SUMMARY FOR OPERATIONAL IT COMMITTEE MEETING

DATE: April 17, 2014
TIME: 1:45-3 p.m.
LOCATION: Marriott Library, Eccles Executive Boardroom

IN ATTENDANCE:
Cathy Anderson    Michele Ballantyne    Martha Bradley    David Browdy
Tom Cheatham       Eric Denna           Cynthia Furse     Mary Parker
Mike Perez         Wayne Samuelson      Jim Turnbull       Raymond Tymas-Jones
Amy Wildermuth

COMMITTEE SUPPORT: Rene Eborn

UNABLE TO ATTEND:
Rich Brown        Alberta Comer          Gordon Crabtree    Patricia Hanna
Chris Ireland     Quinn McKenna         Mike Strong       Jeff West

ALSO IN ATTENDANCE:
Dan Bowden, Chief Information Security Officer
Steven Corbató, Deputy CIO, UIT
Mike Ekstrom, Director, Common Infrastructure Services, UIT

AGENDA ITEMS DISCUSSED:
• Discuss proposed new network security rules

Discuss proposed new network security rules

Eric Denna shared with OITC members that there is always a cost when there is risk. If the risk is not managed then the cost can be significant if the risk becomes reality. The challenge is deciding how much risk to assume and how much to mitigate. Mitigation typically comes in the form of restricting certain activities, requiring others to, or purchasing insurance. Often, managing risk with technology requires restricting or requiring certain activities, such as restricting access to certain Internet sites known to infect devices or requiring the use of passwords to access various services.

Committee members reviewed some of the potential risks that we are currently facing and discussed several areas for mitigation. After a detailed review of the risks, proposed solutions, and OITC suggestions regarding each, there was consensus to move forward with planning to safeguard our university.

There was general agreement to proceed on planning for universal device registration, gathering point of contact information, implementing configuration standards, developing a process for removing unsafe devices, implementing critical system monitoring, addressing compromised credentials, and unauthorized access. There was also general consensus and caution that these plans be addressed in less technical language as they are implemented, and to move forward with an inclusive change management and communication plan. University Information Technology team members will work on the draft rules and share them with the University Institutional Policy Committee.
<table>
<thead>
<tr>
<th>Action</th>
<th>Topic</th>
<th>Person/Group</th>
<th>Next step</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discussion/Agreement</td>
<td>Proposed information security rules</td>
<td>Eric Denna/ Dan Bowden/ Rene Eborn</td>
<td>The team will rewrite the security rules to incorporate OITC suggestions and make them less technical. They will share the rules with the IPC to begin the process for rule/policy approval.</td>
</tr>
</tbody>
</table>