Data Center Security Project

Authored by:

Elliot Hardy

October 2025.

Contents

1. Introduction

1.1 Project Overview

The project aims to provide a full, comprehensive, and professional first attempt at security architecture design and business continuity. The project includes a description of the Physical, Administrative, and Technical security measures and controls used to protect a fictional data center including blueprints and diagrams. This write up of the project includes all policies used to build the design.

2. Physical Security Controls

2.1 Access Control Measures

The building contains the following Access Control Measures: Keycard scanner to gain entry to the main reception of the building, a security/reception desk, a facial recognition barrier to move from the reception to the main office area, all rooms have a fingerprint scanner to gain entry, and the server/data room has a fingerprint scanner man trap to gain access to the facility.

2.2 Surveillance Measures

The building has CCTV covering all entrances and exits to the building and each specific room, each corridor has 2 cameras covering each end, the meeting room and server/data room have CCTV inside the room not only on the entrance, and the main office space has two cameras covering the whole area.

2.3 Environmental and Facility Controls

The building has multiple fire doors which can only be opened from inside the building, a full HVAC system, and the server/data room runs on its own personal CO2 fire suppression system (CO2 is used do to its non conductivity, and the fact it leaves no residue and is non corrosive making it perfect for sensitive technology protection.)

2.4 Room-by-Room Physical Security

2.4.1 Server / Data Room

The server/data room requires you to first gain access to the building through the reception mantrap and then also pass through the fingerprint scanner man trap which is the only entrance and exit to and from the room. The server/data room has CCTV monitoring the entrance and exit, it also has multiple cameras inside the room for monitoring and security purposes.

2.4.2 Network/Electrical/Storage Room

The network/electrical/storage room have CCTV monitoring there entrances and exits which each require you to pass a fingerprint scanner to enter.

2.4.3 Offices and Work Areas

The offices and work areas are monitored by CCTV covering the whole area. The offices and meeting room require fingerprint scanner verification to enter however the main work area/kitchenette do not as no sensitive material or devices are to be left here.

2.4.4 Reception / Lounge / Visitor Area

The reception/lounge/visitor area requires either a keycard to access or a visitor pass gained by ringing the keypad on the door and obtaining a pass from the security desk.

3. Administrative Security Controls

3.1 Security Policies

3.1.1 Access Control Policy

Access to the center is limited to authorized personnel with a legitimate need. All employees, contractors, and visitors must be approved by management, issued appropriate credentials, and adhere to assigned access levels. Physical access to secure areas, server rooms, and network infrastructure requires keycards, biometric verification, or other approved authentication methods. All access must be monitored, logged, and revoked immediately upon termination or role change to ensure the security, integrity, and availability of critical assets.

3.1.2 Visitor Management Policy

All visitors to the center must be pre-approved, registered, and escorted by authorized personnel at all times. Visitors are required to present valid identification upon arrival, sign in at the reception/security desk, and wear a temporary visitor badge indicating their access level. Access is limited to designated areas, and entry into restricted zones requires explicit authorization from center management. Employees hosting visitors are responsible for ensuring compliance with security protocols, and all visitors must sign out and return their badges upon departure.

3.1.3 Incident Reporting Policy

To report an incident you must find the on duty manager as soon as the incident is discovered, the manager will then take appropriate action to mitigate the incident through the right channels and protocols. If for any reason the on duty manager cannot be found or is unavailable the incident must be reported to the most senior member of staff who will then take the lead and attempt to contact the senior team or the cybersecurity team. Prompt and accurate

reporting is essential to mitigate risks and protect personnel and assets.

3.1.4 Device Usage Policy

All activity on work devices must be strictly limited to work related activities. Personal devices not issued by the company are to be left in the lockers upon entry to the building. You are not to sign in to personal accounts on the work devices. work devices are not to be taken outside of the facility. Anyone found to be in breach of this policy will have disciplinary actions taken against them not limited to termination.

3.2 Security Procedures

3.2.1 Onboarding / Offboarding Procedure

[Write your paragraph(s) here.]

3.2.2 Access Issuance Workflow

[Write your paragraph(s) here.]

3.2.3 Maintenance and Contractor Access

[Write your paragraph(s) here.]

3.3 Compliance and Documentation

[Describe GDPR, ISO standards, access and log retention, etc.]

4. Technical Security Controls

4.1 Network Security

[Write your paragraph(s) here.]

4.2 Data Protection Protocols

[Write your paragraph(s) here.]

4.3 System Hardening

[Write your paragraph(s) here.]

4.4 Monitoring and Logging

[Write your paragraph(s) here.]

