Information Security Awareness Training

Contents

Revision History

Standard	Effective Date	Email	Version	Contact	Phone
OIT-ISAT		strevena@csustan.edu	1.0	Stan Trevena	209.667.3137

Executive Summary

Stanislaus State is highly diversified in the information that it collects and maintains on its community members. It is the university's responsibility to be a good steward and custodian of the information that it has been entrusted, which must be upheld by all members of the university. The overall protection of the data assets must begin with the individual who has access to them. Approved by all labor unions, CSU Policy Number 8035.0 states "all employees with access to protected data and information assets must participate in appropriate information security awareness training" on a periodic basis. Information security training will be required annually. The campus information security awareness program will promote campus strategies for protecting information assets containing protected data. The Information Security Awareness Training Standard defines the requirements for training of any individuals who handle sensitive information for the campus. This standard of due care will help prevent the unauthorized access, modification, and loss of sensitive campus information.

Introduction and Purpose

This Information Security Awareness Training standard defines the requirements for training of any individuals who handle sensitive information for the campus. This standard of due care will help prevent the unauthorized access, modification, and loss of sensitive campus information.

Scope

As required by ICSUAM8035, this standard applies to all Stanislaus State, Self-Fund, and Auxiliary ("campus") employees, faculty and staff, including student assistants.

Standard

Training Schedule

Information Security Awareness Training shall be administered to all employees who handle sensitive information for the campus at time of employment and bi-annually thereafter.

Training Assignment

All required information security training for employees who handle sensitive information for the campus will be assigned by the Office of Information Technology (OIT) and Human Resources. Individuals will have 90 days to complete the training, once assignment has been made. If training is not completed in the required timeframe, the Information Security Officer (ISO) shall issue a report to the appropriate Vice President's Office and access may be revoked.

Incomplete Training

Reports of individual failure to complete the mandatory training will be delivered to the AVP of OIT. OIT reserves the right to terminate system access to individuals found to be negligent of required security awareness training.

Training Requirements

Mandatory Training for all individuals

Each individual who handles sensitive information for the campus shall complete a mandatory bi-annual information security awareness and Family Education Rights and Privacy Act (FERPA) training program. Information Security training will be administered by Human Resources in Coordination with OIT. FERPA training will be administered by Human Resources.

Payment Card Industry (PCI) Training

Any individuals who handle credit cards will be issued an annual PCI training. Training for PCI is based on job duties of the individual.

Health Insurance Portability and Accountability Act (HIPAA) Training

Any individuals who have access to medical records will be issued an annual HIPAA training, to be administered by Human Resources as appropriate. Training for HIPAA is based on job duties of the individual.