Information Security and Compliance Committee
Meeting Agenda
University Hall, Room 420B
July 15, 2015

Present: Bo Vykhovanyuk, Kevin Shaffer, Jason Green, Jamie Byrne, Angie Sklenka, Mark Stockman, Todd Beekley, Jane Combs, Lorre Ratley, David Baker, Matt Williams, Jessee Fatheree, Neil Holsing, Kevin Shaffer, Karen Kovach, Tara Wood

Overview
• OIS Charter was approved by the IT Council
• It was discussed for any errors/omissions at the OIS Annual Strategic Planning event held in late July.

Meeting Minutes
• June Meeting Minutes were motioned, seconded and approved.

Policy Development Framework
• Goal is to be agile and approve quickly using the defined policy structure
• Framework has been presented to IT Council, currently waiting on feedback.
• Bo expects it to be approved and then be forwarded to the Office of the President Integrated Decision Making process.

Miscellaneous
• IT@UC Governance is currently reviewing committee memberships, structure and formalizing committee charters
• Bo is working with Jane Combs to review R&D initiatives for security and availability
• OIS will be developing/performing a high-level risk assessment for entire UC community.
  o Already received critical system inventories from units so OIS is aware of critical systems
  o Currently developing a survey sent to unit heads to determine type of data in their custody (restricted, etc.) and their information security posture.
  o Goal is to create a heat map for all of UC at a departmental level to assist with communicating information security posture to university leadership.
  o Developing a matrix to help users determine what type of data they have (i.e. restricted, classified, etc.) and what security controls are required for protection of that data.

• Jane discussed subcommittees out of R&D and how they can collaborate with IS&CC
  • Tara is chair of Export Controls subcommittee

• Jesse Fatherree – McAfee issues causing problems with clients - he will discuss with Bo outside of this meeting
  • Audit issues – need to set some flags in system to be able to audit
  • Encrypting data
  • Neil, Bo, and Jesse will meet outside of this meeting to address

Policy Updates
• Electronic Mail Policy – Review and email Bo with feedback by Monday EOB.
• The purpose of the policy is to restrict official UC business to UC email systems only and not allow duplicate email systems.
• Does this apply to affiliates and CoM faculty who hold multiple appointments?
  • Yes, if they are conducting UC business
  • How to bring policy into alignment with reality?
    • CoM is biggest concern
      • Some work has been done between UCHealth and UC CoM
      • Policy written to restrict auto-forwarding for CoM staff to non-UC or affiliated entities.
      • Does not include Pediatrics – they have opposite situation where all mail goes to UCHealth.
• They run reports monthly to check for compliance
  ▪ Perform risk assessment and allow some exceptions?
  ▪ Rewrite policy to exclude specific entities and continue to monitor the issue
  ▪ Kevin will rewrite and distribute today
  ▪ Employees who work with Economics Center, UCRI, UC Health, VA, Children’s, etc., to be considered for exceptions
• Need to meet with OGC to see if UC can develop an agreement with affiliates to create a policy that that covers this situation
• Bo plans to present the Email Policy to IT Council for approval next week.

• Mobile Device Security Standard (NOT a policy)
  ▪ This is a supplement to a policy and will have links to the policy
  ▪ IPhones already have the required encryption, but not all smart phones do.
  ▪ Bo is working with Integration Services (Jon Adams) to manage this standard via technical means for faculty, staff, and affiliates
  ▪ Students will have another standard
  ▪ Mobile Privacy Policy vs Mobile Device Security Standard
    ▪ Kevin will remove Mobile Privacy Policy from IS&CC website. This policy is being incorporated into the Mobile Device Standard
  ▪ Technically everyone who uses email on their mobile device is most likely in violation of UC policy (Data Protection Policy).
    ▪ Bo is drafting policy framework and vetting it to address this with IT Council
    ▪ Policies/guidelines will follow
  ▪ Need approved policy links in HR documentation

• Data Governance & Classification Policy
  ▪ High level policy to explain data types, in place for few years
  ▪ Bo is proposing policy name change
    ▪ Named Data protection policy in past but has been renamed to Governance and encompasses broader assets
      ▪ Restricted
      ▪ Classified
      ▪ Public Data – Directory data
  ▪ Review & provide feedback to Bo
• Information Security Incident Manage & Response
  • Adding to existing policy
  • Todd will discuss insurance issues with OIS outside of meeting
  • Need to develop incident response team as part of this
  • OIS is responsible for managing breach in conjunction with other members of an incident response team such as Director of Privacy, General Counsel, Risk Management and Registrar’s office.
  • Requires people to notify OIS if they suspect breach.
    ▪ Export Controls must notify Government within 48 hours of discovery of breach
  • Needs to be one entity to manage incident
  • Bo will detail other issues around this with guidelines and standards
    ▪ Provide feedback by EOB Monday
• CoM Policies and Procedures

New Business
• Welcome and Overview
• Review of June Meeting Minutes
• Policy Update
• COM Policies and Procedures
• Security Operations Metrics

Action Items
• Neil Holsing and Tara will meet outside this meeting to discuss export controls
• Todd will discuss insurance issues around the Information Security Incident Manage & Response Policy with OIS outside of the meeting
• Kevin will remove Mobile Privacy Policy from IS&CC website
• Kevin will rewrite and redistribute the Email Policy for final approval

Adjourn
SharePoint Site for shared documents