California State University, Northridge

Information Security Plan

October 2014

REVISION CONTROL

Document Title:	CSUN Information Security Plan
Author:	Chris Olsen

History

Date	Owner	Summary of Action(s)
12/31/2007	Clifford R. Maraschino/ ISO	Created Original Draft
3/1/2012	Chris Olsen/ ISO	Updates to various sections to bring current. Major updates made to the 'Priorities for Action' section.
5/15/2012	Chris Olsen/ ISO	Reviewed and received approval for the IS Plan with the President and President's Cabinet.
12/2013	Chris Olsen/ ISO	Reviewed highlights of IS plan with new university President and Vice President of Information Technology/CIO. This was an interim step taken while developing the annual plan.
3/2014	Chris Olsen/ ISO	Updated the IS Plan for 2014/2015
7/18/14	Kevin Krzewinski	Updates to IS Plan
9/1/14	Hilary Baker	Updates to IS Plan
10/1/2014	Kevin Krzewinski	Minor formatting updates

Table of Contents

I. Introduction

California State University, Northridge (CSUN) is committed to providing a secure and accessible data and networking infrastructure that protects the confidentiality, availability and integrity of information.

The creation, preservation and exchange of information is an intrinsic part of the University's teaching, scholarship and administrative operations. Increasingly that information is processed, handled or stored in electronic form. The growing availability of digital information offers opportunities to improve our collaborations and work in new ways. Unfortunately, it also presents us with new threats. The very technologies we use to gather, share and analyze information also make our institution vulnerable to varied and continually evolving information security risks.

CSUN is entrusted with a wide range of confidential and sensitive information pertaining to our students, faculty staff, donors, and other members of the community (e.g. affiliates). We take seriously our obligation to be stewards of that trust. We are obligated by law and institutional policy to take all reasonable and appropriate steps to protect the confidentiality, availability, privacy, and integrity of information in our custody. This obligation is broad and applies to information in both electronic and material form. Our practices are designed both to prevent the inappropriate disclosure of information and to preserve information in case of intentional or accidental loss.

A. Guiding Principles

The University's strategy is multi-faceted and must continue to evolve to meet an ever-changing threat. At the core, the plan is designed to uphold the following principles:

- The University protects the *privacy of student, employee, and affiliate records* by ensuring the security and protection of confidential and sensitive information in its custody, whether in electronic, paper, or other forms.
- *Proper organizational structures and strategies to assure adequate controls and risk assessment are* a necessary part of protecting the privacy and confidentiality of information systems. Risk is a fact of life for any organization that must maintain the confidentiality of collected data, whether it is online or consists of paper files. Risk management must include analysis to avoid unnecessary efforts and expenses. Risk is managed on an ongoing basis, as the environment changes, new technology is released, user requirements evolve, or cost-risk factors are further analyzed. Adequate controls not only help mitigate risk but generally correspond to best business practice in assuring transparency and consistency of business processes and effectiveness and availability of underlying technologies.

- The continuing *education and awareness* of the faculty, students, and staff on information security issues is a critical factor in minimizing information security risk overall. In particular, as the University refines its guidelines and procedures for maintaining the confidentiality of information that is deemed highly sensitive, employees who handle this data need to be provided appropriate and periodic training on approved procedure.

B. Scope of the Information Security Plan

This Information Security Plan applies to all information that is acquired, transmitted, processed, stored, and/or maintained by CSUN or any CSUN auxiliary organization, whether in digital or paper format. It encompasses all locations in which CSUN information resides including the main campus, remote campus work areas, and hosted environments. It applies to all CSUN faculty, students, employees, consultants, contractors, and any person having access to University information in any form or format.

Information Security plays a leading role in safeguarding the University's protected data and related systems. However, information security planning and assurance cannot be successfully accomplished solely within the IT division; therefore, the plan outlines the responsibilities of CSUN organizational units and the intersecting responsibilities of other CSUN departments and individuals.

C. About this Document

The remainder of this document summarizes CSUN's current plan to maintain the security of its information assets. It conveys both long-term strategies and near-term activities we are pursuing to improve our overall information security environment. The plan is presented in five sections:

- Roles and Responsibilities
- Information Security Policies and Standards
- Risk Assessment and Mitigation
- Securing the CSUN Technical Infrastructure
- Priorities for Improvement –2014-2015

The document includes in an appendix a glossary of common information security terms.

