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 key-cards, 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

Access must be granted based on role changes, different projects, the process must follow the access issuance workflow. Access must be revoked immediately when no longer required due to role changes, project completion, contract termination, or policy violations, including retrieval of physical credentials and disabling of system accounts, ensuring continuous protection of personnel, data, and infrastructure.

3.2.2 Access Issuance Workflow

Access requests must be submitted by the individual or their manager, detailing the purpose, level, and duration of access. Requests are reviewed and approved by the relevant department manager and center security, who verify the individual's identity and eligibility. Once approved, appropriate credentials—such as keycards, badges, biometric authentication, system accounts, or multi-factor authentication—are issued. Individuals are informed of their responsibilities and trained on security protocols. All access is logged, monitored, and audited regularly.

3.2.3 Maintenance and Contractor Access

All contractor access must be strictly controlled and a contractor must only be used when the in house team are not able to complete the repairs or the upgrades. All contractors when on site must follow the visitor management protocol which in turn must follow the access issuance workflow.

3.3 Compliance and Documentation

All personnel, contractors, and visitors at the center must adhere to applicable laws, regulations, industry standards, and internal security policies. All security activities, access requests, incidents, and system changes must be documented, securely stored, and made available for review or audit as required. Personnel are responsible for maintaining records of all documentation that demonstrates compliance. Regular audits and reviews will be conducted to ensure policies are followed, gaps are identified, and corrective actions are implemented promptly.

4. Technical Security Controls

4.1 Network Security

Network security at the center is maintained through a combination of firewalls, intrusion detection and prevention systems, network segmentation, and secure access controls. All network traffic is monitored for unauthorized activity, and all remote connections are secured using encrypted protocols. Regular vulnerability assessments and penetration tests are conducted to ensure the integrity of network defenses, and all devices connected to the network must comply with approved security standards and configurations.

4.2 Data Protection Protocols

All sensitive data stored, processed, or transmitted within the center is protected using encryption, access controls, and data classification policies. Backup and recovery procedures are implemented to ensure availability and integrity, and data retention policies are enforced to comply with legal and regulatory requirements. Personnel are trained on proper handling of confidential information, and any data transfers to external systems require explicit authorization and secure transmission methods.

4.3 Monitoring and Logging

All critical systems, applications, and network activity are continuously monitored and logged to detect anomalies, security incidents, or policy violations. Logs are securely stored, retained according to regulatory requirements, and regularly reviewed by authorized personnel. Monitoring tools include real–time alerts and automated reporting, ensuring timely detection and response to potential threats. Access to logs is restricted to authorized personnel to maintain confidentiality and integrity.

5. Threat Analysis

5.1 Identified Threats

The center is subject to a variety of threats, including unauthorized physical access, cyber attacks, insider threats, equipment failure, and environmental hazards such as fire or power loss. Threats are identified through regular risk assessments, security audits, and analysis of historical incident data. Awareness of these threats informs the implementation of preventative and corrective measures to protect personnel, systems, and data assets.

5.2 Risk Assessment

Risk assessments are conducted periodically to evaluate the likelihood and potential impact of identified threats. Each risk is categorized based on severity, probability, and potential operational or financial consequences. Assessment results guide prioritization of mitigation efforts and inform management decisions regarding security investments, resource allocation, and procedural updates. All assessments are documented for review and compliance purposes.

5.3 Risk Mitigation Measures

Mitigation measures are implemented to reduce the likelihood and impact of identified risks, including physical security controls, network protections, access restrictions, staff training, and disaster recovery planning. Redundant systems, regular backups, and environmental controls ensure continuity of operations like the backup generators and fire suppression system, while policies and procedures establish clear roles and responsibilities for incident response. Mitigation measures are reviewed and updated regularly to address evolving threats and maintain an effective security posture.

6. Incident Response Plan

6.1 Incident Types

Natural disasters, Fire, Burst pipe/Leaks, and Cyber breaches/attacks.

6.2 Reporting and Response Procedures

In the case of a physical emergency that poses threat to human life first evacuate and contact emergency services and following that the most senior member of staff should follow the incident reporting policy to notify the senior management team. In the case of a fire once detected pull the fire alarm and evacuate through the closest fire door and the on duty manager and/or the designated fire marshal will lead the evacuation and attempt to contain the fire if possible. In the case of natural disaster follow the guidance from local emergency services/governments. In the case of a cyber incident once discovered follow the incident reporting policy.

