Information Classification Standards
CSUSB, Information Security Office

Last Revised: **01/14/2014**

Final

REVISION CONTROL

Document Title: CSUSB – Information Classification Standards

Author: Javier Torner

File Reference:

Date	By	Action	Pages
04/06/2010	J Torner	Created Standard	All
06/01/2010	J Macdonell	Updates to various sections (mostly grammar)	All
06/03/2010	J Torner	Updates to asset management	All
01/14/2014	L Carrizales & J Torner	Updated to reflect new business process for authorization	Page 15

Review/Approval History

Date	By	Action	Pages
04/06/2010	J Torner	Approved standard	All
01/14/2014	IT Governance Executive Team	Approved new business process for authorization	Page 15

1.0 Information Classification

Information Classification Guidelines

The responsibility for determining the appropriate classification level is shared by the campus and the Senior Director of Information Security, within the Office of the Chancellor.

The Senior Director of Information Security, within the Office of the Chancellor, will designate what data will be classified as Level 1 and review the requirements for the protection of Level 1 data on a periodic basis. Level 2 and Level 3 Information Classification Standards will be reviewed on an annual basis by the campus.

Each division Vice President will designate Information Authorities responsible for the oversight and implementation of Information protection policies. Information Authorities will evaluate and ensure that data below level 1 has been classified properly according to university and regulatory requirements, and with guidance from the University Information Security Office.

Designated Information Authorities can 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. That is, a data element classified as Level 2 can be moved to a Level 1 classification but a Level 1 data element cannot be moved to a Level 3 classification.

Aggregates of data should 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 should be of the highest applicable level of classification.

Information Classification

Information classification is the process of assigning value to data in order to organize it according to its risk to loss or harm from disclosure. The CSUSB Information Classification Standard establishes a baseline derived from Federal laws, state laws, regulations, California State University (CSU) Executive Orders, and campus policies that govern the privacy and confidentiality of data.

.

1.1 Classification Guidelines

The California State University (CSU) has identified three classification levels that are referred to as level 1, level 2, and level 3. Although all the enumerated data values require some level of protection, particular data values are considered more sensitive and correspondingly tighter controls are required for these values. The most critical level of sensitivity begins with Level 1.

Level 1: Confidential

Confidential Information

Confidential Information means any information not exempted in specific legislation and identified as personal, sensitive, or confidential such as personally-identifiable information, individually-identifiable health information, education records, and non-public information as specified in all applicable federal or state laws, plus CSU and CSUSB policies.

Confidential information may include individually-identifiable health information. This includes any information, including demographic information collected from an individual, created or received by a health care provider, health plan, employer, or health care clearinghouse. This includes information that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to the individual, or the identification of the individual.

Electronic confidential information is defined as any electronic format which includes an individual's first name or first initial and last name or education in combination with any one or more of the following data elements, when either the individual's name or the data elements are not encrypted:

- Social Security number
- Driver’s license number or California Identification Card number
- Account number, e.g., identification number, credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Confidential information also includes any information whose unauthorized disclosure, compromise or destruction would result in financial loss, damage to CSUSB reputation, and possible legal action to CSUSB, its students, or employees.

Level 1 data is intended solely for use within CSUSB and limited to those with a business need-to-know. Statutes, regulation, other legal obligations or mandates protect much of this information.

The State of California and the CSU have identified specific guidelines regarding the disclosure of much of this information to parties outside of the university and controls needed to protect the unauthorized access, modification, transmission, storage, or other use.

Confidential information includes, but is not limited to, the following examples:

- Personal Information Data (PID)
  - Passwords or credentials
  - PINs (Personal Identification Numbers)
  - Birth date combined with last four of SSN and name
  - Tax ID with name
  - Driver's license number, state identification card, and other forms of national or international identification in combination with name
  - Social Security number and name
  - Verbal or written statements made by or attributed to the individual

- Financial Information
  - Credit card numbers with cardholder name
  - Bank account or debit card information

- Health Information
  - Health insurance information
  - Medical records related to an individual
  - Psychological Counseling records related to an individual

- Technical Security Information
  - Vulnerability/security information related to the campus or information system
  - Systems logging information

- Law Enforcement Information
  - Law Enforcement Records related to an individual
  - Law Enforcement individual's home address

Level 2: Internal Use

Internal use information must be guarded due to proprietary, ethical or privacy considerations.

