MINNESOTA STATE COLLEGES AND UNIVERSITIES
BOARD OF TRUSTEES
TECHNOLOGY COMMITTEE
MEETING MINUTES
June 22, 2011

Technology Committee Members Present: *David Paskach, Chair, Christopher Frederick, Vice Chair; Trustees, Jacob Englund, Philip Krinkie, James Van Houten and Michael Vekich*

Technology Committee Members Absent: *Trustees Cheryl Dickson,*

Other Board Members Present: *Scott Thiss, Board Chair, Chancellor James McCormick, Gail Olson, Thomas Renier and Louis Sundin*

Leadership Council Committee Members Present: *Vice Chancellor Darrel Huish and President Judith Ramaley*

The Minnesota State Colleges and Universities Technology Committee held its meeting on June 22, 2011, at Wells Fargo Place, 4th Floor, Board Room, 30 East 7th Street in St. Paul. Chair David Paskach called the meeting to order at 8:33 a.m.

1. **Minutes of April 19, 2011Technology Committee**
   Chair Paskach asked for clarification of the last paragraph in the minutes of May 18, 2011. The Minutes were approved following clarification of the last paragraph.

2. **Information Technology Update**
   Vice Chancellor Huish reported that the Information Technology Services (ITS) Division had little discretionary time the past month. ITS worked on several time-specific projects with June deadlines, including the implementation of the Statewide Integrated Financial Tools project (SWIFT), multiple Students First projects, a mandatory relocation of data center equipment from the seventh floor to the fifth floor and a significant upgrade to the instruction management system. At the same time, ITS was involved in shut down scenario planning both internally and with many of the business process owners. All of this activity occurred against the backdrop of keeping day-to-day technology available and functioning in order to serve campuses and students.

   Vice Chancellor Huish expressed appreciation for the many fine professionals throughout the system and within the ITS division that were productive during this challenging time.

   Trustee Krinkie inquired what happens in the event there is a state shutdown in regards to the SWIFT project. Vice Chancellor Huish responded that the SWIFT update has been deemed essential activity and will proceed as planned.

3. **Information Security Program Review**
   Vice Chancellor Huish introduced Information Security Specialist, John Hoffoss. John Hoffoss thanked the committee for the opportunity to speak about the security

program and shared a power point presentation. This presentation includes information on the information security drivers, program components and current security projects.

There are three primary drivers of security: the constantly shifting threat landscape which and requires vigilance and reprioritization; advances in technology; and compliance, which includes audit requirements, regulations, contractual agreements, policies and laws. The goals of the security program are to protect the confidentiality, integrity and availability of System information resources through information security leadership, strategies, tools, services and solutions. The second goal is to identify and mitigate information security risks to acceptable levels. The third goal is to promote information security throughout the information lifecycle. The drivers of security and goals are used to develop the security work plan.

One activity on the work plan is Payment Card Industry (PCI) compliance. There are over two hundred and fifty separate data security standard requirements, which must be applied at each point that accepts credit cards. This represents a significant effort by both the centralized and campus IT staff. PCI activity has become programmatic; as such, it will never be complete. As technology changes, so does the nature of threats and thus the compliance requirements. Contractual agreements require that the system conduct ongoing scans and other activities.

The security program includes efforts to provide leadership and governance. The Enterprise Security Steering Committee selects and directs system wide information security projects and initiatives. It provides leadership by developing metrics and policies and assists in audit compliance activities.

The security program also includes work in areas like security risk management, which includes functions like risk analysis and assessment, personnel security, and security awareness and training. Efforts in these areas have resulted in a formalized risk assessment process and implementation of assessment tools. The security team has also been involved in planning and preparing for data center penetration testing. A third party vendor attempts to access data, identifies vulnerabilities in the system and provides a report on the findings. The infrastructure and security staff addresses the findings. Chair Paskach inquired about the frequency or the reoccurring need for vulnerability testing. John Hoffoss responded that many studies suggest that penetration testing be conducted every other year. This allows time between tests to develop controls and address vulnerabilities. The system has additional internal processes that perform testing and addresses vulnerabilities on regular bases.

The Security Lifecycle is the third work area addressed by the security team. This is represented by activities like secure application development and deployment; asset management, access control; system protection and information integrity; operations, maintenance, incident response and disaster recovery.

The security team has made significant progress in the area of application security. This has been identified as an increasing area of vulnerability at the national level. Hackers are seeking out applications vulnerabilities to attack data systems and to install automated malware. Trustee Krinkie asked what hackers might be looking for. John Hoffoss explained that the hackers look for easy access to data.

Trustee Van Houten inquired how the system could assure that it is secure and how an audit might determine if the system had done everything needed. John Hoffoss responded that hackers are not willing to use a lot of time; all efforts are made to make sure that the system is secured. The security program is based on the research from the National Institute of Standards and Technology. This group develops many standards that are used across the industry, providing guidance and direction. The nature of security is to be ever vigilant and to never consider the system secure enough, as the threat landscape is always shifting.

Chancellor McCormick inquired who is responsible for protecting the financial data parents enter, the system or the Office of Higher Education. Chris Halling, System Director for Financial Aid, responded that both parties are responsible. When the families enter data into the federal system, the responsibility resides with the federal government's system; once an institution accepts the data it becomes the system's responsibility.

