University of South Carolina
Security Liaisons

Overview

A successful information security program relies on the shared responsibilities of many individuals within the organization to safeguard University assets and resources. Security Liaisons can play a vital role that assists the University in cybersecurity related activities, strategies, and best practices to keep the enterprise and its assets secure.

Selection

In accordance with IT 3.00, each UofSC Organizational Unit (OU) must have a designated Security Liaison who works in conjunction with members of the University Information Security Office (UISO). The designated Security Liaison will be a conduit for communication between the UISO and their represented OU with the purpose of identifying, reducing, and addressing risks with the OU and strengthening the overall information security program for the university.

Recommended Skills

- An effective communicator using written and verbal communication skills to work effectively with a wide range of individuals in a diverse community.
- Ability to use “soft skills” to collaborate, build, and foster strong work relationships.
- Capable of understanding a broad range of technical concepts, cyber security technologies, solutions, and processes.

Roles and Responsibilities

- Serve as the central point of contact for information security incidents and collaborate with members of UISO to respond to security incidents and vulnerabilities within the assigned OU.
- The incumbent should be familiar with the assigned OU’s IT assets, workflows, operational and programmatic processes.
- Ensure that internal information security measures take into consideration any unique data or research needs of the represented OU.
- Be knowledgeable of information security best practices, trends, and relevant frameworks in accordance with applicable UofSC policies, programs, technical standards, and initiatives.
- Actively champion an environment that promotes security awareness best practices and strategies for all stakeholders within the OU.
- Be an active participant on the Information Security Committee.
- Completion of the annual Information Security survey for the assigned OU.