II. Roles and Responsibilities

The University assumes a *coordinated approach* to the protection of information resources and repositories of confidential information that are under its custody by establishing appropriate and reasonable administrative, technical and physical safeguards that include all individuals, related units, and others that administer, install, maintain, or make use of CSUN's computing resources and other depositories of information.

At CSUN, that coordinated approach includes the following administrative structures and responsibilities:

The **Vice President for Information Technology and Chief Information Officer** (VP/CIO) is responsible for the development and implementation of policies and practices that maintain CSUN's information security and ensuring a periodic review of institutional risks and vulnerabilities. The VP/CIO discusses information security findings and required actions with University leadership, including an annual review of the Information Security Plan (Plan) with the University President and President's Cabinet.

The **Information Security Officer** (ISO) is responsible for: the development, maintenance, and periodic update of the campus Information Security Plan; the campus-integration, coordination and interpretation of CSU-wide Information Security policies and standards; and development and implementation of more specific guidelines and procedures to support those policies and standards with the particular context of CSUN.

Other ISO duties include:

- Recommend new guidelines, tools, and practices to enhance CSUN's Information Security posture.
- Coordinate campus IS Risk Assessment.
- Keep current with relevant threats against the campus.
- Deliver targeted Awareness Training seminars in addition to ensuring faculty, staff and student workers complete the online Awareness Training.
- Facilitate information security planning that promotes secure practices and decreases risk to information and data systems.
- Maintain campus procedures, standards, and guidelines in adherence with CSU information security policies
- Identify and coordinate remediation of weaknesses in CSUN's infrastructure, data systems, and applications.

The Computer Security Incident Response Team (CSIRT), responds to serious CSUN Information Security incidents, and works with the VP/CIO and ISO to identify incident-remediation plans and makes recommendations to the President and President's Cabinet on how to reduce future risk and strengthen CSUN's security posture.

Academic and administrative managers including Vice-Presidents, Deans, Associate Deans, Managers of Academic Resources, Department Chairs, Directors and Managers also play an important role in the overall information security strategy. They are responsible for

understanding the importance of managing information security risks both within their organizations and across the campus as a whole, and are ultimately responsible for the protection and use of data/information within their organization. They set an example and establish a tone in their organizations that stresses the importance of information protection, compliance and awareness. They are responsible for classifying, defining controls, authorizing access, monitoring compliance with CSU/campus security policies and standards, and managing risks associated with information assets under their protection. Finally, they are responsible for working with the ISO to mitigate vulnerabilities in their areas and to collaboratively implement good information security practices.

Campus technical staff, both within the IT division and other CSUN divisions, are responsible for the maintenance and protection of systems and applications used to transact or store university data. The duties include but are not limited to adhering to campus security standards, such as those that pertain to system hardening, data sanitization, log/event management, patch management, and password/access controls.

Students, faculty and staff all have the responsibility to remain aware of information security risks, be attentive to sound practices and to report any potential disclosure or loss of information to their supervisors, instructors, or other responsible parties.

III. Information Security Policies

This section introduces the reader to the major information security legal requirements that CSUN is bound to uphold and the policies the University have adopted to facilitate compliance. Detailed information on compliance requirements and policies can be found on the University policy web site (http://www-admn.csun.edu/vp/policies/).

A. Compliance Requirements

CSUN's information security practices must comply with a variety of federal and state laws as well as CSU's and its own campus policies. These laws and policies are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. "Level 1 protected data" as defined by the CSU covers a variety of types including personally identifiable information (e.g., social security numbers), personal financial information (e.g., credit card numbers), health information and other confidential information.

Among the laws and regulations that mandate baseline privacy and information security controls, the most notable include the following:

- **Health Insurance Portability and Accountability Act (HIPAA) -** Protective Health Information (PHI) may be used and disclosed for Treatment, Payment, and Healthcare Operations (TPO). The information that is disclosed must meet the "Minimum Necessary" standard. This means the least information required to accomplish the intended purpose. Under all other circumstances except

an emergency in a patient's health, a signed authorization form must be completed by the patient or his legal representative.

