Security Policies Report for Silverspoon Senior Living Foundation

by

Timi Ogunjobi
Information Security Analyst & Project Manager
timiasservice@gmail.com
470-727-0678

Introduction

This report outlines the comprehensive security policies for Silverspoon Senior Living Foundation, focusing on areas critical to maintaining the integrity and confidentiality of the information and ensuring the safety and privacy of our residents. These policies encompass password management, data protection, and incident response, and are designed to align with industry best practices and regulatory requirements, including the Health Insurance Portability and Accountability Act (HIPAA).

1. Password Management Policy

Policy Overview

The Password Management Policy is designed to protect the security and integrity of all electronic systems and data at Silverspoon Senior Living Foundation. By enforcing strong password creation, management, and usage standards, the Foundation aims to mitigate the risk of unauthorized access and data breaches, ensuring the safety and privacy of residents.

Implementation Guidelines

Password Complexity Requirements:

- Passwords must be a minimum of 12 characters in length and include a mix of the following character types: uppercase letters, lowercase letters, numbers, and special characters (e.g., !, @, , $).
- Common passwords and easily guessable combinations, such as "password123" or "admin," are prohibited.

Password Change and History:

- Users are required to change their passwords every 90 days. The system will automatically prompt for a password change and prevent the reuse of the last four passwords.
- An audit log of password changes will be maintained for each user account, ensuring compliance with this policy.

Secure Storage and Handling:

- The Foundation will provide an approved, secure password manager for all employees. Training on the use of the password manager will be included in the cybersecurity awareness program.
- Writing down or storing passwords in an unsecured manner, such as on sticky notes or in unprotected digital files, is strictly prohibited.

Account Management:

- Each employee will be assigned a unique user account. Sharing of user accounts and passwords between employees is strictly prohibited to ensure individual accountability.
- Temporary accounts for contractors or vendors will be created as needed and monitored closely, with access revoked immediately upon completion of the work or contract.

Two-Factor Authentication (2FA):

- 2FA will be enabled for accessing critical systems, especially those containing resident information or key operational data. This may include, but is not limited to, email accounts, electronic health records (EHR) systems, and financial management systems.
- The IT department will provide 2FA tokens or software and training on how to use them effectively.

User Responsibilities

- Compliance: All users are responsible for complying with the Password Management Policy. Failure to comply may result in disciplinary actions, up to and including termination of employment.
- Reporting: Users must report any suspected compromise of their passwords to the IT department immediately. This includes receiving phishing emails, experiencing unusual account activity, or any instance where a password may have been shared accidentally.

IT Department Responsibilities

- **Enforcement and Support:** The IT department is responsible for enforcing the Password Management Policy, providing support for password management tools, and assisting users with password changes and account security issues.
- **Audit and Review**: Conduct regular audits of user accounts and password compliance. This includes reviewing password complexity, change logs, and ensuring that 2FA is enabled for appropriate systems.
- **Education:** Provide ongoing education and training on secure password creation, the importance of password security, and how to use provided tools such as password managers and 2FA.

Policy Review and Update

This policy will be reviewed annually or more frequently if needed, to adapt to new cybersecurity threats, regulatory requirements, or technological advancements. Feedback from users and insights from security audits will be considered in updates to ensure the policy remains effective and practical.

2. Data Protection Policy

Policy Overview

The Data Protection Policy establishes a framework to safeguard sensitive and confidential information pertaining to residents and the organization from unauthorized access, alteration, disclosure, or destruction. This framework is critical in maintaining the trust of residents and complying with regulatory standards like HIPAA.

Implementation Guidelines

Data Classification and Handling:
- Implement a data classification system that categorizes all data into tiers (e.g., public, internal, confidential, and highly confidential), with clear guidelines for handling and protection measures for each category.
- Sensitive and confidential data, including health records and personal identification information, must be encrypted using industry-standard encryption methods both at rest (on storage devices) and in transit (during transmission over networks).

Access Control Measures:
- Deploy access control systems that enforce authentication and authorization before granting access to sensitive data. Utilize role-based access control (RBAC) to ensure employees can access only the data necessary for their job functions.
- Conduct periodic reviews of access rights and adjust based on changes in job roles or employment

status to prevent unauthorized access to sensitive information.

Data Retention and Secure Disposal:
- Develop a data retention schedule that specifies how long different types of data should be retained based on legal, regulatory, and operational requirements.
- When data is no longer needed or has reached the end of its retention period, it must be disposed of securely using methods such as electronic data wiping or physical destruction of storage media, in accordance with industry best practices.

