Health Tech Security Policies & Procedures

openaccesspolicies.org

Table of Contents

Access Control Policies

Access Control Procedures

Engineering Policies

Engineering Procedures

ISMS Supplements

Operational Policies

Operational Procedures

Resilience Policies

Resilience Procedures

Security Policies

Security Procedures

Access Control Policy (AC-POL-001)

1. Objective

The objective of this policy is to define the requirements for managing access to **[Company Name]**'s information systems, data, and physical facilities. This policy ensures that access is granted based on the principles of least privilege and separation of duties, thereby protecting the confidentiality, integrity, and availability of corporate and customer information, including electronic Protected Health Information (ePHI).

2. Scope

This policy applies to all **[Company Name]** workforce members, third-party contractors, and vendors who require access to any company information asset. This includes, but is not limited to, applications, servers, databases, network devices, and cloud services. This policy applies to all physical and virtual locations where company information assets are accessed, stored, or processed, including corporate offices, remote work locations, and third-party sites.

3. Policy

Access to all **[Company Name]** information assets shall be managed through a formal, documented process that is consistently applied and audited.

3.1 Principle of Least Privilege

All access rights shall be granted based on the principle of least privilege. Workforce members shall only be provided with the minimum level of access to data and systems necessary to perform their assigned job responsibilities. Access that is not explicitly granted is implicitly denied.

3.2 User Access Lifecycle Management

Access rights must be managed throughout the entire duration of a user's relationship with the company.

- **Provisioning:** Access for new workforce members must be requested by their direct manager through the official IT service request process. Access rights will be assigned based on predefined roles and responsibilities documented in the user's job description.
- **Modification:** When a workforce member changes roles or responsibilities within the company, their manager must submit a request to modify access rights. All previous access rights

that are no longer required for the new role must be revoked, and new access rights must be granted according to the principle of least privilege.

- **Deprovisioning:** Upon termination of employment or contract, all access to company systems, applications, and physical facilities must be revoked in a timely manner, not to exceed **[Number, e.g., 24]** hours from the official termination time. For involuntary terminations or other high-risk separation events, all logical and physical access must be revoked immediately, concurrent with the termination event whenever possible.

3.3 Access Reviews

To ensure access rights remain appropriate, formal access reviews must be conducted periodically. The designation of systems as containing ePHI or Confidential data must be formally documented in the **[Company Name]** System & Data Inventory.

- Access to systems containing ePHI or other data classified as Confidential must be reviewed by the respective system owner or manager on a quarterly basis.
- All other user access rights must be reviewed on at least an annual basis.
- The review requires a formal, documented attestation (e.g., digital sign-off via a ticket) from the designated manager or system owner. Failure to complete a required access review within **[Number, e.g., 14]** days of the deadline will result in an automatic escalation to the Security Officer and the manager's direct superior.
- The results of all access reviews, including any modifications made, must be documented and retained as evidence of compliance.

3.4 Privileged Access Management

Accounts with elevated (administrative) privileges pose a significant risk and must be subject to stricter controls.

- Administrative access shall be granted on a limited, as-needed basis. For accounts with the highest level of administrative privilege (e.g., 'root' or 'global administrator'), access should be granted on a time-bound, just-in-time (JIT) basis where technically feasible. All such access sessions must require explicit approval and be automatically logged and terminated after the approved duration.
- Workforce members with administrative privileges must use a dedicated, separate account for performing administrative tasks. Standard day-to-day activities must be performed using a

non-privileged user account.

- Multi-Factor Authentication (MFA) is mandatory for all privileged access accounts.
- All activities performed using a privileged account must be logged and monitored for suspicious behavior.

3.5 System and Network Access Controls

Logical access to systems and networks must be secured as follows:

- **Unique Identification:** Every user must be assigned a unique user ID. The use of shared or generic user accounts is strictly prohibited.
- **Authentication:** All access must be authenticated through a combination of a unique user ID and a strong password, as defined in the Password Policy (SEC-POL-002). MFA is required for all sensitive systems.
- **Session Timeouts:** Systems must be configured to automatically terminate user sessions after a defined period of inactivity, not to exceed **[Duration, e.g., 15 minutes]** for systems containing ePHI.
- **Network Segregation:** The corporate network must be segregated into logical zones (e.g., production, development, DMZ) with access controls and firewalls in place to restrict traffic between zones to only what is explicitly authorized.

3.6 Third-Party Access

Prior to granting any access, all third parties must undergo a formal security and compliance review, as defined in the Vendor Management Policy. Any third party that will access, store, or process ePHI on behalf of **[Company Name]** must have a signed Business Associate Agreement (BAA) in place before access is provisioned.

Third-party access must be:

- Limited to only the specific systems and data required for their function.
- Time-bound, with access automatically expiring upon contract termination.
- Monitored, with all activities logged and reviewed.

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Information Access Management
3.2, 3.5	HIPAA Security Rule	45 CFR § 164.312(a)(1) - Access Control
3.5	HIPAA Security Rule	45 CFR § 164.312(a)(2)(i) - Unique User Identification
All	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.2, 3.3	SOC 2 Trust Services Criteria	CC6.2 - Prior to issuing system credentials…
3.2, 3.6	SOC 2 Trust Services Criteria	CC6.3 - Authorization, modification, and removal of access…

5. Definitions

- **Least Privilege:** The security principle of restricting access rights for users to the bare minimum permissions they need to perform their work.
- **Role-Based Access Control (RBAC):** A method of restricting network access based on the roles of individual users within an enterprise.
- **Privileged Account:** A user account with elevated permissions, such as administrator, root, or system accounts.
- **Business Associate Agreement (BAA):** A written contract between a covered entity and a business associate as required by HIPAA.

6. Responsibilities

Role	Responsibility
Security Officer / Team	Own, review, and update this policy annually. Audit access controls and review compliance.

Role	Responsibility
IT Department	Implement, manage, and monitor technical access controls. Process access provisioning, modification, and deprovisioning requests.
Managers / System Owners	Request and approve access for their direct reports. Conduct periodic access reviews for their teams and systems.
All Workforce Members	Adhere to this policy, use only their assigned accounts, and report any unauthorized access or suspicious activity.

Network Acceptable Use Policy (AC-POL-002)

1. Objective

The objective of this policy is to establish the rules governing the acceptable use of **[Company Name]**'s network, internet access, and communication systems. This policy is designed to protect the integrity and availability of our information resources, safeguard sensitive data such as electronic Protected Health Information (ePHI), and ensure a secure and productive work environment.

2. Scope

This policy applies to all **[Company Name]** workforce members (including employees, contractors, and temporary staff) and any other individuals granted access to the company's network and information systems. It covers the use of all network resources, including but not limited to internet access, email, instant messaging, cloud services, and any device connected to the corporate network.

3. Policy

All use of **[Company Name]**'s network resources must be conducted in a legal, ethical, and secure manner that is consistent with the company's professional standards.

3.1 General Use and Ownership

- **Company Property:** All network infrastructure, systems, and the data created or transmitted over them are the property of **[Company Name]**.
- **No Expectation of Privacy:** Workforce members should have no expectation of privacy in their use of company network resources. To ensure compliance and protect information assets, network traffic is actively monitored for security threats and potential policy violations, in accordance with applicable laws.
- **Business Purpose:** Network resources are provided primarily for business-related activities. Limited and incidental personal use is permitted, provided it does not interfere with job performance, consume significant resources, or violate any other provision of this policy.

3.2 Security and Data Protection

Workforce members are responsible for maintaining the security of the network and protecting company data.

- **Credentials:** Workforce members must not share their account credentials or allow others to use their accounts to access the network.
- **Malicious Software:** Intentionally introducing malicious software (e.g., viruses, worms, spyware) into the network is strictly prohibited. Workforce members must exercise caution when opening email attachments or clicking on links from unknown sources. To support this, workforce members are required to complete annual security awareness training, which provides specific guidance on identifying and avoiding threats like phishing and malware.
- **Security Incidents:** Any suspected security incident, unauthorized access, or vulnerability must be reported immediately to the IT Department and the Security Officer.
- **Data Handling:** The transmission of ePHI or other data classified as Confidential over the network must be done using company-approved, encrypted methods.

3.3 Prohibited Activities

The following activities are strictly prohibited when using **[Company Name]**'s network resources:

- **Illegal or Unethical Activities:** Engaging in any activity that is illegal under local, state, or federal law, including but not limited to harassment, copyright infringement, or fraudulent activities.
- **Circumventing Security:** Attempting to bypass or disable any security controls, such as firewalls, content filters, or monitoring software.
- **Unauthorized Access:** Attempting to access systems, data, or accounts for which the user does not have explicit authorization.
- **Disruptive Behavior:** Engaging in any activity that could disrupt network services or degrade performance for other users, such as initiating a denial-of-service attack or sending spam.
- **Unauthorized Data Transfer:** Using unapproved peer-to-peer file-sharing services or transferring company data to unauthorized personal cloud storage accounts.
- **Inappropriate Content:** Accessing, downloading, or distributing content that is obscene, defamatory, harassing, or otherwise violates **[Company Name]**'s professional conduct policies.

Compliance with these prohibitions is enforced through a combination of administrative oversight and technical controls, including but not limited to, web content filtering, intrusion detection systems, and data loss prevention (DLP) tools.

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Frame	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(1)(i) - Security Management Process
3.2, 3.3	HIPAA Security Rule	45 CFR § 164.308(a)(5)(ii)(B) - Protection from Malicious Software
3.2	HIPAA Security Rule	45 CFR § 164.308(a)(6)(ii) - Response and Reporting
3.3	SOC 2 Trust Services Criteria	CC6.7 - The entity restricts the transmission, movement, and removal of information…
3.3	SOC 2 Trust Services Criteria	CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software.

5. Definitions

- **Network Resources:** All company-owned or managed hardware and software that provide network connectivity and services, including routers, switches, firewalls, servers, wireless access points, internet connections, and communication platforms.
- **Incidental Personal Use:** Infrequent and brief personal use of network resources that does not incur additional cost to the company, interfere with work duties, or violate this policy. Examples of use that is not considered incidental include streaming high-bandwidth media for personal entertainment, engaging in online gaming, or activities related to operating a personal business.

6. Responsibilities

Role	Responsibility
Security Officer / Team	Own, review, and update this policy annually. Oversee the monitoring of network activity for security and compliance purposes.
IT Department	Implement and maintain the technical controls necessary to enforce this policy, such as firewalls and content filters. Investigate and respond to reported security incidents.
Managers	Ensure their direct reports understand and adhere to this policy. Address minor infractions in consultation with the IT and HR departments.
All Workforce Members	Read, understand, and comply with this policy. Use company network resources responsibly and report any violations or security concerns.

Remote Work Policy (AC-POL-003)

1. Objective

The objective of this policy is to establish the requirements for securely accessing **[Company Name]**'s information assets from locations outside of corporate offices. Because we handle sensitive health information, these security measures are not just company rules—they are essential for protecting patients, complying with laws like HIPAA, and maintaining the trust of our clients. This policy is designed to enable workforce productivity while ensuring the confidentiality, integrity, and availability of all data, including electronic Protected Health Information (ePHI), regardless of where work is performed.

2. Scope

This policy applies to all **[Company Name]** workforce members (including employees, contractors, and temporary staff) who work remotely, either on a full-time, part-time, or occasional basis. It covers any and all locations outside of a designated corporate office, including home offices, co-working spaces, and travel locations. This policy governs the use of both company-provided and personally-owned equipment used to access company resources.

3. Policy

All remote work must be conducted in a manner that actively protects company information and systems from unauthorized access, disclosure, or damage.

3.1 Secure Network Connectivity

Workforce members are responsible for ensuring they use a secure network connection for all remote work.

- **VPN Mandate:** All access to internal company systems, applications, and data repositories must be established through the company-approved Virtual Private Network (VPN). The VPN client must be active for the entire duration of the remote work session.
- **Prohibition of Unsecured Networks:** The use of public or untrusted Wi-Fi networks (e.g., in cafes, airports, hotels) for accessing or transmitting ePHI or other data classified as Confidential is strictly prohibited. If such a network must be used for general tasks, the VPN is mandatory.

- **Home Network Security:** Workforce members are required to secure their home wireless networks with strong encryption (WPA2 or better) and a complex, unique password. As part of their annual security attestation, all workforce members must formally attest that their primary remote work network is secured in accordance with this policy.

3.2 Device Security Requirements

Any device used to access company resources remotely, whether company-provided or personally-owned, must meet the following minimum security standards. Compliance with these requirements is enforced through the company's security software (such as Mobile Device Management (MDM) or Endpoint Detection and Response (EDR) solutions). Devices that do not meet these minimum standards may be blocked from accessing corporate resources.

- **Encryption:** Full-disk encryption must be enabled.
- **Access Control:** The device must be protected by a strong password or biometric control, compliant with the Password Policy (SEC-POL-002), and must be configured to automatically lock after **[Number, e.g., 15]** minutes of inactivity.
- **Malware Protection:** Company-approved anti-malware software must be installed, active, and configured to receive automatic updates.
- **Patch Management:** The operating system and all applications must be kept up-to-date with the latest security patches.

3.3 Data Handling and Physical Security

Workforce members must take precautions to protect the physical and digital privacy of information when working remotely.

- **ePHI Storage:** Storing ePHI or other Confidential data on the local hard drive of a personally-owned device is strictly prohibited. All sensitive data must be accessed and stored exclusively on company-managed cloud platforms or network shares.
- **Physical Privacy:** Workforce members must take reasonable measures to prevent unauthorized viewing of their screens in public or shared spaces. This includes the use of privacy screens where appropriate and positioning screens away from public view.
- **Verbal Privacy:** Confidential or sensitive information must not be discussed in public areas where conversations can be overheard.
- **Secure Document Handling:** Any printed documents containing sensitive information must

be handled securely and physically destroyed (e.g., via shredding) when no longer needed. Documents must not be left unattended in unsecured locations.

- **Asset Protection:** Workforce members are responsible for the physical security of company-provided equipment. Devices must never be left unattended in vehicles or unsecured public locations. Any loss or theft of a device used for company business must be reported immediately to the IT Department and the Security Officer, and in no case later than **[Number, e.g., 24]** hours after discovery.
- **Data Removal After Employment:** Upon termination, workforce members must cooperate with the IT Department to ensure the secure removal of all company data, applications, and access credentials from any personally-owned devices used for work.

3.4 Use of Personal Equipment (BYOD)

The use of personally-owned devices to access company resources is a privilege and is contingent upon adherence to specific security requirements. As a condition of using a personal device for work, workforce members must provide formal consent to the installation of required security software and acknowledge **[Company Name]**'s right to remotely wipe corporate data (a process that targets only company information and applications, not personal data like photos, texts, or contacts). All personal devices must be formally registered with the IT Department and may be required to have company-managed security software installed before access is granted, as further defined in the Bring Your Own Device (BYOD) Policy.

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Frame	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(B) - Authorization and/or supervision
3.1, 3.2	HIPAA Security Rule	45 CFR § 164.312(e)(1) - Transmission Security
3.2, 3.3	HIPAA Security Rule	45 CFR § 164.310(d)(1) - Device and Media Controls

Policy Section	Standard/Frame	Control Reference
All	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.2, 3.3	SOC 2 Trust Services Criteria	CC6.6 - The entity implements logical access security measures for assets…
3.3	SOC 2 Trust Services Criteria	CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software.

5. Definitions

- **Remote Work:** Any work performed for **[Company Name]** from a location that is not a designated corporate office.
- **Virtual Private Network (VPN):** A secure, encrypted connection over a public network to a private network.
- **Company-Provided Equipment:** Laptops, mobile devices, and any other hardware owned by **[Company Name]** and issued to a workforce member.
- **Mobile Device Management (MDM):** Software used by the IT Department to manage and secure mobile devices like phones and tablets.
- **Endpoint Detection and Response (EDR):** Security software that monitors devices like laptops for suspicious activity and potential threats.

6. Responsibilities

Role	Responsibility
Security Officer / Team	Own, review, and update this policy annually. Monitor remote access logs for compliance and suspicious activity.

Role	Responsibility
IT Department	Maintain and manage the VPN and other remote access technologies. Assist workforce members with the secure configuration of their devices.
Managers	Ensure their direct reports are aware of and understand this policy. Report any non-compliance or remote-work-related security concerns to the IT Department or Security Officer.
All Workforce Members	Adhere to this policy at all times when working remotely. Ensure the security of their remote work environment and company assets. Immediately report any security incidents or lost/stolen devices.

Acceptable Use Policy Violation Investigation Procedure (AC-PROC-001)

1. Purpose

To define the process for investigating, documenting, and responding to reported violations of the network acceptable use policy.

2. Scope

This procedure applies to all workforce members and all reported or detected violations of the `Network Acceptable Use Policy (AC-POL-002)`.

3. Overview

This procedure outlines the steps for responding to potential violations of the acceptable use policy, from initial report and investigation through to documentation and sanctioning, ensuring a consistent and fair process.

4. Procedure

Provide the detailed, step-by-step instructions for carrying out the procedure. The table format is standard.

Step	Who	What
1	Reporter (User or Automated System)	A potential violation is reported by a user or detected by an automated system.
2	IT Department & Security Officer	Investigate the report to validate the violation and assess its impact.
3	IT Department or Security Officer	The employee's manager is notified.
4	Manager & Human Resources	In consultation with HR, a sanction is determined consistent with the Sanction Policy.
5	Security Officer/IT Department	The outcome is formally documented.

Note: If the security team determines that the violation is critical, an incident post-mortem may be initiated to analyze the incident in detail.

5. Standards Compliance

This section maps the procedure steps to specific controls from relevant information security standards.

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2	CC6.8
1-5	HIPAA	45 CFR § 164.308(a)(5)(ii)(B)

6. Artifact(s)

A completed policy violation investigation report.

7. Definitions

N/A

8. Responsibilities

Clearly assign responsibility for various aspects of the procedure.

Role	Responsibility
Reporter	Any workforce member responsible for reporting suspected policy violations.
IT Department	Investigates reported violations, validates their authenticity, and assesses technical impact.
Security Officer	Oversees the investigation process and ensures compliance with security policies.
Managers	Notified of violations by their direct reports and participate in determining appropriate sanctions.
Human Resources	Consulted on sanctions to ensure consistency with company policy and legal requirements.

Bring Your Own Device (BYOD) Onboarding Procedure (AC-PROC-002)

1. Purpose

To establish the process for registering and securing a personally-owned device (BYOD) for access to company resources.

2. Scope

This procedure applies to all workforce members who wish to use a personal device to access company information or systems.

3. Overview

This procedure details the steps for a workforce member to register a personal device for company use, including obtaining consent, installing required security software, and ensuring the device meets security standards before access is granted.

4. Procedure

Step	Who	What
1	Workforce Member	Requests to use a personal device for work purposes.
2	Workforce Member	Provides formal consent to the installation of security software and acknowledges the company’s right to remotely wipe corporate data.
3	Workforce Member	The device is formally registered with the IT Department.
4	IT Department	Installs and verifies required security software (MDM/EDR) and confirms the device meets minimum security standards (encryption, access control, malware protection).
5	IT Department	Access is granted to company resources.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2	CC6.1, CC6.6
1-5	HIPAA	45 CFR § 164.310(d)(1)

6. Artifact(s)

A completed and signed BYOD Registration and Consent form.

7. Definitions

- **BYOD (Bring Your Own Device):** A policy that allows employees to use their personal devices for work-related purposes.
- **MDM (Mobile Device Management):** Software that allows an organization to manage and secure employees' mobile devices.
- **EDR (Endpoint Detection and Response):** A solution that monitors endpoint and network events and records the information in a central database for analysis, detection, investigation, reporting, and alerting.

8. Responsibilities

Role	Responsibility
Workforce Member	Requests to use a personal device, provides consent, and ensures their device is available for security setup.
IT Department	Manages the device registration process, installs and verifies security software, and grants access.
Managers	Ensure their team members follow this procedure when using personal devices for work.

User Access Review Procedure (AC-PROC-003)

1. Purpose

To define the process for conducting periodic reviews of user access rights to ensure adherence to the principle of least privilege.

2. Scope

This procedure applies to all user accounts with access to company information systems and the managers or system owners responsible for those accounts.

3. Overview

This procedure describes the quarterly and annual process for reviewing user access to sensitive systems. It ensures that access rights are regularly verified and that any unnecessary permissions are revoked in a timely manner, thereby minimizing security risks.

4. Procedure

Step	Who	What
1	IT/Security Team	Generates user access reports for specific systems based on the quarterly and annual review schedule.
2	IT/Security Team	Sends these reports to the designated system owners or employee managers.
3	System Owner/Manager	Reviews each user's access and attests whether it is still appropriate and required for their job function.
4	System Owner/Manager	Returns the signed-off review form to the IT/Security team.
5	System Owner/Manager	Returns the signed-off review form to the IT/Security team.
6	Security Team	Reviews administrative access rights and attests to their necessity.
7	IT/Security Team	Stores all completed reviews as an audit record.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2	CC6.1
1-6	HIPAA	45 CFR § 164.308(a)(4) (Information Access Management)

6. Artifact(s)

A completed and signed User Access Review attestation form or ticket.

7. Definitions

- **Principle of Least Privilege:** The concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, authorized activities.

8. Responsibilities

Role	Responsibility
IT/Security Team	Facilitates the access review process, generates reports, tracks completion, and stores audit records.
System Owners/Managers	Perform the detailed review of access rights for their systems or direct reports and attest to their necessity.
All Workforce Members	Comply with the process and provide any necessary information to their managers.

Access Control Management Procedure (AC-PROC-004)

1. Purpose

To define the process for requesting, approving, implementing, modifying, and revoking user access to company information systems, ensuring the principle of least privilege is enforced.

2. Scope

This procedure applies to all workforce members, managers, system owners, and IT personnel involved in the lifecycle of user access to all company information systems.

3. Overview

This procedure covers the end-to-end management of user access, from initial provisioning and modification to final revocation upon termination. It ensures that all access changes are properly authorized, implemented, and documented to maintain a secure environment.

4. Procedure

4.1 Access Provisioning/Modification

Step	Who	What
1	Requestor (User or Manager)	Submits an access request ticket specifying the system and required permissions.
2	Manager	Approves the request in the ticket, verifying the business need.
3	System or Information Owner	Provides final approval, ensuring the request aligns with data classification and security policies.
4	IT Department / System Administrator	Provisions the approved access.

4.2 Access Revocation (Termination)

Step	Who	What
1	Human Resources	Notifies the IT Department of a workforce member's termination.
2	IT Department	Immediately revokes all logical and physical access for the terminated workforce member.
3	IT Department	Confirms completion of all revocation tasks and updates relevant records.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
4.1, 4.2	SOC 2	CC6.1, CC6.3
4.1, 4.2	HIPAA	45 CFR § 164.308(a)(3)(ii)(C), 45 CFR § 164.308(a)(4)

6. Artifact(s)

A completed access request ticket showing the full request, approval chain, and implementation details. For terminations, a record of the HR notification and IT's confirmation of access revocation.

7. Definitions

- **System Owner:** The individual or group responsible for the overall procurement, development, integration, modification, operation, and maintenance of an information system.
- **Information Owner:** The individual with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

8. Responsibilities

Role	Responsibility
Requestor	Initiates access requests with a clear justification for the required permissions.
Manager	Provides initial approval for access requests, confirming the business need for their direct reports.
System/Information Owner	Provides final approval for access, ensuring it aligns with security and data handling policies.
IT Department/System Administrator	Implements the approved access changes and is responsible for the timely revocation of access upon notification.
Human Resources	Manages the employee lifecycle and provides timely notification of terminations to the IT Department.

Secure Software Development Policy (ENG-POL-001)

1. Objective

The objective of this policy is to establish comprehensive security requirements for the design, development, testing, deployment, and maintenance of software applications and systems at **[Company Name]**. This policy ensures that security controls are integrated throughout the Software Development Lifecycle (SDLC) to protect the confidentiality, integrity, and availability of information systems and electronic Protected Health Information (ePHI), while maintaining compliance with HIPAA, HITECH, and SOC 2 requirements and implementing secure coding practices that minimize vulnerabilities and security risks.

2. Scope

This policy applies to all **[Company Name]** workforce members involved in software development activities, including developers, architects, testers, DevOps engineers, product managers, and project managers. It encompasses all software development projects including new applications, system modifications, third-party integrations, mobile applications, web applications, APIs, and infrastructure-as-code. This policy covers all development environments (development, testing, staging, production), development methodologies (Agile, DevOps, Waterfall), and deployment models (on-premises, cloud, hybrid). It applies to both internally developed software and customizations of third-party applications.

3. Policy

[Company Name] shall implement security controls throughout the entire software development lifecycle to ensure that applications and systems are designed, built, and maintained with appropriate security safeguards.

3.1 Secure Development Lifecycle Framework

All software development projects shall follow a structured secure development lifecycle that integrates security activities into each phase of development.

3.1.1 Security Development Lifecycle Phases

Requirements and Design Phase:

- Security requirements shall be identified and documented during the requirements gathering process

- Threat modeling shall be conducted for all applications that process, store, or transmit sensitive data
- Security architecture reviews shall be performed for new applications and significant modifications
- Privacy impact assessments shall be completed for applications handling ePHI or personal information
- Secure design principles shall be applied including defense in depth, least privilege, and fail-secure defaults

Development Phase:

- Secure coding standards shall be followed for all programming languages and frameworks used
- Security-focused code reviews shall be conducted for all code changes
- Static Application Security Testing (SAST) tools shall be integrated into the development process
- Dependency scanning shall be performed to identify vulnerable third-party components
- Security unit tests shall be developed and executed as part of the testing framework

Testing Phase:

- Dynamic Application Security Testing (DAST) shall be performed on all applications before production deployment
- Interactive Application Security Testing (IAST) shall be implemented where technically feasible
- Penetration testing shall be conducted for all applications handling ePHI or Confidential data
- Security test cases shall validate proper implementation of security controls
- Vulnerability assessments shall be performed on the complete application stack

Deployment Phase:

- Security configuration reviews shall be conducted before production deployment
- Infrastructure security scanning shall validate secure deployment configurations
- Secrets management processes shall ensure secure handling of credentials and keys
- Production environment hardening shall be verified against security baselines
- Security monitoring and logging shall be implemented for all production applications

Maintenance Phase:

- Regular security assessments shall be conducted on production applications
- Security patches and updates shall be applied according to established timelines
- Continuous monitoring shall detect and alert on security vulnerabilities
- End-of-life procedures shall ensure secure decommissioning of applications and data

3.1.2 Security Gates and Approval Process

Security gates shall be implemented at key phases to ensure security requirements are met before proceeding:

- **Design Gate:** Security architecture review and threat model approval required
- **Code Gate:** Static analysis results and code review approval required
- **Test Gate:** Dynamic testing results and penetration test approval required
- **Deploy Gate:** Security configuration review and vulnerability scan approval required
- **Production Gate:** Security monitoring implementation and incident response procedures verified

3.2 Secure Coding Standards

All software development shall adhere to established secure coding practices to prevent common vulnerabilities and security weaknesses.

3.2.1 General Secure Coding Principles

Input Validation and Sanitization:

- All user inputs shall be validated, sanitized, and encoded before processing
- Input validation shall be performed on both client-side and server-side
- Parameterized queries or prepared statements shall be used for all database interactions
- File upload functionality shall include content type validation and malware scanning
- Data length limits and format validation shall be enforced for all input fields

Authentication and Session Management:

- Strong authentication mechanisms shall be implemented including multi-factor authentication
- Session tokens shall be cryptographically secure and include appropriate expiration timeouts
- Password storage shall use approved cryptographic hash functions with salt
- Account lockout mechanisms shall prevent brute force attacks
- Session management shall include secure token generation, validation, and termination

Authorization and Access Control:

- Role-based access control (RBAC) shall be implemented for all application functions
- Principle of least privilege shall be enforced for all user and system accounts
- Authorization checks shall be performed for every request and transaction
- Direct object references shall be validated to prevent unauthorized access
- Administrative functions shall require elevated authentication and approval

Error Handling and Logging:

- Error messages shall not reveal sensitive information or system details
- Comprehensive logging shall capture security-relevant events for audit purposes
- Log data shall be protected against unauthorized access and tampering
- Failed authentication attempts and suspicious activities shall be logged and monitored
- Debug information and stack traces shall not be exposed in production environments

3.2.2 Language-Specific Secure Coding Requirements

Web Application Development:

- Cross-Site Scripting (XSS) prevention through output encoding and Content Security Policy (CSP)
- Cross-Site Request Forgery (CSRF) protection using tokens and SameSite cookie attributes
- SQL injection prevention through parameterized queries and input validation
- Secure HTTP headers implementation (HSTS, X-Frame-Options, X-Content-Type-Options)
- HTTPS enforcement for all communications with proper certificate validation

Mobile Application Development:

- Platform-specific security features utilization (iOS Keychain, Android Keystore)
- Certificate pinning for network communications
- Local data encryption using platform encryption APIs
- Runtime Application Self-Protection (RASP) implementation
- Anti-tampering and reverse engineering protection

API Development:

- OAuth 2.0 or equivalent authentication frameworks for API access
- Rate limiting and throttling to prevent abuse
- API versioning and deprecation procedures with security considerations
- Input validation and output filtering for all API endpoints

- Comprehensive API documentation including security requirements

3.3 Code Review and Static Analysis

All code shall undergo thorough review processes to identify and remediate security vulnerabilities before deployment.

3.3.1 Manual Code Review Requirements

Peer Review Process:

- All code changes shall be reviewed and formally approved by at least one qualified peer before being merged into the main branch. This approval must be documented within the version control system (e.g., via a pull request approval).
- Security-focused code reviews shall be conducted by team members trained in secure coding
- Code reviews shall use standardized checklists covering common security vulnerabilities
- Review comments and resolutions shall be documented and tracked
- Critical or high-risk code changes shall require review by senior developers or security team
- Code review tools powered by AI or static analysis shall be used to assist in identifying potential security issues

Security Review Criteria:

- Authentication and authorization implementation
- Input validation and output encoding
- Error handling and information disclosure
- Cryptographic implementation and key management
- Third-party library usage and dependency management
- Configuration management and secrets handling

3.3.2 Automated Static Analysis

Static Analysis Tools:

- Static Application Security Testing (SAST) tools shall be integrated into the development pipeline
- Code analysis shall be performed automatically on all code commits
- Build processes shall fail if critical or high-severity vulnerabilities are detected
- False positive management processes shall ensure accurate vulnerability identification
- Tool configuration shall be maintained to reflect current security standards and threat landscape

Vulnerability Management:

- All identified vulnerabilities shall be tracked and prioritized based on risk.
- Remediation of vulnerabilities must adhere to the following timelines:
  - Critical vulnerabilities: within **[Timeframe, e.g., 7 days]**
  - High vulnerabilities: within **[Timeframe, e.g., 30 days]**
  - Medium vulnerabilities: within **[Timeframe, e.g., 90 days]**
- Any vulnerability that cannot be remediated within the defined timeframe requires a formal risk acceptance document to be signed by the Information Owner and the Security Officer.
- Vulnerability remediation shall be verified through re-testing.

3.4 Dynamic Testing and Security Assessment

Comprehensive dynamic testing shall validate the security of applications in runtime environments.

3.4.1 Dynamic Application Security Testing (DAST)

Automated Security Scanning:

- DAST tools shall be integrated into the CI/CD pipeline for continuous security testing
- Automated scans shall be performed on all web applications and APIs
- Scanning shall cover common vulnerabilities including OWASP Top 10
- Scan results shall be automatically triaged and assigned for remediation
- Baseline scans shall be established to track security improvements over time

Interactive Application Security Testing (IAST):

- IAST tools shall be deployed in testing environments where technically feasible
- Real-time vulnerability detection during functional testing
- Integration with development tools for immediate feedback on security issues
- Coverage analysis to ensure comprehensive security testing
- Correlation with static analysis results for complete vulnerability assessment

3.4.2 Penetration Testing Requirements

Internal Penetration Testing:

- Applications handling ePHI or Confidential data shall undergo annual penetration testing
- Testing shall be performed by qualified internal security team members or approved third parties

- Testing scope shall include application logic, authentication, authorization, and data protection
- Network-level testing shall validate infrastructure security controls
- Social engineering testing shall assess human factors in application security

External Penetration Testing:

- Critical applications shall undergo annual third-party penetration testing.
- Testing shall be performed by certified security professionals (CISSP, CEH, OSCP).
- Testing methodology shall follow industry standards (OWASP, NIST, PTES).
- A formal remediation plan shall be created for all identified vulnerabilities, with owners and timelines assigned for each finding. This plan shall be tracked to completion by the Security Team.
- Executive summary and technical reports shall be provided to stakeholders.

3.5 Third-Party Component Management

Security assessment and management of third-party libraries, frameworks, and components shall be implemented throughout the development process.

3.5.1 Dependency Scanning and Management

Automated Dependency Scanning:

- Software Composition Analysis (SCA) tools shall scan all third-party dependencies
- Vulnerability databases shall be continuously updated to identify newly discovered issues
- Build processes shall fail if critical vulnerabilities are detected in dependencies
- License compliance scanning shall ensure proper usage of open source components
- Dependency inventory shall be maintained for all applications and systems

Vendor Component Assessment:

- Commercial third-party components shall undergo security assessment before adoption
- Vendor security practices and incident response capabilities shall be evaluated
- Source code review requirements for critical commercial components
- Escrow agreements for critical vendor components to ensure continued access
- End-of-life planning for vendor components approaching obsolescence

3.5.2 Open Source Security Management

Open Source Governance:

- Approved list of open source components and frameworks shall be maintained
- Security review process for introducing new open source dependencies
- Regular assessment of open source component security status
- Community support and maintenance status evaluation
- Legal review of open source licenses and compliance requirements

Vulnerability Response:

- Immediate assessment of newly disclosed vulnerabilities in used components
- Emergency patching procedures for critical vulnerabilities
- Alternative component identification for unmaintained or insecure libraries
- Coordinated disclosure participation for vulnerabilities discovered in open source projects

3.6 DevOps and CI/CD Security

Security controls shall be integrated into DevOps practices and continuous integration/continuous deployment (CI/CD) pipelines.

3.6.1 Secure CI/CD Pipeline

Pipeline Security Controls:

- All CI/CD pipeline components shall be secured and regularly updated
- Access to pipeline systems shall be restricted and monitored
- Pipeline configurations shall be version controlled and reviewed
- Build environments shall be isolated and regularly refreshed
- Artifact integrity shall be verified through cryptographic signing

Infrastructure as Code (IaC) Security:

- All infrastructure definitions shall be version controlled and reviewed
- Security scanning of infrastructure templates and configurations
- Automated compliance checking against security baselines
- Immutable infrastructure practices to prevent configuration drift
- Secret management for infrastructure credentials and certificates

3.6.2 Secrets Management

Credential Protection:

- Application secrets, API keys, and credentials shall never be stored in source code
- Dedicated secrets management systems shall be used for all sensitive credentials

- Secrets shall be encrypted at rest and in transit
- Regular rotation of secrets and credentials
- Audit logging for all secrets access and usage

Environment Separation:

- Clear separation between development, testing, staging, and production environments
- Different credentials and access controls for each environment
- Production data shall not be used in non-production environments
- Data masking and anonymization for testing with realistic data sets
- Network segmentation between development and production environments

3.7 Security Training and Awareness

All development team members shall receive comprehensive security training appropriate to their roles and responsibilities.

