FSCOT Minutes
February 4, 2020 3:30 pm
Business Building-2046

Opening

The meeting was called to order by Brian McCornack, Co-Chair at 3:30 pm, February 4, 2020.

Present

Brian McCornack – Agriculture (17-22) (Co-Chair)
Michael Raine – Business Administration (07-20) (Co-Chair)
Brett DePaola – Arts and Sciences (17-22)
Be Stoney – Education (18-22)
Behrooz Mirafzal – Engineering (17-20)
Ryan Otto – K-State Libraries (17-20)
Lisa Shappee – Technology & Aviation, K-State Polytechnic (15-21)
Scott Finkeldei – Liaison for Chief Information Officer

Guests and presenters

Jahvelle Rhone, Media Coordinator for iTAC's Media Center, Co-Chair on the Innovation Lab Working Group
Chad Currier, IT Chief Operating Officer, Deputy CIO for Enterprise Technology

Approval of Agenda

Agenda was unanimously approved as distributed with slight change in order.

Approval of Minutes

No minutes to approve – Michael is working on getting them caught up.

Recording the Meeting

A brief discussion on Michael Raine's request to record the meeting for those members who could not attend. Several of the details are not clear on where the recording would be published, how long it is retained, and how or if it is protected. Chad Currier asked that the recording be protected by eID and password. *Note, at the time of creating these minutes the recording is not published or available for anyone to view other than Michael Raine.*

Business from the Previous Meetings

Update on Follett text book working group:

Michael Raine reported that he is still developing communication and a first meeting for the working group.

New Business

Update and explanation of the Project Governance Committee:

Brian McCornack serves as the FSCOT and Faculty representative on the K-State Project Governance Committee (PGC). The PGC meets monthly and is made up of central administrators, a Dean, ITS administration, and FSCOT. The group receives requests for large

IT expenditures from across campus or those projects that might have large central IT impact (time, expenses, staffing, security, other resources). The committee approves, disapproves, or requests additional information for a decision. Benefits include better transparency of projects and expenses, possible joint purchasing among units (greater buying power), and better security controls. Brian really enjoys sitting on the committee and feels it is an excellent place for a FSCOT and therefore faculty member. Brian will try to provide ongoing updates as possible.

New innovation lab in library
Jahvelle Rhone, Media Coordinator for iTAC's Media Center, Co-Chair on the Innovation Lab Working Group, provided a presentation on the new innovation lab planned for the second and third floors in the library. The lab is scheduled for opening in the first quarter of 2021. The lab is partially funded by the Sunderland Foundation and might include the following specialty areas: The CAVE, Digital Media Lab, Liquid Galaxy, Hi-Tech, Makerspace, One-Button Studio, Video Production Studio, VR/AR/MR/AI Lab. The lab will provide lots of opportunities for faculty and students to become involved in a technology rich learning environment. The working group has conducted many listening sessions across campus the last two years but are still interested in hearing from faculty, staff, and students, their ideas or suggestions for the lab and its use. Jahvelle's presentation slides are attached to these minutes. For additional information or questions contact one of the following:

Jahvelle Rhone: rhone@ksu.edu
Scott A Finkeldei: curtain@ksu.edu
Academic Services Librarians https://www.lib.k-state.edu/library-contacts
Jeff Sheldon: jsheldon@ksu.edu
Sheila Yeh: sheilayeh@ksu.edu

New Policies from Information Technology Services (ITS)
Chad Currier, IT Chief Operating Officer, Deputy CIO for Enterprise Technology, presented several policies recently approved by ITS. These policies are approved and communication to the university and implementation is scheduled over the next few weeks.

PPM-3420 – Information Technology Usage Policy was rewritten and modernized to meet current trends and needs. The largest changes are in Section .040 Confidentiality and Privacy and discuss when and how the University can monitor individual usage of its computing resources. This section also describes who approves this monitoring. A copy of this policy is attached to these minutes.

