

UCSD POLICY & PROCEDURE MANUAL
SECTION 135-4

Effective: 10/20/98

Supersedes:

Issuing Office: Administrative Computing

ACCESS FOR NON-UCSD PERSONNEL TO UCSD CORE CAMPUS SYSTEMS

I. REFERENCES & RELATED POLICIES

- A.** University Policy, Guidelines, and Legal Requirements on Privacy of and Access to Information, June 9, 1978
- B.** University Policies Applying to the Disclosure of Information from Student Records, February 1, 1977
- C.** California Public Records Act (1976)
- D.** California Information Practices Act (1977)
- E.** California Education Code, Chapter 1.2 Division 16.5
- F.** California Penal Code, Section 502, Chapter 858, relating to Computer Crime
- G.** Federal Privacy Act of 1974
- H.** Federal Family Educational Rights and Privacy Act of 1974
- I.** Electronic Communication Privacy Act of 1986
- J.** UCSD Policy and Procedure Manual (PPM)
 - 135-3 Network Security
 - 160-2 Disclosure of Information from Student Records
 - 230-11 Maintenance of, Access to, and Opportunity to Request Amendment of Academic Personal Records
 - 230-29 Policies and Procedures to Assure Fairness in the Academic Personnel Review Process
 - 460-5 Reporting and Investigating Improper Governmental Activities, Misuse of University Resources, Fraud, and other Financial Irregularities
 - 480-3 Responsibilities & Guidelines for Handling Records Containing Information About Individuals
- K.** Personnel Policies for Staff Members
 - 80 Staff Personnel Records
 - 80
 - HR-S-1 Staff Personnel Records
- L.** Systemwide Business and Finance Bulletin (BFB)
 - RMP-8 Legal Requirements on Privacy of and Access to Information
- M.** Information Systems Policies , Misuse of University Resources, 11/2/87

UCSD POLICY & PROCEDURE MANUAL
SECTION 135-4

Effective: 10/20/98

Supersedes:

Issuing Office: Administrative Computing

N. DSA Handbook

II. DEFINITIONS

- A. A **user** is any individual who accesses UCSD Core Campus systems.
- B. **UCSD Core Campus systems** are UCSD Financial systems, Student systems, Payroll/Personnel systems and ACT Data Warehouse systems.
- C. A **user-id** or login-id is a user's personal identifier used to access UCSD Core Campus systems. A user is usually assigned a **password** in conjunction with their user-id. The combination of user-id and password allow a user access to UCSD Core Campus systems.
- D. **Campus Data Stewards** control access to UCSD Core Campus systems. Data Stewards determine what data is to be secured and whom may access data for which the stewards are responsible.
- E. **Sponsoring Department** is the designated UCSD department affiliated with the non-UCSD entity or individual, and is the department that employs the DSA who grants and sets up the non-UCSD personnel's access.

III. BACKGROUND

Community partnerships and entrepreneurial agreements with industry have resulted in conditions by which persons who are not UCSD employees may have a legitimate business purpose to access UCSD Core Campus systems and data. This document sets forth the policy by which persons who are not employees of the University of California, San Diego, may be allowed to access UCSD Core and Departmental Information Resources and systems, and how they may apply to obtain this access through the appropriate UCSD Data Steward.

IV. POLICY

It is the policy of UCSD to protect its Information assets from unauthorized access. Access to University Core Campus Systems will be limited to only those individuals with a legitimate business purpose. Users granted access to those systems will be held accountable for his/her conduct under applicable University or campus policies and procedures, and local, State or Federal laws and regulations.

Under California law any person who maliciously accesses, alters, deletes, damages or destroys any computer system, network, computer program or data is guilty of a felony. The user understands that the misuse of access to UCSD Core Campus systems will result in loss of access privileges, and misuse may be prosecuted under applicable statutes.

UCSD POLICY & PROCEDURE MANUAL
SECTION 135-4

Effective: 10/20/98

Supersedes:

Issuing Office: Administrative Computing

V. PROCEDURES

A. Responsibilities

1. Data Steward

Access to UCSD Core Campus systems requires written approval by the appropriate Data Steward responsible for the particular category of data to which access is requested. The Data Steward makes a determination to grant or refuse access requests from non-UCSD persons based on whether there is a legitimate business need to access Core Campus systems or data for which they are responsible. Data Stewards will determine the extent of access allowed and impose appropriate terms and conditions such as time period, level of access, or other restrictions as deemed necessary. This condition will be specified in writing on the *Data Steward Authorization Form Exhibit A*. Data Stewards will retain the original copy of the approved *Data Steward Authorization Form*.

2. ACT Security Administrator

The ACT Security Administrator is responsible for establishing access for the non-university personnel as approved by the Campus Data Steward. The ACT Security Administrator will retain a copy of the *Data Steward Authorization Form* and the *Security Statement* on file.

