SECURITY ENHANCEMENT PROJECT

Silverspoon Senior Living Foundation

Project Manager: Timi Ogunjobi

INTRODUCTION AND NOTE:

This document outlines a conceptual project designed to demonstrate the flow of progress through the various stages of a typical project, from the **Initiating** to the **Planning** phase. The purpose of this case study, which is itself a work in progress, is to showcase a structured approach to project management, emphasizing key milestones, deliverables, and strategies that are essential in ensuring a successful project execution.

It is important to note that this is a **hypothetical case study**, created from my personal observations and experiences at **Lenbrook Square Foundation**. While it reflects real-world insights gathered from the operational and project activities within the organization, the scenarios presented here are entirely fictional and intended solely for the purposes of demonstrating my project management abilities. This case study is tailored to support my current application for the position of **Project Manager**.

As such, this document is not intended for public distribution or professional use outside of the job application process. It serves exclusively as an internal tool to highlight my understanding of project management principles, methodologies, and techniques, particularly in environments like those found at Lenbrook Square. The concepts and solutions outlined within are speculative and should not be regarded as actual proposals for implementation within Lenbrook Square or any other organization.

Timi Ogunjobi

PROJECT CONCEPTS

PROJECT OVERVIEW:

The goal of the Silverspoon Senior Living Foundation security enhancement project is to implement a comprehensive security solution that integrates both physical and cybersecurity measures. This dual-focus approach ensures the safety and well-being of residents and staff while protecting sensitive digital infrastructure, personal information, and operational continuity.

KEY COMPONENTS:

- **Physical Security Systems:**
    1. **Access Control:** Advanced keycard systems, biometric authentication (fingerprint, face recognition), and visitor management protocols to ensure that only authorized personnel can enter specific areas.
    2. **Surveillance:** Installation of high-definition CCTV cameras in critical areas with real-time monitoring and motion detection, integrated with remote-access capabilities for real-time intervention.
    3. **Alarms & Sensors:** A network of smart motion detectors, glass-break sensors, and door/window alarms that trigger immediate alerts to security personnel or emergency services.
    4. **Perimeter Security:** Enhanced fencing, gates with vehicle license plate recognition, and automated barriers at entry points, ensuring the physical protection of the entire facility.
    5. **Panic Buttons & Wearable Alerts:** Residents and staff will have access to panic buttons and wearable devices that can send real-time alerts to security personnel during emergencies.
- **Cybersecurity Systems:**
    1. **Network Security:** Implementation of firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to safeguard the digital infrastructure from unauthorized access.
    2. **Data Protection:** Encryption protocols for all data stored on the servers, including residents' personal information, financial records, and medical data.
    3. **Endpoint Security:** Use of antivirus software, malware detection, and regular patching across all endpoints (computers, mobile devices, IoT systems) used by staff and residents.
    4. **Incident Response Plan:** Development of a robust cybersecurity incident response plan to mitigate and recover from cyberattacks or data breaches.

5. **Training & Awareness:** Regular training sessions for staff to improve awareness of phishing attempts, social engineering, and other cybersecurity threats.

- **Integration of Physical & Cybersecurity:**
    1. **Unified Dashboard:** A centralized dashboard where both physical security and cybersecurity threats are monitored and addressed in real time.
    2. **IoT Integration:** Security devices such as cameras, alarms, and access controls will be interconnected through secure IoT networks, ensuring seamless communication between systems.
    3. **Cloud Backup:** Continuous cloud backups of critical data, ensuring that all systems are recoverable in case of an attack or failure.
    4. **Incident Reporting:** A system for logging and reporting both physical and cyber incidents, allowing for analysis and proactive security improvements.

PHASES OF THE PROJECT:

1. **Assessment:** Detailed risk assessment of current physical and cybersecurity vulnerabilities, including an audit of existing systems and infrastructure.
2. **Design:** Creation of a blueprint for an integrated security system that meets the specific needs of the Silverspoon Senior Living Foundation.
3. **Implementation:** Procurement, installation, and configuration of all security hardware and software, ensuring minimal disruption to daily operations.
4. **Testing:** Conduct penetration testing for cybersecurity and stress testing for physical systems to identify potential weaknesses.
5. **Training & Awareness:** Training staff on the use of new systems and conducting cybersecurity workshops to reduce human error.
6. **Monitoring & Maintenance:** Ongoing monitoring and maintenance to ensure that both physical and cyber defenses remain effective as threats evolve.