A new policy references K-State Controlled Unclassified Information Policy. This policy speaks to controlled unclassified information (CUI) and how that information is collected, developed, handled, stored and maintained by the University. The policy is compliant to the standards set forth in National Institute of Standards and Technology (NIST) 800-171 document. The standards and policy are required for many research grants and federal research funding. The Chief Information Security Officer and the Associate Vice President for Research Compliance are responsible for supporting the new policy. Questions about compliance or the new policy should be sent to CUI@ksu.edu. A copy of this policy is attached to these minutes.

eID password change. A huge change is coming for eID passwords. State of Kansas regulations require password changes every 90 days. Realizing this is difficult at academic institutions, the Regent Universities in Kansas have adapted the latest NIST password guidelines. This will remove the need to change passwords but lengthen them to 15 characters and prohibit dictionary words. Individualized phrases are suggested like: "ILoveRiverRaftingOverPonds". Dictionary words are allowed if part of a phrase. This change is scheduled for implementation in a few weeks and users will see it at their next password change cycle which will be the last password change cycle! Compromised accounts will still require a password change.
Annual Security Training is another State of Kansas requirement and ITS plans to change up how often training will be provided. Instead of an annual occurrence, they plan on partnering with SANS institute and they will release three to five minute trainings on a topic of the month. The training can be customized and will be tied into the HRIS training portal.

Chad also discussed International Travel and Export Controls. Some countries now have laws that allow the seizure and ownership of electronic devices and the data brought into their country. The Offices of Chief Information Security Officer and the Associate Vice President for Research Compliance are emphasizing that faculty and staff traveling to other countries should minimize the amount of data they take with them. They should not use their own laptops but participate in the laptop loaner program provide by ITS through the IT Help Desk. They suggest the following:

- Understand the laws regarding data and encryption
    - Some countries outlaw encryption and will seize equipment
    - Some countries have laws stating any data that enters their borders is "their" data and they will seize laptops, thumb drives, etc.
- Don't assume the hotel safe is secure
- Some countries track all activity so ensure you understand the laws
- Any paper documents, notes, etc. will need protection, have a plan
- Best practice is to take a burner phone, do not have sensitive data, or access to sensitive email installed
- If you don't have a need, do NOT access University resources
- Avoid public workstations for accessing sensitive systems (including personal banking, email, etc.)
- University Research Compliance Office should also be contacted prior to travel to a sanctioned country such as Iran, Cuba, Syria, Sudan, North Korea, and Crimea to conduct any university-related business or activity.
- Contact the IT Help Desk to check out a loaner laptop

Additional information from Chad's presentation is attached to these minutes.

Adjournment
The meeting was adjourned at 5:05 pm by Michael Raine, Co-Chair. The next meeting is scheduled for March 3, 3:30 pm, in BB-2046.

PPM-3420 – Information Technology Usage Policy

.010 Overview and Purpose

This document constitutes a University-wide policy for the appropriate use of all University computing and network resources. This policy is subject to all applicable laws and regulations. It is intended to reflect industry standards with regard to data security, technology, and intellectual property (IP) protection and to ensure compliance with local, state, and federal requirements. It is also intended to complement the other University policies on information technology usage and data security. See PPM 3400-3495.

.020 General Policy

Access to K-State networks and computer systems is granted subject to University and Kansas Board of Regents policies and local, state, and federal laws.

It is the responsibility of each individual who has access to K-State networks and computer systems to ensure that their activity will not intentionally have a negative impact on the confidentiality, integrity, or availability of all K-State computing and network resources.

The University is not responsible for inappropriate or unethical use of the information technology environment, including networks and computer systems.

Policy violations shall be reported (see section .070 Reporting Violations).

.030 Appropriate Use

Authorized users are:

- All provisioned eID holders, including those who have been granted a special access eID (see the K-State eID Policy, PPM Chapter 3450).
- Anyone connecting from a public information service.
- Others whose access furthers the mission of the University and whose usage does not interfere with other users' access to resources.

In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.

