Introduction and Background

The University of California, Riverside (UCR) utilizes 100s of electronic systems that store vast amounts of data and information. University of California (UC) policy requires appropriate safeguards of these cyber resources based on the sensitivity of data in question, legal requirements, and risks to the university.

For purposes of University security policy, electronic data resources can be classified as either essential, sensitive, or both. The following notes apply to these terms:

1. **Essential Electronic Resources.** Electronic data and information is classified as essential when it is required for campuses to conduct normal business operations. UCR’s central information technology organization, Computing and Communications (C&C), is responsible for these essential systems and data. C&C’s Disaster Recovery Plan contains a comprehensive inventory of these resources. A partial list of essential campus electronic systems is as follows:
   
   A. Student Information System.
   B. Payroll / Personnel System.
   C. Financial System (and related systems such as Purchasing).
   D. Electronic Mail System.
   E. Various Systems Required to Operate U.C.’s Data Network.

2. **Sensitive Electronic Resources.** Sensitive electronic information typically includes personal information relating to campus faculty, staff, and students (but not exclusively, since sensitive personal data relating to UC applicants, research subjects, etc. may be stored on university computers). Importantly, certain types of data (notably, protected personal data) receive special protection under California law and university policy. Please see cnc.ucr.edu/sb1386 for additional information on protected personal data.

UC policy (specifically Electronic Information Security Policy IS-3) requires each UC campus to evaluate its electronic information resources, determine which resources should be classified as essential and/or sensitive, develop local guidelines and/or policies for securing these electronic assets, and institute a mechanism for ensuring that these guidelines are appropriately implemented (to campus and departmental systems) and reviewed on a periodic basis.
The succeeding text summarizes UCR’s IS-3 campus implementation, including a definition of responsibilities, a suite of guidelines for developing appropriate security measures based on the sensitivity of the electronic resource in question, and a set of definitions relating to IS-3 and UCR’s local implementation.

**Responsibilities**

Under the direction of the Associate Vice Chancellor, Computing and Communications, C&C is responsible for developing appropriate security measures for essential campus systems and systems under C&C’s direct control that contains sensitive and/or protected data. C&C is further responsible for the following:

1. Developing and implementing a campus-wide IS-3 security plan.
2. Collaborating with unit and departmental staff (administrative and technical) to determine which non-C&C systems contain sensitive and/or protected data.
3. Developing guidelines that departments and units should consider when securing sensitive data.
4. Developing appropriate systems, structures, and communications mechanisms allowing departments and units to inventory (and report on) systems with sensitive and/or protected data.
5. Coordinating campus responses to security breaches involving both sensitive and protected data (especially relating to the requirements associated with SB1386).

**Departmental and unit responsibilities are as follows:**

1. **Electronic Information Resource Proprietors.** Units and/or departments must name Resource Proprietors who are responsible for the following:
   
   A. Identifying which computing systems contain sensitive and/or SB1386 protected data and information.
   
   B. Ensuring that appropriate procedures governing access to protected and sensitive data are implemented, and that adequate security plans (consistent with IS-3 and local campus guidelines) are in place for computing systems within their jurisdiction.
   
   C. Preparing an inventory of systems containing sensitive and/or protected data and reporting this inventory to C&C annually. The inventory includes the system’s location and use, its custodian, and an overview of measures in place to secure the system.
   
   D. Communicating the requirements and implications of UC policy and local campus guidelines with appropriate departmental and unit staff and any non-campus users of sensitive and/or protected data or information.

2. **Electronic Information Resource Custodians.** Units and/or departments must name Resource Custodians who are responsible for the following:
A. Protecting electronic resources under their control, such as access passwords, computers, and downloaded data.

B. Ensuring that contractual arrangements with non-campus entities include the third party’s obligations regarding sensitive and/or protected data.

C. Ensuring implementation of adequate security measures for computing systems containing sensitive and/or protected data (please see the section in this document relating to security measures).

**Guidelines for Securing Electronic Systems**

University policy calls for the utilization of appropriate safeguards to protect sensitive and/or protected information resources based upon the sensitivity of data in question, legal requirements, and risks to the university. These safeguards are expressed within a technical plan that addresses (at a minimum) the following:

1. Access Procedures and Controls.
2. System Administration Access Controls.
3. Software Development Controls.
8. Managerial Controls.
9. Disaster Recovery.

