Technology Committee Meeting

Present:  
Committee Members:  Kevin McCarthy, Chair (by polycom); Eleanor Baker (by polycom), Norman Fournier (by polycom), and Tamera Grieshaber (by polycom).  
Student Representatives:  Nathan Grant (by polycom).  
System Staff:  Kelley Wiltbank, Rebecca Wyke (by polycom), Ralph Caruso (by polycom), and Cindy Mitchell (by polycom).  
Campus Staff:  Fred Britten – UMF (by polycom); Janet Waldron – UM (by polycom); John Gregory – UM (by polycom); William Wells – USM (by polycom).  
Guests:  George Doliker – Protiviti (by polycom).

Absent:  Samuel Collins.

Trustee McCarthy called the meeting to order.

Portal Business Case.  Mr. Ralph Caruso, Chief Information Officer presented the business case for selecting a System Portal provider.  The consulting firm Collegiate Project Services (CPS) was hired to evaluate the needs of students, faculty and staff and to determine the best options of Portal providers for the UMS.  CPS recommended two options in which the UMS already has made some investment.  The first option was to implement PeopleSoft Portal 9.1 and the second was to partner with CampusEAI Multi Campus Portal to implement myCampus.  CampusEAI is a more flexible and inexpensive tool over time and from a strategic standpoint and long range return on investment, CampusEAI was the better choice.  CampusEAI is currently operational at UMF.  The Portal Project Team, although ultimately reporting to the Office of the Chief Information Officer, will be located on the Farmington campus and will benefit from the expertise existing there.  Each campus will tailor certain components of the Portal to their needs and some aspects of the Portal will be common for all campuses.  There will be a governance process in place and the campuses will need to integrate the Portal with their websites.

Another advantage of choosing CampusEAI over PeopleSoft is the reduction in risk.  Our security-consulting firm, Protiviti, has questioned the variety of side or “shadow” systems in use at the individual campuses.  A number of these shadow systems would be avoided by providing the common development platform from CampusEAI.  With this platform, the UMS can build applications that access enterprise data directly in a single, secure framework, which can be centrally monitored for security compliance and unusual activity.

Phase I of the project includes implementation at USM and UMA and is estimated to take six to seven months.  Phase I is planned to launch no later than early August 2011 in order to be ready for students as they prepare to return to Fall classes.  Phase II implementation would include UMM, UMPI, UMFK.
and UMaine and would take an additional six months assuming a strong commitment from those campuses.

The cost for CampusEAI is significantly reduced from the other products with a one-time fee of $240,000 and an annual recurring fee of $270,000. Ms. Rebecca Wyke, Vice Chancellor for Finance and Administration and Treasurer, indicated the start up costs would be covered by the System and distribution of the ongoing annual costs will be determined with input from the Shared Services Advisory Council.

On a motion by Trustee Fournier, which was seconded by Trustee Baker, the Information Technology Committee recommend that based upon extensive review and analysis of the business case presented, the Information Technology Committee recommended the selection of CampusEAI for development of the Portal for the University of Maine System and forwarded the recommendation to the Consent Agenda for Board action at the January 10, 2011 meeting.

**Draft Information Security Plan.** Mr. George Dolicker, Protiviti, presented a high level draft of the Information Security Strategic Plan. He outlined the strategic recommendations which include the following areas:

- Executive leadership at the UMS level
  - Creation of the Chief Information Security Officer position and appropriate staffing.
  - The draft Information Security Policy will be presented at the January 2011 Board meeting for review and the final Policy will be presented for Board approval at the March 2011 Board meeting.
- Collaboratively update policy and standards
  - Complete the supporting standards for campus adoption by June 2011.
  - The proposed policy sections would including the following areas: security policy; organization of information security; risk assessment and treatment; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition; development and maintenance; information security incident management, business continuity management security; and compliance.
- System-wide user education
  - Develop and deploy the initial program by September 2011.
  - Deploy the complete role-based hierarchical training program by the start of the 2012-2013 academic year.
- Vulnerability scan
  - All campuses and UMS information technology scans will be completed by December 2010.
  - A rescan is scheduled for April 2011 to confirm remediation of high-impact vulnerabilities.
- Enhance central monitoring and response
Issue a Request for Proposal (RFP) for managed services externally and internally during the first quarter of 2011.
- Centralized IT assets at the campus level
- Recast IT as a service-oriented function

Mr. Dolicker outlined the critical success factors which should include the following:
- Information security policy, standards, objectives, and activities that reflect UMS objectives;
- An approach and framework for implementing, maintaining, monitoring, and improving information security that is consistent with the organization’s culture;
- Visible support and commitment from all levels of management;
- A good understanding of the information security requirements, risk assessment, and risk management;
- Effective marketing of information security to all faculty, staff, students, and other parties to achieve awareness;
- Distribution of guidance on information security policies and standards to all faculty, staff, students, and other parties;
- Provision to fund information security management activities;
- Providing appropriate awareness, training, and education;
- Establishing an effective information security incident management process;
- Implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement.

Trustee McCarthy reviewed the next steps and timeline. At the January Board meeting, the Board will receive an update on the Governance Model, Vulnerability Scan findings, preliminary review of the budget, preliminary review of the draft policy and standards, and a summary of additional changes in campus feedback. The final Plan will be presented to the Board for the March 2011 meeting for approval with a budget and timeline. Upon approval of the Plan, the UMS will move forward with the implementation to transition the Information Technology structure from an operating model to a service orientated model.

Adjournment

Ellen Doughty for
J. Kelley Wiltbank, Clerk of the Board