**Requested Information for Upcoming Information Security Audit**

Needed in advance of the entrance meeting, if possible

1. Information Technology Organizational Chart
2. Information Technology Policies, Procedures and Standards on:
   * Information Security Program
   * Requesting access privileges
   * Acceptable Use
   * Remote Access (VPN) / Mobile Devices
   * Ownership and Classification Password Management
   * Vendor Management
   * Logging, Monitoring, and Data Archival
   * Incident Response
   * Server Room and Network Device Security

Needed at the beginning of the audit.

1. Documentation showing Information Technology Policies are reviewed and approved by management.
2. Meeting minutes and reports discussed during the last four IT Governance/oversight meetings.
3. A current network topology diagram (prefer in PDF format).
4. A listing of electronic alerts received in the last two weeks and documentation of system adjustments made as a result of your receiving alerts from security devices.
5. Documentation from your logging and monitoring activities for the last week. This includes lists of the types of events you note are of interest to you in your logging and monitoring procedure, and documentation of how you disposed / resolved each item.
6. A listing of each security incident report created in the last year.
7. A copy of the latest penetration / network vulnerability testing performed.
8. A listing of all persons currently being paid by the college.
9. A listing of new hires, terminations and transfer / promotions in the last 9 – 12 months.
10. Separate lists of active account names, the user to who the account is assigned and when the account was last used for:

* Network
* Banner
* Administrator Privileges
* A non-expiring password

1. A screenshot of the Active Directory Default Domain Policy and documentation of any other ways that policies are being enforced for both the network and Banner system access.
2. A system-generated listing of persons who have unrestricted key access to the server room.
3. Documentation showing that the hard drives on college-owned mobile devices are encrypted. .
4. Documentation showing controls that restrict data download to mobile devices.