# Assets Table

## Physical Asset

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| LOCATION | Device | Quantity | Classification | Price |
| FLOOR 8 | PC | 50 | Sensitive | $1,500 |
| Printer | 5 | Internal | $100 |
| Scanner | 5 | Internal | $100 |
| Camera | 4 | Sensitive | $100 |
| Switch | 3 | Sensitive | $100 |
| Access point | 3 | Sensitive | $30 |
| Keycard reader | 3 | Internal | $30 |
| UPS 10 kVA | 2 | Sensitive | $4300 |
| FLOOR 7 | PC | 100 | Sensitive | $1,500 |
| Printer | 10 | Internal | $100 |
| Scanner | 10 | Internal | $100 |
| Camera | 4 | Sensitive | $100 |
| Switch | 3 | Sensitive | $100 |
| Access point | 5 | Sensitive | $30 |
| Keycard reader | 3 | Internal | $30 |
| FLOOR 6 | PC | 2 | Highly Sensitive | $1,500 |
| Keycard reader | 3 | Internal | $30 |
| Firewall | 2 | Highly Sensitive | $2,100 |
| Access point | 1 | Sensitive | $30 |
| Camera | 6 | Sensitive | $100 |
| Switch | 4 | Sensitive | $100 |
| Router | 2 | Highly Sensitive | $300 |
| Multilayer switch | 4 | Highly Sensitive | $200 |
| DNS server | 1 | Highly Sensitive | $2300 |
| DHCP server | 1 | Highly Sensitive | $2400 |
| Web server | 1 | Highly Sensitive | $3000 |
| Mail server | 1 | Highly Sensitive | $2200 |
| Log server | 1 | Highly Sensitive | $2500 |
| Database server | 10 | Highly Sensitive | $3000 |
| UPS 30 kVA | 2 | Sensitive | $7500 |
| Company | Security personnels | 10 | Sensitive | N/A |

## Logical Asset

|  |  |
| --- | --- |
| Assets | Classification |
| Website | Public |
| DNS | Public/Internal |
| Mail | Public |
| DHCP | Internal |
| Log server | Highly Sensitive |
| Database | Internal/ Sensitive / Highly Sensitive |
| Camera footage | Sensitive / Highly Sensitive |
| RFID reader data | Sensitive |
| IT security personnels | Highly Sensitive |

# 1. Physical Layout

## 1. Floor 6

### 1.1 Floor layout

The floor layout includes 4 rooms: data center for internal and public servers, security office for guard and camera control, networking devices room, and storage. Refer to the following figure for physical assets arrangement.

