Health Tech Security Policies & Procedures

openaccesspolicies.org

Table of Contents

Identity and Access Management (IAM) Policy (AC-POL-001)

1. Objective

The objective of this policy is to define the requirements for managing user identities and access rights to **[Company Name]**'s information systems and data throughout the complete user lifecycle. This policy ensures that access is granted based on the principles of least privilege and separation of duties, while implementing automated access management processes that minimize administrative overhead and enhance security effectiveness. This policy focuses on standard user access management, while privileged access is addressed in the Privileged Access Management Policy (AC-POL-004) and remote access is covered in the Remote Work Policy (AC-POL-003).

2. Scope

This policy applies to all **[Company Name]** workforce members, third-party contractors, and vendors who require access to company information assets. This includes standard user access to applications, file shares, collaboration tools, and business systems. This policy applies to all physical and virtual locations where company information assets are accessed, stored, or processed, including corporate offices and approved remote work locations. This policy does not cover privileged administrative access (see AC-POL-004) or remote work security requirements (see AC-POL-003).

3. Policy

Access to all **[Company Name]** information assets shall be managed through a formal, documented process that implements automated access management and exception-based reviews to ensure appropriate access while minimizing administrative overhead.

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 shall be managed throughout the entire duration of a user's relationship with the company.

3.2.1 Access Provisioning

Access for new workforce members shall be provisioned through a formal request submitted by their direct manager via the official IT service request process. Access rights shall be assigned exclusively based on pre-defined roles and responsibilities documented in the user's job description and organizational role matrix.

3.2.2 Access Modification

When a workforce member changes roles or responsibilities within the company, their manager shall submit a formal request to modify access rights through the designated change management process. All previous access rights that are no longer required for the new role shall be immediately revoked. New access rights shall be granted strictly according to the principle of least privilege and the requirements of the new role.

3.2.3 Access Deprovisioning

Upon termination of employment or contract, all access to company systems, applications, and physical facilities shall be revoked according to risk-based timelines. **Critical/High-Risk Terminations** (involuntary terminations, security incidents, executive departures): All logical and physical access shall be revoked within **[Number, e.g., 2]** hours of notification. **Standard Terminations** (voluntary resignations, contract completions): All access shall be revoked within **[Number, e.g., 24]** hours from the official termination time. **Low-Risk Extended Transitions** (retirements, internal transfers): Access revocation shall be coordinated over **[Number, e.g., 72]** hours to ensure smooth knowledge transfer while maintaining security controls.

3.3 Automated Access Reviews and Monitoring

Access reviews for standard (non-privileged) access shall be conducted at least annually. Privileged access review cadence is defined in the Privileged Access Management Policy (AC-POL-004) and shall be performed quarterly. Continuous monitoring and event-driven reviews shall supplement these schedules.

3.3.1 Automated Monitoring Requirements

Identity and access management systems shall be configured to automatically detect and alert on access anomalies. These monitoring systems shall identify dormant accounts with no login activity

for **[Duration, e.g., 90 days]**, privilege escalation events, unusual access patterns, and accounts without recent manager validation.

3.3.2 Role-Based Access Control Implementation

Access rights shall be managed primarily through automated role assignment based on job function, department, and manager hierarchy integrated with the HR information system. When employees change roles, access shall be automatically adjusted based on their new role assignment without manual intervention.

3.3.3 Exception-Based Review Schedule

- Standard (non-privileged) access: Annual reviews with manager/system owner attestation and usage analysis
- Privileged accounts: Quarterly reviews per AC-POL-004 (PAM), with detailed usage analysis and anomaly detection
- Event-driven reviews: Conducted upon significant role changes, mergers/acquisitions, security incidents, or when monitoring identifies anomalies

3.4 System and Network Access Controls

Logical access to systems and networks shall be secured through standardized authentication and session management controls.

3.4.1 Unique User Identification

Every user shall be assigned a unique user ID for all system access. The use of shared or generic user accounts is strictly prohibited across all company systems and applications.

3.4.2 Authentication Requirements

All system access shall be authenticated through a combination of a unique user ID and a strong password, as defined in the Password Policy (SEC-POL-002). Multi-factor authentication (MFA) shall be required for all systems containing sensitive data including ePHI.

3.4.3 Session Management

Systems shall 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. Session timeouts shall be enforced at both the application and network levels.

3.4.4 Network Access Controls

Network access controls shall restrict user access to only authorized network segments and resources based on role and business need. Network segregation shall be implemented and maintained to enforce access boundaries.

3.5 Privileged Access Management

Accounts with elevated administrative privileges are subject to enhanced controls as defined in the Privileged Access Management Policy (AC-POL-004). Standard users requiring administrative access shall follow the just-in-time access procedures and enhanced authentication requirements specified in that policy.

3.6 Third-Party Access

Prior to granting any access, all third parties shall 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]** shall have a signed Business Associate Agreement (BAA) in place before access is provisioned.

3.6.1 Third-Party Security Review

Prior to granting any access, all third parties shall 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]** shall have a signed Business Associate Agreement (BAA) in place before access is provisioned.

3.6.2 Third-Party Access Restrictions

Third-party access shall be limited to only the specific systems and data required for their contractual function. Access scope shall be documented and approved by the system owner and security team

before provisioning.

3.6.3 Third-Party Access Management

Third-party access shall be time-bound, with access automatically expiring upon contract termination or completion of work. All third-party activities shall be monitored, with all access attempts and activities logged and reviewed according to the organization's monitoring standards.

3.7 Remote Access

Remote access to company systems and data is governed by the Remote Work Policy (AC-POL-003), which establishes comprehensive security requirements for accessing company resources from locations outside corporate offices. All workforce members working remotely must comply with the network connectivity, device security, and data handling requirements specified in that policy.

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Security Officer / Team	Own, review, and update this policy annually. Audit access controls and review compliance. Configure automated monitoring rules, review access anomalies, and coordinate exception-based reviews.
IT Department	Implement, manage, and monitor technical access controls. Process access provisioning, modification, and deprovisioning requests.
Platform Engineer	Implement RBAC systems, configure automated remediation, and maintain IAM integrations with HR systems.
DevOps Engineer	Set up automated alerting, monitor system performance, and optimize alert thresholds.

Role	Responsibility
Managers / System Owners	Request and approve access for their direct reports. Conduct annual access reviews for their teams and systems and respond to access validation requests.
HR Department	Maintain accurate role and manager information in HR systems for automated access management. Immediately notify IT of employee terminations and role changes.
Compliance Officer	Maintain access management documentation for audit purposes and ensure regulatory compliance requirements are met.
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

3.1.1 Company Property Rights

All network infrastructure, systems, and the data created or transmitted over them shall be considered the property of **[Company Name]**. Workforce members shall acknowledge that their use of these resources is subject to company policies and applicable laws.

3.1.2 Privacy Expectations

Workforce members shall have no expectation of privacy in their use of company network resources. To ensure compliance and protect information assets, network traffic shall be actively monitored for security threats and potential policy violations, in accordance with applicable laws.

3.1.3 Business Purpose Requirements

Network resources shall be provided primarily for business-related activities. Limited and incidental personal use shall be 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.

3.2.1 Credential Security

Workforce members shall not share their account credentials or allow others to use their accounts to access the network. Account credentials shall be protected as confidential information and used only by the authorized individual.

3.2.2 Malicious Software Prevention

Intentionally introducing malicious software (e.g., viruses, worms, spyware) into the network shall be strictly prohibited. Workforce members shall exercise caution when opening email attachments or clicking on links from unknown sources. To support this requirement, workforce members shall complete annual security awareness training, which provides specific guidance on identifying and avoiding threats like phishing and malware.