3. User

All non-UCSD personnel desiring to have access to UCSD information resources and systems are required to complete a *Computer/Information Use and Security Statement for Non-University Personnel, Exhibit B*. By signing the usage agreement, non-UCSD personnel agree to behave in an ethical manner, abide by all applicable UCSD policies and procedures, and that they will be held responsible for their own actions when accessing UCSD Core Campus systems.

Further, the user understands the UCSD Core Campus systems are a shared resource and will not intentionally take actions which will interfere with the operation, integrity or security of the systems. The user will not provide access to, or distribute information from UCSD Core Campus systems to third parties.

The user should understand the misuse of access to UCSD Core Campus systems may result in immediate, unannounced removal of access to those systems; and, misuse may be prosecuted under applicable State and Federal statutes. The user has an obligation to notify the Departmental DSA or Campus Data Steward at the time they no longer have a business need to access UCSD Core Campus systems so their access can be removed.

4. Sponsoring Department

The UCSD sponsoring department head is responsible for delegating access authority as appropriate, determining particular access requirements needed for the non-UCSD personnel, establishing appropriate approval hierarchies

and routing for approvals consistent with guidelines established in the DSA Handbook. Additionally, the sponsoring department head is required to sign the *Data Steward Authorization Form* indicating their approval to grant access to UCSD systems and data requested.

UCSD POLICY & PROCEDURE MANUAL
SECTION 135-4

Effective: 10/20/98

Supersedes:

Issuing Office: Administrative Computing

5. Sponsoring Department DSA

The sponsoring department DSA is responsible for routing requests for access to Core systems, forwarding access requests to the appropriate Data steward for approval, establishing appropriate approval hierarchies upon receipt of approved access requests and accountability structure forms, notifying ACT when access needs to be terminated and deleting approval hierarchies upon access termination. Additionally, departmental DSAs are responsible for ensuring that new users have the appropriate training necessary before granting access to UCSD Core systems. A comprehensive list of DSA responsibilities can be found in the DSA Handbook. The DSA will retain the original *Computer/Information Use and Security Statement for Non-University Personnel* and a copy of the *Data Steward Authorization Form*.

B. Time Period

Access to UCSD Core Campus systems by non-UCSD personnel is limited to one year, subject to one-year extensions upon re-application and approved by the Data Steward. Access to UCSD Core Campus systems will be automatically terminated after one year.

C. Application for Access

All non-UCSD users should apply for access through a sponsoring UCSD department using a *Data Steward Authorization Form*. The following comprises the steps necessary to grant access.

- 1) The sponsoring department DSA identifies what Core Campus system data the non-UCSD personnel is seeking to access and states the specific business need that requires access to this data or system on the *Data Steward Authorization Form*. The form is forwarded to the department head for review and approval.
- 2) Access requests are reviewed and approved by the department official who indicates their approval by his/her signature on the form. The *Data Steward Authorization Form* must be signed by the cognizant sponsoring department head. The DSA then forwards the completed form to the identified Data Steward(s) for review.
- 3) Data Steward indicates approved access to campus Core systems and data by their signature on the original form, add any special instructions to the campus Security Administrator, and return a copy of the signed form to the sponsoring department DSA.
- 4) Upon receipt of the approved *Data Steward Authorization Form*, the DSA obtains the signature of the non-UCSD user on the form entitled "*UCSD Information Systems - Computer/Information Use and Security Statement for Non-University Personnel*." This form acknowledges the non-UCSD individual's responsibilities for access to and use of UCSD systems and data.
- 5) Once these documents are completed, the department DSA processes the access request form, and establishes the appropriate approval hierarchies for authorized system use. The original signed *Use* agreement, along with the copy of the completed and approved *Data Steward Authorization Form* will be retained by the sponsoring department.
- 6) Finally, the sponsoring department DSA assures that the non-UCSD user has

UCSD POLICY & PROCEDURE MANUAL

SECTION 135-4

Effective: 10/20/98

Supersedes:

Issuing Office: Administrative Computing

completed the appropriate training before giving them their new userid and password.

D. Complaints Alleging Misuse

Complaints alleging misuse of UCSD Core Campus systems should be directed to the appropriate Campus Data Steward, Internal Audit, or to ACT Security Administration, in accordance with PPM 460-5, Reporting and Investigating Improper Governmental Activities, Misuse of University Resources, Fraud, and Other Financial Irregularities.

UCSD INFORMATION SYSTEMS
COMPUTER/INFORMATION USE AND SECURITY STATEMENT
FOR NON-UNIVERSITY PERSONNEL

Name _____ Access Number _____

I understand that in the performance of my duties for UCSD, I must hold information in confidence. I have read, understand, and agree to abide by the **Rules of Conduct for University Employees Involved with Information Regarding Individuals** (on reverse side). I understand that unauthorized disclosure of personal/confidential information may result in charges of Invasion of Privacy.