Internal use information is intended for use by CSUSB employees and contractors and vendors covered by non-disclosure agreement. An unauthorized disclosure, compromise or destruction would

directly or indirectly have an adverse impact on CSUSB, its students, or employees. Financial loss, damage to CSUSB's reputation, and possible legal action could occur.

Campus guidelines will indicate the controls needed to protect the unauthorized access, modification, transmission, storage or other use.

Level 2 Information Includes but is not limited to:

- Identity validation keys
- Birth date (full: mm-dd-yy)
- Birth date (partial: mm-dd only)
- Mother's maiden name

- Student information
    - Educational records (Excludes directory information)
    - Home or mailing address
    - Personal telephone numbers
    - Personal email address
    - Ethnicity
    - Gender
    - Birthplace
    - Grades
    - Courses taken
    - Schedule
    - Test Scores
    - Advising records
    - Educational services received
    - Disciplinary actions

- Alumni Information
    - Same as Student Information

Non-directory student information may not be released except with Registrar's Office approval under certain prescribed conditions

- Employee Information
    - Employee net salary
    - Employee tax information - amount of taxes or OASDI withheld

  - Voluntary/involuntary deductions/reductions
  - Survivor's amounts
  - Designee for last payroll warrant
  - Employment history
  - Home address
  - Personal telephone numbers
  - Personal email address
  - Parents and other family members names
  - Payment History
  - Employee evaluations
  - Background investigations
  - Biometric information
  - Electronic or digitized signatures
  - Private key (digital certificate)
  - Birthplace (City, State, Country)
  - Ethnicity
  - Gender
  - Marital Status
  - Personal characteristics
  - Physical description
  - Photograph

- University Donor Information
  - Name
  - Home or mailing address
  - Personal telephone numbers
  - Personal email address

- Legal Information
  - Legal investigations conducted by the University

- Purchasing Information
  - Sealed bids

- University Research
  - Trade secrets or intellectual property such as research activities

- Library Patron Information
    - Linking a library user with the specific subject about which the library user has requested information or materials.

- Facilities Information
    - Building plans and architectural drawings

- Emergency Preparedness Information
    - Location of critical assets
    - Location of hazardous materials or similar assets
    - Emergency Operations Plan
    - Continuity of Operations Plans

Level 3: Public

This information is generally regarded as publicly available. Information at this level are either explicitly defined as public information, intended to be readily available to individuals both on- and off-campus, or not specifically classified elsewhere in the protected data classification standard.

Knowledge of this information does not expose CSUSB to financial loss, or jeopardize the security of CSUSB's information assets. Level 3 information may be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

Level 3 Information Include but is not limited to:

- Campus Identification Keys
    - Coyote ID-Number
    - Coyote ID-Name (do not list in a public or a large aggregate list, protection of SPAM, where it is not the same as the student email address)

- Student Information
    - Name
    - Major Field of Study
    - Participation in officially recognized sports/activities
    - Weight and Height of athletic team members
    - Dates of Attendance
    - Full or Part-time status
    - Degrees and awards received
    - Campus E-mail address

- Most recent or previous college/university/agency attended

Note: If the student has requested confidentiality via the Registrar's Office this information is no longer public for that student.

- Employee Information
  - Employee Title
  - Employee public email address
  - Employee work location and telephone number
  - Employing department
  - Employee classification
  - Employee gross salary
  - Name (first, middle, last) (except when associated with protected information)
  - Signature (non-electronic)

- Financial Information
  - Financial budget information

2.0 Management of classification levels

Classification Process

The first step in the classification process is locating and identifying the information assets. The identification process will include determining the information authorities, users, and custodians. The university information security office will work with the different business units on campus to ascertain the appropriate information classification levels.

Security measures

In addition to applying a classification label to each piece of information, an important part of information classification involves identifying the security measures that can consistently be applied to each level and that are substantially different. The campus custodians must put in place the appropriate technical and organizational measures to prevent the unauthorized or unlawful processing or disclosure of data.

