Information Security and Compliance Committee
Meeting Minutes
University Hall, Room 310
April 20th, 2017

Present: Megan Pfaltzgraff, Cindy Lusby, Matthew Clayton, Todd Beekley, Eira Tansey, Jesse Fatherree, EdDadosky, Bo Vykhovanyuk, Matt Williams, Jane Combs, Mel Sweet, Tara Wood, Brett Harnett, Rick Grant, Lorren Ratley, Katrina Biscay

Guests:

Apologies: Michael Miller, Diane Brueggemann, Conner DuShane, Bruce Burton, David Baker, Mark Stockman, Kyle Hern, Angela Sklenka, Tina Bosworth

New Business

- Welcome and Overview
- Review March Meeting Minutes
  - EdDadosky approved the minutes
  - Eira Tansey seconded the approval
- March Risk Tabletop Summary
  - Matt led a discussion about the results of the risk survey that has been completed with several groups
  - The method for collecting the information was different for UCIT Managers; the questions were the same but Post It Notes rather than iPads were used
  - The balls on the heat map include a set of questions that pertain to that group
  - There was a question about overlap with people who are on multiple committees–there are very few people on multiple committees and there is little concern about the data being skewed due to a single person’s opinion; even if a person is on more than one committee they are a representative of that group’s make up
  - The goal of the exercise is to be able to provide the board with information about areas of highest risk
  - Once high risk areas are identified, the risks can be assessed and plans put into place
  - The heat maps will be shared in August with the board; materials need to be complete by July 1 for distribution to board members
Jane suggested adding eLearning, R&D, and Core Services – agreed to set up the assessment with R&D and BCS.

- Idea is to identify high risk, create mitigation strategies, and reassess annually.
- Survey takes about 40 minutes to an hour to complete.
- The questions were derived from Educause; they had 11 domains and we have 7 so the questions were modified for our environment.

**FISMA Taskforce Update**

- Brett – looking at all components to address.
- Will have a preliminary report in a few weeks to share with committees; progress is faster than expected.
- Many people do not know what FISMA is.

**Policy Updates**

- The Cloud policy was sent out last week for feedback.
- Eira wants to add a bullet about compliance of records retention in the disclaimers.
- Matt explained that the scope of the policy is to deal with expansion of UC’s data center into the cloud.
- Eira is concerned about SaaS that stores our data and they do not have contract language to purge the data at the end of the contract.
- Academic – the term covers more than just teaching.
- Research – there is no public research; the data is classified as Controlled or higher.
- Megan – this policy will apply to the university not just central IT.
- We do not have an enterprise agreement with Amazon Web Services yet.
- We have some agreements with Microsoft Azure.
- There is a State grant being worked on with a multi-university system; no timeframe yet; Akron and Kent State are included.
- Also working on an AWS state contract.
- Jessie – the college of medicine is looking at what is available.
- Nelson has this as a high priority and we are looking at a way to provide IaaS through central IT and we can extend our network into the service and it is not over the public network but rather a local IP address.
- Bo will check with Garry Casson to see if there is a contract with Azure.
- The Policy does not apply to students.
- Matthew Clayton will look into situations of unpaid research student working under the direction of faculty – Bo will consider a way to include this research in the policy.
- SaaS – currently general council catches that there must be a Security Review.
- Tom Guerin said that purchasing already has a statement that all policies must be followed without naming specific policies.

**Miscellaneous**

- Jane Combs – putting together a proposal for a central HPC.
- Jane is on the search committee for the Director of Cyber Research position; this person will work on opportunities to get research funded.
- The May meeting will be canceled due to many conflicts; Jane Haniefy will cancel the meeting.
- Eira had a question about faculty for this committee.
  - Eira has been elected to stay on committee another 2 years.
  - Bo will reach out to the faculty appointed – Eira will send Bo an email with the information.
IT Risk Assessment Heat Map
UCIT Managers

- Information Systems & Applications
- Research Computing Services
- Educational Technology Services
- Network & Data Centers Infrastructure
- Unified Governance & Aligned Management of IT
- Identity Management & Security Integration
- IT Support Services

Direction of Increasing Concern
Background

Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) offer a number of advantages including low cost, high performance and quick delivery of services. However, security controls are required to protect university IT resources.

**Infrastructure as a Service (IaaS)** refers to solutions that provide services such as storage, virtual server hosting, networking or other infrastructure components via the Internet. IaaS offers many advantages, including scalability based on resource demands.

**Platform as a Service (PaaS)** allows customers to develop, run and manage applications without building and maintaining infrastructure. PaaS provides methods to interact with services like databases and file storage, without having to deal with low level requirements.

**Software as a Service (SaaS)** is a software licensing and delivery model in which software is licensed to or on behalf of the university and is hosted by the vendor, typically the university accesses the application via a web browser.

Policy

This policy addresses the use of IaaS, PaaS and SaaS for university enterprise purposes where the service essentially becomes an extension of the university network.

Faculty, Staff and Affiliates are not permitted to enter into IaaS or PaaS service contracts for the storage, manipulation or exchange of university data. University departments who need IaaS or PaaS services must use the IaaS and PaaS vendors that have been vetted and contracted by IT@UC.

Purchases of SaaS services require a [Security Review](#) prior to implementation. Failure to adequately plan for the security review will result in delay or termination of the project.
Academic use of IaaS, PaaS and SaaS are permitted. The academic use must not use Export Controlled, Restricted or Controlled data, as classified by the Data Governance & Classification Policy.

The following safeguards are required:

- The use of IaaS, PaaS and SaaS services must comply with the university’s existing computing policies. These policies include but are not limited to:
  - Data Governance & Classification Policy
  - Acceptable Use of IT Resources Policy
  - Other information Technology Policies
- The use of IaaS, PaaS and SaaS services must comply with all laws and regulations governing the variety of data types used by the university.
- Export Controlled data may not be stored in Cloud based file storage unless specifically approved by the Export Controls Office.
- Personal cloud service accounts may not be used for the storage, manipulation or exchange of university-related communications or university-owned data.
- Data stored in the cloud and data in transit to and from the cloud, must be encrypted.
- Privileged access users accessing the management console or other privileged access accounts in the cloud, must use multi-factor authentication.

Vendors for IaaS or PaaS services are vetted and contracted on an enterprise contract for the university, the vendor must accept the terms as stated in the Data Security Rider. The terms of use for SaaS vendors must be closely scrutinized to insure adequate protection of the confidentiality, integrity and availability of university data.

IaaS, PaaS and SaaS services must not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans. The university must determine how data would be recovered from the vendor and/or transferred to a different vendor. The university must also work with the vendor to establish procedures on data sanitization from the vendor’s services.

Contact Information

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

Related Links

Acceptable Use of IT Resources Policy
Data Governance & Classification Policy
Data Security Rider
Purchasing Policy
Security Review

Revision History

Draft: 03/03/2017
IaaS, PaaS, SaaS Policy v1.0