5. Threat Analysis

5.1 Identified Threats

[List and explain threats such as tailgating, theft, insider misuse, etc.]

5.2 Risk Assessment

[Insert table or text.]

5.3 Risk Mitigation Measures

[Write your paragraph(s) here.]

6. Incident Response Plan

6.1 Incident Types

[Fire, power outage, unauthorized access, etc.]

6.2 Incident Response Steps

[Detection, containment, eradication, recovery.]

6.3 Reporting and Communication Procedures

[Write your paragraph(s) here.]

7. Business Continuity and Disaster Recovery

7.1 Backup and Recovery

[Write your paragraph(s) here.]

7.2 Continuity Planning

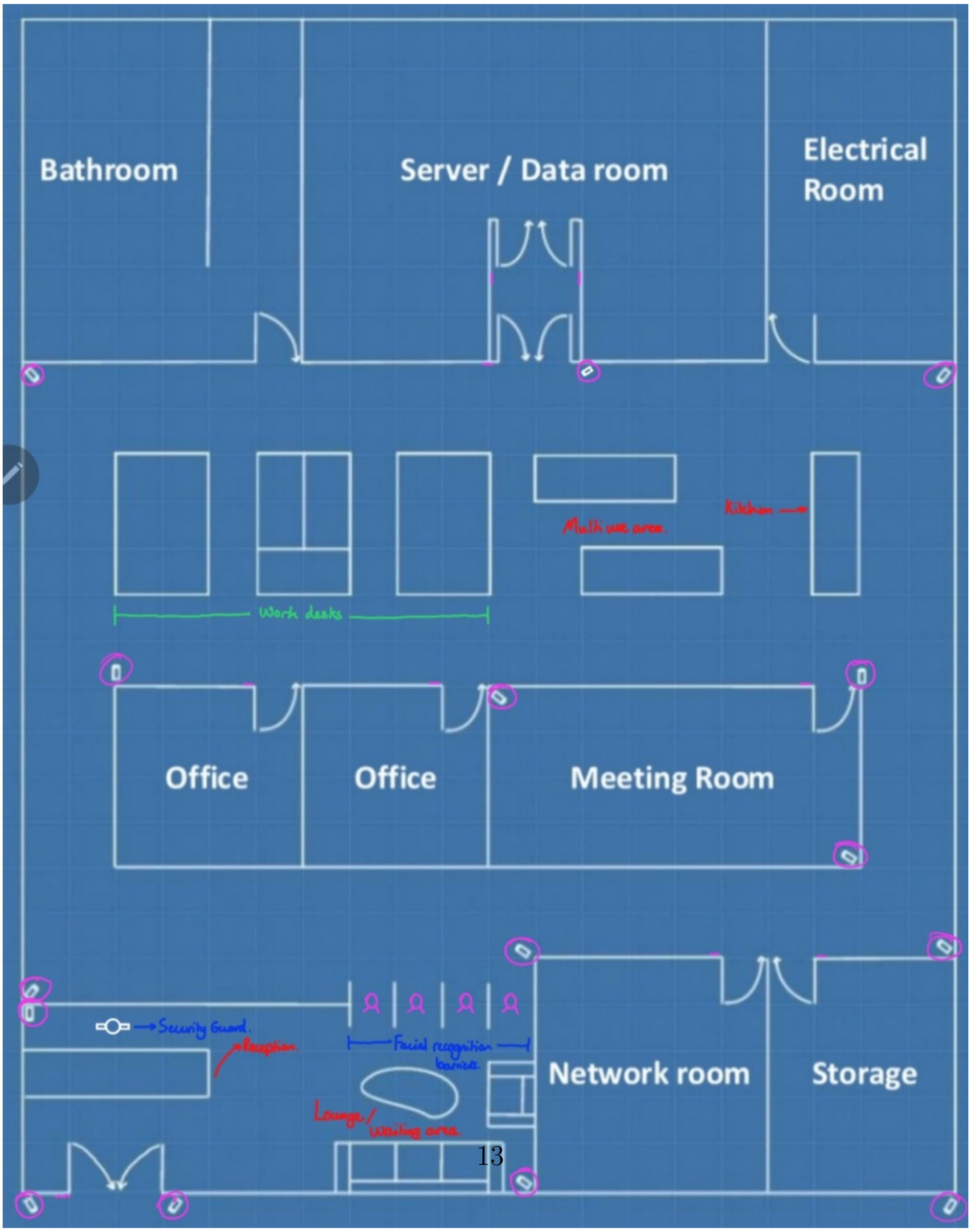
[Write your paragraph(s) here.]

