California State University Northridge

POLICIES & PROCEDURES

Privacy of Personal Information

Policy 500-8025
Revision Date: 11/07/2011

POLICY PURPOSE:

California State University, Northridge (CSUN) is responsible for taking all reasonable and appropriate steps for the protection of the confidentiality, availability, privacy, and integrity of information in its custody. This includes the physical security of the equipment where information is processed and maintained, and the preservation of information in case of intentional, accidental, or natural disaster. In addition, CSUN is responsible for the maintenance and currency of applications that use this information.

POLICY STATEMENT:

Enforcement of CSUN's Information Security Policies and compliance with Federal and State regulations regarding information technology is the responsibility of the President. Policy enforcement may be delegated to the Chief Information Officer (CIO). All CSUN Information Security Policies are to be reviewed on an annual basis by the Information Security Officer (ISO) for compliance with the CSU Information Security Policy and Federal and State regulations.

This policy applies to all students (see Student Records Administrative Policy, #RR650-30), faculty and staff, consultants, or any other persons having access to CSUN Information Technology. All unauthorized modifications, deletions, or disclosures of information included in CSUN data resources that compromise the integrity of CSUN's educational, scholarly, and administrative programs, violate individual privacy rights, or constitute a criminal act are expressly forbidden.

This policy is not limited to those systems and equipment operated and maintained by CSUN's central technology organization, Information Technology (IT), but applies to all data, systems and equipment on and off campus that contain protected, confidential, or mission critical data, including college and departmental level systems and equipment, and vendor hosted solutions.

APPLICABILITY AND AREAS OF RESPONSIBILITY:

I. Privacy of Personal Information:

All users of campus information systems or network resources are advised to consider the open nature of information disseminated electronically and must not assume any degree of privacy or restricted access to information they create or store on campus systems. CSUN is a public university and information stored on campus information systems may be subject to disclosure under state law. No campus information system or network resource can absolutely ensure that unauthorized persons will not gain access to information or activities. However, CSUN acknowledges its obligation to respect and protect confidential and protected information about individuals stored on campus information systems and network resources.

II. Collection of Personal Information:

To comply with state and federal laws and regulations, CSUN will not collect personally identifiable information unless the need for it has been clearly established.

1. Where such information is collected:

    - The campus will use reasonable efforts to ensure that personally identifiable information is adequately protected from unauthorized disclosure.
    - The campus will store personally identifiable information only when it is appropriate and relevant to the purpose for which it has been collected.
    - Access to Personal Information

2. Except as noted elsewhere in CSUN policy, information about individuals stored on campus information systems may only be accessed by:

    - The individual to whom the stored information applies or his/her designated representative(s).
    - Authorized CSUN employees with a valid related business need to access, modify, or disclose that information.
    - Appropriate legal authorities.

When appropriate, authorized CSUN personnel following established campus procedures may access, modify, and/or disclose information about individuals stored on campus information systems or a user's activities on campus information systems or network resources without consent from the individual. For example, CSUN may take such actions for any of the following reasons:

1. To comply with applicable laws or regulations.
2. To comply with or enforce applicable CSUN policy.
3. To ensure the confidentiality, integrity or availability of campus information.
4. To respond to valid legal requests or demands for access to campus information.

If CSUN personnel accesses, modifies, and/or discloses information about an individual and/or his/her activities on campus information systems or network resources, staff, faculty, and any other employees will make every reasonable effort to respect information and communications that are privileged or otherwise protected from disclosure by CSU policy or applicable laws.

The CSU Records Access Manual will be used as a guide to determine which records must be made available for public inspection under the California Public Records Act.

III. Access to Electronic Data Containing Personal Information:

Individuals who access or store protected data must use due diligence to prevent unauthorized access and disclosure of such assets.

Browsing, altering, or accessing electronic messages or stored files in another user's account, computer, or storage device is prohibited, even when such accounts or files are not password protected, unless specifically authorized by the user for university related business reasons. This prohibition does not affect:

1. Authorized access to shared files and/ or resources based on assigned roles and responsibilities.
2. Authorized access by a network administrator, computer support technician, or departmental manager where such access is within the scope of that individual's job duties.
3. Access to implicitly publicly accessible resources such as University websites.
4. Campus response to subpoenas or other court orders.
5. Campus response to a request pursuant to public record disclosure laws.

THE FOLLOWING INDIVIDUALS AND ORGANIZATIONAL UNITS HAVE POLICY RESPONSIBILITIES:

The President delegates the Information Security responsibility to the Vice President for Information Technology/CIO.

IV. Information Security Officer:

The Information Security Officer is responsible for ensuring that the campus incident response process for computing systems and data resources is followed. For more information on the responsibilities of the ISO, please see the Campus Incident Response Procedure for Security Breaches of Personal Information.

V. Campus Units: (divisions, units, departments, colleges, centers)

The Campus Units must:

1. Adhere to all CSU and CSUN Security Policies and have plans and procedures for the protection for their data centers and networks. These plans and procedures must insure business continuity, including protection against natural, accidental, or intentional disasters. The plans must include access control, password security, backup and off-site storage of mission critical data, and procedure for cost/effective security systems including virus scanners and firewalls that insure protection against known vulnerabilities.
2. Inform users granted access to personal information of their responsibilities to secure such data from unauthorized release.
3. Develop and maintain control records in a secure environment.
4. Establish monitoring procedures to identify unauthorized access to or anomalous activity.
5. Report suspected unauthorized acquisition of personal information to the Information Security Officer.

VI. Data Users:

Data Users Must:

- Protect the resources under their control, such as access passwords, computers, and data they download.
- Report any unauthorized acquisition or anomalous activity of personal information to the Information Security Officer which may have resulted in the release of personal information to unauthorized individuals.

VII. Campus Incident Response Team (CIRT):

The campus incident response team is responsible for coordinating a review of any security breach that potentially involves the unauthorized access of personal information. For more information on the responsibilities of the CIRT team, please see the Campus Incident Response Procedure for Security Breaches of Personal information.

RESOURCES AND REFERENCE MATERIALS:

500-10 Use of Computing Resources

Security Breach of Personal Information

Data Classification Standards

Digital Media Sanitization Standard

Application Development Standard

FURTHER INFORMATION:

Vice President for Information Technology and CIO

APPROVED BY THE PRESIDENT