3.2.3 Security Incident Reporting

Any suspected security incident, unauthorized access, or vulnerability shall be reported immediately to the IT Department and the Security Officer. Workforce members shall not attempt to investigate or remediate security incidents independently.

3.2.4 Data Protection Requirements

The transmission of ePHI or other data classified as Confidential over the network shall be conducted using company-approved, encrypted methods. Unencrypted transmission of sensitive data shall be prohibited.

3.3 Prohibited Activities

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

3.3.1 Prohibited Illegal Activities

Engaging in any activity that is illegal under local, state, or federal law shall be strictly prohibited, including but not limited to harassment, copyright infringement, or fraudulent activities.

3.3.2 Security Control Circumvention

Attempting to bypass or disable any security controls, such as firewalls, content filters, or monitoring software, shall be strictly prohibited.

3.3.3 Unauthorized System Access

Attempting to access systems, data, or accounts for which the user does not have explicit authorization shall be strictly prohibited.

3.3.4 Network Disruption Activities

Engaging in any activity that could disrupt network services or degrade performance for other users shall be strictly prohibited, such as initiating a denial-of-service attack or sending spam.

3.3.5 Unauthorized Data Transfer

Using unapproved peer-to-peer file-sharing services or transferring company data to unauthorized personal cloud storage accounts shall be strictly prohibited.

3.3.6 Inappropriate Content Access

Accessing, downloading, or distributing content that is obscene, defamatory, harassing, or otherwise violates **[Company Name]**'s professional conduct policies shall be strictly prohibited.

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. This policy focuses on network connectivity, workspace security, and data handling requirements. Device security requirements are comprehensively addressed in the Mobile Device Security Policy (OP-POL-002).

3.1 General Remote Work Security

Remote work arrangements shall be formally authorized and conducted in accordance with documented security procedures. Workforce members shall maintain the same level of information security when working remotely as when working in company facilities.

3.3 Network Security

Workforce members shall ensure secure network connectivity for all remote work activities.

3.3.1 VPN Requirements

All access to internal company systems, applications, and data repositories shall be established through the company-approved Virtual Private Network (VPN). The VPN client shall remain active for the entire duration of the remote work session.

3.3.2 Network Security Restrictions

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 shall be strictly prohibited. If such a network must be used for general tasks, the VPN shall be mandatory.

3.3.3 Home Network Security Standards

Workforce members shall 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 shall formally attest that their primary remote work network is secured in accordance with this policy.

3.2 Endpoint Device Security Requirements

All devices used to access company resources remotely shall comply with the comprehensive security requirements defined in the Mobile Device Security Policy (OP-POL-002). This includes but is not limited to encryption, access controls, malware protection, patch management, and mobile device management (MDM) enrollment requirements.

Workforce members shall ensure their devices meet all applicable security standards as specified in OP-POL-002 before accessing company systems remotely. Device compliance verification and ongoing monitoring shall be conducted according to the procedures established in the Mobile Device Security Policy.

3.3 Data Handling and Physical Security

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

3.3.1 Data Storage Restrictions

Storing ePHI or other Confidential data on the local hard drive of a personally-owned device shall be strictly prohibited. All sensitive data shall be accessed and stored exclusively on company-managed cloud platforms or network shares.

3.4 Data Handling and Storage

Workforce members shall take precautions to protect the confidentiality and integrity of company information when working remotely.

3.4.1 Data Storage Restrictions

Storing ePHI or other Confidential data on the local hard drive of any remote device shall be strictly prohibited. All sensitive data shall be accessed and stored exclusively on company-managed cloud platforms or network shares.

3.4.2 Physical Privacy Controls

Workforce members shall ensure their remote workspace provides adequate visual and auditory privacy to prevent unauthorized access to or disclosure of ePHI. This includes positioning screens away from public view and using privacy screens when working in shared environments.

3.5 Physical Security of Remote Workspace

The remote workspace shall be secured against unauthorized physical access to company equipment and information.

3.5.1 Workspace Security

Company equipment and sensitive information shall be secured when not in use. Workstations shall be locked when unattended, and devices shall be stored securely.

3.5.2 Visitor Access Controls

Workforce members shall ensure that visitors to their remote workspace do not have access to company equipment or confidential information unless authorized.

3.6 Incident Reporting

Any security incident, including but not limited to loss or theft of devices, suspected unauthorized access, or potential data breaches, shall be reported immediately to the Security Officer or IT Department according to the Incident Response Policy (RES-POL-001).

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 shall 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 shall 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	HITRUST CSF v11.2.0	11.g - Remote Access Control
3.3	HITRUST CSF v11.2.0	08.e - Network Security Controls
3.2	HITRUST CSF v11.2.0	02.f - Remote Endpoint Security (via OP-POL-002)
3.3	HITRUST CSF v11.2.0	09.f - Secure Remote Access
All	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(B) - Authorization and/or supervision

Policy Section	Standard/Frame	Control Reference
3.3	HIPAA Security Rule	45 CFR § 164.312(e)(1) - Transmission Security
3.2, 3.4	HIPAA Security Rule	45 CFR § 164.310(d)(1) - Device and Media Controls (via OP-POL-002)
All	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.2, 3.4	SOC 2 Trust Services Criteria	CC6.6 - The entity implements logical access security measures for assets…
3.5	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.
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.

Privileged Access Management (PAM) Policy (AC-POL-004)

1. Objective

The objective of this policy is to establish comprehensive controls for managing privileged accounts and administrative access within **[Company Name]**'s information systems and infrastructure. This policy ensures that accounts with elevated privileges are subject to enhanced security controls, monitoring, and governance to protect the confidentiality, integrity, and availability of critical systems and electronic Protected Health Information (ePHI). This policy implements just-in-time access principles, enhanced authentication requirements, and comprehensive monitoring to minimize the risk associated with privileged account compromise.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, and third parties who require elevated administrative privileges to perform their job functions. It encompasses all privileged accounts including system administrators, database administrators, cloud administrators, network administrators, security administrators, and service accounts with elevated privileges. This policy covers all systems and platforms including on-premises infrastructure, cloud services, applications, databases, network devices, and security tools. It applies to all environments (production, staging, development, testing) where privileged access is required.

3. Policy

Privileged accounts and administrative access shall be managed through rigorous controls that implement just-in-time access principles, enhanced authentication, comprehensive monitoring, and strict approval processes to minimize security risks.

3.1 Principles of Privileged Access Management

Privileged access management shall be based on fundamental security principles that minimize risk and ensure accountability.

3.1.1 Least Privilege and Separation of Duties

3.1.1.1 Minimal Privilege Assignment

Privileged accounts shall be granted only the minimum level of access necessary to perform specific administrative functions. Broad administrative privileges shall be avoided in favor of granular, function-specific permissions.

3.1.1.2 Role-Based Privilege Assignment

Privileged access shall be assigned based on clearly defined administrative roles with documented responsibilities and access requirements. Role definitions shall be regularly reviewed and updated to reflect current business needs.

3.1.1.3 Separation of Duties

Critical administrative functions shall be divided among multiple individuals to prevent single points of failure and reduce the risk of unauthorized actions. No single individual shall have complete administrative control over critical systems.

3.1.1.4 Temporary Privilege Elevation

Standard user accounts shall be used for routine activities, with privilege elevation requested only when administrative functions are required. Permanent assignment of elevated privileges shall be minimized.

