The meeting was opened with a welcome from Jim Sibenaller. He introduced the new Information Security Officer, and Council Chair, Jim Pardonek. All then went around the table introduced themselves.

**Old Business**

**Approval of Minutes**
The agenda was presented and accepted by the group. It was noted that there were no minutes available from the last meeting.

**New Business**

**UISO Overview**
Jim Sibenaller presented a brief history of the staffing of the University Information Security Office (UISO) since its inception. This was to allow the team to have some background information on where the security program at the University has been and the direction the new ISO is taking. Jim Pardonek then presented a brief overview of the different security operations that are currently in place at the University Information Security Office.

**Vulnerability Assessment Status**
Jim Pardonek gave an overview of the 2012 security assessment noting that of the six systems reviewed there were 11 high priority vulnerabilities, 21 medium priority vulnerabilities, and 17 low priority vulnerabilities. These findings will next be reviewed first, in a meeting with our assessment vendor and then will be sent to the system owners for remediation.

**Network Liability Insurance**
Shauna was asked to give a brief overview of the network liability insurance that was purchased by the University to protect in the event of a large data breach whether it is printed or electronic data. This insurance has a $250,000 deductible although for any breach we must notify the insurance company and advise them of our steps.

**Policy Status**
Jim Pardonek gave an overview of where we are with policies.
First, a draft of the cloud computing policy was distributed to the team for a brief overview. Because of a pending contract with box however, a cloud storage provider, the cloud computing policy was fast tracked and sent to ITESC for approval.
Second, the decoupling of the hospital from the university showed a necessity to create a social media policy that describes the expectations of professional behavior that a student in one of our professional schools would be expected to maintain. A red line of the social media policy will be distributed to the team upon completion of an internal ITS review.
Third, for future policy review, it was proposed to the team that an enterprise review of all policies be performed along with a review of all working draft approvals.

**Security Breach Overview**
Jim Sibenaller did a brief overview of the two breaches that occurred over the last year. These breaches totaled
PII Program Update
Jim Pardonek gave a brief update of the PII program stating that the program schedule has been rearranged so that the scans can run a perpetual basis with a better alignment of the results submissions. Submissions are now due in July and December. Jim also mentioned that for Windows machines that the Identity Finder product was in full production and being used by the data stewards. Jim also noted that although we are still finding PII on devices having the ability to scan for them allows this data to be removed from the computers, noting that in the current scan cycle less than one half of one percent of the computers on campus are known to have PII on them. Corey asked the question as to whether or not the PII program will be extended to the new HSD at the Maywood campus. Jim Sibenaller stated that the project scope was created and that the PII process will be rolled out to the HSD campus following the opening of school in August.

2012 PCI-DSS Compliance Review
The next topic was the PCI DSS compliance review. Jim Pardonek mentioned that we've partnered with our vendor to streamline the process so that it will be easier to complete year-over-year, and that the documentation evidencing configuration correct collection processes are near completion.

Other New Business
Diane Hullinger mentioned a recent phishing e-mail that she had received and turned into the helpdesk and that she had not gotten a timely response as to whether this was a valid e-mail or not. Jim made note of this and agreed that a more timely response needed to occur in these situations.

Jim Sibenaller gave a brief overview of the ISAC charter and mission statement. The team was asked how often they wanted to meet, to verify the departments that are members of the team, and to verify the current membership and the membership roles. Based on this it was decided that the team would meet every other month and that in addition to the existing departments we would request representation from HSD and General Counsel. It was also discussed whether or not alternates should be allowed to attend the meeting when the primary is attending. This was left up to each department to decide who they would want to attend. However, it was noted that we do not want too many members at the meeting because of space and schedule requirements etc.

Next Meeting
The next meeting will be located at the Lakeshore campus, the room will be determined later. Tentative agenda item is an overview of the information security program, and a review of the 2012 security assessment. The meeting was adjourned by Jim Pardonek.

The meeting adjourned at 1:00pm.

<table>
<thead>
<tr>
<th>#</th>
<th>Task</th>
<th>Owner</th>
<th>Goal Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>