FSCOT Agenda
October 5, 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**

   a. Don minutes taker

3.) Approve agenda (additions) – **Brett**

4.) Approve minutes – **Brett**

   a. **Attachment # 1** (page 5): Minutes provide by Colby

5.) 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**

      i. Developing a working group on Teams Retention

      ii. Action:

         1. Determine what academic or administrative groups are affected?

         2. Clarify use of Teams, don't discourage use, but use correctly

   d. Project Governance Group – **Brett**

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

      i. Action:

         1. Designate replacement FSCOT member on the Record and Retention Committee

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

6.) Old Business (Business from Previous Meetings)

a. 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 # 2** (page 6): Security Technologies and Equipment Policy

   ii. Action:

      1. Feedback for Division of IT

b. Other Q&A from last meeting – **Brett & Chad Currier**, Division of IT, Chief Operations Officer, Deputy CIO for Enterprise Technology, Chief Information Security Officer

   i. 10-minute time limit

   ii. Action:

      1. Feedback for Division of IT

c. TopHat Resolution update and next action – **Brett** and **Ryan Otto**

   i. **Attachment # 3** (page 12): Resolution provided by Ryan

   ii. Action:

      1. Decide next steps

7.) New Business

a. Zoom retirees deprovision we are above 80% account utilization – **Brett** and **Scott Finkeldei**, Liaison for Chief Information Officer, Division of IT

   i. Failure to take the training results in eID deactivation

   ii. Action:

      1. Feedback for Division of IT

b. Cybersecurity Awareness Training for Faculty, Staff, and Student Employees – **Michael & Chad Currier**, Division of IT, Chief Operations Officer, Deputy CIO for Enterprise Technology, Chief Information Security Officer

   i. **Attachment # 4** (page 14): Copy of the email

   ii. Action:

      1. Awareness and communication about the training

8.) Other Items – **Group**

9.) 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 19

   d. Future Agenda Items

      i. Open/Alternative Textbook Initiative

      ii. Non-Technical Update on the Data Center

      iii. Classroom Updates

      iv. McGraw Hill Inclusive Access Program

      v. Agenda requests?

10.) 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:

FSCOT Meeting Minutes

September 21, 2021, 3:30 pm

The meeting was called to order by Brett and Michael

All attendees introduced themselves.

Members Attending: Brett DePaola, Colby Moorberg, Don Crawford, Jason Maseberg-Tomlinson, Justin Thomason, Katherine Jones, Kevin Wanklyn, Lisa Rubin, Michael Raine, Nathan Vontz, Phil Vardiman, Ryan Otto

Non-voting Attendees: Gary Pratt, Scott Finkeldei

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

The committee agreed that minute-taking duties will be performed on a rotating basis based on alphabetical order of first names, beginning with Colby Moorberg for this meeting.

The retention policy for MS Teams was discussed. The proposed retention policy is available at this link. A date for the beginning of implementation of this policy has not yet been determined. MS Teams is problematic from a records retention standpoint due to open records laws and other issues. Exemptions to this records retention policy are discouraged, but impacted people and units should contact Chad Currier or Gary Pratt to discuss alternatives to MS Teams for record retention and communication. Three separate examples of use cases from the committee were presented, outlining potential impacts of the retention policy. People should contact the IT Services Center to get help with file management and moving away from MS Teams. Chad Currier will meet with the help desk staff soon to provide them guidance for helping people get out of Teams.

The process for providing extended access to campus IT resources for emeritus faculty was discussed. Interested persons who are retiring and wish to retain extended access to IT resources must complete the Extended Access Form. Without completing that form, faculty will lose access to all resources except email.

Chad Currier updated the committee on the Legislative Post Audit, which is available here: Kansas Legislative Division of Post Audit – Kansas State Auditors (kslpa.org), along with the Password Lockout Policy. Kansas State University cannot comply with all regulations due to the nature of business that is performed at this university, such as problems with password resets every 90 days potentially causing havoc when students return to school in the fall without having logged into their accounts for over 90 days. In such cases where KSU could not comply with the regulation, policies defaulted to standards from the National Institute of Standards and Technology (NIST).

An update was provided on the creation of the “Academic Tools Committee”. The committee is expected to be created by the Provost’s Office by the end of September.

The meeting was adjourned.

The next meeting will be held on October 5, 2021.

Attachment # 2:

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.

Attachment # 3:

Resolution Addressing K-State IT Support for TopHat and Other Educational Learning Platforms

BY: FSCOT, Ryan Otto, Be Stoney

WHEREAS, The Kansas State University Faculty Senate Committee on Technology (FSCOT) was asked to seek input and render judgement on whether it would recommend to Kansas State University IT to downgrade, keep at current levels, or enhance contract terms and/or support levels with Tophatmonocle Corp regarding supporting the TopHat educational learning platform on K-State campuses.

WHEREAS, FSCOT supports academic freedom, where faculty are trusted to make decisions on how best to support the pedagogical goals of their courses;

WHEREAS, FSCOT recognizes the importance of Kansas State University's IT to create and sustain a technology environment on K-State campuses that supports faculty's exercise of academic freedom;

WHEREAS, FSCOT understands that educational learning platforms and ecosystems, like TopHat, can and do provide value, often in unique and significant ways, to faculty and students as faculty seek to drive course engagement, create, store and provide access to course content, and provide tools for student assessment;

WHEREAS, FSCOT recognizes the benefits of TopHat for the following reasons:

1. Cost: when students enroll with TopHat, the cost of is not based on per number of classes the students are enrolled, rather the students pay one price and may use the platform across multiple classes.
2. Students have consistent access to their grades, course content, and know which assignment they are missing through integration between the platform and Canvas.
3. Students can access TopHat on a variety of devices.
4. Through TopHat's assessment tools, it offers the opportunity for faculty to learn where students are lacking in learning the material, can ask questions for real time responses from students, and helps align course objectives with learning outcomes.
5. "One of the best engagement platforms used in the classroom. Students are engaged through questions that are written directly before/after the PowerPoint slide. As students respond to questions, the faculty receives real time responses/feedback (anonymously) what students are learning. As a faculty who used TopHat for the first time, I have observed how students are more engaged with class discussions versus the traditional textbook discussions." -Faculty testimonial on the benefits of TopHat.