3.1.2 Enhanced Authentication and Authorization

3.1.2.1 Multi-Factor Authentication Requirements

All privileged accounts shall require multi-factor authentication using approved authentication methods. Hardware tokens or biometric authentication may be required for critical infrastructure access.

3.1.2.2 Privileged Access Workstation Requirements

Dedicated secured workstations shall be used for privileged access to critical systems, isolated from general-purpose computing activities.

3.1.2.3 Network-Based Access Controls

Privileged access shall be restricted to authorized networks and locations, with additional controls for remote privileged access.

3.2 Just-in-Time (JIT) Access Implementation

Privileged access shall be granted on a time-limited, just-in-time basis to minimize exposure and reduce the attack surface of elevated privileges.

3.2.1 Time-Limited Access Sessions

3.2.1.1 Session Duration Limits

Critical Infrastructure Access (production databases, cloud administrative consoles) shall have a maximum session duration of **[Duration, e.g., 4 hours]** with automatic termination. **Standard Administrative Access** (system administration, application management) shall have a maximum session duration of **[Duration, e.g., 8 hours]** with renewal available. **Development and Testing Access** shall have a maximum session duration of **[Duration, e.g., 24 hours]** with self-service renewal.

3.2.1.2 Automatic Session Termination

Privileged access sessions shall automatically terminate upon expiration, with no automatic renewal. Users shall request new access through established approval processes.

3.2.1.3 Emergency Access Procedures

Break-glass access procedures shall be established for emergency situations, with enhanced monitoring and immediate notification requirements.

3.2.2 Dynamic Access Approval

3.2.2.1 Request-Based Access

Privileged access shall be requested through automated workflows with business justification and approval requirements. Standing privileged access shall be minimized.

3.2.2.2 Approval Workflows

Access requests shall require approval from appropriate managers and security personnel based on the risk level and scope of requested privileges.

3.2.2.3 Access Reviews

All active privileged access shall be reviewed at least quarterly to ensure continued business justification and appropriate usage. Privileged access review cadence is authoritative in this policy; standard (non-privileged) access review cadence is defined in AC-POL-001 (annual).

3.3 Privileged Account Provisioning and Management

Comprehensive processes shall govern the creation, modification, and termination of privileged accounts throughout their lifecycle.

3.3.1 Privileged Account Management Implementation

- **Privileged Account Provisioning and Approval:**
  - Privileged account requests shall be submitted through **[Access Management System]** with business justification, required access level, and duration specification
  - Hiring managers shall review and approve privileged account requests confirming business need and appropriate access level for role responsibilities
  - Information Security Officer shall conduct risk assessment for privileged account requests evaluating access scope, duration, and potential security impact
  - Privileged accounts shall be created with minimum necessary permissions and configured with multi-factor authentication requirements
  - All privileged accounts shall be enrolled in Privileged Access Management (PAM) system with session recording and access approval workflows
- **Privileged Account Security Controls:**
  - Account owners shall complete privileged account security training within **[Duration, e.g., 5 business days]** of account creation
  - PAM system shall require approval for each privileged session through **[Approval Process, e.g., manager approval, security team approval]**
  - All privileged account usage shall be monitored in real-time by the Security Operations Center with investigation of suspicious activities within **[Duration, e.g., 15 minutes]**

  - PAM system shall record all privileged sessions including keystrokes, commands, and file access for audit and investigation purposes
  - Emergency access accounts and break-glass procedures shall be implemented with enhanced monitoring and immediate notification requirements
- **Privileged Account Monitoring and Reporting:**
  - Quarterly privileged account usage reports and attestation reviews shall be generated and documented, including login times, commands executed, and systems accessed
  - Quarterly privileged account activity summaries shall be reviewed by the Information Security Officer to investigate any anomalous or unauthorized usage patterns
  - Monthly reviews of assigned privileged accounts shall be conducted by account managers to verify continued business need and appropriate access levels
  - Real-time monitoring shall include detection of privileged access anomalies, unusual command execution, and potential abuse patterns
  - Integration with SIEM systems shall provide comprehensive visibility into privileged account activities across all systems and platforms
- **Privileged Account Lifecycle Management:**
  - Quarterly comprehensive review of all privileged accounts shall be performed including access validation, usage analysis, and compliance assessment
  - Privileged account passwords shall be rotated quarterly using **[Password Management System]** with **[Complexity Requirements, e.g., 20+ characters]**
  - Annual privileged access risk assessment shall be conducted with updates to access controls based on threat landscape and business requirements
  - Privileged account deprovisioning shall include secure deletion of recorded sessions and access logs according to retention policies

3.4 Session Monitoring and Recording

Comprehensive monitoring and recording of privileged access sessions shall provide accountability and forensic capabilities.

3.4.1 Real-Time Session Monitoring

3.4.1.1 Continuous Monitoring

All privileged access sessions shall be monitored in real-time by security personnel or automated systems. Suspicious activities shall trigger immediate alerts and investigation.

3.4.1.2 Behavioral Analysis

User behavior analytics shall identify anomalous privileged access patterns, unusual command execution, or potential insider threats.

3.4.1.3 Geographic and Time-Based Monitoring

Privileged access from unusual locations or outside normal business hours shall trigger enhanced monitoring and approval requirements.

3.4.2 Session Recording and Audit

3.4.2.1 Comprehensive Session Recording

All privileged access sessions shall be recorded including keystrokes, commands, screen activity, and file access for audit and forensic purposes.

3.4.2.2 Audit Trail Maintenance

Complete audit trails shall be maintained for all privileged account activities with secure storage and tamper-evident controls.

3.4.2.3 Forensic Capabilities

Session recordings and audit logs shall provide sufficient detail for incident investigation and forensic analysis.

3.5 Separated Administrative Accounts

Administrative functions shall be performed using dedicated accounts separate from standard user accounts to limit exposure and improve security.

3.5.1 Account Separation Requirements

3.5.1.1 Dedicated Administrative Accounts

Workforce members with administrative privileges shall use separate, dedicated accounts for administrative functions. These accounts shall not be used for general productivity tasks.

3.5.1.2 Standard Account Usage

Routine business activities including email, web browsing, and document creation shall be performed using standard, non-privileged user accounts.

3.5.1.3 Account Naming Conventions

Administrative accounts shall follow standardized naming conventions to clearly identify their privileged nature and associated user.

3.5.2 Administrative Account Security

3.5.2.1 Enhanced Security Controls

Administrative accounts shall be subject to additional security controls including stronger authentication requirements, network access restrictions, and enhanced monitoring.

3.5.2.2 Limited Network Access

Administrative accounts shall only be permitted to access systems and networks necessary for their administrative functions.

3.5.2.3 Regular Security Assessments

Administrative accounts shall undergo regular security assessments to validate proper configuration and usage.

3.6 Emergency Access and Break-Glass Procedures

Emergency access procedures shall provide rapid access to critical systems during security incidents or business emergencies while maintaining security controls.

3.6.1 Emergency Access Procedures

3.6.1.1 Break-Glass Account Management

Emergency access accounts shall be maintained for critical systems with enhanced monitoring and immediate notification when accessed.

3.6.1.2 Emergency Approval Process

Emergency access shall require approval from designated emergency responders and security personnel, with justification documented.

3.6.1.3 Post-Emergency Review

All emergency access usage shall be reviewed within **[Duration, e.g., 24 hours]** to validate appropriateness and document lessons learned.

3.6.2 Emergency Access Monitoring

3.6.2.1 Immediate Notification

Emergency access activation shall trigger immediate notifications to security personnel, management, and relevant stakeholders.

