration date (maximum of 12 months from now):Relationship to K-StateSpecific reason for extended access / Coursework being completed

Attachment # 4:

Security Technologies and Equipment Policy

Chapter XXXX (34?? Computing & Information Technology)

Issued September ??, 2021

Table of Contents

.010 Introduction

Access Controls are critical to providing convenient physical access to resources while maintaining security and control over those resources emphasizing personal safety.

Video surveillance improves the University's ability to ensure consistent and effective response to deter crime, enhance personal safety, protect property, and assist in police functions.

Panic Buttons are electronic devices designed to alert law enforcement in emergency situations where a threat to persons or property exists.

Scope

This policy establishes rules and guidelines for any University entity that intends to purchase, install and/or record or monitor controlled electronic access or other security devices to resources, services, or locations that are accessible to the university population, as well as video surveillance that meets the University's mission. This policy governs Security Credential Devices, Credential Readers, Control Hardware, Panic Button Systems, Access Control Systems, and Video Technology Systems. This ensures compatibility with current Division of Information Technology standards and consistent usage for all stakeholders.

This policy does not require that live video feeds be monitored 24 hours a day, seven days a week.

Definitions

Access Control System: A system consisting of electronic devices used to control or monitor access to university resources, services, or locations.

Control Hardware: Any electronic hardware used to connect and process data for credential readers such as door controllers, building controllers, network adapters, and Panel Interface Modules (PIMs).

Security Credential Device: A physical or virtual item (cards, mobile devices, fobs, etc.) used to gain access to a university-controlled resource, service, or location that are issued/assigned to individual university population or community members.

Security Credential Reader: An instrument used to scan, read, or sense a credential device.

Security Technology Governance Group: Work group that oversees the review and enforcement of this policy and procedures.

Local Owner: A designated individual who is responsible for assigning and removing access to a given resource, service, or location.

Panic Button System: Any kind of device, either hard-wired or wireless, along with required accompanying equipment installed with the intent of soliciting a law enforcement response in the event of an emergency. Departments can request panic buttons by submitting a service request through facilities.

Security Technology: Any Access Control System, Video Technology System, or Panic Button System.

University Partner: Any entity that is an external member of a university-sponsored partnership or outreach program that may access university-controlled resources, services, or locations.

University Community: Faculty, staff, and students.

University Server: Any server, regardless of physical location, that is part of any university network system infrastructure.

Video Technology: Any camera or camera equipment and/or accessories used to capture video – with or without audio – that is recorded, stored, and/or transmitted.

Video Technology System: A system consisting of electronic devices such as cameras, microphones, and recording systems, the data from which is transmitted, recorded, and/or controlled remotely via a direct or network connection, and which is designed or used for the purposes of electronic surveillance. This includes any monitoring or recording software.

.020 Policy

All University departments or units that utilize University servers and equipment, whether owned by Division of IT or individual departments/units, must use an approved Security Technology to ensure service continuity throughout all University campuses and operations. All equipment must meet technological standards as established by the Security Technology Governance Group. Only University-issued credential devices will be used for Access Control Systems. All Security Technology will be housed on University Servers and must meet the IT standards identified in PPM 3433, PPM 3480, and PPM 3310.

Replacement of existing systems and all new systems must be compatible with an approved vendor, available through Purchasing.

Any University employee who may review surveillance footage and/or service Video Technology Systems, or who may have access to Security Technology as part of their employment must receive training, including but not limited to technical, legal, and ethical guidelines and compliance with local, state, and federal law, including the Family Educational Rights and Privacy Act (FERPA). Access to, and review of, Security Technology or any information accessed from such systems shall be in compliance with applicable laws, regulations, and University policies.

Video acquired from approved Video Technology Systems may be used only for University-designated safety, security, and conduct-related issues. Improper use of this video may result in disciplinary action, up to and including termination of employment. Individuals found in violation may also be subject to civil and/or criminal liability.

Video Technology Systems may not be installed in any location as to expose private information or KSU intellectual property. Video Technology Systems installed in housing buildings must restrict views to protect the privacy of occupants and be limited to the interior and exterior common areas. Installation of equipment in private areas or the use of hidden cameras is allowed only under extenuating circumstances such as a criminal investigation of an on-going or threatening situation. Installation of the equipment must be approved by the University Police Chief or their designee in coordination with appropriate housing and Division of IT personnel.

All Video Technology Systems installed must be secured to prevent unauthorized tampering or duplication of video recordings.

Any University employees who manage Access Control systems will receive training as determined by the Governance Committee.

The Security Technology Governance Group will establish and maintain a list/roster of approved, authorized local owners. The process for determining who will be authorized local owners will be determined by the Governance Committee. Local owners will have the authority to assign and remove access to resources, services, and locations that the local owners have responsibility over. The only exception will be employee termination or student dismissal. University Police will have assigned access to all locations.

The K-State ID Center will have the authority and responsibility to issue credential devices to individual members of the university population and community. The credential device information will be shared with all established access control systems through an automated process. The assignment of building access will be the responsibility of the appropriate unit head.