3.7.1 Developer Security Training

Initial Training Requirements:

- Secure coding training for all new developers within **[Timeframe, e.g., 30 days]** of hire
- Language and framework-specific security training
- OWASP Top 10 awareness and prevention techniques
- Threat modeling and security design principles
- Security tool usage and integration training

Ongoing Training and Awareness:

- Annual security training updates covering emerging threats and vulnerabilities
- Specialized training for developers working on critical or high-risk applications
- Security conference attendance and knowledge sharing
- Internal security awareness presentations and workshops
- Gamification and hands-on security challenges

3.7.2 Security Champions Program

Security Champion Selection:

- Designated security champions within each development team
- Additional security training and certification for champions
- Regular security champion meetings and knowledge sharing

- Champion responsibility for promoting security within their teams
- Recognition and incentives for effective security championship

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(1) - Security Management Process
3.1, 3.2	HIPAA Security Rule	45 CFR § 164.312(a)(1) - Access Control
3.2.1	HIPAA Security Rule	45 CFR § 164.312(a)(2)(i) - Unique User Identification
3.2.1	HIPAA Security Rule	45 CFR § 164.312(e)(1) - Transmission Security
3.4	HIPAA Security Rule	45 CFR § 164.308(a)(8) - Evaluation
All	SOC 2 Trust Services Criteria	CC8.1 - System Development
3.3, 3.4	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
3.6	SOC 2 Trust Services Criteria	CC6.8 - System Security
All	OWASP SAMM	Software Assurance Maturity Model
3.2	OWASP Top 10	Web Application Security Risks
All	NIST Cybersecurity Framework	PR.IP-1 - Baseline Security
3.5	NIST SP 800-161	Supply Chain Risk Management

5. Definitions

Continuous Integration/Continuous Deployment (CI/CD): Development practice that enables frequent integration and automated deployment of code changes.

Dynamic Application Security Testing (DAST): Security testing method that analyzes applications in their running state to identify vulnerabilities.

Infrastructure as Code (IaC): Practice of managing and provisioning infrastructure through machine-readable definition files.

Interactive Application Security Testing (IAST): Security testing that combines static and dynamic analysis to provide real-time vulnerability detection.

Penetration Testing: Simulated cyber attack against applications or systems to evaluate security defenses.

Software Composition Analysis (SCA): Automated process of identifying open source and third-party components and their associated security vulnerabilities.

Static Application Security Testing (SAST): Security testing method that analyzes source code to identify potential vulnerabilities.

Threat Modeling: Structured approach to identifying, analyzing, and mitigating potential security threats to applications and systems.

6. Responsibilities

Role	Responsibility
Security Officer	Develop secure development policies, oversee security testing programs, coordinate security training, and ensure compliance with security standards.
Development Team Lead	Ensure team compliance with secure development practices, coordinate security reviews, manage security training, and implement security tools and processes.

Role	Responsibility
Software Developers	Follow secure coding standards, participate in code reviews, use security tools, remediate identified vulnerabilities, and complete required security training.
Security Engineers	Perform security assessments, conduct penetration testing, review security architecture, provide security guidance, and maintain security tools.
DevOps Engineers	Implement secure CI/CD pipelines, manage secrets and credentials, maintain security tools integration, and ensure infrastructure security.
Quality Assurance Team	Execute security test cases, validate security controls, coordinate dynamic testing, and verify vulnerability remediation.
Product Managers	Define security requirements, prioritize security features, coordinate threat modeling, and ensure security considerations in product decisions.
Architecture Team	Design secure system architectures, conduct security design reviews, establish security patterns, and provide security guidance to development teams.
All Workforce Members	Report security vulnerabilities and concerns, follow established security procedures, complete required training, and support security initiatives.

Change Control Policy (ENG-POL-002)

1. Objective

The objective of this policy is to establish a formal process for managing all changes to **[Company Name]**'s production systems, applications, and infrastructure. This policy ensures that all modifications are properly authorized, tested, documented, and reviewed to maintain system stability, security, and integrity, thereby protecting sensitive data, including electronic Protected Health Information (ePHI).

2. Scope

This policy applies to all workforce members involved in the development, testing, approval, and deployment of changes to any production environment. This includes all applications, source code, infrastructure-as-code configurations, and databases that support **[Company Name]**'s services.

3. Policy

All changes to the production environment must adhere to a structured and auditable lifecycle, from initiation to deployment and post-implementation review. GitHub is the designated system of record for tracking all code and configuration changes.

3.1 Standard Change Process

All non-emergency changes must follow this standard process:

- **Initiation:** Every change must begin with a ticket in the company's issue tracking system, which details the business justification and technical requirements.
- **Development:** All code and configuration changes must be developed in a separate feature branch within the designated GitHub repository.
- **Peer Code Review:** Before a change can be promoted for testing, it must be submitted as a pull request in GitHub and receive a formal, documented approval from at least one other qualified engineer who was not an author of the change. A qualified reviewer is defined as an engineer with equivalent or greater seniority or subject-matter expertise. The review must assess code quality, functionality, and adherence to secure coding standards.
- **Security Review:** All pull request templates must include a mandatory security checklist. If the developer indicates the change touches sensitive data, authentication, authorization, en-

cryption, or ePHI, a security review is automatically required and must be completed by the Security Team before merging.

- **Testing:** All changes must pass a full suite of automated tests. Evidence of successful test runs (e.g., a link to the CI/CD build results) must be included in the pull request. Additionally, the Quality Assurance (QA) team must conduct manual testing where applicable and provide formal sign-off within the pull request, confirming the change meets requirements and does not introduce regressions.

- **Deployment Approval:** Final approval to merge the change into the production release branch must be granted by authorized personnel (e.g., Engineering Lead or Manager) within the GitHub pull request. This approval signifies that the approver has verified that all required steps, including peer review, security review, and QA sign-off, have been successfully completed and documented. All approved production release branches must be tagged to ensure traceability and that the exact code deployed to production can be identified.

3.2 Emergency Changes

An emergency change is defined as a modification required to resolve a critical production outage, a severe service degradation, or to patch a critical security vulnerability.

- **Authorization:** An emergency change requires documented approval from at least one authorized Engineering Lead and one member of the Security Team.

- **Expedited Review:** Peer code review and security review are still mandatory but may be expedited. The focus is on validating the fix and assessing any immediate risks.

- **Post-Mortem:** All emergency changes must be followed by a formal post-mortem review within **[Number, e.g., 3]** business days to analyze the root cause and identify opportunities for process improvement. The standard change documentation, including linking the pull request to a ticket, must be completed retroactively.

- **Oversight:** A log of all emergency changes will be maintained and reviewed on a quarterly basis by Engineering Management to identify trends and ensure the emergency process is not being used to bypass standard change controls.

3.3 Data-Only Changes

Data-only changes, such as manual database updates that are not part of a standard code release, must be treated with extreme caution.

- **Formal Request:** All data-only changes require a formal request ticket that includes the script to be run, the business justification, the expected impact, and a detailed rollback plan.
- **Approval:** The request must be approved by the data or system owner. If the change affects ePHI or other Confidential data, approval from the Security Officer is also required.
- **Execution:** Changes must be executed as peer-reviewed scripts by authorized personnel with privileged database access (e.g., a Database Administrator). The execution of the approved script, including the system-generated output (e.g., number of rows affected), must be captured and appended to the original request ticket upon completion. Direct production database access for developers is prohibited.

3.4 Change Documentation and Tracking

- **System of Record:** GitHub pull requests serve as the auditable record for all code and configuration changes.
- **Traceability:** Every pull request must be linked to its corresponding issue tracking ticket. The pull request description must summarize the change, the testing performed, and the outcome of all required reviews. Approvals must be captured via the native review and approval features within GitHub.
- **Technical Enforcement:** The `main` and any `production` or `release` branches in all repositories within the scope of this policy must be technically protected to prevent direct commits. All changes must be enforced through the pull request workflow.
- **Pull Request Template:** All pull requests must use a standardized template that includes sections for the change description, testing performed, security checklist, and links to related tickets. This template must be enforced via GitHub repository settings.

3.5 Change Notifications

- **Internal Notification:** The engineering team must notify relevant internal stakeholders (e.g., Customer Support, Operations) of all upcoming production deployments via designated communication channels (e.g., Slack, email).
- **External Notification:** For changes that will have a noticeable impact on customers or partners, the Product Management team is responsible for providing advance notification with sufficient lead time.

3.6 Branch Protection

To enforce the change control process described in this policy, all `main`, `production`, and `release` branches in repositories within the scope of this policy must have GitHub branch protection rules configured. At a minimum, these rules must be enabled to:

- **Require a pull request before merging:** Direct pushes to protected branches must be disabled. All changes must be made via a pull request.
- **Require approvals:** Enforce the peer review and deployment approval requirements outlined in section 3.1.
- **Require status checks to pass before merging:** Enforce that all required CI/CD checks (e.g., automated tests, security scans) pass successfully before a change can be merged.

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framewor	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(C) - Authorization and/or supervision
3.1, 3.2	HIPAA Security Rule	45 CFR § 164.312(c)(1) - Integrity
3.4	HIPAA Security Rule	45 CFR § 164.312(b) - Audit Controls
All	SOC 2 Trust Services Criteria	CC8.1 - The entity designs, develops, and implements controls over change management.

5. Definitions

- **Change:** Any modification to production code, system configurations, or database schemas.
- **Production Environment:** The live environment that serves **[Company Name]**'s customers and processes real data.
- **Pull Request:** A feature in GitHub that facilitates the peer review and merging of code from one branch into another.

6. Responsibilities

Role	Responsibility
Engineering Team	Develop, test, and document changes in accordance with this policy. Conduct peer code reviews.
Security Team	Review changes for security implications and approve or reject them based on risk.
Quality Assurance (QA) Team	Verify that changes meet functional requirements and do not introduce defects. Provide formal testing sign-off.
Engineering Management	Provide final approval for changes to be deployed to production. Authorize emergency changes.
System / Data Owners	Provide approval for changes affecting their specific systems or data domains, particularly for Data-Only Changes.

Infrastructure Security Policy (ENG-POL-003)

1. Objective

The objective of this policy is to establish comprehensive security requirements for the design, implementation, operation, and maintenance of **[Company Name]**'s cloud-based IT infrastructure. This policy ensures that all infrastructure components including cloud services, networks, servers, databases, and supporting systems are configured and managed with appropriate security controls to protect the confidentiality, integrity, and availability of information systems and electronic Protected Health Information (ePHI). This policy addresses cloud-native security, infrastructure-as-code, container security, and hybrid cloud environments while maintaining compliance with HIPAA, HITECH, and SOC 2 requirements.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, and third parties involved in the design, deployment, configuration, or management of IT infrastructure. It encompasses all infrastructure components including cloud platforms (AWS, Azure, GCP), virtual machines, containers, serverless functions, databases, networks, storage systems, backup infrastructure, monitoring systems, and security tools. This policy covers all environments (production, staging, development, testing) and deployment models (public cloud, private cloud, hybrid cloud, multi-cloud). It applies to both infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) implementations, as well as infrastructure-as-code (IaC) and configuration management practices.

3. Policy

[Company Name] shall implement defense-in-depth security controls across all infrastructure layers to ensure comprehensive protection against threats and compliance with regulatory requirements.

3.1 Cloud Infrastructure Security Framework

A comprehensive security framework shall be implemented across all cloud infrastructure components to ensure consistent security posture and compliance.

3.1.1 Cloud Security Architecture

Multi-Layered Security Design:

- Network security controls including Virtual Private Clouds (VPCs), security groups, and network access control lists
- Identity and access management (IAM) with role-based access control and principle of least privilege
- Data protection through encryption at rest and in transit across all cloud services
- Logging and monitoring integration across all infrastructure components
- Incident response capabilities with automated response and recovery procedures

Cloud Service Security Requirements:

- Use of cloud services with appropriate compliance certifications (SOC 2, HIPAA, ISO 27001)
- Shared responsibility model understanding and implementation for each cloud service
- Data residency controls ensuring data remains within approved geographic regions
- Service level agreements (SLAs) including security and availability requirements
- Vendor risk assessments and ongoing security monitoring for all cloud providers

3.1.2 Infrastructure Hardening Standards

System Hardening Requirements:

- Security baselines for all operating systems and platforms (CIS Benchmarks, NIST guidelines) shall be documented and implemented.
- Removal of unnecessary services, protocols, and software components
- Security configuration management and drift detection
- Vulnerability scanning shall be conducted at least quarterly for all production systems, and patch management shall be performed in accordance with defined SLAs.
- Endpoint detection and response (EDR) deployment on all applicable systems

Network Hardening:

- Network segmentation and micro-segmentation for different security zones
- Zero-trust network architecture implementation where technically feasible
- Intrusion detection and prevention systems (IDS/IPS) deployment
- Network access control (NAC) for device authentication and authorization
- Regular network security assessments and penetration testing

3.2 Identity and Access Management (IAM)

Comprehensive IAM controls shall be implemented to ensure appropriate access to infrastructure resources while maintaining security and compliance.

3.2.1 Cloud IAM Implementation

Access Control Framework:

- Centralized identity management with single sign-on (SSO) integration
- Multi-factor authentication (MFA) required for all administrative access
- Role-based access control (RBAC) with predefined roles and permissions
- Privileged access management (PAM) for high-risk administrative functions
- Just-in-time (JIT) access for temporary elevated privileges

Service Account Management:

- Unique service accounts for each application and service with minimal required permissions
- Regular rotation of service account credentials and API keys
- Monitoring and alerting for service account usage and anomalies
- Automated provisioning and deprovisioning of service accounts
- Documentation and approval process for service account creation and modification

3.2.2 Access Reviews and Monitoring

Regular Access Certification:

- Quarterly access reviews for all administrative and privileged accounts
- Annual comprehensive review of all infrastructure access permissions
- Automated access recertification workflows with manager approval
- Immediate access revocation upon role changes or employment termination
- Exception handling process for emergency access requirements

Access Monitoring and Auditing:

- Real-time monitoring of all administrative and privileged access activities
- Automated alerting for suspicious access patterns or policy violations
- Comprehensive audit logging for all infrastructure access and changes
- Regular analysis of access logs for security anomalies and compliance validation
- Integration with security information and event management (SIEM) systems

3.3 Network Security and Segmentation

Network security controls shall provide comprehensive protection against unauthorized access and lateral movement within the infrastructure.

3.3.1 Network Architecture Security

Network Segmentation Strategy:

- Production, staging, development, and management network separation
- Application-tier segmentation (web, application, database layers)
- Security zone implementation with different trust levels and access controls
- DMZ (demilitarized zone) for external-facing services and applications
- Management network isolation for administrative access and monitoring

Traffic Control and Filtering:

- Default-deny network access policies with explicit allow rules
- Application-layer firewalls and web application firewalls (WAF) deployment
- Network traffic inspection and filtering for known threats and malicious content
- Rate limiting and DDoS protection for internet-facing services
- Network access control lists (ACLs) and security groups for granular traffic control

3.3.2 Network Monitoring and Detection

Network Security Monitoring:

- 24/7 network traffic monitoring and analysis
- Intrusion detection and prevention systems (IDS/IPS) with signature and anomaly-based detection
- Network behavior analysis for detecting advanced persistent threats (APTs)
- DNS monitoring and filtering for malicious domain detection
- Integration with threat intelligence feeds for proactive threat detection

Network Incident Response:

- Automated response capabilities for detected network threats
- Network isolation and quarantine procedures for compromised systems
- Traffic capture and analysis capabilities for incident investigation
- Network forensics tools and procedures for security incident analysis
- Coordination with security operations center (SOC) for incident response

3.4 Data Protection and Encryption

Comprehensive data protection controls shall ensure the confidentiality and integrity of all data within the infrastructure.

3.4.1 Encryption Implementation

Data at Rest Encryption:

- Full disk encryption for all virtual machines and storage systems
- Database encryption using transparent data encryption (TDE) or column-level encryption
- File system encryption for network-attached storage (NAS) and object storage
- Encryption of backup data and archive storage
- Hardware security module (HSM) or cloud HSM integration for key management

Data in Transit Encryption:

- TLS 1.3 or equivalent encryption for all network communications
- VPN encryption for all remote access and site-to-site connections
- End-to-end encryption for sensitive data transmissions
- Certificate management and validation for all encrypted communications
- Perfect forward secrecy (PFS) implementation where technically feasible

3.4.2 Key Management and Protection

Centralized Key Management:

- Cloud-native key management services (AWS KMS, Azure Key Vault, Google Cloud KMS)
- Customer-managed encryption keys (CMEK) for sensitive data and ePHI
- Key rotation policies and automated rotation procedures
- Key escrow and recovery procedures for business continuity
- Hardware security module (HSM) usage for high-value keys

Key Security Controls:

- Separation of key management from data management functions
- Multi-person authorization for key generation and recovery operations
- Audit logging for all key management activities
- Geographic distribution of keys for disaster recovery
- Secure key deletion and destruction procedures

3.5 Infrastructure as Code (IaC) and Configuration Management

Infrastructure deployments shall use code-based approaches with appropriate security controls and change management processes.

3.5.1 Secure IaC Practices

IaC Security Requirements:

- All infrastructure code shall be stored in a version control system. All changes must be reviewed and formally approved via the version control system (e.g., pull request approval) before being merged.
- Security scanning of infrastructure templates and configurations
- Automated compliance checking against security policies and standards
- Immutable infrastructure principles to prevent configuration drift
- Secrets management for infrastructure credentials and sensitive configuration

Configuration Management:

- Centralized configuration management with automated deployment pipelines
- Configuration drift detection and automated remediation
- Security baseline enforcement across all infrastructure components
- Change tracking and rollback capabilities for configuration modifications
- Documentation and approval process for infrastructure changes

3.5.2 CI/CD Pipeline Security

Secure Deployment Pipelines:

- Security scanning integration into CI/CD pipelines for infrastructure code
- Automated security testing and validation before deployment
- Staged deployment process with security validation at each stage
- Rollback procedures for failed or insecure deployments
- Deployment approval gates for production environment changes

Pipeline Protection:

- Access controls and authentication for CI/CD systems and pipelines
- Secure storage and management of deployment credentials and secrets
- Audit logging for all pipeline activities and deployments
- Code signing and integrity verification for deployment artifacts
- Isolation of deployment environments and access controls

3.6 Container and Serverless Security

Specialized security controls shall be implemented for containerized applications and serverless computing environments.

3.6.1 Container Security

Container Image Security:

- Base image security scanning and vulnerability assessment
- Minimal base images with only necessary components and dependencies
- Regular image updates and patch management processes
- Image signing and verification for deployment integrity
- Private container registries with access controls and scanning capabilities

Container Runtime Security:

- Container orchestration platform security (Kubernetes, ECS, AKS)
- Runtime security monitoring and anomaly detection
- Resource limits and isolation between containers
- Network policies and micro-segmentation for container communications
- Secrets management for container applications and services

3.6.2 Serverless Security

Function Security Controls:

- Code security scanning for serverless function code
- Principle of least privilege for function execution roles and permissions
- Environment variable security and secrets management
- Function timeout and resource limits configuration
- Monitoring and logging for function execution and security events

Serverless Architecture Security:

- API Gateway security controls and rate limiting
- Event source security and validation for function triggers
- Data encryption for serverless function storage and communications
- Dependency management and vulnerability scanning for function dependencies
- Cold start security considerations and optimization

3.7 Backup and Disaster Recovery

Comprehensive backup and disaster recovery capabilities shall ensure business continuity and data protection.

3.7.1 Backup Security

Backup Strategy Implementation:

- Regular automated backups for all critical systems and data
- Geographic distribution of backups for disaster recovery
- Encryption of all backup data at rest and in transit
- Access controls and monitoring for backup systems and data
- Backup integrity and restoration validation shall be performed at least quarterly for critical systems.

Backup Retention and Management:

- Retention policies aligned with business and regulatory requirements
- Secure disposal of expired backup media and data
- Version management and point-in-time recovery capabilities
- Backup monitoring and alerting for failed or incomplete backups
- Documentation of backup and recovery procedures

3.7.2 Disaster Recovery Planning

Recovery Infrastructure:

- Geographically separated disaster recovery infrastructure
- Automated failover capabilities for critical systems and services
- Recovery time objectives (RTO) and recovery point objectives (RPO) definition and validation
- Disaster recovery testing and validation exercises shall be conducted at least annually.
- Documentation and maintenance of disaster recovery procedures

Business Continuity Integration:

- Coordination with business continuity planning and requirements
- Communication procedures for disaster recovery activation
- Stakeholder notification and coordination during recovery operations
- Post-incident review and improvement of recovery procedures
- Training and awareness for disaster recovery procedures

3.8 Monitoring and Incident Response

Comprehensive monitoring and incident response capabilities shall provide early threat detection and rapid response to security incidents.

3.8.1 Security Monitoring

Infrastructure Monitoring:

- 24/7 monitoring of all infrastructure components and services
- Security information and event management (SIEM) integration
- Automated threat detection and alerting capabilities
- Performance monitoring and capacity management
- Compliance monitoring and reporting for regulatory requirements

Log Management and Analysis:

- Centralized log collection and analysis for all infrastructure components
- Log retention policies aligned with regulatory and business requirements
- Real-time log analysis and correlation for security event detection
- Secure log storage and access controls for log data
- Log integrity protection and tampering detection

3.8.2 Incident Response Integration

Infrastructure Incident Response:

- Automated incident response capabilities for infrastructure security events
- Integration with organizational incident response procedures
- Evidence preservation and forensics capabilities for infrastructure incidents
- Communication procedures for infrastructure-related security incidents
- Recovery and restoration procedures for compromised infrastructure

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(1) - Security Management Process
3.2	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Information Access Management
3.4	HIPAA Security Rule	45 CFR § 164.312(a)(2)(iv) - Encryption and Decryption

Policy Section	Standard/Framework	Control Reference
3.4	HIPAA Security Rule	45 CFR § 164.312(e)(1) - Transmission Security
3.8	HIPAA Security Rule	45 CFR § 164.312(b) - Audit Controls
All	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.3	SOC 2 Trust Services Criteria	CC6.6 - Network Security
3.4	SOC 2 Trust Services Criteria	CC6.7 - Data Transmission
3.7	SOC 2 Trust Services Criteria	A1.1 - System Availability
3.8	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
All	NIST Cybersecurity Framework	PR.AC - Identity Management
3.3	NIST Cybersecurity Framework	PR.DS - Data Security
All	CIS Controls	Critical Security Controls

5. Definitions

Container: Lightweight, portable software package that includes application code and all dependencies needed to run the application.

Defense in Depth: Security strategy employing multiple layers of defense to protect information and systems.

Infrastructure as Code (IaC): Practice of managing and provisioning infrastructure through machine-readable definition files.

Micro-segmentation: Security technique that creates secure zones in data centers and cloud environments to isolate workloads.

Serverless Computing: Cloud computing model where the cloud provider manages infrastructure and automatically allocates resources.

Software-Defined Perimeter (SDP): Network security approach that creates secure, encrypted connections between users and resources.

Virtual Private Cloud (VPC): Isolated virtual network environment within a public cloud infrastructure.

Zero Trust: Security model that requires verification for every user and device trying to access resources.

6. Responsibilities

Role	Responsibility
Infrastructure Security Team	Develop infrastructure security policies, implement security controls, monitor infrastructure security, and respond to infrastructure security incidents.
Cloud Engineers	Design and implement secure cloud infrastructure, manage cloud security configurations, and ensure compliance with security policies.
DevOps Engineers	Implement secure CI/CD pipelines, manage infrastructure as code, integrate security tools, and automate security controls.
Network Engineers	Design and maintain secure network architecture, implement network security controls, and monitor network security events.
System Administrators	Configure and maintain secure systems, implement security baselines, manage system access, and monitor system security.
Security Operations Center (SOC)	Monitor infrastructure security events, analyze security alerts, coordinate incident response, and provide 24/7 security monitoring.

Role	Responsibility
Compliance Team	Ensure infrastructure compliance with regulations, conduct compliance assessments, and coordinate audit activities.
Database Administrators	Implement database security controls, manage database encryption, monitor database access, and ensure database compliance.
All Engineering Staff	Follow infrastructure security policies, implement security controls in their areas, report security issues, and participate in security training.

Application Security Testing Procedure (ENG-PROC-001)

1. Purpose

The purpose of this procedure is to detail the process for conducting static application security testing (SAST), dynamic application security testing (DAST), and penetration testing to identify and remediate security vulnerabilities in applications.

2. Scope

This procedure applies to all company-developed applications, with specific requirements for those that handle electronic Protected Health Information (ePHI) or data classified as Confidential.

3. Overview

This procedure outlines the required security testing for applications, including automated SAST and DAST scans integrated into the development lifecycle and annual penetration tests for sensitive applications. It covers the process from testing and triaging findings to tracking remediation.

4. Procedure

4.1 Static Application Security Testing (SAST)

Step	Who	What
1	Developer	Integrates SAST tooling into the CI/CD pipeline for automated code analysis on every build or pull request.
2	Developer	Reviews SAST reports for security vulnerabilities, focusing on high and critical severity findings.
3	Developer	Triages identified vulnerabilities, creating tickets to track remediation efforts. False positives are documented and suppressed.
4	Development Team	Remediates vulnerabilities according to their severity and documents the fixes in the corresponding tickets.

4.2 Dynamic Application Security Testing (DAST)

Step	Who	What
1	Security Team / Developer	Configures and runs DAST scans against applications in a staging or testing environment before production deployment.
2	Security Team / Developer	Analyzes DAST scan results to identify runtime vulnerabilities.
3	Developer	Triages, prioritizes, and remediates identified vulnerabilities based on risk.

4.3 Penetration Testing

Step	Who	What
1	Security Team	Engages a qualified third-party vendor to conduct penetration tests at least annually on all applications that handle ePHI or Confidential data.
2	Security Team	Receives the final penetration test report from the vendor.
3	Security & Development Teams	Review the report findings, develop a remediation plan for identified vulnerabilities, and create tickets to track the required work.
4	Development Team	Implements the remediation plan and provides evidence of fixes for re-testing and validation.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
4.1 - 4.3	SOC 2	CC7.1, CC8.1
4.1 - 4.3	HIPAA Security Rule	45 CFR § 164.308(a)(8)

6. Artifact(s)

A test report from the relevant security tool (SAST, DAST) or a final penetration test report with a remediation plan.

7. Definitions

DAST (Dynamic Application Security Testing): A method of testing an application during its running state to find security vulnerabilities.

ePHI (electronic Protected Health Information): Any protected health information that is created, stored, transmitted, or received in any electronic format.

SAST (Static Application Security Testing): A method of testing an application's source code, bytecode, or binary code to find security vulnerabilities without executing the application.

8. Responsibilities

Role	Responsibility
Developer	Integrates and runs SAST/DAST tools, reviews findings, and remediates vulnerabilities.
Security Team	Manages the penetration testing program, assists with DAST, and provides guidance on vulnerability remediation.
Development Team	Ensures vulnerabilities are triaged and remediated in a timely manner based on risk.

Third-Party Component Security Review Procedure (ENG-PROC-002)

1. Purpose

The purpose of this procedure is to define the steps for scanning, reviewing, and approving the use of new open-source or commercial software components to minimize security and licensing risks.

2. Scope

This procedure applies to all new open-source and commercial third-party software components, libraries, and dependencies being considered for inclusion in company software.

3. Overview

This procedure describes the process for managing the security of third-party components. It begins with a developer proposing a new component, followed by automated scanning, a formal review of the results by engineering and security teams, and concludes with a documented approval or denial.

4. Procedure

Step	Who	What
1	Developer	Proposes the use of a new third-party component by creating an issue ticket and documenting the component's purpose and source.
2	Developer / CI/CD Pipeline	Uses automated Software Composition Analysis (SCA) tools to scan the component for known vulnerabilities (CVEs) and potential software license compliance issues.
3	Development Team Lead & Security Team	Review the SCA scan results. They assess the severity of any identified vulnerabilities and the implications of the component's license.
4	Development Team	If significant vulnerabilities are found, the team must create a remediation plan (e.g., wait for a patched version) or formally document a risk acceptance rationale.
5	Development Team Lead	Based on the review and any remediation plan, formally approves or denies the use of the component in the project documentation or ticket.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2	CC8.1
1-5	NIST SP 800-161	

6. Artifact(s)

A record of the SCA scan results and a formal approval or denial for the component in the project documentation or tracking system.

7. Definitions

SCA (Software Composition Analysis): An automated process that identifies the open-source software in a codebase to evaluate security, license compliance, and code quality.

CVE (Common Vulnerabilities and Exposures): A list of publicly disclosed computer security flaws.

8. Responsibilities

Role	Responsibility
Developer	Proposes new components and initiates the SCA scan.
Development Team Lead	Reviews scan results, makes the final decision on component use, and ensures proper documentation.
Security Team	Assists in reviewing SCA scan results, provides guidance on vulnerability risk, and reviews risk acceptance cases.

Standard Change Management Procedure (ENG-PROC-003)

1. Purpose

The purpose of this procedure is to detail the end-to-end process for a standard, non-emergency change to a production application or its configuration, ensuring that all changes are properly developed, tested, reviewed, and approved.

2. Scope

This procedure applies to all standard, non-emergency changes to production applications, infrastructure, and related system configurations.

3. Overview

This procedure outlines the standard workflow for managing changes. It begins with a developer creating a ticket and a feature branch, followed by code development, a peer and security review via a pull request, QA testing, and final approval from an Engineering Lead before being merged for deployment.

4. Procedure

Step	Who	What
1	Developer	Creates an issue ticket in the tracking system to document the planned change and creates a new feature branch in the source code repository.
2	Developer	Submits a pull request when development is complete, filling out the required pull request template, including a security checklist.
3	Peer Reviewer	A qualified peer reviews the code for correctness, quality, and adherence to coding standards, and provides approval on the pull request.
4	Security Team	Reviews the pull request for any security implications. Approval is required for changes impacting security controls or sensitive data.
5	QA Team	Tests the changes in a dedicated staging environment to verify functionality and ensure no regressions are introduced. Provides sign-off.

Step	Who	What
6	Engineering Lead	Provides the final review and approval to merge the pull request into the main branch, authorizing its deployment to production.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2	CC8.1
1-6	HIPAA Security Rule	45 CFR § 164.312(b)
1-6	HIPAA Security Rule	45 CFR § 164.312(c)(1)

6. Artifact(s)

A merged GitHub pull request containing all required reviews, approvals, test results, and a link to the original issue ticket.

7. Definitions

Pull Request: A mechanism for a developer to notify team members that they have completed a feature. It allows others to review, discuss, and approve the code before it is merged into the main codebase.

Feature Branch: A source-control branch used to develop a new feature in isolation. When the feature is complete, the branch is merged back into the main branch.

8. Responsibilities

Role	Responsibility
Developer	Implements the change, creates the pull request, and responds to feedback.
Peer Reviewer	Conducts a thorough review of the code changes.
Security Team	Assesses the security impact of the change and provides approval.

Role	Responsibility
QA Team	Validates the functionality and quality of the change before release.
Engineering Lead	Provides final authorization for the change to be deployed to production.

Emergency Change Management Procedure (ENG-PROC-004)

1. Purpose

The purpose of this procedure is to outline the expedited process for authorizing, deploying, and retrospectively documenting an emergency change to resolve a critical issue, such as a service outage or a severe security vulnerability.

2. Scope

This procedure applies to all emergency changes required to restore service, fix a critical security flaw, or address an urgent operational issue in the production environment.

3. Overview

This procedure defines the workflow for emergency changes. It starts with the identification of a critical issue, followed by obtaining expedited approvals, performing a focused review, deploying the fix, and conducting a formal post-mortem review to ensure proper documentation is completed after the fact.

4. Procedure

Step	Who	What
1	Engineer	Identifies a critical issue requiring an emergency change and immediately notifies the Engineering Lead and Security Team.
2	Engineer	Obtains and documents verbal or written approval from an Engineering Lead and a member of the Security Team in an emergency change ticket.
3	Engineer / Peer Reviewer	An expedited peer and security review is performed on the proposed change to ensure it is a targeted and necessary fix.
4	Engineer	Deploys the approved change to the production environment to resolve the critical issue.
5	Engineering & Security Teams	Conduct a formal post-mortem review within 3 business days of the change. The standard change documentation and pull request are completed retroactively.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2	CC8.1
1-5	HIPAA Security Rule	45 CFR § 164.312(b)

6. Artifact(s)

An emergency change ticket with documented approvals and a link to a post-mortem report.

7. Definitions

Post-Mortem Review: A formal meeting and report that analyzes an incident or emergency change to understand the cause, impact, and actions taken, and to identify lessons learned to prevent recurrence.

Critical Issue: An issue that causes a service outage, data corruption, a severe security vulnerability, or significantly impacts customers' ability to use the service.

8. Responsibilities

Role	Responsibility
Engineer	Identifies the need for an emergency change, implements the fix, and obtains necessary approvals.
Engineering Lead	Provides approval for the emergency change and participates in the post-mortem review.
Security Team	Provides approval for the emergency change, assesses security risk, and participates in the post-mortem review.

System Hardening and Baselining Procedure (ENG-PROC-005)

1. Purpose

The purpose of this procedure is to describe the process for applying documented security baselines to new systems and verifying their ongoing compliance to ensure a consistent and secure configuration.

2. Scope

This procedure applies to all new production servers, virtual machines, and container images provisioned in the company's infrastructure.

3. Overview

This procedure details the steps for system hardening. It begins with the provisioning of a new system, followed by the automated application of a security baseline, removal of unnecessary software, and concludes with a compliance scan to verify the configuration and detect any drift.

4. Procedure

Step	Who	What
1	Engineer / Automated System	A new server or service is provisioned using Infrastructure as Code (IaC) templates.
2	Automated Configuration Script	An automated configuration management script (e.g., Ansible, Puppet) applies the documented security baseline, such as the relevant CIS Benchmark.
3	Automated Configuration Script	The script removes or disables unnecessary services, ports, and software packages to reduce the system's attack surface.
4	Automated Compliance Tool	A compliance scan is automatically run after provisioning to verify that the baseline was applied correctly and to establish the initial secure state.

Step	Who	What
5	Security Team	Periodically runs compliance scans to detect any configuration drift from the established baseline and alerts the system owner if deviations are found.

Note: If the security team determines the configuration drift is critical, an incident post-mortem may be initiated to analyze the incident in detail.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2	CC6.1
2, 4	CIS Controls	Control 4, 5
1-5	HIPAA Security Rule	45 CFR § 164.308(a)(1)

6. Artifact(s)

A compliance scan report confirming adherence to the security baseline.

7. Definitions

CIS Benchmarks: A set of globally recognized and consensus-developed best practices for the secure configuration of a target system.

Configuration Drift: The process by which a system’s configuration changes over time from its established, secure baseline.

Infrastructure as Code (IaC): The management of infrastructure (networks, virtual machines, load balancers, and connection topology) in a descriptive model, using the same versioning as DevOps team uses for source code.