3.6.2.2 Enhanced Logging

All emergency access activities shall be subject to enhanced logging and monitoring with detailed audit trails.

3.6.2.3 Incident Response Integration

Emergency access procedures shall be integrated with incident response processes to ensure coordinated response 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	HITRUST CSF v11.2.0	11.a - Access Control Policy
3.2, 3.3	HITRUST CSF v11.2.0	11.b - User Access Management
3.3.1	HITRUST CSF v11.2.0	11.a - User Access Provisioning
3.3.1	HITRUST CSF v11.2.0	11.b - Privileged Access Management

Policy Section	Standard/Framework	Control Reference
3.3.1	HITRUST CSF v11.2.0	11.c - User Access Review
3.3.1	HITRUST CSF v11.2.0	11.d - User Access Revocation
3.4	HITRUST CSF v11.2.0	12.a - Audit Logging and Monitoring
3.1, 3.5	HITRUST CSF v11.2.0	11.c - User Responsibilities
All	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Information Access Management
3.3.1	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Access Management
3.4	HIPAA Security Rule	45 CFR § 164.312(b) - Audit Controls
All	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.3.1	SOC 2 Trust Services Criteria	CC6.2 - Logical Access Controls
3.1, 3.4	SOC 2 Trust Services Criteria	CC6.3 - Multi-Factor Authentication
3.4	SOC 2 Trust Services Criteria	CC7.2 - System Monitoring

5. Definitions

- **Break-Glass Access:** Emergency access procedure that provides rapid access to critical systems during emergencies with enhanced monitoring and approval requirements.
- **Just-in-Time (JIT) Access:** Security approach that provides privileged access only when needed and for limited time periods to minimize exposure.
- **Privileged Access Management (PAM):** Comprehensive approach to controlling, monitoring, and managing privileged accounts and administrative access.
- **Privileged Access Workstation (PAW):** Dedicated, hardened workstation used exclusively for privileged administrative functions.
- **Privileged Account:** User account with elevated permissions beyond those of standard users,

typically used for administrative functions.

- **Session Recording:** Comprehensive recording of privileged access sessions including keystrokes, commands, and screen activity for audit purposes.

6. Responsibilities

Role	Responsibility
Security Officer	Develop privileged access policies, oversee PAM program implementation, approve high-risk privileged access requests, and conduct quarterly privileged access assessments.
Information Security Team	Monitor privileged access activities, investigate security alerts, maintain PAM systems, and provide security guidance for privileged access requirements.
System Administrators	Create and manage privileged accounts, configure PAM systems, generate usage reports, rotate passwords according to schedule, and ensure compliance with privileged access controls.
Managers	Approve privileged access requests for their team members, conduct quarterly reviews of assigned privileged accounts, verify continued business need for privileged access, and ensure team compliance with privileged access policies.
Human Resources	Immediately notify IT and Security teams of employee terminations and role changes affecting privileged access, maintain accurate role information for privileged access management.
Compliance Officer	Maintain audit logs and session recordings for regulatory compliance, document privileged access procedures for audit purposes, and ensure retention requirements are met.
Privileged Users	Use privileged accounts only for authorized administrative functions, complete required security training, report suspected privileged account compromise, and comply with session monitoring requirements.
All Workforce Members	Report suspicious privileged access activities, protect privileged account credentials, and support privileged access security initiatives.

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

See Annex: Control Mapping

6. Artifact(s)

A completed policy violation investigation report.

7. Definitions

See Annex: Glossary

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	HITRUST CSF v11.2.0	04.b - Mobile Device Management
1-5	HITRUST CSF v11.2.0	11.b - User Access Management
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.

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

See Annex: Control Mapping

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

See Annex: Glossary

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.

Role	Responsibility
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 Lifecycle (SDLC) Policy (ENG-POL-001)

1. Objective

The objective of this policy is to establish a comprehensive framework for integrating security controls throughout the Software Development Lifecycle (SDLC) at **[Company Name]**. This policy ensures that security considerations are systematically incorporated into every phase of software development, from initial requirements gathering through deployment and maintenance. By implementing a structured secure development lifecycle framework and comprehensive security training programs, **[Company Name]** ensures that all software applications and systems are designed, developed, and maintained with appropriate security safeguards to protect electronic Protected Health Information (ePHI) and maintain compliance with HIPAA, HITECH, and SOC 2 requirements.

2. Scope

This policy applies to all **[Company Name]** workforce members involved in software development activities, including developers, architects, testers, DevOps engineers, product managers, project managers, and security engineers. 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 methodologies (Agile, DevOps, Waterfall), deployment models (on-premises, cloud, hybrid), and development environments (development, testing, staging, production). It applies to both internally developed software and customizations of third-party applications, establishing the overarching framework that is implemented through the Secure Coding and Testing Policy (ENG-POL-005) and Third-Party Component Management Policy (ENG-POL-006).

3. Policy

[Company Name] shall implement a comprehensive secure development lifecycle framework that systematically integrates security controls into every phase of software development, supported by comprehensive security training programs to ensure all development team members possess the knowledge and skills necessary to build secure applications.

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 for all software development projects.
  - Threat modeling shall be conducted for all applications that process, store, or transmit sensitive data to identify potential security risks.
  - Security architecture reviews shall be performed for new applications and significant modifications to ensure secure design principles.
  - Privacy impact assessments shall be completed for applications handling ePHI or personal information to meet regulatory requirements.
  - Secure design principles shall be applied including defense in depth, least privilege, and fail-secure defaults to establish foundational security.
- **Development Phase:**
  - Secure coding standards shall be followed for all programming languages and frameworks used in software development.
  - Security-focused code reviews shall be conducted for all code changes to identify potential security vulnerabilities.
  - Static Application Security Testing (SAST) tools shall be integrated into the development process for automated vulnerability detection.
  - Dependency scanning shall be performed to identify vulnerable third-party components and libraries.
  - Security unit tests shall be developed and executed as part of the testing framework to validate security controls.
- **Testing Phase:**
  - Dynamic Application Security Testing (DAST) shall be performed on all applications before production deployment to identify runtime vulnerabilities.
  - Interactive Application Security Testing (IAST) shall be implemented where technically feasible to provide real-time security feedback.
  - Penetration testing shall be conducted for all applications handling ePHI or Confidential data to validate security controls.
  - Security test cases shall validate proper implementation of security controls and requirements.
  - Vulnerability assessments shall be performed on the complete application stack to identify

security weaknesses.

- **Deployment Phase:**
  - Security configuration reviews shall be conducted before production deployment to ensure secure system settings.
  - Infrastructure security scanning shall validate secure deployment configurations against established baselines.
  - Secrets management processes shall ensure secure handling of credentials and keys throughout deployment.
  - Production environment hardening shall be verified against security baselines before application release.
  - Security monitoring and logging shall be implemented for all production applications to enable threat detection.
- **Maintenance Phase:**
  - Regular security assessments shall be conducted on production applications to identify emerging vulnerabilities.
  - Security patches and updates shall be applied according to established timelines based on vulnerability severity.
  - Continuous monitoring shall detect and alert on security vulnerabilities and threats in production environments.
  - End-of-life procedures shall ensure secure decommissioning of applications and data when systems are retired.

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 shall be required before proceeding to development.
- **Code Gate:** Static analysis results and code review approval shall be required before proceeding to testing.
- **Test Gate:** Dynamic testing results and penetration test approval shall be required before proceeding to deployment.
- **Deploy Gate:** Security configuration review and vulnerability scan approval shall be required before production release.