John Hoffoss stated that the application security task force have been developed to work with the developers to develop standards, promote best practices, provide training and other resources used to secure applications used thorough the systems and on individual campuses.

In the area of software and hardware security, IT has implemented a vulnerability management infrastructure to internally identify systems that are missing patches or configuration improvements. It also assists campuses with patch management solutions and remediation of issues.

In spite of all of these efforts, things may still go wrong. The system's last line of defense is the Incident Response Process. This process is used to identify malicious activities, stop the activity, investigate to see if there was any loss of data and help restore campus and/or system operations as quickly as possible.

Chair Paskach inquired if John Hoffoss would provide more information on Trustee Van Houten's question about how security works with audit. The security team works closely with Internal Audit to support efforts to identity findings and resolving them as quickly as possible. Historically the security team has been a small group that accomplishes many things. With the increases in resources, including staff in this area, the ability to provide technology practitioners with the support and resources needed has increased.

Trustee Van Houten inquired if the system has quick response plans for different technology areas. John Hoffoss affirmed that there is an Incident Response plan that describes forensic investigations. The security office supports campus technical staff in responding to incidents. A system guideline was developed to provide the campuses with the information needed to develop their own plans. When a campus identifies a breach, the Incident Response team assists in identifying data loss and determines the appropriate response.

Chair Paskach inquired how many people make up the security staff. John Hoffoss responded that the security team has five members plus the Director of Security Bev

Schuft, who retires at the end of the month. The search for a Chief Information Security Officer has begun.

4. 2011 Office of the Chancellor Performance Report- Technology Division

Vice Chancellor Huish presented the Technology Division's 2011 Office of the Chancellor Performance Report calling attention to the footnote below the financial and personnel data chart. Vice Chancellor Huish provided clarification on the chart stating that the previous year's Full Time Equivalent (FTE) was 191 authorized positions last year. The FTE at the beginning of this year is 174. This is a reduction of seventeen FTE. The technology budget in 2010 was 36.5 million; in 2011, it was 35 million and in 2012, the budget is about 34 million. This is a budget reduction of about 1.6 million in the last two years.

Vice Chancellor Huish highlighted the major accomplishments of the Information Technology Services (ITS) division. The vast majority of the ITS activities are for the campuses.

- Students First has dominated both ITS activity and accomplishments.
- In the data center and network area, the noteworthy accomplishment is that the last two semester start-ups have been exemplary in terms of network availability.
- The development and implementation of the application security and web based campus security program that is self-administered is a huge improvement in compliance efforts.
- Instruction Management system is running rock solid. 100-99% availability is fantastic.

Vice Chancellor Huish described the ITS work plan for the coming year, highlighting a few goals:

- Work will continue to advance the Service Delivery Strategy so that it may be used to in inform ITS decisions.
- ITS is beginning to develop measurements that can be used to assess the health of technology on the various campuses.
- Roll out of the Students First projects will be completed. ITS will continue to support implementation and other improvements to these projects.
- Tier one Help Desks will be consolidated to improve routing for users.
- Identity and Access Management will rollout and continue to be promoted.
- ITS embraces and looks forward to the evolution of shared services.

5. Students First Report

Jonathan Eichten, Director of Students First provided an update on each of the Students First projects, noting that the Single Search, Single Application and Single Registration projects are on schedule. The Student Loans Acceptance and Certification application has been rolled out to all campuses. The email component of the Communications Module has been implemented.

The Single Bill / Single Payment functionality is being piloted at Alexandria Technical Community College and Winona State University. Over two thousand students have used this new functionality to pay over 1.2 million dollars. Because so

many students attend more than one institution, over twenty-one institutions have received funds using this new application.

Jonathan Eichten reported that a video is being created that will promote the Students First initiative.

Trustee Frederick inquired on the progress of the Graduation Planner project. Jonathan Eichten reported that the Graduation Planner application is being tested in a small scale; until the next version of software is received, it cannot be fully tested.

6. Technology Committee Goals

Vice Chancellor Huish provided a review of committee goals. The trustees had heard a report on the Students First initiative. The second goal was to ensure that we were responsive to audit items and third goal was to develop a strategy for delivery of technology services.

Vice Chancellor Huish reported that in working together the goals have been accomplished.

Chair Paskach expressed his opinion that all three goals have been met and inquired if the trustees needed further discussion. In considering all IT has accomplished especially when one considers the Students First initiative and all the other tasks completed, it has been a great year.

7. Technology Committee Goal - Service Delivery Strategy

(Action)

Vice Chancellor Huish asked the trustees if they would formally recognize the completion of Service Delivery Strategy goal. Chair Paskach stated that this document provides the framework that will assist IT in developing the strategic plan. The plan is expected in the spring.

Chair Paskach inquired if there was a motion to approve the completion of the goals and the Service Delivery Strategy.

Trustee Vekich moved that the committee adoption of the following motion. Trustee Frederick seconded the motion, which carried with no dissent.

Recommended Committee Motion:

The Board of Trustees Technology Committee acknowledges the completion of the development of the Service Delivery Strategy.

Chair Paskach invited President Ramaley to comment on the Service Delivery Strategy. President Ramaley stated that the campus Presidents and Chief Information officers have expressed appreciation and support for the work completed by Vice Chancellor Huish and ITS.

Chair Paskach adjourned the Technology Committee meeting at 9:52 a.m.

Respectfully submitted,
Christine Benner