



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
February 16th, 2017**

Present: Tina Bosworth, Kyle Hern, Ed Dadosky, Megan Pfaltzgraff, Mel Sweet, Matthew Clayton, Rick Grant, Katrina Biscay, Geoff Costa, Matt Williams, David Baker, Jesse Fatherree, Todd Beekley, Lorre Ratley

Guests: David Gearing

Apologies: Bo Vykhovanyuk, Cindy Lusby, Tara Wood, Eira Tansey, Brett Harnett, Angie Sklenka, Jane Combs, Mark Stockman, Bruce Burton, MB Reilly

New Business

- **Welcome and Overview**
- **Review of January Meeting Minutes**
 - Lorre Ratley motioned the committee to accept the minutes; Todd Beekley seconded the motion. The committee voted unanimously to accept the minutes.
- **David Gearing – Data Security Requirements in Grants**
 - Grants and Contract must adhere to information security requirements, especially for federal contracts.
 - UCIT and local IT help review contracts for security purposes.
 - David shared a packet with the committee titled, Inside Government Contracts.
 - Some language is required in all contracts but may not always be applicable but is always applicable for sensitive but unclassified data. Office of Grants and Contracts has OIS review contracts for applicability.
 - DHS and DOD contracts are considered sensitive but unclassified. UC does not perform any classified research.
 - The bulk of federal awards at UC are grants. FISMA applies to all grants and is congressionally mandated since 2002. Any unit/researcher at UC not in compliance with FISMA puts the whole university federal grant portfolio at risk
 - More than \$250 million in grants over a two year period is at risk for non-compliance with FISMA

- Primary Investigators (PIs) for a research project have responsibility to submit all the necessary data protections and controls, including FISMA compliance, with their grant proposals. UC must be in full compliance with FISMA requirements by December 2017.
 - Bo and Brett Harnett are forming a FISMA task force at UC to help ensure compliance. The membership will consist of Jane Strasser, Office of Research, R&D, IS&CC, Core Services, IT Managers Governance committee representatives as well as graduate and undergraduate scholar representatives. They hope to have final recommendations to University Leadership by summer semester.
 - The task force will reach out to the UC research community with policies, recommendations, requirements, and any changes to future grants and contracts.
 - UC Irvine and Purdue are leaders in FISMA compliance.
 - David Baker, Todd Beekley, David Gearing, Tara Wood, Matthew Clayton and Megan Pfaltzgraff volunteered to serve on the FISMA task force. Matthew will recruit another undergrad student for the committee. David Gearing will recruit faculty representation from College of Engineering who have DOD grants and contracts.
 - Bo and Brett will be in touch soon to schedule FISMA task force committee meetings
- **Multi-factor/Flex Integration Update (Geoff Costa)**
 - Multi-factor authentication is a mandate coming from the senior leadership team at UC for access to UC Flex.
 - VPN using multi-factor is in proof-of-concept used by Information Security and UCIT Helpdesk.
 - UC is Implementing Duo to be the enterprise multi-factor solution. RSA is currently in production for Central IT.
 - Multi-factor will be implemented in phases at UC, starting with BCS, OIS, HR, and Controller departments as pilots.
 - Once pilot departments have it successfully implemented, it will be rolled out to the whole university.
 - Duo is capable of using various mobile devices, including smart and dumb phones, tokens, and other methods for multi-factor authentication.
 - Infrastructure to start pilot should be in place by the end of February.
 - A Communication plan, documentation, and training will be available before implementation.
- **Policy Updates**
 - Matt Williams shared an updated policy status sheet. Information Security Review and Privileged Access review policies will be presented to the ITCAC governance committee on Friday, 2/17.
 - IT Council approved retiring the HIPAA policy owned by OIS and using the updated HIPAA policy owned by The Office of General Council instead.
 - Data Governance and Classification policy was approved by IT Council in January
- **Other Items**
 - Risk Tabletop Exercise
 - Some UCIT teams (UCIT Managers, UCIT Lead Team) have undergone the Risk Assessment exercise.
 - OIS will lead the exercise for IT Council at their meeting next week on 2/22/2017.

- IS&CC committee will perform the exercise for IS&CC at the March meeting.
- BCS and IT Managers are not on the schedule yet but will also perform the exercise in a future meeting as well.
- **Research Education**
 - Matthew Clayton will work with the student government tribunals and the Office of Research to help develop a program for research requirements for students. One suggestion is to create a 4-hour workshop for students to learn about HRPP and security related policy requirements in research.
 - All colleges on uptown campus would participate in the workshop with the exception of DAAP.
 - **Matt Williams is meeting with Angela Braggs-Brown and Bo today regarding HRPP requirements in research and will follow up with Matthew about their discussion.**
- IT Governance draft bylaws are being reviewed by ITCAC on Friday. Feedback and suggestions from various governance committees has been incorporated and more is under consideration. A [shared Box account](#) has been created for the draft bylaws and includes a log of the suggestions submitted. A link to the folder with read access will be shared with all governance committees after the ITCAC reviews the latest draft tomorrow.
- **Adjournment**
 - The committee adjourned at 11:05 AM.