- **Production Gate:** Security monitoring implementation and incident response procedures shall be verified before full production deployment.

3.2 Secure Coding and Testing Implementation

All secure coding practices, code review requirements, static analysis tools, and security testing methodologies shall be implemented as defined in the Secure Coding and Testing Policy (ENG-POL-005). This includes comprehensive secure coding standards for all programming languages and frameworks, mandatory code review processes, automated static and dynamic security testing, and regular penetration testing requirements.

3.3 Third-Party Component and DevOps Security Management

All third-party component management, DevOps security practices, CI/CD pipeline security, and supply chain risk management shall be implemented as defined in the Third-Party Component Management Policy (ENG-POL-006). This includes automated dependency scanning, vendor security assessments, secure CI/CD pipeline implementation, secrets management, and comprehensive supply chain security controls.

3.4 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 shall be completed within **[Timeframe, e.g., 30 days]** of hire.
  - Language and framework-specific security training shall be provided to ensure developers understand secure practices for their technology stack.
  - OWASP Top 10 awareness and prevention techniques shall be included in all developer security training programs.
  - Threat modeling and security design principles shall be taught to enable developers to identify and mitigate security risks.

  - Security tool usage and integration training shall be provided to ensure effective use of security testing tools.
- **Ongoing Training and Awareness:**
  - Annual security training updates covering emerging threats and vulnerabilities shall be provided to all development team members.
  - Specialized training for developers working on critical or high-risk applications shall be provided to address specific security requirements.
  - Security conference attendance and knowledge sharing shall be encouraged to maintain current security expertise.
  - Internal security awareness presentations and workshops shall be conducted to share security knowledge across teams.
  - Gamification and hands-on security challenges shall be implemented to engage developers in security learning.

3.7.2 Security Champions Program

- **Security Champion Selection:**
  - Designated security champions within each development team shall be identified and formally appointed.
  - Additional security training and certification for champions shall be provided to enhance their security expertise.
  - Regular security champion meetings and knowledge sharing shall be conducted to maintain security awareness across teams.
  - Champion responsibility for promoting security within their teams shall be clearly defined and communicated.
  - Recognition and incentives for effective security championship shall be provided to encourage participation and excellence.

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Security Officer	SDLC security policies shall be developed and maintained, security training programs shall be overseen, security gate reviews shall be coordinated, and compliance with security standards and regulations shall be ensured.
Development Team Lead	Team compliance with SDLC security requirements shall be ensured, security gate approvals shall be coordinated, team security training shall be managed, and security processes within development workflows shall be implemented.
Software Developers	SDLC security requirements shall be followed, participation in security gates and reviews shall be provided, required security training shall be completed, and security considerations shall be integrated into development activities.
Security Engineers	Security requirements and gates shall be defined, security architecture reviews shall be performed, threat modeling sessions shall be conducted, security guidance shall be provided, and security gate approvals shall be validated.
Product Managers	Security requirements for products shall be defined, threat modeling activities shall be coordinated, security features shall be prioritized, and security considerations shall be ensured in product planning and decisions.

Role	Responsibility
Architecture Team	Secure system architectures shall be designed, security design reviews shall be conducted, security patterns and standards shall be established, and architectural security guidance shall be provided to development teams.
Project Managers	Security gates shall be incorporated into project timelines, security activities shall be coordinated, security requirements completion shall be tracked, and security training for project teams shall be facilitated.
Quality Assurance Team	Security requirements implementation shall be validated, security test cases shall be executed, security testing activities shall be coordinated, and security gate completion criteria shall be verified.
All Workforce Members	Security training programs shall be participated in, established SDLC security procedures shall be followed, security concerns shall be reported, and security initiatives shall be supported within their respective roles.

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 shall 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 shall follow this standard process:

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

If the developer indicates the change touches sensitive data, authentication, authorization, encryption, ePHI, or external integrations, a security review shall be required and shall be completed by the Security Officer or designated security team member before merging. For low-risk changes (documentation, minor UI updates, configuration updates with no security implications), the security checklist shall be completed by the developer without additional review.

- **Testing:** All changes shall pass a full suite of automated tests. Evidence of successful test runs (e.g., a link to the CI/CD build results) shall be included in the pull request. Quality Assurance (QA) involvement shall be risk-based: **High-risk changes** (new features, database schema changes, authentication/authorization modifications, ePHI handling) shall require formal QA sign-off. **Medium-risk changes** (bug fixes, configuration updates, UI improvements) shall require QA review only if the change affects user-facing functionality. **Low-risk changes** (documentation, internal tooling, minor refactoring) shall not require QA sign-off but shall pass automated testing.
- **Deployment Approval:** Final approval to merge the change into the production release branch shall be granted by authorized personnel (e.g., Engineering Lead or Manager) within the GitHub pull request. This approval shall signify 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 shall 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 that requires immediate remediation.

- **Authorization:** An emergency change shall require documented approval from at least one Engineering Lead or the CTO. For security-related emergency changes, the Security Officer shall be notified immediately, but approval may proceed without waiting for Security Officer availability to prevent business disruption.
- **Expedited Review:** Peer code review shall remain mandatory but may be expedited. For critical outages, the review shall be performed during or immediately after deployment to restore service quickly. Security review requirements shall follow the same risk-based approach as

standard changes but with expedited timelines.

- **Post-Implementation Review:** All emergency changes shall be followed by a formal post-implementation review within **[Number, e.g., 5]** business days (extended from 3 days to allow for proper analysis). This review shall analyze the root cause, validate the emergency response, and identify opportunities for process improvement. The standard change documentation shall be completed retroactively within **[Number, e.g., 2]** business days.
- **Oversight:** A log of all emergency changes shall be maintained and reviewed on a quarterly basis by Engineering Management to identify trends and ensure the emergency process is not being misused 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, shall follow a streamlined but secure process appropriate for a growing organization.

- **Formal Request:** All data-only changes shall require a formal request ticket that includes the script to be run, the business justification, the expected impact, and a rollback plan. For routine operational changes (e.g., updating configuration values, correcting data entry errors), a simplified approval process may be used.
- **Risk-Based Approval: High-risk changes** affecting ePHI, financial data, or critical business operations shall require approval from both the data/system owner and the Security Officer. **Medium-risk changes** affecting operational data shall require approval from the data/system owner only. **Low-risk changes** (configuration updates, non-sensitive data corrections) shall require approval from the requesting team lead.
- **Execution:** Changes shall be executed using approved, peer-reviewed scripts by authorized personnel with privileged database access. For routine changes, a qualified Database Administrator or DevOps Engineer may execute the change. The execution output shall be captured and appended to the original request ticket. Direct production database access for developers shall be prohibited except for emergency troubleshooting under supervision.

3.4 Change Documentation and Tracking

- **System of Record:** GitHub pull requests shall serve as the auditable record for all code and configuration changes.

- **Traceability:** Every pull request shall be linked to its corresponding issue tracking ticket. The pull request description shall summarize the change, the testing performed, and the outcome of all required reviews. Approvals shall 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 shall be technically protected to prevent direct commits. All changes shall be enforced through the pull request workflow.
- **Pull Request Template:** All pull requests shall use a standardized template that includes sections for the change description, testing performed, security checklist, and links to related tickets. This template shall be enforced via GitHub repository settings.

