8.2. Servers And Network Devices

Objective

8.2.1. Secured server and communications rooms provide appropriate physical security for servers and network devices.

Context

Scope

8.2.2. This section covers the physical security of servers and network devices. Information relating to network infrastructure and IT equipment can be found in other sections of this chapter.

Secured server and communications rooms

8.2.3. In order to reduce physical security requirements for information systems infrastructure, other network devices and servers, agencies may choose to certify and accredit the physical security of the site or IT equipment room to the standard specified in the PSR. This has the effect of providing an additional layer of physical security. See PSR - Physical Security

8.2.4. Agencies choosing NOT to certify and accredit the physical security of the site or IT equipment room, must continue to meet the full storage requirements specified in the PSR. See PSR - Physical Security, PSR - Information Security.

Rationale & Controls

Securing servers and network devices

8.2.5.R.01. **Rationale**

Security containers for IT infrastructure, network devices or servers situated in an unsecure area must be compliant with the requirements of the PSR. Installing IT infrastructure, network devices or servers in a secure facility can lower the storage requirements, provided multiple layers of physical security have been implemented, certified and accredited.

8.2.5.R.02. **Rationale**

The establishment of a secure communications room to house IT infrastructure, network devices, and other related equipment will provide a further physical security layer.

8.2.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1349]

Agencies MUST ensure that servers and network devices are secured within cabinets as outlined in PSR Policy Framework - Physical security and supporting documentation.

Securing server rooms, communications rooms and security containers

8.2.6.R.01. **Rationale**

If personnel decide to leave server rooms, communications rooms or security containers with keys in locks, unlocked or with security functions disabled it negates the purpose of providing security in the first place. Such activities will compromise the security efforts of the agencies and should not be permitted by the agency.

8.2.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1353]

Agencies MUST ensure that keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled.

8.2.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:1354]

Agencies MUST NOT leave server rooms, communications rooms or security containers in an unsecured state unless the server room is occupied by authorised personnel.

Administrative measures - Site security plans

8.2.7.R.01. **Rationale**

Site security plans (SitePlan), the physical security equivalent of the SSP and SOPs for systems, are used to document all aspects of physical security for systems. Formally documenting this information ensures that standards, controls and procedures can easily be reviewed by security personnel.

8.2.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1357]

Agencies MUST develop a Site Security Plan (SitePlan) for each server and communications room. Information to be covered includes, but is not limited to:

- a summary of the security risk review for the facility the server or communications room is located in;
- roles and responsibilities of facility and security personnel;
- the administration, operation and maintenance of the electronic access control system or security alarm system;
- key management, the enrolment and removal of system users and issuing of personal identification number codes and passwords;
- personnel security clearances, security awareness training and regular briefings;
- regular inspection of the generated audit trails and logs;
- end of day checks and lockup;
- reporting of information security incidents; and
- what activities to undertake in response to security alarms.

No-lone-zones

8.2.8.R.01. **Rationale**

Areas containing particularly sensitive materials or IT equipment can be provided with additional security through the use of a designated no-lone-zone. The aim of this designation is to enforce two-person integrity, where all actions are witnessed by at least one other person.

8.2.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1360]

Agencies operating no-lone-zones MUST suitably signpost the area and have all entry and exit points appropriately secured.