7. Business Continuity and Disaster Recovery

7.1 Backup and Recovery

All critical systems and data at the center are subject to regular backup procedures to ensure integrity, availability, and recoverability in the event of a disruption or data loss. Backups are performed on a defined schedule, stored securely both on-site and off-site, and tested periodically to verify successful restoration. Recovery procedures are documented, reviewed, and updated to reflect changes in systems, data, or operational requirements.

7.2 Continuity Planning

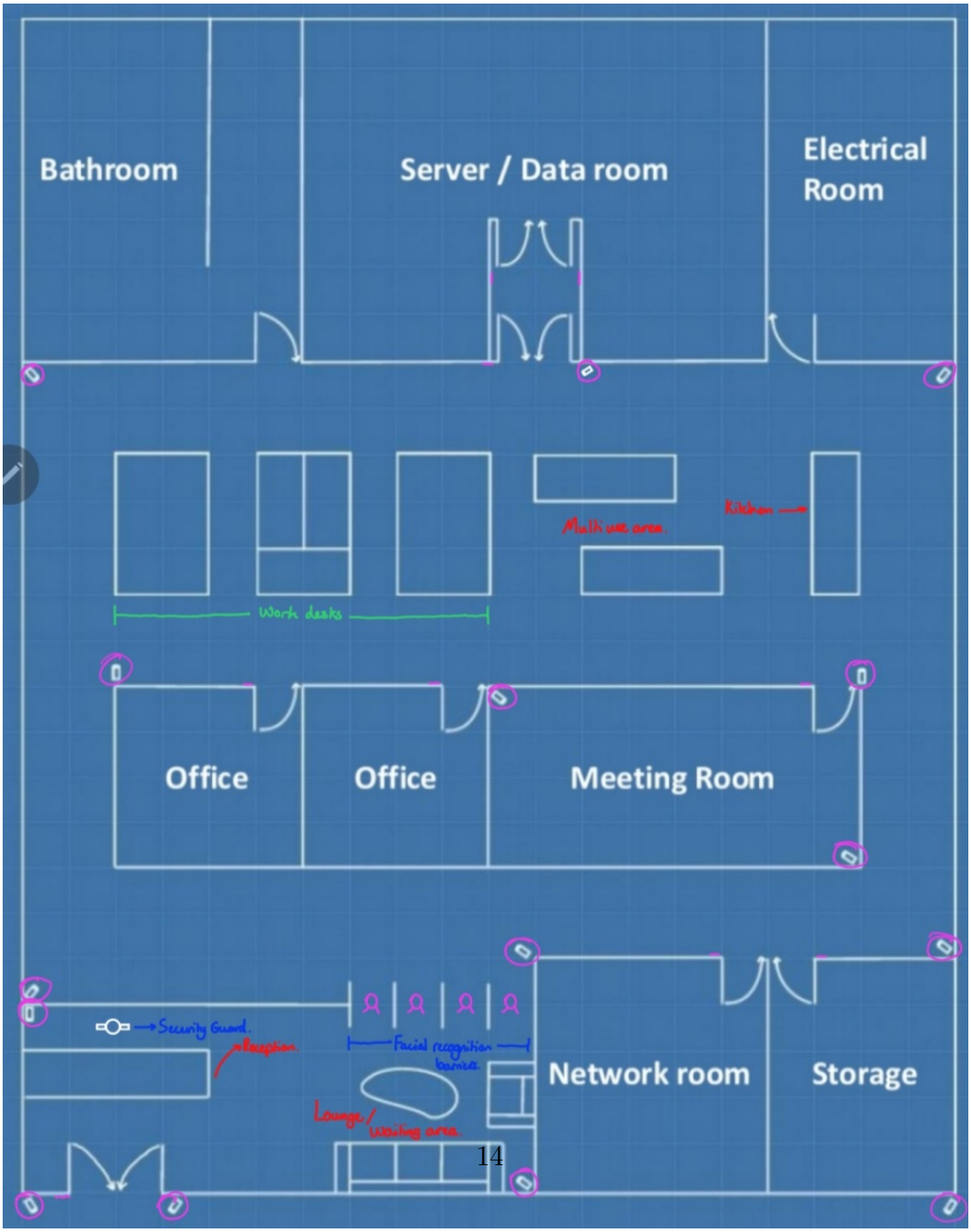
A comprehensive business continuity plan is maintained to ensure that essential operations can continue during and after disruptive events. The plan outlines roles, responsibilities, communication protocols, and procedures for maintaining critical functions. Staff are trained in continuity procedures, and periodic drills and simulations are conducted to validate effectiveness and identify areas for improvement. The plan is reviewed regularly to address evolving threats and operational changes.

