Information and Digital Technologies
March 2, 2009

SDSU Information Classification Standard

Information classification is the process of assigning labels to information in order to organize it according to its sensitivity to loss or harm from disclosure.

The CSU draft Data Classification Standard is based on federal laws, state laws, regulations, CSU executive orders, and university policies that govern the privacy and confidentiality of information.

The CSU draft Data Classification Standard applies to all information generated and/or maintained by the CSU (such as student, research, financial and employee information) except when superseded by grant, contract, or federal copyright law.

Protected Information Levels
SDSU has adopted the draft CSU Data Classification standard as a minimum information classification standard. This standard outlines three levels of classification to which information must be secured.

Protected Level-1

Protected level-1 information is information primarily protected by statutes, regulation, other legal obligation or mandate. The CSU has identified standards regarding the disclosure of this type of information to parties outside the university and controls needed to protect the unauthorized access, modification, transmission, storage or other use. Included in this level are:

- Passwords or credentials
- PINs (Personal Identification Numbers)
- Private key (digital certificate)
- Name with credit card number
- Name with Tax ID
- Name with driver's license number, state identification card, and other forms of national or international identification in combination with SSN
- Name with Social Security Number
- Name with birth date combined with last four of SSN
- Medical records related to an individual
- Psychological counseling records related to an individual
- Name with bank account or debit card information (and/or with password)

NOTE: Credit card number with expiration date and/or card verification code is also considered protected information.

Protected Level-2

Protected level-2 information must be guarded due to proprietary, ethical or privacy considerations. University standards will indicate the controls needed to protect the unauthorized access, modification, transmission, storage or other use of:

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

Name with personally identifiable educational records

- Courses taken
- Schedule
- Test scores
- Advising records
- Educational services received
- Disciplinary actions
- Grades
- SDSU identification number (RedID)
- Race & Ethnicity
- Gender
- Transcripts
- E-mail addresses

Note: Considered directory information by FERPA, but considered non-directory information by SDSU for SDSU student employees.

Name with personally identifiable employee information

- Employee net salary
- 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
- Birthplace (City, State, Country)
- Ethnicity
- Gender
- Marital status
- Personal characteristics
- Physical description
- Photograph

Other

- Legal investigations conducted by the university
- Sealed bids
- Trade secrets or intellectual property such as research activities
- Location of highly sensitive or critical assets (e.g. safes, check stocks, etc.)
- Linking a person with the specific subject about which the library user has requested information or materials

Protected Level-3

Protected level 3 is information that is regarded as publicly available. This information is either explicitly defined as public information (such as state employee salary ranges), intended to be available to individuals both on-campus and off-campus (such as employee work email addresses), or not specifically classified elsewhere in the protected information classification standard. Publicly available information may still be subject to University review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

Student information designated as Educational Directory Information:

- Student name
- Photograph
- Major field of study
- Dates of attendance
- Degrees, honors and awards received
- Most recent educational agency or institution attended
- Participation in officially recognized activities and sports
- Weight and height of members of athletic team

Student Employee information designated as Educational Directory Information:

- Student employee name
- Enrollment status
- Department employed
- Work telephone number
- Work e-mail address
- Status as student employee (such as TA, GA, ISA)
- SDSU identification number (RedID)

Employee information designated as Directory Information:

- Employee title
- Employee work 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)
- Financial budget information
- Signature (non-electronic)

- SDSU identification number (RedID)

SDSU may disclose Directory Information without prior written consent unless the student has requested the information stay confidential using the "Confidential Directory Information" option in the SDSU WebPortal. Students may change their "confidentiality" status at any time through the SDSU WebPortal.

Non-SDSU (personal) protected information, such as personal credit reports or personal bank statements, must not be stored on university systems as the university does not assume responsibility for securing this information and many systems may not be secured for this information by default.