# ROLES AND RESPONSIBILITIES POLICY FOR SECURITY AND ACCESS OF UCSC ELECTRONIC INFORMATION RESOURCES

## I. PURPOSE/SCOPE OF THIS POLICY

This document describes and establishes policy regarding roles and responsibilities of employees and campus affiliates with respect to stewardship, security and access of campus electronic information resources (EIRs). An individual may perform any or all of the roles identified below depending on their relationship to a specific EIR.

## II. PRINCIPLES

### 1. Principles of Responsibility for Information Security

A fundamental principle of information security at UC Santa Cruz is that every individual in the University community has a responsibility for appropriate information management and protection of confidential and restricted information and EIRs, as defined by law or University policy, under their jurisdiction or control, and the access to them, according to their role(s).

### 2. Principles of Access to Information

#### a. Granting Access.

It is the policy and principle of UC Santa Cruz to allow broad access to public institutional information, as defined by the California Public Records and Information Practices Acts, and University policy (see References).

All confidential or restricted information, as defined by applicable federal and state statutes and regulations, and by University of California and campus policy, shall be restricted to authorized personnel. Access to confidential EIRs, including institutional information and reports generated from these resources, shall be provided to employees, campus affiliates, or others who are authorized for that data, when that information is relevant and necessary in the ordinary course of the performance of their official duties (otherwise known as "business need to know"), or as required by law.

Access to EIRs shall be modified or revoked in a timely fashion in response to changes in status, affiliation or authorization, or inappropriate use.

#### b. Use of Access.

Employees or campus affiliates who properly have access to confidential EIRs, as defined by law or University policy, including institutional information and reports generated from these resources, may not disclose information from these resources to others, except to the extent such disclosure is to other University employees or affiliates, and the disclosure is relevant and necessary to the performance of those others' official duties ("business need to know"), or as required by law.

Additionally, individuals may not use their access or seek out confidential information in any way that is not relevant and necessary in the ordinary course of the performance of their official duties, or that is inconsistent with the purpose for which the access was granted.

# ROLES AND RESPONSIBILITIES POLICY FOR SECURITY AND ACCESS OF UCSC ELECTRONIC INFORMATION RESOURCES

## III. DEFINITIONS

The following terms used in this policy are defined in the online *Glossary of selected terms in UCSC IT-related policies, procedures and guidelines*, available at http://its.ucsc.edu/security/policies/glossary.php.

Business "need to know" or "need to access"
Campus Information Privacy Officer
Campus Information Security Officer
Confidential Information
Data Integrator
Data Expert
Electronic Information Resource (EIR)
IT Security Committee (ITSC)
Public Information
Restricted data or information types (including personal identity information (PII))
Service Provider
System Steward

## IV. DETAILED POLICY STATEMENT: ROLES AND RESPONSIBILITIES

### 1. System Stewards (also known as Data Stewards).

a) **Responsibilities and Authority.** System Stewards have responsibility and authority for managing the information needed to conduct University business, in consultation with data expert(s) and Service Providers, as appropriate. The System Steward responsible for a given set of data has responsibility and authority for determining the purpose, function, appropriate access to and use of, degree of sensitivity, criticality, and risk tolerance of a data set in accordance with law or University policy and consistent with the mission of the University as a whole. This responsibility includes working in partnerships to ensure that individuals in other roles have the information necessary for appropriate implementation of policies, rules, and security requirements established by the System Steward.

b) **Accountability.** Although System Stewards may delegate day-to-day operations associated with the responsibilities listed above, they are ultimately accountable for the execution of these responsibilities and for any exposure to risk that may accrue to the campus as a result of their policy decisions.

### 2. Data Integrators.

Data Integrators have the same responsibilities for their integrated data as System Stewards (see above). Data Integrators must meet the combined security and access requirements of all original System Stewards whose data is included in the integrated data. They must also assess the risks associated with data aggregation or integration and identify and implement additional access and security requirements as appropriate.

# ROLES AND RESPONSIBILITIES POLICY FOR SECURITY AND ACCESS OF UCSC ELECTRONIC INFORMATION RESOURCES

**3. Data Experts and Functional Offices**

Data Experts (including Principle Investigators (PIs)) and Functional Offices are responsible for advising on the appropriate use, protection, access, degree of sensitivity, criticality, and risk tolerance of a specific data set.

