**Task 1: Assess VIP Events' Cybersecurity Requirements**

As VIP Events transitions to its new business facility, it is crucial to prioritize cybersecurity to protect sensitive data, ensure operational continuity, and maintain the trust of clients.

The company’s operations involve

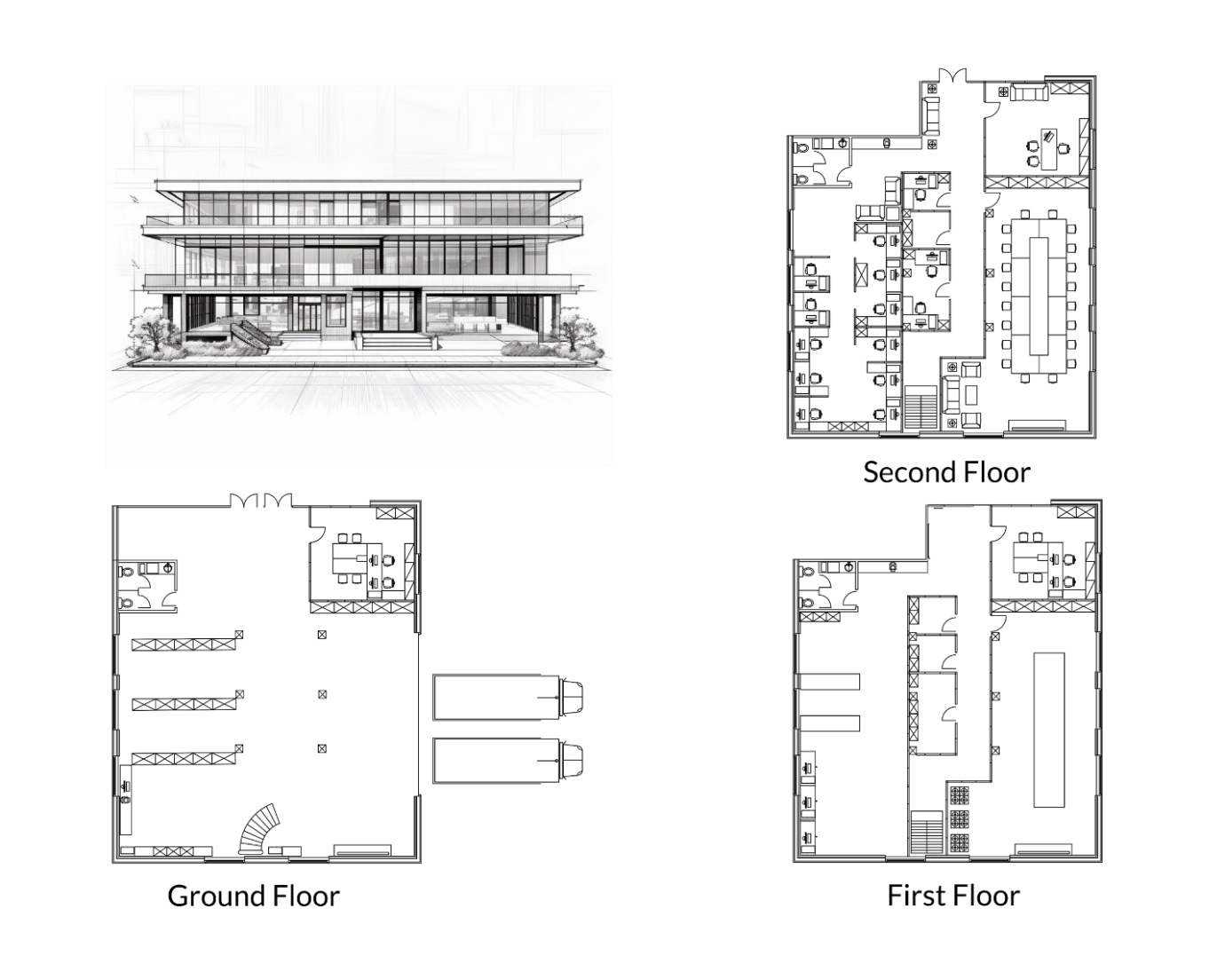
* handling equipment,
* food preparation,
* event management,
* and administrative tasks

all of which require secure access to digital systems.

With a growing workforce and transient staff, there is an increased risk of unauthorized access, data breaches, and cyberattacks. Enhancing cybersecurity will safeguard intellectual property, financial information, and personal data while ensuring compliance with industry standards.

**Task 2: Document the Building Structure and Network Design**

Building Structure



The new premises consist of three floors, each serving a specific function:

1. Ground Floor: Loading dock and storage space for machinery.

2. First Floor: Food preparation kitchens and storage.

3. Second Floor: Office space and conference rooms.

Proposed Subnets

To enhance security and manage traffic efficiently, the building network should be divided into subnets. Below are the proposed subnets:

1. Dock\_Operations

- Purpose: Supports loading dock operations.

- Justification: Isolates machinery and equipment handlers from other parts of the network to prevent unauthorized access and reduce congestion. This segregation ensures that only authorized personnel can interact with loading dock systems, minimizing the risk of operational disruptions.

