Information Security Program Roles and Responsibilities Policy D 108

This policy defines the roles and responsibilities of those functions that are responsible for the implementation of the Information Security Program.

Security Functions

- Internet Security Officer (ISO)
  - Overall responsibility for ensuring the implementation, enhancement, monitoring and enforcement of the information security policies
  - Coordinates the development and implementation of Information security policies, standards, procedures, and other control processes that meet the business needs of the University
  - Develops, deploys, and maintains an information security architecture that that meets the current and future business needs of the University.
  - Provides consultation services to computing and business operations and recommends methods to mitigate security risks
  - Coordinates the development and implementation of a training and awareness program to educate University employees, contractors, and vendors with regard to the University’s security requirements
  - Investigates breaches of security controls, and implements additional compensating controls when necessary
  - Supervises and coordinates with the security administrator to ensure that security measures implemented meet the requirements of the security policy.
  - Reviews and approves all external network connections
  - Manages security incidents and file mandatory reports to SUNY, CSCIC, and other agencies as required by the incident
  - Ensures that appropriate follow-up is conducted for security violations
  - Be aware of laws and regulations that could affect the security controls and classification requirements of the University’s information

Functions of the Information Security Steering Committee

- Composition of this committee must include individuals that have responsibility for the protection of information and have the necessary skills to understand and implement policies relating to the Security Program.
- Provides approval of new or modifications of existing security policies
- Advises the ISO on all matters relating to the protection and use of information assets
- Approves major initiatives to enhance security
- Communicates the Security Program to the campus
- Formally assign duties of security responsibilities
• Implements a security awareness program
• Monitors significant changes in the exposure of information assets
• Coordinates the creation of a security incident management team
• Develops a process to measure compliance

**Roles and Responsibilities for Guardians of Information**

- **Information owner** – An individual or group responsible for the data under their control. They determine appropriate access rights and communicate with the ISO for disclosure requests (legal)
- **Security Administrator** – Responsible for administering security tool, reviewing security practices, identifying and analyzing security threats and solutions, and responding to security violations
- **IT Management** – Responsible for the data processing infrastructure and computing network which support the information owners.

**INQUIRIES/REQUESTS:**

Chair, Information Security Steering Committee

Office of the Chief Information Officer
ECC 231