8. Responsibilities

Role	Responsibility
Engineer	Develops and maintains the Infrastructure as Code templates and automated configuration scripts.
Security Team	Defines the security baselines, manages the compliance scanning tools, and reviews scan reports for deviations.
System Owner	Is responsible for remediating any configuration drift detected on their systems.

Privileged Infrastructure Access Review Procedure (ENG-PROC-006)

1. Purpose

The purpose of this procedure is to outline the steps for conducting and documenting the required quarterly reviews of all user accounts with privileged access to production infrastructure, ensuring the principle of least privilege is maintained.

2. Scope

This procedure applies to all user accounts, service accounts, and roles with administrative or privileged access to any production system, database, or network component.

3. Overview

This procedure describes the quarterly access review process. It begins with the Security Team generating a list of privileged accounts, which is then distributed to system owners for review. Managers must attest to the continued need for each access right. Any unnecessary access is then revoked, and the completed attestations are stored for audit purposes.

4. Procedure

Step	Who	What
1	Security Team	On a quarterly basis, generates a report from the identity and access management system listing all users and service accounts with privileged access to production infrastructure.
2	Security Team	Sends the access report to the relevant system owners or managers responsible for the systems listed.
3	System Owner / Manager	Reviews each user’s access rights on the report and attests in writing (e.g., via a signed form or an approval in a tracking ticket) that the access is still required for their job function.
4	IT Team / System Administrator	Upon notification from the manager or Security Team, revokes any access that is no longer necessary or has been denied during the review.

Step	Who	What
5	Security Team	Collects and stores the completed, signed attestations as an audit record of the quarterly review.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2	CC6.1
1-5	HIPAA Security Rule	45 CFR § 164.308(a)(4)

6. Artifact(s)

A signed access review attestation form or a completed access review ticket with documented approvals from the system owner or manager.

7. Definitions

Privileged Access: Access rights beyond those of a standard user. This includes administrative rights to servers, databases, applications, or network devices.

Least Privilege: The principle of restricting access rights for users to the minimum permissions they need to perform their work.

Attestation: The act of formally confirming that something is true, correct, or has been completed.

8. Responsibilities

Role	Responsibility
Security Team	Manages the overall access review process, generates reports, distributes them, and stores the final attestations.
System Owner / Manager	Reviews the access for their systems and personnel, and attests to the ongoing need for privileged access.

Role	Responsibility
IT Team / System Administrator	Revokes access rights as directed by the outcome of the review.

Schedule of Security Procedures (ISMS-SUP-001)

Quarterly Procedures These procedures must be conducted and documented every three months to ensure ongoing compliance and security posture management.

Procedure (Code)	Primary Owner	Description
Information Security Committee Charter Procedure (SEC-PROC-001)	Committee Chair	Defines the operating rules and responsibilities of the Information Security Committee, which holds quarterly meetings.
Facility Access Management Procedure (SEC-PROC-006)	Facilities/Se Team	Describes the process for managing physical facility access, including conducting and documenting quarterly access reviews.
User Access Review Procedure (AC-PROC-003)	IT/Security Team	Defines the process for conducting periodic reviews of user access rights to ensure adherence to the principle of least privilege.
Privileged Infrastructure Access Review Procedure (ENG-PROC-006)	Security Team	Outlines the steps for conducting and documenting the required quarterly reviews of all user accounts with privileged access.

Annual Procedures These procedures must be performed at least once per year to satisfy major compliance, assessment, and testing requirements.

Procedure (Code)	Primary Owner	Description
Internal Audit Procedure (SEC-PROC-002)	Head of Internal Audit	Outlines the process for planning, conducting, and reporting on annual internal audits of the Information Security Management System.

Procedure (Code)	Primary Owner	Description
Risk Assessment Procedure (SEC-PROC-004)	Security Officer	Establishes a systematic process for conducting risk assessments annually and on an ad-hoc basis when significant changes occur.
Incident Response Plan (IRP) ([RES-PROC-001])	Security Team	Provides actionable steps for responding to incidents, including conducting annual training and simulation exercises.
Business Impact Analysis (BIA) Procedure ([RES-PROC-004])	Business Continuity Manager	Defines the methodology for conducting the annual Business Impact Analysis to identify critical functions and establish recovery objectives.
BCDR Testing and Exercise Procedure ([RES-PROC-007])	Business Continuity Manager	Details the requirements for planning and executing the annual disaster recovery tests and business continuity exercises.
Cryptographic Key Lifecycle Management Procedure (OP-PROC-001)	Security Engineering Team	Provides technical steps for the secure lifecycle of cryptographic keys, including their annual rotation.
Application Security Testing Procedure (ENG-PROC-001)	Security Team	Details the process for conducting security testing, including annual penetration tests for applications handling sensitive data.

Ad-Hoc / As-Needed / Event-Driven Procedures These procedures are not performed on a fixed schedule but are triggered by specific events such as a new hire, a security incident, or a request for a new system.

Procedure (Code)	Primary Owner	Description
Password Policy Exception Procedure (SEC-PROC-003)	Security Officer	Provides a formal process for requesting, reviewing, and documenting exceptions to the Password Policy.
Vendor Risk Assessment and Onboarding Procedure (SEC-PROC-005)	Security Team	Details the process for assessing a new vendor’s security posture before engagement.
AI Tool Risk Assessment and Approval Procedure (SEC-PROC-007)	AI Governance Committee	Defines the process for performing a risk assessment on new AI tools before they are approved for use.
Vulnerability Management Procedure (SEC-PROC-008)	Security Team	Describes the continuous workflow for identifying, prioritizing, remediating, and verifying system vulnerabilities.
Vulnerability Management Exception Procedure (SEC-PROC-009)	Security Officer	Outlines the process for formally requesting and documenting an exception to a vulnerability remediation Service Level Agreement (SLA).
Acceptable Use Policy Violation Investigation Procedure (AC-PROC-001)	Security Officer	Defines the process for investigating and responding to reported violations of the acceptable use policy.
Bring Your Own Device (BYOD) Onboarding Procedure (AC-PROC-002)	IT Department	Establishes the process for registering and securing a personally-owned device for access to company resources.
Access Control Management Procedure (AC-PROC-004)	IT Department	Defines the process for managing the lifecycle of user access, including provisioning, modification, and revocation.
HIPAA Breach Risk Assessment Procedure ([RES-PROC-002])	Privacy Officer	Guides the formal risk assessment required to determine if an incident qualifies as a notifiable HIPAA breach.

Procedure (Code)	Primary Owner	Description
Post-Incident Review Procedure ([RES-PROC-003])	Incident Commander	Outlines the process for conducting a formal 'lessons learned' review after a significant incident is resolved.
IT Disaster Recovery Plan (DRP) ([RES-PROC-005])	BCDR Steering Committee	Provides technical procedures for recovering IT infrastructure in the event of a declared disaster.
Business Continuity Plan (BCP) ([RES-PROC-006])	BCDR Steering Committee	Outlines procedures for activating emergency response and continuing critical business functions during a disruption.
Mobile Device Onboarding and Security Configuration Procedure (OP-PROC-002)	IT Security Team	Details the steps for enrolling a mobile device in the MDM system and ensuring it meets security requirements.
Lost or Stolen Mobile Device Response Procedure (OP-PROC-003)	IT Security Team	Provides the immediate steps to take when a mobile device used for company business is reported lost or stolen.
Secure Media Disposal and Sanitization Procedure (OP-PROC-004)	IT Team	Provides instructions for securely destroying or sanitizing media that is at the end of its lifecycle.
Legal Hold Procedure (OP-PROC-005)	Legal Team	Outlines the steps for issuing, tracking, and releasing a legal hold on information relevant to legal matters.
Workforce Screening and Background Check Procedure (OP-PROC-006)	Human Resources (HR)	Outlines the formal process for conducting required background checks on all candidates for employment.
Employee Onboarding and Offboarding Security Procedure (OP-PROC-007)	Human Resources (HR)	Provides a formal checklist to ensure all security tasks are completed during employee onboarding and termination.

Procedure (Code)	Primary Owner	Description
Security Policy Sanction Procedure (OP-PROC-008)	Manager & HR	Describes the process for documenting security policy violations and applying appropriate disciplinary actions.
Third-Party Component Security Review Procedure (ENG-PROC-002)	Developmen Team Lead	Defines the steps for reviewing and approving the use of new third-party software components.
Standard Change Management Procedure (ENG-PROC-003)	Engineering Lead	Details the process for managing a standard, non-emergency change to a production application or configuration.
Emergency Change Management Procedure (ENG-PROC-004)	Engineering & Security Teams	Outlines the expedited process for authorizing and deploying an emergency change to resolve a critical issue.
System Hardening and Baselining Procedure (ENG-PROC-005)	Security Team	Describes the process for applying security baselines to new systems and verifying their ongoing compliance.

ISMS High-Level RACI Chart (ISMS-SUP-002)

RACI Definitions:

- **R = Responsible:** The person(s) who does the work to achieve the task.
- **A = Accountable:** The person ultimately answerable for the correct and thorough completion of the deliverable or task (the "owner"). There is only one 'A' per task.
- **C = Consulted:** The person(s) who provides input, feedback, and expertise (two-way communication).
- **I = Informed:** The person(s) kept up-to-date on progress or completion (one-way communication).

Consolidated Roles for a ~50-Person Company:

- **Leadership:** CEO / Executive Team
- **CISO:** Chief Information Security Officer (also assumes Privacy Officer & AI Ethics Officer roles)
- **Eng. Lead:** Head of Engineering / CTO
- **IT/DevOps:** IT & DevOps Lead / Team
- **Legal:** Legal & Compliance Officer
- **HR:** Human Resources Manager
- **Workforce:** All Workforce Members

Deliverable / Task	Leadershi	CISO	Eng. Lead	IT/DevOp	Legal	HR	Workforce
ISMS Governance & Policy Management	A	R	C	I	C	C	I
Annual Risk Assessment	C	A	R	R	C	C	I
Vulnerability Management Program	I	A	R	R			
Vendor & Third-Party Risk Management	I	A	C	R	C	C	
Access Control & Review (Quarterly)	I	A	R	R			

Deliverable / Task	Leadershi	CISO	Eng. Lead	IT/DevOp	Legal	HR	Workforce
Secure Development & Change Mgt.	I	C	A	R			R
Incident Response & Post-Mortem	I	A	R	R	C	C	R
BCDR Planning & Annual Testing	A	R	R	R	C	C	I
HR Security Lifecycle (On/Offboarding)	I	C	I	R		A	R
Security Awareness Training	I	A	I	I		R	R
Internal & External Audits	A	R	C	C	C	C	I
AI Tool Assessment & Approval	C	A	R	C	C		R
Encryption & Key Management	I	C	A	R			
Legal Hold & eDiscovery	C	C	C	R	A		

12-Month ISMS Implementation Roadmap (ISMS-SUP-003)

Quarter 1 (Months 1-3): Foundation & Visibility **Goal:** Establish baseline security controls and gain visibility into the environment.

Mo	Key Deliverables & Activities	Key Metrics for Success
1	**Official Kick-Off & Scoping:** • Finalize policies & obtain leadership sign-off. • Formally assign key roles (Security Officer, etc.). • Complete Gap Analysis and Data Discovery.	• **100%** of policies formally approved and signed. • **100%** of key security roles assigned in a RACI chart. • Gap analysis and data inventory documents completed.
2	**Identity & Endpoint Security:** • Deploy and enforce Multi-Factor Authentication (MFA) for all critical systems. • Deploy an Endpoint Detection & Response (EDR) solution to all workstations. • Roll out a company-wide Password Manager.	• **95%+** of users enrolled in MFA for critical systems. • **100%** of corporate endpoints have an active EDR agent. • **80%+** of workforce actively using the password manager.
3	**Initial Vulnerability Management:** • Implement a vulnerability scanning tool for cloud and application assets. • Conduct initial baseline scans to understand the current risk posture. • Begin triaging critical and high-risk findings.	• **90%+** of production assets covered by vulnerability scans. • **100%** of identified critical vulnerabilities have a remediation ticket created. • Reduction in the number of "quick win" high-risk vulnerabilities by **25%**.

Quarter 2 (Months 4-6): Control & Process Implementation **Goal:** Move from ad-hoc actions to repeatable, defined security processes.

Mo	Key Deliverables & Activities	Key Metrics for Success
4	**Formalize Core Processes:** • Implement the formal `Change Control Procedure` using GitHub. • Implement the `Vendor Risk Assessment Procedure` for all *new* vendors. • Implement the formal `HR Onboarding/Offboarding Procedures`.	• **100%** of production code changes are deployed via the new change control process. • **100%** of new vendors undergo a documented risk assessment. • **100%** of new hires and terminations follow the documented security checklists.
5	**Training & Access Control:** • Conduct the first company-wide Security Awareness Training campaign. • Conduct the first `Quarterly User Access Review` for critical systems. • Begin hardening critical systems based on defined baselines.	• **95%+** of workforce completes security awareness training. • **100%** of required access reviews are completed and signed off by managers. • **0** critical deviations from the security baseline on newly hardened systems.
6	**Incident Response Preparation:** • Finalize the `Incident Response Plan (IRP).` • Define and document Incident Commander and IRT roles. • Configure SIEM/logging to capture critical events for detection.	• IRP document is formally approved. • Incident Response Team roster is published and communicated. • **90%+** of critical systems are sending logs to a central SIEM.

Quarter 3 (Months 7-9): Hardening & Testing **Goal:** Validate the effectiveness of implemented controls and mature security practices.

Mo	Key Deliverables & Activities	Key Metrics for Success
7	**Engage Third-Party Assessors:** • Select and contract a vendor for the annual penetration test. • Select and contract an audit firm for the future SOC 2 audit. • Conduct the first `BCDR Tabletop Exercise`.	• Pen test and audit contracts signed. • BCDR tabletop exercise completed with a post-exercise report generated. • **100%** of IRT members participate in the exercise.

Mo	Key Deliverables & Activities	Key Metrics for Success
8	**Penetration Testing & Remediation:** • Execute the annual third-party penetration test. • Triage findings from the test report and create a remediation plan. • Begin remediating high-risk findings from the pen test.	• Pen test report received. • **100%** of critical and high-risk findings have a remediation plan with an assigned owner. • Mean Time to Remediate (MTTR) for critical vulnerabilities is under **15 days**.
9	**Mature Vendor & AI Governance:** • Begin reviewing *existing* high-risk vendors against the new policy. • Implement the `AI Tool Risk Assessment Procedure` for any new AI tools being considered by teams.	• **50%** of existing high-risk vendors have a completed risk assessment on file. • **100%** of new AI tool requests follow the formal assessment procedure. • **0** unapproved AI tools are detected processing company data.

Quarter 4 (Months 10-12): Audit Readiness & Optimization **Goal:** Prepare for external audits and ensure the ISMS is a continuous, improving program.

Mo	Key Deliverables & Activities	Key Metrics for Success
10	**Internal Audit & Evidence Gathering:** • Conduct the first `Internal Audit` against the policy set. • Begin systematically collecting evidence (artifacts) for the upcoming SOC 2 audit. • Remediate any gaps found during the internal audit.	• Internal audit completed and report issued. • **75%+** of evidence requests for the upcoming SOC 2 are fulfilled and organized. • **100%** of high-risk internal audit findings have a documented corrective action plan.
11	**Formal Risk & BIA Assessment:** • Conduct the formal `Annual Risk Assessment`. • Conduct the formal `Business Impact Analysis (BIA)`. • Present findings to the Information Security Committee.	• Annual Risk Assessment report is approved by leadership. • Business Impact Analysis (BIA) report is approved by leadership. • **Top 5** company risks are identified and have a documented treatment plan.

Mo	Key Deliverables & Activities	Key Metrics for Success
12	**Final Review & Planning for Year 2:** • Hold the final quarterly Information Security Committee meeting of the year. • Review progress against the roadmap and finalize the audit schedule. • Develop the roadmap for the following year based on risk assessment and audit findings.	• Q4 committee meeting held with documented minutes. • Formal audit date is scheduled. • **Year 2 Roadmap** is drafted and presented to leadership for approval.

Encryption and Key Management Policy (OP-POL-001)

1. Objective

The objective of this policy is to establish comprehensive requirements for the implementation, management, and governance of cryptographic controls and encryption key management at **[Company Name]**. This policy ensures that sensitive information, particularly electronic Protected Health Information (ePHI), is protected through appropriate encryption technologies and that cryptographic keys are securely generated, distributed, stored, and disposed of in compliance with HIPAA, HITECH, and SOC 2 requirements.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, and third parties who handle, process, store, or transmit encrypted information or manage cryptographic keys. It encompasses all information systems, applications, databases, storage devices, communication channels, and backup media containing sensitive data. This policy covers all encryption technologies, including symmetric and asymmetric encryption, digital signatures, and cryptographic hashing, across all computing environments including on-premises, cloud, and mobile platforms.

3. Policy

[Company Name] shall implement and maintain comprehensive, auditable cryptographic controls to protect the confidentiality, integrity, and authenticity of sensitive information throughout its lifecycle.

3.1 Encryption Requirements

Encryption shall be implemented for all sensitive information based on data classification levels and regulatory requirements.

3.1.1 Mandatory Encryption Requirements

The following data types and scenarios require mandatory encryption using algorithms approved in section 3.1.2 of this policy:

Electronic Protected Health Information (ePHI):

- ePHI at rest: Encrypted using AES-256 or a stronger approved algorithm.
- ePHI in transit: Encrypted using TLS 1.2 or higher, with a strong cipher suite configuration.

- ePHI on mobile devices and removable media: Full device/media encryption is mandatory.

Confidential and Restricted Data:

- Database encryption for sensitive data fields using transparent data encryption (TDE) or column-level encryption
- File system encryption for servers and workstations storing sensitive information
- Email encryption for messages containing sensitive data
- Backup encryption for all backup media and archives

Authentication Credentials:

- Password hashes using a strong, salted cryptographic hash function (e.g., bcrypt, Argon2).
- API keys and tokens encrypted at rest.
- Digital certificates and private keys protected by hardware security modules (HSMs) or equivalent secure key storage mechanisms.

3.1.2 Encryption Standards and Algorithms

Only cryptographically strong, industry-standard algorithms and protocols approved by the Security Officer shall be used. The use of any algorithm not on the approved list is prohibited.

Approved Symmetric Encryption Algorithms:

- AES (Advanced Encryption Standard) with key lengths of 128, 192, or 256 bits
- ChaCha20-Poly1305 for authenticated encryption

Approved Asymmetric Encryption Algorithms:

- RSA with minimum key length of 3072 bits (4096 bits preferred).
- Elliptic Curve Cryptography (ECC) with minimum key length of 256 bits.

Approved Hash Functions:

- SHA-256, SHA-384, SHA-512 for data integrity
- bcrypt, scrypt, or Argon2 for password hashing

Prohibited Algorithms:

- DES (Data Encryption Standard) and 3DES
- MD5 and SHA-1 hash functions
- RC4 stream cipher
- RSA keys shorter than 3072 bits

- SSL v2, SSL v3, TLS 1.0, TLS 1.1

3.2 Key Management Framework

A comprehensive key management system shall be implemented to ensure the secure lifecycle management of all cryptographic keys.

3.2.1 Key Management Principles

- **Separation of Duties:** Key management roles and responsibilities shall be formally assigned and separated to prevent any single individual from having unilateral control over a key's lifecycle.
- **Least Privilege:** Access to cryptographic keys shall be restricted to the minimum necessary for an individual or system to perform its authorized function.
- **Key Escrow:** Critical encryption keys required for data recovery shall be securely escrowed. The process for accessing escrowed keys must require documented approval from at least two authorized individuals.
- **Audit Trail:** All key management activities, including generation, distribution, rotation, and destruction, shall be logged in a secure, immutable audit trail and monitored for anomalies.

3.2.2 Key Generation

- Keys shall be generated using approved cryptographically secure random number generators (CSRNGs)
- Key generation shall occur in secure, controlled environments
- Hardware Security Modules (HSMs) or equivalent secure hardware shall be used for high-value key generation
- Weak or predictable keys shall be rejected through automated validation processes

3.2.3 Key Distribution and Exchange

- Key distribution shall use secure, authenticated channels (e.g., TLS 1.2 or higher).
- Public key infrastructure (PKI) shall be the primary method for asymmetric key distribution.
- Key exchange protocols shall be configured to provide perfect forward secrecy (PFS). Any deviation must be documented and approved by the Security Officer.
- Manual key distribution is prohibited without dual control and documented, time-bound approval from the Security Officer.

3.2.4 Key Storage and Protection

- Encryption keys shall be stored separately from the data they protect

- Master keys shall be stored in HSMs or equivalent tamper-resistant hardware
- Key storage systems shall be hardened and subject to strict access controls
- Encryption keys shall themselves be encrypted at rest using a separate key encryption key (KEK).
- Cloud-based key management services (e.g., AWS KMS, Azure Key Vault) must be configured in accordance with the **[Company Name]** `Infrastructure Security Policy (ENG-POL-003)` and `Vendor and Third-Party Risk Management Policy (SEC-POL-005)`.

3.2.5 Key Usage and Access Controls

- Key access shall be granted only to authorized personnel and applications
- Multi-factor authentication shall be required for access to key management systems
- Key usage shall be logged and actively monitored for unauthorized access attempts or anomalous usage patterns.
- Automated key rotation shall be implemented. Where automation is not technically feasible, the justification must be documented and approved by the Security Officer, and a manual rotation schedule must be tracked.
- Emergency key access procedures shall be documented, tested annually, and require multi-person control.

3.2.6 Key Rotation and Lifecycle Management

Encryption keys shall be rotated at or before the following minimum frequencies. A shorter rotation period shall be used if required by a specific regulation, standard, or risk assessment.

- Data encryption keys: Annually or after encrypting **[Amount, e.g., 1TB]** of data, whichever comes first.
- Key encryption keys: Every 2 years.
- SSL/TLS certificates: Annually, or as required by the Certificate Authority.
- Authentication keys (e.g., API keys): Every 6 months.
- Emergency key rotation shall be performed immediately upon:
  - Suspected key compromise
  - Workforce member termination with key access
  - System security incidents involving key management systems
  - Vendor security breaches affecting key material

3.2.7 Key Destruction and Disposal

- Cryptographic keys shall be securely destroyed as soon as they are no longer required for business or legal purposes.
- Key destruction shall use cryptographically secure deletion methods (e.g., cryptographic erasure, overwriting with random data multiple times).
- HSMs shall perform secure key zeroization procedures.
- Physical destruction of media that stored keys shall be performed in accordance with the `Data Retention and Disposal Policy (OP-POL-003)` and be verified and documented.
- All key destruction activities shall be logged and auditable.

3.3 Digital Certificates and Public Key Infrastructure (PKI)

[Company Name] shall maintain appropriate PKI capabilities to support digital certificates and public key cryptography.

3.3.1 Certificate Authority (CA) Management

- Internal CA infrastructure shall be established for organizational certificates
- Root CA systems shall be offline and stored in physically secure locations
- Intermediate CAs shall be used for day-to-day certificate issuance
- External CAs shall be evaluated and approved for specific use cases

3.3.2 Certificate Lifecycle Management

- Certificate requests shall be validated and approved through a formal, documented process managed by the IT Security Team.
- Certificate templates shall be used to enforce appropriate key usage, algorithm strength, and validity periods.
- Certificate revocation capabilities shall be maintained and tested annually through Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP).
- Automated monitoring and alerting shall be implemented to ensure expired or revoked certificates are removed from systems at least 7 days prior to expiration.

3.4 Cloud Encryption and Key Management

All use of cloud services must adhere to the following cryptographic requirements, as detailed in the `Infrastructure Security Policy (ENG-POL-003)`.

3.4.1 Cloud Encryption Requirements

- Customer-managed encryption keys (CMEK) shall be used for all production data stores containing ePHI or other Restricted data in cloud environments.
- Encryption shall be implemented at multiple layers (e.g., application, database, storage, network) to provide defense-in-depth.
- Cloud provider encryption services and configurations shall be reviewed and approved by the IT Security Team before use.
- Data sovereignty and residency requirements shall be enforced through technical controls for all data stored in the cloud.

3.4.2 Cloud Key Management

- **[Company Name]**-controlled key management services (e.g., AWS KMS, Azure Key Vault) shall be the required standard for all cloud-based encryption.
- Hybrid key management architectures (e.g., "Hold Your Own Key" or HYOK) shall be implemented where feasible to maintain on-premises control of master keys for the most sensitive data.
- Cloud HSM services shall be used for high-security applications as determined by the Security Officer.
- Key export capabilities shall be tested annually to ensure data can be decrypted and migrated, preventing vendor lock-in.

3.5 Encryption Performance and Monitoring

Encryption implementations shall be monitored for performance impact and security effectiveness.

3.5.1 Performance Monitoring

- Encryption overhead shall be measured and optimized
- Hardware acceleration shall be used where available and appropriate
- Application performance impact shall be assessed and mitigated
- Capacity planning shall account for encryption processing requirements

3.5.2 Security Monitoring

- Cryptographic failures, errors, and misconfigurations shall be logged and trigger automated alerts to the IT Security Team for immediate investigation.
- Key management system access and activity logs shall be ingested into a Security Information and Event Management (SIEM) system and monitored for suspicious activity.
- Automated certificate expiration monitoring and alerting shall be implemented to prevent

service disruptions.

- An annual review of cryptographic standards shall be conducted to maintain a crypto-agility plan, addressing algorithm obsolescence and emerging threats such as quantum computing.

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
3.1.1	HIPAA Security Rule	45 CFR § 164.312(a)(2)(iv) - Encryption and Decryption
3.1.1	HIPAA Security Rule	45 CFR § 164.312(e)(2)(ii) - Encryption
All	HIPAA Security Rule	45 CFR § 164.312(e)(1) - Transmission Security
3.2	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.1, 3.2	SOC 2 Trust Services Criteria	CC6.6 - Other Controls to Achieve Logical Access Security Objectives
3.2	SOC 2 Trust Services Criteria	CC6.8 - Restricts Access to Encrypted Data
All	NIST Cybersecurity Framework	PR.DS-1: Data-at-rest is protected.
All	NIST Cybersecurity Framework	PR.DS-2: Data-in-transit is protected.
3.2	NIST SP 800-57	Recommendation for Key Management
All	ISO/IEC 27001:2022	A.8.24 - Use of cryptography

5. Definitions

Advanced Encryption Standard (AES): A symmetric encryption algorithm adopted as a U.S. Federal Government standard.

Certificate Authority (CA): An entity that issues digital certificates certifying the ownership of public keys.

Cryptographically Secure Random Number Generator (CSRNG): A random number generator that meets cryptographic security requirements.

Hardware Security Module (HSM): A dedicated cryptographic device designed to securely generate, store, and manage cryptographic keys.

Key Escrow: The practice of storing cryptographic keys with a trusted third party for recovery purposes.

Public Key Infrastructure (PKI): A framework for managing digital certificates and public key encryption.

Transport Layer Security (TLS): A cryptographic protocol for secure communication over computer networks.

Transparent Data Encryption (TDE): Database encryption technology that encrypts data files at rest.

6. Responsibilities

Role	Responsibility
Security Officer	Develop encryption policies, oversee key management program, and ensure compliance with cryptographic standards.
IT Security Team	Implement encryption technologies, manage key management systems, and monitor cryptographic controls.
System Administrators	Configure and maintain encryption systems, perform key rotation procedures, and ensure proper encryption deployment.

Role	Responsibility
Database Administrators	Implement database encryption, manage database encryption keys, and ensure encrypted backup procedures.
Cloud Engineers	Configure cloud encryption services, manage cloud-based key management, and ensure proper cloud cryptographic controls.
Application Developers	Implement application-level encryption using approved cryptographic libraries, protect secrets in code, and follow secure coding practices as defined in the `Secure Software Development Policy (ENG-POL-001)`.
Privacy Officer	Ensure encryption requirements meet privacy obligations, oversee ePHI encryption protections, and coordinate with the Security Officer on data protection strategies.
All Workforce Members	Use encryption tools as required, protect credentials used for encryption systems, and immediately report suspected encryption failures or key compromises to the IT Security Team.

7. Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract, in accordance with **[Company Name]**'s `Human Resources Security Policy (OP-POL-004)`. Violations may also carry civil and criminal penalties.

8. Exceptions

Any exception to this policy must be documented, identifying the associated risks and mitigating controls, and must be submitted to the Security Officer for formal written approval. Approved exceptions will be reviewed on an annual basis.

Mobile Device Policy (BYOD) (OP-POL-002)

1. Objective

The objective of this policy is to establish comprehensive security requirements for mobile devices used to access **[Company Name]**'s information systems and data, including both company-owned devices and personal devices used for business purposes (Bring Your Own Device - BYOD). This policy ensures that mobile device usage maintains the confidentiality, integrity, and availability of company information, particularly electronic Protected Health Information (ePHI), while supporting workforce mobility and productivity in compliance with HIPAA, HITECH, and SOC 2 requirements.

2. Scope

This policy applies to all **[Company Name]** workforce members, including employees, contractors, temporary staff, and third parties who use mobile devices to access company information systems, email, applications, or data. It covers all mobile computing devices including smartphones, tablets, laptops, wearable devices, and any other portable computing device capable of storing, processing, or transmitting company information. This policy applies regardless of device ownership (company-owned or personal) and includes both managed and unmanaged device scenarios.

3. Policy

All mobile devices accessing **[Company Name]** information systems and data shall be subject to appropriate security controls to protect against unauthorized access, data loss, and security breaches.

3.1 Mobile Device Classification and Requirements

Mobile devices shall be classified based on their access to company information and subject to corresponding security requirements.

3.1.1 Device Classification Levels

Level 1 - Basic Access: Devices with access only to email and basic business applications

- Standard security configuration required
- Basic mobile device management (MDM) enrollment
- Passcode/PIN protection mandatory

Level 2 - Standard Access: Devices with access to internal systems and Confidential information

- Enhanced security configuration required
- Full MDM enrollment with compliance monitoring
- Multi-factor authentication required
- Encryption mandatory

Level 3 - Restricted Access: Devices with access to ePHI or other Restricted information

- Maximum security configuration required
- Must be company-owned devices only
- Advanced MDM with containerization/app wrapping
- Hardware-based encryption required
- Continuous compliance monitoring
- Dedicated business profile/container

3.1.2 Acceptable Mobile Devices

Only approved mobile device types and operating systems shall be permitted to access company information:

Approved Device Types:

- Smartphones running iOS **[Version, e.g., 15.0]** or later
- Smartphones running Android **[Version, e.g., 11.0]** or later with security patch level within **[Timeframe, e.g., 90 days]**
- Tablets running iPadOS **[Version, e.g., 15.0]** or later
- Tablets running Android **[Version, e.g., 11.0]** or later with security patch level within **[Timeframe, e.g., 90 days]**
- Laptops running Windows **[Version, e.g., 10]** or later with latest security updates
- Laptops running macOS **[Version, e.g., 12.0]** or later with latest security updates

Prohibited Devices:

- The Mobile Device Management (MDM) system shall be configured to automatically block access from devices with modified firmware (jailbroken/rooted devices).
- Devices running unsupported or end-of-life operating systems
- Devices with known critical vulnerabilities that are unpatched
- Personal gaming devices or IoT devices

3.2 Mobile Device Management (MDM)

All mobile devices accessing company information shall be enrolled in the **[Company Name]** Mobile

Device Management system.

3.2.1 MDM Enrollment Requirements

- All devices must be enrolled in MDM before accessing company information
- Device enrollment requires management approval and IT verification
- Users must accept MDM terms and conditions including remote wipe capabilities
- Device compliance must be verified before initial access is granted

3.2.2 MDM Security Policies

The following security policies shall be enforced through MDM:

Device Configuration:

- Minimum passcode/password complexity requirements (must use 6-digits or more for passcodes, gesture-based authentication is not acceptable)
- Automatic screen lock after **[Duration, e.g., 5 minutes]** of inactivity
- Maximum failed unlock attempts before device lock/wipe
- Automatic device encryption enforcement
- Bluetooth and Wi-Fi security restrictions
- Camera and microphone restrictions for high-security areas

Application Management:

- Approved application catalog with pre-approved business applications
- Prohibition of unauthorized application installation
- Automatic application updates for security patches
- Application sandboxing and data isolation
- Mobile application management (MAM) for business applications

Network Security:

- VPN requirements for accessing internal systems
- Prohibition of unsecured Wi-Fi networks for business use
- Corporate Wi-Fi certificate installation and management
- Network traffic monitoring and filtering

3.3 Bring Your Own Device (BYOD) Program

Personal devices may be used for business purposes under the BYOD program with appropriate security controls and user agreements.

3.3.1 BYOD Eligibility and Approval

- BYOD participation requires a formal application and approval process.
- Device compatibility assessment and security evaluation required.
- A signed BYOD agreement is mandatory. This agreement must explicitly state the user's consent to the company's right to enforce all security policies on the device, including the ability to remotely wipe company data and applications.
- Background check requirements for access to Restricted information
- Annual device revalidation and security assessment

3.3.2 BYOD Security Requirements

Mandatory Requirements for all BYOD devices:

- Current operating system with latest security patches
- Strong device passcode/biometric authentication
- Automatic screen lock configuration
- Full device encryption enabled
- Remote wipe capability acceptance
- Separation of business and personal data through containerization

Additional Requirements for Restricted Access:

- Dedicated business profile or secure container application
- Hardware-based key storage for encryption
- Regular malware scanning and threat detection
- Geolocation services for device tracking
- Prohibition of certain high-risk applications

3.3.3 BYOD Data Separation

Business and personal data shall be kept separate on BYOD devices:

- Business applications and data contained within managed workspace
- Personal applications isolated from business environment
- Separate email profiles for business and personal use
- Selective wipe capability for business data only
- Data loss prevention (DLP) controls for business information

3.4 Security Controls and Monitoring

Comprehensive security controls shall be implemented to protect mobile devices and monitor for security threats.

3.4.1 Authentication and Access Controls

- Multi-factor authentication required for all business applications
- Single sign-on (SSO) integration where technically feasible
- Certificate-based authentication for high-security applications
- Regular authentication credential rotation
- Privileged access restrictions for mobile devices

3.4.2 Encryption Requirements

- Full device encryption mandatory for all devices accessing company information
- Data-in-transit encryption using approved protocols (TLS 1.3 or equivalent)
- Application-level encryption for sensitive data storage
- Secure key management for encryption keys
- Hardware security module utilization where available

3.4.3 Monitoring and Threat Detection

- Continuous device compliance monitoring through MDM
- Mobile threat detection and response capabilities
- Anomalous behavior detection and alerting
- Network traffic monitoring for suspicious activity
- Integration with security information and event management (SIEM) systems

3.5 Mobile Application Security

Business applications on mobile devices shall meet specific security requirements.

3.5.1 Application Approval Process

- All mobile applications must be reviewed and approved before installation
- Security assessment of applications including code review and penetration testing
- Vendor security assessments for third-party applications
- Application risk classification and appropriate controls implementation
- Regular application security updates and patch management

3.5.2 Application Security Standards

Mandatory Security Features:

- Local data encryption and secure storage
- Certificate pinning for network communications
- Application sandboxing and isolation
- Secure authentication mechanisms
- Session management and timeout controls
- Anti-tampering and runtime application self-protection (RASP)

3.6 Incident Response and Device Management

Procedures shall be established for responding to mobile device security incidents and managing device lifecycle events.