More information relating to system (server security) can be found at the following web site:

http://cnc.ucr.edu/avc/index.php?content=security

A complete enumeration of these guidelines is contained in Appendix A of this document. Appendix B contains definitions relating to systems security, UC policy, and local guidelines. Appendix C contains references and links to electronic resources.
Appendix A

Guidelines for Securing Electronic Systems - DETAILS

1. Access Procedures and Controls.

   Campus authorities, for example, Proprietors, should develop access policies (and username and password systems) and withdraw access when circumstances warrant.

   PLEASE NOTE: A major aid to controlling and monitoring who may gain access to specified services and data is to utilize the campus user identity management (authentication) system, specifically, a directory service that is a central repository for campus entities and affiliates. Employing a centralized identity management system provides a structure for easier password use and control by users since it facilitates single sign on and the utilization of fewer usernames and passwords.

   A second aid to controlling the roles that campus entities can perform is via the use of a centralized authorization infrastructure.

   Passwords.

   A. Several examples of acceptable use policies that promote the practice of good password strategies are as follows:

      UCR’s College of Engineering.
      http://www.engr.ucr.edu/systems/security.html

      University of Michigan (security campaign to help users practice safe password management).
      http://net-services.ufl.edu/security/public/passwords.shtml

      UCR C&C Access Policy.

   Access Logs.

   A. Systems should send log information in a secure fashion to a central host, where it can be scanned and saved in an automated way. This practice enables alerts to be sent if log information indicates suspicious activity.
B. Personally identifiable information should be protected in system logs or eliminated per UC policy and UCR Electronic Communications Policy guidelines.

2. **System Administration Access Controls.**

A. Privileged accounts should only be used when necessary; otherwise, administrators should be using normal user accounts.

B. All privileged account activity should be logged and monitored when related to essential and restricted data. The logged activity should connect to the same central log server as above.

C. The number of privileged accounts should be kept to a minimum, given only to those whose jobs require it, as determined by the Proprietor.

3. **Software Development Controls.**

A. At some point in the development life cycle, software must transition from a loose collection of functions and routines to a controlled and managed application. Once in production, the production version should be captured and preserved; then appropriate control measures should be in place for governing changes, testing, and the implementation of the tested version.

B. When third party software is being utilized, including operating systems and applications, management of this software should include similar controls (as outlined above) designed to ensure to a robust and secure production environment.

4. **Data Security.**

A. Stored data requires backups. These backups should be stored both locally, for easy recovery, as well as remotely (depending on the nature of the data), for disaster recovery. Both local and remote backups should be stored in a secure environment.

B. Systems storing electronic data should have the latest updates and patches (to both operating system software and application software); otherwise controls and procedures should be utilized when it is not possible to utilize the most current versions or patches.

5. **Communications Security.**

A. At its most basic level, communications security involves implementing systems and controls to restrict inappropriate traffic from penetrating systems and data stores.

B. When appropriate, firewalls should be utilized to restrict traffic to servers containing essential, sensitive, and/or protected data.

C. When appropriate, intrusion detection systems should be utilized. Since the volume of information generated by these systems can be large, a great deal of time is required for
tuning these systems to display information and send alerts when appropriate. However, such efforts may be warranted give the nature of the data requiring protection.

D. When appropriate, web server and data servers should be run on separate systems. This design permits private communication between the web system and the data system while simultaneously isolating essential, sensitive, and/or protected data from the general campus network (and possibly the Internet).

E. Any sensitive and/or protected data that is temporarily in electronic transition should be encrypted, and both the sending and receiving systems ought to be secured with access controls on both ends (for example, the receiver can only get data from sender, and the sender can only send data to receiver). This includes using certificates on web servers from vendors such as Verisign, or Thawte.


A. Host-based firewalls possess the advantage of customized protection and should be widely utilized.

B. Anti-virus protection should be mandatory for personal systems that send and receive data in some fashion (email, downloaded files, web browsing). Since users access and sometimes store sensitive and/or protected data on personal computers, it is important that these systems be protected against virus. Microsoft servers should also run anti-virus software.

C. Systems that play a role in the storage, access, and transfer of data should have current (and/or patched) and secure operating systems.

D. Systems should be monitored for correct hardware and software functioning, and an automated alert system should be utilized if possible.


A. All electronic information resources (especially those containing essential, sensitive, and/or protected data) should be housed in secure and environmentally appropriate facilities.

B. Monitoring systems should be in place to detect hazardous environment failures, such as power failure, high heat conditions, physical break-ins, moisture, etc.