3.5 Change Notifications

- **Internal Notification:** The engineering team shall 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 shall be 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 shall have GitHub branch protection rules configured. At a minimum, these rules shall be enabled to:

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

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Engineering Team	Changes shall be developed, tested, and documented in accordance with this policy. Peer code reviews shall be conducted.
Security Team	Changes shall be reviewed for security implications and approved or rejected based on risk assessment.
Quality Assurance (QA) Team	Changes shall be verified to meet functional requirements and not introduce defects. Formal testing sign-off shall be provided.
Engineering Management	Final approval for changes to be deployed to production shall be provided. Emergency changes shall be authorized.
System / Data Owners	Approval for changes affecting their specific systems or data domains shall be provided, particularly for Data-Only Changes.

Cloud and Core 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 computing infrastructure and core IT systems. This policy ensures that all infrastructure components including cloud services, servers, containers, databases, storage systems, and supporting computing platforms 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, system hardening, 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 computing infrastructure and cloud services. It encompasses all infrastructure components including cloud platforms (AWS, Azure, GCP), virtual machines, containers, serverless functions, databases, 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 cloud infrastructure and computing platform 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:**
  - Identity and access management (IAM) shall be implemented with role-based access control and principle of least privilege across all cloud infrastructure components.
  - Data protection shall be implemented through encryption at rest and in transit across all cloud services and infrastructure components.
  - Logging and monitoring integration shall be implemented across all infrastructure components to provide comprehensive security visibility and event correlation.
  - Incident response capabilities shall be implemented with automated response and recovery procedures for infrastructure security events.
  - Security baselines and configuration management shall be implemented for all cloud resources to ensure consistent security posture and compliance.
- **Cloud Service Security Requirements:**
  - Cloud services shall be used only when they have appropriate compliance certifications including SOC 2, HIPAA, or ISO 27001 validation.
  - Shared responsibility model understanding and implementation shall be documented and implemented for each cloud service utilized by the organization.
  - Data residency controls shall be implemented to ensure data remains within approved geographic regions as defined by organizational and regulatory requirements.
  - Service level agreements (SLAs) shall include security and availability requirements that meet or exceed organizational standards for business continuity and data protection.
  - Vendor risk assessments and ongoing security monitoring shall be conducted for all cloud providers to validate security controls and compliance posture.

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.
  - Unnecessary services, protocols, and software components shall be removed or disabled to reduce the system attack surface.
  - Security configuration management and drift detection shall be implemented to maintain consistent security posture across all infrastructure components.
  - 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) shall be deployed on all applicable systems to provide advanced threat detection and response capabilities.
- **System Hardening and Baselining Implementation:**
  - Infrastructure systems shall be deployed using approved hardened images that comply with industry standard security baselines.
  - Configuration management tools shall maintain system configurations in a consistent state and prevent unauthorized modifications.
  - Regular validation of security configurations shall be performed through automated scanning and manual review processes.
  - Non-compliance with hardening standards shall trigger automatic remediation or security incident escalation procedures.
  - Hardening standards shall be reviewed and updated annually or when significant security threats are identified.

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 shall be implemented to provide unified authentication across all infrastructure systems.
  - Multi-factor authentication (MFA) shall be required for all administrative access to production and critical infrastructure components.
  - Role-based access control (RBAC) shall be implemented with predefined roles and permissions that follow the principle of least privilege.
  - Privileged access management (PAM) shall be deployed for high-risk administrative functions requiring elevated access controls.
  - Just-in-time (JIT) access shall be implemented for temporary elevated privileges with automated time-based access expiration.
- **Service Account Management:**
  - Unique service accounts shall be created for each application and service with minimal

required permissions following the principle of least privilege.
  - Regular rotation of service account credentials and API keys shall be performed according to established security schedules.
  - Monitoring and alerting for service account usage and anomalies shall be implemented to detect unauthorized or suspicious activities.
  - Automated provisioning and deprovisioning of service accounts shall be integrated with change management processes.
  - Documentation and approval process for service account creation and modification shall be maintained for audit and compliance purposes.

3.2.2 Access Reviews and Monitoring

- **Regular Access Certification:**
  - Quarterly access reviews shall be conducted for all administrative and privileged accounts to validate continued business need and appropriateness.
  - Annual comprehensive review of all infrastructure access permissions shall be performed with documented approval from appropriate business owners.
  - Automated access recertification workflows with manager approval shall be implemented to streamline the review process.
  - Immediate access revocation shall be performed upon role changes or employment termination to prevent unauthorized access.
  - Exception handling process for emergency access requirements shall be documented and include appropriate approval and monitoring controls.
- **Access Monitoring and Auditing:**
  - Real-time monitoring of all administrative and privileged access activities shall be implemented to detect unauthorized or suspicious behavior.
  - Automated alerting for suspicious access patterns or policy violations shall be configured to enable rapid response to security incidents.
  - Comprehensive audit logging for all infrastructure access and changes shall be maintained with adequate retention periods for compliance and forensic analysis.
  - Regular analysis of access logs for security anomalies and compliance validation shall be performed by designated security personnel.
  - Integration with security information and event management (SIEM) systems shall be maintained to correlate access events with other security indicators.

3.3 Data Protection and Encryption

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

3.3.1 Encryption Implementation

- **Data at Rest Encryption:**
  - Full disk encryption shall be implemented for all virtual machines and storage systems using industry-standard encryption algorithms.
  - Database encryption using transparent data encryption (TDE) or column-level encryption shall be applied to protect sensitive data at rest.
  - File system encryption shall be implemented for network-attached storage (NAS) and object storage containing sensitive or regulated data.
  - Encryption of backup data and archive storage shall be mandatory to protect data during long-term retention periods.
  - Hardware security module (HSM) or cloud HSM integration for key management shall be implemented for cryptographic operations requiring high assurance.
- **Data in Transit Encryption:**
  - TLS 1.3 or equivalent encryption shall be implemented for all network communications and data transmissions.
  - VPN encryption shall be required for all remote access and site-to-site connections to protect data traversing untrusted networks.
  - End-to-end encryption shall be implemented for sensitive data transmissions requiring additional protection beyond transport-layer security.
  - Certificate management and validation for all encrypted communications shall be maintained with proper certificate lifecycle management.
  - Perfect forward secrecy (PFS) shall be implemented where technically feasible to prevent retrospective decryption of captured traffic.

3.3.2 Key Management and Protection

- **Centralized Key Management:**
  - Cloud-native key management services (AWS KMS, Azure Key Vault, Google Cloud KMS) shall be utilized for centralized cryptographic key management.
  - Customer-managed encryption keys (CMEK) shall be implemented for sensitive data and

ePHI to maintain organizational control over encryption operations.
  - Key rotation policies and automated rotation procedures shall be established and enforced according to industry best practices and regulatory requirements.
  - Key escrow and recovery procedures shall be documented and tested for business continuity and disaster recovery scenarios.
  - Hardware security module (HSM) usage shall be implemented for high-value keys requiring additional protection and tamper resistance.
- **Key Security Controls:**
  - Separation of key management from data management functions shall be maintained to prevent unauthorized access and reduce security risks.
  - Multi-person authorization shall be required for key generation and recovery operations involving critical or high-value encryption keys.
  - Audit logging for all key management activities shall be implemented with comprehensive tracking of key lifecycle events.
  - Geographic distribution of keys shall be implemented for disaster recovery and high availability requirements.
  - Secure key deletion and destruction procedures shall be followed to ensure complete removal of cryptographic materials when no longer needed.

