

SECURITY FOR ELECTRONIC INFORMATION AT UCSD

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	IMPLEMENTATION AT UCSD	1
III.	ELECTRONIC COMMUNICATIONS AND ESSENTIAL ELECTRONIC INFORMATION RESOURCES	2
IV.	PROPRIETORS: UCSD POSITIONS HAVING DIRECT RESPONSIBILITY FOR ELECTRONIC INFORMATION RESOURCES	2
	Table 1, Requirements for Resource Security Under IS-3	
	Table 2, EIR Proprietor Assignment	
V.	UCSD PHYSICAL SECURITY GUIDELINES FOR ELECTRONIC INFORMATION RESOURCES	4
VI.	VIEW OF PHYSICAL SECURITY	4
	A. Inventory	4
	B. Physical Issues	5
	C. Disaster Scenarios	5
	D. Procedural Issues	5
VII.	UCSD LOGICAL SECURITY GUIDELINES FOR ELECTRONIC INFORMATION RESOURCES	5
	A. Authentication and Authorization	5
	B. Revision control	5
	C. Logging	5
	D. Backup	5
	E. Privacy	5
VIII.	CONCLUSION	6

[SUPPLEMENT I, Physical Security Considerations](#)

[Table 3, Example: Physical Inventory](#)

[SUPPLEMENT II, Logical Security](#)

[SUPPLEMENT III, Guidelines for Secondary Holders](#)

[Table 4, Case Student Sensitivity/Criticality Checklist](#)

[SUPPLEMENT IV, References and Related Links](#)

SECURITY FOR ELECTRONIC INFORMATION AT UCSD

I. INTRODUCTION

The University of California Office of the President issued Business and Finance Bulletin (BFB) [IS-3, Electronic Information Security](#), on November 12, 1998. Campuses are required to establish local implementation guidelines for electronic information resources (EIRs) in their control. Individuals should become familiar with it before reviewing UCSD implementation guidelines.

The UCSD Electronic Information Security Task Force (EISTF), a campus-wide advisory group to the Administrative Computing and Telecommunications Policy Committee (ACTPC), was charged to establish local procedures and practices for implementing [BFB IS-3](#). The EISTF is active in classifying information resources for disaster-recovery planning, establishing standards and practices for providing security based on data levels described in [BFB IS-3](#) and communicating requirements to the UCSD community.

II. IMPLEMENTATION AT UCSD

UCSD has designated the Director of Academic Computing Services (ACS) as coordinator for this policy.

In conjunction with the ACS Manager of Network Security, the coordinator will:

- Develop campus guidelines for determining which positions have job responsibilities that directly support Essential EIRs.
- Develop campus guidelines for the physical security of EIRs.
- Develop campus guidelines for the logical security of EIRs.
- Conduct an annual survey of EIR holders to determine which EIRs are both “Essential” and “Restricted” [See [Table 2](#), Electronic Information Resources – Proprietor Assignment]
- Verify that Essential EIRs have a disaster plan.
- Verify that Essential EIRs have a backup procedure.
- Review the physical security controls for Essential-Restricted EIRs.
- Review the logical controls (access control, change management, backup and retention, communications security, and protection against intrusive software) on Essential-Restricted EIRs
- Verify with EIR holders that managerial security guidelines from [BFB IS-3](#) have been established to pertain to those positions that have access to Essential EIRs.
- Verify that security roles are filled for Essential EIRs.
- Communicate problems that are revealed by the surveys to responsible management and provide advice on appropriate remedies.
- Track, take preventative measures, and react to intrusive computer software (viruses, etc).

This document offers guidelines intended to reduce risks to Electronic Information Resources through preventative measures and controls. The guidelines apply to certain EIRs on all campuses in the UC System including applications, operating systems, communication systems, data, and associated hardware used in University business administration. Holders of other forms of data, such as research data, would benefit from applying the guidelines as well.

III. ELECTRONIC COMMUNICATIONS AND ESSENTIAL ELECTRONIC INFORMATION RESOURCES

Most, if not all, Essential EIRs depend on the reliable operation of network and other electronic communications services. Short of a natural disaster these services can and must be made reliable enough that they can meet the requirements of an Essential EIR. It should be understood, however, that during large-scale outages, such as those that would be experienced during the aftermath of a major earthquake, most electronic communications services would not be fully operational. The intended recipient may not be physically present or able to receive communications or may be present but not have a working method for access. For this reason, those doing disaster planning should provide for alternate, reliable, methods to communicate with and access Essential EIRs.

