



Information Security & Compliance
IT@UC
University of Cincinnati
PO Box 210658
Cincinnati, Ohio 45221-0658
Suite 400, University Hall
51 Goodman Drive
(513) 558-4732

**Information Security and Compliance Committee
Meeting Minutes
University Hall, Room 310
August 17th, 2017**

Present: Michael Miller, Megan Pfaltzgraff, Matthew Clayton, Bo Vykhovanyuk, Brett Harnett, Jesse Fatherree, Kyle Hern, Tina Bosworth, Katrina Biscay, David Baker, Matt, Nick, Greg, Rick Grant, Eira Tansey, Greg Case, Nicholas Lotts

Apologies: Jane Combs, Ed Dadosky, Angela Sklenka, Mark Stockman, Mel Sweet, Tara Wood, Bruce Burton, Cindy Lusby, Todd Beekley, Diane Brueggemann

New Business

- **Welcome and Overview**
- **Review of June Meeting Minutes**
 - Jesse Fatherree motioned the committee to approve the minutes, Lorre Ratley seconded the motion. The committee voted unanimously to accept the minutes.
- **Panel to Discuss Challenges in IT**
 - How to increase security and control at individual units? – UCIT is doing well in this respect but individual college's need assistance because there is a lack of knowledge in this area (Nick?)
 - More End-User Awareness
 - Suggests there be a training administered by InfoSec that is available a couple times per year (that way to address new employees) consisting of a **repeatable 60 minute presentation with a Q&A session to follow**
 - To attract more people and keep the training sessions from being too dry, tie the info back to the "why" and recent national and local events.
 - Need good marketing at the college and local department level to make it relevant – advertise training via e-Currents

- Reach out to Faculty Senate and Associate Deans about the best ways to communicate to the faculty
 - Suggests the training to be available in October for IS Awareness Month and possibly included in the onboarding process along with HIPAA, Title IX, etc.
 - Other suggestions for training:
 - Already have custom short course for central IT and custom modules for a few other units; suggest a phishing article advertised in eCurrents and offer a raffle for participants, create local admin policies
- Use SCCM for managing computers
 - SCCM is a systems management software product developed by MS that manages a large groups of computers. Provides remote control, patch management, operating system deployment, network access protection and hardware and software inventory.
 - It is set up by Central IT and supported by Eric Tribbe, Desktop Support.
 - Should some of these issues be discussed with CSSI committee, such as AD and SCCM?
- 2. CEAS – uses AD but some faculty buy their own machines and manage outside of AD. Should a 1-hour security awareness class be required by specific topic?
- Megan invited IS to present Data Protection policy at new faculty orientation. Other suggestions included:
 - Engage Faculty Senate IT about policy updates
 - Work with HR LMS system to mandate and track security training
 - Suggest blocking phishing emails and deactivating them in mailboxes. Infosec is already working with email team and vendors to deactivate the threat at a higher level even if the emails continue to be sent.
- **Policy Updates**
 - Nelson met with Provost Landgren to discuss: (ASK Matt for this update)
 - **Incident Management and Response Policy**
 - Next steps are being worked out
 - **Cloud Policy**
 - Should be fast tracked
 - A packet with all other policies will be distributed to the committee before the September meeting – will be looking for an endorsement to start the Governance process
 - If one is held up/questioned, policies not in question will start the process through Governance
 - Nelson is pushing for release of all of them at once!
 - Some concerns about Acceptable Use policy (which policy?) from FSIT. No major revisions but some minor changes may be made before it is submitted for approval.
 - Framework policy will be distributed.

- **FISMA Update**
 - Created a recommendation for possible solution to FISMA
 - Final version of recommendation is being drafted by the task force and will be shared with Jane Strasser first for her feedback.
 - Have a meeting with PIs from CEAS to have them create real-world test scenario of the recommendation.
 - Once recommendation has been approved, will be shared with this committee.
 - UC must be in FISMA compliance by Dec 2017.
 - Federal contracts fall under FISMA compliance but grants do not as of now, but will be soon.
 - FISMA compliance requires a mix of central IT and distributed IT effort.
 - Fully implemented AD and SCCM across the university would help with FISMA compliance.
 - Provost wants data governance task force to form. Expect that to continue even with transition of interim Provost.
- **Miscellaneous**
 - Don Rainwater is on the agenda for next month to discuss Central IT's Disaster Recovery and Initiatives
 - Compliance and Audit Committee Presentation/Update in a future meeting.
- **Adjourn at 11:25 am**