7.3 Failover and Redundancy

Redundant systems, infrastructure, and network paths are implemented to minimize downtime and maintain uninterrupted service. Critical components such as power supplies, cooling systems, network connectivity, and storage are configured with failover capabilities to automatically switch to backup systems in the event of failure. Redundancy and failover mechanisms are tested regularly to ensure operational reliability and resilience against both planned and unplanned disruptions.

8. Blueprint and Visual Documentation

8.1 Blueprint Overview



8.2 Access Flow Diagram

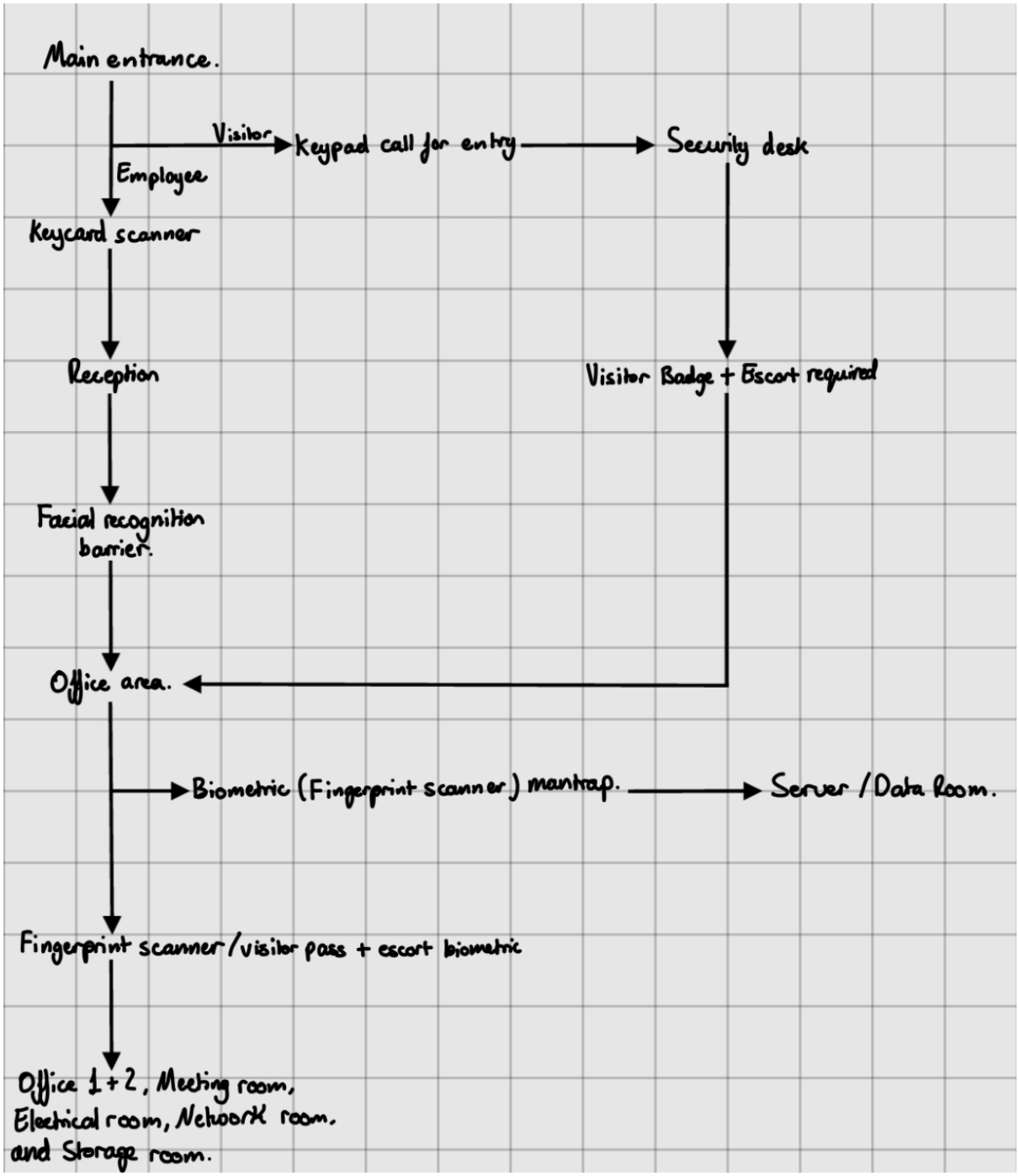


Figure 8.2: Access Flow Diagram