BUSINESS REQUIREMENTS DOCUMENT

Project Name:
Silverspoon Senior Living Foundation Security Enhancement Project

Prepared By:
Timi Ogunjobi, Project Lead

Date:
10/15/2024

1. Business Overview

Project Objective: The Silverspoon Senior Living Foundation Security Enhancement Project aims to protect its residents, staff, physical premises, and digital infrastructure through an integrated solution combining both physical security and cybersecurity measures. The project will deploy interconnected systems that enable real-time monitoring, incident detection, and swift responses to potential security threats.

2. Functional Requirements

The **functional requirements** specify what the system should do to meet the business needs. This section covers the operational aspects that directly address how the system interacts with users and its key functions.

2.1. Access Control

- **Requirement 1:**
  Implement an access control system using keycards and biometric authentication. The system must limit access to restricted areas based on role, time, and security clearance.
    - **Function:** Restrict unauthorized personnel from entering sensitive areas such as data centers, medical wings, or administrative offices.
    - **Users:** Residents, Staff, Visitors
- **Requirement 2:**
  The system must allow real-time monitoring of entries and exits at all access points.
    - **Function:** Provide a detailed log of all entries and exits for reporting and auditing purposes.

2.2. Surveillance and Monitoring

- **Requirement 3:**
  Deploy CCTV cameras across all critical zones within the facility, including entry and exit points, hallways, and common areas. The system must support 24/7 real-time monitoring.
    - **Function:** Continuous visual surveillance for incident detection, enabling security personnel to monitor all activities in the facility.
- **Requirement 4:**
  Enable remote access to camera feeds for authorized personnel to monitor incidents from mobile devices and computers.
    - **Function:** Security personnel can respond quickly from remote locations, especially in emergency situations.

2.3. Intrusion Detection and Alarm Systems

- **Requirement 5:**
  Install smart motion sensors, glass-break detectors, and door/window alarms to detect unauthorized entry.
    - **Function:** Provide instant alerts to security personnel if an unauthorized breach is detected, reducing response time.
- **Requirement 6:**
  Panic buttons must be available throughout the facility, with wearable devices for residents and staff, enabling instant alerts during emergencies.
    - **Function:** Allow individuals in distress to signal security for immediate assistance.

2.4. Incident Management

- **Requirement 7:**
  Implement an incident reporting system that logs physical and cybersecurity incidents with detailed descriptions, timestamping, and alerting mechanisms.
    - **Function:** Facilitate accurate reporting and auditing of security-related events.
- **Requirement 8:**
  The system must support escalation procedures based on the severity of the incident, triggering alerts to designated personnel and management as needed.
    - **Function:** Ensure proper handling of security incidents based on established protocols.

2.5. Cybersecurity Systems

- **Requirement 9:**
  Deploy firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to secure the network from unauthorized access and cyberattacks.
    - **Function:** Block, detect, and prevent cyberattacks on the facility's IT infrastructure.
- **Requirement 10:**
  Implement data encryption to protect resident, staff, and financial information both in storage and in transit.
    - **Function:** Ensure sensitive data is securely stored and transmitted.

2.6. User Training and Awareness

- **Requirement 11:**
  Provide comprehensive training sessions for staff to understand the use of physical security systems (e.g., access control, panic buttons) and cybersecurity protocols (e.g., phishing detection, password security).
    - **Function:** Ensure all staff are well-prepared to use the system and prevent security incidents caused by human error.

2.7. System Integration

- **Requirement 12:**
  All physical and cybersecurity systems must be integrated into a centralized dashboard that provides real-time status updates, incident reporting, and control over the entire facility's security network.

- **Function:** Allow authorized personnel to monitor both physical and cybersecurity threats from a single control point.

Functional Requirements

	Requirement ID	Requirement Description	Function
1	FR-01	Implement access control system using keycards and biometric authentication.	Restrict unauthorized access.
2	FR-02	Allow real-time monitoring of entries and exits at all access points.	Provide detailed entry/exit logs.
3	FR-03	Deploy CCTV cameras in critical zones for 24/7 monitoring.	Continuous visual surveillance.
4	FR-04	Enable remote access to camera feeds for security personnel.	Remote monitoring for quicker response.
5	FR-05	Install smart motion sensors, glass-break detectors, and alarms.	Detect and alert unauthorized entry.
6	FR-06	Provide panic buttons and wearable devices for emergency alerts.	Enable immediate alerts during emergencies.
7	FR-07	Implement incident reporting system for physical and cyber incidents.	Facilitate accurate incident reporting.
8	FR-08	Support escalation procedures based on incident severity.	Proper escalation handling of incidents.
9	FR-09	Deploy firewalls, IDS, and IPS to secure the network from cyber threats.	Protect IT infrastructure from cyber threats.
10	FR-10	Implement data encryption for resident, staff, and financial data.	Ensure secure data storage and transmission.
11	FR-11	Provide training for staff on physical and cybersecurity systems.	Prepare staff to prevent human error.
12	FR-12	Integrate all systems into a centralized monitoring dashboard.	Unified security management and monitoring.