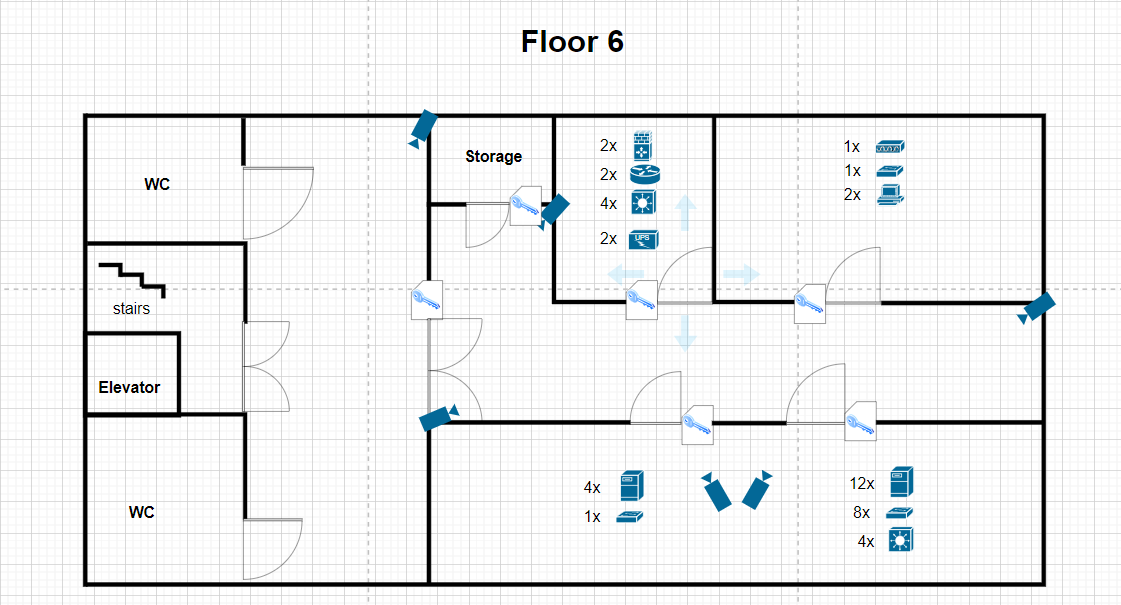


Figure 1.1.1.1 Floor 6 layout

Access to this floor is restricted and only accessible by guard and some IT personnels, each room also has a second layer of authentication to ensure only authorized personnel can access. Cameras are deployed to monitor and manage access to the area. The floor has 2 uninterruptible power supplies (UPS) installed, preventing any power disruption. The area is highly secure and strictly monitored.

### 1.2 Areas classification

The floor contains sensitive assets which are extremely important to DigiTech operations and security, assets within the floor are considered highly sensitive.

* **Highly Sensitive**:
  + **Networking devices room**: handles communication between floors and the company to the internet, failures can disrupt operations and cause great damage.
  + **Servers room:** the room contains both internal and public servers, failures can disrupt operations and cause great damage.
* **Sensitive**:
  + **Workstations**: workstations contain camera footage.
  + **Company areas**: can only access by authorized personnels
* **Public**:
  + **Outside of company areas**: elevator, restrooms, stairs, outside hall

### 1.3 CIA triad evaluation

With the classified asset in mind, physical and logical security requirements will be evaluated based on the CIA triad.

* **Confidentiality:**
  + **Physical:**

Use RFID readers to ensure access control, deploy surveillance cameras and guards to monitor and secure the area.

* + **Logical:**

Enforce strict access control, encrypt all data at rest and in-transit, and implement authentication to access critical areas.

* **Integrity:**
  + **Physical:**

Use tamper-evident mechanism on all hardware, conduct routine physical audits, and limit access to only those authorized.

* + **Logical:**

Implement strong access controls, conduct regular integrity checks, maintain detailed logs for all activities.

* **Availability:**
  + **Physical:**

Install UPS, backup generators, backup servers, and ensure an efficient heating venting air conditioning system is in place.

* + **Logical:**

Verify system redundancy for all critical assets, frequently backup important assets, and have a comprehensive disaster recovery plan.

## 2. Floor 7

### 2.1 Floor layout

The Applications Development lab layout consists of 8 rooms, including 5 department rooms, a networking devices room, a meeting room and a lounge. Refer to the following figure for physical assets arrangement.

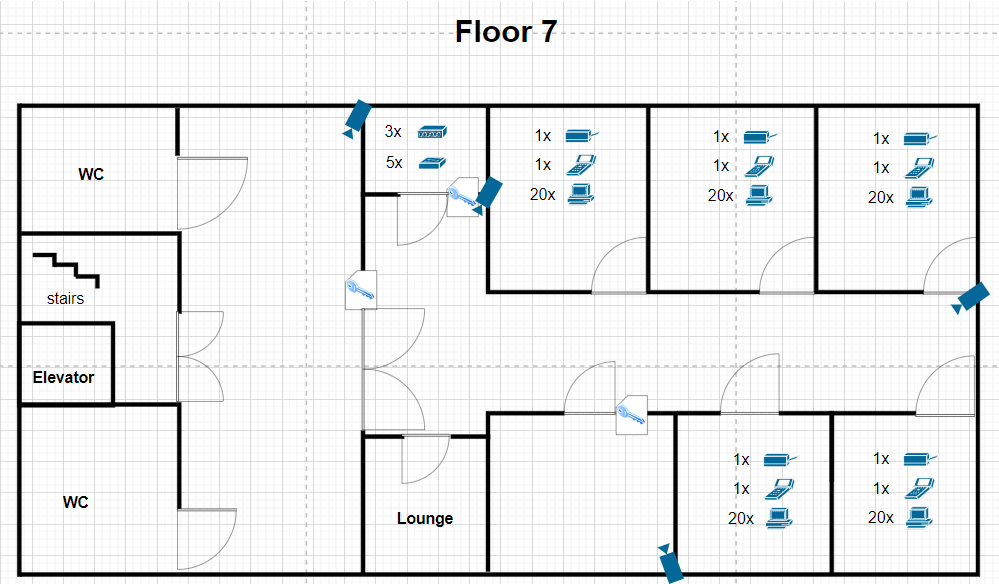


Figure 1.2.1.1 Floor 7 layout

As shown in the figure, employees are required to use their keycard to access the company development area. Other rooms such as the meeting room and networking devices room require a keycard with equivalent privilege to access. Cameras are placed around the facility for surveillance and managing access within the floor. With this layout, the area should be physically secured.

