Physical Security Design Standards

v1.0

Jadarah For Dept Collections Co.

This document is a property of **Jadarah For Dept Collections Co.** and contains sensitive and confidential information which should not be disclosed, transmitted, duplicated, and used in whole or part other than for its intended purpose and recipients

Document Control Information

Document Version Control Information				
Version	Date	Author	Reviewer	Approver
1.0	**03 Oct 2024**	Abdulrahman AlJamani	Ahmed Al-Kelani	Misfer Al-Ajmi

Document Change History Information			
Author	Date	Version	Change Description

Contents

Document Control Information **2**

1 Introduction **4**

2 Physical Security Design Standards **5**

2.1 Principles of Secure Areas 5

2.2 Physical Security Perimeter 5
2.2.1 Perimeter Definition 5
2.2.2 Reception Area 5
2.2.3 Physical Barriers 5
2.2.4 Intruder Detection Systems 5

2.3 Physical Entry Controls 6
2.3.1 Visitors 6
2.3.2 Access Controls 6
2.3.3 Audit Trail 6
2.3.4 Visible Identification 6

2.4 Securing Offices, Rooms, Facilities 6
2.4.1 Additional Security 6
2.4.2 Recording Equipment 6
2.4.3 Vacant Areas 6
2.4.4 Directories 6

2.5 Protecting Against External and Environmental Threats 7
2.5.1 Public Access, Delivery Areas 7
2.5.2 Separation of Incoming and Outgoing Goods 7

2.6 Equipment Siting and Protection 7
2.6.1 Siting 7
2.6.2 Protection 7
2.6.3 Environmental 7
2.6.4 Lightening Protection 7

2.7 Supporting Utilities 8
2.7.1 Capacity 8
2.7.2 Inspection and testing 8
2.7.3 Alarms 8
2.7.4 Redundancy 8

2.8 Cabling security 8
2.8.1 Cable routing 8
2.8.2 Shielding 8
2.8.3 Access control 8

1 Introduction

Secure areas are necessary in order to protect the physical and information assets of the organization from a loss of confidentiality, integrity or availability. This document sets out standards to be used in creating a secure area in Jadarah For Dept Collections Co. to ensure that it remains secure whilst not compromising the business carried out within it.

2 Physical Security Design Standards

2.1 Principles of Secure Areas

The design of secure areas is a complex business that requires that the designer undertake a full and comprehensive assessment of the risks associated with each specific facility, second-guessing the most likely methods of unauthorised access and addressing them one by one.

The level of security applied to any given site should be appropriate to the classification of the information processed within it.

As with all security design the measures put in place must remain appropriate so that the users of the facility are not unreasonably hampered by them and are able to carry out their tasks.

2.2 Physical Security Perimeter

2.2.1 Perimeter Definition

The first consideration is to define the location and perimeter of the secure area. In general, secure areas should be sited to avoid access or visibility to the public or unauthorised people and measures taken to avoid drawing attention to them. If possible, they should be physically separate from public areas and not shared with any third parties.

All entry points around the physical security perimeter must be risk assessed including lift shafts, ceilings and walls to ensure they offer a good degree of protection with no weak points.

External doors should be secure with a level of additional protection appropriate to the required security level (e.g., bars, chains, alarms and multiple locks) with due consideration of applicable fire safety regulations.

External windows around the perimeter should be locked and those on the ground floor secured with bars where possible (subject to relevant regulations).

2.2.2 Reception Area

A defined reception area should be created through which all access is controlled. This should be adequately manned when the site is open and only authorised personnel admitted.

2.2.3 Physical Barriers

Where appropriate, physical barriers should be installed to prevent access without the correct level of authorisation. These should prevent tailgating i.e., an unauthorised person following an authorised person through the barrier.

2.2.4 Intruder Detection Systems

Where justified by the level of security required, intruder alarms and Closed-Circuit Television (CCTV) should be installed to protect entry points and warn of security breaches.

2.3 Physical Entry Controls

2.3.1 Visitors

A procedure must be put in place to sign all visitors in at reception and record details of their identity and date/time of entry and departure.

