8065.S001 Information Security Asset Management

Implements:	CSU Policy #8065
Policy Reference:	http://www.calstate.edu/icsuam/sections/8000/8065.0.shtml

12.0 Asset Management

Each campus must provide for the integrity and security of its information assets by identifying ownership responsibility, as defined with respect to the following:

a) Owners of the information within the campus.

b) Custodians of the information.

c) Users of the information.

d) Classification of information to ensure that each information asset is identified as to its information class in accordance with law and administrative policy.

12.1 Data Ownership

Campuses must complete an inventory identifying Level 1 protected data. Campuses must assign ownership of each information asset containing Level 1 protected data. Normally, responsibility for Level 1 protected data resides with the manager of the campus program that employs the information. When the information is used by more than one program, considerations for determining ownership responsibilities include the following:

a) Which program collected the information.

b) Which program is responsible for the accuracy and integrity of the information.

c) Which program budgets the costs incurred in gathering, processing, storing, and distributing the information.

d) Which program has the most knowledge of the useful value of the information.

e) Which program would be most affected, and to what degree, if the information were lost, inaccurate, compromised, delayed, or disclosed to unauthorized parties.

12.2 Data Classification

The designated owner of an information asset is responsible for making the determination as to how an asset must be classified (e.g., Level 1, Level 2, or Level 3). Data stored on campus hardware or media (both paper and electronic) must be classified per the campus's *Data Classification Standard,* which must meet or exceed the *CSU Data Classifcation Standard* listed in Appendix A of this document.

12.2.1 Use of the CSU Data Classification Standard

a) Campuses may elect to move or add data elements from one classification level to another classification level with higher protection requirements, but never to a classification level with lower protection requirements than the CSU Data Classificaton Standard. For example, a data element classified as Level 2 can be moved to a Level 1 classification but it cannot be moved to a Level 3 classification.

b) Aggregates of data must be classified based upon the most secure classification level. That is, when data of mixed classification exist in the same file, document, report or memorandum, the classification of that file, document, report or memorandum must be of the highest applicable level of classification. If additional guidance is needed, then the campus ISO must be consulted.

12.2.2 Maintaining the CSU Data Classification Standard

a) The CSU's Senior Director for Information Security Management (CISO) must determine what data will be designated Level 1 data and must identify appropriate minimum controls.

b) The CISO must establish a process for the review and maintenance of the data classification standard. The CISO must review the classification standard on an annual basis.

12.3 Data Handling

a) Data owners are responsible for identifying procedures that must be followed to ensure the integrity, security, and appropriate level of confidentiality of their information, subject to ISO review. These procedures may include but are not limited to methods for or restrictions on storage of hardcopy, verbal communication of data, etc. Data stored on campus hardware or media must be appropriately labeled and protected according to its classification.

b) When Protected Level 1 data is transmitted electronically, it must be sent via a method that uses strong encryption.

c) When Protected Level 2 data is transmitted electronically, it must be protected using approved campus processes.

12.4 Data Storage

a) Each campus must develop and implement appropriate controls for securing protected data. These controls must ensure the confidentiality, integrity, and availability of the asset.

b) Campus electronic media and hardware on which protected data is stored, distributed or accessed must be located and stored in secure locations that are protected by appropriate physical and environmental controls. Hardcopy material containing protected data must be stored in a locked enclosure.

c) The level of protections provided by these controls must be commensurate with identified risks to the media and hardware including appropriate inventory records and labeling of content.

d) Where the combination of assessed risk, technical feasibility and operational practicality allow, protected level 1 data stored electronically must be encrypted using strong encryption methods.

12.5 Data Retention and Disposition

All data on campus hardware and electronic and non-electronic media must be retained and disposed of in accordance with CSU Executive Order 1031.

Information that has been identified as or is reasonably believed to be relevant to an existing or potential legal proceeding must be retained while the matter is ongoing in accordance with established campus procedures.

12.6 Data Backup

Information systems or files must be backed up using a schedule which is based on the value of the information asset and the requirements of the campus business continuity plan.

Transportation procedures for backup media containing protected data must be documented and reviewed annually.

Backup media containing protected level 1 data must be encrypted using strong encryption methods.

Backups of campus electronic media, records of the backup copies, and documented restoration procedures must be stored in secure locations with an appropriate level of physical and environmental protection.

13.0 REVISION CONTROL

Last Revised:

FINAL:

Revision History

Version	Revision Date	Revised By	Summary of Revisions	Section(s) Revised
1.0	6/20/2011	Macklin	Draft Standard	All
1.1	6/20/2011	Moske	Format draft.	All
1.2	6/22/2011	Macklin	Incorporating ISAC comments	§ 12.3 – 12.5
1.3	9/1/2011	Macklin	Added hardcopy restriction to	§ 12.4
1.4	9/14/2011	Macklin	Modified to scope “Protected Level 1”	§ 12.1
1.5	10/11/2011	Macklin	Updated with comments from ISAC	§ 12.3, § 12.6
1.6	1/17/2012	Macklin	Updated with comments from ISAC	§ 12.3, § 12.6

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
10/26/12	ISAC	Recommended
6/5/13	ITAC	Reviewed
7/16/13	Perry (CISO)	Approved for Posting