California Health Sciences University

CHSU DATA CLASSIFICATION STANDARDS POLICY

I. PURPOSE

The purpose of this policy is to provide direction for identifying the information security level of University data and records as a framework to ensure proper security procedures are used.

II. LEVEL 1 – CONFIDENTIAL – HIGH RISK

Confidential information can cause the most serious harm to individuals and the University as a result of unauthorized access. Much of this information is protected by statutes, regulation, other legal obligations and mandates including the Health Insurance Portability and Accountability Act (HIPPA), the Family Educational rights and Privacy Act (FERPA), and information regulated by the Payment Card Industry (PCI). Confidential information is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws or classified as confidential by CHSU.

A. Information may be classified as confidential based on criteria including:

1. Severe Risk – Information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the University, its students, employees, or customers. Financial loss, damage to CHSU's reputation, and legal action could occur.

2. Limited Use – Information intended solely for use within the University, its auxiliary employees, contractors, and vendors covered by a confidentially-security agreement and limited to those with a business "need-to know."

3. Legal Obligations – Information for which disclosure to persons outside the University is governed by specific standards and controls designed to protect the information.

B. Examples of Level 1

1. Passwords or credentials that grant access to level 1 and level 2 data
2. Personal Identification Numbers (PIN)
3. Birth Date – mm/dd/yy or mm/dd
4. Credit card numbers with cardholder name

5. Driver's license number, state identification number, or other forms of national or international identification (passports, visas, etc.)
6. Tax ID
7. Social Security Number
8. Health insurance information
9. Medical records
10. Psychological counseling records
11. Bank account or debit card information in combination with any required security code
12. Biometric Information (fingerprints, voice recordings, palm print, iris scan, DNA)
13. Employee home or mailing address
14. Electronic or digitized signatures
15. Private key (digital certificates)
16. Law enforcement personnel records
17. Criminal background check results
18. Vulnerability/security information related to the campus or computer information systems
19. Vulnerability/security information related to campus law enforcement operations

III. LEVEL 2 – INTERNAL USE ONLY - MODERATE

While possibly not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to CHSU's reputation, violate an individual's privacy rights or legal action could occur.

A. Information may be classified as internal use only based on criteria including:

1. Sensitivity – Information protected due to proprietary, ethical, contractual, or privacy concerns.
2. Limited Use – Information intended solely for use within the University, its auxiliary employees, contractors, and vendors covered by a confidentially-security agreement and limited to those with a business "need-to know."

B. Examples of Level 2

1. Photo (taken for identification purposes)
2. Student Information
    a. Educational records, grades, courses taken, schedule, test scores, advising records, educational services received, disciplinary actions.
    b. Non-directory student information
3. Library circulation information
4. Linking a library user with a specific subject area
5. Sealed bids prior to award
6. Identifiable information (Purchase order) of the supplier/company
7. Trade secrets and intellectual property
8. Information covered by a specific non-disclosure agreement
9. Location of critical protected assets
    a. Maps of campus utility systems
    b. Construction drawings of campus buildings
    c. Detailed drawings of sensitive campus facilities
10. Licensed software
11. Campus attorney-client communications
12. Accident reports and investigations
13. Employee Information
    a. Net Salary
    b. Personal telephone numbers
    c. Personal email address
    d. Payment history
    e. Evaluations
    f. Mother's maiden name
    g. Race and ethnicity
    h. Family members' names
    i. Birthplace
    j. Gender
    k. Marital Status
    l. Physical Description
14. University Donor Information
    a. Name
    b. Home or mailing address
    c. Personal telephone numbers
    d. Personal email address
    e. Donation if request is for anonymous gift/donation

IV. LEVEL 3 – PUBLICLY AVAILABLE – LOW RISK

Publicly available information is information intended to be publicly available or provided to the public. Disclosure of this information does not expose CHSU to financial loss, diminish reputation, or jeopardize the security of information assets.

A. Examples of Level 3

1. CHSU ID (Emplid, Student ID)
2. Employee Information
    a. Work email address
    b. Work mailing address
    c. Title
    d. Office location and telephone number
3. Student Information (Non-FERPA students only)
    a. Name
    b. Dates of attendance
    c. Full or part-time status
    d. Degrees and awards received
    e. Campus email address

- Policy Owner: Executive Director of Information Technology
- Effective Date: 9/02/2020
- Revised Date:
- Approval by the President: 9/14/2020