7.3 Failover and Redundancy

[Write your paragraph(s) here.]

8. Blueprint and Visual Documentation

8.1 Blueprint Overview



8.2 Access Flow Diagram

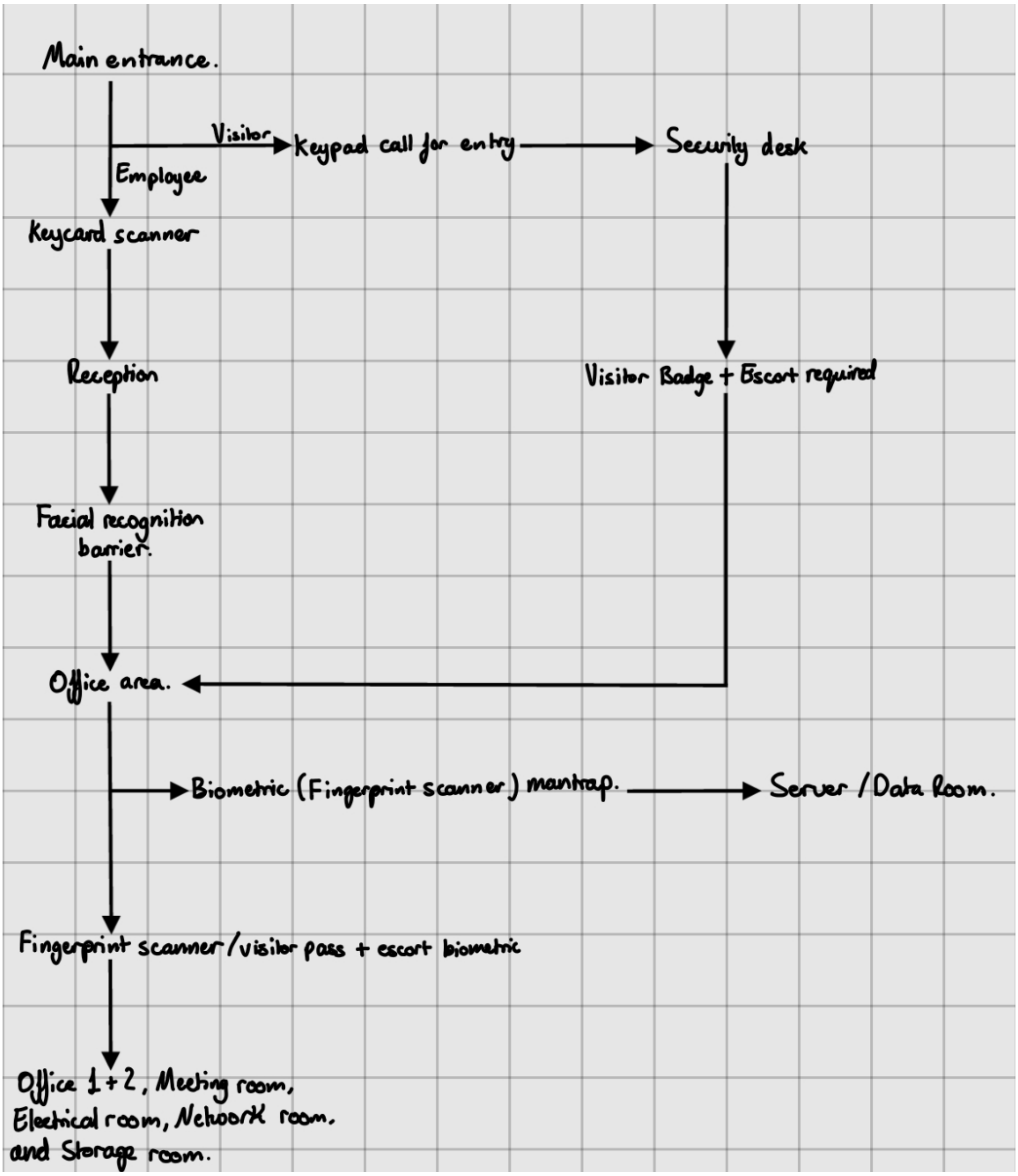

Main entrance.
Visitor
Keypad call for entry
Security desk
Employee
Keycard scanner
Reception
Visitor Badge + Escort required
Facial recognition barrier.
Office area.
Biometric (Fingerprint scanner) mantrap.
Server / Data Room.
Fingerprint scanner / visitor pass + escort biometric
Office 1+2, Meeting room,
Electrical room, Network room.
and Storage room.

Figure 8.2: Data Centre Blueprint