**4. Service Providers.**

Service Providers are responsible for regular operational support, backup, maintenance, and security of EIRs, as well as for ensuring appropriate technical measures and checks are in place for the protection of EIRs under their control. These protections may be based on information provided by clients and System Stewards/Data Integrators. This responsibility includes working in partnerships to ensure that individuals in other roles have the information necessary for appropriate assessment of risk and of options to address risk.

**5. Campus Information Security Officer.**

The Campus Information Security Officer has overall responsibility for and management of the campus electronic information security program. The Vice Provost, Information Technology, is the Campus Information Security Officer for the Santa Cruz campus.

**6. Campus Information Privacy Officer.**

The Campus Information Privacy Officer has overall responsibility for and management of the campus information privacy program, as well as for overall campus information management and information requests. The Assistant Campus Provost is the Campus Information Privacy Officer for the Santa Cruz campus.

**7. UCSC Information Technology Security Committee (ITSC).**

The IT Security Committee (ITSC) is charged to coordinate and direct the development of appropriate policy to protect campus information assets and electronic systems. This charge also includes providing advice regarding education and communication that may be needed to support the policy and compliance measures developed, as well as resources needed for the campus to manage IT security.

**8. Unit or Departmental Managers/Supervisors and Deans.**

Unit or Departmental Managers, Supervisors and Deans are responsible for ensuring that all individuals have appropriate authorization, skills and training before access to campus EIRs is granted, and that access is modified or terminated promptly as appropriate in response to status, affiliation, or authorization changes.

**9. Individuals.**

All members of the University community are responsible for appropriate access, use and protection of information and EIRs to which they have access or over which they have jurisdiction or control. This includes storage and distribution of information. Individuals are responsible for working in partnership with Service Providers to ensure appropriate awareness and protection of confidential EIRs.

# ROLES AND RESPONSIBILITIES POLICY FOR SECURITY AND ACCESS OF UCSC ELECTRONIC INFORMATION RESOURCES

## V. APPLICABILITY AND AUTHORITY

**Applicability.** These roles and responsibilities apply to all campus electronic information resources as defined by the *University of California Business and Finance Bulletin Information Security (IS) Series* (see Definitions and References).

This is a new policy and thus supersedes any conflicting campus practices in existence prior to its effective date.

**Authority.** The campus Information Security Officer on behalf of the Office of the Chancellor and the Office of the Campus Provost/Executive Vice Chancellor is the campus authority for the policy on *Roles and Responsibilities for UCSC Electronic Information Resources.*

This policy was reviewed and approved by the Campus Provost/Executive Vice Chancellor on xx/xx/200x. Next review date is xx/xx/200x.

## VI. GETTING HELP

For questions or feedback about this policy, contact the ITS Service Manager for Community and Compliance at itpolicy@ucsc.edu or (831) 459-2779.

For information about laws or University policies relating to access to information at UCSC, contact the Operations Director in the Campus Provost/Executive Vice Chancellor's office (pco@ucsc.edu).

## VII. RELATED POLICIES/REFERENCES FOR MORE INFORMATION

**Related Policies and Procedures**

*UC Santa Cruz University Administrative Information System Access to Information Statement:*
http://its.ucsc.edu/services/accounts/online_forms/acc_info_stmt.pdf

*University of California Business and Finance Bulletins:*
IS Series - Information Security
http://www.ucop.edu/ucophome/policies/bfb/bfbis.html

RMP Series - Records Management and Privacy
http://www.ucop.edu/ucophome/policies/bfb/bfbrmp.html:

*University of California Electronic Communications Policy*
http://www.ucop.edu/ucophome/policies/ec/

*Other IT policies at the University of California:* http://www.ucop.edu/irc/policy/

*IT policies at UC Santa Cruz:* http://its.ucsc.edu/security/policies/

# ROLES AND RESPONSIBILITIES POLICY FOR SECURITY AND ACCESS OF UCSC ELECTRONIC INFORMATION RESOURCES

**References**

*State of California statutes:*

State of California Information Practices Act of 1977 (Civil Code Section 1798 *et seq*.)
http://www.privacy.ca.gov/code/ipa.htm

State of California Public Records Act (Government Code Section 6250 *et seq*.)
http://www.privacyprotection.ca.gov/code/pra.htm

*Federal statutes:*

Federal Privacy Act of 1974: http://www.usdoj.gov/foia/privstat.htm

## VIII. ATTACHMENTS

Under development:

- Additional guidance for fulfilling identified roles and responsibilities
- Educational information for System Stewards
- Identification of System Stewards for select categories of data (for illustrative purposes; not intended to be a comprehensive list)