Information Security and Compliance Committee
Meeting Agenda
University Hall, Room 310
November 16th, 2017

Attendees: Elizabeth Aumann, David Baker, Jesse Fatherree, Brett Harnett, Kyle Hern, Cindy Lusby, Megan Pfaltzgraff, Lorre Ratley, Eira Tansey, Bo Vykhovanyuk, Matt Williams, Mel Sweet, Tara Wood

Guests: Aretha Abrams, Tyler Hopperton

Apologies: Todd Beekly, Diane Brueggemann, Bruce Burton, Matthew Clayton, Jane Combs, EdDadosky, Rick Grant, Tamie Grunow, Michael Miller, Mark Stockman

New Business

• Welcome and Overview
• Review of October Meeting Minutes
  o The minutes were unanimously approved.
• DFARS Discussion – Tara Wood, Aretha Abrams (PowerPoint linked)
  o DFAR clauses and Collaboration Reporting are being reviewed to ensure that UC is meeting the requirements. DFARS is the Defense Federal Acquisition Regulation Supplement – rulemaking authority by DoD in connection with purchasing/acquisitions.
  o When David returns, they will discuss with him where UC is in this process and what they need to do to collaborate with IT@UC.
• Identity Access and Management Survey Discussion – Tyler Hopperton (IAM Doc, IAM Timeline)
  o Tyler and his team have been working on conducting a survey about information security. The survey questions were distributed towards the beginning of October and they are receiving good feedback.
  o Identity Access and Management (IAM) will automate the process of defining who needs access, how much and for how long. Successful IAM programs take between 3-5 years to implement. The biggest risk UC faces is not following through with this program. With
existing and new compliance rules on the rise comes larger fines for not complying with them (i.e. EU GDPR – European Union’s General Data Protection Regulation). UC’s biggest current problem is that there are no centralized list that tell who has access to what. Completing the project in segmented pieces that fit together guarantee a larger percent chance of success. Project 1/Phase 1 will consist of identifying how people interact with the university from an access point (this is a large chunk of the entire program). Overall, this program needs to be ‘left to right’ where we are speaking to the business owners first to find out what they need in a tool before identifying any kind of technology. To nail down how people are interacting and their processes allows the ability to apply a software/build a tool on how to manage the access automatically.

- Miscellaneous
  - Annual Policy Review
    8 policies were batched together and approved by IT Council during the October meeting
    3 policies are in IDM. This process has changed since President Pinto joined UC, Nelson Vincent and Kristi Nelson (Provost) are trying to figure out what they will do next time.
    Acceptable Use Policy was originally accepted by Faculty Senate, but recently there has been some concerns raised to change some of the verbiage. The approved policy is still in place and the overall meaning will not change with said verbiage changes.
  - Governance Bylaws were approved
  - Two sets of training available to the committee
    Phishing training is available via LawRoom
    Information Security Annual Training is available via Blackboard
    - More targeted towards Admins and people within IT to increase security awareness and review policies
    - Required by UCIT and BCS – Highly encouraged for everyone to take it!
  - Duo Access Gateway
    2FA is being implemented in phases
    July 31st was the initial pilot (Controller, HR, OIS, BCS)
    Sept 1st – mandatory enrollment for pilot members
    Sept 11th – Opened it up to business users to opt-in (anyone other than ESS)
    Nov 1st – Mandatory enrollment of all business users (~2000 users)
    Dec 1st – will start to communicating with the rest of the university – 13,000 people will be required to enroll
    March 1, 2018 – Duo will be required for all users of UC Flex. (after open benefits enrollment, winter holidays, and W2 period)
    Goal – to provide one easy tool to protect identification
    UCFlex is the first enterprise system to use Duo, expected early 2018 to expand to other systems
    Per the Password Policy, if a system stores protected data, 2FA is required
- Use of the Duo app via smart phone is recommended, but land lines or tokens may also be used. Mobile devices will require installation of the Duo Mobile app. Users should contact their local IT for app installation help first and if additional help is needed, contact UC Service Desk.
  - There will be no December meeting!