Backup and Disaster Recovery:
- Implement regular backup procedures for all critical data, ensuring backups are stored in a secure, off-site location that is geographically separated from the primary data center.
- Develop and regularly test a disaster recovery plan that includes procedures for restoring data from backups in the event of data loss due to cyberattacks, natural disasters, or system failures.

Mobile Device Security:
- Enforce a mobile device policy that requires the installation of security features, such as password or biometric locks, on all devices that access foundation data.
- Implement mobile device management (MDM) solutions that allow for the remote wiping of data on lost or stolen devices to prevent unauthorized access.

Training and Awareness

- Provide regular training sessions for all staff on the importance of data protection, secure data handling practices, and the specific requirements of this policy.
- Include guidelines on recognizing and reporting potential data breaches or security incidents as part of the training program.

Compliance and Monitoring

- Regularly audit compliance with the Data Protection Policy, including checks on data encryption practices, access controls, backup procedures, and secure data disposal methods.
- Establish a reporting mechanism for any suspected data breaches or policy violations, with clear procedures for investigation and remediation.

Policy Review and Update

- Review the Data Protection Policy annually or in response to significant changes in technology, regulatory requirements, or organizational practices.
- Update the policy as needed to address new security challenges, regulatory changes, or findings from compliance audits and data breach investigations.

By implementing this expanded Data Protection Policy, Silverspoon Senior Living Foundation will strengthen its defenses against data breaches and unauthorized access, ensuring the confidentiality, integrity, and availability of all resident and organizational data.

3. Incident Response Policy

Policy Overview

This Incident Response Policy aims to establish a systematic, organized approach to addressing and managing the aftermath of security incidents to limit damage and reduce recovery time and costs.

The policy applies to all employees, contractors, and third-party service providers with access to the organization's digital assets.

Implementation Guidelines

Incident Reporting:
- Develop clear guidelines on what constitutes a security incident, including examples such as data breaches, malware infections, unauthorized access, and phishing attempts.
- Implement a secure, accessible incident reporting system, allowing employees to report incidents anonymously if necessary, to ensure that potential incidents are reported without delay.

Incident Response Team (IRT) Structure and Roles:
- Assemble an IRT with members from IT, legal, human resources, and communications departments to ensure a multifaceted response capability.
- Assign specific roles within the IRT, including but not limited to Incident Manager, Security Analyst, Communications Officer, and Legal Advisor, each with defined responsibilities during an incident.

Incident Analysis and Recovery:
- Outline procedures for initial assessment and classification of incidents based on their severity and potential impact, guiding the allocation of resources and urgency of the response.
- Develop standardized processes for containing and eradicating threats, preserving evidence for investigation, and initiating recovery efforts to restore affected systems and data.

Post-Incident Review:
- Establish a protocol for conducting post-incident reviews within a defined timeframe following the resolution of an incident. This review should involve all stakeholders involved in the incident response to discuss what happened, how it was handled, and what could be improved.
- Document findings and recommendations from the post-incident review, updating incident response plans and security policies as necessary to prevent recurrence of similar incidents.

Communication:
- Create templates and protocols for internal and external communication during and after an incident, ensuring that messages are clear, accurate, and consistent.
- Define thresholds for when incidents should be reported to external entities, including regulatory bodies, affected individuals, and law enforcement, in compliance with legal and regulatory requirements.

Training and Exercises

- Conduct regular training for the IRT and all employees on their roles in the incident response process, including hands-on exercises and simulations to prepare them for real incidents.
- Schedule annual or bi-annual incident response drills that involve not just the IRT but also other employees, to test the effectiveness of communication plans, role clarity, and procedural adherence.

Compliance and Legal Considerations

- Review and incorporate legal and regulatory requirements related to incident response and reporting, particularly those pertaining to healthcare information, into the policy.
- Ensure the policy allows for flexibility to adapt to changing legal landscapes and regulatory obligations.

Policy Review and Update

- Commit to a regular review cycle for the Incident Response Policy, at least annually, or following significant changes to technology, organizational structure, or after a major incident, to ensure it remains effective and relevant.

Policy Enforcement

Failure to comply with these security policies may result in disciplinary action, up to and including termination of employment for employees, or termination of contracts for vendors and third parties. Regular audits and reviews will be conducted to ensure compliance and identify areas for improvement.

Review and Update

These policies will be reviewed annually and updated as necessary to reflect changes in technology, business operations, laws, and regulatory requirements.

Conclusion

The implementation and adherence to these comprehensive security policies are vital to protecting the Silverspoon Senior Living Foundation's data assets and ensuring the privacy and security of our residents. All employees and stakeholders are responsible for understanding and complying with these policies to maintain a secure and resilient information environment.