Third-party visitor access to the secure area will usually need to be requested in advance and such visitors must always be supervised by an authorised member of staff.

2.3.2 Access Controls

Appropriate access controls should be used at all points where the level of security changes. Server room or other similar facilities should have their own access control. Two factor authentication such as a swipe or proximity card and a Personal Identification Number (PIN) must be used where information classified as confidential is stored or processed. A regular review of access rights should be undertaken to ensure that they remain current.

2.3.3 Audit Trail

An audit trail of access to secure areas must be maintained either via manual completion of a signing in book or via electronic means.

2.3.4 Visible Identification

All users of secure areas (including visitors) will be required to wear a visible and current ID badge.

2.4 Securing Offices, Rooms, Facilities

2.4.1 Additional Security

Individual rooms within the secure area may also be protected by additional security. Such rooms will typically include server rooms, communications rooms, Human Resources, directors' offices and plant rooms (such as power and air conditioning).

Depending on the type of facility, users of such individual rooms may need to have specific access and be required to sign in and out.

2.4.2 Recording Equipment

Cameras or other video or audio recording equipment will not be allowed in secure areas without explicit prior permission.

2.4.3 Vacant Areas

Vacant areas within the secure perimeter will be locked and regularly checked for signs of unauthorised entry or use. Where possible they should be alarmed.

2.4.4 Directories

Phone directories or other information regarding secure areas should not be made generally available.

2.5 Protecting Against External and Environmental Threats

In addition to being covered by the organization's business continuity plans, secure areas may require further consideration to ensure that any external events such as fire, flood or earthquake will not expose the confidentiality, integrity or availability of the contents.

This may affect the siting of secure locations and the procedures used for reacting to events such as fires, subject to health and safety considerations.

2.5.1 Public Access, Delivery Areas

A separate delivery or holding area should be used so that deliveries may be inspected prior to them being accepted into the secure area. Such inspection should happen as soon as possible after the delivery and be comprehensive enough to assess the likelihood of any threats being present.

Delivery staff should not have access to the secure area.

2.5.2 Separation of Incoming and Outgoing Goods

Areas should be designed such that deliveries and outgoing items are not stored or processed in the same place.

2.6 Equipment Siting and Protection

2.6.1 Siting

The secure area should be designed such that equipment such as server farms cannot be viewed from public areas. Screens that may display sensitive information must be sited away from positions where unauthorised people might view them.

2.6.2 Protection

Where appropriate, additional protection against threats such as dust, vibration, electrical interference and chemicals should be designed into the secure area. This should be based on a comprehensive risk assessment.

2.6.3 Environmental

Appropriate environmental controls such as air conditioning must be provided and its health capable of being monitored on an ongoing basis.

2.6.4 Lightening Protection

Appropriate protection from lightning damage to equipment must be designed into the secure area.

2.7 Supporting Utilities

Care must be taken to ensure the correct design of supporting utilities such as:

- Gas and electricity
- Water
- Ventilation
- Network communications

2.7.1 Capacity

A capacity assessment must be undertaken by a qualified individual when considering the requirements of the secure area and its contents for supporting utilities. This should allow for estimated usage plus adequate room for growth.

2.7.2 Inspection and testing

Plans should be put in place for initial and repeated inspection and testing of supporting utilities to ensure they continue to operate within manufacturer's recommended parameters.

2.7.3 Alarms

Alarms will be installed to detect circumstances where supporting utilities are operating or are about to operate outside of normal levels.

2.7.4 Redundancy

Appropriate redundancy of supporting utilities should be designed in e.g., diverse routing for network communications and excess capacity for air conditioning.

2.8 Cabling security

2.8.1 Cable routing

Where possible, cabling should be routed underground and away from any potential sources of interference.

2.8.2 Shielding

Additional shielding against electromagnetic interference should be implemented where required. Power cables should not be routed with data cables.

2.8.3 Access control

Access to patch panels and cabling termination points should be controlled via the use of locked access panels and cabinets. Cabling should not be routed via public areas.