Exemptions

This policy does not apply to the following uses of Video Technology or Video Technology Systems:

1. Video and audio recordings used for legitimate academic purposes, such as recording lectures or performances, experimental lab observation, and video conferencing, for example.
2. Video and audio recordings made pertaining to the operations of the Kansas Board of Regents Educational Communication Center (Dole Hall) and intercollegiate athletics.
3. Video and audio recordings made by law enforcement personnel for all tasks directly related to job duties, to include but not limited to body worn cameras and mobile video equipment. These uses are subject to University Police internal policies. All University law enforcement personnel must adhere to all University policies.
4. Video and audio recordings made for non-University purposes using Video Technology that is not owned or controlled by the University.

These uses, however, may still be subject to privacy and workplace laws. Compliance with applicable University policies regarding conduct, ethical behavior, and Information Technology usage is required. See Section .050 for related polices.

.030 Implementation

i. University Operations and Information Technology Services

The Vice President for University Operations and Chief Information Officer are responsible for consulting stakeholders, establishing a committee to develop consistent standards, and overseeing the implementation of this policy. All contracts and maintenance agreements must be approved by the Vice President for University Operations.

ii. Security Technology Governance Group

1. Security Technology Governance Group (STGG) will make recommendations to the Vice President for University Operations and the Chief Information Officer regarding policy and standard changes.
2. STGG will coordinate with Purchasing to maintain the current approved Security Technology vendors and technology standards lists.
3. STGG will review and recommend approval or denial of all requests forwarded from Division of IT for new and/or replacement Security Technology and related hardware that do not meet existing STGG standards.
4. The STGG will be comprised of 4 permanent positions and 2 at-large positions. The 4 permanent positions will be one person from each of the following areas: Information Technology, K-State ID Center, University Facilities, and University Police. The 2 at-large positions will be selected by The Vice President for University Operations and Chief Information Officer from other campus units for 2-year rotating terms.

iii. University Police

1. University Police staff will access video footage, surveillance equipment, and electronic access doors in coordination with responsible departments and agencies for safety, security, and misconduct-related purposes, including but not limited to crime prevention and investigations.

2. The University Police IT and Support Services Lieutenant will coordinate with the applicable open records custodian regarding all requests for video recordings possessed by University Police, including those requesting criminal investigation records as defined by K.S.A. 45-254.
3. University Police will provide facility security and camera placement recommendations upon request.

iv. University Departments and Units

1. University Departments and Units will own the Video Technology or Access Control Systems equipment and be responsible for consulting University Police where appropriate for camera placement, monitoring, and all videos obtained from the system. For Access Control Systems, Departments and Units will have the authority to assign and remove access to resources, services, and locations that the local owners have responsibility over.
2. Unless exempted by this policy, University entities will not install or modify any Security Technology or other electronic surveillance system without prior written approval from STGG
3. University Departments/Units must report to the University Police any incident where a Video Technology System records an activity that involves the commission of an unlawful act, injury to people, damage to property, violation of University policy, or any observed suspicious activity, immediately upon discovery of the recorded incident.
4. University Departments/Units must maintain video recordings a period of time consistent with PPM 3090 and must plan for adequate storage capacity. Video recordings must be maintained for longer if notified by University Police, another law enforcement agency with proper authority, or the Office of General Counsel. Video involved in active investigations will be retained by the investigating entity.
5. University Department/Unit heads must confirm that all new equipment has been STGC -approved, and that replacement equipment is compatible with the current approved vendors before purchasing the equipment.
6. University Departments/Units must conduct annual audits of authorized users and access levels for all Security Technology.

v. Division of Information Technology

1. Except as otherwise provided in this policy, Division of IT will be responsible for the approval of security technology if the established standards are met. The approval application is available online.
2. Division of IT is responsible for the approval and installation of network connections, data storage and servers. Any installation of cabling or wiring must be installed by Division of IT personnel or other authorized personnel and meet existing standards. This includes all new construction. Equipment that is not compliant with existing standards will not be supported by Division of IT and may be subject to removal at the direction of the Chief Information Officer or the Vice President for University Operations.
3. Division of IT will develop and maintain a registry of Security Technology on campus. All systems, including those that were implemented prior to this policy, must be registered

through the standard application process and may be reviewed to verify compatibility with approved standards and adherence to Division of IT policies. Division of IT will provide University Police access to registry.

4. Access to the servers and central IT facilities where servers are located shall be limited to Division of IT, Police IT, and other University personnel with proper clearance.
5. The physical and environmental security of any equipment and data must meet Division of IT guidelines as established in PPM 3438. Access authorization to data is defined under PPM 3435.

.040 Contracts

Vice President for University Operations may seek STGG's recommendations regarding standards, vendors, upgrades, and other changes to contracts. All contracts relating to Security Technology must have sufficient available financial resources (upfront one-time and recurring), must complete contract review under PPM 3070, and must be approved by the Vice President for University Operations. Failure to comply with these requirements may result in removal of the Security Technology.

.050 Related Policies and References

Security Technology Equipment Request/Application Form

Security Technologies and Equipment Standards

Telecommunications PPM 3310

Computing and Information Technology Policies PPM 3400

Public Safety Policies PPM 3700

University Handbook Section C: 161.1

Unclassified Employee Personnel Actions PPM 4650

University Support Staff Employee Personnel Actions PPM 4460

Disciplinary Action Procedures for University Support Staff PPM 4020

University Retention Schedules

.060 Questions

Questions regarding this policy are to be directed to the Vice President for University Operations at (785) 532-6226 or the Chief Information Officer at (785) 532-6520.