Store-and-forward services such as voicemail and email depend on there being a recipient present who is equipped with a functioning access device. This will not be the case in most large-scale outages. Disaster planners should develop procedures that verify that essential communications are actually received.

Network connectivity is dependent on the physical integrity of infrastructure spread over a large geographic area. During a large-scale event it is likely that connectivity to Essential EIRs will not be available from all areas of the campus. Planners should provide for minimal access at a facility close to the Essential EIR processing facility.

IV. PROPRIETORS: UCSD POSITIONS HAVING DIRECT RESPONSIBILITY FOR ELECTRONIC INFORMATION RESOURCES

In order to determine the applicability of [BFB IS-3](#) to specific electronic information resources at UCSD, the EISTF developed [Table 2](#), Electronic Information Resources – Proprietor Assignment. UCSD EIRs were identified and classified according to definitions found in [BFB IS-3](#) and [Table 1](#), Requirements for Resource Security, below. Holders are required to address issues of Disaster Recovery, Backup, Logical and Physical Security, and Personnel Security as is appropriate to the cell of [Table 2](#) containing their EIR.

TABLE 1 – REQUIREMENTS FOR RESOURCE SECURITY UNDER IS-3

		Resource Criticality		
		Essential	Required	Deferrable
Sensitivity	Restricted	Requires access security; must be in Disaster Recovery plan	Requires access security; may be in DR plan	Requires access security; need not be in DR plan
	Unrestricted	Minimal security required; must be in DR plan	Minimal security required; may be in DR plan	Minimal security required; need not be in DR plan

TABLE 2 – ELECTRONIC INFORMATION RESOURCES –PROPRIETOR ASSIGNMENT

	Criticality			
		Essential	Required	Deferrable
Sensitivity	Restricted	ISIS/SAM IFIS Monthly and Bi-Weekly Payroll Payments ACT Authentication System Student Financial Services Name Service * Network ** Email gateway	ISIS PPS Non-ISIS Student Systems Authentication Systems Kerberos DHCP/BOOTP Active Directory Network Operations Email distribution Restricted Course Sites Instructional Support Servers Library Automation – Circulation Student Health Services	Non-IFIS Financial Systems Non-PPS Personnel/Payroll Development BFS Applications HR Applications Recharge Billing Systems Dial In Grant Proposals Link Family (Individual members may be Required)
	Unrestricted	Emergency Telephone System 800MHz Radio System EH&S Applications	Telephone Basic Network Services Library Automation – Public Access Open Course Web Sites Darwin/SQLDSE InfoPath Internet Service Physical Plant Applications	Grant Reporting Wireless Services

* Backup in ACT.

** Portions necessary to provide sufficient access for minimal processing.

Notes:

Some portion of IFIS, ISIS and PPS must be running as soon as possible since some functions such as check-printing (related to payroll and financial aid) are Essential/Restricted. Lower criticality activities such as payroll update, can be relegated to the Required or Deferrable column. The applications and databases that support IFIS, ISIS and PPS are somewhat inseparable so the large subsystems or the entire facility is placed in the cell appropriate to the most critical/sensitive aspect.

General network access to IFIS, ISIS, and PPS outside of Torrey Pines Center South (TPCS) is probably infeasible immediately following the worst kind of disaster so Data Network related activities have been relegated to the Required column. This implies that there be some network services available in ACT to support rudimentary operations.

Basic Network Services include on-campus connectivity, routing and name service.

Outages can occur for a wide variety of problems – local to campus wide and more. A longer outage might be acceptable during a widespread outage. Downtime near a deadline may shorten the acceptable outage length. Individual proprietors must establish appropriate standards for acceptable downtime.

During an outage that covers all or most of the campus it is impractical to expect or require that electronic records will be available in *all* locations. Units that are expecting to have such records available should include provision for hardcopies in their disaster plans.

Anything not listed is either not covered by [BFB IS-3](#) or can be deferred for a much longer interval.

V. UCSD PHYSICAL SECURITY GUIDELINES FOR ELECTRONIC INFORMATION RESOURCES

The purpose of physical security planning is to provide protection for UCSD facilities housing information system resources, the system resources themselves, and the facilities used to support their operation. Goals include:

- Documentation of service interruption/disaster controls.
- Appropriate network isolation, both within segment and externally.
- Secure housing for computers and network distribution equipment.
- Secure storage of media and output.

