UNIVERSITY OF SOUTH CAROLINA
Division of Information Technology

University Information Security Office

Information Security Training and Certification for IT Staff - Guidelines

Issued Date: 16-Jan-2014

Effective Date: 16-Jan-2014

Purpose

This document establishes expectations for information security training of IT staff employed by the University. It is critical for IT staff to understand information security topics and techniques in order to properly protect University IT assets.

These Guidelines may at some future date become requirements.

Scope

These Guidelines apply to all University units who have staff members with principal duties in IT.

Who Should Be Trained

Ideally all IT staff should have some amount of information security training. But at a minimum, any University unit that has been identified for representation on the Data Procedures Advisory Committee (DPAC) must designate an IT staff member to serve as their primary security contact (per University Policy IT 3.00, section II.A.7) and that security contact should receive appropriate training as described below.

It is expected that IT staff members who receive training will share this knowledge as appropriate with their peers.

Recommended Training and Associated Certifications

IT staff members who have duties in any of the following areas should have training as indicated. The associated certification for a training course is not required, but may be accepted as proof of competency when considering job applicants.

Security Contact

For a unit's designated Security Contact, who serves as liaison between unit staff and the UISO.

Minimum: SANS SEC301, Intro to Information Security (Certification: GISF)
Also Consider:
- SANS SEC401, Security Essentials Bootcamp Style (Certification: GSEC)
- CompTIA Security+
- Microsoft Security Fundamentals
- Red Hat Certified Security Specialist

IT Management

For any staff member whose duties include coordination of IT deployment, operation, or support.

Minimum, year 1: SANS SEC301, Intro to Information Security (Certification: GISF)
Minimum, year 2: SANS SEC512, Security Leadership Essentials for Managers (Certification: GSLC)
Also Consider:
- SANS SEC401, Security Essentials Bootcamp Style (Certification: GSEC)
- CompTIA Security+
- Microsoft Security Fundamentals
- Red Hat Certified Security Specialist
- SANS SEC501, Advanced Security Essentials, Enterprise Defender (Certification GCED)
- SANS MGT414, +S Training for CISSP (Certification: CISSP)
- ISACA CISM, Certified Information Security Manager

Server Support

For any staff member whose duties include administration of server computers.

Minimum, year 1: SANS SEC401, Security Essentials Bootcamp Style (Certification: GSEC)
Minimum, years 2-3:
if supporting Windows platforms: SANS SEC505, Securing Windows and Resisting Malware (Certification: GCWN)
if supporting Linux platforms: SANS SEC506, Securing Linux/Unix (Certification: GCUX)
Also Consider:
CompTIA Security+
Microsoft Security Fundamentals
Red Hat Certified Security Specialist
SANS SEC501, Advanced Security Essentials, Enterprise Defender (Certification GCED)
SANS MGT414, +S Training for CISSP (Certification: CISSP)

Desktop/Laptop/Mobile Support

For any staff member whose duties include administration of desktop computers, laptop computers, or mobile devices.

Minimum, year 1: SANS SEC464, Hacker Guard: Security Baseline Training for IT Administrators and Operations with Continuing Education and SANS SEC301, Intro to Information Security (Certification: GISF)
Minimum, year 2: SANS SEC401, Security Essentials Bootcamp Style (Certification: GSEC)
Also Consider:
SANS SEC505, Securing Windows and Resisting Malware (Certification: GCWN)
SANS SEC506, Securing Linux/Unix (Certification: GCUX)
SANS SEC575, Mobile Device Security and Ethical Hacking (Certification: GMOB)
CompTIA Security+
Microsoft Security Fundamentals
SANS SEC501, Advanced Security Essentials, Enterprise Defender (Certification GCED)

Database/Application Support

Duties include support of database systems (e.g. Oracle, MSSQL, MySQL) or web applications.

Minimum, year 1: SANS SEC401, Security Essentials Bootcamp Style (Certification: GSEC)
Minimum, year 2: SANS DEV522, Defending Web Applications Security Essentials (Certification: GWEB)
Also Consider:
SANS AUD445: Auditing Security and Controls of Oracle Databases (Certification: none)
SANS SEC505, Securing Windows and Resisting Malware (Certification: GCWN)
SANS SEC506, Securing Linux/Unix (Certification: GCUX)

Obtaining Training and Certification

UISO has purchased training credits from SANS, and has committed to providing one (1) SANS training course for each department that has representation on the DPAC. Usage of these credits should be requested by the department's DPAC representative or department head.

UISO does not have credits to cover certification testing attempts. It is recommended that employees who seek certification request preauthorization from their department, and that the department reimburse the testing fee upon successful completion.

Related Documents

University Policy IT 3.00 – **http://www.sc.edu/policies/it300.pdf**

Contacts

http://security.sc.edu

Revision History

Author	Date	Comments
Jeff Whitson	11-Dec-2013	training specifications

Author	Date	Comments
David Wilhite	16-Jan-2014	certification association and formatting