Sharing allow:
TLP - GREEN

Approved

Physical Security of Data Centres Standard

Document ID: **SEC-08**
For: Alliance Federation
Approval Date: 2024-04-03
Approved By: NSC

1. Introduction

This standard defines the physical security requirements for data centres which host Alliance Federation Systems and Services. Complying with the requirements stipulated in this document is essential to keep Alliance Federation Systems and Services safe from physical security threats.

2. Definitions

Refer to *SEC-00 Information Security Glossary* for definitions used in this Standard.

3. Applicability

This standard applies to the data centres hosting Alliance Federation Systems and Services.

4. Physical Security Requirements

4.1 Structure / Enclosure

4.1.1. Public access to the data centre perimeter should be restricted. Signage(s) should be placed to clearly delineate publicly accessible space from Authorized Personnel-Only areas. An outer security perimeter with access controls should be established to prevent direct public access.

4.1.2. The data centre must be located in a fully enclosed room. Walls must extend from floor to ceiling slab and be constructed from a solid, resistant material such as concrete or brick. If the walls are not (e.g., drywall), then they must be reinforced with wire mesh.

4.1.3. Doors must be closed and locked at all times when not in use and include a fail-safe mechanism that allows personnel to exit the data centre in the event of an access system failure.

4.1.4. Doors must close automatically, except loading bay doors.

4.1.5. Security grade door fastening hardware must be used and be constructed of metal, including the frame.

4.1.6. Any windows in the data centre perimeter walls or doors must be reinforced. Installation of high-grade security film (Profilon AXA1-15Mil or above) should be considered.

4.1.7. For new construction, plumbing (e.g., potable water and drainage) must not run across the ceiling of the data centre, or mitigations must be put in place (e.g., deflection, drains, etc.) this does not apply to cooling systems specifically designed for the data centre equipment.

4.1.8. It is considered a best practice to prevent electronic interference (e.g., through the use of shielding plates, enclosed and grounded metal cabinets, etc.).

4.2 Visibility and Access to Equipment

4.2.1. All racks and cabinets in the data centre should be locked to isolate the equipment inside (including restricting access to USB and other ports) unless the data centre is dedicated exclusively to Alliance Federation Systems and Services.

4.2.2. Blinds or coverings should be installed on windows where necessary to reduce sightlines from outside of the data centre to equipment, screens, and valuables.

4.3 Power and Network Cabling

4.3.1. All network cabling for transmission of data between data centre devices should be physically located inside the data centre perimeter. Network cabling carrying this data or supporting information services that must run physically outside of the data centre perimeter through an area accessible to the public, must be protected from interception or damage.

4.3.2. Critical systems should be connected through a Uninterruptible Power Supply (UPS) in order to remain running in the event of brief power outages. New construction should be designed to physically separate the main power including UPS and data equipment to prevent risk of damage to data equipment in the event of catastrophic failure of power system batteries.

4.3.3. It is considered a best practice to install redundant power to the data centre and consider installing additional power backup systems (e.g., generators) for longer outages based on system criticality.

4.4 Access Management

4.4.1. The following access mechanisms are preferred and should be installed: electronic proximity access cards / fobs, keypad type entry locks, and biometric locks that uniquely identify an individual.

4.4.2. Access to the data centre must be logged electronically or in a logbook in cases where the access mechanism does not uniquely identify an individual.

4.4.3. Named individuals must be assigned with the authority to grant access to the data centre. A formal management process must be established to manage physical access to the data centre, including the revocation of access using fobs, cards, and keypad access.

4.4.4. Contractors who will be accessing the data centre must be pre-authorized in accordance with section 4.4.3.

4.4.5. Any Individuals, including contractors, who have not been authorized to access the data centre, must be escorted at all times by an authorized individual.

4.4.6. Taking photo(s) and recording(s) in a data centre must be pre-authorized.

4.5 Environmental Controls

4.5.1. Sufficient Heating, Ventilation and Air Conditioning (HVAC) systems must be in place to effectively maintain all systems within the manufacturers' required temperature and humidity operating ranges.

4.5.2. Temperature and humidity must be monitored to detect when thresholds are exceeded, subsequently triggering an alarm.

4.6 Fire Suppression

4.6.1. Fire detection and suppression devices, such as fire detectors and extinguishers, must be in place.

4.6.2. Automated fire-suppression systems must take into account the safety of data centre personnel.

4.7 Monitoring and Response

4.7.1. Security alarms must be implemented for the data centre perimeter access points (doors, windows) and should include motion detection systems where possible to identify and alert in the case of unauthorized access.

4.7.2. Security and environmental alarms must be monitored 24/7.

4.7.3. Physical security response time (during and outside business hours) must be less than 60 minutes for physical unauthorized access and/or environmental hazard.

4.7.4. Video monitoring must be installed within the data centre to provide coverage of assets and spaces, and care must be taken to avoid recording sensitive/personal information. Video recordings must be retained for a minimum of 30 days and access to recordings restricted according to a documented procedure.

4.8 Equipment and Inventory

4.8.1. A log of equipment entering and leaving the data centre should be maintained.

4.8.2. An inventory of spare and in-service equipment should be maintained.

5. Related Information

SEC-00 Information Security Glossary