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

SUPPLEMENT I

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

Physical access controls must be addressed not only the 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?

TABLE 3: Example: Physical Inventory

Physical System Matrix

SYSTEM	CRITICALITY			SENSITIVITY		FORMS	Hardware Inventory Required	Client Software Required	Procedures Y/N
	Essential	Required	Deferrable	Restricted	Unrestricted				
IFIS	x			x		x	9672(1), E4000(2), SunBlade(4), modems, switches, routers	TN3270, etc..	
ISIS	x			x		x	9672(1), E4000(2), SunBlade(4), modems, switches, routers		
PPS	x			x		x	9672(1), E4000(2), SunBlade(4), modems, switches, routers		
Email		x		x			NT Servers(x)		
Non-ISIS Systems		x		x			Sun Server(x)		
Kerbros Authentication		x		x					
Dial-In			x	x			Modem(x), Switch(x), Router(x)		
Non-IFIS Systems			x	x					
Non-PPS Systems			x	x					
800 MHz Radio	x				x				
Telephone		x			x				
Link Family			x		x		9672(1), E4000(2), SunBlade(4), modems, switches, routers		
Wireless			x		x				
Research Models	x								
Provisional Controls	x								
Department Email		x		x			NT Servers(x)		
Department Servers		x		x			Sun Server(x)		
Department Calendars		x		x		x	Sun Server(x)		
Access Controls									x
Fire controls									x
Offsite Procedures									x
Tape Inventory Procedures									x
Escalation Procedures									x