8. Managerial Controls.

A. Employees hired to work with essential, sensitive, and/or protected data must undergo background checks prior to being granted access to any secure system.

B. In the event of breach or any modifications of user privileges, the Electronic Resource Proprietor must be promptly notified concerning the breach or the changes.
C. Procedures and/or systems must provide timely revocation of access privileges for individuals whose employment has been terminated.

D. When possible, no single individual should have authorization for both implementing software (and/or software updates) and maintaining production data containing sensitive and/or protected data.

E. Supervisors and other employees with responsibilities for sensitive and/or protected data should periodically review the work of system administrators (or others, e.g. database administrators) with privileged accounts.

9. **Disaster Recovery.**

A. Departments and units maintaining databases, web servers, etc. should create and periodically test disaster recovery plans aimed at restoring electronic systems after an unexpected calamity. Disaster recovery plans should be shared with business / functional staff to ensure information technology Disaster Recovery plans are included with campus Business Continuity plans.
Appendix B

Definitions relating to systems security, UC policy, and local guidelines.

Electronic Resource Proprietors: Electronic Resources Proprietors are responsible for identifying which computing systems contain protected Electronic Information Resources or have access to protected data. They will ensure that appropriate procedures are deployed for systems within their jurisdiction governing access to protected data and adequate security plans, consistent with Business and Finance bulletin IS-3. Data Proprietors will work with C&C to maintain an inventory of systems containing protected data. An up to date systems inventory will usually include the system’s location and use, its custodian, and type of security protection. Data Proprietors will inform their Data Custodians, affected staff within their jurisdiction, and third party users, of University policy and their responsibilities regarding any use they may make of protected data.

Electronic Resource Custodians: Electronic Resources Custodians are responsible for protecting the resources under their control, such as access passwords, computers, and downloaded data. Contractual arrangements with outside affiliates must include the third party users' obligations regarding protected data. Data Custodians will ensure implementation of adequate security measures for computing systems containing protected data (e.g. monitoring access logs for computing systems housing protected data can disclose unauthorized access or anomalous activity) as well as appropriate encryption strategies for both transmission and storage of protected data.

Electronic Information Resource: Electronic Information Resources are a resource used in support of the University business administration that involves the electronic storage, processing or transmitting of data, as well as data itself. Electronic Information Resources include application systems, operating systems, tools, communications systems, data- in raw, summary, and interpreted form- and associated computer server, desktop, communications and other hardware used in support of University business administration.

Security: Measures taken to reduce the risk of 1) unauthorized access to Electronic Information Resources and 2) damage to or loss of Electronic Information Resources through any type of disaster. Security also encompasses measures taken to reduce the impact of any violation of security or a disaster that occurs despite preventative measures.

Authorized User: An Authorized User is a University employee, student or other individual affiliated with the University who has been granted authorization by the Electronic Information Resource Proprietor, or his or her designee, to access an Electronic Information Resource for the purpose of performing his or her job duties or other affiliation with the University.
Appendix C

References and links to electronic resources.

1. National and State Resources

   A. California Information Practices Act of 1977 (IPA)
      (http://www.privacy.ca.gov/code/ipa.htm)

   B. California Public Records Act (CPRA)
      (http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=06001-07000&file=6250-6270)

   C. Federal Family Educational Rights and Privacy Act of 1974 (FERPA)
      (http://www.ucop.edu/ucophome/policies/bfb/rmp8.html#IV)

2. University of California Resources

   A. UCOP Electronic Communications Policy, November 17, 2000
      (http://www.ucop.edu/ucophome/policies/ec/)

   B. UCOP Policies Applying to Campus Activities, Organizations, and Students, August 1994
      (http://www.ucop.edu/ucophome/uwnews/aospol/toc.html)

   C. UC Business and Finance Bulletins
      (http://www.ucop.edu/ucophome/policies/bfb/is3toc.html)

   D. UCOP IS-3, Electronic Information Security
      (http://www.ucop.edu/ucophome/policies/bfb/is3toc.html)

   E. UCOP IS-10, Systems Development and Maintenance Standards
      (http://www.ucop.edu/ucophome/policies/bfb/is10.pdf)

   F. UCOP RMP-8, Legal Requirements on Privacy of and Access to Information
      (http://www.ucop.edu/ucophome/policies/bfb/rmp8toc.html)

3. University of California, Riverside Resources

   A. Campus Policies and Procedure Manual
B. UCR Server Side Security and Firewalls
(http://cnc.ucr.edu/security/index.php)