Appropriate use of University IT resources shall:

- Be for the purposes of furthering the mission of the University.
- Be for the purposes for which they are assigned.
- Be in accordance with all license and contractual agreements to which the University is a party.
- Comply with policies of any network over which such data or information must be routed to reach its final destination.
- Not interfere with the operation of University IT resources nor unreasonably interfere with the appropriate use of University IT resources by other users.
- Not indirectly violate this policy by using any device, software, or services of another network provider to circumvent the intent or meaning of this policy.

- Not compromise the security and confidentiality of data that is the property of University or any other user of University IT resources.
- Not attempt to circumvent or subvert any system's security measures.
- Not represent yourself electronically as another user.
- Not disrupt services, damage files, or intentionally damage or destroy equipment, software or data belonging to the University or other users.
- Not be for personal purpose other than incidental and minimal use.
- Not be for private commercial use unless authorized by contract.
- Not intentionally misrepresent personal identity.
- Be in accordance with state and federal law.
- Not conflict with or violate any other University or Kansas Board of Regents policy.

.040 Confidentiality and Privacy

While the University does not routinely monitor individual usage of its computing resources, the University may monitor the activity and access the accounts of individual users of University computing resources, including individual login sessions and communications, without notice, for any University purpose; there is no expectation of privacy for users. Some examples of monitoring and access include, but are not limited to:

1. The user has given permission, or has voluntarily given access, for example, by posting to a publicly-accessible web page or providing publicly-accessible network services.
2. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the University or other computing resources or to protect the University from liability.
3. There is reason to believe the user has violated, or is violating, this or any University policy.
4. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the reviewing of general activity and usage patterns.
5. Normal operation and maintenance of the University's computing resources require the backup and caching of data and communications, logging of activity, reviewing of general usage patterns for the unauthorized disclosure of institutional data, scanning of systems and network ports for anomalies and vulnerabilities, and other such activities that are necessary to render service or to meet University legal obligations.
6. It is otherwise required or permitted by law.

Any such monitoring or access must be authorized in advance by the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO). The CIO or CISO will work with the appropriate Cabinet level administrator(s), and/or President before giving approval to proceed.

The University, in its discretion, through the CIO or CISO, may disclose the results of any such general or individual monitoring and information accessed, including but not limited to the contents and records of individual communications, to appropriate University personnel, and/or in reporting to appropriate authorities. The University also may use those results in University disciplinary proceedings and as the University otherwise deems necessary. Additionally, communications made by means of University computing resources are generally subject to the Kansas Open Records Act to the same extent as they would be if made on paper.

.050 Responsible Use of Library-provided Electronic Content

Electronic content made available by the K-State Libraries is provided through specific license agreements. These licenses describe who can use the resource, how it may be used, and the consequences of misuse. Excessive or systematic downloading may result in denial of access. While definitions differ, publishers generally consider multiple sequential chapters of a book or more than half of an entire issue of a journal excessive. Many licenses limit the use of materials to authorized users. Authorized users are K-State faculty, staff, and currently enrolled students. Sharing electronic resources with non-authorized users is prohibited. Sharing passwords, placing licensed materials on a publicly accessible website, and commercial use of licensed information is prohibited. Use of any Library electronic resources constitutes acceptance of K-State's Information Technology Usage Policy, PPM Chapter 3420.

.060 Training

Annual cybersecurity and data protection training is provided for all users and mandatory for all K-State employees.

.070 Reporting Violations

All users and units shall report unauthorized access attempts or other violations of this policy on K-State computers, networks, or other information processing equipment. If a user observes or learns of a security or abuse problem with any University computer or network facilities, including violations of this policy, the user should notify the Chief Information Officer (CIO), or the Chief Information Security Officer (CISO).

.080 Sanctions

Persons in violation of this policy are subject to the full range of sanctions, including but not limited to the loss of computer or network access privileges without notification, disciplinary action, dismissal from the University, and legal action. Some violations may constitute criminal offenses, as outlined in Kansas statutes and other local, state, and federal laws; the University will report such violations to the appropriate authorities.

Unit heads have the authority to deny access, for unauthorized use, to K-State's network and computers systems under their control.