- **Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. S1232g; 34 CFR Part 99) -** Protects the privacy of student education records and gives parents certain rights with respect to their children's education records.

- **Gramm-Leach-Bliley Act (GLBA) -** These requirements mandate the design, implementation, and maintenance of specific policies to protect customer information. The GLBA protects consumers' personal financial information held by financial institutions.

- **Federal Trade Commission Regulations (16 CFR, Part 314), Standards for Safeguarding Customer Information; Final Rule, May 23, 2002 -** Implements the safeguarding provisions of the Gramm-Leach-Bliley Act. Establishes standards for safeguarding customer information and calls for the establishment by organizations of information security plans to bring about compliance.

- **Payment Card Industry (PCI) Data Security Standards –** A framework of standards and compliance-requirements designed to protect consumer payment card data.

Additional laws and regulations apply in the wake of unauthorized disclosure of individuals' data, requiring the University to take specific actions if any protected data may have been disclosed either accidentally or maliciously to unauthorized parties. A detailed list of regulations and compliance requirements is included in Appendix B. Individuals who handle protected data are encouraged to speak with their managers or the Information Security Officer (ISO) to better familiarize themselves with relevant laws and regulations.

A. University Information Security Policy and Standards

The university has a body of information security policies that proscribe methods of compliance with relevant laws and regulations as well as generally accepted current best practices. Our policies take the further step of establishing practices to safeguard not only information protected by law, but also information that CSUN leadership has deemed to be of a sufficiently confidential nature that it should be treated as legal protected data. Detailed information on University policies can be found at:

IS Policies: http://www.csun.edu/afvp/university-policies-procedures

IS Standards and Guidelines: http://www.csun.edu/it/information-security-standards

B. Information Security Practices

Our information security plan is further enabled by three core practices:

- Risk assessment and vulnerability management
- Incident response
- Employee education and training

These practices enable us to proactively identify risks, continuously improve our strategy, and direct our response in case of an information security incident.

1. Information Security Risk Assessment and Vulnerability Management

In accordance with campus policy, CSUN performs periodic assessments of its information security risks and vulnerabilities. Risk assessments may focus particular types of information, areas of the organization, or technologies. Each year the ISO, in consultation with the VP/CIO and the Cabinet, identifies a set of priorities for information security risk assessments.

The results of risk assessments are shared with the VP/CIO and the Cabinet, together with a plan for implementing specific actions to address risks and vulnerabilities. The ISO is responsible for monitoring the implementation of agreed upon actions and reporting their completion to University leadership.

2. Managing Compromises or Breaches of Information Security – Incident Response Team

Planning for incident management involves organizing an Incident Response Team that is responsible for *problem identification and resolution*. This team has clearly defined membership, roles, and responsibilities, which include, but are not limited to, the following:

a) Incident Management
    a. How to trigger a response
    b. Automated and manual responses
    c. Reporting responsibilities
    d. Certification of actions
    e. Post-Incident review and recommendations
b) Existing and Evolving Threats

A security incident begins when a security related event is reported to the California State University, Northridge IT Help Center or the IT Information Security Office. When an alert involves personally identifiable information, a cross-functional team of members from different areas of the University will analyze and recommend the best course of action. Current members of the Computer Security Incident Response Team (CSIRT) include:

1. Information Security Officer (chair)
2. VP for Information Technology/Chief Information Officer
3. Associate VP, Public Relations
4. Associate VP, Human Resources
5. Chief of Police
6. Internal Auditor
7. Director, Risk Management

3. Employee Education and Training

The entire University Community needs to understand and support the information security objectives of availability, confidentiality and integrity, and what tradeoffs may be necessary for effective control of the information infrastructure's vulnerabilities. The California State University has established an online information security awareness program to serve all 23 campuses that will promote an ongoing dialogue about information security risks and recommended practices.

CSUN has a multi-pronged approach to training and awareness. Current strategies include the following:

- A privacy and confidentiality agreement signed by all newly hired staff.
- A brief overview of key information security awareness training as part of all new employee hire orientations.
- An online CSU Information Security Awareness Training course for all staff, faculty, and student staff.
- An information security website that serves as a repository of information for CSUN information security standards and guidelines, educational materials, as well as information about current issues/alerts, policies and practices.
- Periodic communiqués to the University community, or targeted audience(s), alerting CSUN students and employees to alert of specific vulnerabilities.
- Presentations and discussions with college management-council groups, new department chair orientations, and other college/department forums.