3.6.1 Lost or Stolen Device Procedures

- All lost or stolen devices must be reported to the IT Security Team immediately, and in no case later than 1 hour after discovery.
- Remote location and tracking attempts
- Remote lock and wipe procedures
- Access credential revocation and reset
- Law enforcement reporting if required
- Incident documentation and lessons learned

3.6.2 Device Lifecycle Management

Device Onboarding:

- Security assessment and approval process
- MDM enrollment and configuration
- User training on security requirements
- Initial compliance verification

Device Maintenance:

- Regular compliance monitoring and reporting
- Security patch management and updates
- Periodic security assessments
- User training and awareness updates

Device Offboarding:

- Complete data wipe and sanitization

- MDM unenrollment and access revocation
- Certificate and credential removal
- Device return procedures (company-owned devices)
- Exit interview and security debriefing

3.7 Privacy and Legal Considerations

Mobile device usage shall balance security requirements with workforce privacy rights and legal obligations.

3.7.1 Privacy Protection

- Clear communication of monitoring capabilities and data access rights
- Separation of business and personal data on BYOD devices
- Limited monitoring to business-related activities
- Data minimization principles for collected information
- Secure disposal of personal information upon employment termination

3.7.2 Legal and Compliance Requirements

- Compliance with employment law and privacy regulations
- Data retention and legal hold requirements for mobile data
- Cross-border data transfer restrictions and compliance
- eDiscovery procedures for mobile device data
- Documentation of security measures for audit purposes

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Information Access Management
3.4.2	HIPAA Security Rule	45 CFR § 164.312(a)(2)(iv) - Encryption

Policy Section	Standard/Framework	Control Reference
3.4.2	HIPAA Security Rule	45 CFR § 164.312(e)(1) - Transmission Security
3.4.1	HIPAA Security Rule	45 CFR § 164.312(a)(1) - Access Control
3.4.3	HIPAA Security Rule	45 CFR § 164.312(b) - Audit Controls
All	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.4.2	SOC 2 Trust Services Criteria	CC6.7 - Data Transmission
3.6.1	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
3.2, 3.4	SOC 2 Trust Services Criteria	CC6.3 - Access Management
All	NIST Cybersecurity Framework	PR.AC-1 - Access Management
3.4.2	NIST Cybersecurity Framework	PR.DS-1 - Data Protection

5. Definitions

Bring Your Own Device (BYOD): A policy allowing employees to use personal devices for business purposes.

Containerization: Technology that separates business and personal data on mobile devices.

Jailbreaking/Rooting: The process of removing software restrictions imposed by the device manufacturer or carrier.

Mobile Application Management (MAM): Software that secures and manages business applications on mobile devices.

Mobile Device Management (MDM): Software that manages, monitors, and secures mobile devices across the organization.

Mobile Threat Detection (MTD): Security technology that identifies and responds to threats targeting mobile devices.

Remote Wipe: The ability to remotely delete data from a mobile device.

Sandboxing: Security mechanism that separates applications and prevents them from accessing unauthorized data.

6. Responsibilities

Role	Responsibility
IT Security Team	Develop mobile security policies, manage MDM systems, monitor device compliance, and respond to mobile security incidents.
IT Support Team	Assist with device enrollment, provide technical support, manage device lifecycle, and maintain MDM configurations.
Privacy Officer	Ensure mobile device usage complies with privacy requirements, oversee BYOD privacy protections, and manage privacy impact assessments.
Human Resources	Integrate mobile security requirements into employment agreements, conduct security training, and manage BYOD program participation.
Legal Team	Review mobile device agreements, ensure compliance with employment law, and manage legal aspects of device monitoring and data access.
Security Incident Response Team	Respond to mobile security incidents, coordinate device recovery procedures, and conduct incident investigations.

Role	Responsibility
Business Unit Managers	Approve mobile device usage for their teams, ensure workforce compliance with mobile security policies, and support incident response activities.
Device Users	Comply with mobile security requirements, maintain device security configurations, promptly report security incidents, and participate in security training.
Application Owners	Ensure mobile applications meet security requirements, coordinate application security testing, and manage application lifecycle.

Data Retention and Disposal Policy (OP-POL-003)

1. Objective

The objective of this policy is to establish comprehensive requirements for the retention, archival, and secure disposal of **[Company Name]**'s information assets throughout their lifecycle. This policy ensures that information is retained for appropriate periods to meet business, legal, and regulatory requirements, particularly for electronic Protected Health Information (ePHI), while ensuring secure disposal when information is no longer needed, in compliance with HIPAA, HITECH, state privacy laws, and SOC 2 requirements.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, and third parties who create, process, store, or dispose of company information. It encompasses all information in any format (electronic, physical, audio, video) and storage medium (databases, file systems, email, backup media, cloud storage, paper documents, optical media). This policy covers all phases of the information lifecycle from creation through final disposition, including active use, archival storage, and secure destruction.

3. Policy

[Company Name] shall implement systematic data retention and disposal practices that balance business needs, legal requirements, regulatory compliance, and security considerations.

3.1 Data Retention Framework

All information assets shall be subject to defined retention periods based on their type, sensitivity, regulatory requirements, and business value. These periods shall be formally documented in the official **[Company Name]** Data Retention Schedule.

3.1.1 Data Retention Schedule

The Records Manager, in coordination with the Retention Committee, shall develop and maintain a formal Data Retention Schedule. This schedule is the official source of truth for all data retention periods and must be reviewed and approved annually by the Retention Committee. The schedule shall, at a minimum, categorize data types and assign a specific, non-ambiguous retention period for each. Examples of categories include:

- **Corporate Governance:** Records related to the legal and operational structure of the company.
- **Financial and Tax:** Records required for financial reporting and tax compliance.
- **Personnel Records:** Information related to employees and human resources.
- **Contracts and Agreements:** Legal agreements with customers, vendors, and partners.
- **Electronic Protected Health Information (ePHI):** Health data subject to HIPAA and state laws.
- **Operational Data:** General business records, correspondence, and system data.

3.1.2 Electronic Protected Health Information (ePHI) Retention

ePHI shall be retained in accordance with HIPAA requirements and applicable state laws, as specified in the Data Retention Schedule:

- **Minimum Retention Period:** All policies, procedures, and other documentation required by the HIPAA Security Rule must be retained for a minimum of six (6) years from the date of their creation or the date when they were last in effect, whichever is later. State-specific laws may require longer retention periods.
- **Extended Retention:** ePHI for minors shall be retained in accordance with applicable state laws, as documented in the Data Retention Schedule.
- **Research Records:** ePHI used in research retained per research protocol requirements
- **Legal Hold:** ePHI subject to litigation hold retained until legal matter resolution
- **State Requirements:** Compliance with state-specific retention requirements where more stringent

3.1.3 Backup and Archive Retention

- **Operational Backups:** Retained for **[Duration, e.g., 30 days]** for immediate recovery needs
- **Monthly Archives:** Retained for **[Duration, e.g., 12 months]** for historical recovery
- **Annual Archives:** Retained per data classification retention requirements
- **Legal Hold Archives:** Retained until legal matter resolution and hold release
- **Disaster Recovery Archives:** Maintained at geographically separate locations

3.2 Legal Hold and Litigation Support

Special procedures shall govern information retention when legal proceedings are anticipated or active.

3.2.1 Legal Hold Procedures

- Legal hold notices shall be issued immediately upon notification of potential litigation
- All relevant custodians shall be notified and acknowledge receipt of legal hold instructions
- Automated deletion processes shall be suspended for information subject to legal hold
- Legal hold inventory shall be maintained documenting preserved information
- Regular legal hold reminders shall be sent to ensure ongoing compliance

3.2.2 eDiscovery Support

- Information systems shall be capable of identifying, preserving, and producing relevant information
- Search and collection capabilities shall be maintained for electronic information
- Chain of custody procedures shall be followed for all collected information
- Metadata preservation shall be maintained during collection and production processes
- Privileged information shall be identified and protected during discovery processes

3.3 Data Disposal Framework

Information shall be securely disposed of when retention periods expire or when no longer needed for business purposes.

3.3.1 Disposal Triggers

Information disposal shall be triggered by:

- Expiration of defined retention periods
- Completion of business processes requiring the information
- System decommissioning or migration activities
- Employee termination (personal information only)
- Contract termination with appropriate notice periods
- Legal hold release after litigation conclusion

3.3.2 Disposal Classification Requirements

Disposal methods shall correspond to information sensitivity levels:

Public Information:

- Standard deletion or disposal methods acceptable
- No special security requirements
- Standard recycling procedures for physical media

Internal Information:

- Secure deletion using approved software tools
- Physical media shredding or incineration
- Verification of deletion completion

Confidential Information:

- Cryptographic erasure or secure overwriting (minimum 3 passes)
- Cross-cut shredding for physical documents
- Degaussing for magnetic media
- Certificate of destruction required for third-party disposal

Restricted Information (including ePHI):

- Cryptographic erasure using approved methods
- Physical destruction for all storage media
- Witnessed destruction with certificates of completion
- Chain of custody documentation throughout disposal process
- Hardware Security Module (HSM) secure deletion for cryptographic keys

3.4 Secure Disposal Methods

Specific disposal methods shall be employed based on media type and information sensitivity.

3.4.1 Electronic Media Disposal

Hard Disk Drives:

- Software-based secure deletion using NIST SP 800-88 approved methods
- Cryptographic erasure where full disk encryption is implemented
- Physical destruction for Restricted information or failed drives
- Degaussing using approved degaussing equipment

Solid State Drives (SSDs):

- Cryptographic erasure preferred method
- Manufacturer secure erase commands
- Physical destruction for high-sensitivity information
- Verification of successful deletion

Removable Media:

- Physical destruction for all Confidential and Restricted information

- Secure overwriting for reusable media containing less sensitive information
- Degaussing for magnetic media (tapes, floppy disks)

Mobile Devices:

- Factory reset combined with encryption
- Physical destruction of storage components for Restricted information
- Remote wipe verification for lost or stolen devices
- Removal of SIM cards and memory cards

3.4.2 Physical Document Disposal

- Cross-cut shredding with particle size **[Size, e.g., 4mm x 32mm]** or smaller
- Incineration for highly sensitive documents
- Pulping for large volumes of confidential documents
- Witnessed destruction for Restricted information

3.4.3 Cloud Data Disposal

- Cryptographic erasure using customer-managed encryption keys
- Verification of data deletion from all storage tiers and backups
- Certificate of deletion from cloud service providers
- Contractual guarantees for secure disposal processes

3.5 Disposal Documentation and Verification

All disposal activities shall be documented and verified to ensure completeness and compliance.

3.5.1 Documentation Requirements

Disposal records shall include:

- Description of information or systems disposed
- Disposal method used and justification
- Date and time of disposal activities
- Personnel involved in disposal process
- Verification of successful disposal
- Certificates of destruction from third-party vendors
- Chain of custody documentation

3.5.2 Verification Procedures

- Independent verification of disposal completion
- Random sampling and testing of disposal processes
- Third-party validation for high-sensitivity disposals
- Photographic evidence for physical destruction
- Digital signatures for electronic disposal certificates

3.6 Third-Party Disposal Services

External disposal services shall meet **[Company Name]** security requirements and provide appropriate assurances.

3.6.1 Vendor Requirements

- Security assessment and approval before engagement
- Appropriate certifications (e.g., NAID AAA, R2, e-Stewards)
- Comprehensive insurance coverage for data breaches
- Signed confidentiality and security agreements
- On-site destruction capabilities or secure chain of custody

3.6.2 Vendor Oversight

- Regular audits of disposal vendor processes
- Witness disposal activities for high-sensitivity information
- Validation of certificates of destruction
- Incident reporting requirements for disposal failures
- Performance monitoring and contract compliance reviews

3.7 Data Retention Governance

Formal governance processes shall ensure consistent application of retention and disposal policies.

3.7.1 Retention Committee

- A cross-functional committee including Legal, Compliance, IT, and Records Management shall be maintained.
- The committee shall meet at least quarterly to review retention and disposal activities.
- The committee is responsible for the annual review and formal approval of the Data Retention Schedule and this policy.
- Resolution of retention conflicts and exceptions
- Approval of retention schedule modifications

3.7.2 Records Management Program

- A designated Records Manager shall be responsible for program oversight.
- The Records Manager is responsible for the maintenance, accuracy, and communication of the official Data Retention Schedule.
- Training programs for workforce members
- Compliance monitoring and reporting
- Technology solutions for automated retention management

3.8 Monitoring and Compliance

Regular monitoring shall ensure adherence to retention and disposal requirements.

3.8.1 Compliance Monitoring

- Automated monitoring of retention periods and disposal triggers
- Regular audits of disposal activities and documentation
- Compliance reporting to management and regulators
- Exception reporting and corrective action procedures
- Key performance indicators (KPIs) for retention and disposal programs

3.8.2 Training and Awareness

- Annual training on retention and disposal requirements
- Role-specific training for records custodians
- New employee orientation including retention policies
- Regular communications on policy updates
- Testing and validation of training effectiveness

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
3.1.2	HIPAA Security Rule	45 CFR § 164.308(a)(4)(ii)(A) - Information Access Management

Policy Section	Standard/Framework	Control Reference
3.3, 3.4	HIPAA Security Rule	45 CFR § 164.310(d)(2)(i) - Media Disposal
3.1.2	HIPAA Privacy Rule	45 CFR § 164.530(j)(2) - Record Retention
3.4	NIST SP 800-88	Guidelines for Media Sanitization
All	SOC 2 Trust Services Criteria	CC6.5 - Data Disposal
3.7	SOC 2 Trust Services Criteria	CC2.1 - Communication and Information
3.8	SOC 2 Trust Services Criteria	CC4.1 - Monitoring Activities
All	ISO/IEC 27001:2022	A.8.3 - Media Handling

5. Definitions

Chain of Custody: Documentation of the chronological transfer of evidence or information from collection to disposal.

Cryptographic Erasure: Data destruction method that renders data unrecoverable by destroying encryption keys.

Degaussing: Process of reducing or eliminating magnetic fields from magnetic storage media.

eDiscovery: Process of identifying, preserving, and producing electronically stored information for legal proceedings.

Legal Hold: Suspension of normal records disposal to preserve information that may be relevant to litigation.

Media Sanitization: Process of removing information from storage media such that recovery is not feasible.

Retention Schedule: Documented plan specifying how long different types of records should be kept.

Secure Deletion: Method of data destruction that makes recovery of deleted data infeasible.

6. Responsibilities

Role	Responsibility
Records Manager	Develop and maintain retention schedules, oversee disposal activities, coordinate legal holds, and ensure compliance with retention policies.
Legal Team	Establish legal retention requirements, issue legal hold notices, support eDiscovery activities, and ensure compliance with legal obligations.
Privacy Officer	Ensure ePHI retention complies with HIPAA requirements, oversee privacy-related disposals, and coordinate with legal team on privacy matters.
IT Security Team	Implement secure disposal technologies, verify disposal completion, manage disposal vendors, and ensure security of disposal processes.
System Administrators	Execute disposal procedures, maintain disposal documentation, implement automated retention controls, and support legal hold activities.
Information Owners	Determine business retention requirements, approve disposal activities, participate in retention reviews, and ensure appropriate information handling.
Compliance Team	Monitor retention compliance, conduct disposal audits, report compliance status, and coordinate regulatory requirements.
All Workforce Members	Comply with retention requirements, participate in legal holds, properly dispose of information, and report retention violations.

Role	Responsibility
Audit Team	Conduct retention and disposal audits, validate compliance with policies, review disposal documentation, and report audit findings.

Legal Hold: Suspension of normal records disposal to preserve information that may be relevant to litigation.

Media Sanitization: Process of removing information from storage media such that recovery is not feasible.

Retention Schedule: Documented plan specifying how long different types of records should be kept.

Secure Deletion: Method of data destruction that makes recovery of deleted data infeasible.

6. Responsibilities

Role	Responsibility
Records Manager	Develop and maintain retention schedules, oversee disposal activities, coordinate legal holds, and ensure compliance with retention policies.
Legal Team	Establish legal retention requirements, issue legal hold notices, support eDiscovery activities, and ensure compliance with legal obligations.
Privacy Officer	Ensure ePHI retention complies with HIPAA requirements, oversee privacy-related disposals, and coordinate with legal team on privacy matters.
IT Security Team	Implement secure disposal technologies, verify disposal completion, manage disposal vendors, and ensure security of disposal processes.

Role	Responsibility
System Administrators	Execute disposal procedures, maintain disposal documentation, implement automated retention controls, and support legal hold activities.
Information Owners	Determine business retention requirements, approve disposal activities, participate in retention reviews, and ensure appropriate information handling.
Compliance Team	Monitor retention compliance, conduct disposal audits, report compliance status, and coordinate regulatory requirements.
All Workforce Members	Comply with retention requirements, participate in legal holds, properly dispose of information, and report retention violations.
Audit Team	Conduct retention and disposal audits, validate compliance with policies, review disposal documentation, and report audit findings.

Human Resources Security Policy (OP-POL-004)

1. Objective

The objective of this policy is to define the security requirements and procedures that govern the lifecycle of all **[Company Name]** workforce members. This policy ensures that individuals with access to sensitive company information, including electronic Protected Health Information (ePHI), are trustworthy, properly trained, and managed in a way that minimizes insider risk and upholds the company's commitment to security and compliance.

2. Scope

This policy applies to all prospective, current, and former workforce members of **[Company Name]**, including full-time and part-time employees, contractors, and temporary staff. It covers all stages of the employment lifecycle, from pre-employment screening through termination and separation.

3. Policy

[Company Name] shall implement and maintain procedures to ensure that the workforce is managed securely and in accordance with all applicable legal and regulatory requirements.

3.1 Screening and Background Checks

To ensure a trusted workforce, all candidates for employment or engagement must undergo a formal screening process before being granted access to company information assets.

- **Contingent Offers:** All offers of employment or contract are contingent upon the successful completion of a background check, conducted by a company-approved third-party provider.
- **Scope of Checks:** The standard background check includes, at a minimum, identity verification, a criminal history check, and employment history verification, in accordance with applicable local, state, and federal laws. For roles with elevated access to financial or sensitive data, additional checks (e.g., credit history) may be required.
- **Adverse Findings:** Any adverse findings from a background check will be reviewed by the Human Resources Department and the Security Officer to determine eligibility for employment based on the nature of the finding and the requirements of the role.

3.2 Onboarding and Security Training

Upon joining the company, all new workforce members must complete a formal onboarding process to ensure they understand their security responsibilities.

- **Confidentiality Agreements:** All new workforce members must sign a Confidentiality and Non-Disclosure Agreement as a condition of their employment or engagement.
- **Security Awareness Training:** New workforce members must complete the mandatory security and privacy awareness training within **[Number, e.g., 30]** days of their start date.
- **Access Provisioning:** Access to systems and data will be provisioned in accordance with the Access Control Policy (SEC-POL-001), based on the principle of least privilege.

3.3 Termination and Separation

A formal process must be followed to ensure a secure and orderly separation when a workforce member leaves the company, regardless of the reason.

- **Notification:** Managers must immediately notify the Human Resources and IT Departments of any voluntary or involuntary termination.
- **Revocation of Access:** All logical and physical access rights must be promptly revoked upon termination, as defined in the Access Control Policy (SEC-POL-001).
- **Return of Assets:** The departing workforce member is required to return all company-owned property, including laptops, mobile devices, access badges, and any documents containing sensitive information. The Human Resources Department is responsible for tracking and confirming the return of all assets.
- **Exit Interview:** Where appropriate, the Human Resources Department will conduct an exit interview to remind the departing workforce member of their ongoing confidentiality obligations.

3.4 Sanction Policy

Failure to comply with **[Company Name]**'s information security policies may result in disciplinary action.

- **Framework:** A formal sanction policy shall be maintained to address violations of the ISMS policies. This framework ensures that disciplinary actions are fair, consistent, and commensurate with the severity of the violation.
- **Disciplinary Actions:** Sanctions may range from verbal or written warnings and mandatory

retraining to suspension, termination of employment, and, where applicable, civil or criminal legal action.

- **Documentation:** All policy violations and the resulting sanctions must be formally documented by the Human Resources Department in consultation with the workforce member's manager and the Security Officer.

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framewc	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(3)(i) - Workforce Security
3.3	HIPAA Security Rule	45 CFR § 164.308(a)(3)(ii)(C) - Termination Procedures
3.4	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(C) - Sanction Policy
3.1, 3.2	SOC 2 Trust Services Criteria	CC2.1 - The entity establishes and communicates the importance of integrity and ethical values…
3.1, 3.2	SOC 2 Trust Services Criteria	CC2.2 - The board of directors and management establish a commitment to competence…

5. Definitions

- **Workforce Member:** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for **[Company Name]**, is under the direct control of the company, whether or not they are paid by the company.
- **Background Check:** A process of verifying the identity and credentials of a candidate for employment, which may include criminal history, employment verification, and other checks as permitted by law.
- **Sanction:** A penalty or disciplinary action imposed for violating a rule or policy.

6. Responsibilities

Role	Responsibility
Human Resources Department	Own, review, and update this policy annually. Manage the screening, onboarding, and termination processes. Administer the sanction policy in consultation with management.
Security Officer / Team	Advise on the security aspects of HR processes, including background checks and termination procedures. Participate in the investigation of security policy violations.
Managers	Ensure their direct reports complete all required security training. Promptly notify HR of all terminations. Participate in the enforcement of the sanction policy.
All Workforce Members	Comply with all information security policies. Report any suspected policy violations to their manager or the Security Officer.

Acceptable Software and Browser Extension Policy (OP-POL-005)

1. Objective The objective of this policy is to establish clear guidelines for the installation and use of all third-party software, applications, and browser extensions on company-managed endpoints. This policy is designed to protect [Company Name] from security risks, including malware, data leakage, and privacy breaches, while enabling workforce members to use legitimate tools that enhance productivity.

2. Scope This policy applies to all [Company Name] workforce members (including employees, contractors, and temporary staff) and any third party using a company-managed endpoint. It covers all software, including desktop applications, command-line tools, and browser extensions, installed on any company-owned or managed device, such as laptops and workstations.

3. Policy All software installed on company endpoints must be properly licensed, have a valid business justification, and be approved in accordance with the procedures outlined in this policy. The principle of least functionality shall be applied, meaning only necessary software should be installed.

3.1 Software Governance Model

[Company Name] employs a hybrid governance model to manage software risk effectively:

- **Allowlist (for High-Risk Software):** Software and browser extensions that require elevated privileges or access to sensitive data (e.g., ePHI, Confidential data) must be explicitly approved and listed on the company's official **Software Allowlist**. Any software not on this list is implicitly denied.
- **Blocklist (for Prohibited Software):** Certain categories of software are explicitly prohibited and are maintained on a **Software Blocklist**.

3.2 Software Approval Process

Workforce members who wish to install software that is not already on the Software Allowlist must submit a formal request.

- **Request Submission:** A request must be submitted via an IT support ticket, detailing the software's name, purpose, and a justification for its business use.
- **Security Review:** The Security Team will conduct a risk assessment of the requested software.

The assessment will consider the software's function, the data it will access, its vendor's reputation, and any known vulnerabilities.

- **Approval or Denial:** Based on the risk assessment, the Security Team will either approve or deny the request. Approved software will be added to the Software Allowlist. The decision will be documented in the IT ticket.

3.3 Prohibited Software Categories

The installation and use of software in the following categories are strictly prohibited on any company endpoint:

- Unlicensed or pirated software ("warez").
- Peer-to-peer (P2P) file-sharing clients.
- Cryptocurrency mining software.
- Tools designed to disable or circumvent security controls (e.g., password crackers, security tool disablers).
- Any software from untrusted or unverified sources.
- Software that collects or transmits sensitive data without explicit user consent or knowledge.
- Software that is known to have significant security vulnerabilities or is no longer supported by the vendor.

3.4 Browser Extension Security

Browser extensions pose a unique risk and are subject to heightened scrutiny.

- **High-Risk Permissions:** Extensions that request broad permissions (e.g., "Read and change all your data on the websites you visit") require a formal risk assessment and must be on the Software Allowlist before installation.
- **Source:** All extensions must be installed from official, reputable browser web stores (e.g., Chrome Web Store, Firefox Add-ons).
- **Review and Removal:** The Security Team will periodically review installed browser extensions for compliance with this policy. Extensions that no longer meet security standards or are deemed unnecessary will be removed.

- **End-of-Life Extensions:** Extensions that are no longer maintained or updated by the vendor will be removed from all company endpoints to mitigate security risks.

3.5 Auditing and Enforcement

The IT Department will use endpoint management tools to enforce this policy and maintain system integrity.

- **Automated Audits:** Regular, automated scans of all company endpoints will be conducted to inventory installed software and check for compliance with this policy.
- **Remote Removal:** [Company Name] reserves the right to remotely remove any unauthorized, prohibited, or non-compliant software from a company-managed endpoint without prior notice to the user.
- **Policy Violations:** The discovery of prohibited or unauthorized software may result in disciplinary action, in accordance with the `Security Policy Sanction Procedure (OP-PROC-008)`.

4. Standards Compliance This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Frame	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(B) - Risk Management
3.1, 3.3	HIPAA Security Rule	45 CFR § 164.308(a)(5)(ii)(B) - Protection from Malicious Software
All	SOC 2 Trust Services Criteria	CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software.
3.5	SOC 2 Trust Services Criteria	CC7.1 - The entity uses detection and monitoring procedures to identify changes… that are indicative of a control failure.

5. Definitions

- **Endpoint:** Any company-owned or managed computing device, such as a laptop or workstation.
- **Software Allowlist:** An official, centrally managed list of all software and browser extensions that have been vetted and are approved for installation on company endpoints.
- **Software Blocklist:** An official list of specific software applications or categories that are explicitly forbidden from being installed on company endpoints.
- **Shadow IT:** Technology, software, or services used inside an organization without explicit organizational approval.

6. Responsibilities

Role	Responsibility
Security Team	Own, review, and update this policy annually. Conduct risk assessments for new software requests and maintain the Allowlist and Blocklist.
IT Department	Implement and manage the technical controls to enforce this policy, including endpoint management tools. Process software requests and perform remote removal of non-compliant software.
Managers	Ensure their direct reports understand and adhere to this policy.
All Workforce Members	Comply with this policy at all times. Request approval for new software as required and refrain from installing prohibited software.

Cryptographic Key Lifecycle Management Procedure (OP-PROC-001)

1. Purpose

To provide the technical steps for the secure generation, distribution, storage, rotation, and destruction of cryptographic keys.

2. Scope

This procedure applies to all cryptographic keys used to protect company and customer data, including keys used for data at rest and data in transit encryption. It applies to all personnel involved in the management of cryptographic keys.

3. Overview

This procedure outlines the secure lifecycle management of cryptographic keys, from generation to destruction. It ensures that all cryptographic keys are handled in a secure manner, using approved hardware security modules (HSMs) and secure channels, with all actions logged for audit purposes.

4. Procedure

4.1 Key Generation

Step	Who	What
1	Security Engineering Team	Generate cryptographic keys using the company's approved Hardware Security Module (HSM) to ensure randomness and security.
2	Security Engineering Team	Ensure key strength meets the requirements defined in the Encryption and Key Management Policy (e.g., AES-256 or stronger).
3	Security Engineering Team	Log the generation event in the key management system, including the key identifier, generation time, and responsible personnel.

4.2 Key Distribution

Step	Who	What
1	Security Engineering Team	Distribute keys to systems or services requiring them using secure, encrypted channels (e.g., TLS-protected connections).
2	Security Engineering Team	Never transmit keys in plaintext or through insecure methods like email.
3	Security Engineering Team	Log the distribution event, noting the recipient system/service and timestamp.

4.3 Key Storage

Step	Who	What
1	Security Engineering Team	Store all cryptographic keys in the approved Hardware Security Module (HSM) or a secure, encrypted key vault.
2	Security Engineering Team	Implement strict access controls to the key storage system, limiting access to authorized personnel only.
3	Security Engineering Team	Ensure that key storage systems are physically and logically secured and monitored.

4.4 Key Rotation

Step	Who	What
1	Security Engineering Team	Rotate cryptographic keys at least annually, or more frequently if required by policy or regulation.
2	Security Engineering Team	Generate a new key and securely distribute it to all relevant systems.
3	Security Engineering Team	Deactivate the old key but retain it in a secure state for a defined period to decrypt previously encrypted data if needed.
4	Security Engineering Team	Log the rotation event, including the identifiers for both the old and new keys.

4.5 Key Destruction

Step	Who	What
1	Security Engineering Team	When a key is no longer needed and its retention period has expired, securely destroy it using the key management system’s functions.
2	Security Engineering Team	Ensure the destruction process is irreversible (e.g., cryptographic erasure).
3	Security Engineering Team	Log the destruction event, including the key identifier and destruction timestamp.

5. Standards Compliance

This section maps the procedure steps to specific controls from relevant information security standards.

Procedure Step(s)	Standard/Framework	Control Reference
4.1-4.5	SOC 2	CC6.1, CC6.8
4.1-4.5	HIPAA Security Rule	45 CFR § 164.312(a)(2)(iv)
4.1-4.5	HIPAA Security Rule	45 CFR § 164.312(e)(2)(ii)

6. Artifact(s)

An auditable log entry in the key management system for every lifecycle action (generation, distribution, storage, rotation, destruction).

7. Definitions

HSM (Hardware Security Module): A physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.

Key Lifecycle: The complete process of managing a cryptographic key from its creation through to its eventual destruction.

8. Responsibilities

Role	Responsibility
Security Engineering Team	Responsible for executing all phases of the key lifecycle management procedure.
Security Officer	Responsible for overseeing the key management program and ensuring compliance.

Mobile Device Onboarding and Security Configuration Procedure (OP-PROC-002)

1. Purpose

To detail the steps for enrolling a new or personal device in the Mobile Device Management (MDM) system and ensuring it meets all security configuration requirements before being granted access to company resources.

2. Scope

This procedure applies to all employees, contractors, and other authorized users who wish to use a personal or company-issued mobile device to access company data or systems.

3. Overview

This procedure describes the process for onboarding a mobile device, from obtaining management approval to final verification of security compliance. It ensures that all devices connecting to the corporate network are properly managed and secured, minimizing the risk of data loss or unauthorized access.

4. Procedure

Step	Who	What
1	User	Submits a request to their manager for approval to use a mobile device for business purposes.
2	Manager	Reviews the request. If approved, forwards the approval to the IT Security Team.
3	IT Security Team	Provides the user with instructions for enrolling their device into the company's Mobile Device Management (MDM) solution.
4	User	Enrolls their device in the MDM system and accepts the company's terms and conditions for mobile device usage.

Step	Who	What
5	MDM System (Automated)	Automatically scans the device to verify compliance with all required security policies, including passcode complexity, device encryption, and OS version.
6	IT Security Team	Reviews the compliance report from the MDM system. If the device is compliant, grants the device access to the approved company resources.
7	IT Security Team	If the device is not compliant, notifies the user of the specific remediation steps required. Access is denied until the device meets all security requirements.

5. Standards Compliance

This section maps the procedure steps to specific controls from relevant information security standards.

Procedure Step(s)	Standard/Framework	Control Reference
1-7	SOC 2	CC6.1, CC6.3
1-7	HIPAA Security Rule	45 CFR § 164.312(a)(1)

6. Artifact(s)

A record of MDM enrollment and a compliance verification report stored within the MDM system.

7. Definitions

MDM (Mobile Device Management): Software that allows an organization to secure, monitor, and manage mobile devices, such as smartphones and tablets.

BYOD (Bring Your Own Device): A policy that allows employees to use their personal devices for work-related purposes.

8. Responsibilities

Role	Responsibility
User	Responsible for requesting approval, enrolling their device, and ensuring it remains compliant with policies.
Manager	Responsible for approving or denying requests for mobile device usage for their direct reports.
IT Security Team	Responsible for managing the MDM system, providing enrollment instructions, and verifying device compliance.

Lost or Stolen Mobile Device Response Procedure (OP-PROC-003)

1. Purpose

To provide the immediate steps a user and the IT Security Team must take when a mobile device used for company business is reported lost or stolen.

2. Scope

This procedure applies to all users of company-issued or personal mobile devices (BYOD) that are enrolled in the company's Mobile Device Management (MDM) system.

3. Overview

This procedure details the rapid response actions required to mitigate the security risk arising from a lost or stolen mobile device. The primary goals are to protect company data by remotely locking and wiping the device and to prevent unauthorized access by revoking associated credentials.

4. Procedure

Step	Who	What
1	User	Immediately (within 1 hour of discovery) reports the lost or stolen device to the IT Security Team through the designated emergency contact channel.
2	IT Security Team	Upon receiving the report, immediately initiates the remote lock command via the MDM system to prevent access to the device.
3	IT Security Team	Initiates the remote wipe command via the MDM system to erase all corporate data from the device.
4	IT Security Team	Immediately revokes all access credentials associated with the device, including disabling the user's primary account, VPN access, and any application-specific passwords.
5	IT Security Team	Creates a formal incident report to document the event, the actions taken, and the outcome.

5. Standards Compliance

This section maps the procedure steps to specific controls from relevant information security standards.

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2	CC7.1
1-5	HIPAA Security Rule	45 CFR § 164.310(d)(1)

6. Artifact(s)

A completed incident report documenting the loss/theft, response actions, and resolution.

7. Definitions

Remote Lock: A feature of MDM software that allows an administrator to remotely make a device inaccessible.

Remote Wipe: A feature of MDM software that allows an administrator to remotely delete all data from a device.

8. Responsibilities

Role	Responsibility
User	Responsible for the timely reporting of a lost or stolen device.
IT Security Team	Responsible for executing the remote lock and wipe procedures, revoking credentials, and documenting the incident.

Secure Media Disposal and Sanitization Procedure (OP-PROC-004)

1. Purpose

To provide step-by-step instructions for securely destroying or sanitizing different types of electronic media and physical documents to prevent the unauthorized disclosure of sensitive information.

2. Scope

This procedure applies to all company-owned and managed media, both electronic and physical, that contains company or customer data. This includes, but is not limited to, hard drives, solid-state drives (SSDs), USB drives, backup tapes, mobile devices, and paper documents.

3. Overview

This procedure outlines the required methods for disposing of or sanitizing media based on the classification level of the data it contains. It ensures that all sensitive information is rendered unrecoverable, in compliance with regulatory and industry standards.

4. Procedure

4.1 Electronic Media (Hard Drives, SSDs)

Step	Who	What
1	Asset Custodian / IT Team	Identify media that is at the end of its lifecycle or is being decommissioned.
2	IT Team	For media containing **Confidential** or **Restricted** data, perform cryptographic erasure according to NIST SP 800-88 guidelines.
3	IT Team	For media that cannot be cryptographically erased, or for media containing the most sensitive **Restricted** data, physically destroy the media (e.g., shredding, degaussing).
4	IT Team	Document the disposal method, date, and personnel involved in the asset management system. If a third-party vendor is used, obtain and file a certificate of destruction.