.090 Questions

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

PPM XXX K-State Controlled Unclassified Information Policy

.010 Preface/Overview

This Policy provides University requirements for collecting, developing, handling, storing, and maintaining Information provided by or collected on behalf of the executive branch of the federal government and that falls into at least one of the Controlled Unclassified Information (CUI) registry categories. University employees must safeguard Information to at least the National Institute of Standards and Technology (NIST) "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" standards (NIST 800-171). The NIST 800-171 documents provide guidance and standards on how to protect CUI data in order to reduce or eliminate security incidents from occurring. These standards include many different physical and IT-related security controls, such as access control, physical security standards, and IT system security. This Policy implements those controls, as is required as a condition of the University receiving federally-sponsored research funding.

. 020 Scope of Policy

The following requirements apply to all University Researchers who receive federally sponsored funding and would interact with CUI. Researchers include the Principal Investigator (s) and any additional member of the research team, including undergraduate and graduate students.

.030 CUI and Researcher Requirements for Federal Funding Proposals

All proposals submitted for federal funding, including proposals submitted through government prime contractors, that contain or have the potential to involve CUI program components, shall include appropriate budget line(s) to underwrite the cost associated with meeting the CUI compliance requirement, as further set forth below. This requirement applies regardless of the anticipated contracting vehicle that will be issued to the University, i.e. contract, grant, cooperative agreement, subaward, or the like and regardless if the contracting vehicle supporting the collaboration includes funding or not, such as unfunded Cooperative Research and Development Agreements (CRADA). Researchers should email CUI@ksu.edu for a consultation on how much funding to request.

.040 CUI and Post-Award Requirements for Researchers

If researchers receive federal funding that is subject to CUI security requirements, the Researcher(s) shall:

- Safeguard information and any physical materials through a set of defined standards, outlined in the K-State Controlled Unclassified Information System Security Plan before any work can begin on the project.
- Complete and obtain approval from the Chief Information Security Officer and the Associate Vice President for Research, Compliance for a CUI Information and Physical Security Plan (IPSP), prior to work beginning. The IPSP can be found here.
- Use the University-approved CUI computing service for any information classified as CUI. K-State's approved CUI computing service meets the requirements for secured research requirements. Stand-alone computer systems or alternate systems to the University-approved CUI computing service for information classified as CUI is prohibited, except on a case by case basis that must be approved by the Chief Information Officer (CIO) and the Vice President for Research (VPR), as set out below in subsection .100 Exceptions.

- Researchers working with CUI shall store and handle said materials in controlled environments that prevent or detect unauthorized access. Researchers shall ensure that areas where CUI is stored or used are equipped with locks and doors, and overhead bins, file cabinets, and drawers are locked when not in use. Researchers should email CUI@ksu.edu for a consultation to discuss if doors need to be re-keyed and other physical security requirements designed to prevent or detect unauthorized access.

.050 Security Plan

The University maintains a Controlled Unclassified Information System Security Plan in compliance with federal standards. The offices of the CIO and VPR are responsible for maintaining, updating, and controlling the Plan, as needed.

.060 Awareness and Training

Training is a key part in creating and maintaining a culture of compliance and stewardship of information security requirements. Each Researcher participating in a CUI project shall complete the appropriate training prior to engaging in research and maintains training on at least an annual basis. Training includes but is not limited to; CUI training, cyber security and insider threat. The Associate Vice President for Research Compliance is responsible for the training and any questions about the training, the requirements, or the frequency shall be directed to URCO. The training can be accessed here.

.070 Monitoring and Auditing

The Offices of the CIO and VPR will conduct various monitoring and audit reviews of any CUI-funded project to include physical and information security reviews.

1. Physical Reviews: The University Research Compliance Office (URCO) will annually review the activities covered by CUI IPSPs. The review may include, but is not limited to, reviewing activities and/or items covered by the IPSP; reviewing physical and information security plans; personnel review to ensure that all researchers are listed in the IPSP as participants; visiting facilities to review physical security requirements implementation; and, review of training completions.

   URCO will create a report of the review and provide a copy to the Principal Investigator and/or department, as applicable. In the case of any deficiencies, URCO will work with PI and/or department to address the deficiencies. In addition to the annual review, the PI is responsible for conducting periodic self-audit and evaluations throughout the life of an IPSP and informing the URCO of any change in the research project. The specifics of PI led self-audits are detailed in each IPSP.