### 2.2 Areas classification

The floor primarily handles normal business operations but still contains sensitive assets, addressing and classifying sensitive areas is crucial:

* **Sensitive**:
  + **Workstations**: data in workstations can contain important business information and development progress.
  + **Networking devices room**: the room connects the floor to company network; unauthorized access can disrupt the floor ongoing operations.
  + **Meeting room**: conversations and topics discussed in the meeting room might be sensitive and highly sensitive.
* **Internal**:
  + **Company areas**: can only access by someone with company keycard or invited guests
* **Public**:
  + **Lounge**: despite inside the company area, the lounge can be used by both employees and guests
  + **Outside of company areas**: elevator, restrooms, stairs, outside hall

### 2.3 CIA triad evaluation

With the classified asset in mind, physical and logical security requirements will be evaluated based on the CIA triad.

* **Confidentiality:**
  + **Physical:**

Use RFID readers to ensure access control, surveillance cameras and guards to monitor entry and sensitive areas and manage visitor access strictly.

* + **Logical:**

Enforce strict access control, encrypt all development and sensitive data, and implement authentication to access development environments.

* **Integrity:**
  + **Physical:**

Use tamper-evident mechanism on hardware to detect unauthorized access, conduct regular audits, and limit access to only those authorized.

* + **Logical:**

Implement version control system, maintain development logs for all development activities, and have periodic code reviews.

* **Availability:**
  + **Physical:**

Ensure having reliable power supply and backup storage.

* + **Logical:**

Regularly backup code repositories and have a disaster recovery plan in place

## 3. Floor 8

### 3.1 Floor layout

The Cyber Security intelligence lab layout is like the Applications Development lab; refer to the following figure.

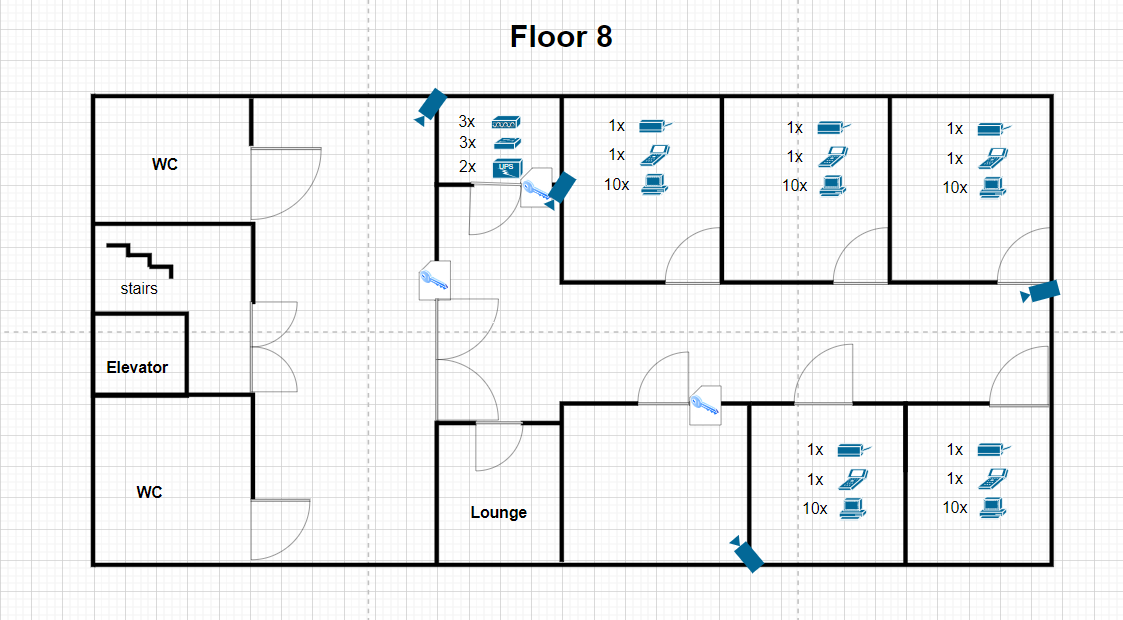


Figure 1.3.1.1 Floor 8 layout

Similarly, employees can only access the area with their keycard, sensitive areas such as the meeting and networking devices room requires equivalent privileges to access. Surveillance cameras are placed in positions allowing them to monitor and manage access within the area. In addition, with 2 UPS equipped, the floor is physically secured and redundant.

