IT Governance Research & Development Committee
Meeting Minutes

November 12, 2013

AGENDA
Welcome and Introductions - Mark Faulkner

- IT Governance Structure – (Mark)
- Committee FY14/15 Meeting Schedule (Mark)
- Draft Policies (see attachments) (Bo)
  - HIPAA Privacy and Security
  - Password
  - Risk Acceptance
- Draft University Information Security Plan (Bo)
- ePorfolios (Pamela)

CALL TO ORDER
Present: Shannon Funk, Brian Verkamp, Steve Marine, Brett Harnett, Dama Ewbank, Matt Hartman, Charles Jake and Mark Faulkner

Apologies: Pamela Baker, Kaleb Posey, Kumar Vemaganti, Aparna Sundar, Tara Smith

BUSINESS
Mark opened the meeting by welcoming all the members and thanked them for their willingness to serve on the committee. Introductions went around the table.

The group reviewed the IT governance structure and the specific charge for this subcommittee. It has a broad and diverse scope.

The group will meet on the 2nd Tuesday of the month to enable preparation of topics for IT Council meetings scheduled later in the month.

Today's meeting focus is around institutional policies, data compliance and institution-wide information security plan.

Privacy and Security Policies
The group of privacy and security policies has been vetted via most Integrated Decision Making Committees. The final step is to go to the Executive Committee for approval. Discussion ensured and the group reviewed the university’s Integrated
Decision Making Process. The policies were also presented to Faculty Senate and Associate Deans.

Charles indicated Provost’s office has the capability to add university units as a covered entity per the original BOT rule.

Bo – UCIT submitted only the security policy. He explained the three main points of the policy:

1. The annual HIPAA risk assessment – it’s pervasive throughout all university.
2. HIPAA systems inventory database - OIS track all systems that contain patient data.
3. Annual HIPAA training – anyone dealing with electronic patient data must take it.

The committee discussed cloud storage and associated compliance issues. Mark and Bo indicated this is addressed in the university-wide information security plan. They are awaiting notice that the service provider has incorporated the appropriate Business Associate Agreement into its Master Services Agreement.

UCIT and Office of General Counsel also co-authored a Data Security Rider security to provide guidance to university units when executing a hosted or cloud agreement where an external service provider will be storing university data assets. It explains UC storage policies and security assessments.

**Password & Risk Acceptance Policies**

The committee discussed the major change in the Password policy is moving to a 90-day expiration from the current 180-day expiration. Committee members indicated the need to comply with industry best practices, federal authentication standards, alignment with UC Health practices and Internal Audit recommendations.

Mark indicated he anticipated future subcommittee conversations about password policies as the National Institute for Standards and Technology recently released a new draft standard. Further investigation is needed, however initial review indicates a stronger emphasis on password strength and potentially greater flexibility expiration timeframes.

A risk acceptance policy is needed for documenting and acceptance of risk when it is understood that it is not possible or practical to eliminate all business risk. The risk acceptance process provides an organization that elects not to institute a control or process to reduce the risk any further, and the opportunity to document and have UC senior management or their designee accept the risk.

**Information Security Plan**
OIS developed an institution-wide plan for the next three years. The plan is divided in three parts:

1. **Enterprise Risk Management** – how Information Security is governed at UC, reviewing existing polices, developing new policies, monitoring and assessment of infrastructure and systems, etc.

2. **Enterprise Shared Services** – the importance of delivering secure and compliant shared applications, services, tools, and education and awareness to university communities.

3. **Unified Information Security Architectures** – IT systems are distributed, which makes managing security complex. The goal of unified information security architectures is to design and build better information security systems in order to reduce vulnerabilities to a manageable level.

The plan was presented at the October Board of Trustees Governance and Audit Committee meeting. The BOT is supportive of the recommendations and UCIT will be working across Vice Presidential areas to secure funding investments.

**ePorfolios**
This item was tabled since Pamela Baker was unable to attend the meeting today.

**NEW BUSINESS**
Mark opened the floor for general discussion.

The committee held an open discussion on roles and overlap among all the IT Governance Committees.

Matt Hartman asked for clarification – how do university citizens submit ideas, requests, etc. to the IT Governance structure? Mark indicated he would take the question to the next IT Council meeting for discussion and clarification.

Steve Marine suggested the committees communicate results early and often to build momentum around IT Governance structure.

Mark closed the meeting by inviting the members to submit agenda items for future meetings. This committee is a collaborative body and everyone can bring items to the table for discussion.

**ACTION ITEMS**

- Mark Faulkner - Take the university submission process to the next IT Council meeting for discussion and clarification.

**ADJOURNMENT**