2. Information Security Reviews: Logs will be collected and stored for continuous monitoring. Logs that will be collected include management, resource/system security, and diagnostics. The CISCO and URCO will conduct an investigation in the case of any anomalies or concerns.

.080 Reporting Violations

All Researchers shall report CUI@k-state.edu any information or physical security violation of this Policy related to any federally funded project subject to CUI requirements.

.090 Sanctions

Persons in violation of this policy are subject to the full range of sanctions, including but not limited to the loss of privileges to K-State's approved CUI computing service without notification, a hold on research funding, disciplinary action, dismissal from the University, and legal action. Some violations may constitute criminal offenses, as set out in applicable laws; the University will report such potential criminal offenses to the appropriate authorities.

.100 Exceptions

Any exceptions to this Policy will be considered on a case by case basis by the Chief Information Officer (CIO) and the Vice President for Research (VPR) at CUI@ksu.edu. The researcher requesting an exemption will be requested to provide a justification for the exemption.

.110 References

- National Institute of Standards and Technology Handbook 162, "Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements"
- National Institute of Standards and Technology Special Publication 800-171 Special Publication "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."
- National Institute of Standards and Technology Special Publication 800-171 family, Assessing Security Requirements for Controlled Unclassified Information.
- National Institute of Standards and Technology Special Publication 800-53 family, Security and Privacy Controls for Federal Information Systems and Organizations.
- PPM 3420 Information Technology Usage Policy
- PPM 3430 Security for Information, Computing and Network Resources
- PPM 3434 IT Security Incident Reporting and Response Policy
- PPM 3436 Media Sanitization and Disposal Policy
- PPM 3439 System Development and Maintenance Security Policy
- PPM 3450 K-State eID Policy
- PPM 3480 Wireless Local Area Network Policy
- K-State Controlled Unclassified Information System Security Plan

.120 Questions

Questions regarding this Policy should be sent to CUI@ksu.edu.

International Travel and Export Controls Presentation

International Travel and Export Controls

- Most travel for conferences will fall under exclusions to the export control regulations.
- Travelers should limit the information and technology they share to information that is published, and/or publicly available.
- Travelers should not share or take information, software, or technology that is proprietary, or designated for military, space, encryption software, or nuclear related applications; or may have been received under a nondisclosure agreement, or otherwise subject to contractual restraints.
- URCO should also be contacted prior to travel to a sanctioned country such as Iran, Cuba, Syria, Sudan, North Korea, and Crimea to conduct any university-related business or activity.

Research, Fieldwork, Course Instruction, or Related Activities

- Activities such as engaging in research, field work or course instruction abroad may be restricted based on content and export control restrictions applicable to the country of destination.
- Activities that do not meet the criteria for fundamental research may or may not be subject to export controls and an export control review is necessary.
- URCO should also be contacted prior to travel to a sanctioned country such as Iran, Cuba, Syria, Sudan, North Korea, and Crimea to conduct any university-related business or activity.

Keeping Research Data Secure while Abroad

- Understand the laws regarding data and encryption
  - Some Countries outlaw encryption and will seize equipment
  - Some Countries have laws stating any data that enters their borders is “their” data and they will seize laptops, thumb drives, etc.
- Don’t assume the hotel safe is secure
- Some Countries track all activity so ensure you understand the laws
- Any paper documents, notes, etc. will need protection, have a plan
- Best practice is to take a burner phone, do not have sensitive data, or access to sensitive email installed
- If you don’t have a need, do NOT access University resources
- Avoid public workstations for accessing sensitive systems (including personal banking, email, etc.)

Resources on International Travel

- https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/
- https://travel.state.gov/content/travel/en/internationaltravel/International-Travel-Country-Information-Pages.html
- https://www.fbi.gov/file-repository/business-travel-508.pdf/view
- https://www.fcc.gov/consumers/guides/cybersecurity-tipsinternational-travelers
- Jonathon Snowden can give country specific briefings

International Travel Tips

Procedure for requesting a loaner laptop:

1) Request a loaner laptop at least one week in advance of travel by calling 785-532-4918.