IV. Securing the CSUN Technical Infrastructure

This section identifies some of the specific strategies in place to secure the core technology infrastructure (e.g., network, hardware, data center) of the University. It describes some of information security concerns unique to specific technology areas and highlights the measures being employed to secure CSUN infrastructure.

A. Networking Environment (e.g. data, email, and web)

Among the concerns at CSUN for network and operations security are assurance of service, spam rejection, fraudulent email/phishing-scam processing, copyright protection, appropriate authorization for the use of resources, privacy/confidentiality, protection against unauthorized network access, protecting web sites from typical attacks (e.g. defacement, protected information theft), and maintaining auditable documentation of plans and procedures. The following technologies and tools supported by the appropriate policies, standards, and procedures are implemented to address these needs:

- Internet and Data Center Firewalls, Traffic Monitoring, Intrusion Detection/Prevention Systems
- Virtual Private Network (VPN) and Secure Access Gateways
- Campus-wide Authentication Services including system-wide Federation using Shibboleth
- Desktop Management Systems with Policy Enforcement tools
- Application and Server Security Certificates
- Enterprise Anti-virus/malware and Patch-management systems
- Server, Network, and Application-level Vulnerability Scanning Tools
- Physical and Logical Access Controls to Servers and other Protected Resources
- Confidential network zone to logically separate and protect confidential data systems
- Transport layer encryption for campus technology services such as email, CSUN's myNorthridge portal, and wireless network.
- Encrypted data-back-ups for enterprise systems with confidential data
- Windows and Apple computer encryption for systems that store/access confidential data.
- Organization of staff to respond to the range of security Issues

B. Enterprise Server Environment

Two IT-managed campus data center facilities protect campus servers and storage from unauthorized physical access and assures appropriate logging, data protection and monitoring/alerting. Operational procedures allow physical and logical access only to authorized users and helps ensure that all other staff access servers only to the degree appropriate to their job roles.

C. Identity and Access Management

CSUN's identity management and authentication system ensures appropriate access to all campus computing resources. Network, application, and server access is logged by individual logins to facilitate investigation of possible intrusions or misuse of resources. For applications, only the minimum set of privileges allowed for a user to accomplish his/her objective is granted.

V. Priorities for Action

CSUN's Information Security priorities center on tasks associated with addressing CSUN's greatest risk areas.

2014 – 2015 Goals

- Deploy the new CSU Online Information Security Awareness Training program, campus-wide and achieve 100% completion by all faculty, staff, and student employees with access to critical systems or protected university data.
- Enhance the campus Password Standard to require password-expiration for students so that they are required to reset their campus password at least annually.
- Complete the implementation of whole-disk encryption on laptops/desktops used by campus confidential data handlers.
- Migrate confidential university files that are currently stored on separate department/college file servers to the university confidential file server.
- Build and deliver a virtual web browser (leveraging Citrix XenApp) for confidential data users to browse the Internet without risk of introducing malware and other Internet-born threats to university desktops and laptops that interface/store confidential data.
- Acquire and implement two-factor authentication services (leveraging RSA soft and physical tokens, as well as a campus-hosted RSA key server) to enhance the level of protection for data stored on confidential desktops, and accessed via the Portal, and other confidential systems. This project will be completed in two phases: 1) implement the campus RSA key server and integrate with Active Directory to require two-factor for confidential desktop users. 2) integrate with Shibboleth to require two-factor authentication for those accessing the Portal (with access to confidential data) from any workstation.
- Acquire and implement laptop theft-recovery/data destruction software (Computrace/LoJack) to deploy on campus mobile workstations that access confidential data.
- Review the new Payment Card Industry Standards (3.0) and refine campus PCI processes in coordination with the PCI officer to remain in compliance.

- Conduct an inventory of confidential and protected data systems campus-wide, and migrate protected systems to one of two University data centers.

- Deploy a campus-wide file-storage and file-collaboration solution (myCSUNbox) to enable secure sharing of university data for departments, colleges, faculty, staff, and students. (Providing a single trusted solution reduces the risk of university data being stored in self-chosen public cloud offerings).