4.2 Paper Documents

Step	Who	What
1	All Employees	Identify paper documents containing **Confidential** or **Restricted** information that are no longer needed.
2	All Employees	Place documents in designated secure shredding bins provided throughout the office.
3	Approved Disposal Vendor	The approved vendor collects the contents of the shredding bins on a scheduled basis for secure, off-site destruction.
4	Facilities / IT Team	Obtain and file the certificate of destruction provided by the vendor.

5. Standards Compliance

This section maps the procedure steps to specific controls from relevant information security standards.

Procedure Step(s)	Standard/Framework	Control Reference
4.1-4.2	SOC 2	CC6.5
4.1	NIST	SP 800-88
4.1-4.2	HIPAA Security Rule	45 CFR § 164.310(d)(2)(i)

6. Artifact(s)

A completed disposal record in the asset management system or a certificate of destruction from a third-party vendor.

7. Definitions

Cryptographic Erasure: The process of using encryption software to render targeted data on a storage device unreadable.

Degaussing: The process of reducing or eliminating an unwanted magnetic field (or data) stored on tape and disk media.

Physical Destruction: The process of rendering media unusable and its data unrecoverable by physically altering it (e.g., shredding, pulverizing).

8. Responsibilities

Role	Responsibility
IT Team	Responsible for the secure sanitization and destruction of electronic media and for managing disposal vendors.
All Employees	Responsible for properly disposing of sensitive paper documents in the provided secure shred bins.
Approved Disposal Vendor	Responsible for the secure collection and destruction of media and providing certificates of destruction.

Legal Hold Procedure (OP-PROC-005)

1. Purpose

To outline the steps for issuing, tracking, and releasing a legal hold on information that is relevant to reasonably anticipated or actual litigation, government investigation, or audit.

2. Scope

This procedure applies to all employees and systems where company data is stored. It covers all forms of information, including electronic documents, emails, databases, and physical records.

3. Overview

This procedure ensures that all potentially relevant information is preserved and protected from destruction or modification when the company is notified of a legal action. It details the formal process managed by the Legal team to suspend normal data retention and disposal schedules for the duration of the legal matter.

4. Procedure

Step	Who	What
1	Legal Team	Identifies the need for a legal hold based on notification of a lawsuit, investigation, or other legal dispute.
2	Legal Team	Issues a formal Legal Hold Notice to all relevant employees (custodians) and system administrators. The notice specifies the subject matter and the scope of the data to be preserved.
3	IT Team	Upon receipt of the notice, suspends all automated deletion and data disposal processes for the identified data and systems.
4	Custodians	Acknowledge receipt of the hold notice and take necessary steps to preserve all relevant information under their control.
5	Legal Team	Maintains an inventory of all data subject to the hold and sends periodic reminders to custodians to ensure ongoing compliance.

Step	Who	What
6	Legal Team	When the legal matter is fully resolved, issues a formal Hold Release Notice to all custodians and the IT team, authorizing the resumption of normal data retention policies.

5. Standards Compliance

This section maps the procedure steps to specific controls from relevant information security standards.

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2	CC2.1

6. Artifact(s)

- A formal Legal Hold Notice, including a list of custodians.
- A formal Hold Release Notice.
- Acknowledgement receipts from custodians.

7. Definitions

Legal Hold: A process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated.

Custodian: An individual who has possession, custody, or control of potentially relevant information.

8. Responsibilities

Role	Responsibility
Legal Team	Responsible for identifying the need for a legal hold, issuing notices, tracking compliance, and releasing the hold.

Role	Responsibility
IT Team	Responsible for implementing the technical measures required to suspend data disposal for the information on hold.
Custodians	Responsible for preserving all information relevant to the legal hold notice.

Workforce Screening and Background Check Procedure (OP-PROC-006)

1. Purpose

To outline the formal process for conducting required background checks on all candidates for employment to verify their qualifications and identify any potential security risks.

2. Scope

This procedure applies to all prospective employees, contractors, and temporary staff who are extended a contingent offer of employment or engagement with the company.

3. Overview

This procedure ensures that all individuals with access to company information and systems undergo appropriate screening before their employment begins. It describes the steps for obtaining consent, conducting the check through an approved third-party provider, and reviewing the results to make a final hiring decision.

4. Procedure

Step	Who	What
1	Human Resources (HR)	Extends a contingent offer of employment to the selected candidate. The offer explicitly states that employment is conditional upon the successful completion of a background check.
2	Candidate	Receives the contingent offer and provides written consent for the company to conduct a background check via the approved third-party screening provider.
3	Third-Party Provider	Conducts the background check, which may include criminal history, employment verification, and education verification, in accordance with applicable laws.

Step	Who	What
4	Human Resources (HR) & Security Officer	Receive and review the background check report from the provider.
5	Human Resources (HR) & Security Officer	If the report contains adverse findings, they jointly review the findings to determine if they pose an unacceptable risk and would disqualify the candidate from employment.
6	Human Resources (HR)	If the check is passed, confirms the final offer of employment. If the check is not passed, follows legal requirements for adverse action.
7	Human Resources (HR)	Documents the completed background check in the candidate's confidential personnel file.

5. Standards Compliance

This section maps the procedure steps to specific controls from relevant information security standards.

Procedure Step(s)	Standard/Framework	Control Reference
1-7	SOC 2	CC2.1, CC2.2
1-7	HIPAA Security Rule	45 CFR § 164.308(a)(3)(i)

6. Artifact(s)

A completed background check report and the candidate's consent form, stored securely in the employee's confidential HR file.

7. Definitions

Contingent Offer: An offer of employment that is dependent on the successful fulfillment of certain conditions, such as a background check or drug screening.

Adverse Findings: Information discovered during a background check that could negatively impact a hiring decision (e.g., a criminal conviction).

8. Responsibilities

Role	Responsibility
Human Resources (HR)	Responsible for managing the overall background check process, including making offers, obtaining consent, and maintaining records.
Security Officer	Responsible for reviewing adverse findings in background checks to assess potential security risks.
Candidate	Responsible for providing consent for the background check and providing accurate information.
Third-Party Provider	Responsible for conducting the background check in a legally compliant manner and providing a report of the findings.

Employee Onboarding and Offboarding Security Procedure (OP-PROC-007)

1. Purpose

To provide a formal checklist and process to ensure all security-related tasks are consistently and verifiably completed during employee onboarding and termination.

2. Scope

This procedure applies to all new and departing employees, contractors, and temporary staff. It involves the Human Resources (HR) department, the IT department, and the hiring manager.

3. Overview

This procedure establishes standardized checklists for the security-related aspects of employee onboarding and offboarding. The onboarding process ensures new hires are properly provisioned, trained, and aware of their security responsibilities. The offboarding process ensures timely revocation of access and return of company assets to prevent unauthorized access after departure.

4. Procedure

4.1 Onboarding

Step	Who	What
1	Human Resources (HR)	Initiates the onboarding process upon a candidate's acceptance of an offer.
2	New Hire	Signs the Confidentiality and Non-Disclosure Agreement (NDA) and the Acceptable Use Policy (AUP) as part of their employment agreement.
3	IT Department	Provisions user accounts, access credentials, and necessary hardware based on the role defined by the hiring manager.
4	New Hire	Completes the mandatory security awareness training within the first week of employment.

Step	Who	What
5	Hiring Manager & HR	Complete and sign the onboarding checklist, verifying all steps have been completed. The checklist is filed in the employee's HR record.

4.2 Offboarding

Step	Who	What
1	Manager / HR	Immediately notifies the IT department of the employee's departure, providing the exact time and date of termination.
2	IT Department	Immediately upon notification, revokes all physical and logical access, including disabling user accounts, VPN access, and email.
3	Departing Employee & Manager	The departing employee returns all company assets, including laptops, mobile devices, and security badges, to their manager. The manager verifies the return of all items.
4	Manager & HR	Complete and sign the offboarding checklist, verifying all access has been revoked and all assets have been returned. The checklist is filed in the employee's HR record.

5. Standards Compliance

This section maps the procedure steps to specific controls from relevant information security standards.

Procedure Step(s)	Standard/Framework	Control Reference
4.1-4.2	HIPAA Security Rule	45 CFR § 164.308(a)(3)(i)
4.2	HIPAA Security Rule	45 CFR § 164.308(a)(3)(ii)(C)

6. Artifact(s)

A completed and signed onboarding/offboarding checklist stored in the employee's confidential HR file.

7. Definitions

Onboarding: The process of integrating a new employee into an organization.

Offboarding: The formal process of separation when an employee leaves a company.

AUP (Acceptable Use Policy): A document stipulating constraints and practices that a user must agree to for access to a corporate network or the Internet.

8. Responsibilities

Role	Responsibility
Human Resources (HR)	Manages the overall onboarding/offboarding process and maintains official employee records.
IT Department	Responsible for provisioning and revoking access to systems and hardware.
Hiring Manager	Responsible for defining access needs, ensuring asset return, and verifying checklist completion.
Employee	Responsible for completing required agreements and training, and for returning assets upon departure.

Security Policy Sanction Procedure (OP-PROC-008)

1. Purpose

To describe the formal process for documenting violations of information security policies and applying consistent, fair, and appropriate disciplinary actions.

2. Scope

This procedure applies to all members of the workforce, including employees, contractors, and temporary staff, who are found to be in violation of the company's established information security policies.

3. Overview

This procedure ensures that security policy violations are handled in a structured and predictable manner. It outlines the steps for identifying a violation, conducting an investigation, determining a commensurate disciplinary action in consultation with Human Resources, and formally documenting the outcome.

4. Procedure

Step	Who	What
1	Manager or Security Officer	Identifies a potential violation of an information security policy through a report, an audit finding, or a security alert.
2	Security Officer & Manager	Conduct an investigation to gather facts and evidence related to the potential violation. This may involve reviewing logs, interviewing individuals, and analyzing data.
3	Security Officer, Manager, & HR	Review the findings of the investigation to confirm whether a policy violation occurred.

Step	Who	What
4	Manager & HR	In consultation with the Security Officer, determine the appropriate disciplinary action. The sanction will be commensurate with the severity of the violation, its impact, and the employee's history.
5	Manager & HR	Formally document the violation and the resulting sanction using a standard disciplinary action form. The documentation is stored in the employee's confidential HR file.
6	Manager	Communicates the decision and the sanction to the employee.

5. Standards Compliance

This section maps the procedure steps to specific controls from relevant information security standards.

Procedure Step(s)	Standard/Framework	Control Reference
1-6	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(C)

6. Artifact(s)

A formal disciplinary action form or memo detailing the policy violation, the findings of the investigation, and the applied sanction. This document is stored in the employee's confidential personnel file.

7. Definitions

Sanction: A penalty or disciplinary action imposed for violating a policy or rule.

Commensurate: Corresponding in size, extent, amount, or degree; proportionate.

8. Responsibilities

Role	Responsibility
Manager	Responsible for identifying and reporting potential violations and for communicating disciplinary actions.
Security Officer	Responsible for investigating potential security policy violations.
Human Resources (HR)	Responsible for ensuring the sanction process is fair, consistent, and legally compliant, and for maintaining official records.

Incident Response Policy (RES-POL-001)

1. Objective

The objective of this policy is to establish a comprehensive incident response framework for **[Company Name]** to effectively detect, respond to, contain, and recover from information security incidents. This policy ensures that security incidents are handled in a coordinated, timely, and effective manner to minimize impact on business operations, protect electronic Protected Health Information (ePHI) and other sensitive data, maintain regulatory compliance with HIPAA, HITECH, and SOC 2 requirements, and preserve evidence for potential legal proceedings.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, third parties, and business associates who may detect, report, or respond to information security incidents. It encompasses all information systems, applications, networks, devices, and data owned, operated, or managed by **[Company Name]**, including cloud services, mobile devices, and third-party systems. This policy covers all types of security incidents including but not limited to data breaches, malware infections, unauthorized access, denial of service attacks, and physical security breaches.

3. Policy

[Company Name] shall maintain a formal incident response capability that enables rapid detection, assessment, containment, eradication, and recovery from security incidents while ensuring compliance with regulatory notification requirements.

3.1 Incident Response Framework

[Company Name] shall implement a structured incident response process based on industry best practices and regulatory requirements.

3.1.1 Incident Response Lifecycle

The incident response process shall follow a systematic lifecycle approach based on the NIST Cybersecurity Framework (Prepare, Detect & Analyze, Contain/Eradicate/Recover, Post-Incident Activity).

1. **Preparation:**

   - Development and at least annual review of the Incident Response Plan (IRP).

- Establishment and maintenance of a designated Incident Response Team (IRT) with clearly defined roles and responsibilities.
- Annual training and simulation exercises (e.g., tabletop exercises) for the IRT to ensure readiness, with outcomes documented for improvement tracking.
- Deployment and maintenance of tools and technologies required for incident detection, analysis, and response.
- Maintenance of secure, out-of-band communication channels for the IRT.
- At least annual testing of incident response capabilities, with results documented and used to drive improvements.

2. Detection and Analysis:

- Continuous monitoring of information systems to detect security events.
- Initial triage of detected events to determine if a potential incident has occurred.
- Formal declaration of an incident and activation of the Incident Response Team (IRT).
- Initial impact and severity assessment to classify the incident according to the criteria in section 3.1.2.
- Establishment of a secure repository for evidence collection and chain of custody documentation.
- Prioritization of response activities based on the incident classification.

3. Containment, Eradication, and Recovery:

- Execution of containment strategies to prevent the incident from spreading and to minimize further damage.
- Identification of the root cause and all affected systems.
- Eradication of the threat (e.g., removing malware, disabling breached accounts, patching vulnerabilities).
- Systematic recovery of affected systems and data from trusted sources.
- Validation that systems are clean and secure before returning them to production.
- Enhanced monitoring of recovered systems to ensure the threat has been fully removed.

4. Post-Incident Activity:

- Incident documentation and reporting
- Lessons learned analysis and improvement recommendations
- Incident response plan updates
- Stakeholder communication and follow-up

- Legal and regulatory compliance activities

3.1.2 Incident Classification

All incidents shall be classified based on their severity and potential impact:

Critical (P1) - Emergency Response Required:

- Confirmed data breach involving ePHI or large volumes of sensitive data
- Active compromise of critical systems affecting business operations
- Widespread malware infection or ransomware attack
- Suspected nation-state or advanced persistent threat (APT) activity
- Physical security breach affecting critical assets
- Response Time: Immediate (within 15 minutes)

High (P2) - Urgent Response Required:

- Unauthorized access to sensitive systems or data
- Malware infection on critical systems
- Denial of service attacks affecting business operations
- Suspected insider threat activity
- Social engineering attacks targeting executives or privileged users
- Response Time: Within 1 hour

Medium (P3) - Standard Response Required:

- Unsuccessful attack attempts against critical systems
- Malware infection on non-critical systems
- Policy violations with potential security impact
- Suspicious network activity or anomalous behavior
- Physical security violations in non-critical areas
- Response Time: Within 4 hours

Low (P4) - Routine Response Required:

- Security policy violations without immediate risk
- Failed login attempts within normal thresholds
- Spam or phishing emails reported by users
- Minor physical security issues
- Security awareness training opportunities
- Response Time: Within 24 hours

3.2 Incident Response Team

A designated Incident Response Team (IRT) shall be established with clearly defined roles and responsibilities.

3.2.1 Core Team Members

Incident Commander:

- Overall incident response coordination and decision-making authority
- Communication with executive leadership and external stakeholders
- Resource allocation and escalation decisions
- Post-incident review and improvement oversight

Security Analyst:

- Technical investigation and analysis
- Evidence collection and preservation
- Malware analysis and threat intelligence gathering
- System forensics and artifact examination

System Administrator:

- System containment and isolation procedures
- System restoration and recovery activities
- Network security controls implementation
- Infrastructure monitoring and maintenance

Privacy Officer:

- HIPAA breach assessment and notification requirements
- Regulatory compliance coordination
- Patient notification and communication
- Risk assessment for privacy violations

Legal Counsel:

- Legal implications assessment and guidance
- Law enforcement coordination and communication
- Litigation hold and evidence preservation requirements
- Regulatory notification and compliance support

Communications Lead:

- Internal and external communication coordination
- Media relations and public communications
- Customer and stakeholder notification
- Crisis communication management

3.2.2 Extended Team Members

Additional team members may be activated based on incident type and severity:

- Human Resources representative for insider threat incidents
- Facilities manager for physical security incidents
- Third-party forensics and investigation specialists
- Public relations and crisis communication experts
- External legal counsel and regulatory specialists
- Business unit leaders and system owners

3.3 Incident Detection and Reporting

Multiple detection methods shall be employed to identify potential security incidents as early as possible.

3.3.1 Detection Methods

Automated Detection:

- Security Information and Event Management (SIEM) system alerts
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) alerts
- Antivirus and anti-malware system notifications
- Data Loss Prevention (DLP) system alerts
- Network anomaly detection and behavioral analysis
- File integrity monitoring and system change detection

Manual Detection:

- Workforce member reports of suspicious activity
- System administrator observation of anomalous behavior
- Security team proactive monitoring and hunting activities
- Third-party security service provider notifications
- Customer or partner reports of potential compromise

- Physical security observations and reports

3.3.2 Incident Reporting Procedures

Immediate Reporting Channels:

- 24/7 security hotline: **[Phone Number]**
- Email reporting: **[Email Address]**
- Online incident reporting portal: **[URL]**
- In-person reporting to Security Officer or designee

Reporting Requirements:

- All suspected incidents must be reported within **[Timeframe, e.g., 2 hours]** of discovery
- Initial reports may be verbal with written follow-up required within **[Timeframe, e.g., 24 hours]**
- Reports must include all available information about the incident
- Workforce members shall not attempt to investigate incidents independently
- No retaliation for good faith incident reporting

3.4 Incident Response Procedures

Standardized procedures shall be followed for responding to different types of security incidents.

3.4.1 Initial Response Procedures

Incident Verification:

- Confirm that a security incident has actually occurred
- Gather initial information about the scope and impact
- Classify the incident according to established criteria
- Activate appropriate incident response procedures
- Notify relevant incident response team members

Evidence Preservation:

- Preserve all relevant evidence in its original state
- Document all actions taken and decisions made
- Maintain chain of custody for digital and physical evidence
- Take system snapshots or images before making changes
- Collect network traffic captures and log files

3.4.2 Containment Procedures

Short-term Containment:

- Isolate affected systems from the network
- Disable compromised user accounts and change passwords
- Block malicious IP addresses and domains
- Implement temporary firewall rules to prevent spread
- Preserve system state for forensic analysis

Long-term Containment:

- Rebuild compromised systems from clean backups
- Implement enhanced monitoring on affected systems
- Apply security patches and configuration hardening
- Conduct security validation before system restoration
- Monitor for signs of persistent compromise

3.4.3 Eradication and Recovery Procedures

Threat Eradication:

- Remove malware and malicious artifacts from systems
- Close security vulnerabilities that enabled the incident
- Improve security controls to prevent recurrence
- Validate that all traces of compromise have been eliminated
- Conduct security assessment of remediated systems

System Recovery:

- Restore systems and data from clean backups
- Implement additional security monitoring and controls
- Gradually restore full system functionality
- Conduct user acceptance testing and validation
- Monitor systems for signs of compromise or instability

3.5 Regulatory and Legal Compliance

Incident response procedures shall ensure compliance with all applicable legal and regulatory requirements.

3.5.1 HIPAA Breach Notification Requirements

Breach Assessment:

- Determine whether incident constitutes a HIPAA breach
- Assess the probability that ePHI has been compromised
- Evaluate risk of harm to affected individuals
- Document the breach assessment decision and rationale

Notification Timelines:

- HHS notification within **60 days** of breach discovery
- Individual notification within **60 days** of breach discovery
- Media notification if breach affects **500 or more individuals** in a state/jurisdiction
- Immediate notification to HHS if breach affects **500 or more individuals** nationwide

3.5.2 Other Regulatory Requirements

State Data Breach Notification Laws:

- Comply with applicable state notification requirements
- Determine residency of affected individuals for notification purposes
- Meet varying state timelines and notification methods
- Coordinate with state attorneys general as required

Federal and Industry Requirements:

- SEC notification for material cybersecurity incidents (public companies)
- Financial industry notifications (if applicable)
- Professional licensing board notifications (if applicable)
- Insurance carrier notification and claim procedures

3.6 Communication and Coordination

Effective communication shall be maintained throughout the incident response process.

3.6.1 Internal Communications

Executive Reporting:

- Immediate notification to CEO/Executive Leadership for Critical incidents
- Regular status updates throughout incident response
- Final incident report with lessons learned and recommendations
- Board of Directors notification for significant incidents

Workforce Communications:

- Need-to-know basis for incident details
- General security awareness messages as appropriate
- Post-incident training and awareness updates
- Recognition for effective incident reporting and response

3.6.2 External Communications

Customer Communications:

- Timely notification of customers potentially affected by incidents
- Clear explanation of incident impact and remediation efforts
- Regular updates on investigation and recovery progress
- Contact information for customer questions and concerns

Vendor and Partner Communications:

- Notification of business associates and vendors as required
- Coordination with third-party service providers for response activities
- Information sharing with industry partners and threat intelligence communities
- Coordination with insurance carriers and coverage providers

3.7 Post-Incident Activities

Comprehensive post-incident activities shall ensure organizational learning and improvement.

3.7.1 Incident Documentation

Incident Report Contents:

- Complete timeline of incident detection, response, and recovery
- Root cause analysis and contributing factors
- Impact assessment including affected systems and data
- Response effectiveness evaluation and lessons learned
- Recommendations for security improvements and process enhancements

3.7.2 Lessons Learned and Improvement

Post-Incident Review:

- Formal review meeting within **[Timeframe, e.g., 2 weeks]** of incident closure
- Analysis of response effectiveness and areas for improvement

- Review of incident response plan adequacy and updates needed
- Evaluation of team performance and training requirements
- Assessment of detection capabilities and monitoring effectiveness

Process Improvement:

- Update incident response procedures based on lessons learned
- Implement additional security controls to prevent similar incidents
- Enhance monitoring and detection capabilities
- Improve training and awareness programs
- Update business continuity and disaster recovery plans

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(6) - Security Incident Procedures
3.5.1	HIPAA Breach Notification Rule	45 CFR § 164.400-414 - Notification Requirements
3.3, 3.4	HIPAA Security Rule	45 CFR § 164.312(b) - Audit Controls
All	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
3.4, 3.6	SOC 2 Trust Services Criteria	CC7.2 - Controls Monitor Effectiveness
3.7	SOC 2 Trust Services Criteria	CC2.1 - Communication and Information
All	NIST Cybersecurity Framework	RS.RP - Response Planning
3.4	NIST Cybersecurity Framework	RS.CO - Communications

Policy Section	Standard/Framework	Control Reference
3.7	NIST Cybersecurity Framework	RC.IM - Improvements

5. Definitions

Business Associate: A person or entity that performs functions or activities on behalf of a covered entity involving access to ePHI.

Chain of Custody: Documentation of the chronological transfer of evidence from collection to presentation.

Incident Commander: Individual with overall authority and responsibility for incident response coordination.

Incident Response Team (IRT): Designated group of individuals responsible for detecting, responding to, and recovering from security incidents.

Indicators of Compromise (IOCs): Artifacts observed on networks or operating systems that indicate computer intrusion.

Mean Time to Detection (MTTD): Average time between when an incident occurs and when it is detected.

Mean Time to Recovery (MTTR): Average time to restore normal operations after an incident.

Security Incident: Any event that could result in unauthorized access to, disclosure, modification, or destruction of information assets.

6. Responsibilities

Role	Responsibility
Security Officer	Develop incident response policies, maintain incident response team, oversee incident investigations, and ensure regulatory compliance.

Role	Responsibility
Incident Commander	Lead incident response activities, coordinate team efforts, communicate with stakeholders, and make critical response decisions.
Privacy Officer	Assess HIPAA breach requirements, coordinate breach notifications, manage patient communications, and ensure privacy compliance.
IT Security Team	Detect and analyze security incidents, perform technical investigations, implement containment measures, and conduct system recovery.
Legal Counsel	Provide legal guidance, coordinate law enforcement relations, manage litigation holds, and ensure regulatory compliance.
Communications Team	Manage internal and external communications, coordinate media relations, and support crisis communications.
System Administrators	Implement technical containment measures, perform system restoration, maintain evidence integrity, and support forensic activities.
Human Resources	Support insider threat investigations, manage workforce communications, coordinate with legal team, and handle personnel actions.
All Workforce Members	Report suspected incidents promptly, cooperate with investigations, follow incident response procedures, and participate in post-incident training.

Business Continuity and Disaster Recovery Policy (RES-POL-002)

1. Objective

The objective of this policy is to establish a comprehensive business continuity and disaster recovery framework for **[Company Name]** that ensures the continuation of critical business operations and the timely recovery of information systems following disruptions. This policy ensures that **[Company Name]** can maintain the availability of essential services, protect electronic Protected Health Information (ePHI) and other sensitive data, meet regulatory obligations under HIPAA, HITECH, and SOC 2, and minimize the impact of disruptions on patients, customers, and business operations.

2. Scope

This policy applies to all **[Company Name]** workforce members, facilities, information systems, business processes, and third-party service providers that support critical business operations. It encompasses all types of disruptions including natural disasters, technology failures, cyber attacks, pandemic events, supply chain disruptions, and other events that could impact business operations. This policy covers both preventive measures to reduce the likelihood of disruptions and responsive measures to ensure rapid recovery when disruptions occur.

3. Policy

[Company Name] shall maintain comprehensive business continuity and disaster recovery capabilities that enable the organization to continue critical operations during disruptions and recover normal operations within acceptable timeframes.

3.1 Business Continuity Framework

[Company Name] shall implement a structured approach to business continuity management based on industry best practices and regulatory requirements.

3.1.1 Business Continuity Principles

Life Safety Priority:

- The safety and security of workforce members, patients, and visitors is the highest priority in all emergency situations
- Emergency evacuation and safety procedures take precedence over business operations
- Clear communication channels and emergency coordination procedures shall be maintained

Essential Services Continuity:

- Critical business functions shall be identified and prioritized for continuity
- Minimum service levels shall be defined for essential operations
- Alternative methods and resources shall be available to maintain critical services
- Patient care and safety functions receive highest priority for resource allocation

Regulatory Compliance:

- Business continuity plans shall ensure continued compliance with HIPAA, HITECH, and other applicable regulations
- ePHI availability and protection shall be maintained during disruptions
- Audit trails and documentation requirements shall be met even during emergency operations
- Regulatory notification requirements shall be incorporated into emergency procedures

Stakeholder Communication:

- Clear, timely, and accurate communication shall be maintained with all stakeholders
- Multiple communication channels shall be available for redundancy
- Regular updates shall be provided during extended disruptions
- Post-incident communication shall address lessons learned and improvements

3.1.2 Business Impact Analysis (BIA)

The Business Continuity Manager, in coordination with Business Unit Leaders, shall conduct and formally document a comprehensive Business Impact Analysis (BIA) at least annually, or whenever a significant change to business operations occurs. The BIA report, which defines the recovery requirements for all critical functions, must be reviewed and formally approved by the Information Security Committee.

Critical Function Identification:

- **Immediate (0-4 hours):** Patient care systems, emergency services, life safety systems
- **Urgent (4-24 hours):** Clinical documentation, pharmacy systems, laboratory services
- **Important (1-3 days):** Billing systems, administrative functions, non-critical applications
- **Deferrable (3+ days):** Training systems, development environments, archival processes

Impact Assessment Criteria:

- **Financial Impact:** Revenue loss, additional costs, regulatory fines, contractual penalties
- **Operational Impact:** Service disruption, productivity loss, customer dissatisfaction

- **Regulatory Impact:** Compliance violations, reporting failures, audit findings
- **Reputational Impact:** Public relations damage, loss of stakeholder confidence
- **Patient Safety Impact:** Risk to patient care, safety concerns, clinical service disruption

Recovery Time Objectives (RTO):

- Maximum acceptable downtime for each critical business function
- Immediate: **[Duration, e.g., 1 hour]** maximum downtime
- Urgent: **[Duration, e.g., 4 hours]** maximum downtime

- Important: **[Duration, e.g., 24 hours]** maximum downtime
- Deferrable: **[Duration, e.g., 72 hours]** maximum downtime

Recovery Point Objectives (RPO):

- Maximum acceptable data loss for each critical system
- Critical ePHI systems: **[Duration, e.g., 15 minutes]** maximum data loss
- Financial systems: **[Duration, e.g., 1 hour]** maximum data loss
- Administrative systems: **[Duration, e.g., 4 hours]** maximum data loss
- Development systems: **[Duration, e.g., 24 hours]** maximum data loss

3.2 Disaster Recovery Planning

Comprehensive disaster recovery plans shall be developed for all critical information systems and infrastructure.

3.2.1 IT Disaster Recovery Strategy

Primary Data Center Protection:

- Redundant systems and infrastructure components
- Uninterruptible Power Supply (UPS) and backup generator systems
- Fire suppression and environmental monitoring systems
- Physical security and access controls
- Network redundancy with multiple internet service providers

Secondary Site Operations:

- Geographically separated backup data center located **[Distance, e.g., 100+ miles]** from primary site
- Real-time data replication for critical systems

- Standby infrastructure capable of supporting minimum service levels
- Alternative network connectivity and communication systems
- Pre-positioned equipment and supplies for extended operations

Cloud-Based Recovery:

- Cloud infrastructure for scalable recovery capabilities
- Hybrid cloud strategy combining on-premises and cloud resources
- Multi-cloud approach to avoid single vendor dependency
- Automated failover and recovery procedures where technically feasible
- Data sovereignty and regulatory compliance in cloud environments

3.2.2 Data Backup and Recovery

Backup Strategy:

- **3-2-1 Backup Rule:** 3 copies of critical data, 2 different media types, 1 offsite location
- Daily incremental backups for all production systems
- Weekly full backups with long-term retention
- Real-time replication for critical databases and applications
- Encrypted backup storage for all sensitive information

Backup Testing and Validation:

- Monthly restore testing for critical systems
- Quarterly full disaster recovery testing
- Annual comprehensive business continuity exercise
- Documentation of all test results and identified improvements
- Regular validation of backup integrity and completeness

3.3 Emergency Response Procedures

Standardized emergency response procedures shall guide initial response actions during various types of disruptions.

3.3.1 Emergency Activation Procedures

Incident Assessment:

- Initial situation assessment and impact determination
- Activation of appropriate emergency response level
- Notification of emergency response team members

- Establishment of emergency operations center
- Communication with key stakeholders and authorities

Emergency Response Levels:

- **Level 1 - Facility Emergency:** Local facility impact requiring immediate response
- **Level 2 - Regional Emergency:** Multi-facility or regional impact requiring coordinated response
- **Level 3 - Enterprise Emergency:** Organization-wide impact requiring full emergency response activation

3.3.2 Communication Procedures

Emergency Notification System:

- Automated notification system for workforce members
- Multiple communication channels (phone, email, text, mobile app)
- 24/7 emergency hotline for situation updates
- Social media and website updates for public communication
- Integration with local emergency management systems

Stakeholder Communication:

- Immediate notification of executive leadership
- Regular updates to workforce members and their families
- Communication with patients, customers, and business partners
- Coordination with regulatory agencies and oversight bodies
- Media relations and public communication management

3.4 Alternative Operations

Alternative operating procedures shall enable continuation of critical business functions during disruptions.

3.4.1 Alternate Work Arrangements

Remote Work Capabilities:

- Work-from-home infrastructure and technology
- Secure remote access to critical systems and applications
- Video conferencing and collaboration tools
- Remote printing and document management capabilities

- Virtual private network (VPN) capacity for all workforce members

Alternate Facility Operations:

- Pre-arranged alternate facilities for critical operations
- Mobile command centers for field operations
- Temporary workspace arrangements with business partners
- Equipment and supply pre-positioning at alternate sites
- Vendor agreements for rapid facility setup and provisioning

3.4.2 Critical System Alternatives

Manual Procedures:

- Paper-based backup procedures for critical electronic systems
- Manual patient registration and medical record procedures
- Alternative communication methods (phone, fax, radio)
- Cash-based transaction procedures for payment systems
- Physical key management for electronic access control failures

Vendor Support Services:

- Emergency vendor agreements for rapid response
- 24/7 vendor support for critical systems and infrastructure
- Expedited procurement procedures for emergency equipment
- Alternative vendor options for single points of failure
- Service level agreements with guaranteed emergency response times

3.5 Testing and Maintenance

Regular testing and maintenance shall ensure the effectiveness of business continuity and disaster recovery capabilities.

3.5.1 Testing Schedule and Requirements

Monthly Testing:

- Backup and recovery procedures for critical systems
- Emergency communication systems and notification procedures
- Alternate facility and equipment readiness
- Vendor emergency response capabilities
- Documentation updates and contact information verification

Quarterly Testing:

- Tabletop exercises for emergency response scenarios
- Partial system recovery testing and validation
- Workforce training and awareness programs
- Business impact analysis updates and revisions
- Emergency supply inventory and expiration date management

Annual Testing:

- Full-scale business continuity exercise
- Complete disaster recovery simulation
- Comprehensive plan review and updates
- Third-party assessment of continuity capabilities
- Regulatory compliance validation and reporting

3.5.2 Plan Maintenance and Updates

Regular Plan Updates:

- Annual comprehensive review and revision of all plans
- Quarterly updates based on organizational changes
- Monthly contact information and resource verification
- Immediate updates following significant incidents or changes
- Version control and distribution management for all plans

Training and Awareness:

- Annual business continuity training for all workforce members
- Specialized training for emergency response team members
- New employee orientation including emergency procedures
- Regular drills and exercises to maintain readiness
- Cross-training programs to reduce single points of failure

3.6 Vendor and Third-Party Management

Business continuity requirements shall be incorporated into vendor management and third-party relationships.

3.6.1 Vendor Continuity Requirements

Service Level Agreements:

- Specific business continuity and disaster recovery requirements
- Guaranteed response times for emergency situations
- Alternative service delivery methods during disruptions
- Regular testing and validation of vendor continuity capabilities
- Financial penalties for continuity failures and service level breaches

Vendor Assessment and Monitoring:

- Annual assessment of vendor business continuity capabilities
- Regular review of vendor disaster recovery plans and procedures
- Monitoring of vendor financial stability and business viability
- Evaluation of vendor geographic risk factors and concentration
- Validation of vendor backup and alternative service arrangements

3.6.2 Business Associate Agreements

HIPAA Compliance Requirements:

- Business continuity provisions in all Business Associate Agreements
- ePHI protection and availability requirements during emergencies
- Breach notification procedures for continuity-related incidents
- Audit and compliance requirements for emergency operations
- Data backup and recovery requirements for ePHI systems

3.7 Recovery and Restoration

Systematic procedures shall guide the restoration of normal operations following emergency situations.

3.7.1 Recovery Procedures

Damage Assessment:

- Comprehensive assessment of facilities, equipment, and systems
- Safety inspection and clearance for facility reoccupancy
- Data integrity validation and system functionality testing
- Workforce accountability and fitness for duty assessment
- Business process and service capability evaluation

Phased Recovery Approach:

- **Phase 1:** Life safety and immediate emergency response

- **Phase 2:** Critical system restoration and essential service resumption
- **Phase 3:** Full operational capability restoration
- **Phase 4:** Normal operations resumption and lessons learned integration

3.7.2 Post-Incident Review

Following any activation of the BCDR plan, a formal post-incident review shall be conducted.

