Senate Advisory Committee on Information Technology (SACIT)
Report to the Senate for Academic Year 2019-20

Committee Charge and Role

The primary function of the Senate Advisory Committee on Information Technology (SACIT) is to provide a mechanism for faculty input in the University Information Technology (IT) governance process, as specified by university Policy 6.002 III D.1.I:

> *The primary role of the Committee is to ensure ongoing robust communication among representatives of the University's academic users of information technology (especially faculty and students), and administrators responsible for planning, acquiring, employing and operating information technology resources. Such administrators shall regularly inform and consult with the Committee regarding information technology resources. The Committee should regularly consult with information technology user constituencies and convey input to relevant administrators.*

The committee was established to ensure that faculty members could contribute to the governance and strategic planning of the University Information Technology (UIT) office. The committee takes direction from the Academic Senate and is willing to provide advice on any IT policy and assist with strategic decisions.

The committee is expected to provide input to IT governance both reactively and proactively. In its reactive role, the committee comments on new and ongoing projects that are likely to have an impact on the academic mission of the University. The committee chair monitors issues arising in IT governance committees that should be brought to the SACIT for discussion and reports back to those committees with the SACIT input. The proactive contribution of the SACIT involves identifying and discussing emerging issues affecting the academic mission, especially those that may not already be under discussion by UIT.

As is the case for other Senate committees, the SACIT is required to provide each year a report documenting the committee's work. In this report, we summarize the issues addressed during the 2019-20 academic year.

2019-2020 Committee Members

Chair, V. Kim Martinez — Fine Arts, Associate Chair, David Goldenberg-Science
Steve Hess- Chief Information Officer
Kelly Brodhead-Engineering, Alexey Zaitsev-Medicine, Lauri Linder- Nursing
Trisha Weeks-Social & Behavioral Sciences, Phoebe McNeally- Social & Behavioral Sciences
Amy Thompson-Libraries, Brandon Patterson- Libraries, Kathy Sward-Nursing
Mary Burbank- Education, Thomas Cheatham III-Pharmacy
Andrew Sturgell ASUU, Tracey Mai-ASUU
Department of Art & Art History Support: Sandie Crook

Ex officio

Julio Facelli-Medicine Senate - Academic Senate President

2018-2019 The committee did a commendable job by working in tandem with Pat Hanna's task force to successfully revise University policy 4-003: World Wide Web Resources. Along with multiple rules created/updated to enforce the policy and account for changes in electronic technology on our campus.

Our main accomplishments for 2019-2020 were:

Trevor Long Information Security Office, Susan Schaefer / Tom Howa Business Intelligence group

- **Rule 4-004A Acceptable Use** All Utah networks must require users to authenticate via password or other means. This includes all wired and wireless access to University resources. **Approved to move forward as is with clarification/discussion around timelines.**

- **4-004A -** no un-authenticated network access**. Approved to move forward.**

- **Rule 4-004B Information Security Risk Management-** Discussed changing the security framework to NIST. Must pay attention to grant requirements. According to FISMA people from certain countries cannot access certain data. **Clarification needed.**

- **Rule 4-004C Data Classification and Encryption**
  Require encryption of devices containing sensitive as well as restricted data. This policy would apply to any device containing such data, whether owned by the university or individuals, and would include computers, external storage devices and mobile devices. **Approved to move forward with clarification/discussion around timelines.**

- **4-004G procedure - Vulnerability management notification process.**
  Approved as is.

- **G4-004B guideline - Security and HIPAA Champs.**
  Approved as is.

November 15, 2019

Ratified a leadership change conducted by Julio Facelli in favor of V. Kim Martinez's one-year appointment as Chair and David Goldenberg as Associate Chair.

Oracle/Java Update Brad Millet, Associate Director for Strategic Infrastructure Initiatives, discussed the support, maintenance, and licensing changes to Oracles Java usage.
Committee members raised the following concerns:

- What to look for? How to find out if a system is using Java?
  Recommendation – Meet with Libraries – their computers have the most software that students use on campus
- Central IT has a responsibility to help support colleges
- Security risks involved if Java is not replaced
- Each college to inform faculty, staff and IT department to help find what's best for them.
- Follow-up plan for May 2020 is to make sure all programs are off; Central IT will be off Java. Offending departments will be responsible for audit costs
- Blocking Java while on campus (student/personal computers) is not practical.

