IT Security-Related Roles and Responsibilities – Page 1 of 3

All members of the University community are responsible for safeguarding the University’s information and technology infrastructure, enabling the University to comply with its institutional and legal obligations for electronic data. This document describes the IT security roles and responsibilities for the Office of Information Technology and other related campus groups.

Senior Advisor for Information Security

Oversee the University’s Information Security Program
- Work with members of the University’s academic and administrative departments to define information security-related objectives that will enable the University to meet its legal, contractual and business-related requirements for data confidentiality, integrity and availability through the effective use of technology controls, procedural controls and information security awareness and educational objectives.
- Ensure that the University’s security-related objectives are being met.
- Continually assess the overall effectiveness of the information security program.

Coordinate the development and maintenance of the University’s Information Security Policy and ensure that it coordinates with other Information Technology Policies
- Working with the Office of the General Counsel and members of the University’s academic and administrative departments, define and maintain the University’s Information Security Policies regarding information classification, the proper handing of University information at all sensitivity levels, the rules for the issuance of computer accounts and the assignment of privileges, the definition of acceptable proof of identity for accessing information resources, who authorizes access to information, how authorization decisions are documented and enforced, and the process of responding to information security-related incidents.

Coordinate the development, maintenance and documentation of technology standards and procedures
- Work with IT development and support teams to confirm that technology-related standards and procedures effectively implement the University’s IT security-related policies in a cost-effective, practical manner.

Support Services

Provide IT Security products and services to the University community
- Research, recommend, install, configure, operate, maintain and monitor security-related products that satisfy the University’s information security-related objectives, such as:
  - Firewalls
  - Intrusion detection and prevention
  - Anti-malware
  - Security information and event management
  - Vulnerability analysis
  - Account provisioning/de-provisioning
  - Directory management
  - Cryptography
  - Enhanced authentication (e.g., Multi-Factor, Tokens, Biometrics)

-infrastructure Support Teams
- Research, recommend, install, configure, administer, operate, maintain and monitor hardware and software solutions that provide levels of security that ensure University data is protected in a manner commensurate with its confidentiality, integrity and availability requirements in the areas of:
  - File servers, E-Mail servers, Database servers, Web servers, Application servers, Monitoring devices, Backup servers, Print servers, New technologies.
- Effectively document the security procedures utilized by the group.

Senior Policy Advisor
- Coordinate and serve as OIT’s Representative to the University’s committee responsible for the maintenance of the University’s Core Information Technology Policy that defines the proper use of the University’s technology.
- Assist members of the University community in interpreting policy requirements.
- Coordinate the investigation and response to suspected computer abuse, information privacy violation and copyright infringement claims involving appropriate members of the University administration as necessary.
- Serve as a Process Manager, coordinating the University’s investigation of and response to the possible exposure of sensitive University information.
- Create a daily report of security-related incidents for the Director of the Department of Public Safety.

Support and Operations Center (Help Desk)
- Reset passwords
- Diagnose authorization problems.
- Manually update computer identities and privileges under the direction of the Person Office.
- When any situations arise that may involve the compromise of University systems or data, immediately initiate the University’s Possible Data Breach Response Plan.

Person Office (AIS)
- Manage the University’s central computer identity management function.
- Issue, correct, reset and disable computer accounts and privileges as required.

Application Development Teams (AIS and AS)
- Develop systems that satisfy the University’s information security-related goals and objectives.
- Utilize application development tools that effectively protect the integrity of the program code being developed, such as industry recognized version control systems.
- Ensure that application designs are effectively vetted through the OIT Architectural Review Board (ARB).
- Applications should include logging functions that track at a minimum unsuccessful access attempts and application administrative activity.

Academic Services and Administrative Information Services

- Manage the University’s central computer identity management function.
- Issue, correct, reset and disable computer accounts and privileges as required.

Other individuals and groups that perform IT Security Functions

IT Security Cross Functional Team
- The mission of the IT Security Cross Functional Team is to assist the University IT Senior Management in developing and maintaining an IT security strategy. The IT security strategy and the implementation of its component programs seeks to minimize risks to the University’s electronic information, to enable the University to comply with its institutional and legal obligations for electronic data, and to support the University’s mission.
- To support its mission, IT Security Cross Functional Team’s goals are to:
  - Create and maintain an inventory of IT security responsibilities.
  - Identify and document ongoing IT security-related initiatives across all OIT.
  - Identify and document potential, future IT security-related projects.
  - Identify cases where OIT and/or customer initiatives conflict with the IT Security Strategy, and investigate and propose alternatives.
  - Keep each other informed of the status of each OIT department’s IT security-related efforts.