Comprehensive Analysis:

- A formal Post-Incident Report shall be created, detailing the timeline of events, response effectiveness, and root cause analysis.
- Root cause analysis and contributing factor identification
- Cost analysis and financial impact assessment
- Stakeholder feedback collection and analysis
- Regulatory compliance validation and reporting

Improvement Implementation:

- All findings and lessons learned shall be documented.
- Action items for improvement shall be assigned an owner and due date and tracked to completion in a formal Plan of Action and Milestones (POA&M).
- The BCDR plan and related procedures shall be updated based on the approved action items.
- Training program updates and workforce development
- Technology and infrastructure improvements
- Vendor relationship and agreement modifications

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(7) - Contingency Plan
3.2.2	HIPAA Security Rule	45 CFR § 164.308(a)(7)(ii)(A) - Data Backup Plan

Policy Section	Standard/Framework	Control Reference
3.7	HIPAA Security Rule	45 CFR § 164.308(a)(7)(ii)(B) - Disaster Recovery Plan
3.4	HIPAA Security Rule	45 CFR § 164.308(a)(7)(ii)(C) - Emergency Mode Operation
3.5	HIPAA Security Rule	45 CFR § 164.308(a)(7)(ii)(D) - Testing and Revision
All	SOC 2 Trust Services Criteria	A1.1 - Availability
3.2	SOC 2 Trust Services Criteria	A1.2 - System Capacity
3.5	SOC 2 Trust Services Criteria	A1.3 - System Monitoring
All	ISO/IEC 27001:2022	A.17.1 - Business continuity planning
3.2	NIST Cybersecurity Framework	RC.RP - Recovery Planning

5. Definitions

Business Continuity: The capability to continue delivery of products or services at predefined levels following a disruptive incident.

Business Impact Analysis (BIA): Process to determine the impact of losing business functions and processes.

Disaster Recovery: Process of restoring IT infrastructure and systems following a disaster.

Emergency Operations Center (EOC): Centralized location for emergency response coordination and decision-making.

Recovery Point Objective (RPO): Maximum acceptable amount of data loss measured in time.

Recovery Time Objective (RTO): Maximum acceptable length of time to restore business functions.

Resilience: Ability to adapt and recover quickly from disruptions while maintaining operations.

Risk Assessment: Process of identifying threats and vulnerabilities that could impact business operations.

6. Responsibilities

Role	Responsibility
Executive Leadership	Provide strategic direction and resources for business continuity program, approve plans and resource allocation, and communicate with stakeholders during emergencies.
Business Continuity Manager	Develop and maintain business continuity plans, coordinate testing and training, manage emergency response activities, and ensure regulatory compliance.
IT Recovery Team	Implement disaster recovery procedures, restore IT systems and data, maintain backup systems, and coordinate technical recovery activities.
Emergency Response Team	Coordinate emergency response activities, manage emergency operations center, communicate with stakeholders, and ensure workforce safety.
Facilities Management	Maintain emergency systems and supplies, coordinate with emergency services, assess facility damage, and manage alternate facility arrangements.
Human Resources	Manage workforce accountability and communications, coordinate with families, support workforce welfare, and maintain emergency contact information.

Role	Responsibility
Legal and Compliance	Ensure regulatory compliance during emergencies, manage legal implications of incidents, coordinate with authorities, and handle insurance claims.
Business Unit Leaders	Implement business unit specific continuity plans, coordinate with recovery teams, manage departmental communications, and support workforce needs.
All Workforce Members	Follow emergency procedures, participate in training and drills, report safety concerns, and support recovery efforts as assigned.

Incident Response Plan (IRP) ([RES-PROC-001])

1. Purpose

To provide detailed, actionable steps for responding to information security incidents to minimize impact and ensure a coordinated response.

2. Scope

This procedure applies to all personnel involved in the incident response process and covers all information systems and data.

3. Overview

This procedure outlines the formal process for managing information security incidents, from initial detection and analysis through containment, eradication, recovery, and post-incident review, following the NIST incident response lifecycle.

4. Procedure

Step	Phase	Who	What
1	**Preparation**	Security Team	Conduct annual incident response training and exercises.
2		Security Team	Maintain and test incident response tools and systems.
3	**Detection & Analysis**	All Personnel	Report suspected incidents to the Security Team immediately.

Step	Phase	Who	What
4		Security Analyst	Triage and classify incoming alerts and reports to determine if an incident has occurred.
5		Incident Commander	Activate the Incident Response Team (IRT) for confirmed incidents.
6	**Containment, Eradication, & Recovery**	IRT	Isolate affected systems to prevent further damage.
7		IRT	Identify and remove the root cause of the incident (e.g., malware, unauthorized access).
8		IRT	Restore systems to normal operation from clean backups.
9	**Post-Incident Activity**	Incident Commander	Conduct a post-incident review (lessons learned) meeting.
10		Incident Commander	Complete and file a formal Incident Report.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-10	SOC 2	CC7.1, CC7.2
1-10	HIPAA Security Rule	45 CFR § 164.308(a)(6)

6. Artifact(s)

A completed Incident Report for each declared incident.

7. Definitions

Incident: An event that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits.

Incident Response Team (IRT): A dedicated or virtual team responsible for responding to security incidents.

8. Responsibilities

Role	Responsibility
Incident Commander	Leads and coordinates the overall incident response effort.
Security Analyst	Performs initial triage, analysis, and technical investigation of incidents.
Privacy Officer	Assesses incidents for potential data breach notification requirements, particularly under HIPAA.
Legal Counsel	Provides legal guidance on incident handling, evidence preservation, and external communications.

HIPAA Breach Risk Assessment Procedure ([RES-PROC-002])

1. Purpose

To guide the Privacy Officer and Incident Response Team through the formal risk assessment required to determine if a security incident qualifies as a notifiable breach under the HIPAA Breach Notification Rule.

2. Scope

This procedure applies to any security incident involving the potential compromise of electronic Protected Health Information (ePHI).

3. Overview

This procedure details the steps for conducting a formal risk assessment to determine the probability that ePHI has been compromised, in accordance with the HIPAA Breach Notification Rule.

4. Procedure

Step	Who	What
1	Privacy Officer / IRT	Determine if the security incident involves Protected Health Information (PHI) or electronic Protected Health Information (ePHI).
2	Privacy Officer / IRT	Assess the probability that the PHI/ePHI has been compromised by evaluating the following factors: - The nature and extent of the PHI involved. - The unauthorized person who used the PHI or to whom the disclosure was made. - Whether the PHI was actually acquired or viewed. - The extent to which the risk to the PHI has been mitigated.
3	Privacy Officer	Document the complete risk assessment findings and the final rationale for the determination (i.e., whether it is a notifiable breach or not) on the HIPAA Breach Risk Assessment form.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-3	HIPAA Breach Notification Rule	45 CFR § 164.400-414

6. Artifact(s)

A completed and signed HIPAA Breach Risk Assessment form.

7. Definitions

ePHI (electronic Protected Health Information): Any protected health information (PHI) that is created, stored, transmitted, or received in any electronic format.

Breach: The acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the protected health information.

8. Responsibilities

Role	Responsibility
Privacy Officer	Leads the breach risk assessment process and makes the final determination of a notifiable breach.
Incident Response Team (IRT)	Provides technical details and context about the security incident to support the risk assessment.

Post-Incident Review Procedure ([RES-PROC-003])

1. Purpose

To outline the process for conducting a formal ‘lessons learned’ review after a significant incident is resolved and for tracking resulting action items to completion.

2. Scope

This procedure applies to all major information security incidents as determined by the Incident Commander.

3. Overview

This procedure ensures that after a significant incident, a formal review is conducted to analyze the response, identify improvements, update documentation, and track corrective actions to enhance future incident response capabilities.

4. Procedure

Step	Who	What
1	Incident Commander	Schedule a formal post-incident review meeting within two weeks of the incident’s resolution.
2	Incident Response Team (IRT)	During the meeting, analyze the incident timeline, the effectiveness of the response actions, and identify areas for improvement.
3	Security Team	Update the Incident Response Plan (IRP) and any other relevant procedures or documentation based on the findings from the review.
4	Incident Commander	Assign any identified action items to specific owners with clear due dates and track them to completion in a designated log.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-4	SOC 2	CC2.1
1-4	NIST Cybersecurity Framework	RC.IM

6. Artifact(s)

A Post-Incident Report including a "lessons learned" section and an action item tracking log.

7. Definitions

Action Item Tracking Log: A formal record used to document, assign, and monitor the status of corrective actions identified during a post-incident review.

8. Responsibilities

Role	Responsibility
Incident Commander	Chairs the post-incident review meeting and ensures action items are assigned and tracked.
Incident Response Team (IRT)	Actively participates in the review, providing insights into the response process.
Security Team	Is responsible for updating security documentation based on the outcomes of the review.

Business Impact Analysis (BIA) Procedure ([RES-PROC-004])

1. Purpose

To define the methodology for conducting the annual Business Impact Analysis (BIA) to identify critical business functions and establish recovery objectives.

2. Scope

This procedure applies to all business units and departments within the organization.

3. Overview

This procedure outlines the annual process for identifying and prioritizing critical business functions, assessing the impact of a disruption to these functions, and defining their Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

4. Procedure

Step	Who	What
1	Business Continuity Manager	Distribute BIA questionnaires to all Business Unit Leaders at the start of the annual BIA cycle.
2	Business Unit Leaders	Complete the questionnaires, identifying critical business processes, their dependencies (technical and non-technical), and the potential impact of a disruption.
3	Business Unit Leaders	For each critical process, determine the maximum tolerable downtime (Recovery Time Objective - RTO) and the maximum acceptable data loss (Recovery Point Objective - RPO).
4	Business Continuity Manager	Collect and analyze the completed questionnaires, compile the findings into a formal BIA report, and present it to the BCDR Steering Committee for review and approval.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-4	SOC 2	A1.1
1-4	HIPAA Security Rule	45 CFR § 164.308(a)(7)

6. Artifact(s)

A formally approved Business Impact Analysis (BIA) Report.

7. Definitions

Recovery Time Objective (RTO): The maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.

Recovery Point Objective (RPO): The maximum acceptable amount of data loss an organization can tolerate, measured in time.

8. Responsibilities

Role	Responsibility
Business Continuity Manager	Manages the overall BIA process, including questionnaire distribution, analysis, and report creation.
Business Unit Leaders	Are responsible for accurately identifying critical processes, dependencies, and recovery objectives for their respective areas.
BCDR Steering Committee	Reviews and formally approves the final BIA report.

IT Disaster Recovery Plan (DRP) ([RES-PROC-005])

1. Purpose

To provide detailed technical procedures for recovering IT infrastructure, systems, and data at an alternate site in the event of a disaster.

2. Scope

This plan applies to all critical IT systems, infrastructure, and data required to support essential business functions as defined in the Business Impact Analysis (BIA).

3. Overview

This document outlines the technical steps for the IT Disaster Recovery Team to respond to a declared disaster. It covers team activation, damage assessment, failover to the secondary recovery site, data restoration, and system validation to ensure a timely and effective recovery of IT services.

4. Procedure

Step	Phase	Who	What
1	**Activation & Assessment**	BCDR Steering Committee	Declare a disaster and formally activate the DRP.
2		DR Team Lead	Activate the Disaster Recovery (DR) Team.
3		DR Team	Conduct an initial damage assessment to understand the extent of the outage.

Step	Phase	Who	What
4	**Recovery**	DR Team (Infrastructure)	Initiate failover procedures for network, servers, and other infrastructure to the secondary site (including cloud resources).
5		DR Team (Data)	Restore application data from the most recent, consistent backups, respecting defined RPOs.
6		DR Team (Applications)	Bring critical applications online at the recovery site.
7	**Validation & Resumption**	DR Team / Business Users	Validate that recovered systems and data are functional and consistent.
8		DR Team Lead	Formally declare that IT systems are operational and ready to support business functions.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-8	SOC 2	A1.2
1-8	HIPAA Security Rule	45 CFR § 164.308(a)(7)(ii)(B)

6. Artifact(s)

A log of all recovery activities performed, including timelines, actions taken, and the results of system validation tests.

7. Definitions

Failover: The process of switching to a redundant or standby computer server, system, or network upon the failure or abnormal termination of the previously active application, server, system, or network.

Disaster Recovery (DR) Site: A secondary location where an organization can relocate its technology and operations following a disaster.

8. Responsibilities

Role	Responsibility
DR Team Lead	Manages and coordinates all technical recovery activities during a disaster.
DR Team (Infrastructure)	Responsible for recovering core infrastructure components like networks and servers.
DR Team (Data)	Responsible for restoring data from backups.
DR Team (Applications)	Responsible for bringing business applications back online and validating their functionality.

Business Continuity Plan (BCP) ([RES-PROC-006])

1. Purpose

To outline the procedures for activating emergency response, managing communications, and continuing critical business functions during a disruption.

2. Scope

This plan applies to all personnel and covers the processes and resources needed to continue critical business functions identified in the Business Impact Analysis (BIA).

3. Overview

This plan provides a framework for responding to a business disruption. It details the procedures for plan activation, establishing an Emergency Operations Center (EOC), crisis communications, and implementing alternate work arrangements and manual backup procedures to ensure business continuity.

4. Procedure

Step	Who	What
1	BCDR Steering Committee	Activate the Business Continuity Plan upon declaration of a significant business disruption.
2	Emergency Response Team	Establish and staff the Emergency Operations Center (EOC) to serve as the central command for the response.
3	Communications Lead	Use the emergency notification system to disseminate critical information and instructions to all employees.

Step	Who	What
4	Business Unit Leaders	Instruct teams to implement alternate work arrangements (e.g., remote work) as outlined for their functions.
5	All Affected Personnel	Utilize manual backup procedures and workarounds for critical processes if systems are unavailable.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2	A1.1
1-5	HIPAA Security Rule	45 CFR § 164.308(a)(7)(ii)(C)

6. Artifact(s)

- Emergency response team activation logs.
- Copies of all emergency communications sent via the notification system.

7. Definitions

Emergency Operations Center (EOC): A central command and control facility responsible for carrying out the principles of emergency preparedness and emergency management, or disaster management functions at a strategic level during an emergency.

Emergency Notification System: A platform used to rapidly communicate with employees, stakeholders, and other contacts in the event of an emergency.

8. Responsibilities

Role	Responsibility
BCDR Steering Committee	Authorizes the activation of the BCP.
Emergency Response Team	Manages the overall business response to the disruption from the EOC.
Communications Lead	Manages all internal and external communications during the event.
Business Unit Leaders	Direct their teams in executing continuity strategies and manual workarounds.

BCDR Testing and Exercise Procedure ([RES-PROC-007])

1. Purpose

To detail the requirements for planning, executing, and documenting annual disaster recovery tests and business continuity exercises.

2. Scope

This procedure applies to all components of the Business Continuity and Disaster Recovery (BCDR) program, including the BCP, DRP, and associated teams.

3. Overview

This procedure ensures that the organization's BCDR plans are effective and up-to-date by mandating a regular testing cycle. It covers the creation of an annual test plan, the execution of various test scenarios, and the formal documentation of results and lessons learned to drive continuous improvement.

4. Procedure

Step	Who	What
1	Business Continuity Manager	At the beginning of each year, create an annual BCDR test plan that includes a schedule and specific scenarios (e.g., tabletop exercise, full DR simulation, call tree test).
2	Business Continuity Manager	Coordinate with all required participants (e.g., DR Team, Business Unit Leaders, IRT) and ensure necessary resources are available for each scheduled test.
3	Test Participants	Execute the test according to the defined plan and scenario, documenting all actions, decisions, and outcomes as they occur.
4	Business Continuity Manager	Following the test, create a formal post-exercise report that includes an analysis of the test, findings, lessons learned, and recommendations for plan improvements.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-4	SOC 2	A1.3
1-4	HIPAA Security Rule	45 CFR § 164.308(a)(7)(ii)(D)

6. Artifact(s)

- A completed annual test plan.
- A post-exercise report with lessons learned for each test conducted.

7. Definitions

Tabletop Exercise: A discussion-based session where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation.

Full DR Simulation: A comprehensive test where the organization's IT systems are actually failed over to the disaster recovery site and operated from there for a period of time.

8. Responsibilities

Role	Responsibility
Business Continuity Manager	Owns the overall testing process, from planning and coordination to creating the final post-exercise report.
Test Participants	Actively engage in the test execution according to their defined BCDR roles and responsibilities.
BCDR Steering Committee	Reviews and approves the annual test plan and post-exercise reports.

Information Security Policy (SEC-POL-001)

1. Objective

The objective of this policy is to establish **[Company Name]**'s comprehensive Information Security Management System (ISMS) and define the overarching framework for protecting the confidentiality, integrity, and availability of all information assets. This policy serves as the foundation for all security controls and demonstrates **[Company Name]**'s commitment to safeguarding electronic Protected Health Information (ePHI), maintaining compliance with applicable regulations, and supporting business objectives through effective risk management.

2. Scope

This policy applies to all **[Company Name]** workforce members, including employees, contractors, temporary staff, and interns. It encompasses all information assets owned, operated, or managed by **[Company Name]**, regardless of format (electronic, physical, or verbal), location (on-premises, cloud, or remote), or lifecycle stage (creation, processing, storage, transmission, or disposal). This policy also applies to all third parties, vendors, and business associates who access, process, or store **[Company Name]** information.

3. Policy

[Company Name] is committed to implementing and maintaining a comprehensive information security program that protects information assets and ensures regulatory compliance.

3.1 Information Security Governance

[Company Name] shall establish and maintain a formal information security governance structure to oversee the implementation and effectiveness of the ISMS.

- A designated Security Officer shall be appointed with ultimate responsibility for the information security program. The Security Officer shall report directly to executive leadership and have the authority to implement security controls across the organization.
- An Information Security Committee shall be established, comprising representatives from key business functions including executive leadership, IT, legal, compliance, human resources, and operations. The committee shall meet at least quarterly to review security performance, approve policy changes, and make strategic security decisions. Meeting minutes shall be documented and retained to provide an audit trail of all decisions.

- Information security objectives and requirements shall be integrated into all business processes, system development lifecycles, and vendor management activities.
- Security roles and responsibilities shall be clearly defined, documented, and communicated to all workforce members through formal job descriptions and training programs.

3.2 Risk Management Framework

[Company Name] shall implement a systematic approach to identifying, assessing, and managing information security risks.

- A formal risk assessment shall be conducted annually and whenever significant changes occur to the business environment, technology infrastructure, or regulatory landscape.
- Risk treatment decisions shall be documented and approved by appropriate management levels based on risk tolerance and business impact.
- Residual risks shall be monitored continuously, and risk treatment effectiveness shall be reviewed quarterly.
- A risk register shall be maintained to track all identified risks, treatment actions, and ownership assignments.

3.3 Information Classification and Handling

All information assets shall be classified according to their sensitivity level and handled in accordance with established security controls.

- Information shall be classified into defined categories (e.g., Public, Internal, Confidential, Restricted) based on the potential impact of unauthorized disclosure, modification, or destruction.
- Appropriate security controls shall be applied to each classification level, including access restrictions, encryption requirements, storage limitations, and disposal procedures.
- Data handling procedures shall comply with applicable privacy regulations, including HIPAA for ePHI and other data protection requirements.
- Information owners shall be designated for all critical information assets and shall be responsible for classification decisions and access approvals.

3.4 Access Control and Authentication

Access to information systems and data shall be controlled through formal processes that implement the principles of least privilege and separation of duties.

- All users shall be assigned unique identifiers and shall be authenticated before accessing any company systems or data.
- Multi-factor authentication shall be required for all systems containing sensitive information, including ePHI.
- Access rights shall be reviewed at least quarterly for systems containing Confidential or Restricted data and at least annually for all other systems. These reviews shall be documented.
- Privileged access shall be subject to additional controls, including time-limited sessions, enhanced monitoring, and separate administrative accounts.

3.5 Security Awareness and Training

All workforce members shall receive comprehensive security awareness training to understand their security responsibilities and recognize potential threats.

- New workforce members shall complete security awareness training within **[Number, e.g., 30]** days of hire.
- Annual refresher training shall be provided to all workforce members, with additional specialized training for roles with elevated security responsibilities.
- Training effectiveness shall be measured through assessments and security metrics.
- Targeted awareness campaigns shall be conducted to address emerging threats and security trends.

3.6 Incident Management

[Company Name] shall maintain the capability to detect, respond to, and recover from security incidents in a timely and effective manner.

- A formal incident response plan shall be maintained and tested regularly through tabletop exercises and simulations.
- All suspected security incidents shall be reported immediately through established channels and investigated according to documented procedures.
- Incident response activities shall be documented, and lessons learned shall be incorporated into security improvements.

- Regulatory notification requirements shall be met for incidents involving ePHI or other regulated data.

3.7 Business Continuity and Resilience

Critical business functions and information systems shall be protected through comprehensive business continuity and disaster recovery planning.

- Business impact assessments shall be conducted to identify critical functions and acceptable recovery timeframes.
- Backup and recovery procedures shall be implemented and tested at least annually to ensure data and system availability. Test results shall be documented.
- Alternative processing arrangements shall be established for critical systems to maintain operations during disruptions.
- Full recovery testing shall be performed annually and after significant infrastructure changes, with results documented and reviewed by the Information Security Committee.

3.8 Vendor and Third-Party Management

Security requirements shall be established and enforced for all vendors and third parties with access to **[Company Name]** information or systems.

- Security assessments shall be conducted before engaging vendors who will access, process, or store company information.
- Contractual agreements shall include specific security requirements, liability provisions, and audit rights.
- Business Associate Agreements (BAAs) shall be executed with all vendors who will handle ePHI.
- Vendor security performance shall be monitored through regular assessments and security questionnaires.

3.9 Compliance and Audit

[Company Name] shall maintain compliance with all applicable laws, regulations, and contractual obligations related to information security.

- Regular compliance assessments shall be conducted to verify adherence to HIPAA, SOC 2, and other applicable requirements.

- Internal audits shall be performed annually to evaluate the effectiveness of security controls and identify improvement opportunities.
- External audits and assessments shall be facilitated as required by regulatory or contractual obligations.
- Audit findings and corrective actions shall be tracked to completion and reported to appropriate management levels.

3.10 Continuous Improvement

The information security program shall be subject to continuous monitoring and improvement based on changing threats, business requirements, and industry best practices.

- Security metrics and key performance indicators (KPIs) shall be established and monitored to measure program effectiveness.
- Regular reviews of policies, procedures, and controls shall be conducted to ensure they remain current and effective.
- Industry threat intelligence and security advisories shall be monitored and incorporated into security planning.
- Employee feedback and suggestions for security improvements shall be encouraged and evaluated.

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(1) - Security Management Process
3.1	HIPAA Security Rule	45 CFR § 164.308(a)(2) - Assigned Security Responsibility
3.2	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(A) - Conduct periodic risk assessment

Policy Section	Standard/Framework	Control Reference
3.4	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Information Access Management
3.5	HIPAA Security Rule	45 CFR § 164.308(a)(5) - Security Awareness and Training
3.6	HIPAA Security Rule	45 CFR § 164.308(a)(6) - Security Incident Procedures
3.7	HIPAA Security Rule	45 CFR § 164.308(a)(7) - Contingency Plan
3.9	HIPAA Security Rule	45 CFR § 164.308(a)(8) - Evaluation
All	SOC 2 Trust Services Criteria	CC1.1 - Control Environment
3.1	SOC 2 Trust Services Criteria	CC2.1 - Communication and Information
3.2	SOC 2 Trust Services Criteria	CC3.1 - Risk Assessment Process
3.4	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.6	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
3.7	SOC 2 Trust Services Criteria	A1.1 - Availability

5. Definitions

Business Associate Agreement (BAA): A written contract between a covered entity and a business associate as required by HIPAA, establishing permitted uses and disclosures of ePHI.

Electronic Protected Health Information (ePHI): Individually identifiable health information that is created, stored, transmitted, or maintained electronically.

Information Security Management System (ISMS): A systematic approach to managing sensitive company information to keep it secure, including policies, procedures, and controls.

Least Privilege: The security principle of restricting access rights for users to the bare minimum permissions needed to perform their work.

Risk Assessment: The process of identifying vulnerabilities and threats to information assets and determining the risk posed by those threats.

Security Incident: Any event that could result in unauthorized access to, or disclosure, modification, or destruction of information assets.

6. Responsibilities

Role	Responsibility
Executive Leadership	Provide strategic direction and resources for the information security program. Approve security policies and ensure accountability.
Security Officer	Develop, implement, and maintain the ISMS. Oversee security operations, incident response, and compliance activities.
Information Security Committee	Provide governance oversight, approve policy changes, and make strategic security decisions.
IT Department	Implement technical security controls, manage system security configurations, and support security operations.
Human Resources	Integrate security requirements into hiring processes, conduct background checks, and manage workforce security training.
Legal/Compliance Team	Ensure regulatory compliance, review contracts for security requirements, and manage legal aspects of security incidents.

Role	Responsibility
Information Owners	Classify information assets, approve access requests, and ensure appropriate handling of sensitive data.
All Workforce Members	Comply with security policies, complete required training, and report security incidents or concerns.
Managers/Supervisors	Ensure their teams comply with security policies, approve access requests, and conduct regular access reviews.

Password Policy (SEC-POL-002)

1. Objective

The objective of this policy is to establish and enforce minimum standards for the creation, management, and protection of passwords. Strong password management is a critical control for safeguarding the confidentiality, integrity, and availability of **[Company Name]**'s information assets, particularly electronic Protected Health Information (ePHI), and for preventing unauthorized access to systems and data.

2. Scope

This policy applies to all **[Company Name]** workforce members (including employees, contractors, and temporary staff) and any third party that requires access to corporate systems, applications, network devices, and data. It governs all passwords used to access company resources, whether managed internally or by external service providers.

3. Policy

All systems and applications must be configured to enforce the following password parameters. Exceptions must be formally documented and approved by the Security Officer through the risk management process.

3.1 Password Construction Requirements

To ensure passwords are resistant to common attack vectors, all user-created passwords must adhere to the following complexity standards:

- **Length:** The minimum acceptable length for any password is twelve (12) characters. For accounts with elevated privileges (e.g., system administrators), the minimum length is sixteen (16) characters.
- **Complexity:** Passwords must contain characters from at least three (3) of the following four categories:
  - Uppercase letters (A-Z)
  - Lowercase letters (a-z)
  - Numbers (0-9)
  - Special characters (e.g., `!@#$%^\&*()`)

- **Prohibited Content:** Passwords must not contain common or easily guessable information. Systems shall be configured to check new passwords against a blocklist of common passwords and previously breached credentials. This includes, but is not limited to:
  - Company names (e.g., `[Company Name]`) or variations.
  - Usernames, personal names, family names, or pet names.
  - Dictionary words or common keyboard patterns (e.g., “password”, “qwerty”).
  - Consecutive or repeating characters (e.g., “111111”, “abcdefg”).

3.2 Password Lifecycle Management

Passwords must be actively managed throughout their lifecycle to limit the window of opportunity should a credential be compromised.

- **Password Age:** All user passwords must be changed at least every **[Number, e.g., 90]** days. This requirement may be waived for specific systems where strong MFA is enforced and breached password screening is active, subject to a documented risk assessment approved by the Security Officer.
- **Password History:** Systems must be configured to prevent the reuse of the previous **[Number, e.g., 5]** passwords for a given account.
- **Account Lockout:** User accounts must be automatically locked for a minimum of **[Duration, e.g., 30 minutes]** after **[Number, e.g., 5]** consecutive failed login attempts. The lockout must only be reversible by an authorized administrator or after the lockout duration has expired.

3.3 Multi-Factor Authentication (MFA)

MFA is required to provide an additional layer of security and shall be enforced for all workforce members across all company systems where the feature is supported.

- MFA must be enabled for all remote access to the corporate network (e.g., VPN).
- MFA is mandatory for accessing any system, application, or service that stores, processes, or transmits data classified as Confidential or Restricted, including ePHI.
- Approved MFA methods include authenticator applications (TOTP), hardware tokens, or biometric identifiers. SMS-based MFA is prohibited for accessing systems containing Restricted data.

3.4 Password Protection and Storage

Workforce members are responsible for the protection of their credentials.

- Passwords must never be written down, stored in plain text files, or shared with any other individual, including managers or IT staff. Passwords must not be transmitted via insecure channels such as email or instant messaging.
- The use of a company-approved and encrypted password manager is strongly encouraged for managing credentials.
- Systems must store passwords in a secure, salted, and hashed format using a strong, industry-recognized cryptographic algorithm (e.g., bcrypt, Argon2).

3.5 Initial Password Management and Resets

The process for establishing and resetting passwords must be secure.

- All new user accounts must be assigned a randomly generated, single-use temporary password.
- Users must be required to change their temporary password upon their first login.
- The identity of a user requesting a password reset must be verified by an authorized administrator through a secure, pre-defined process before the reset is performed.

3.6 System and Service Accounts

Non-interactive accounts (e.g., service accounts, API keys) must be securely managed.

- Service account credentials must be unique to that service and must not be shared between systems.
- Default vendor-supplied passwords for any application or device must be changed before the system is connected to the production network.
- Service account passwords must be rotated at least annually or immediately upon the departure of any workforce member who had access to them.

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
3.1, 3.2, 3.4	HIPAA Security Rule	45 CFR § 164.308(a)(5)(ii)(D) - Password Management
3.3, 3.5	HIPAA Security Rule	45 CFR § 164.312(a)(2)(i) - Unique User Identification
3.3	HIPAA Security Rule	45 CFR § 164.312(d) - Person or Entity Authentication
All	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.2, 3.5	SOC 2 Trust Services Criteria	CC6.2 - Prior to issuing system credentials…

5. Definitions

- **ePHI (electronic Protected Health Information):** Any protected health information (PHI) that is created, stored, transmitted, or received in any electronic format.
- **Workforce Member:** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for **[Company Name]**, is under the direct control of the company, whether or not they are paid by the company.
- **Multi-Factor Authentication (MFA):** An authentication method that requires the user to provide two or more verification factors to gain access to a resource.
- **Strong Password:** A password that meets the length and complexity requirements defined in section 3.1 of this policy.

6. Responsibilities

Role	Responsibility
Security Officer / Team	Own, review, and update this policy annually. Monitor for compliance and report on password-related security metrics.
IT Department	Implement and maintain the technical controls required to enforce this policy across all systems and applications. Manage the password reset process.
All Workforce Members	Adhere to this policy for all company-related accounts. Protect their credentials and immediately report any suspected compromise.

Risk Management Policy (SEC-POL-003)

1. Objective

The objective of this policy is to establish a comprehensive risk management framework for identifying, assessing, treating, and monitoring information security risks across **[Company Name]**. This policy ensures that security risks are systematically managed to protect the confidentiality, integrity, and availability of information assets, particularly electronic Protected Health Information (ePHI), and to maintain compliance with regulatory requirements while supporting business objectives.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, and third parties. It encompasses all information assets, systems, processes, and facilities owned, operated, or managed by **[Company Name]**, including cloud services, third-party systems, and remote work environments. This policy covers all types of information security risks, including cybersecurity threats, operational risks, compliance risks, and business continuity risks.

3. Policy

[Company Name] shall implement and maintain a systematic risk management process that is integrated into all business activities and decision-making processes.

3.1 Risk Management Framework

[Company Name] shall establish and maintain a formal risk management framework based on industry best practices and regulatory requirements.

- The risk management process shall follow a continuous cycle of identification, assessment, treatment, monitoring, and review.
- Risk management activities shall be documented, consistent, and repeatable across the organization.
- The framework shall be reviewed annually and updated as needed to reflect changes in the business environment, threat landscape, or regulatory requirements.
- Risk management shall be integrated into strategic planning, project management, system development, and vendor management processes.

3.2 Risk Identification

[Company Name] shall proactively identify information security risks through multiple sources and methods.

- Comprehensive risk assessments shall be conducted at least annually and whenever significant changes occur to systems, processes, or the business environment.
- Threat intelligence sources shall be monitored to identify emerging risks and attack vectors relevant to the healthcare industry.
- Vulnerability scanning shall be conducted at least quarterly for external-facing systems and annually for internal systems. External penetration testing shall be conducted at least annually.
- Business process reviews shall be conducted to identify operational and procedural risks.
- Risk identification shall consider internal and external threats, including but not limited to:
  - Cybersecurity threats (malware, phishing, unauthorized access)
  - Natural disasters and environmental hazards
  - Human error and insider threats
  - Technology failures and system outages
  - Regulatory and compliance changes
  - Third-party and vendor risks

3.3 Risk Assessment and Analysis

All identified risks shall be analyzed to determine their potential impact and likelihood of occurrence.

- Risk assessment shall consider both inherent risk (before controls) and residual risk (after controls are applied).
- Impact assessment shall evaluate potential consequences across multiple dimensions:
  - Financial impact (direct costs, regulatory fines, business disruption)
  - Operational impact (service disruption, productivity loss)
  - Reputational impact (customer trust, market confidence)
  - Regulatory impact (compliance violations, sanctions)
  - Patient safety and privacy implications
- Likelihood assessment shall consider:

  - Threat actor capabilities and motivations
  - Asset vulnerabilities and exposure
  - Effectiveness of existing controls
  - Historical incident data and industry trends

- Risk levels shall be determined using a standardized risk matrix. The criteria for impact, likelihood, and the resulting risk levels (**High**, **Medium**, **Low**) shall be formally documented and approved by the Information Security Committee.

3.4 Risk Treatment

[Company Name] shall implement appropriate risk treatment strategies based on risk levels and business priorities.

- Risk treatment options include:
  - **Accept:** Acknowledge and monitor risks that fall within acceptable tolerance levels
  - **Avoid:** Eliminate the risk by discontinuing or modifying activities
  - **Mitigate:** Implement controls to reduce likelihood or impact
  - **Transfer:** Share or transfer risk through insurance, contracts, or outsourcing
- High-risk items shall be addressed with priority and escalated to executive leadership for treatment decisions.
- Risk treatment plans shall include:
  - Specific actions and controls to be implemented
  - Responsible parties and timelines
  - Resource requirements and budget allocations
  - Success criteria and monitoring measures
- The effectiveness of risk treatments shall be monitored and measured regularly.

3.5 Risk Monitoring and Review

[Company Name] shall continuously monitor the risk environment and the effectiveness of risk treatments.

- A formal risk register shall be maintained to track all identified risks, their assessments, treatments, and current status.
- Risk levels shall be reviewed quarterly or when significant changes occur.

- Key risk indicators (KRIs) shall be established and monitored to provide early warning of increasing risk levels.
- Regular reports on risk status and trends shall be provided to executive leadership and the Information Security Committee.
- Annual risk assessment reviews shall validate the continued relevance of identified risks and assess the effectiveness of the overall risk management program.

3.6 Risk Communication and Reporting

Risk information shall be communicated effectively to all relevant stakeholders to support informed decision-making.

- Risk reporting shall be tailored to the audience, with executive summaries for leadership and detailed technical reports for operational teams.
- Critical risks and significant risk changes shall be escalated immediately to appropriate management levels.
- Risk communication shall include:
  - Current risk landscape and trends
  - Status of risk treatment activities
  - Emerging threats and vulnerabilities
  - Recommendations for risk mitigation
  - Compliance and regulatory implications

3.7 Third-Party Risk Management

Risks associated with third-party vendors, business associates, and service providers shall be assessed and managed as part of the overall risk management program.

