Division of Information Technology

Information Security Awareness Training Standard

Executive Sponsor:
Associate Vice President for Information Technology/CIO

Responsible Office:
Information Security

Issued: 8/2016
Revised: 12/2019
Reviewed: 12/2021

I. Standard Statement

This standard defines the requirements and procedures for Information Security Awareness training which has been established as part of the Information Security Program described in the Information Security Policy.

II. Reason for Standard

The University of Scranton is committed to protecting the confidentiality, integrity, and availability of its information and technology assets. Formal Information Security Awareness training will aid employees in the protection of the data entrusted to the University by providing information and instruction related to both risks and best practices for handling this data. Formal training is also a requirement by some regulations, such as Payment Card Industry Data Security Standards (PCI-DSS).

III. Entities Affected By This Standard

This standard applies to the following University employees:

A. BANNER users with access to forms and reports containing restricted data elements
B. Employees who store, process, or transmit consumer credit and debit card transactions
C. Information Technology Personnel

IV. Website Address for this Standard

https://www.scranton.edu/information-technology/policies.shtml

V. Related Documents, Forms, and Tools

Information Classification & Protection Policy

Information Security Policy

Credit Card Handling Security Standards

BANNER Access Procedure

VI. Contacts

For more information, please contact the Information Security Office at 570-941-4226 or email infosec@scranton.edu.

VII. Definitions

PCI-DSS: Payment Card Industry Data Security Standards, a proprietary information security standard for organizations that handle branded credit cards from the major card schemes.

VIII. Responsibilities (required)

Information Security Office (ISO): Responsible for establishing an Information Security awareness training program. The Information Security Office will ensure that all applicable employees have completed training.

IT Training Specialist: Responsible for assisting the ISO in the development of training materials/systems and the administration of training content.

Applicable Employees: Responsible for the completion of the training program established by the ISO.

IT Database Management Services: Responsible for verifying an employee has received the required training before granting access to restricted data within the BANNER system.

IX. Procedures

1. On an annual basis, the ISO will review the training program and make adjustments to content as required by regulations or recommended based on evolving threat landscapes.
2. Employees covered by this standard will be required to complete security awareness training on an annual basis.
3. Employees covered by this standard will be required to complete the assigned training in order to maintain access to data and/or as required by their job function.
4. Employees requesting access to restricted data in the BANNER system for the first time will complete the training prior to receiving access, following the process defined in the BANNER Access Procedure.
5. On an annual basis, the ISO will verify that all employees covered by this standard have completed the required training.

X. Appendix (optional)