### 3.2 Areas classification

The floor has an important role and crucial in DigiTech’s security and operations, including research and development, incident response, policies and upheld sensitive data. The lab is required to be always active.

* **Highly Sensitive**:
  + **Workstations**: data in workstations contains research data and security threatening documents (floor plan, protocols, etc.). If exposed, they would cause great damage to DigiTech
  + **Networking devices room**: Operations within the floor are very crucial, disruptions will make the company vulnerable to attacks.
  + **Meeting room**: conversations and topics discussed in the meeting room should be confidential.
* **Sensitive**:
  + **Cyber Security intelligence lab**: can only be accessed by someone with suitable role or related to its operation.
* **Public**:
  + **Outside of company areas**: elevator, restrooms, stairs, outside hall

### 3.3 CIA triad evaluation

With the classified asset in mind, physical and logical security requirements will be evaluated based on the CIA triad.

* **Confidentiality:**
  + **Physical:**

Use RFID readers to ensure access control, use surveillance cameras and guards to secure the area and manage access.

* + **Logical:**

Enforce strict access control, encrypt all sensitive data, and maintain a least privilege access policy.

* **Integrity:**
  + **Physical:**

Use tamper-evident mechanism on hardware to detect unauthorized access, conduct regular audits and integrity check, and limit access to only maintenance.

* + **Logical:**

Use hashing and digital signature to ensure integrity, implement logging and monitoring, and IDS, IPS to detect and prevent unauthorized changes.

* **Availability:**
  + **Physical:**

Install UPS, backup generators, and ensure climate control practices are in place

* + **Logical:**

Make sure critical assets are redundant with high performance, and have a disaster recovery plan in place