Web Policy Update Ken Pink, Deputy Cio, lead discussion around Policy 4-003 next steps and the Holistic Web Strategy.

- Web policy – Agreement between UMarketing and UIT. UMarketing runs the U home page
- Accessibility – University wide policy in progress. Tools are in place for audits. Similar policy is used by US Dept of Education and Justice Department
- RFP Vendors must comply with policy. Six mandatory questions asked in the RFP. Some vendors are refusing to sign.
- As long as faculty is putting in an effort into making programs accessible the auditors are willing to allow for vulnerable of accessibility issues.
- Tag pictures and add descriptions, must have descriptive text.
- Webmaster – new appointment – Barb Iannucci, Associate Director of Content & Usability for UIT University Support Services (USS).
- If faulty are selling products on a university site IT must approve (ex – providing a link to Amazon to sell book)
- What defines a University website? Future discussion issue. Sites that are hosted off campus but focused on university business/research, must follow all University guidelines. Sites need to be registered
- Suggestion to create a research site that is unbiased including apps. IT is reviewing and how it is linked for reporting sensitive findings that are unbiased.

Committee Input

- UIT Collaboration tools. More faculty input by conducting faculty interviews for additional assistance.
- UBox February 2020– additional tools in BoxDrive, any updates must be shared with faculty
- CIS Portal is changing in Dec (by the 28th) –Search driven not tile driven.

December 2019 Meeting cancelled

January 17, 2020
Trevor Long Information Security Office
Susan Schaefer / Tom Howa Business Intelligence group

Rule 4-004A Acceptable Use,

All Utah networks must require users to authenticate via password or other means. This includes all wired and wireless access to University resources. It is the department's responsibility to ensure that this happens. In most cases this service can be provided by UIT. UIT will also provide guest access authentication. The privacy of students, faculty and staff will be protected.
Question concerning implementation:

- How to detect users that bypass security mechanisms
- College Deans signed a Network Connection Agreement 2 years ago.
- Time Scale: implementation and deadline.

Faculty: Implementing authorization on UGuest and EduRoam shouldn't be a big problem. But, some colleges and departments will need a significant lead time for authorization on wired networks. For academic units, the summer is the only practical time for major network changes six months for adoption over summer, in effect 2021.

4-004A - no un-authenticated network access. Approved to move forward as is with clarification/discussion around timelines.

Rule 4-004B Information Security Risk Management

Discussed changing the security framework to NIST. Must pay attention to grant requirements. According to FISMA people from certain countries cannot access certain data.

4-004B update - NIST 800-53.

Return for clarification. The concern (as outlined by Dr. Cheatham) is that the university is committing to FISMA controls and requirements. Trevor Long will investigating.

Rule 4-004C Data Classification and Encryption

Current university policy requires the encryption of institutional data classified as restricted and strongly encourages encryption of data classified as sensitive. In order to enhance the security of sensitive data, and bring the university into compliance with USHE Policy R345, UIT has proposed changes to Rule 4-004C that would require encryption of devices containing sensitive as well as restricted data. This policy would apply to any device containing such data, whether owned by the university or individuals, and would include computers, external storage devices and mobile devices.
Faculty Concerns/Suggestions: The big issue will be the timing of implementation. In addition, the committee strongly recommends a required online training program for faculty, staff who handle sensitive or restricted data. It is probably impossible to ensure compliance with the encryption requirement, but we need to implement a process to ensure that nearly everyone is aware of the requirement.

4-004C update - data encryption. Approved to move forward as is with clarification/discussion around timelines.

4-004G procedure - Vulnerability management notification process.
Approved as is.

G4-004B guideline - Security and HIPAA Champs. Approved as is

Committee input presented *to Julio Facelli, February 3, 2020*

February 2020 meeting cancelled

March 20, 2020 Agenda- May be cancelled due to school closure.
Steve Hess, UIT, Chief Information Officer
Corey Roach, UIT, Chief Information Security Officer
Discussions concerning university-wide information security programs. current discussions concerning university-wide information security programs. The conversation could include compliance concerning Umail, Hipaa, Email Access Task Force, and any other security issue that could be advantageous information for faculty and students.

Trevor Long, UIT, Associate Director for Governance, Risk & Compliance
Update on Policy 4-004B - NIST 800-53. The concern raised by SACIT member Dr. Tom Cheatam at our January meeting, was that the university is committing to FISMA controls and requirements.