UC San Diego
Policy & Procedure Manual

COMPUTING SERVICES
Section: 135-7 SUPPLEMENT III
Effective: 09/15/2003
Supersedes: N/A
Review Date: TBD
Issuance Date: 09/15/2003
Issuing Office: Administrative Computing & Telecommunications (ACT)

SUPPLEMENT III

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).

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

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.