2. Equipment\_Storage

- Purpose: Support storage for equipment, while providing   
 - Justification: Ensures efficient tracking and management of culinary tools and resources while segregating sensitive equipment data from other operational areas. This isolation protects critical inventory and maintenance systems from unauthorized access, ensuring optimal utilization and safeguarding against potential cyber threats.

3. Kitchen

- Purpose: Dedicated to food preparation and kitchen management on the first floor.

- Justification: Ensures chefs and catering managers have secure access to kitchen-related systems while protecting sensitive recipes and operational data.

4. Office

- Purpose: Serves office workers, management, and conference rooms on the second floor.

- Justification: Segregates administrative tasks and sensitive business data from other operational areas.

5. Guest

- Purpose: Provides internet access to visitors and transient staff.

- Justification: Limits guest access to external resources only, preventing them from interacting with internal systems.

6. Management

- Purpose: Exclusive access for the CEO and senior management.

- Justification: Protects strategic oversight and decision-making processes by isolating high-level access.

**Task 3: Wireless Network Configuration**

Proposed Wireless Network Segments:

1. VIP\_Staff\_WiFi

- Purpose: For permanent employees (equipment handlers, chefs, office workers, etc.).

- Device Types Allowed: Desktops, laptops, tablets, and mobile phones assigned to employees.

- Justification: Ensures secure access to internal systems while segregating employee devices from guest devices.

2. VIP\_Guest\_WiFi

- Purpose: For visitors and transient staff.

- Device Types Allowed: Personal devices brought by guests or temporary workers.

- Justification: Prevents unauthorized access to internal networks while providing basic internet connectivity.

3. VIP\_IoT\_WiFi

- Purpose: For Internet of Things (IoT) devices such as smart kitchen appliances, cameras and inventory trackers.

- Device Types Allowed: IoT-enabled equipment and sensors.

- Justification: Reduces the risk of IoT devices being compromised and used as entry points for attacks.

4. VIP\_Management\_WiFi

- Purpose: Exclusive wireless access for the CEO and senior management.

- Device Types Allowed: Laptops, tablets, and mobile phones used by management.

- Justification: Ensures secure and private communication for high-level decision-makers.

**Task 4: Access Control and Security Policies**

Access Control Measures

- Dock\_Operation and Equipment\_Storage: Restricted to equipment handlers and the equipment manager. Access controlled via role-based authentication.

- Kitchen: Limited to chefs, head chefs, and catering managers. Devices must authenticate using MAC address filtering.

- Office: Accessible to office workers, management, and the CEO. Multi-factor authentication (MFA) required.

- Guest: Open access with bandwidth throttling and content filtering.

- Management: Exclusive access for the CEO and senior management. Requires MFA and IP whitelisting.

Custom Policies

- Role-Based Access Control (RBAC): Define permissions based on user roles (e.g., EquipHandlersRole, ChefsRole).

- Time-Based Access: Temporary staff permissions expire after a predefined period.

- Data Encryption: All data transmitted within the network must be encrypted using TLS/SSL protocols.

Policies to Be Created in Stage 5

- Incident response plan for cyberattacks.

- Regular auditing and monitoring policies.

- Employee training programs on cybersecurity best practices.

**Task 5: User Roles and Access Requirements**

User Roles:

1. Equipment Handlers

- Access: Equipment management functionalities via tablets.

- Devices: 4 Tablets.

2. Equipment Manager

- Access: Full equipment management and maintenance tools.

- Devices: Desktop computer, tablet.

3. Chefs

- Access: Food preparation and kitchen management features.

- Devices: 3 Mobile phones, 3 tablets.

4. Head Chef

- Access: Elevated kitchen management and coordination tools.

- Devices: Tablet, desktop computer.

5. Catering Manager

- Access: Event planning and logistics management.

- Devices: Tablet, desktop computer.

6. Office Workers

- Access: Administrative and data management functionalities.

- Devices: 3 Desktop computers.

7. CEO (Owner)

- Access: Unrestricted access to all functionalities.

- Devices: Desktop computer, Tablet, mobile phone.

8. Transient Staff

- Access: Limited permissions for day-specific tasks.

- Devices: 30 Mobile phones.

**Task 6: Physical Security Guidelines**

Layer 0 Defense Measures:

1. Access Control Systems: Install biometric scanners and keycard readers at entry points to restrict unauthorized access.

2. Surveillance Cameras: Deploy CCTV cameras in critical areas (loading dock, kitchens, offices).

3. Secure Storage: Use locked cabinets for sensitive documents and equipment.

4. Visitor Management: Implement a sign-in system for guests and issue temporary badges.

5. Environmental Controls: Install fire suppression systems and temperature monitors in server rooms.

**Documentation Summary**

Project Scope:

The project aims to design a robust cybersecurity framework and network infrastructure for VIP Events’ new facility. Key deliverables include:

1. Building and Subnets: Three floors with dedicated subnets for dock operations, equipment management, kitchen, office, guest, and management areas.

2. Wi-Fi Setup: Four wireless segments tailored to staff, guests, IoT devices, and management.

3. Access Control and Policies: Role-based access, time-limited permissions, and encryption protocols.

4. User Roles: Defined access requirements for 8 user groups based on job functions.

5. Physical Security: Comprehensive measures to protect Layer 0, including access controls, surveillance, and environmental safeguards.

This scope ensures VIP Events meets its cybersecurity and operational needs while preparing for future growth and challenges.