University of San Diego
Information Security Program Outline

Background

The University of San Diego is required by the Gramm–Leach–Bliley Act ("GLBA") and its implementing regulations at 16 CFR Part 314, to implement and maintain a comprehensive written Information Security Program ("ISP") and to appoint coordinators for the program. The objectives of the ISP are to (1) ensure the security and confidentiality of covered information; (2) protect against anticipated threats or hazards to the security and integrity of such information; and (3) protect against unauthorized access or use of such information that could result in substantial harm or inconvenience to customers.

Related Policies

This ISP is in addition to existing university policies and procedures that address various aspects of information privacy and security, including but not limited to, Family Educational Rights and Privacy Act (FERPA), Policy Prohibiting Illegal, Dishonest or Fraudulent Conduct, Policy on Responsible Use of University Computing Resources, procedures applicable to PCI DSS (Payment Card Industry Data Security Standards), Cash & Treasury Procedure 3.0, Credit Card Operational Procedures and Information Security Requirements and additional procedures referenced therein.

ISP Coordinator

University of San Diego has designated the Vice Provost and CIO as its ISP Technical Coordinator and the Controller as the ISP Functional Coordinator. The Coordinators may designate other individuals to oversee and/or coordinate particular elements of the ISP.

Covered Information

"Covered information" means nonpublic personal information about a student or other third party who has a continuing relationship with the university, where such information is obtained in connection with the provision of a financial service or product by the university. Nonpublic personal information includes students or other 3rd party's names, addresses and social security numbers as well as financial information. Covered information does not include records obtained in connection with single or isolated financial transactions such as ATM transactions or credit card purchases.

Elements of the ISP

	ISP Technical Coordinator	ISP Functional Coordinator
Risk Identification and Assessment	University of San Diego intends through its ISP to identify and assess external and internal risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The ISP Technical Coordinators will provide guidance to appropriate personnel in the administrative, academic, and other university units in evaluating their current practices and procedures and in assessing reasonably anticipated risks to covered information in their respective areas. Each ISP Coordinator will work with appropriate personnel to establish procedures for identifying and assessing risks in the following technical and functional areas.	University of San Diego intends through its ISP to identify and assess external and internal risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The ISP Functional Coordinators will provide guidance to appropriate personnel in the administrative, academic, and other university units in evaluating their current practices and procedures and in assessing reasonably anticipated risks to covered information in their respective areas. Each ISP Coordinator will work with appropriate personnel to establish procedures for identifying and assessing risks in the following technical and functional areas.
Employee Training and Management	The ISP Technical Coordinator will work with the appropriate personnel to maintain employee training and management procedures relating to the access and use of covered information. Signed confidentiality statements will be executed annually for all ITS staff with privileged account access to enterprise systems. University employees who relinquish their account credentials are required to complete computer security awareness training at the ITS Help Desk.	The ISP Functional Coordinator will coordinate with the appropriate personnel to evaluate the effectiveness of current employee training and management procedures relating to the access and use of covered information.
Information Systems	The ISP Technical Coordinator will coordinate with the appropriate personnel to assess the risks to covered information associated with the university's information systems, including network, applications and databases as well as information processing, storage, transmission and disposal.	
Detecting, Preventing & Responding to Attacks & System Failures	The ISP Technical Coordinator will coordinate with the appropriate personnel to evaluate procedures for and methods of detecting, preventing and responding to attacks, intrusions or other system failures. This will include	The ISP Functional Coordinator will coordinate with the appropriate personnel to evaluate procedures for and methods of detecting, preventing and responding to attacks, intrusions or other system failures.

	annual penetration and vulnerability testing conducted by an IT Security firm, as well as quarterly internal vulnerability scans conducted by ITS Systems/Security staff.	
Designing and Implementing Safeguards	The ISP Technical Coordinator will coordinate with appropriate personnel to design and implement safeguards, as needed, to control the risks identified in assessments and will develop ongoing monitoring and alert tools as effective safeguards. Such safeguards may be accomplished through existing network monitoring and problem escalation procedures.	The ISP Functional Coordinator will coordinate with appropriate personnel to design and implement safeguards, as needed, to control the risks identified in assessments and will develop a plan to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

Overseeing Service Providers	The ISP Technical Coordinator, in conjunction with the Office of the General Counsel and with University Procurement, will assist in instituting methods for selecting and retaining service providers that are capable of maintaining appropriate safeguards for covered information. The ISP Coordinator will work with the Office of the General Counsel to develop and incorporate standard, contractual provisions for service providers that will require those providers to implement and maintain appropriate safeguards. These standards will apply to all existing and future contracts entered into with service providers to the extent required under GLBA., The review of Service Providers will be determined through (1) the Review and Identification of Critical Systems Policy, and (2) an annual memorandum summarizing the University Finance and ITS Review of Critical Systems (done annually).	The ISP Functional Coordinator, in conjunction with the Office of the General Counsel and with University Procurement, will assist in instituting methods for selecting and retaining service providers that are capable of maintaining appropriate safeguards for covered information. The ISP Coordinator will work with the Office of the General Counsel to develop and incorporate standard, contractual provisions for service providers that will require providers to implement and maintain appropriate safeguards. These standards will apply to all existing and future contracts entered into with service providers to the extent required under GLBA. The review of Service Providers will be determined through (1) the Review and Identification of Critical Systems Policy, and (2) an annual memorandum summarizing the University Finance and ITS Review of Critical Systems (done annually).

Adjustments to Program

The ISP Coordinators will evaluate and adjust the ISP as needed, based on the risk identification and assessment activities undertaken pursuant to the ISP, as well as any material changes to the university's operations or other circumstances that may have a material impact on the ISP.