WHEREAS, FSCOT recognizes the need for faculty to have readily available technology tools to aid in the taking of attendance and a response system to measure and drive engagement in their courses;

WHEREAS, Prices for college textbooks and academic journals have been rising dramatically because students, colleges, and universities are captive markets for those publishers. Captive markets result in higher prices and less diversity for consumers due to the fact the only choices that exist are to purchase what is available or to not purchase at all. Use of higher education learning platforms and content ecosystems, like TopHat, is an emerging area that threatens students, colleges, and universities with platform lock-in, and which may contribute to captive market environments in higher education. Leaning further into a captive market environment by institutionally supporting education learning platforms and content ecosystems exacerbates rather than lessens the underlying causes of the textbook affordability crisis;

WHEREAS, FSCOT recognizes the importance of being strategic in working to lowering costs incurred by K-State students through the course of their education. Institutionally supporting education learning platforms and

content ecosystems, especially supporting one platform over another, presents challenges to the goal of strategically working to lower costs to students;
WHEREAS, Digital content paid for by students such as required materials and readings for courses, accessed through an educational learning platform like TopHat is likely not owned by those student consumers, merely rented or licensed to them. In contrast, physical course materials and readings may be purchased and owned by a consumer, in perpetuity. Purchased, licensed digital content therefore provides less value to student consumers in certain circumstances;

BE IT RESOLVED THAT:
Section 1: FSCOT supports the Kansas State University Student Governing Association's (KSU SGA) resolution 19/20/63, Opposition to TopHat and Other Costly Educational Platforms.
Section 2: FSCOT encourages faculty, where possible and practical, to explore if free, low-cost, or already available technology tools could be used to replace or supplement more expensive tools that have comparable uses.
Section 3: FSCOT strongly encourages faculty who have employed free, low-cost, or already available technology tools to aid in the taking of attendance, provide student assessment, and/or drive engagement in their courses to engage with the Teaching & Learning Center and University IT to support knowledge sharing and to aid in the goal of driving down course related costs to students.
Section 4: FSCOT supports the freedom for faculty to use TopHat, or other educational learning platforms they deem useful, in support of the pedagogical goals of their courses.
Section 5: For those faculty who choose to use TopHat within their courses they are highly encouraged to do the following in order to maximize the tool's value to student users:

1. Take every effort to be trained in TopHat and to be effective users of the tool to its fullest extent.
2. Ensure TopHat's integration with K-State's learning management system, CANVAS, in transporting grades, attendance, and assignments for their courses.
3. Where warranted, consult with the Student Access Center and work to ensure content stored and delivered through the TopHat Platform meets required standards for accessibility.

Section 6: In support of those faculty who choose to use TopHat within their courses, FSCOT supports and requests University IT to engage in the following:

1. Where necessary and to a reasonable degree, dedicate resources and enter into agreements with appropriate parties to support training for interested faculty on how to use the TopHat platform.
2. Maintain the integration of K-State's LMS, Canvas, with the TopHat platform.
3. Maintain the same no-cost contract terms (active as of 2021-05-12) with Tophatmonocle Corp regarding support for the TopHat platform on the K-State campus. FSCOT recommends against enhancement of contract terms.

Section 7: The TopHat platform is one of many current and emerging educational technology tools used in K-State classrooms. FSCOT supports and encourages University IT, where possible and practical, to maintain a technology environment that supports faculty's exercise of academic freedom, exploration, and use of various educational technology tools which may meet the current and future needs of K-State faculty and students.
Section 8: Upon passage and signatures by FSCOT co-chairs and committee members, a copy of this resolution shall be sent to Faculty Senate,

Attachment # 4:

From: helpdesk
Sent: Monday, October 4, 2021 6:26 PM
To: Michael Raine <maraine@ksu.edu>
Subject: 2021 Cybersecurity Awareness Training

Hello Michael,

The Division of Information Technology delivers annual Cybersecurity Awareness Training for faculty, staff, and student employees.

Cybersecurity awareness training provides you with the knowledge to identify and prevent potential cybersecurity attacks. It is estimated that 95% of cybersecurity breaches are caused by human error. By increasing our knowledge and behavior, we can create a cyber secure culture at K-State and beyond.

This training is mandatory for all state agencies through the **State of Kansas ITEC Policy 7230 – Information Technology Enterprise Security Policy section 8.0 Awareness and Training Standard**.

To ensure we are compliant with this standard, all faculty, staff, and student employees will be required to complete this training by **December 31, 2021**.

The President's Cabinet has authorized the **suspension of eID's that fail to complete the required training after the due date**. If your eID is suspended, you will lose access to all University systems until the training is completed.

This training is developed by the SANS Institute and is delivered using the Litmos Learning Management System. The training introduces basic computer security concepts and good security practices. It takes about 2 hours to complete. You can take all training modules at once or proceed through the training at your own pace.

Sign in to the training

Thank you for doing your part.

If you have any questions, contact the IT Help Desk (helpdesk@k-state.edu).

Dr. Gary L. Pratt
Vice President for Information Technology Chief Information Officer

Chad Currier
Chief Information Security Officer, Deputy CIO