The intent of this section is to provide UCSD administration managers and network administrators with an overview of a practical approach for developing both physical and environmental security capability within their organizations. Use this section of the implementation guidelines and [Supplement I, Physical Security Considerations](#), as a tool to help define the organization's physical EIRs and procedures for keeping them physically secure.

VI. VIEW OF PHYSICAL SECURITY

Physical Security is defined as measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. Such threats, and the measures taken to mitigate them, depend on four factors:

A. Inventory

Refer to Section 7 of [BFB IS-3](#), Electronic Information Security, with regard to completing an inventory of equipment for all critical, Restricted, Essential, etc. systems. Organizations should make and maintain inventories of Physical EIRs in accordance with [BFB BUS-29](#), Management and Control of University Equipment. This physical inventory, together with the inventory of data used by the organization, can be the point of departure for constructing policies and procedures.

B. Physical Issues

The basic physical characteristics of the UCSD facility housing the information system or systems determine the level of such physical threats as fire, roof leaks, or unauthorized access. In particular, whether the facility is fixed (e.g., a building), or mobile (e.g., a trailer or boat) is significant in deriving appropriate security measures.

C. Disaster Scenarios

The particular location of the UCSD facility housing the information system or systems determines the characteristics of natural threats (including earthquakes and flooding), man-made threats (such as burglary, civil disorders, or interception of transmissions and emanations), and damaging nearby activities (including toxic chemical spills, explosions, fires, and electromagnetic interference from emitters such as radar).

D. Procedural Issues

The operation of UCSD information systems sometimes depends on supporting materials such as special forms, unique hardware (e.g. check printers), etc. The failure or substandard performance of these materials may interrupt operation of the system and may cause non-performance of critical systems in the event of a disaster.

VII. UCSD LOGICAL SECURITY GUIDELINES FOR ELECTRONIC INFORMATION RESOURCES

“Logical” security appropriate to an EIRs placement in the matrix is mandated by the [BFB IS-3](#). The purpose of logical security planning is to ensure the reliability and integrity of the data being secured, and to prevent its unintentional disclosure.

Logical security can be considered to consist of 5 factors:

A. Authentication and Authorization

Controls must be in place to ensure that requested access to an EIR is allowed (*authorization*), and that the entity requesting the access is what it appears to be (*authentication*). It is generally desirable to somewhat decouple these so that new schemes for either may be introduced as technology and need decree.

B. Revision control

Appropriate procedures must be documented and in place such that modification to software or data can be tracked and audited.

C. Logging

Activity logs must be enabled and reviewed regularly for signs of anomalous events.

D. Backup

Data and associated software systems need to be backed up on an appropriate schedule, and backups stored in a location which meets the security needs of the *most* critical or sensitive EIR expected to be present on any of the media.

E. Privacy

Data must not be accessible, either on the server or in transit, by non-authorized entities.

VIII. CONCLUSION

[BFB IS-3](#) is a long and complex guideline whose goals are to educate the University population about the need to protect data resources and to establish a framework that will ensure that the most critical resources are protected. To that end, we have created this local guideline, which should be of use to all departments whether they are the proprietors of any Essential Information Resources or not.

For those holders of EIRs these local implementation guidelines mandate certain actions from the campus, and by extension, campus departments.

The IS-3 Coordinator will conduct an annual survey of incumbents of certain titles and positions to identify EIRs. This list will include:

- Programmer/Analyst III, IV, and V (including Supervisors)
- Computer Resource Manager II and III
- Senior and Principal Administrative Analyst
- Management Services Officer

These individuals will review data resources held by their departments and identify EIRs based on the technical definitions of Essential and Restricted contained in [BFB IS-3](#).

For EIRs in their charge, they will:

- A. Complete the Logical Security Checklist.
- B. Complete the Physical Security Checklist.
- C. Describe their backup plan.
- D. Describe their disaster recovery plan. These forms will be returned to the Coordinator for review. The Coordinator will track compliance with these guidelines.

