Server Room Standard

Objective

Servers should be located in the ViaWest data center when feasible because it offers the optimal mix of physical security and environmental control; servers placed within the ViaWest data center are automatically considered compliant for all data center security requirements.

If location of servers in the ViaWest data center is not feasible, the chosen server room must comply with the following standard. Any room containing one or more computers used to provide services to a group of users via the network is considered a server room. This ranges from small server closets to larger datacenters.

Location

Site locations should be chosen to ensure both proper environmental and physical controls:

- Site locations should be safe from exposure to fire, flood, explosions and other similar hazards.
- Server rooms should be located in areas where noise will not disturb classrooms, offices, etc.

Perimeter Security

All server rooms should have solid walls extending from the floor to ceiling. In areas where raised floors or a drop ceiling are in place, walls should extend below the raised floor and above the drop ceiling to prevent an individual from entering the room by climbing under the raised floor or over the wall by accessing the maintenance space. Locked racks or a cage may also be used to provide a secure perimeter layer.

Physical Access

Physical access to the server room must be limited to only those individuals who have legitimate responsibilities justifying such access. Use of card readers and electronic locks to permit access is recommended over traditional keys; if keys are used, they must be marked “Do Not Duplicate.” Procedures must be in place to ensure access is removed when an individual no longer has such need and access lists of authorized individuals must be reviewed at least quarterly by data center owners. Procedures must also be in place to address lost or stolen keys or access cards.

- Video cameras are recommended to monitor and record individuals entering or working in the space.
- When warranted by business needs, a log may be kept, recording the time of entry, time of exit, and purpose of physical access by visitors and/or authorized personnel.
- Visitors must wear an identification badge.
- Visitors should be escorted by authorized personnel at all times.

Structural Considerations

- The server room must be located in an area that can bear the weight of all systems, including foreseeable planned growth.
- When feasible, door frame size should be sufficient to allow for easy introduction and removal of equipment. For new construction, doors should be 42 inches wide and 9 feet tall. If hinges are exterior to the room, doors should use locking hinge pins.
- The ceiling of the room should be at least 9 feet high.
- The server room should not have exterior windows.
- The arrangement of equipment should provide for adequate clearance around computing racks; 4 feet at the front and 3 feet at the rear is recommended.
- For new construction, an anti-static floor surface is recommended. Raised floors with a minimum clearance of 24 inches are recommended for new construction of large server rooms.

Power

- The server room should have sufficient dedicated circuits for all equipment, plus one or more additional circuits, as needed for flexibility in the event a circuit fails.
- All systems must be properly grounded.
- Critical systems should be connected to uninterruptable power supplies (UPS) and/or generator power, depending on the business requirements for server uptime.
- Uninterruptable power supplies (UPS) and/or generator power should be tested at least annually and maintained according to manufacturer specifications.
- Based on UPS monitoring thresholds, automatic shutdown features should be configured when feasible to gracefully shutdown and protect systems prior to power loss.
- Large rooms should have a clearly-labeled emergency power-off switch.
- Procedures should be posted in the room explaining how to respond in the event of a power failure.
- Server rooms should have emergency lighting to provide for life safety in the event of a power outage.

Temperature Control

- The server room must have sufficient temperature control to maintain temperatures within the operational limits defined for the hardware located in the room.
- The server room should have dedicated, redundant air conditioning sufficient to maintain temperatures between 65 and 70 degrees Fahrenheit. Fully enclosed racks with built-in cooling may also be used.
- Environmental monitoring should be configured to alert administrators in the event of a cooling failure (i.e., a NetBotz monitoring system that sends text messages; a thermostat with only a local alarm is not sufficient).
- For large rooms, cooling systems and equipment should be installed in a hot aisle / cold aisle configuration to maximize efficiency.
- Procedures should be posted in the room explaining how to respond in the event of a cooling failure.

Fire / Flood

- The server room must have some form of fire detection and suppression, adequately maintained and routinely tested.
- Server rooms must be reasonably free of fire hazards such as boxes, papers, etc.
- Each server room may have an easily visible and accessible clean-agent fire extinguisher. A standard “ABC” fire extinguisher is not recommended for use around electronic equipment.
- If the server room is located near potential leak hazards (AC condensers, overhead water lines, sprinklers, kitchens, break rooms, restrooms, etc.) sufficient steps should be taken to protect systems, such as racks with solid tops, systems elevated off the floor, etc. Moisture sensors should be used in areas where leaks are most likely or would be most problematic.

Other

- Cabling must be maintained in an orderly fashion to reduce the possibility of an accidental outage.
- The manager of the server room must maintain an accurate inventory of all systems in the server room.
- Server rooms should not have conspicuous signage that could attract unnecessary attention or attack.

Exemptions

In the event that compliance with this server room standard cannot be met, please contact infosecurity@utdallas.edu to submit an exemption request which will be approved or denied by the CISO. Denied exemption requests may be appealed to the UTD President for final decision.