- Due diligence assessments shall be conducted before engaging third parties that will access, process, or store company information.
- Contractual agreements shall include specific security requirements and risk allocation provisions.
- Ongoing monitoring of third-party security posture shall be conducted through security questionnaires, audits, and performance reviews.

- Third-party incidents and security events shall be tracked and incorporated into risk assessments.

3.8 Business Continuity and Operational Risk

Risk management shall include consideration of business continuity and operational resilience requirements.

- Business impact assessments (BIAs) shall be conducted to identify critical business functions and acceptable downtime limits.
- Single points of failure shall be identified and addressed through redundancy or alternative arrangements.
- Disaster recovery and business continuity plans shall be developed based on risk assessment results.
- Regular testing of continuity plans shall be conducted to validate their effectiveness.

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(A) - Conduct risk assessments
All	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(B) - Implement security measures
3.3	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(A) - Periodic risk assessment
3.7	HIPAA Security Rule	45 CFR § 164.314(a)(1) - Business Associate contracts
All	SOC 2 Trust Services Criteria	CC3.1 - Risk Assessment Process
3.2, 3.3	SOC 2 Trust Services Criteria	CC3.2 - Risk Identification and Analysis

Policy Section	Standard/Framework	Control Reference
3.4	SOC 2 Trust Services Criteria	CC3.3 - Risk Mitigation Activities
3.5	SOC 2 Trust Services Criteria	CC3.4 - Risk Monitoring Activities
3.8	SOC 2 Trust Services Criteria	A1.1 - Availability and Business Continuity
All	ISO/IEC 27001:2022	A.5.2 - Information security risk management

5. Definitions

Business Impact Assessment (BIA): Analysis to identify and evaluate potential impacts resulting from business disruption.

Inherent Risk: The level of risk that exists before any controls or mitigation measures are applied.

Key Risk Indicators (KRIs): Metrics that provide early warning signals of increasing risk exposure.

Residual Risk: The level of risk remaining after controls and mitigation measures have been applied.

Risk Appetite: The level of risk that an organization is willing to accept in pursuit of its objectives.

Risk Assessment: The systematic process of identifying, analyzing, and evaluating risks.

Risk Register: A document that records identified risks, their analysis, and risk response plans.

Risk Tolerance: The acceptable level of variation around risk appetite.

Threat Intelligence: Information about current and emerging security threats and vulnerabilities.

6. Responsibilities

Role	Responsibility
Executive Leadership	Formally document, approve, and annually review the company's risk appetite and tolerance levels. Approve risk treatment strategies for high-risk items. Provide resources for risk management activities.
Security Officer	Own and maintain the risk management program. Conduct risk assessments and coordinate risk treatment activities. Report risk status to leadership.
Information Security Committee	Review and approve risk management policies and procedures. Oversee high-risk treatment decisions and resource allocation.
Risk Management Team	Support risk assessment activities, maintain the risk register, and monitor risk treatment effectiveness.
IT Department	Identify technical risks and vulnerabilities. Implement technical risk controls and participate in risk assessments.
Business Unit Managers	Identify business risks within their areas. Participate in risk assessments and implement assigned risk treatments.
Asset/System Owners	Assess risks for their assigned assets or systems. Implement and maintain appropriate risk controls.
All Workforce Members	Report potential risks and security concerns. Comply with risk mitigation controls and procedures.

Role	Responsibility
Audit and Compliance Team	Validate risk assessment processes and control effectiveness. Ensure regulatory compliance requirements are addressed.

Data Classification and Handling Policy (SEC-POL-004)

1. Objective

The objective of this policy is to establish a comprehensive framework for classifying, handling, and protecting **[Company Name]**'s information assets based on their sensitivity, value, and regulatory requirements. This policy ensures that appropriate security controls are applied consistently across all information types, with particular emphasis on protecting electronic Protected Health Information (ePHI) and other sensitive data in accordance with HIPAA, HITECH, and SOC 2 requirements.

2. Scope

This policy applies to all **[Company Name]** workforce members, including employees, contractors, temporary staff, and third parties who create, access, process, store, transmit, or dispose of company information. It encompasses all information in any format (electronic, physical, or verbal) and at any location (on-premises, cloud, mobile devices, or third-party facilities). This policy covers the entire information lifecycle from creation to secure disposal.

3. Policy

All **[Company Name]** information shall be classified according to its sensitivity level and handled in accordance with established security controls that protect confidentiality, integrity, and availability.

3.1 Information Classification Framework

[Company Name] shall use a four-tier classification system to categorize all information assets:

Public: Information that can be freely shared with the general public without risk to **[Company Name]** or its stakeholders.

- Examples: Marketing materials, public website content, published research, press releases
- No special handling requirements beyond standard business practices

Internal: Information intended for use within **[Company Name]** that should not be disclosed to external parties without authorization.

- Examples: Internal policies, organizational charts, general business communications, non-sensitive system documentation
- Requires basic access controls and confidentiality agreements

Confidential: Sensitive information that could cause significant harm to **[Company Name]**, its customers, or business partners if disclosed without authorization.

- Examples: Financial records, strategic plans, customer lists, proprietary technology, employee personal information
- Requires enhanced security controls, encryption for transmission, and formal access approval

Restricted: Highly sensitive information that could cause severe harm if disclosed and is subject to regulatory protection requirements.

- Examples: ePHI, payment card data, social security numbers, authentication credentials, encryption keys
- Requires maximum security controls, encryption at rest and in transit, audit logging, and compliance with specific regulations

3.2 Information Classification Responsibilities

Information classification shall be assigned by designated information owners and applied consistently throughout the information lifecycle. The Security Officer shall maintain an Information Asset Inventory that documents all major information assets, their designated Information Owner, and their classification level.

- Information owners are responsible for the initial classification of data for which they are responsible, approving access requests, and ensuring data is handled according to this policy.
- Classification shall be assigned at the time of creation or acquisition and documented in the Information Asset Inventory.
- When information of different classification levels is combined, the resulting information shall be classified at the highest level of any component.
- Information owners shall review the classification of their information assets at least annually. This review shall be documented to provide an audit trail.

3.3 Handling Requirements by Classification Level

Specific security controls shall be implemented based on information classification levels.

3.3.1 Public Information

- No special access restrictions required
- Standard backup and archival procedures apply

- May be stored on standard business systems
- Can be transmitted via standard email or file sharing

3.3.2 Internal Information

- Access restricted to authorized **[Company Name]** workforce members
- Password-protected when stored on portable devices
- Transmitted via secure channels (encrypted email, secure file transfer)
- Stored on company-approved systems with appropriate access controls
- Covered by confidentiality agreements for third-party access

3.3.3 Confidential Information

- Access granted only on a need-to-know basis with formal approval
- Encrypted when stored on laptops, mobile devices, or removable media
- Transmitted only via encrypted channels (secure email, VPN, HTTPS)
- Stored on hardened systems with enhanced access controls and audit logging
- Protected by multi-factor authentication for system access
- Requires Non-Disclosure Agreements (NDAs) for third-party access
- Must be clearly labeled or marked to indicate classification level

3.3.4 Restricted Information

- Access granted only to specifically authorized individuals with business justification
- Encrypted at rest using **[Encryption Standard, e.g., AES-256]** or equivalent
- Encrypted in transit using **[Protocol, e.g., TLS 1.3]** or equivalent
- Stored only on systems specifically approved for Restricted data
- Protected by multi-factor authentication and privileged access controls
- All access logged and monitored for unauthorized activity
- Requires Business Associate Agreements (BAAs) for third-party handling
- Must be clearly labeled and handled according to regulatory requirements
- Subject to data loss prevention (DLP) monitoring and controls

3.4 Electronic Protected Health Information (ePHI) Handling

ePHI represents a subset of Restricted information requiring special handling under HIPAA regulations.

- ePHI shall be classified as Restricted and subject to all applicable controls
- Access limited to workforce members whose job functions require ePHI to perform their duties

- Minimum necessary standard applied to all ePHI access, use, and disclosure
- All ePHI access logged with user identification, date/time, and specific information accessed
- ePHI transmitted only via HIPAA-compliant secure methods
- Regular audits conducted to verify appropriate ePHI access and usage
- Breach notification procedures followed for any suspected ePHI compromise

3.5 Data Labeling and Marking

Information classification shall be clearly indicated through appropriate labeling mechanisms.

- Electronic documents shall include classification markings in headers, footers, or metadata
- Email communications containing Confidential or Restricted information shall include classification in subject lines
- Physical documents shall be marked with classification levels on each page
- Storage media shall be labeled with the highest classification level of contained information
- System interfaces shall display classification levels for data being accessed
- Classification labels shall remain with information throughout its lifecycle

3.6 Information Storage and Access Controls

Storage requirements shall be implemented based on information classification levels.

- All information systems shall maintain access control lists (ACLs) restricting access based on classification and business need
- Confidential and Restricted information shall be stored only on systems with appropriate security controls
- Cloud storage of Confidential and Restricted information requires encryption and compliance with security standards
- Regular access reviews shall be conducted quarterly for Restricted information and annually for Confidential information
- Automated tools shall be used where possible to enforce classification-based access controls

3.7 Information Transmission and Sharing

Information transmission methods shall align with classification requirements and recipient authorization levels.

- Public and Internal information may be transmitted via standard business communication channels

- Confidential information shall be encrypted during transmission using approved encryption methods
- Restricted information shall only be transmitted via secure, encrypted channels with confirmed recipient authorization
- File sharing services shall be approved for specific classification levels and configured with appropriate security settings
- Email systems shall include data loss prevention capabilities to prevent unauthorized transmission of sensitive information

3.8 Information Retention and Disposal

Information shall be retained according to business requirements and regulatory obligations, then securely disposed of when no longer needed.

- Retention schedules shall be established for each information type considering business, legal, and regulatory requirements
- ePHI shall be retained in accordance with HIPAA requirements and state regulations
- Secure disposal methods shall be used for all Confidential and Restricted information:
  - Electronic media: Cryptographic erasure, degaussing, or physical destruction
  - Physical documents: Cross-cut shredding or incineration
  - Optical media: Physical destruction
- Disposal activities shall be documented and verified for Restricted information
- Third-party disposal services shall provide certificates of destruction and maintain appropriate insurance coverage

3.9 Data Loss Prevention (DLP)

Technical controls shall be implemented to prevent unauthorized disclosure of sensitive information.

- DLP systems shall monitor network traffic, email, and endpoint devices for sensitive data patterns
- Automatic blocking or quarantine shall be implemented for attempted unauthorized transmission of Restricted information
- User education and warnings shall be provided when DLP systems detect potential policy violations
- DLP policies shall be regularly updated to address new data types and transmission methods
- Incident response procedures shall address DLP alerts and potential data loss events

3.10 Mobile Device and Remote Access

Special considerations shall apply to information access via mobile devices and remote locations.

- Mobile devices accessing Confidential or Restricted information shall be enrolled in mobile device management (MDM) systems
- Remote access to sensitive information shall require VPN connections and multi-factor authentication
- Personal devices used for business purposes shall comply with bring-your-own-device (BYOD) security requirements
- Cloud synchronization services shall be approved and configured appropriately for each classification level
- Lost or stolen devices shall be reported immediately and remotely wiped if containing sensitive information

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Information Access Management
3.4	HIPAA Security Rule	45 CFR § 164.502(b) - Minimum Necessary
3.4, 3.8	HIPAA Security Rule	45 CFR § 164.312(a)(1) - Access Control
3.3.4, 3.7	HIPAA Security Rule	45 CFR § 164.312(e)(1) - Transmission Security
3.3.4, 3.6	HIPAA Security Rule	45 CFR § 164.312(a)(2)(iv) - Encryption
3.4	HIPAA Security Rule	45 CFR § 164.312(b) - Audit Controls
All	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security

Policy Section	Standard/Framework	Control Reference
3.6, 3.7	SOC 2 Trust Services Criteria	CC6.7 - Data Transmission
3.8	SOC 2 Trust Services Criteria	CC6.5 - Data Disposal
3.9	SOC 2 Trust Services Criteria	CC7.2 - System Monitoring
All	ISO/IEC 27001:2022	A.5.12 - Classification of Information

5. Definitions

Business Associate Agreement (BAA): A written contract between a covered entity and a business associate establishing permitted uses and disclosures of ePHI.

Data Loss Prevention (DLP): Technology and processes designed to detect and prevent unauthorized transmission of sensitive information.

Electronic Protected Health Information (ePHI): Protected health information that is created, stored, transmitted, or maintained electronically.

Information Owner: The person responsible for the business content and context of information, including classification and access decisions.

Minimum Necessary: The HIPAA principle requiring that uses and disclosures of ePHI be limited to the smallest amount necessary to accomplish the intended purpose.

Non-Disclosure Agreement (NDA): A legal contract establishing confidential relationships and restricting information sharing.

6. Responsibilities

Role	Responsibility
Information Owners	Classify information assets, approve access requests, conduct periodic classification reviews, and ensure appropriate handling.

Role	Responsibility
Security Officer	Develop and maintain classification policies, monitor compliance, and investigate classification violations.
IT Department	Implement technical controls for each classification level, maintain DLP systems, and provide secure storage and transmission capabilities.
Data Stewards	Ensure day-to-day compliance with classification requirements, assist with labeling, and report classification issues.
Privacy Officer	Oversee ePHI classification and handling, ensure HIPAA compliance, and manage privacy impact assessments.
All Workforce Members	Follow classification and handling requirements, properly label information, and report suspected violations or data loss.
Managers/Supervisors	Ensure their teams understand and comply with classification requirements, approve access requests within their authority.
Records Management	Maintain retention schedules, coordinate secure disposal activities, and ensure compliance with legal hold requirements.

Vendor and Third-Party Risk Management Policy (SEC-POL-005)

1. Objective

The objective of this policy is to establish comprehensive requirements for assessing, managing, and monitoring security and compliance risks associated with vendors, third-party service providers, and business associates. This policy ensures that **[Company Name]** maintains appropriate oversight of external parties who access, process, store, or transmit company information, particularly electronic Protected Health Information (ePHI), while maintaining compliance with HIPAA, HITECH, and SOC 2 requirements.

2. Scope

This policy applies to all **[Company Name]** workforce members involved in vendor selection, contract negotiation, or ongoing vendor management. It encompasses all external parties including vendors, service providers, consultants, contractors, business associates, and any other third parties that have access to **[Company Name]** information systems, data, or facilities. This policy covers the entire vendor lifecycle from initial assessment through contract termination and data return.

3. Policy

[Company Name] shall implement a comprehensive vendor risk management program to ensure that all third-party relationships meet security, privacy, and compliance requirements.

3.1 Vendor Classification and Risk Assessment

All vendors shall be classified based on their risk level and subject to appropriate due diligence and ongoing monitoring.

3.1.1 Vendor Risk Classification

Vendors shall be classified into risk categories based on the following factors:

- Type and sensitivity of data accessed (ePHI, Confidential, Internal, Public)
- Level of system access required (network, applications, databases, privileged access)
- Geographic location and regulatory jurisdiction
- Financial impact and business criticality
- Duration and scope of engagement

Risk Classifications:

- **High Risk:** Vendors with access to ePHI, Restricted data, or critical systems; cloud service providers; vendors with privileged access
- **Medium Risk:** Vendors with access to Confidential data or internal systems; vendors providing business-critical services
- **Low Risk:** Vendors with limited access to Internal data or no direct system access; vendors providing non-critical services

3.1.2 Pre-Engagement Risk Assessment

Prior to engaging any vendor, the designated Business Owner, in coordination with the Security Officer, shall conduct and document a formal risk assessment appropriate to the vendor's risk classification. The results of this assessment must be formally approved before contracts are executed.

High-Risk Vendor Requirements:

- Comprehensive security questionnaire (e.g., SIG Lite, CAIQ, or equivalent)
- Third-party security assessment report (SOC 2 Type II, ISO 27001, or equivalent)
- Financial stability assessment
- Reference checks with existing customers
- On-site security assessment for critical vendors
- Cyber insurance verification
- Background check requirements for vendor personnel

Medium-Risk Vendor Requirements:

- Standard security questionnaire
- Third-party assessment report or self-attestation
- Financial stability review
- Reference checks
- Insurance verification

Low-Risk Vendor Requirements:

- Basic security questionnaire or self-attestation
- General insurance verification

3.2 Business Associate Agreements and Contractual Requirements

All vendor contracts shall include appropriate security, privacy, and compliance provisions based on the vendor's risk level and data access requirements, as approved by the Legal and Security teams.

3.2.1 Business Associate Agreements (BAAs)

A signed BAA shall be executed before any vendor is granted access to ePHI.

BAAs shall include:

- Permitted uses and disclosures of ePHI
- Prohibition of unauthorized use or disclosure
- Safeguarding requirements equivalent to the HIPAA Security Rule
- Requirement to report any Security Incident, including any Breach of Unsecured PHI, to **[Company Name]** without unreasonable delay and in no case later than 24 hours after discovery.
- Access, amendment, and accounting of disclosures rights
- Requirement to return or destroy all ePHI upon contract termination, and to provide a certificate of destruction.
- Audit rights and compliance monitoring provisions
- Subcontractor requirements and flow-down of all BAA obligations

3.2.2 Security Contract Provisions

All vendor contracts shall include security provisions appropriate to the risk level:

Mandatory Security Clauses:

- Data protection and confidentiality requirements
- Incident notification and response procedures, including a maximum notification timeframe.
- Right to audit and conduct security assessments
- Personnel security and background check requirements
- Data location restrictions and cross-border transfer limitations
- Insurance and liability provisions
- Compliance with applicable laws and regulations
- Requirement for secure data return or destruction upon contract termination, with verification.

Additional High-Risk Vendor Clauses:

- Specific security control requirements (encryption, access controls, logging)
- Regular security reporting and metrics
- Breach notification timelines and procedures
- Limitation of data retention and use
- Subcontractor approval and oversight requirements

- Business continuity and disaster recovery provisions
- Right to terminate for security violations

3.3 Vendor Security Monitoring and Ongoing Assessment

Ongoing monitoring shall be conducted to ensure vendors maintain appropriate security posture throughout the engagement lifecycle.

3.3.1 Continuous Monitoring Requirements

- Annual security questionnaire updates for High and Medium-risk vendors
- Review of updated security certifications and assessment reports
- Monitoring of vendor security incidents and breach notifications
- Financial stability monitoring for critical vendors
- Performance and service level monitoring
- Compliance with contractual security requirements

3.3.2 Periodic Assessments

- High-Risk vendors: Annual comprehensive security assessment
- Medium-Risk vendors: Biennial security assessment
- Low-Risk vendors: Assessment upon contract renewal

3.3.3 Vendor Security Incident Management

- Vendors shall notify **[Company Name]** of security incidents within contractually specified timeframes
- **[Company Name]** shall assess the impact of vendor incidents on company operations and data
- Incident response coordination with vendors shall follow documented procedures
- Lessons learned from vendor incidents shall be incorporated into future risk assessments

3.4 Vendor Access Management

Access granted to vendors shall be controlled and monitored in accordance with the principle of least privilege.

3.4.1 Access Provisioning

- Vendor access requests shall be formally approved by the business owner and security team
- Access shall be limited to the minimum necessary to perform contracted services
- Vendor personnel shall be individually identified and authenticated

- Shared or generic accounts shall not be used for vendor access
- Multi-factor authentication shall be required for all High-risk vendor access

3.4.2 Access Monitoring and Review

- All vendor access shall be logged and monitored for inappropriate activity
- Quarterly access reviews shall be conducted for High-risk vendors
- Annual access reviews shall be conducted for Medium and Low-risk vendors
- Access shall be promptly revoked upon contract termination or personnel changes

3.5 Vendor Onboarding and Offboarding

Formal processes shall be established for vendor onboarding and offboarding to ensure security requirements are met.

3.5.1 Vendor Onboarding Process

1. Risk assessment and classification
2. Security questionnaire and documentation review
3. Contract negotiation including security provisions
4. BAA execution (if handling ePHI)
5. Security orientation and training (if required)
6. Access provisioning and testing
7. Ongoing monitoring setup

3.5.2 Vendor Offboarding Process

1. Access revocation and account deactivation
2. Data return or secure destruction verification
3. Equipment and credential return
4. Final security assessment and documentation
5. Contract closure and relationship termination
6. Lessons learned documentation

3.6 Cloud Service Provider Management

Cloud service providers shall be subject to enhanced security requirements due to the sensitivity of data and critical nature of services.

3.6.1 Cloud Provider Requirements

- SOC 2 Type II certification or equivalent (ISO 27001, FedRAMP)

- Compliance with relevant industry standards (HIPAA, PCI-DSS if applicable)
- Data encryption at rest and in transit
- Geographic data location controls and restrictions
- Incident response and breach notification procedures
- Business continuity and disaster recovery capabilities
- Regular penetration testing and vulnerability assessments

3.6.2 Cloud Service Monitoring

- Regular review of service provider security posture and certifications
- Monitoring of provider security advisories and incident notifications
- Assessment of configuration changes and security updates
- Periodic review of data access logs and administrative activities

3.7 Subcontractor and Fourth-Party Risk Management

Vendors shall be required to manage risks associated with their subcontractors and ensure equivalent security standards.

- Vendors shall obtain written approval before engaging subcontractors for services involving **[Company Name]** data
- Subcontractors shall be subject to the same security requirements as primary vendors
- Vendors shall maintain oversight of subcontractor security practices
- Flow-down of security requirements through the entire supply chain
- Notification requirements for subcontractor changes or incidents

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
3.2.1	HIPAA Security Rule	45 CFR § 164.314(a)(1) - Business Associate Contracts
3.2.1	HIPAA Security Rule	45 CFR § 164.314(a)(2) - Business Associate Safeguards
3.1, 3.3	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(A) - Risk Assessment

Policy Section	Standard/Framework	Control Reference
3.4	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Information Access Management
3.3.3	HIPAA Security Rule	45 CFR § 164.308(a)(6) - Security Incident Procedures
All	SOC 2 Trust Services Criteria	CC9.1 - Vendor Management
3.1, 3.3	SOC 2 Trust Services Criteria	CC9.2 - Vendor Risk Assessment
3.2	SOC 2 Trust Services Criteria	CC9.3 - Vendor Agreements
3.6	SOC 2 Trust Services Criteria	A1.2 - System Capacity
All	ISO/IEC 27001:2022	A.5.19 - Information security in supplier relationships

5. Definitions

Business Associate: A person or entity that performs functions or activities on behalf of a covered entity that involve access to ePHI.

Business Associate Agreement (BAA): A written contract between a covered entity and a business associate required by HIPAA.

Cloud Service Provider: A company that offers network services, infrastructure, or business applications in the cloud.

Due Diligence: The investigation or exercise of care that a reasonable business or person is expected to take before entering into an agreement or contract.

Fourth Party: A subcontractor or service provider used by a third-party vendor.

Service Level Agreement (SLA): A contract between a service provider and customer that defines the level of service expected.

Subcontractor: An entity engaged by a business associate to perform functions or activities on behalf of the business associate.

Vendor Risk Assessment: The process of evaluating the potential risks associated with engaging a third-party vendor.

6. Responsibilities

Role	Responsibility
Procurement Team	Coordinate vendor selection process, ensure security requirements are included in RFPs, and facilitate contract negotiations.
Security Officer	Develop vendor security requirements, conduct risk assessments, and monitor vendor security compliance.
Privacy Officer	Ensure BAA requirements are met, oversee ePHI handling by vendors, and manage privacy impact assessments.
Legal/Contracts Team	Negotiate security contract provisions, ensure legal compliance, and manage contract lifecycle.
Business Owners	Define business requirements, approve vendor selections, and monitor service delivery performance.
IT Department	Implement technical controls for vendor access, monitor vendor system activity, and manage vendor integrations.
Risk Management Team	Assess vendor-related risks, maintain vendor risk register, and coordinate risk treatment activities.
Finance Team	Assess vendor financial stability, manage vendor insurance requirements, and oversee payment processes.

Role	Responsibility
All Workforce Members	Report vendor security concerns, comply with vendor interaction policies, and protect company information shared with vendors.

Physical Security Policy (SEC-POL-006)

1. Objective

The objective of this policy is to establish comprehensive physical security requirements for **[Company Name]**'s facilities, equipment, and workforce in a cloud-first environment. This policy ensures that appropriate physical safeguards are implemented to protect against unauthorized access to facilities, equipment theft, environmental hazards, and physical threats while maintaining the confidentiality, integrity, and availability of information assets and electronic Protected Health Information (ePHI) in compliance with HIPAA, HITECH, and SOC 2 requirements. Given **[Company Name]**'s cloud-based infrastructure, this policy focuses on corporate facilities, endpoint devices, and the oversight of cloud provider physical security controls.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, visitors, and third parties who access company facilities or handle company equipment. It encompasses all physical locations including corporate offices, remote work environments, temporary workspaces, and any location where company information is accessed or processed. This policy covers all physical assets including workstations, laptops, mobile devices, printed materials, storage media, networking equipment, and any other tangible assets containing or providing access to company information. While **[Company Name]** operates with cloud-based infrastructure, this policy also addresses the oversight and validation of cloud provider physical security controls.

3. Policy

[Company Name] shall implement layered physical security controls appropriate to the cloud-based operating model while ensuring comprehensive protection of all physical assets and facilities.

3.1 Facility Security and Access Control

Physical access to all **[Company Name]** facilities shall be controlled and monitored to prevent unauthorized entry and protect information assets.

3.1.1 Office Facility Security

Access Control Systems:

- Electronic badge access systems shall be implemented for all corporate facilities
- Multi-factor authentication required for access to areas containing sensitive information

- Visitor management system with registration, identification verification, and escort requirements
- Access permissions based on role and business need with quarterly access reviews
- Emergency access procedures and override capabilities for authorized personnel

Physical Security Zones:

- **Public Areas:** Reception, common areas - basic access controls and monitoring
- **General Office:** Standard work areas - badge access required, visitor escort beyond this point
- **Restricted Areas:** IT equipment rooms, executive offices, records storage - enhanced access controls
- **Highly Restricted:** Server rooms, telecommunications closets - maximum security controls with biometric access

Facility Monitoring:

- CCTV surveillance systems covering all entry/exit points and sensitive areas
- Motion detection systems for after-hours monitoring
- 24/7 monitoring service or security personnel for critical facilities
- Video retention for minimum **[Duration, e.g., 90 days]** with secure storage
- Integration with local law enforcement and emergency services

3.1.2 Remote Work Environment Security

Home Office Security Requirements:

- Dedicated workspace with physical security measures to prevent unauthorized access
- Locking mechanisms for desks, filing cabinets, and storage areas containing company information
- Privacy screens or positioning to prevent visual access to company information
- Secure storage for company equipment when not in use
- Environmental protections against theft, damage, and unauthorized access

Co-working and Public Space Restrictions:

- Prohibition of accessing ePHI or Restricted information in public spaces
- Privacy screens required when working on Confidential information in shared spaces
- Secure Wi-Fi requirements and VPN usage for all company system access
- Physical security of devices and materials in temporary work environments
- Clean desk practices and secure storage of sensitive materials

3.2 Equipment and Asset Protection

All company equipment and physical assets shall be protected against theft, damage, and unauthorized access throughout their lifecycle.

3.2.1 Endpoint Device Security

Physical Device Protection:

- Cable locks or security devices required for desktop computers in office environments
- Laptop encryption and remote wipe capabilities for all mobile devices
- Asset tagging and inventory tracking for all company equipment
- Secure storage requirements for devices containing sensitive information
- Insurance coverage for high-value equipment and mobile devices

Device Lifecycle Management:

- Secure provisioning process with pre-configured security settings
- Regular physical inventory audits (quarterly for mobile devices, annually for fixed assets)
- Maintenance and repair procedures that protect data confidentiality
- Secure decommissioning with verified data destruction
- Return procedures for workforce member separation or equipment refresh

3.2.2 Removable Media and Storage Security

Media Handling Requirements:

- Encrypted storage required for all removable media containing company information
- Locked storage for backup media, USB drives, and optical media
- Chain of custody procedures for media transportation
- Inventory management system for tracking media location and usage
- Environmental protection for media storage (temperature, humidity, magnetic fields)

Secure Disposal Procedures:

- Physical destruction required for all media containing ePHI or Restricted information
- Certified disposal vendors with appropriate security clearances and insurance
- Witnessed destruction for high-sensitivity media with certificates of completion
- Degaussing or physical destruction for magnetic media
- Secure overwriting followed by physical destruction for solid-state media

3.3 Cloud Provider Physical Security Oversight

[Company Name] shall validate and monitor the physical security controls implemented by cloud service providers to ensure appropriate protection of company data and systems. This oversight is the responsibility of the designated Cloud Security Team or Security Officer.

3.3.1 Cloud Provider Assessment

Physical Security Requirements:

- SOC 2 Type II certification or equivalent demonstrating physical security controls
- Multi-factor authentication and biometric access controls for data center facilities
- 24/7 physical security monitoring and surveillance systems
- Environmental controls including fire suppression, climate control, and power management
- Geographic separation of data centers for disaster recovery and business continuity

Compliance Validation:

- The Cloud Security Team shall conduct and document an annual review of all critical cloud providers' security certifications (e.g., SOC 2 Type II, ISO 27001) and audit reports.
- Validation of physical security controls through review of third-party assessments.
- Contractual agreements must include requirements for physical security standards and incident notification within a defined timeframe.
- Right-to-audit clauses shall be included in contracts for critical cloud services where feasible.
- Geographic data location controls shall be configured to align with legal and regulatory requirements.

3.3.2 Cloud Security Monitoring

Ongoing Oversight:

- The Cloud Security Team shall conduct and document a quarterly review of cloud provider security incident reports and notifications.
- Continuous monitoring of cloud provider security advisories and documentation for significant control changes.
- An annual assessment of cloud provider business continuity and disaster recovery test results shall be conducted and documented.
- The Cloud Security Team shall validate that data center certifications and compliance status remain active and in good standing.
- Coordination with cloud providers for security investigations and incident response shall be managed by the Security Officer and Incident Response Team.

3.4 Physical Document and Information Security

Physical documents and printed materials containing sensitive information shall be protected throughout their lifecycle.

3.4.1 Document Handling Requirements

Secure Document Management:

- Classification and marking of all physical documents based on sensitivity levels
- Locked storage for documents containing Confidential or Restricted information
- Clean desk policy requiring secure storage of sensitive documents when unattended
- Controlled access to document storage areas with access logging
- Regular inventory and review of stored documents

Document Transportation:

- Secure transportation methods for sensitive documents between facilities
- Chain of custody documentation for document transfers
- Encrypted digital alternatives preferred over physical document transportation
- Approval requirements for removing sensitive documents from secure facilities
- Insurance coverage for valuable or sensitive document shipments

3.4.2 Printing and Output Security

Secure Printing Controls:

- Follow-me printing or secure print release for sensitive documents
- Physical presence required at printer for document retrieval
- Automatic deletion of print jobs after specified time periods
- Monitoring and logging of all print activities for sensitive information
- Secure disposal of misprints and unwanted printouts

Print Environment Security:

- Printers located in secure areas with appropriate access controls
- Network printing security with authentication and encryption
- Regular maintenance and service with data protection requirements
- Secure disposal of printer components containing data (hard drives, memory)
- Vendor agreements for secure printer maintenance and support

3.5 Environmental and Infrastructure Security

Environmental controls and infrastructure security measures shall protect against natural disasters, power failures, and other environmental threats.

3.5.1 Environmental Controls

Climate and Power Management:

- Uninterruptible Power Supply (UPS) systems for critical equipment and systems
- Surge protection and power conditioning for all electronic equipment
- Emergency lighting and communication systems for facility emergencies
- Temperature and humidity monitoring for equipment areas
- Backup power systems for extended outages

Fire and Safety Protection:

- Fire detection and suppression systems appropriate for electronic equipment
- Emergency evacuation procedures and regular drills
- First aid and emergency response equipment and training
- Safety equipment and procedures for equipment maintenance
- Integration with local emergency services and authorities

3.5.2 Physical Infrastructure Security

Building and Perimeter Security:

- Secure building construction with reinforced entry points
- Perimeter fencing and lighting for standalone facilities
- Vehicle access controls and parking security measures
- Landscape design that supports security monitoring and access control
- Regular security assessments and penetration testing of physical controls

Utility and Service Protection:

- Secure access to utility rooms and service areas
- Protection of telecommunications and network infrastructure
- Backup communication systems for emergency situations
- Service provider security requirements and background checks
- Regular inspection and maintenance of physical infrastructure

3.6 Workplace Security and Safety

Comprehensive workplace security measures shall protect workforce members and maintain a secure working environment.

3.6.1 Personnel Security

Workplace Safety:

- Background check requirements for personnel with physical access to sensitive areas
- Security awareness training including physical security procedures
- Identification badge requirements for all workforce members and visitors
- Reporting procedures for suspicious activities and security incidents
- Security escort requirements for unauthorized individuals

Emergency Procedures:

- Emergency contact information and notification procedures
- Evacuation plans and assembly points for different emergency scenarios
- Emergency communication systems and backup procedures
- Business continuity procedures for facility unavailability
- Coordination with law enforcement and emergency services

3.6.2 Visitor and Contractor Management

Visitor Control Procedures:

- Advance registration and approval for all visitors
- Photo identification verification and temporary badge issuance
- Continuous escort requirements for visitors in sensitive areas
- Visitor activity logging and monitoring
- Background check requirements for contractors with extended facility access

Contractor Security Requirements:

- Security agreements and confidentiality requirements for all contractors
- Equipment and tool inspection procedures for maintenance personnel
- Supervised access for contractors working on sensitive systems
- Verification of contractor personnel authorization and identification
- Secure disposal of any materials generated during contractor activities

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
All	HIPAA Security Rule	45 CFR § 164.310(a)(1) - Facility Access Controls
3.1	HIPAA Security Rule	45 CFR § 164.310(a)(2)(i) - Authorized Access Procedures
3.2	HIPAA Security Rule	45 CFR § 164.310(b) - Workstation Use
3.2, 3.4	HIPAA Security Rule	45 CFR § 164.310(d)(1) - Device and Media Controls
3.2.2	HIPAA Security Rule	45 CFR § 164.310(d)(2)(i) - Media Disposal
All	SOC 2 Trust Services Criteria	CC6.4 - Physical Access Controls
3.5	SOC 2 Trust Services Criteria	A1.1 - System Availability
3.3	SOC 2 Trust Services Criteria	CC9.1 - Vendor Management
All	ISO/IEC 27001:2022	A.7.1 - Physical security perimeters
3.2	ISO/IEC 27001:2022	A.7.2 - Physical entry controls

5. Definitions

Clean Desk Policy: Security practice requiring sensitive materials to be secured when workspaces are unattended.

Cloud Service Provider: Third-party organization providing cloud computing services including infrastructure, platforms, or software.

Environmental Controls: Systems and procedures designed to protect against environmental hazards such as fire, flood, temperature extremes, and power failures.

Follow-Me Printing: Secure printing system requiring user authentication at the printer before documents are released.

Multi-Factor Authentication: Security process requiring two or more authentication factors for access verification.