- Implement an Advanced Threat Protection (ATP) solution to monitor Internet activity to/from the campus to 1) actively block malware (including "zero-day" or unknown signature malware), 2) block call-back activity from campus workstations to foreign call-back servers, and 3) integrate with university log/event management systems to enable correlated threat assessments based on other network/application behaviors.

- Implement a targeted email security solution to reduce the effects of social engineering attacks via email (e.g. phishing scams).

- Implement a new log/event management system to replace the current aged system, and accommodate log/event data for all production environments that interface with university protected data and key network systems.

- Implement additional network infrastructure security features across building-level network equipment and connected systems. CSUN migrated from Cisco to Alcatel-Lucent and the new equipment has different security features that require separate configuration.

- In a phased deployment and in accordance with system-wide meet and confer process, pilot and deploy Identity Finder to identify the location of university confidential and protected data stored on university computers. Using a self-service model, faculty and staff will have visibility into the data stored on their computing systems and take steps to protect the data via 1) deletion (and instead accessing the data from a primary data source; e.g. the Portal), or 2) protection via encryption (if level 1) or password-protection (if level 2).

Appendix A: Glossary of Terms

Attacks are deliberate actions taken by an entity that exploit certain vulnerabilities.

Authoritative Decision Maker is the person who made the decision regarding compliance in the referenced section.

Availability is a property that assures that the system has the capacity to meet service needs. It includes timeliness and usability. The property of availability protects against threats of denial of service.

Controls are mechanisms or procedures that mitigate threats. Among the goals of information security controls are to provide confidentiality, integrity, availability, or privacy to a computer system.

Confidentiality is a property that assures the assets of a computer system are accessible only by authorized parties or entities. The property of confidentiality protects a system from the threat of disclosure. A disclosure threat is the possibility that data will be accessed by unauthorized entities.

Consultants are experts hired by the university to provide assistance with its information systems or other activities.

Contracted service providers are third parties including businesses that are hired by the University to provide assistance with the information systems infrastructure.

Integrity is a property that assures that unauthorized changes in data cannot occur or can be detected if they do occur. The property of integrity protects against threats of modification and fabrication.

Privacy is a subset of confidentiality. It concerns data about an entity and assures that this data is not made public or is accessible by unauthorized individuals.

Risk analysis is the study of the consequences involved in doing something or not doing it. It improves the basis for information security related decisions and helps justify expenditures for information security.

Threats are potential occurrences, malicious or otherwise, that can have undesirable effects on assets or resources associated with computer systems.

Vulnerabilities are characteristics of systems, applications, and processes that make it possible for a threat to potentially occur. They are not necessarily weaknesses in a system and may be otherwise desirable qualities of a system.

Appendix B: Regulatory Compliance Requirements

Regulation	Summary
Family Educational Rights and Privacy Act (FERPA)(20 U.S.C. S1232g; 34 CFR Part 99)	This protects the privacy of student education records and gives parents certain rights to their children's education records.
California State Constitution, Article 1, Section 1	This is a general description of the rights of citizens in California.
California Penal Code, Section 502	This defines the criminality and responsibility for specific computing activities and associated punishments.
Gramm-Leach-Bliley Act	GLBA requirements mandate the design, implementation, and maintenance of specific policies to protect customer financial information.
Federal Trade Commission Regulations (16 CFR, Part 314), Standards for Safeguarding Customer Information; Final Rule, May 23, 2002	This establishes standards for safeguarding customer information and creates a method to guarantee the uniform application of these standards.
California Business and Professions Code Section 17538.45	This protects electronic mail providers from liability and provides them with a remedy in the event of unauthorized use of email functionality.
State of California Government Code, Section 11015.5	This law pertains to the confidentiality of electronically collected personal information.
California Information Practices Act of 1977	This act gives specific direction on how to handle personal information and describes the right to privacy of individuals.
State of California Government Code, 6254 (j), 6254.4, 6255, 6267	These laws govern the privacy of library users' records.
California Education Code 89546, Employee Access to Information Pertaining to Themselves	This summarizes an employee's rights to review his or her employment records.
HIPAA (Health Insurance Portability and Accountability Act)	This describes the protection for Health records and accountability for its disclosure.