3.4 Infrastructure as Code (IaC) and Configuration Management

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

3.4.1 Secure IaC Practices

- **IaC Security Requirements:**
  - All infrastructure code shall be stored in a version control system. All changes shall 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 shall be performed to identify misconfigurations and security vulnerabilities before deployment.
  - Automated compliance checking against security policies and standards shall be integrated into the infrastructure deployment pipeline.
  - Immutable infrastructure principles shall be implemented to prevent configuration drift

and unauthorized modifications to deployed systems.
  - Secrets management for infrastructure credentials and sensitive configuration shall be implemented using secure vaults and encryption mechanisms.
- **Configuration Management:**
  - Centralized configuration management with automated deployment pipelines shall be implemented to ensure consistent and secure system configurations.
  - Configuration drift detection and automated remediation shall be deployed to identify and correct unauthorized changes to system configurations.
  - Security baseline enforcement shall be maintained across all infrastructure components to ensure compliance with organizational security standards.
  - Change tracking and rollback capabilities for configuration modifications shall be implemented to enable rapid recovery from configuration errors.
  - Documentation and approval process for infrastructure changes shall be maintained to ensure proper change management and audit trails.

3.4.2 CI/CD Pipeline Security

- **Secure Deployment Pipelines:**
  - Security scanning integration into CI/CD pipelines for infrastructure code shall be implemented to identify vulnerabilities before deployment.
  - Automated security testing and validation shall be performed before deployment to ensure compliance with security policies and standards.
  - Staged deployment process with security validation at each stage shall be implemented to reduce deployment risks and enable thorough testing.
  - Rollback procedures for failed or insecure deployments shall be documented and tested to enable rapid recovery from deployment issues.
  - Deployment approval gates for production environment changes shall be implemented to ensure proper authorization and review of critical changes.
- **Pipeline Protection:**
  - Access controls and authentication for CI/CD systems and pipelines shall be implemented to prevent unauthorized access to deployment infrastructure.
  - Secure storage and management of deployment credentials and secrets shall be maintained using dedicated secret management systems.
  - Audit logging for all pipeline activities and deployments shall be implemented to provide comprehensive tracking of deployment events.

  - Code signing and integrity verification for deployment artifacts shall be performed to ensure authenticity and prevent tampering.
  - Isolation of deployment environments and access controls shall be maintained to prevent cross-environment contamination and unauthorized access.

3.5 Container and Serverless Security

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

3.5.1 Container Security

- **Container Image Security:**
  - Base image security scanning and vulnerability assessment shall be performed before deployment to identify and remediate security vulnerabilities.
  - Minimal base images with only necessary components and dependencies shall be used to reduce the attack surface and potential security risks.
  - Regular image updates and patch management processes shall be implemented to maintain current security posture and address emerging threats.
  - Image signing and verification for deployment integrity shall be implemented to ensure authenticity and prevent unauthorized modifications.
  - Private container registries with access controls and scanning capabilities shall be utilized to maintain control over container image distribution and security.
- **Container Runtime Security:**
  - Container orchestration platform security (Kubernetes, ECS, AKS) shall be implemented with appropriate security configurations and access controls.
  - Runtime security monitoring and anomaly detection shall be deployed to identify suspicious container behavior and potential security threats.
  - Resource limits and isolation between containers shall be enforced to prevent resource exhaustion and lateral movement attacks.
  - Network policies and micro-segmentation for container communications shall be implemented to restrict inter-container communication based on business requirements.
  - Secrets management for container applications and services shall be implemented using secure secret stores and injection mechanisms.

3.5.2 Serverless Security

- **Function Security Controls:**
  - Code security scanning for serverless function code shall be performed to identify vulnerabilities and security issues before deployment.
  - Principle of least privilege for function execution roles and permissions shall be implemented to minimize potential security impact.
  - Environment variable security and secrets management shall be implemented to protect sensitive configuration data and credentials.
  - Function timeout and resource limits configuration shall be implemented to prevent denial of service and resource exhaustion attacks.
  - Monitoring and logging for function execution and security events shall be implemented to provide visibility into serverless operations and security incidents.
- **Serverless Architecture Security:**
  - API Gateway security controls and rate limiting shall be implemented to protect serverless functions from abuse and denial of service attacks.
  - Event source security and validation for function triggers shall be implemented to ensure only authorized events can invoke serverless functions.
  - Data encryption for serverless function storage and communications shall be implemented to protect data confidentiality and integrity.
  - Dependency management and vulnerability scanning for function dependencies shall be performed to identify and remediate security vulnerabilities.
  - Cold start security considerations and optimization shall be addressed to minimize security risks during function initialization.

3.6 Backup and Disaster Recovery

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

3.6.1 Backup Security

- **Backup Strategy Implementation:**
  - Regular automated backups shall be performed for all critical systems and data according to established schedules and retention requirements.
  - Geographic distribution of backups shall be implemented for disaster recovery to ensure

availability in case of localized disasters.
  - Encryption of all backup data at rest and in transit shall be mandatory to protect data confidentiality during backup operations.
  - Access controls and monitoring for backup systems and data shall be implemented to prevent unauthorized access to backup infrastructure.
  - 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 shall be implemented and enforced for all backup systems.
  - Secure disposal of expired backup media and data shall be performed according to data destruction standards and regulatory requirements.
  - Version management and point-in-time recovery capabilities shall be maintained to enable recovery to specific points in time as needed.
  - Backup monitoring and alerting for failed or incomplete backups shall be implemented to ensure backup reliability and effectiveness.
  - Documentation of backup and recovery procedures shall be maintained and regularly updated to ensure accuracy and completeness.

3.6.2 Disaster Recovery Planning

- **Recovery Infrastructure:**
  - Geographically separated disaster recovery infrastructure shall be maintained to ensure availability in case of regional disasters or outages.
  - Automated failover capabilities for critical systems and services shall be implemented to minimize downtime and service disruption.
  - Recovery time objectives (RTO) and recovery point objectives (RPO) shall be defined and validated through regular testing to ensure business requirements are met.
  - Disaster recovery testing and validation exercises shall be conducted at least annually.
  - Documentation and maintenance of disaster recovery procedures shall be performed to ensure procedures remain current and effective.
- **Business Continuity Integration:**
  - Coordination with business continuity planning and requirements shall be maintained to ensure alignment between technical recovery capabilities and business needs.
  - Communication procedures for disaster recovery activation shall be documented and

tested to ensure effective coordination during emergencies.
  - Stakeholder notification and coordination during recovery operations shall be managed through established communication channels and escalation procedures.
  - Post-incident review and improvement of recovery procedures shall be conducted after each activation to identify lessons learned and improvement opportunities.
  - Training and awareness for disaster recovery procedures shall be provided to relevant personnel to ensure readiness and capability.

3.7 Monitoring and Incident Response

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

3.7.1 Security Monitoring

- **Infrastructure Monitoring:**
  - 24/7 monitoring of all infrastructure components and services shall be implemented to provide continuous visibility into system health and security status.
  - Security information and event management (SIEM) integration shall be maintained to correlate security events across multiple systems and platforms.
  - Automated threat detection and alerting capabilities shall be deployed to enable rapid identification and response to security threats.
  - Performance monitoring and capacity management shall be implemented to ensure optimal system performance and availability.
  - Compliance monitoring and reporting for regulatory requirements shall be automated where possible to ensure continuous compliance verification.
- **Log Management and Analysis:**
  - Centralized log collection and analysis shall be implemented for all infrastructure components to provide comprehensive visibility into system activities.
  - Log retention policies aligned with regulatory and business requirements shall be established and enforced to ensure adequate log availability.
  - Real-time log analysis and correlation for security event detection shall be performed to identify potential security incidents and policy violations.
  - Secure log storage and access controls for log data shall be implemented to protect log integrity and ensure only authorized personnel can access log information.