Physical Security Perimeter: Physical boundary around facilities, systems, or areas requiring protection.

Tailgating: Unauthorized access gained by following an authorized person through a controlled access point.

Visitor Management System: Automated system for registering, tracking, and managing facility visitors.

6. Responsibilities

Role	Responsibility
Security Officer	Develop physical security policies, oversee security system implementation, coordinate with facilities management, and ensure compliance with security standards.
Facilities Management	Maintain physical security systems, manage environmental controls, coordinate building security, and ensure compliance with safety regulations.
IT Security Team	Secure IT equipment and infrastructure, coordinate physical and logical security measures, and monitor security events.
Human Resources	Manage badge access provisioning, conduct background checks, coordinate visitor management, and integrate security into HR processes.

Role	Responsibility
Reception/Administrative Staff	Manage visitor registration and badging, monitor lobby areas, enforce visitor policies, and coordinate with security team.
Cloud Security Team	Assess cloud provider physical security controls, monitor cloud security compliance, and coordinate cloud security requirements.
All Workforce Members	Comply with physical security policies, secure workspaces and equipment, challenge unauthorized individuals, and report security incidents.
Managers/Supervisors	Ensure team compliance with physical security policies, approve visitor access, support emergency procedures, and manage physical asset inventory.
Remote Workers	Implement home office security measures, protect company equipment, follow secure work practices, and report security concerns.

AI Acceptable Use Policy (SEC-POL-007)

1. Objective

The objective of this policy is to establish comprehensive guidelines for the acceptable and secure use of Artificial Intelligence (AI) and Machine Learning (ML) technologies at **[Company Name]**. This policy ensures that AI tools and systems are used responsibly, ethically, and securely while protecting the confidentiality, integrity, and availability of company information, particularly electronic Protected Health Information (ePHI). This policy addresses the unique risks associated with AI technologies including data privacy, bias, transparency, and regulatory compliance with HIPAA, HITECH, and SOC 2 requirements while enabling innovation and productivity improvements through responsible AI adoption.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, third parties, and business associates who use, develop, deploy, or manage AI and ML technologies on behalf of the organization. It encompasses all AI applications including but not limited to generative AI tools (ChatGPT, Claude, Bard), machine learning models, automated decision-making systems, natural language processing tools, computer vision systems, and AI-powered business applications. This policy covers both internally developed AI systems and third-party AI services, regardless of deployment model (cloud-based, on-premises, or hybrid), and applies to all use cases including business operations, software development, clinical decision support, and administrative functions.

3. Policy

[Company Name] shall implement comprehensive governance and security controls for AI technologies to ensure responsible, ethical, and compliant use while protecting sensitive information and maintaining stakeholder trust.

3.1 AI Governance Framework

A formal AI governance structure shall be established to oversee the evaluation, approval, deployment, and monitoring of AI technologies across the organization.

3.1.1 AI Governance Committee

Committee Structure:

- AI Governance Committee comprising representatives from Security, Privacy, Legal, Clinical, IT, and Business units
- Designated AI Ethics Officer responsible for ethical AI oversight and compliance
- Regular committee meetings (monthly) to review AI initiatives and address emerging issues
- Clear escalation procedures for AI-related risks and ethical concerns
- Annual review of AI governance policies and procedures

Committee Responsibilities:

- Approval of new AI tools and applications for organizational use
- Risk assessment and mitigation for AI implementations
- Policy development and maintenance for AI acceptable use
- Incident response coordination for AI-related security or ethical issues
- Training and awareness program oversight for AI usage

3.1.2 AI Risk Assessment Process

Pre-Implementation Assessment:

- A formal, documented risk assessment is required for all new AI tools or significant changes to existing tools before deployment.
- Data sensitivity analysis to identify the use of ePHI, PII, or other confidential information.
- Bias and fairness evaluation for AI systems that could impact individuals.
- Privacy Impact Assessment (PIA) for AI applications processing personal data.
- Security assessment of the AI tool and its vendor, including data protection and access controls.
- The completed risk assessment must be submitted to and formally approved by the AI Governance Committee prior to use.

Risk Categories:

- **High Risk:** AI systems processing ePHI, making automated decisions affecting individuals, or handling Restricted data
- **Medium Risk:** AI systems processing Confidential data or providing business-critical functions
- **Low Risk:** AI systems processing only Public or Internal data with limited business impact

3.2 Data Protection and Privacy

AI systems shall implement comprehensive data protection measures to safeguard sensitive information and ensure privacy compliance.

3.2.1 Data Handling Requirements

ePHI and Sensitive Data Protection:

- The use of ePHI or any other Restricted data is *strictly prohibited* in any public or third-party AI system unless the service is explicitly listed in the company's Approved AI Service Catalog and is governed by a signed Business Associate Agreement (BAA).
- Data minimization principles shall be applied to all AI training and inference data, ensuring only the minimum necessary data is used for the intended purpose.
- Encryption is required for all data at rest and in transit for AI systems handling Confidential or Restricted data.
- Access to AI systems handling sensitive data shall be logged and reviewed at least quarterly.

Data Anonymization and De-identification:

- When healthcare data is used for AI model training, it must be de-identified in accordance with the standards set forth in the HIPAA Privacy Rule (45 CFR § 164.514), using either the Safe Harbor method or Expert Determination.
- The de-identification method used must be documented and the documentation retained.
- Regular validation of de-identification effectiveness shall be conducted.
- Any attempt to re-identify individuals from a de-identified dataset is strictly prohibited.

3.2.2 Third-Party AI Service Usage

Approved AI Services:

- The AI Governance Committee shall maintain an inventory of approved AI services, including documentation of their security and privacy assessments
- Contractual requirements for data protection, privacy, and compliance
- Vendor assessment including data handling practices, security controls, and compliance certifications
- Geographic data location restrictions and cross-border transfer limitations
- Service level agreements including data breach notification and incident response

Prohibited AI Services:

- Public AI systems without appropriate enterprise controls and data protection
- AI services with inadequate privacy protection or unclear data usage policies
- AI tools that retain or use input data for training without explicit consent
- AI systems operating in jurisdictions with inadequate data protection laws
- Free or consumer-grade AI services for processing company information

3.3 Ethical AI Use and Bias Prevention

AI systems shall be developed and deployed in accordance with ethical principles and bias prevention measures to ensure fair and responsible outcomes.

3.3.1 Ethical AI Principles

Fairness and Non-Discrimination:

- Regular testing for bias in AI systems affecting hiring, promotion, or patient care decisions
- Diverse training data and validation datasets to minimize algorithmic bias
- Monitoring of AI system outcomes for disparate impact on protected groups
- Remediation procedures for identified bias or discriminatory outcomes
- Documentation of fairness measures and bias testing results

Transparency and Explainability:

- Clear documentation of AI system capabilities, limitations, and decision-making processes
- Explainable AI requirements for systems making decisions affecting individuals
- User notification when interacting with AI systems or AI-generated content
- Model interpretability measures for critical business decisions
- Regular communication about AI system changes and updates

3.3.2 Human Oversight and Control

Human-in-the-Loop Requirements:

- Human review and approval required for AI-generated decisions affecting individuals
- Override capabilities for all automated AI decisions
- Training for workforce members supervising AI systems
- Clear escalation procedures for AI system malfunctions or unexpected outcomes
- Regular validation of AI system performance and accuracy

3.4 AI Security Controls

Comprehensive security controls shall be implemented to protect AI systems from threats and ensure system integrity.

3.4.1 AI System Security

Access Controls and Authentication:

- Role-based access control for all AI systems and platforms

- Multi-factor authentication required for AI system access
- Privileged access management for AI system administration
- Regular access reviews and recertification for AI system users
- API security controls for AI service integrations

Model Security and Protection:

- Protection of AI models as intellectual property and trade secrets
- Secure storage and versioning of AI models and training data
- Adversarial attack prevention and detection measures
- Model integrity validation and tampering detection
- Secure deployment pipelines for AI model updates

3.4.2 AI Data Security

Training Data Protection:

- Encryption of all AI training datasets containing sensitive information
- Secure data pipelines for AI model training and validation
- Data lineage tracking and documentation for AI datasets
- Regular data quality and integrity assessments
- Secure deletion of training data when no longer needed

Inference Data Security:

- Real-time data protection for AI system inputs and outputs
- Monitoring and logging of all AI system interactions
- Data loss prevention controls for AI-generated content
- Backup and recovery procedures for AI system data
- Incident response procedures for AI data breaches

3.5 AI Development and Deployment

Secure development practices shall be applied to all AI system development and deployment activities.

3.5.1 AI Development Lifecycle

Secure AI Development:

- Security requirements integration into AI development lifecycle
- Code review and security testing for AI applications

- Vulnerability assessment of AI frameworks and libraries
- Secure coding practices for AI model development
- Version control and change management for AI systems

Model Validation and Testing:

- Comprehensive testing of AI models before production deployment
- Performance monitoring and accuracy validation in production
- A/B testing and gradual rollout procedures for new AI models
- Rollback procedures for AI model failures or performance degradation
- Documentation of model validation results and limitations

3.5.2 AI System Monitoring

Continuous Monitoring:

- Real-time monitoring of AI system performance and accuracy
- Anomaly detection for unusual AI system behavior or outputs
- User feedback collection and analysis for AI system improvements
- Regular audits of AI system decisions and outcomes
- Incident detection and alerting for AI system failures

Performance Metrics:

- Key performance indicators (KPIs) for AI system effectiveness
- Accuracy, precision, recall, and other relevant metrics tracking
- User satisfaction and experience metrics for AI applications
- Business impact measurement of AI system implementations
- Regular reporting on AI system performance to governance committee

3.6 Acceptable Use Guidelines

Specific guidelines shall govern the appropriate use of AI technologies by workforce members across different business functions.

3.6.1 General Use Guidelines

Permitted AI Use Cases:

- Content creation assistance for marketing, documentation, and communications
- Code generation and software development assistance
- Data analysis and business intelligence support

- Process automation and workflow optimization
- Research and information gathering for business purposes

Prohibited AI Use Cases:

- Clinical diagnosis or treatment recommendations without appropriate oversight
- Automated decision-making for hiring, firing, or promotion without human review
- Processing of ePHI through unauthorized AI systems
- Generation of misleading, false, or deceptive content
- Circumvention of security controls or policy violations

3.6.2 Role-Specific Guidelines

Healthcare and Clinical Staff:

- AI clinical decision support tools must be FDA-approved or validated through appropriate processes
- Human clinician review required for all AI-generated clinical recommendations
- Patient consent required for AI system involvement in care delivery
- Documentation of AI system use in patient medical records
- Compliance with medical ethics and professional standards

Software Development Teams:

- Code review required for all AI-generated code before production deployment
- Security testing of AI-generated code for vulnerabilities
- Intellectual property review for AI-generated content and code
- Documentation of AI tool usage in development processes
- Compliance with secure development lifecycle requirements

Business and Administrative Functions:

- Data privacy review for AI applications processing personal information
- Accuracy validation for AI-generated business documents and reports
- Human review for AI-assisted decision-making processes
- Compliance with regulatory requirements for automated processing
- Documentation of AI system use in business processes

3.7 Training and Awareness

Comprehensive training programs shall ensure workforce members understand AI policies, risks, and best practices.

3.7.1 AI Training Requirements

General AI Awareness:

- Annual training for all workforce members on AI acceptable use policies
- Role-specific training for users of AI systems and tools
- Ethics and bias awareness training for AI system developers and users
- Privacy and security training for AI applications handling sensitive data
- Regular updates on new AI technologies and policy changes

Specialized Training:

- Advanced training for AI governance committee members
- Technical training for AI system developers and administrators
- Clinical training for healthcare staff using AI decision support tools
- Legal and compliance training for AI oversight roles
- Incident response training for AI-related security events

3.7.2 AI Literacy and Competency

Competency Assessment:

- Regular assessment of workforce AI literacy and competency
- Certification requirements for critical AI system users
- Continuing education for AI technology developments
- Knowledge sharing and best practices documentation
- Performance evaluation integration of AI policy compliance

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framework	Control Reference
3.2.1	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Information Access Management

Policy Section	Standard/Framework	Control Reference
3.2.1	HIPAA Privacy Rule	45 CFR § 164.502(b) - Minimum Necessary Standard
3.2.2	HIPAA Security Rule	45 CFR § 164.314(a)(1) - Business Associate Contracts
3.4	HIPAA Security Rule	45 CFR § 164.312(b) - Audit Controls
All	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.2	SOC 2 Trust Services Criteria	CC6.7 - Data Transmission and Disposal
3.1	SOC 2 Trust Services Criteria	CC2.1 - Communication and Information
3.5	SOC 2 Trust Services Criteria	CC8.1 - System Development
All	EU AI Act	Risk-based AI governance and compliance
3.3	NIST AI Risk Management Framework	AI risk management and governance

5. Definitions

Algorithm Bias: Systematic prejudice in AI systems that results in unfair treatment of certain groups or individuals.

Artificial Intelligence (AI): Computer systems that can perform tasks typically requiring human intelligence, including learning, reasoning, and perception.

Business Associate Agreement (BAA): Contract required under HIPAA when third parties access or process ePHI on behalf of covered entities.

De-identification: Process of removing personal identifiers from data to protect individual privacy.

Explainable AI (XAI): AI systems designed to provide understandable explanations for their decisions and recommendations.

Large Language Model (LLM): Type of AI model trained on vast amounts of text data to understand and generate human-like text.

Machine Learning (ML): Subset of AI that enables systems to learn and improve from data without explicit programming.

Model Drift: Degradation in AI model performance over time due to changes in underlying data patterns.

6. Responsibilities

Role	Responsibility
AI Ethics Officer	Develop AI governance policies, oversee ethical AI practices, coordinate AI risk assessments, and ensure compliance with AI regulations.
AI Governance Committee	Approve AI implementations, review AI risks, make policy decisions, and provide strategic guidance for AI initiatives.
Security Officer	Ensure AI security controls, assess AI-related risks, monitor AI security incidents, and integrate AI into security programs.
Privacy Officer	Ensure AI privacy compliance, oversee ePHI protection in AI systems, conduct privacy impact assessments, and manage AI-related privacy risks.
Data Scientists/AI Engineers	Develop secure and ethical AI systems, implement bias testing, document AI model limitations, and ensure model validation and monitoring.

Role	Responsibility
IT Security Team	Implement AI security controls, monitor AI system security, respond to AI security incidents, and maintain AI security infrastructure.
Business Unit Leaders	Ensure team compliance with AI policies, approve AI tool usage, provide business requirements for AI systems, and support AI governance activities.
Legal and Compliance Team	Ensure AI regulatory compliance, review AI contracts and agreements, assess legal risks, and provide guidance on AI liability issues.
All Workforce Members	Comply with AI acceptable use policies, report AI-related concerns, complete required AI training, and use AI tools responsibly and ethically.

Vulnerability Management Policy (SEC-POL-008)

1. Objective

The objective of this policy is to establish a systematic and continuous process for identifying, prioritizing, remediating, and verifying security vulnerabilities across all of **[Company Name]**'s information assets. This policy ensures that risks to the confidentiality, integrity, and availability of data, including electronic Protected Health Information (ePHI), are managed in a timely and effective manner.

2. Scope

This policy applies to all information systems and assets owned or managed by **[Company Name]**, including but not limited to, servers, workstations, network devices, applications (both internally developed and third-party), and cloud infrastructure.

3. Policy

[Company Name] shall implement and maintain a comprehensive vulnerability management program that covers the full lifecycle of a vulnerability.

3.1 Vulnerability Management Lifecycle

The program is structured around a continuous four-phase lifecycle:

- **1. Discovery:** The Security Team is responsible for identifying vulnerabilities through multiple methods, including:
  - **Automated Scanning:** Regular, automated vulnerability scans of the environment.
  - **Threat Intelligence:** Monitoring security feeds, vendor notifications, and public disclosures.
  - **Penetration Testing:** Annual internal and external penetration tests.
  - **Manual Reporting:** Reports from workforce members or external security researchers.
- **2. Prioritization:** All discovered vulnerabilities must be assigned a severity rating to prioritize remediation efforts.
  - The primary method for rating vulnerabilities will be the Common Vulnerability Scoring System (CVSS) version 3.x.

- The Security Team will enrich the CVSS base score with the following contextual factors to determine a final, internal Risk Rating:
  - ⋆ **Asset Criticality:** As defined in the **[Company Name]** System & Data Inventory (e.g., is the asset mission-critical, does it store ePHI?).
  - ⋆ **Data Sensitivity:** The classification of data stored or processed by the asset.
  - ⋆ **Network Exposure:** Whether the vulnerability is exploitable from the internet or requires internal access.
  - ⋆ **Threat Intelligence:** Any evidence of active exploitation of the vulnerability in the wild.
  - ⋆ **Compensating Controls:** The presence of other security layers (e.g., WAF, MFA) that might reduce the likelihood of exploitation.
- Severity levels are defined as:
  - ⋆ **Critical:** CVSS Score 9.0 - 10.0
  - ⋆ **High:** CVSS Score 7.0 - 8.9
  - ⋆ **Medium:** CVSS Score 4.0 - 6.9
  - ⋆ **Low:** CVSS Score 0.1 - 3.9

- **3. Remediation:** Vulnerabilities must be remediated by the responsible asset owner within a defined timeframe, based on their severity rating. The Remediation SLA begins at the time a vulnerability is formally validated and assigned to the relevant asset owner by the Security Team in the vulnerability tracking system. Remediation may include applying vendor patches, implementing configuration changes, or deploying compensating controls. All remediation activities must follow the Change Control Policy (ENG-POL-002).

Severity	**Remediation Service Level Agreement (SLA)**
Critical	**[Number, e.g., 15]** calendar days
High	**[Number, e.g., 30]** calendar days
Medium	**[Number, e.g., 90]** calendar days

Low	**[Number, e.g., 180]** calendar days or at the next scheduled maintenance

- **4. Verification:** After remediation has been applied, the Security Team must perform a verification scan to confirm that the vulnerability has been successfully resolved. All verification results must be documented in the vulnerability tracking system.

3.2 Vulnerability Scanning

To ensure comprehensive discovery, the following scanning schedule will be maintained:

- **External Scans:** Unauthenticated scans of all internet-facing systems must be performed at least weekly.
- **Internal Scans:** Authenticated scans of all internal production systems and workstations must be performed at least monthly.
- **Application Scans:** Dynamic and/or static analysis of in-house developed applications must be performed prior to any major release.
- **Scan Result Processing:** All vulnerability scan results must be automatically ingested into a centralized tracking system. The Security Team is responsible for reviewing scan reports within **[Number, e.g., 1]** business day(s) and initiating the Prioritization and Remediation lifecycle for all new, valid findings.

3.3 Exception Management and Risk Acceptance

In cases where a vulnerability cannot be remediated within the defined SLA (e.g., due to a lack of a vendor patch or a high risk of business disruption), a formal exception must be requested.

- **Request:** The asset owner must submit a formal exception request to the Security Team. The request must include a business justification, a risk analysis, and details of any proposed compensating controls. An acceptable compensating control must be a documented and testable measure that measurably reduces the likelihood or impact of the specific vulnerability being exploited.
- **Approval:** All exception requests require documented approval from the asset owner's manager and the **[Role Title, e.g., Security Officer]**. For Critical or High severity vulnerabilities, approval from the **[Role Title, e.g., Chief Technology Officer]** is also required.

- **Duration:** Approved exceptions are temporary and must be reviewed at least quarterly. An exception is not a permanent solution.
- **Documentation:** All approved exceptions, including the justification and compensating controls, must be documented in a centralized risk register.

4. Standards Compliance

This policy is designed to comply with and support the following industry standards and regulations.

Policy Section	Standard/Framewo	Control Reference
All	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(A) - Risk Analysis
All	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(B) - Risk Management
3.1, 3.2	SOC 2 Trust Services Criteria	CC7.1 - The entity uses detection and monitoring procedures to identify… vulnerabilities.

5. Definitions

- **Vulnerability:** A weakness in an information system, security procedure, internal control, or implementation that could be exploited by a threat source.
- **CVSS (Common Vulnerability Scoring System):** An open industry standard for assessing the severity of computer system security vulnerabilities.
- **Remediation:** The process of fixing or eliminating a discovered vulnerability.
- **Compensating Control:** An alternative security measure put in place to reduce the risk of a vulnerability that cannot be directly remediated.

6. Responsibilities

Role	Responsibility
Security Team	Own, review, and update this policy annually. Manage the vulnerability scanning tools, prioritize vulnerabilities, track remediation efforts, and manage the exception process.
IT / System Owners	Remediate vulnerabilities on systems under their control within the defined SLAs. Request exceptions when necessary and implement approved compensating controls.
Engineering Team	Remediate vulnerabilities discovered in internally developed applications.

Information Security Committee Charter Procedure (SEC-PROC-001)

1. Purpose

To define the operating rules, membership, authority, and responsibilities of the Information Security Committee.

2. Scope

This procedure applies to the Information Security Committee and all personnel involved in the governance of the Information Security Management System (ISMS).

3. Overview

This procedure outlines the process for scheduling and conducting Information Security Committee meetings, setting agendas, documenting minutes, and managing policy changes to ensure effective oversight of the company's security posture.

4. Procedure

Step	Who	What
1	Committee Chair	Schedules quarterly meetings and distributes the agenda to all committee members at least one week prior.
2	Committee Members	Attend scheduled meetings, participate in discussions, and vote on proposed policy changes.
3	Committee Secretary	Records detailed meeting minutes, including key decisions, action items, and voting results.
4	Committee Secretary	Distributes the signed and dated meeting minutes to all members within five business days of the meeting.
5	Policy/Procedure Owner	Submits proposed changes to policies or procedures to the Committee Chair for agenda inclusion.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2	CC2.1
1-5	HIPAA/HITECH	45 CFR § 164.308(a)(2)

6. Artifact(s)

Signed and dated meeting minutes are stored in the company's document management system.

7. Definitions

ISMS: Information Security Management System.

8. Responsibilities

Role	Responsibility
Committee Chair	Presides over meetings, sets the agenda, and ensures procedures are followed.
Committee Members	Attend meetings, provide input, and vote on security-related matters.
Committee Secretary	Documents and distributes meeting minutes and maintains committee records.

Internal Audit Procedure (SEC-PROC-002)

1. Purpose

To outline the process for planning, conducting, and reporting on annual internal audits of the Information Security Management System (ISMS).

2. Scope

This procedure applies to all internal audits of the ISMS, including all systems, processes, and controls that fall under its scope.

3. Overview

This procedure details the end-to-end process for the annual internal audit of the ISMS. It covers the creation of an audit plan, the execution of audit fieldwork, the documentation of findings, the generation of a formal report, and the tracking of corrective actions through to resolution.

4. Procedure

Step	Who	What
1	Head of Internal Audit	Develops and documents an annual internal audit plan, including scope, objectives, and resources.
2	Internal Auditor(s)	Conducts audit fieldwork by gathering and analyzing evidence to assess control effectiveness.
3	Internal Auditor(s)	Documents all findings, including non-conformities, observations, and opportunities for improvement.
4	Head of Internal Audit	Creates and distributes a formal audit report detailing the scope, findings, and recommendations.
5	Management/Proces Owners	Develops and implements corrective action plans for identified findings.
6	Head of Internal Audit	Tracks the status of all corrective actions to completion in a tracking log.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	HIPAA/HITECH	45 CFR § 164.308(a)(8)

6. Artifact(s)

A final internal audit report and a corrective action tracking log.

7. Definitions

ISMS: Information Security Management System.

8. Responsibilities

Role	Responsibility
Head of Internal Audit	Oversees the entire audit process, from planning to reporting and tracking.
Internal Auditor(s)	Executes the audit plan, documents findings, and assists in report creation.
Management/Process Owners	Responsible for implementing corrective actions to address audit findings.

Password Policy Exception Procedure (SEC-PROC-003)

1. Purpose

To provide a formal process for requesting, reviewing, and documenting exceptions to the Password Policy.

2. Scope

This procedure applies to all personnel and systems within the organization when a deviation from the established Password Policy is required.

3. Overview

This procedure outlines the steps for submitting, evaluating, and documenting requests for exceptions to the company's Password Policy. It ensures that any deviation is subject to a formal risk assessment and approval by the Security Officer, and that all approved exceptions are tracked.

4. Procedure

Step	Who	What
1	User or System Owner	Submits a formal Password Policy Exception Request form, including a detailed justification and any proposed compensating controls.
2	Security Officer	Conducts a risk assessment of the request to evaluate potential security impacts and formally approves or denies the request in writing.
3	Security Officer	Documents all approved exceptions, including the justification, risk assessment, and expiration date, in a central tracking log.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-3	SOC 2	CC6.1
1-3	HIPAA/HITECH	45 CFR § 164.308(a)(5)(ii)(D)

6. Artifact(s)

A completed and approved Password Policy Exception Request form.

7. Definitions

N/A

8. Responsibilities

Role	Responsibility
User/System Owner	Initiates the exception request and provides all necessary information and justification.
Security Officer	Performs a risk assessment, makes the final decision on the exception request, and maintains all documentation.

Risk Assessment Procedure (SEC-PROC-004)

1. Purpose

To establish a systematic process for conducting annual and ad-hoc risk assessments to identify, analyze, and evaluate risks to the organization's information assets.

2. Scope

This procedure applies to all information assets and processes within the scope of the Information Security Management System (ISMS). Risk assessments are performed annually and on an ad-hoc basis when significant changes occur.

3. Overview

This procedure details the methodology for conducting risk assessments. It covers the identification of assets, threats, and vulnerabilities; the analysis of likelihood and impact; the calculation of risk levels; and the documentation of results in the risk register and a formal report.

4. Procedure

Step	Who	What
1	Risk Assessment Team	Identifies and documents critical information assets and their owners.
2	Risk Assessment Team	Identifies potential threats and vulnerabilities associated with each asset.
3	Risk Assessment Team	Analyzes the likelihood of a threat exploiting a vulnerability and the potential impact to the organization.
4	Risk Assessment Team	Calculates the overall risk level for each identified threat/vulnerability pair based on predefined risk criteria.

Step	Who	What
5	Risk Assessment Team	Documents the results of the assessment, including identified risks, risk levels, and recommended treatments, in the risk register.
6	Security Officer	Compiles a formal Risk Assessment Report summarizing the key findings and recommendations for management review.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2	CC3.2
1-6	HIPAA/HITECH	45 CFR § 164.308(a)(1)(ii)(A)

6. Artifact(s)

An updated Risk Register and a formal Risk Assessment Report.

7. Definitions

Risk Register: A log of identified risks, their characteristics, and their status.

8. Responsibilities

Role	Responsibility
Risk Assessment Team	Conducts the risk assessment activities as outlined in this procedure.
Security Officer	Oversees the risk assessment process and is responsible for the final report.
Asset Owners	Provide necessary information about their assets for the risk assessment.

Vendor Risk Assessment and Onboarding Procedure (SEC-PROC-005)

1. Purpose

To detail the process for assessing a new vendor's security posture before engagement to ensure they meet the company's security requirements.

2. Scope

This procedure applies to all new vendors that will handle, store, process, or transmit company data, or will be connected to the company's network or systems.

3. Overview

This procedure outlines the steps for conducting due diligence on prospective vendors. It includes initiating the request, classifying the vendor's risk level, performing a security assessment tailored to that risk level, and obtaining formal approval before a contract is signed.

4. Procedure

Step	Who	What
1	Business Owner	Initiates a new vendor request and provides details about the services and data involved.
2	Security Team	Classifies the vendor's inherent risk level (e.g., High, Medium, Low) based on the nature of the service and data access.
3	Security Team	Performs due diligence activities based on the risk level. This may include sending security questionnaires, reviewing SOC 2 reports, or conducting technical calls.
4	Security Team	Documents the findings in a Vendor Risk Assessment Report and provides a recommendation.
5	Business Owner/Manag	Reviews the assessment report and formally approves or denies the vendor engagement.
6	Legal/Procurei	Executes the contract only after receiving formal approval from the security review.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2	CC9.2
1-6	HIPAA/HITECH	45 CFR § 164.308(a)(1)(ii)(A)

6. Artifact(s)

A completed Vendor Risk Assessment Report.

7. Definitions

SOC 2 Report: A report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy.

8. Responsibilities

Role	Responsibility
Business Owner	Initiates the vendor request and acts as the primary point of contact for the vendor relationship.
Security Team	Conducts the risk classification and due diligence assessment and produces the final report.
Management	Provides final approval for vendor engagement based on the risk assessment findings.

Facility Access Management Procedure (SEC-PROC-006)

1. Purpose

To describe the process for provisioning, reviewing, and revoking physical access to company facilities to ensure a secure physical environment.

2. Scope

This procedure applies to all employees, contractors, and visitors requiring access to company-controlled facilities.

3. Overview

This procedure outlines the standardized steps for managing physical access. It covers the issuance of access badges for new personnel, the process for registering and escorting visitors, and the requirement for regular reviews of access rights to ensure they remain appropriate.

4. Procedure

Step	Who	What
1	Hiring Manager/HR	Submits a facility access request form for a new employee or contractor.
2	Facilities/Securit Team	Provisions and issues a physical access badge based on the approved request, corresponding to the individual's role and location.
3	Employee/Host	Registers visitors at the front desk. Visitors must sign in, be issued a temporary badge, and be escorted at all times.
4	Facilities/Securit Team	Conducts and documents quarterly reviews of all physical access permissions to ensure they are still required and appropriate.
5	Manager/HR	Notifies the Facilities/Security Team immediately upon termination of an employee or contractor to revoke physical access.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2	CC6.4
1-5	HIPAA/HITECH	45 CFR § 164.310(a)(2)(i)

6. Artifact(s)

A completed access request form and an access review log.

7. Definitions

N/A

8. Responsibilities

Role	Responsibility
Hiring Manager/HR	Initiates and approves access requests for new personnel and reports terminations promptly.
Facilities/Security Team	Manages the physical access control system, issues badges, conducts access reviews, and manages visitor logs.
Employee/Host	Responsible for their assigned access badge and for escorting any visitors they host.

AI Tool Risk Assessment and Approval Procedure (SEC-PROC-007)

1. Purpose

To define the formal process for submitting a new AI tool for consideration and for the AI Governance Committee to perform a risk assessment to ensure its use aligns with company policies and risk appetite.

2. Scope

This procedure applies to all employees and contractors who wish to use a new Artificial Intelligence (AI) tool for business purposes, especially those that may process sensitive or confidential company or customer data.

3. Overview

This procedure outlines the workflow for the review and approval of new AI tools. It details the submission process for an employee, the required information for the request, and the steps the AI Governance Committee takes to conduct a thorough risk assessment before formally approving or denying its use.

4. Procedure

Step	Who	What
1	Employee/Req	Submits an “AI Tool Risk Assessment and Approval Form” to the AI Governance Committee.
2	Employee/Req	Provides all required information, including the tool’s purpose, data sensitivity, privacy impact, and vendor documentation.
3	AI Governance Committee	Reviews the submission and conducts a risk assessment, considering factors like data security, privacy, compliance, and operational impact.
4	AI Governance Committee	Formally approves or denies the request in writing, documenting the rationale for the decision and any conditions for use.

Step	Who	What
5	AI Governance Committee	Maintains a register of all approved and denied AI tools.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2	CC2.1
1-5	NIST AI Risk Management Framework	Entire Framework

6. Artifact(s)

A completed AI Risk Assessment and Approval Form.

7. Definitions

AI: Artificial Intelligence.

8. Responsibilities

Role	Responsibility
Employee/Reque	Initiates the review process and provides complete and accurate information about the proposed AI tool.
AI Governance Committee	Conducts the risk assessment, makes the final approval decision, and maintains records of all assessments.

Vulnerability Management Procedure (SEC-PROC-008)

1. Purpose

To describe the workflow for identifying, prioritizing, remediating, and verifying vulnerabilities across the organization's systems and applications.

2. Scope

This procedure applies to all company-owned or managed systems, networks, and applications. It covers the entire lifecycle of a vulnerability from discovery to closure.

3. Overview

This procedure outlines the systematic process for managing vulnerabilities. It begins with the discovery of vulnerabilities through various means, followed by prioritization based on risk. It then details the assignment of remediation tasks to asset owners, the remediation process itself, and the final verification by the Security Team to confirm the fix.

4. Procedure

Step	Who	What
1	Security Team	Discovers vulnerabilities through automated scans, penetration tests, and other sources.
2	Security Team	Prioritizes identified vulnerabilities using CVSS scores and contextual business risk factors.
3	Security Team	Assigns prioritized findings to the appropriate asset owners for remediation, including defined Service Level Agreements (SLAs).
4	Asset Owner	Performs remediation actions to fix the vulnerability within the specified SLA.
5	Security Team	Performs verification scans or other tests to confirm that the vulnerability has been successfully remediated.
6	Security Team	Closes the finding in the vulnerability tracking system upon successful verification.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2	CC7.1
1-6	HIPAA/HITECH	45 CFR § 164.308(a)(1)(ii)(B)

6. Artifact(s)

An entry in the vulnerability tracking system showing the lifecycle of a vulnerability from discovery to verified remediation.

7. Definitions

CVSS: Common Vulnerability Scoring System. A standard for assessing the severity of computer system security vulnerabilities. **SLA:** Service Level Agreement. A commitment between a service provider and a client.

8. Responsibilities

Role	Responsibility
Security Team	Responsible for discovering, prioritizing, assigning, and verifying vulnerabilities.
Asset Owner	Responsible for remediating identified vulnerabilities on their assigned assets within the defined SLAs.

Vulnerability Management Exception Procedure (SEC-PROC-009)

1. Purpose

To outline the process for formally requesting, approving, and documenting an exception to a remediation Service Level Agreement (SLA) for an identified vulnerability.

2. Scope

This procedure applies when an asset owner cannot remediate a vulnerability within the timeframe defined in the Vulnerability Management Policy and requires a formal exception.

3. Overview

This procedure provides a structured pathway for managing situations where immediate vulnerability remediation is not feasible. It details the steps for an asset owner to request an exception, the multi-level approval workflow based on vulnerability severity, and the requirement to document approved exceptions in the risk register for regular review.

4. Procedure

Step	Who	What
1	Asset Owner	Submits a formal Exception Request Form, including a detailed justification, risk analysis, and any compensating controls in place.
2	Asset Owner's Manager	Reviews the request for business validity and approves or denies it.
3	Security Officer	Reviews the request for security implications and approves or denies it.
4	CTO	For Critical or High-risk vulnerabilities, provides the final layer of approval.
5	Security Team	Documents the approved exception, including its expiration date, in the risk register.
6	Security Team	Reviews all active exceptions on a quarterly basis to ensure they are still valid and necessary.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2	CC7.1
1-6	HIPAA/HITECH	45 CFR § 164.308(a)(1)(ii)(B)

6. Artifact(s)

A completed and approved Exception Request Form documented in the risk register.

7. Definitions

SLA: Service Level Agreement. **CTO:** Chief Technology Officer.

8. Responsibilities

Role	Responsibility
Asset Owner	Initiates the exception request and provides all necessary justification and documentation.
Asset Owner's Manager	Provides the initial business approval for the exception request.
Security Officer	Provides security approval and ensures proper documentation in the risk register.
CTO	Provides final approval for exceptions related to high-impact vulnerabilities.