3. Technical Requirements

The **technical requirements** define how the system should be built and implemented from an engineering and technology perspective. This section covers hardware, software, and system architecture details.

3.1. Hardware Requirements

- **Requirement 1:**
  Install high-definition CCTV cameras with night vision capabilities and at least 1080p resolution.
  - **Justification:** High-resolution footage is essential for identifying potential intruders and maintaining evidence quality.
- **Requirement 2:**
  Keycard and biometric access devices should be deployed at all sensitive entry points, and all hardware should be compliant with existing security protocols (ISO/IEC 27001).
  - **Justification:** Ensures compatibility with security standards and guarantees future system upgrades.
- **Requirement 3:**

Motion detectors and sensors must be connected via a secured IoT network, with backup battery systems to ensure continued functionality in case of power outages.

- **Justification:** Continuous system uptime is critical for security coverage, even during power failures.

3.2. Software Requirements

- **Requirement 4:**
  Install a firewall, IDS, and IPS on all servers and network-connected devices. The software must be capable of deep packet inspection and support updates for the latest cyber threat intelligence.
  - **Justification:** Ongoing threat detection is critical for protecting against evolving cyber threats.
- **Requirement 5:**
  Data encryption must follow the Advanced Encryption Standard (AES-256) for all sensitive data.
  - **Justification:** AES-256 is a robust encryption standard suitable for safeguarding personal and financial data.

3.3. Network Requirements

- **Requirement 6:**
  The system must have redundancy across all network connections, ensuring that security systems remain functional during outages or technical malfunctions.
  - **Justification:** High availability is critical in ensuring that the security systems remain active and connected at all times.
- **Requirement 7:**
  All security devices (CCTV, motion sensors, alarm systems) must be connected over a secure, encrypted, and isolated network to prevent unauthorized access or interception.
  - **Justification:** Isolating the security network from other operational networks prevents potential breaches from spreading across the facility's IT infrastructure.

3.4. Data Storage Requirements

- **Requirement 8:**
  Implement a cloud-based backup solution with encryption to store security footage, incident logs, and access records. Data must be stored for a minimum of 12 months to comply with local and federal regulations.
  - **Justification:** Cloud backups ensure data integrity and recovery in case of breaches, loss, or hardware failure.
- **Requirement 9:**
  Ensure real-time data syncing between the physical security and cybersecurity systems for live updates and monitoring.
  - **Justification:** Synchronization allows immediate cross-referencing of physical and cyber events, improving response times.

3.5. Compliance Requirements

- **Requirement 10:**
  The cybersecurity solution must comply with local, state, and federal regulations concerning data privacy and security, including but not limited to HIPAA, GDPR, and the CCPA.
    - **Justification:** Compliance ensures that the facility is not exposed to legal or financial penalties due to data breaches.

Functional Requirements

	Requirement ID	Requirement Description	Function
1	FR-01	Implement access control system using keycards and biometric authentication.	Restrict unauthorized access.
2	FR-02	Allow real-time monitoring of entries and exits at all access points.	Provide detailed entry/exit logs.
3	FR-03	Deploy CCTV cameras in critical zones for 24/7 monitoring.	Continuous visual surveillance.
4	FR-04	Enable remote access to camera feeds for security personnel.	Remote monitoring for quicker response.
5	FR-05	Install smart motion sensors, glass-break detectors, and alarms.	Detect and alert unauthorized entry.
6	FR-06	Provide panic buttons and wearable devices for emergency alerts.	Enable immediate alerts during emergencies.
7	FR-07	Implement incident reporting system for physical and cyber incidents.	Facilitate accurate incident reporting.
8	FR-08	Support escalation procedures based on incident severity.	Proper escalation handling of incidents.
9	FR-09	Deploy firewalls, IDS, and IPS to secure the network from cyber threats.	Protect IT infrastructure from cyber threats.
10	FR-10	Implement data encryption for resident, staff, and financial data.	Ensure secure data storage and transmission.
11	FR-11	Provide training for staff on physical and cybersecurity systems.	Prepare staff to prevent human error.
12	FR-12	Integrate all systems into a centralized monitoring dashboard.	Unified security management and monitoring.