2) The loaner laptop is available for pickup from ITS equipment checkout, currently located behind the K-State Student Union Cat's Pause Lounge.

3) Included with the laptop will be a case, charger, and international power adapter.

4) For security reasons, travel laptops have limited software and functionality. The laptop applications and software will include a browser, the MS Office Suite, antivirus software, Zoom and access to the VPN.

5) Upon your return, move any data stored on the laptop during travel to a flash drive or external hard drive. ITS is not responsible for any lost data.

5) The laptop will be erased/re-imaged upon return.

6) The loaner laptop program is free to faculty/staff. However, the individual borrowing the laptop will be responsible for replacement costs due to damage, loss, or theft.

NOTE: Faculty/staff might check their individual units for the availability of loaner laptops.

Innovation Lab Presentation

Note: See PowerPoint File for Full Presentation with Graphics

Sunderland Foundation Innovation Lab Use Cases

iTAC and Library ITS

Innovation Lab Specialty Areas

- The CAVE
- Digital Media Lab
- Liquid Galaxy
- Hi-Tech Makerspace
- One-Button Studio
- Video Production Studio
- VR/AR/MR/AI Lab

The CAVE - Cave Automatic Virtual Environment

https://www.cityu.edu.hk/lib/about/newsletter/article/article_201705_01.htm

Ideate The CAVE

- What is the Cave?
- Where viewers can have an immersive experience viewing and interacting with 3D virtual-reality worlds
- What makes the Cave?
- VR Head Mount Display
- Motion capture sensor
- When to use the CAVE?
- Present a scene in 360 degrees for a project/assignment
- Create an interactive VR interface for a project
- Work on design or engineering problems in a virtual space

Digital Media Lab

https://www.lib.ncsu.edu/spaces/digital-media-lab

Ideate Digital Media Lab

- What is Digital Media Lab?
- A space supports "multimodal learning" by way of multimedia audio and video editing
- What makes Digital Media Lab?
- High resolution monitor
- Large format monitor
- Graphic card
- Video/audio editing software
- When to use Digital Media Lab?
- Produce a movie, blog post, podcast, or website
- Build digital 3D models
- Create digital animations
- Create original digital content or convert older media to digital formats

Liquid Galaxy

https://liquidgalaxy.org/

Ideate Liquid Galaxy

- What is Liquid Galaxy?
- Where an immersive panoramic data visualization can be experienced by groups at a time and where incredible interactive presentations can be built
- What makes Liquid Galaxy?
- 7 Large-paneled HDTVs
- Touchscreen
- 3D joystick

Ideate Liquid Galaxy Continued

- When to use Liquid Galaxy?
- When an environment as immersive as the cave is not needed
- When presenting to/demonstrating for larger groups than the cave
- Presenting an interactive map with the most populated cities in the world
- Showing which European football stadiums have the most capacity
- Mapping the longest rivers in the world
- The most important monuments in the world
- The biggest natural parks in the world
- Showcasing a navigable map of historic Paris built by faculty
- Showcasing visualized faculty data and data projects
- Showcasing campus labs that might not be accessible due to health and safety reasons
- Creating interactive museum exhibits

Hi-Tech Makerspace

https://awelearning.com/makerspaces/

Ideate Hi-Tech Makerspace

- What is Hi-Tech Makerspace?
- Is a venue for students to construct a variety of real-world products at the collegiate level using science and technology standards
- What makes Hi-Tech Makerspace?
- 3D printer
- Laser cutter

Ideate Hi-Tech Makerspace Continued

- When to use High-Tech Makerspace?
- Chemistry faculty print prototypes of molecules
- Workshops about rapid prototyping, 3D printing, 3D design, Arduino and etextiles
- Classes, clubs and projects including "American Studies", "Physics", "Freshman Seminar: Makerbots and Mashups", helping "first year students transition into college
- From the College of Education: in Pompeii using 3D design programs to recreate buildings and artifacts on 3D printers
- A theatre project: a staged production of Lady Windemere's Fan by designing an elaborate chandelier for the set