PHYSICAL SECURITY CONSIDERATIONS

Inventory

Physical inventory of equipment must be completed and maintained on a regular basis. The example *Physical System Matrix* below has been provided as a guide to developing a matrix of information systems and their physical security components. A suggested course of action:

- Identify what equipment is required for Essential-Restricted [see [Table 2](#), Electronic Information Resources – Proprietor Assignment] services
- Identify servers on which Essential-Restricted data resides
- Identify any clients that must be used to access Essential-Restricted data
- If the Essential-Restricted function(s) are not self-contained, identify what interconnect equipment is required
- Inventory the parts of this interconnect (hubs, switches, etc) that are your organization's responsibility.

Best practice: Install Restricted-Essential servers in monitored, secured, non-public space. This "server room" must be climate-controlled with sufficient backup power to enable 60 minutes of functionality/soft shutdown time if power is interrupted.

Physical Issues

Properly applied, physical security controls can prevent losses due to interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft.

Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a local area network (LAN) server(s).

Consider both normal access and surreptitious access when evaluating methods for restricting physical access. Restricting normal access may include barriers that isolate each area, entry points in the barriers, and screening measures at each of the entry points (e.g., badges or card-key devices). Physical modifications to barriers can reduce the vulnerability to surreptitious entry. Intrusion detectors, such as closed-circuit television cameras, motion detectors, and other devices, can detect intruders in unoccupied spaces.

Access for the people in the following categories:

- Computer Operations
- IT Staff
- Service and Maintenance Personnel
- Security Guards
- Non-affiliated Personnel (visitors, delivery agents)

must be defined to ensure that only those with proper authorization can access various restricted areas, including;

- Server Room
- Wiring Closets
- Mechanical Room
- Secured Forms-Rooms
- Data Vault

**UCSD POLICY AND PROCEDURE MANUAL
COMPUTING SERVICES**

Section: 135-7 SUPPLEMENT I PAGE 2

Effective: 9/15/2003

Supersedes:

Issuing Office: Academic Computing Services/Administrative Computing & Telecommunications

Physical access controls must be addressed not only for areas containing system hardware, but also for locations containing wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation.

Things to consider include:

- Ensure secure area architecture
 - Walls all the way up to the ceiling (no access to secured area via air plenum)
 - Doors that swing shut and locked with hinges *inside* the secured space
 - Motion detectors/alarms for spaces not staffed 24x7
 - Access via card/key/cipher lock; preferably logged
- How is access granted? How is it revoked? How often are access logs checked?

Disaster Scenarios

The particular location any of the UCSD facilities housing the critical information system or systems determines the characteristics of natural threats (including earthquakes and flooding), man-made threats (such as burglary, civil disorders, or interception of transmissions and emanations), and damaging nearby activities (including toxic chemical spills, explosions, fires, and electromagnetic interference from emitters such as radar). Risk assessment must be considered when developing disaster control plans and should take into account the areas above.

Items to be included in developing plans for protecting utilities that support an organization's information systems include:

- Identifying the failure modes of each utility (air conditioning, electric power distribution, heating plants, water, sewage, and other utilities) required for system operation or staff comfort.
- Determining the need for dual-redundant or backup utilities for critical system support (such as Uninterruptible Power Supplies).
- Ensuring that emergency lighting exists in computer rooms.
- Ensuring that supporting utilities such as power distribution panels, communications and telephone closets, and air conditioning systems, when located outside restricted zones established within the facility are appropriately secured by such measures as locks.
- Considering the screening or filtering of external openings for air condition systems to protect against the insertion of hazardous objects or the intrusion of pollutants.
- Ensuring, if possible, that utility service lines (water, gas, oil, etc.) that provide support to facilities enter the building underground or are physically protected by other means, such as enclosing exposed lines in conduit, installing barriers around water and gas mains or meters, and locking fuel tank inlet pipes.

Items to be included in developing plans for preventing the structural collapse of an organization's facility include:

- Determining, for a building in the construction planning stage, the likelihood of structural collapse due to natural or man-made disasters, such as an earthquake, major fire, gas explosion or sabotage, again ensuring that adequate precautions are taken regarding structural design strengths.
- Ensuring hardware is strapped or secured where open racks are used.

Items to be included in developing plans for preventing plumbing leaks include:

- Locating plumbing lines that might endanger system hardware. These lines include hot and cold water, chilled water supply and return lines, steam lines, automatic sprinkler lines, fire hose standpipes, and drains. If a building includes a laboratory or manufacturing spaces, there may be other lines that conduct water, corrosive or toxic chemicals, or gases.