4. Performance Requirements

- **Requirement 1:**
  The surveillance system must provide real-time video feeds with no more than a 2-second delay to ensure live monitoring accuracy.
- **Requirement 2:**
  The access control system must authenticate users in less than 2 seconds to avoid any delays in operational flow.
- **Requirement 3:**
  The incident reporting system should generate real-time alerts within 5 seconds of detecting an anomaly, with automatic escalation based on the severity of the incident.

5. Security Requirements

- **Requirement 1:**
  All physical devices connected to the security network must use encrypted communication protocols (e.g., TLS 1.2 or higher).
- **Requirement 2:**
  Implement multi-factor authentication (MFA) for all system administrators and privileged accounts accessing the security dashboard and servers.
- **Requirement 3:**
  The system must log all access attempts (successful and failed) and generate a report of suspicious activity, such as multiple failed login attempts, for security audits.

6. Testing and Validation Requirements

- **Requirement 1:**
  Conduct penetration testing on the cybersecurity infrastructure to identify potential vulnerabilities and weaknesses before go-live.
- **Requirement 2:**
  Perform stress testing on physical security systems, including surveillance cameras, access controls, and alarm systems, to ensure they remain functional during high-load conditions.

7. Implementation Requirements

- **Requirement 1:**
  The implementation must occur in phases to ensure minimal disruption to ongoing operations at the senior living facility.
- **Requirement 2:**
  Post-installation, a 30-day testing period must be conducted to identify and resolve any system bugs or integration issues before full deployment.

8. Maintenance and Support

- **Requirement 1:**
  Ensure ongoing software updates for both physical and cybersecurity systems to address emerging threats and vulnerabilities.
- **Requirement 2:**
  Set up a 24/7 helpdesk support system for any incidents or issues reported by security personnel or system users.

9. Stakeholders

- **Primary Stakeholders:**
  - Residents
  - Staff (Security and Admin)
  - Board of Directors
  - IT Department
- **Secondary Stakeholders:**
  - Vendors (Security systems providers, IT service providers)
  - Contractors for installation

PROJECT CHARTER DOCUMENT

Project Name:
Silverspoon Senior Living Foundation Security Enhancement Project

Project Sponsor:
Silverspoon Senior Living Foundation Board of Directors

Project Manager:
Timi Ogunjobi

Prepared By:
Timi Ogunjobi, Project Lead

1. Project Purpose:

The purpose of this project is to enhance the overall security of the Silverspoon Senior Living Foundation by integrating advanced physical security measures with cutting-edge cybersecurity protocols. The goal is to provide a safe and secure environment for residents, staff, and visitors while protecting sensitive digital information and operational infrastructure.

2. Objectives:

1. To reduce physical security vulnerabilities by installing state-of-the-art access control, surveillance, and alarm systems.
2. To protect the digital infrastructure from cyber threats by implementing robust cybersecurity protocols.
3. To ensure seamless integration of physical and cybersecurity systems for real-time monitoring and response.
4. To train staff on both physical security protocols and cybersecurity best practices to prevent breaches.
5. To develop a long-term maintenance and monitoring plan to ensure continued security improvements.

3. Scope:

In Scope:

- Installation of physical security systems (CCTV, alarms, access controls).
- Implementation of cybersecurity systems (firewalls, encryption, IDS/IPS).
- Integration of IoT devices across both physical and cybersecurity systems.
- Training of staff on new systems and security protocols.
- Continuous monitoring, testing, and maintenance post-implementation.

Out of Scope:

- Major structural renovations of the facility.
- Non-security related IT infrastructure upgrades.
- Services related to healthcare data compliance (HIPAA), though data protection systems will comply with best practices.

4. Deliverables:

1. **Physical Security Deliverables:**
    - Fully installed and operational CCTV network.
    - Biometric and keycard access systems.
    - Smart motion detectors, glass-break sensors, and alarm systems.
    - Wearable panic devices for residents and staff.
2. **Cybersecurity Deliverables:**
    - Secured digital infrastructure with firewalls and IDS/IPS.
    - Encrypted data storage for sensitive information.
    - Endpoint protection for all devices connected to the network.
    - Incident response and logging system for cybersecurity events.
3. **Integration:**
    - Centralized dashboard to monitor and manage both physical and cybersecurity incidents in real time.
4. **Training & Documentation:**
    - Comprehensive training manual for system users.
    - Scheduled training workshops for staff on security protocols.
    - Incident reporting and response documentation.