The campus information authorities and information custodians must ensure that the security measures in terms of physical security (e.g., control access to buildings or rooms, correctly handle and dispose of printed material containing personal data), administrative controls (e.g., restrict password, restrict access on the basis of role or authority), and technical controls (e.g., store personal data on a

secure server, make use of privacy enhancing technologies) are appropriate for the data being processed and maintained.

Information security measures must be implemented commensurate with data value, sensitivity, and risk. Information in each classification will require varying security measures appropriate to the degree to which the loss or corruption of the data would: be harmful to individuals, impair the business or academic functions at CSUSB, result in financial loss, or violate law, policy or CSUSB contracts.

The security measures implemented for a given data value will be dictated by the classification level. Measures will include, but not be limited to, an appropriate combination of the following:

- Physical Access Control
- Administrative Access Control
- Technical Access Control

Levels of Control

Each category of information should have an established level of control mechanisms.

Security Controls

Level 1: Confidential

- Confidential data should be limited in distribution to those employees with an established business need to know.
- Employee access to confidential data should be reviewed on an annual basis.
- Strong consideration should be given to encrypting this data while in storage. Confidential data should always be encrypted when traversing a public network (e.g., Internet) or when traveling between CSUSB locations.
- Printed copies of this type of information should be closely guarded to prevent unauthorized disclosure.
- Due care should also be taken when in verbal contact with another party.
- Employees should receive training annually on their responsibilities regarding appropriate use and steps they can take to protect confidential data.
- Confidential Personal Identifiable Information (PII):
    - Should be encrypted when in transit and in storage.
    - Distribution of this data must be strictly controlled.
    - It is imperative that the Data Retention and Disposal standards be strictly followed when dealing with personal information data (PII).

- PII should only exist within the confines of a production environment. Any exceptions must be documented and explicitly accepted by the information authority.

Level 2: Internal Use Only

- Internal Use Only data should be limited in distribution to those employees with an established business need to know.
- Information should always be encrypted when traversing a public network or when traveling outside the CSUSB private network.
- Printed copies of this type of information should be protected to prevent unauthorized disclosure.
- Due care should also be taken when in verbal contact with another party.

Level 3: Public

- Public information may be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

3.0 Information Labeling and Handling

The following table describes how information should be labeled and handled according to its classification and as it relates to systems development. For example, if a report is printed and automatically distributed, labeling information and distribution standards would be required. Additional notes can be found at the end of the table.

	Public	**Internal use**	**Confidential**
	Level 3	Level 2	Level 1
Labeling	No Labeling is required. Control Statements, which classify a label, may be added at the bottom of the first page or screen, or on removable media labels.	"CSUSB, Internal Use" should appear on the bottom of each page and on removable-media labels. Control statements which clarify a label, should be added directly under the "Internal Use" label on the first page; they may be added on each subsequent page as necessary.	"CSUSB Confidential", must appear on the bottom of each page. Control statements which clarify a label must be added directly under the "Confidential" label on each page. "Confidential" must also appear on removable media labels.
Reproduction	No restrictions	Reproduction is authorized if not prohibited by the control statement	Reproduction is discouraged, however, if done, must be done with permission from the owner.