- The membership of the team includes:
  - The Executive Sponsor of the IT Security Cross-Functional Team is Nadine Stern, the Associate CIO for Operations and Planning.
  - The team is chaired by Anthony Scaturro, the Senior Advisor for Information Security.
  - Additionally, the team includes representatives from each of the following OIT departments:
    - Academic Services
    - Administrative Information Services
    - Enterprise Infrastructure Services
    - Support Services.
Senior Advisor for Information Security

- Develop standards and procedures for the implementation, configuration, administration and monitoring of the above systems that are consistent with the University's IT security-related policies.
- Effectively document the security procedures utilized by the group.
- Participate in system and application design and implementation reviews to ensure that proposed solutions comply with the University’s policies and standards and technology best practices.
- Help support personnel assess the technology-related risks of their solutions and make recommendations for mitigating risk.
- Provide information about security-related technology solutions to OIT and our customers.
- Educate support staff in security best practices for configuring, administering, operating and monitoring technology solutions.

Security and Data Protection Team

- Recommend, install, configure, maintain and monitor University desktop and laptop workstation hardware and software solutions that provide levels of security that ensure University data is protected in a manner commensurate with its confidentiality, integrity and availability requirements.
- Ensure that department managers understand:
  - How the strategy relates to department objectives.
  - Who in the department should be used, and how the information should be used.
  - The impact of the classification.
  - The impact of the classification.

Enterprise Infrastructure Services

- Regularly review system activity logs to proactively uncover potential threats to University data and systems, and to ensure that operational and administrative controls are functioning appropriately.
- Review and authorize access requests beyond standard user access, e.g., highly privileged system access, access by outside contractors, access requiring tokens, certificates and other forms of enhanced authentication, and “special cases”, i.e., requests for non-standard access privileges.

Support Services

- Effectively document the security procedures utilized by the group.
- Analyze and recommend security policies and standards and procedures.
- Help support personnel assess the security-related risks of their solutions and make recommendations for mitigating these risks.
- Provide technical assistance to support staff to help them effectively implement security policies and procedures.
- Effectively document the security procedures utilized by the group.

Hardware and Software Support

- Implement best practices in application development, including the use of design and code reviews and data masking technology for the creation of test data sets where feasible.
- Ensure that department managers understand:
  - The importance of maintaining and implementing security policies and procedures.
  - How the security program relates to department objectives.
  - Who in the department should be used, and how the information should be used.
  - The impact of the classification.

Academic Services and Administrative Information Services

- Follow best practices in application development, including the use of design and code reviews and data masking technology for the creation of test data sets where feasible.
- Ensure that department managers understand:
  - The importance of maintaining and implementing security policies and procedures.
  - How the security program relates to department objectives.
  - Who in the department should be used, and how the information should be used.
  - The impact of the classification.

Other IT Security-Related Groups

- Each member of IT Security Cross-Functional Team is responsible for representing the various work groups within his or her department by:
  - Representing the concerns of the members of his or her department about the IT security program and individual IT security-related initiatives, as well as suggestions for program improvements.
  - Monitoring the progress of his or her department’s initiatives associated with the IT security strategic plan and providing the team with regular status reports.
- Serve as an IT security advocate, actively promoting IT security awareness to his or her department’s members and constituents.

Information Guardians and their Designees

- Classify the information that is associated with the Information Guardian in the areas of confidentiality, integrity and availability.
- Ensure that it is necessary to test with data that is a copy of confidential production data, the use of such data must be authorized by the appropriate Information Guardian and must be protected by the development teams to the same extent as production data is protected.
- Bring this issue to the attention of the Information Guardian and his or her department.
- Call the attention of the Information Guardian and his or her department.
- Bring the issue to the attention of the Information Guardian and his or her department.
- Bring the issue to the attention of the Information Guardian and his or her department.

May 4, 2012
# IT Security-Related Roles and Responsibilities – Page 3 of 3

All members of the University community are responsible for safeguarding the University's information and technology infrastructure, enabling the University to comply with its institutional and legal obligations for electronic data. This document describes the IT security roles and responsibilities for the Office of Information Technology and other related campus groups.