5. Project Milestones:

1. **Risk Assessment Complete:** [TBD]
2. **System Design Approved:** [TBD]
3. **Procurement of Equipment:** [TBD]
4. **Installation Phase Begins:** [TBD]
5. **System Testing & Penetration Testing:** [TBD]
6. **Staff Training Complete:** [TBD]
7. **Go-Live:** [TBD]

6. Budget:

Category	Estimated Cost
Security Hardware (Cameras, Alarms, etc.)	$100,000
Cybersecurity Software & Tools	$75,000
Installation & Labor	$50,000
Training & Awareness Programs	$20,000
Ongoing Monitoring & Maintenance	$15,000/year
Total Estimated Cost	**$245,000**

7. Project Risks and Mitigation:

Risk	Likelihood	Impact	Mitigation Strategy
Installation Delays	Medium	High	Engage multiple vendors to ensure equipment availability.
Cybersecurity Breach During Implementation	Low	High	Implement temporary safeguards during installation.
System Integration Challenges	Medium	Medium	Conduct phased testing to ensure seamless integration.
Lack of Staff Adoption	Medium	Medium	Comprehensive training programs and easy-to-use systems.
Budget Overruns	Medium	High	Strict budget management with contingency funds.

8. Stakeholders:

- **Primary Stakeholders:**
    - Residents of Silverspoon Senior Living Foundation
    - Staff and caregivers
    - Board of Directors
    - IT and Security Departments
- **Secondary Stakeholders:**
    - Vendors (Security equipment and software providers)
    - Contractors responsible for installation and maintenance

9. Assumptions:

- The project will be completed within the approved budget.
- All systems will be compatible with existing infrastructure.
- The project will not disrupt the daily lives of residents or critical operations.

10. Approvals:

Role	Name	Signature	Date
Project Sponsor			
Project Manager			
Security Director			
IT Manager			
Finance Manager			

PROJECT MANAGEMENT PLAN

Project Name:
Silverspoon Senior Living Foundation Security Enhancement Project

Project Manager:
Timi Ogunjobi

Date:
10/15/2024

1. Executive Summary

The **Silverspoon Senior Living Foundation Security Enhancement Project** is designed to strengthen both physical and cybersecurity at the foundation's facility. This project will ensure the safety of residents, staff, and visitors while protecting sensitive data and digital infrastructure from potential threats. The project will be implemented through an integrated approach that combines the latest physical security systems (e.g., CCTV, access control, alarms) and advanced cybersecurity measures (e.g., firewalls, encryption, and incident response protocols).

2. Objectives

The main objectives of this project are:

- To safeguard residents, staff, and the physical premises with state-of-the-art security systems.
- To protect the digital infrastructure and sensitive data from unauthorized access, breaches, and cyberattacks.
- To integrate physical and cybersecurity measures for real-time monitoring and coordinated response.
- To ensure the project is completed within the stipulated time frame, budget, and quality requirements.

3. Project Scope

In Scope:

- Installation of CCTV surveillance systems with real-time monitoring capabilities.
- Deployment of biometric and keycard-based access control systems.
- Installation of intrusion detection systems (motion sensors, glass-break detectors).
- Implementation of firewalls, intrusion detection systems (IDS), and encryption protocols.
- Integration of physical and cybersecurity systems into a centralized control dashboard.
- Training for staff on how to use the new security systems and respond to incidents.
- Development of a comprehensive incident reporting and management protocol.

Out of Scope:

- Structural renovations of the facility.
- Non-security-related IT upgrades.
- Healthcare compliance services (e.g., HIPAA) beyond implementing encryption for data protection.

4. Project Deliverables

- **Physical Security Deliverables:**
    - Fully operational CCTV system with night vision and motion detection.
    - Biometric and keycard access control system installed and tested.
    - Smart alarms and panic buttons in critical areas and with residents and staff.
- **Cybersecurity Deliverables:**
    - Deployed firewalls and IDS for protecting the digital network.
    - Encrypted sensitive resident and staff data using AES-256.
    - Backup solutions implemented for critical security footage and logs.
- **Training and Documentation:**
    - Training manuals for staff on using security systems and responding to incidents.
    - Documentation for system installation, configurations, and incident response plans.
- **Integrated System:**
    - Unified security dashboard for real-time monitoring of physical and cybersecurity incidents.