# 2. Network Layout

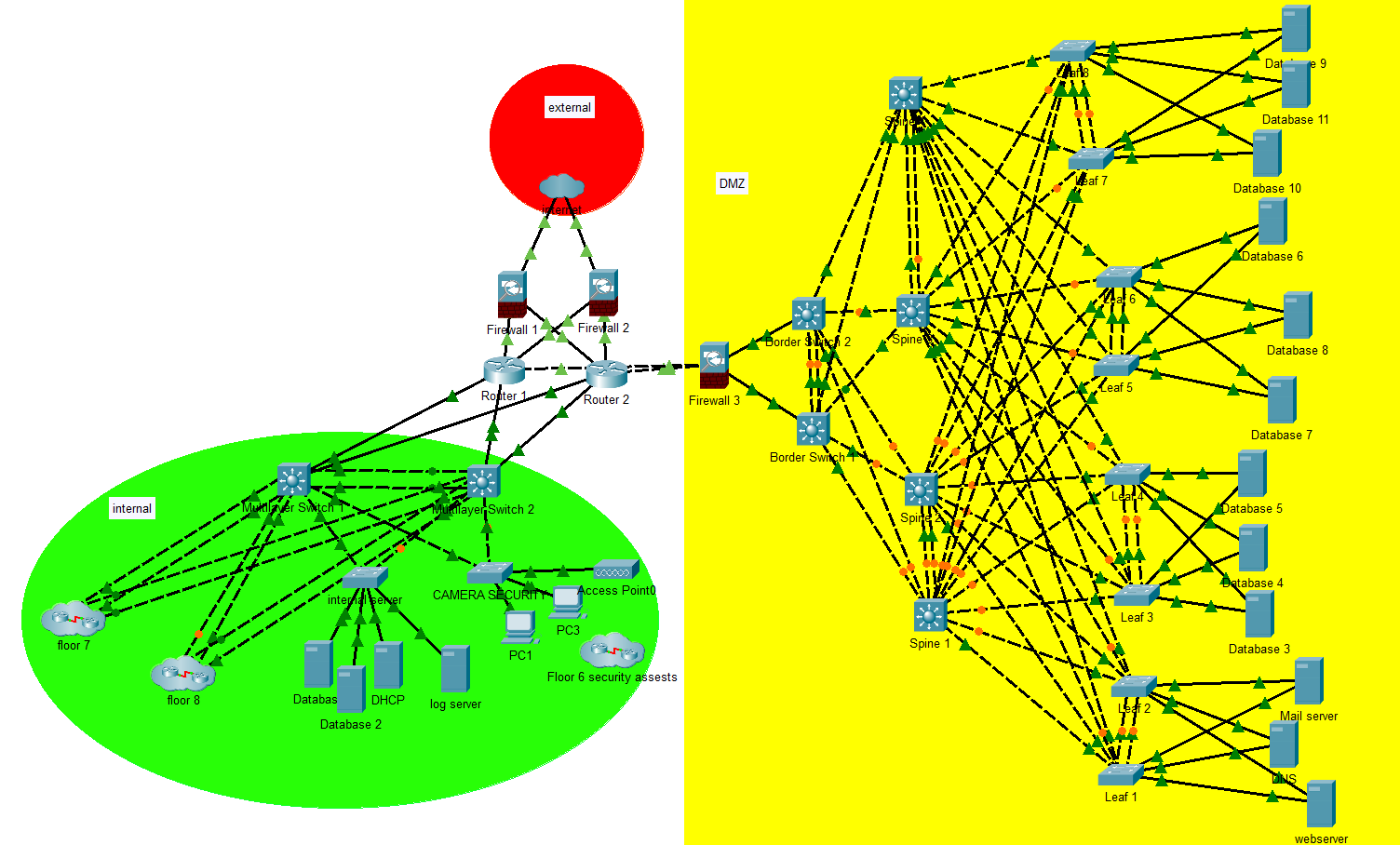


Figure 1.2.0.1 Network Topology (Floor 7,8 can be viewed in appendix)

DigiTech network is divided into three areas: Internal, DMZ and External. The internal network is only accessible by the company strict policy; DMZ, the data center, contains servers and services available to the public. The 2 networks are connected using routers. Firewalls are placed between the company network (Internal and DMZ) and the External network (Internet), providing a layer of protection. Since DMZ allows public access, a fire wall is used as a second layer of protection.

The internal network is built based on the 3-tier network architecture with access, distribution and core layer:

* **Core layer**: Routers connect the entire network together and the internet with high speed
* **Distribution layer**: Layer 3 switches govern local traffic between the access layer with the core layer
* **Access layer:** Layer 2 switches are used to connect with end devices

Data centers should be high performance and scalable, the DMZ network is designed with that in mind, using Spine-Leaf architecture. Spine-Leaf architecture is optimized for server-to-server communications with high scalability, low latency, load-balancing and cost efficiency. The DMZ is be divided into 3 layers:

* + **Core layer**: Routers connect the entire network together and the internet with high speed
  + **Spine layer**: Interconnect the leaves within the network topology.
  + **Leaf layer:**
    - Layer 2 switches are used to connect with end devices
    - Border leaf consist of a pair of layer 3 switches providing high performance external connectivity.

Server latency can be controlled by the number of hops to reach its destination, in this case, 2 hops from one leaf to another. Since the network is connected in full-mesh and travels in fixed hops, Equal Cost Multi-Path can be used to reduce cost and provide load-balancing. The network is highly scalable due to the simplicity of just adding more leaf switch or spine for the need of access or bandwidth, respectively.

Using this architecture also increases availability and redundancy of services running in the data center. Virtualization methods can be used virtual extensible local area network (VxLAN) to smoothly migrate servers with minimal down time. In this scenario, switches are made into pairs using multi-chassis link aggregation group links, providing redundancy without the risk of looping. Furthermore, software defined networking (SDN) solutions can be implemented to the architecture, allowing dynamic and programmatically efficient network configuration.

# 3. Overall CIA evaluation and area classification

## 1. Overall CIA evaluation

1. **Confidentiality:**
   * **Logical Measures:** Encryption, strong access control, least privilege access policies.
   * **Physical Measures:** RFID readers, cameras, security personnel.
2. **Integrity:**
   * **Logical Measures:** Hashing, digital signatures, comprehensive logging and monitoring, IDS/IPS.
   * **Physical Measures:** Tamper-evident seals, regular integrity checks, restricted access.
3. **Availability:**
   * **Logical Measures:** Redundant systems, high-availability configurations, regular backups, disaster recovery planning.
   * **Physical Measures:** UPS, backup generators, HVAC systems.

## 2. Area classification

* **Highly sensitive**: Data center, Cyber security intelligence lab
* **Sensitive**: Application development lab
* **Public**: Non-company areas

# Appendix

A diagram of a computer network

Description automatically generatedA computer network diagram with icons

Description automatically generated