CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

User Responsibility for Information Assets
CSUSB, Information Security Office

Last Revised: **01/09/2013**

DRAFT

REVISION CONTROL

Document Title: CSUSB – User Responsibility for Information Assets

Author: Javier Torner

File Reference:

Date	By	Action	Pages
4/06/10	J Torner	Created Procedures Guide	All

Review/Approval History

Date	By	Action	Pages
			All

1.0 Roles 4
1.1 Information owner 4
1.2 Information Authorities 4
1.3 Information Custodians/Stewards 4
1.4 Information Users 5
1.5 University Information Security Officer 5
2.0 Acceptable Use of Assets 5
2.1 Information Owner 5
2.2 Information Authority 5
2.3 Information Custodian 6
2.4 Information User 6

1.0 Roles

Any campus business unit may have confidential or personally identifiable information in its records collections, both paper and electronic. For each such collection of information, there always exists an information owner, information authority, information custodian/steward and information users.

1.1 Information owner

Information owner normally is identified by law or contract. For example, the student is the owner of his or her personal information that is stored in campus records. A principal investigator might be the owner of research data, or the contract with the granting agency might specify that the agency is the owner.

1.2 Information Authorities

Information Authorities senior University officials (or their designees) who have planning and policy-level responsibility for the information assets within their functional areas and management responsibilities for defined segments of institutional data. Responsibilities include: assigning information custodians/stewards, participating in establishing policies, and promoting information resource management for the good of the entire University. Information authorities are responsible for knowing and understanding the information for which they are responsible. They are also responsible for evaluating the confidentiality, criticality, and sensitivity of data; and for ensuring that information below Level 1 has been appropriately classified based on: state and federal law, regulatory agency requirements, contractual obligations, and University regulations.

For example, the Family Educational Rights and Privacy Act requires the campus to appoint a information authority (i.e., the FERPA Compliance Officer) for student academic records and the Health Insurance Portability and Privacy Act requires the campus to appoint a information authority (i.e., the HIPAA Privacy Officer) for medical records. A principal investigator typically is the information authority for research data.

1.3 Information Custodians/Stewards

Information Custodians/ Stewards have direct operational-level responsibility for information management – usually department directors. Information custodians/stewards have operational responsibility for the physical and/or electronic security of the information assets and are generally

responsible for ensuring the appropriate use of the information. Information custodians/stewards are responsible for data access and policy implementation issues, and ensure that systems containing information assets are in compliance with all applicable information security polices and standards.

1.4 Information Users

Information Users are CSUSB faculty, staff and employees of Auxiliary Organizations, who in the course and scope of their duties and responsibilities access, collect, distribute, process, store, use, transmit or dispose University information assets. Information users are responsible for following established information security policies, standards, and procedures.

1.5 University Information Security Officer

University Information Security Officer is responsible for communicating Level 1 information to Information Authorities and assisting in the identification and classification of information types within their respective areas. The University Information Security Officer is responsible for providing advice and guidance to Information Authorities regarding the implementation of this Standard within their respective divisions or area. The University Information Security Officer is also responsible for conducting an annual review of this Sandard and amending it as appropriate.

2.0 Acceptable Use of Assets

2.1 Information Owner

The information owner is responsible for the following activities:

- Ensuring that he or she does not put his or her data at risk through his or her own actions.
- Work with the university information security officer, information authority, information custodian/steward, and other authorized individuals in the investigation and mitigation of information security incidents/breaches affecting the integrity and confidentiality of their data.
- Performing such other information security duties as appropriate and as required by other CSU and CSUSB policies, executive orders, coded memorandums, etc.

2.2 Information Authority

The information authority is responsible for the following activities:

- Establishing procedures granting and revoking access privileges.
- Ensuring that those with access to the data understand their responsibilities for collecting, using, and disposing of the data only in appropriate ways.
- Monitoring the usage of the data.
- Working with the ISO, information owner, information custodian/steward, and other authorized individuals in the investigation and mitigation of information security incidents/breaches affecting the integrity and confidentiality of the data.
- Performing such other information security duties as required by other CSU policies, executive orders, coded memorandums, etc.

2.3 Information Custodian

The information custodian/steward is responsible for the following activities:

- Ensuring that access to and protection of data and the file systems that host them are in compliance with all applicable information security policies and the authorized directives of the information owner and information authority
- Ensuring that any electronic systems have all appropriate security features installed. This includes operating systems and systems software, database management systems, applications systems, computer hardware, firewalls where appropriate, and communications hardware and software being administered by the information custodian/steward.
- Working with the ISO, information owner, information authority, and other authorized individuals in the investigation and mitigation of information security incidents/breaches affecting the integrity and confidentiality of the data.
- Performing as appropriate such other information security duties as required by other CSU policies, executive orders, coded memorandums, etc.

2.4 Information User

The information user is responsible for the following activities:

- Ensuring that he or she does not put at risk through his or her own actions any University data for which he/she has been given access.
- Working with the ISO, information authority, information custodian/steward, and other authorized individuals in the investigation and mitigation of information security incidents/breaches affecting the integrity and confidentiality of their data.
- Performing as appropriate such other information security duties as required by other CSU policies, executive orders, coded memorandums, etc.