Items to be considered in developing plans for guarding against the interception of data include:

- Guarding against interception of data transmissions. If an intruder can gain access to data transmission lines, it may be feasible to tap into the lines and read the data being transmitted. Improperly secured wireless (802.11b) networking can also be easily co-opted; wireless access must be closely monitored.
- Preventing electromagnetic interception. Systems routinely radiate electromagnetic energy that can be detected with special-purpose radio receivers.

Depending on the scale of the operation, not all of these may apply, though power and environmental (temperature, humidity) control must be considered.

Procedural Issues

- Special forms and hardware (e.g. AP and Payroll check stock, special forms printers) for unique processing must be inventoried.
- Backup form stock, hardware and tapes must be stored in offsite vault area.
- Procedures for access to the stock and hardware and the circumstances under which that access may occur must be codified and documented.

Things to consider:

- How are backup tapes for servers housing Restricted/Essential data handled?
- Where are the tapes stored? How are the tapes transported to the storage facility?
- Are there logs of what data is on which tapes, and where the tapes currently are? Are these logs verified? How often?
- Input/stock forms: what type of sensitive stock (paychecks, official seal stock) is kept, and where? How is it accounted for?
- Output: how is access to sensitive output controlled?

LOGICAL SECURITY

Authentication and Authorization

Access to *Restricted* Electronic Information Resources must be limited to authorized users. Authentication methods must be periodically reviewed in light of current technological advances.

For each *Restricted* EIR procedures must be in place that address the following issues:

- How is an authentication token (account) granted? When? Who authorizes new authentication tokens? Are “temporary” tokens permitted?
- How is authentication revoked? Under what circumstances may this happen?
- How often are authentication tokens audited?

Strong authentication methods have at least two of the following three properties:

- something the entity has (e.g. a hardware token which will generate a password)
- something the entity knows (e.g. a password)
- something the entity *is* (e.g. fingerprint)

Currently, the general authentication mechanism tends to be login name/password combinations, which really use only the second property. Until circumstances change, therefore, passwords must be carefully constructed to make them difficult to guess. Password-based authentication mechanisms must possess rules which enforce selection of strong passwords. Passwords must be kept securely; they should not be written down.

Authentication tokens for *Restricted* or *Essential* data should not be shared between entities. If it is imperative that such sharing occur, a special token must be constructed, and the use of this token monitored.

The Principal Holder of the EIR will specify authorization procedures.

“Superuser” accounts often possess the ability to circumvent established authentication and authorization schemes on locally kept data. The following guidelines must be enforced:

- access to superuser accounts must be limited to personnel whose job duties require them.
- provide superusers with less powerful accounts to use when not performing system administration tasks.
- superuser accounts should not be used for other than authorized purposes.
- activities performed using a superuser account must be securely logged, and those logs reviewed periodically.

Revision Control

Development and maintenance of administrative applications performed by University personnel or performed by any vendor engaged by University personnel must conform to the specifications of [BFB IS-10](#), Systems Development Standards.

Logging

Activity logging is an important tool for logical security. Where ever possible, logs should be made recording:

- system access
- authentication (especially failed authentication attempts)
- data access
- software or data modification
- elevation of privilege

Logs, once made, should be monitored for anomalies, preferably by automated means (to protect authorized user privacy, where applicable, and also to provide timely notification of potential problems). Systems containing Restricted EIRs must log, and those logs must be closely monitored. All logs must be retained according to defined data retention schedules; must be backed up following the most stringent requirements governing the criticality and/or sensitivity of the EIRs involved in the logged activity.

As logs themselves may contain sensitive information (account names, passwords, individual usage patterns), they must be kept securely, ideally on a separate machine dedicated to logging (secured against unauthorized access) and/or on write-once media.

Backup

The purpose of Backup (as distinct from Archive) is to protect the system from unintentional loss or catastrophic system failure. Most EIRs will require some sort of regularly scheduled backup; *Restricted* and *Essential* EIRs must have a clearly defined schedule and procedure.

Backups must be treated according to requirements of the most critical/sensitive data contained therein; if an EIR is in the *Restricted-Essential* category, guidelines for scheduling of backups and storage of media must be consistent with the corresponding Disaster Recovery Plan. In any event, backups must be periodically verified by performing test restores – the time to find out that things are not working is not when the data has gone missing.

Physical security of backup media must be consistent with requirements for the EIRs backed up.