One-Button Studio

https://libraries.psu.edu/services/rooms-spaces/one-button-studio

Ideate One-Button Studio

- What is One-Button Studio?
- A studio with the newest video technology to produce crisp and clear audiovisual recordings
- It offers an easy way for a novice to produce quality recordings
- What makes One-Button Studio?
- Video camera
- Projector
- iMac computer
- Blue/green screen capabilities
- Monitor
- Ceiling lights and microphone
- One button control

Ideate One-Button Studio Continued

- When to use One-Button Studio?
- Dissertation and thesis rehearsals, class presentations, and TED Talk–style recordings.
- Student video assignments
- Easy-to-record video offers the ability to capture lectures for flipped or online classes or to present video explanations on course topics that are of interest to only a subset of the class.
- Record a presentation for class
- Practice interviewing
- Act out a scene from Shakespeare

Video Production Studio

https://commons.library.upenn.edu/recordingstudio

Ideate Video Production Studio

- What is Video Production Studio?
- A studio to experiment with emerging video technologies and learn best

practices in educational technology

- What makes Video Production Studio?
- Green wall
- Camera
- Audio recording equipment
- Recorders
- When to use Video Production Studio?
- Create educational content or promotional marketing videos
- Help student groups record and market their message
- Story-telling

VR/AR/MR/AI Lab

https://www.smartdatacollective.com/ai-augmented-reality-merge-fornew-business-solutions/

Ideate VR/AR/MR/AI Lab

- What is VR/AR/MR/AI Lab?
- A lab with tools to build Virtual Reality/Augmented Reality/Mixed Reality virtual models and to educate the community on the ethical, technological, and social consequences of artificial intelligence
- What makes VR/AR/MR/AI Lab?
- Google Home
- Amazon Echoes
- Workstations for VR, 3D rendering, and AI computation
- Graphics Cards (GPUs) optimized for AI operations such as "tensor mathematics", which allow machine learning models to be built and run rapidly
- GPUs allow virtual models to be built and tested efficiently

VR/AR/MR/AI Lab Continued

- When to use VR/AR/MR/AI Lab?
- Engineering course on wearable IoT, in which students use the lab to enhance devices designed to collect data on health and fitness
- A neural engineering course, in which the lab can help explore the use of the brain’s electrical activity to control robots
- An intro to philosophy course, in which students undertake foundational programming exercises and engaging in discussions related to relationships between man and machine
- Building a virtual environment for a class
- Creating a machine learning model to test a social science hypothesis
- Creating an augmented reality model to allow users to explore a museum

Campus and Community Partners

- What campus departments have been contacted by the Innovation Lab Committee?
- Mechanical Engineering
- Computer Science
- College of Education
- Department of Geography
- What community groups have been informed by the Innovation Lab Committee?
- MHK Makerspace Club

Campus and Community Partners Continued

- Who are other possible campus partners?
- Research and Extension (budgetary support)
- Precision Agriculture
- Global Campus
- Weigel Advisory Committee

Campus and Community Partners Continued

- Who are possible local and national business partners (budgetary support, internship possibility, certificate development)?
- JNT Company
- CivicPlus
- Network Plus
- Architecture firms in Manhattan
- Microsoft
- Google

The Lab Logistics

- High level technical support is needed
- Equipment vendors

- Staff experts
- Student experts
- Training methods
- Scheduled sessions
- Pop up sessions
- Requested sessions
- Policies and procedures
- Use Policies
- Schedule of charges
- Hours
- To be determined, but not 24x5 or 24x7
- May offer after hours for special programs

- iTAC contacts:
- Jahvelle Rhone: rhone@ksu.edu
- Scott A Finkeldei: curtain@ksu.edu
- Rebecca Gould: ragou@ksu.edu
- Library contacts:
- Academic Services Librarians https://www.lib.k-state.edu/library-contacts
- Jeff Sheldon: jsheldon@ksu.edu
- Sheila Yeh: sheilayeh@ksu.edu