The University of the South
IT Security Awareness Training Policy

Purpose

The quality and integrity of the University of the South's security awareness training ensures that the workforce members (exempt, non-exempt, temporary), including management of the University's information systems, understand the security implications of their actions. This policy sets out the training that will increase the likelihood that information system security will not be breached, either intentionally or unintentionally, through technical measures (such as hacking) or non-technical measures (such as social engineering).

Scope

The policy applies to all employees of the University of the South, including all temporary, exempt, non-exempt, part-time, or student employees granted access to University information technology resources.

Responsible Party

The Associate Provost of the Library and Information Technology Services division of the University is responsible for maintaining this policy and may be contacted with any questions.

Definitions

Term	Definition
Security information assets	Assets that generally include hardware (computers, phones or servers), software and applications with confidential information
Security awareness program	Program that explains and supplies University employees the knowledge and attitude they need regarding the protection of the physical and information assets of the University
Security tools	A general phrase used to describe any software that provides security for a computer or network
SANS module	Online source for information security training that all employees are required to complete

Policy Statement

All employees of the University of the South are required to participate in security awareness training within thirty days of starting employment and thereafter on an annual basis. Additional training beyond the general training will also be required for some departments and some job duties. Examples of such departments include IT, the Wellness Center, Financial Aid and the Treasurer's Office. Examples of job duties include those handling credit cards such as cashiers.

Security Training will be ongoing at The University of the South and employees will be kept up to date on new improvements or threats to watch out for. This information will be distributed by email, posters, work newsletters, or meetings.

Consequences

All University of the South employees are expected to abide by this policy. Violations of this policy will be treated like other allegations of wrongdoing at the University of the South. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for noncompliance may include, but are not limited to, one or more of the following:

a. Disciplinary action according to applicable University policies;
b. Termination of employment; and/or suspension of University network accounts (Banner, Email, etc.).

Responsibilities

a. The University will provide mandatory security modules through the online SANS program.
b. All employees will complete the SANS modules annually and within 30 days of hire.
c. The University will provide up to date information on new security threats in the form of newsletters, email, or weblinks.

Procedures

Security tools are a vital part of our information security framework but do not alone provide for the security of the University's information assets. To have a secure and effective environment, awareness and proactive support is required of all employees. Without security awareness training, employees are less likely to recognize or react correctly to security threats and more likely to expose information assets through ignorance and carelessness. In order to protect important information assets, all employees must be informed about threats, kept current on security matters and motivated to do their part in fulfilling security obligations through the following procedures:

a. All University employees will be required to participate in completing the basic supplied SANS (Securing the Human) module.
b. Additional training may be provided for employees with special obligations toward information assets that are not covered in the SANS module. The particular training will reflect employee's job requirements.

REVISION DATE: August 24, 2021