Distribution	No restrictions	Distribution should be only to CSUSB employees and those individuals with a business need to know.	Distribution must be only to those who have a business need to know and are either CSUSB employees or someone who has signed a confidentiality statement. Information distributed outside of CSUSB must have valid, current, and properly executed Non-Disclosure Agreement in place approved by the Information Authority.
Computer Printing	No restrictions	Remove printouts immediately if using an office printer or as appropriate for internal shared printers	Printing is discourage, however if done, remove printouts immediately if using an office printer or as appropriate for internal shared printers
Mail (Hard Copies)	No restrictions	May be sent through interoffice of U.S. Mail with no special handling. If being sent to another building, it must be placed in an interoffice envelope with proper labeling.	May be sent through interoffice or U.S. Mail but must be sealed in a plain envelope having no classification marking and clearly marked on the outside "To be Opened by Addressee Only".
Electronic Mail (email)	No restrictions	May be sent to other CSUSB employees but not over a public network and must be protected by CSUSB Information Security Office sanctioned encryption package or algorithm.	May be sent internally but not over public networks and must be protected by CSUSB Information Security Office sanctioned encryption package or algorithm. No forwarding and automatic labeling should be used if the email package supports this feature.
Data Transmission	No restrictions	Data transmission is authorized to other CSUSB employees, but not over public networks unless protected by CSUSB Information Security Office sanctioned encryption package or algorithm	Data transmission is authorized to only those who have a business need to know and are either CSUSB employees or someone who has signed a confidentiality statement. Data transmission must be protected by CSUSB Information Security Office sanctioned encryption package or algorithm.
Fax	No restrictions	May be sent to other CSUSB employees as long as the receiving and send fax are CSUSB controlled. Fax from a public location is	Authorized only from and to CSUSB controlled fax machines. Confidential information including PII should not be sent to public fax machines.

		not allowed.	
Telephone	No restrictions	No restrictions, but conversations must be limited to other CSUSB employees or individuals covered by non-disclosure agreement.	Authorized, but only to CSUSB employees and others with a business need to know.
Visual Disclosure	No restrictions	Whenever possible, do not leave documents and screen unattended and unsecured in public locations. Ensure that documents and screens are positioned to prevent inadvertent disclosure.	Do not leave documents and screens unattended and unsecured in a location. Ensure that documents and screens are positioned to prevent inadvertent disclosure. Erase all white boards at the end of meetings.
Storage and Backup	No restrictions	When on CSUSB property, no special requirements. If transported outside, appropriate care must be taken to prevent disclosure or theft. Strongly recommended that paper or removable media be stored in a locked enclosure when not in use. Media should not be left unattended on a desk.	Electronic storage requires access controls and file protection mechanisms. If these are not found in the operating system in use, then additional security packages are required. Backups require the same security controls as originals to maintain confidentiality and integrity. Backups must be encrypted using CSUSB Information Security Office sanctioned encryption package or algorithm.
Record Retention	Records of any type of medium, such as paper, microfiche, magnetic, or optical, must be retained as required by the record retention and disposal schedule published by the campus.	Records of any type of medium, such as paper, microfiche, magnetic, or optical, must be retained as required by the record retention and disposal schedule published by the campus.	Records of any type of medium, such as paper, microfiche, magnetic, or optical, must be retained as required by the record retention and disposal schedule published by the campus
Disposal	Normal waste disposal	Hard copy should use a secure disposal container or shredder. Normal deletion commands or utilities within operating systems are sufficient for files. Reformatting of media is also valid.	Hard copy requires a secure disposal container or shredder. Electronic storage media must be irretrievably erased or disposed of in a secure fashion.

Inventory	All paper and electronic repositories must be identified. Security measures and access controls should be reassessed annually.	Access control Employee must have signed a copy of the CSUSB Employee Confidentiality Statement before access is granted. Vendors must have a copy of the non-disclosure agreement before access is granted.	Employee must have signed a copy of the CSUSB Employee Confidentiality Statement before access is granted. Vendors must have a copy of the non-disclosure agreement before access is granted. Vice President/Provost must approve all access to confidential data.
Reclassify or declassify	No requirements	Only the information authority can reclassify or declassify	Only the information authority can reclassify or declassify

Control Statements

Add control statements next to or underneath the classification label. Control statements further describe the need to take care of information required by information owner. While control statements are virtually unlimited in meaning, some of the most common are:

- Modification or reproduction is prohibited
- Copyright ©2007 CSUSB rights reserved
- Electronic transmission allowed only if encrypted
- To be opened by addressee only
- CSUSB - Internal Use Only
- Document classified PUBLIC after month, day, year
- Under Advice of Counsel

Labels

A label must clearly display the classification of the information. Labels have the following attributes:

- Labels must be clearly visible.
- Use highlighting to make the label stand out from the body of the page.
- Use elements such as bolding, asterisks (*), all capital letters, or color to accentuate the label.