5. Project Milestones

Milestone	Estimated Completion Date
Project Kickoff	[TBD]
Risk Assessment Complete	[TBD]
Design and Planning Approved	[TBD]
Procurement of Equipment	[TBD]
Installation of Physical Security Systems	[TBD]
Installation of Cybersecurity Systems	[TBD]
System Integration Complete	[TBD]
Testing and Debugging Complete	[TBD]
Staff Training Completed	[TBD]
Go-Live	[TBD]

6. Roles and Responsibilities

Role	Responsibilities	Name
Project Sponsor	Provides overall project direction, support, and resources	Silverspoon Board
Project Manager	Manages project scope, budget, timeline, and deliverables	Timi Ogunjobi
IT Manager	Oversees cybersecurity implementations	[Gary]
Security Director	Oversees physical security systems implementation	[Kevin]
Vendor(s)	Supplies security hardware and software	[Vendor Name(s)]

Role	Responsibilities	Name
Staff Trainer	Delivers staff training on the new systems	[Trainer Name]

7. Project Schedule

Task	Start Date	End Date	Duration (Days)
Project Kickoff	[TBD]	[TBD]	2
Conduct Risk Assessment	[TBD]	[TBD]	5
System Design and Blueprint	[TBD]	[TBD]	10
Procurement of Equipment and Software	[TBD]	[TBD]	15
Install Physical Security Systems	[TBD]	[TBD]	20
Install Cybersecurity Systems	[TBD]	[TBD]	15
System Integration Testing	[TBD]	[TBD]	7
Staff Training	[TBD]	[TBD]	5
Go-Live	[TBD]	[TBD]	1

8. Budget

Category	Estimated Cost
Security Hardware (CCTV, Alarms, etc.)	$100,000
Cybersecurity Software (Firewalls, IDS)	$75,000
Installation & Labor	$50,000
Staff Training	$20,000
Maintenance and Monitoring	$15,000/year
Total Estimated Cost	**$245,000**

9. Risk Management

Risk	Likelihood	Impact	Mitigation Strategy
Delays in Equipment Delivery	Medium	High	Work with multiple vendors for contingency planning.
Cybersecurity Breach During Installation	Low	High	Implement temporary firewalls during installation.
System Integration Challenges	Medium	Medium	Conduct phased testing to ensure compatibility.
Staff Resistance to New Systems	Medium	Medium	Provide thorough training and easy-to-use interfaces.

10. Quality Management Plan

Quality Standards:

- All systems must comply with local security and cybersecurity regulations.
- The CCTV system must provide a minimum resolution of 1080p for surveillance.
- Cybersecurity protocols (e.g., firewalls, IDS, encryption) must adhere to industry standards like ISO/IEC 27001.
- Incident response times must be under 2 minutes for critical alerts.

Testing Approach:

- Conduct penetration testing for cybersecurity systems to identify vulnerabilities.
- Perform stress testing on the physical security systems (e.g., surveillance cameras, access controls) to ensure they can handle high activity periods.
- User Acceptance Testing (UAT) will be conducted after installation to verify that the systems meet operational requirements.

11. Communications Plan

Communication Type	Frequency	Owner	Audience	Purpose
Project Status Reports	Weekly	Project Manager	Project Team, Stakeholders	Provide updates on progress, milestones, risks
Steering Committee Meetings	Bi-weekly	Project Sponsor	Board of Directors	Review progress and address escalated issues
Team Meetings	Weekly	Project Manager	Project Team	Coordinate tasks and resolve issues
Training Sessions	As needed during phase	Staff Trainer	Security and IT Staff	Train staff on the use of the new systems
Go-Live Announcements	Day of Go-Live	Project Manager	All staff and residents	Inform everyone about the new system launch

12. Change Management Plan

Any changes to the project scope, budget, or timeline will follow a formal **Change Control Process**. Change requests must be submitted to the **Project Manager**, evaluated for impact on the project, and approved by the **Project Sponsor** before implementation.

13. Project Closure

Upon successful completion of the project, a formal project closure will take place, which will include:

- A final review of the project to ensure all deliverables have been met.
- Transfer of system documentation, training materials, and support information to the relevant teams.
- Post-project evaluation to assess project success and gather lessons learned for future projects.
- A project closure report summarizing all activities and outcomes.