Information Security Advisory Council

Friday, April 11 2014
Student Union, Plemons (room 120)
Meeting Agenda

1. Review/Approval of Council Minutes

2. OIS Operations Report

3. Current University IS policies and need areas.


5. Best method for scheduling future ISAC meetings.

6. Other Business?
ITS-OIS Operations Report

- Regulatory compliance
- Attack detection
- Incident response
- Computer/network forensics
- Consultant/advising roles
- Example: HeartBleed
1. Review/Approval of Council Minutes

2. OIS Operations Report

3. Current University IS policies and need areas.


5. Best method for scheduling future ISAC meetings.

6. Other Business?
<table>
<thead>
<tr>
<th>Document Title</th>
<th>Type</th>
<th>Dept / Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus Guide</td>
<td>Guidelines</td>
<td>ITS - NICS</td>
</tr>
<tr>
<td>Clear Text Access</td>
<td>Procedure</td>
<td>ITS - NICS</td>
</tr>
<tr>
<td>Guidelines For Setting and Protecting Your Passwords</td>
<td>Guideline</td>
<td>ITS</td>
</tr>
<tr>
<td>Identity Theft Prevention Plan</td>
<td>Procedure</td>
<td>Comptroller</td>
</tr>
<tr>
<td>Information System Audits</td>
<td>Policy</td>
<td>Internal Audits</td>
</tr>
<tr>
<td>Network Registration Procedure</td>
<td>Procedure</td>
<td>ITS - NICS</td>
</tr>
<tr>
<td>Network Risk Assessment Policy</td>
<td>Policy</td>
<td>ITS - NICS</td>
</tr>
<tr>
<td>Document Title</td>
<td>Type</td>
<td>Dept / Unit</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>OpenServers VLAN Policy</td>
<td>Policy</td>
<td>ITS</td>
</tr>
<tr>
<td>PCI Policy</td>
<td>Policy</td>
<td>Comptroller</td>
</tr>
<tr>
<td>Remote Access Policy</td>
<td>Policy</td>
<td>ITS</td>
</tr>
<tr>
<td>Review of Research Involving Human Subjects</td>
<td>Policy</td>
<td>IRB</td>
</tr>
<tr>
<td>Router and Switch Security Procedure</td>
<td>Procedure</td>
<td>ITS</td>
</tr>
<tr>
<td>PCI Security Incident Communication Plan</td>
<td>Yes</td>
<td>Comptroller</td>
</tr>
<tr>
<td>Document Title</td>
<td>Type</td>
<td>Dept / Unit</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>--------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Statement of Confidentiality</td>
<td>Policy</td>
<td>ITS</td>
</tr>
<tr>
<td>Trusted Access Policy</td>
<td>Policy</td>
<td>ITS</td>
</tr>
<tr>
<td>Third Party Network Connection Agreement</td>
<td>Agreement / MOU</td>
<td>ITS</td>
</tr>
<tr>
<td>Use of Computers and Data Communications</td>
<td>Policy</td>
<td>ITS</td>
</tr>
<tr>
<td>VPN Policy</td>
<td>Policy</td>
<td>ITS</td>
</tr>
</tbody>
</table>
The primary deliverables of the Information Security Advisory Council work includes the following:

- A collaboratively developed **Information Security Plan** that defines strategic initiatives, objectives, and areas for continual improvement.
- A collaboratively developed **Security Awareness and Training Plan** that addresses key issues, needs, and concerns.
- A collaboratively developed set of proposed and/or ratified **Information Security Policies** that address the important information security needs of Appalachian State University.
Achieving Cohesion ....

Strategic Vision, Mission

Tactical Key Objectives

Operational Execution Plans

IS Policy

Gap + Risk Assessment

IS Plan
  Standards, Guidelines
  Key Initiatives & Improvements

IS Program
  Project Plans, Procedures, Practices, Roadmap
ISO 27002:2013: Information Security Policy

“At the highest level, organizations should define an “information security policy” which is approved by management and which sets out the organization’s approach to managing its information security objectives.”
ISO 27002:2013: Information Security Policy

“Information security policies should address requirements created by:

a) business strategy;

b) regulations, legislation and contracts;

c) the current and projected information security threat environment.”
ISO 27002:2013: Information Security Policy

“The information security policy should contain statements concerning:

a) definition of information security, objectives and principles to guide all activities relating to information security;

b) assignment of general and specific responsibilities for information security management to defined roles;

c) processes for handling deviations and exceptions.”
Next Steps?

- **Strategic**
  - Vision, Mission

- **Tactical**
  - Key Objectives

- **Operational**
  - Execution Plans

- **IS Policy**
  - Gap + Risk Assessment
    - Standards, Guidelines
      - Key Initiatives & Improvements
  - IS Plan
    - Project Plans, Procedures, Practices, Roadmap