An acceptable backup plan will address the following issues:

- how often are backups performed?
- Who is responsible for ensuring that backups are done?
- How is the media labeled?
- Where is the media stored?
- How often is the backup process verified (by performing a test restore), and whose responsibility is the verification?
- When is the media eligible for reuse?

Privacy

All access to *Restricted* data must be restricted to authorized entities only. This implies that proper access controls be in place on any system on which such data resides, and any place it might pass in transit. *Restricted* data

- Must be encrypted whenever it is transmitted (encryption accomplished either by the medium or at the endpoints of the transmission)
- Must be stored in a manner consistent with its sensitivity (servers must be secured

Supersedes:

Issuing Office: **Academic Computing Services/Administrative Computing & Telecommunications**

- against unauthorized use)
- Must not be kept in insecure circumstances (unencrypted on a desktop, for example)

In defining data privacy standards, the following questions must be addressed:

- How is the data access authorization defined? How is it maintained?
- How is access to the server containing the data appropriately controlled?
- What logging is in place to guard against unauthorized access?
- What applications access the data? If they are run from client machines, how is the privacy of the data in transit maintained?
- What procedures are in place to prevent unauthorized "cacheing" of the data in non-secure environments (office desktops, for example)

UCSD GUIDELINES FOR *SECONDARY* HOLDERS OF DATA DERIVED FROM RESTRICTED ELECTRONIC INFORMATION RESOURCES

Holders of EIRs derived from primary sources are required to maintain the same level of access security as are found on the primary source. Disaster recovery requirements, however, will vary depending on the criticality of the EIR to end-users and on the difficulty of reconstructing it from the primary source.

[Table 1](#), Requirements for Resource Security Under IS-3, indicates the level of access security and disaster recovery protection that are required. Note that access security has three components: Logical Security, such as access control (approval procedures, passwords, logs, etc.), Physical Security (locked rooms, protection from physical damage), and Managerial Security

Steps to determining security requirements

- Identify your data sources. What information do you have that is derived from primary EIRs or contains information that needs to be protected?
- Where does it fit in the grid? Required/restricted etc? See [Table 1](#), Requirements for Resource Security under IS-3, and [Table 4](#), Sensitivity/Criticality Checklists.
- Implement appropriate procedures based on level of sensitivity/criticality.

Case studies: Classifying data for Risk, Sensitivity and Criticality

The following case studies concern four different Organizational Units – A, B, C, and D. Each of these organizations answers the checklist of questions to determine the level of sensitivity and criticality of the data it manages.

Step 1 Identify the resources. In this example four secondary systems either derive data from, or provide data to, primary Electronic Information Resources holders (Proprietors).

Supersedes:

Issuing Office: Academic Computing Services/Administrative Computing & Telecommunications

Step 2 Using the checklist below, assign sensitivity and criticality to each resource.

TABLE 4: SENSITIVITY/CRITICALITY CHECKLISTS

Case Study Sensitivity/Criticality Assignment		
Case Study	Description	Assignment
OU-A	Department maintains records of salary information supplemental to the employee's normal appointment salary. This information is uploaded to PPS monthly, and the employee's paycheck amount reflects both the salary based on job title and level, and the supplemental amount. Until upload, this additional amount only resides in the secondary resource holder's systems.	Restricted/ Essential
OU-B	Department maintains a labor clearing account database for salary recharge. All employees are paid from a single departmental fund. A journal is uploaded to IFIS monthly that debits various indexes and credits the clearing account fund. The amount debited per index reflects the time an employee works on the project represented by that index.	Restricted/ Deferrable
OU-C	Department maintain a database of student information for residential management. Student data are downloaded from ISIS including SSN and PID. These data are supplemented with additional student self-reported info such as living preferences and/or medical conditions.	Restricted/ Deferrable
OU-D	Department maintains a graduate application and recruitment database. The data are downloaded from OGSR and supplemented/modified to include recruitment decisions and process information.	Restricted/ Required