I also understand that it is against UCSD Information Systems policy to seek out or use personal or confidential information relating to others for my own interest or advantage.

I understand that under California State Law any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, network, computer program, or data is guilty of a felony.

I also agree to abide by the References and Related Policies on the reverse side outlining University policies and State and Federal laws which govern use of computer systems and disclosure of information. I understand that violation of UCSD regulations and local, state, or federal statutes may carry the additional consequence of prosecution under the law, where judicial action may result in specified fines or imprisonment, or both, plus the costs of litigation or the payment of damages, or both.

I understand that this agreement expires one year from the date indicated on this form, and that any extension of access must be approved again by the appropriate Data Steward. If access is no longer required before the one year term has ended, I understand I am obligated to request of the Data Steward that my access be terminated immediately to avoid misuse of my computer access.

I acknowledge receipt of a UCSD Administrative Computing & Telecommunications computer access code (user-id) and password; and understand that I will be responsible for all entries made thereunder. I understand that my user-id and password are to be accorded the same significance as my handwritten signature and that the delegation of user-id and password to another person, or my use of another persons user-id, may be considered False Representation.

Signature _____ Date _____

RULES OF CONDUCT FOR UNIVERSITY SYSTEM USERS INVOLVED WITH INFORMATION REGARDING INDIVIDUALS

- | | |
|--|---|
| <p>A. Users responsible for the collection, maintenance, use and dissemination of information about individuals which relates to their personal life, including their employment and medical history, financial transactions, marital status and dependents, shall comply with the State of California Information Practices Act. PPM-480-3 Privacy of and Access to Information, Legal Requirements and Implementing Procedures, shall be used as a basic source of guidance in administering the ACT's provisions.</p> | <p>E. Users shall respond to inquiries from individuals, and requests from them to review, obtain copies of, amend, correct, or dispute their personal records in a courteous and business-like manner, and in accordance with PPM-480-3.</p> |
| | <p>F. Users shall not disclose personal and confidential information relating to individuals to unauthorized persons or entities. The intentional disclosure of such information to such persons may be cause for disciplinary action.</p> |

- B. Users shall not require individuals to disclose personal information which is not necessary and relevant to the purposes of the University or to the particular function for which the User is responsible.
- C. Users shall make every reasonable effort to see that inquiries and requests relating to personal records of individuals are responded to quickly and without requiring the individual to unnecessarily repeat his or her inquiry to others. In other words, reasonable efforts will be made to place the responsibility on the Department for responding to the individual after his/her initial contact.
- D. Users shall assist individuals who seek information pertaining to themselves in making their inquiries sufficiently specific and descriptive so as to facilitate locating the records.

REFERENCES

- A. Policy and Procedure Manual (PPM 480-3) Responsibilities and Guidelines for Handling Records Containing Information about Individuals.
- B. University Policy, Guidelines, and Legal Requirements on Privacy of and Access to Information, June 9, 1978.
- C. University Policies Applying to the Disclosure of Information from Student Records, February 1, 1977.
- D. California Public Records Act (1976).
- E. California Information Practices Act (1977).
- F. California Education Code, Chapter 1.2 Division 16.5.
- G. California Penal Code, Section 502, Chapter 858, relating to Computer Crime.
- H. Federal Privacy Act of 1974.
- I. Federal Family Educational Rights and Privacy Act of 1974.
- J. Electronic communication Privacy Act of 1986.

- G. Users shall not seek out or use personal or confidential information relating to others for their own interest or advantage. The intentional violation of this rule may be cause for disciplinary action.
- H. Users responsible for the maintenance of personal and confidential records shall take all necessary precautions to assure that proper administrative, technical, and physical safeguards are established and followed in order to protect the confidentiality of records containing personal information and to assure that such records are not disclosed to unauthorized individuals or entities.

RELATED POLICIES

- A. POLICY AND PROCEDURE MANUAL (PPM)
 - 1. 135-3 Network Security.
 - 2. 160-2 Disclosure of Information from Student Records.
 - 3. 230-11 Maintenance of, Access to, and Opportunity to Request Amendment of Academic Personal Records.
 - 4. 230-29 Policies and Procedures to Assure Fairness in the Academic Personnel Review Process.
 - 5. 250-605 Staff Employee Personnel Records.
 - 6. 250-605 (L-1) Staff Employee Personnel Records.
 - 7. 460-5 Misappropriation of University Assets.
 - 8. 480-3 Responsibilities & Guidelines for Handling Records Containing Information About Individuals.
- New Policy University of California Electronic Mail Policy.
- B. BUSINESS AND FINANCE BULLETIN
 - 1. RMP-8 Legal Requirements on Privacy of and Access to Information.
- C. INFORMATION SYSTEMS POLICIES
 - 1. Misuse of University Resources, 11/2/87.