<table>
<thead>
<tr>
<th>Senior Advisor for Information Security</th>
<th>Security and Data Protection Team</th>
<th>Enterprise Infrastructure Services</th>
<th>Support Services</th>
<th>Academic Services and Administrative Information Services</th>
<th>Other IT Security-Related Groups</th>
</tr>
</thead>
</table>
| • Review departmental plans to implement third party products and services to ensure that their preferred solutions do not increase the risk of the University’s information being compromised. In cases where a preferred solution appears to increase risk, assist the department is selecting a more appropriate alternative. | • Advise other OIT and non-OIT support areas in the development of standards and procedures for:  
  o Servers and workstations  
  o Handheld devices  
  o Network equipment  
  o Databases  
  o Middleware  
  o Applications | | | |
| | | | | | **ID Card Office** |
| | | | | | • Issue, correct, reset and disable physical IDs and building access privileges. |
| | | | | | **Department Managers** |
| | | | | | • Ensure that staff members in the department understand the IT security requirements of the data they use. |
| | | | | | **SCAD/DCS Personnel** |
| | | | | | • Research, recommend, install, configure, maintain and monitor departmental workstations and server solutions that provide levels of security that ensure University data is protected in a manner commensurate with its confidentiality, integrity and availability requirements. |
| | | | | | • Effectively document the security procedures utilized by the group. |
| | | | | | • Promote IT security awareness in the University’s academic and administrative departments. |
| | | | | | **SCAD/DCS Computer Security Team** |
| | | | | | • Open to all members of the SCAD/DCS community, the team facilitates communication between OIT and SCAD/DCS regarding:  
  o The proposal and status of OIT security initiatives,  
  o Departmental security concerns and ideas.  
  o Opportunities for solution sharing.  
  o Educational opportunities. |
| | | | | | **Architectural Review Board (ARB)** |
| | | | | | • Review systems and applications being considered or being implemented at the University, providing guidance to the implementation team in best practices across a number of technology disciplines, including IT Security. |
| | | | | | **Residential Computing Consultants (RCC)** |
| | | | | | • Assist students in securely configuring and maintaining their computing devices. |
| | | | | | • Promote IT security awareness among the student population. |

**Promote security awareness and education**

• Convey security-related policies and procedures to our customers utilizing a variety of communication vehicles, e.g., Web content, presentations, articles in IT periodicals, product demonstrations, e-mail, posters, video, etc.

• Develop and manage the University’s information security awareness program for members of the University community.

• Assist the University Communications area as necessary in the development of responses to media requests

**Lead cross-functional IT security projects**

• Manage information security-related projects as needed.

• Coordinate the University’s response to information security-related audit findings and requests made by law enforcement agencies and court-issued subpoenas as they relate to the investigation of information security-related incidents.

**Provide technology forensic services**

• Perform technical investigations of suspected system compromises  
  • Provide technical support, as needed, to law enforcement agencies that have been appropriately authorized.

**Support cross-functional IT security projects**

• Participate in security-related projects as needed.

**Support the Security Assessment Process**

• Research, recommend, install, configure, maintain and operate software products that can detect:  
  • Improperly configured servers  
  • Application program code weaknesses.  
  • The location of personally identifiable information and other confidential data types.

**Telephone Services**

• Investigate and recommend methods of securing mobile phones.  
  • Manage University-owned mobile phones.  
  • Participate in the Data Breach Response process by assisting users in remotely erasing devices that have been lost or stolen.

**Student Computing Group**

• Maintain student computing clusters that provide a high level of security to ensure that data is not compromised across sessions.  
  • Design and deliver standard, secure workstation configurations as part of the Student Computing Initiative program.  
  • Provide an effective, compliant e-business site for students to securely place their computer orders.  
  • Promote IT security awareness among the student population.

**Research, recommend, install, configure, maintain and monitor departmental workstations and server solutions that provide levels of security that ensure University data is protected in a manner commensurate with its confidentiality, integrity and availability requirements.**

**Effectively document the security procedures utilized by the group.**

**Promote IT security awareness in the University’s academic and administrative departments.**

**Open to all members of the SCAD/DCS community, the team facilitates communication between OIT and SCAD/DCS regarding:**

**The proposal and status of OIT security initiatives,**

**Departmental security concerns and ideas.**

**Opportunities for solution sharing.**

**Educational opportunities.**

**Review systems and applications being considered or being implemented at the University, providing guidance to the implementation team in best practices across a number of technology disciplines, including IT Security.**

**Assist students in securely configuring and maintaining their computing devices.**

**Promote IT security awareness among the student population.**

May 4, 2012