Sensitivity/Criticality Checklist					
Type	Description	OU-A	OU-B	OU-C	OU-D
S1	Does the data include information that identifies or describes an individual?	YES	YES	YES	YES
S2	Would unauthorized access, modification, or loss of the data seriously affect the University?	YES	NO	NO	YES
S3	Would unauthorized access, modification, or loss of the data seriously affect a business partner of the University?	NO	NO	NO	NO
S4	Would unauthorized access, modification, or loss of the data seriously affect the public?	NO	NO	NO	NO
S5	Has the Proprietor chosen to protect the data from general access or modification?	YES	YES	YES	YES
C1	Does PPS directly depend upon the resource for ongoing successful operation?	YES	NO	NO	NO
C2	Does the campus data network directly depend upon the resource for ongoing successful operation?	NO	NO	NO	NO
C3	Does the campus telephone system directly depend upon the resource for ongoing successful operation?	NO	NO	NO	NO
C4	Does the campus public safety system directly depend upon the resource for ongoing successful operation?	NO	NO	NO	NO
C5	Will the campus be unable to perform an important administrative function correctly and on schedule if the resource fails?	NO	NO	NO	NO
C6	Will the campus sustain a significant loss of funds if the resource fails to function correctly and on schedule?	NO	NO	NO	NO
C7	Will the campus sustain a significant liability or other legal exposure if the resource fails to function correctly and on schedule?	YES	NO	NO	NO
C8	Will the campus be able to continue operation for a designated period of time if the resource fails to function correctly and on schedule?	YES	YES	YES	YES*
C9	Will the campus be able to continue operation for an extended period of time if the resource fails to function correctly and on schedule?	YES	YES	YES	NO

*Depends on the time of year

Supersedes:

Issuing Office: Academic Computing Services/Administrative Computing & Telecommunications

Step 3 - Evaluate existing security procedures compared to requirements based on sensitivity/criticality assignment.

Example 1 – OU-A

Department A's local personnel database was determined to have a sensitivity level of restricted and a criticality of essential, requiring this EIR to both be in a disaster recovery plan and to require access security.

Disaster Recovery Plan			
	Recommended Steps	Actual	Actions required
Process	Create formal plan	None in writing. Informal procedures in place.	Create formal disaster recovery plan.
	Update plan	Not done	Ongoing after step above
	Test plan	Not done formally.	Ongoing after step above
	Coordinate with campus	No formal coordination in place	Develop plan with ACT how to coordinate uploads of PPS data
	Include disaster recovery in vendor agreements	Not applicable	None
Plan	Provide for running on alternative sites or by alternative methods	Servers running the same OS and NOS are available offsite, and could be restored to functionality from backup tape in under a day.	None
	Specify emergency response procedures	No formal procedure in place.	Develop formal procedure.
	Include requirements and procedures for offsite backup	Tapes are stored offsite weekly (at employee's residence) but no formal procedure in place.	Develop formal procedure. Consider commercial vendor for secure storage in addition to informal procedures.

REFERENCES AND LINKS

RELATED UC SYSTEMWIDE AND UCSD LINKS

UC Business and Finance Bulletin Manual (BFB)

[IS-3](#) Electronic Information Security
[IS-10](#) Systems Development Standards

[UC Electronic Communications Policy](#)

UCSD Policy and Procedure Manual (PPM)

[135-3](#) UCSD Network Security Policy
[135-5](#) UCSD Email Procedures and Practices.
[135-6](#) UCSD Web Policy Procedures and Practices.

REFERENCE SITES:

Professional Practices for Business Continuity Planners
(<http://www.drii.org/displaycommon.cfm?an=2>)

MIT Business Continuity Planning site
(<http://web.mit.edu/security/www/isorecov.htm#public-plan>)

The Business Continuity Planning & Disaster Recovery Planning Directory
(<http://www.disasterrecoveryworld.com/>)

Security Self-Assessment Guide for Information Technology Systems
(<http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>)

Disaster Recovery Journal (<http://www.drj.com/>)
DRJ free links page (<http://www.drj.com/freelinks/links.html>)

Disaster Planning for Libraries: Lessons from California State University, Northridge
(http://www.access.gpo.gov/su_docs/fdlp/pubs/proceedings/99pro29.html)

Techniques for System and Data Recovery
(<http://csrc.nist.gov/publications/nistbul/itl02-april.txt>)

A PDF file containing the original document can be found at

<http://www.ucop.edu/ucophome/policies/bfb/bfbis.html>.

Readers should become familiar with it before reviewing UCSD implementation guidelines. An unofficial HTML version of this document can be found at http://isecurity.ucsf.edu/ucop_is3.html.

Section VII of [BFB IS-3](#) (Electronic Information Security) states: "Each campus should establish procedures for the physical protection of its Electronic Information Resources (EIRs)."