  - Log integrity protection and tampering detection shall be implemented to identify unauthorized modifications to log data.

3.7.2 Infrastructure Incident Response

- **Infrastructure Incident Response:**
  - Automated incident response capabilities for infrastructure security events shall be implemented to enable rapid response to identified threats.
  - Integration with organizational incident response procedures shall be maintained to ensure coordinated response across all organizational functions.
  - Evidence preservation and forensics capabilities for infrastructure incidents shall be implemented to support investigation and legal requirements.
  - Communication procedures for infrastructure-related security incidents shall be documented and followed to ensure appropriate notification and coordination.
  - Recovery and restoration procedures for compromised infrastructure shall be documented and tested to enable rapid restoration of normal operations.

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Infrastructure Security Team	Develop cloud infrastructure security policies, implement security controls, monitor infrastructure security, and respond to infrastructure security incidents.

Role	Responsibility
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.
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.
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.
Container Platform Team	Manage container orchestration platform security, implement container security controls, and monitor container environments.
Cloud Security Architects	Design secure cloud architecture, establish security standards, and provide security guidance for cloud implementations.
All Engineering Staff	Follow infrastructure security policies, implement security controls in their areas, report security issues, and participate in security training.

Network Security Policy (ENG-POL-004)

1. Objective

The objective of this policy is to establish comprehensive security requirements for the design, implementation, operation, and monitoring of **[Company Name]**'s network infrastructure and communications. This policy ensures that all network components including perimeter security, internal network segmentation, wireless networks, and network traffic monitoring are configured and managed with appropriate security controls to protect the confidentiality, integrity, and availability of data in transit and electronic Protected Health Information (ePHI). This policy addresses network-level security controls, traffic monitoring, intrusion detection and prevention, and network access management 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 network infrastructure and communications. It encompasses all network components including routers, switches, firewalls, wireless access points, network security appliances, VPN concentrators, and network monitoring systems. This policy covers all network environments (production, staging, development, testing) and connection types including wired networks, wireless networks, remote access connections, site-to-site connections, and cloud network services. It applies to both on-premises network infrastructure and cloud-based networking services including Virtual Private Clouds (VPCs), software-defined networks, and hybrid network configurations.

3. Policy

- **[Company Name]** shall implement comprehensive network security controls across all network infrastructure to ensure secure data transmission, prevent unauthorized network access, and maintain regulatory compliance through defense-in-depth network protection strategies.

3.1 Network Security Architecture

A comprehensive network security architecture shall be implemented to provide layered protection against network-based threats and unauthorized access.

3.1.1 Network Segmentation and Micro-Segmentation

- **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
- **Production Network Isolation:**
  - Dedicated VLANs or VPCs for production, staging, development, and management networks
  - Inter-VLAN routing restrictions with explicit allow rules only
  - Production database isolation with application-layer access controls
  - DMZ implementation for external-facing services with restricted internal access
  - Network address translation (NAT) and firewall controls for internet access
- **Micro-Segmentation Strategy:**
  - Application-tier segmentation isolating web, application, and database layers
  - East-west traffic inspection and filtering between network segments
  - Zero-trust network access implementation for privileged users
  - Software-defined perimeter (SDP) implementation where technically feasible
  - Container network policies for microservices isolation
- **Segregation Monitoring and Enforcement:**
  - Continuous monitoring of network traffic between segments
  - Automated violation detection and remediation for unauthorized cross-segment communication
  - Regular testing of segregation effectiveness through penetration testing
  - Documentation and approval required for all cross-segment communication
  - Quarterly review of network segregation policies and implementation
- **Security Zone Access Controls:**
  - **Internet Zone**: External internet access with full inspection and filtering
  - **DMZ Zone**: External-facing services with restricted internal network access
  - **Internal Zone**: Corporate network with standard access controls and monitoring
  - **Restricted Zone**: High-security network segments with enhanced access controls
  - **Management Zone**: Administrative network with privileged access and monitoring

3.1.2 Traffic Control and Network Filtering

- **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

3.2 Network Security Monitoring and Detection

Comprehensive network security monitoring shall provide real-time threat detection and rapid response capabilities across all network infrastructure.

3.2.1 Network Security Monitoring Implementation

- **Cloud-Native Security Monitoring:**
  - Cloud-native security monitoring services (AWS GuardDuty, Azure Sentinel, GCP Security Command Center) shall be configured to automatically monitor VPC flow logs, DNS logs, and network traffic for suspicious activities
  - Managed Security Service Provider (MSSP) shall provide 24/7 network security monitoring, threat analysis, and incident response capabilities with HIPAA/HITECH compliance and HITRUST CSF certification
  - Cloud security monitoring tools shall be integrated with MSSP SIEM platforms with automated log forwarding and proper data retention
- **Network Traffic Analysis:**
  - Automatic baseline learning for normal network traffic patterns using cloud-native machine learning capabilities with automated alerting for significant deviations
  - Threat intelligence integration with commercial and government feeds for enhanced detection capabilities
  - Weekly security reviews and monthly executive summary reports including threat trends, incident summaries, and service performance metrics
- **Network Security Monitoring Operations:**
  - 24/7 network traffic monitoring and analysis
  - 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

3.2.2 Network Incident Response

- **Automated Network 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

3.3 Intrusion Detection and Prevention Systems

Comprehensive intrusion detection and prevention capabilities shall protect against network-based attacks and unauthorized access attempts.

3.3.1 Intrusion Detection and Prevention Implementation

- **Cloud-Native IDS/IPS Services:**
  - Cloud-native intrusion detection services shall be enabled with default threat detection rule sets and automatic threat intelligence updates
  - Network security groups and access control lists (NACLs) shall be configured to provide network-level intrusion prevention with default-deny policies
  - Web Application Firewall (WAF) services shall be deployed on internet-facing applications to detect and block common web attacks including SQL injection, XSS, and DDoS attempts
- **Automated Threat Response:**
  - Automated threat response capabilities shall include automatic IP blocking, traffic inspection escalation, and alert generation for security team review
  - DNS-based threat protection services shall block access to known malicious domains and command & control servers automatically
  - VPC Flow Logs and virtual network monitoring shall capture network traffic metadata for analysis with automated detection of suspicious patterns and geographic anomalies
- **IDS/IPS Management:**
  - Intrusion detection and prevention systems (IDS/IPS) with signature and anomaly-based detection

  - Regular updates of IDS/IPS signatures and threat detection rules
  - Tuning and optimization of IDS/IPS systems to minimize false positives
  - Integration with network security monitoring and incident response systems

3.4 Firewall Management and Administration

Comprehensive firewall management shall provide perimeter protection and network access control across all network boundaries.

3.4.1 Firewall Management Implementation

- **Firewall Architecture:**
  - Firewall deployment architecture shall provide defense-in-depth protection including perimeter firewalls, internal segmentation firewalls, web application firewalls, and cloud security groups
  - Network security zones shall be defined and implemented including Internet, DMZ, Internal, Management, and High-Security zones with zone-based access controls
- **Firewall Rule Management:**
  - Firewall rule development shall require business justification, security risk assessment, specific rule parameters, and documented purpose with expiration dates
  - Change management workflows shall require Security Officer approval for high-risk firewall rules with additional approvals for critical external access
  - Firewall logs shall be monitored continuously for security events including blocked connections, policy violations, and administrative access attempts
  - Quarterly firewall rule reviews shall identify unused or expired rules, overly permissive access, and opportunities for optimization and consolidation

3.5 Wireless Network Security

Comprehensive wireless network security controls shall ensure secure wireless communications while protecting against unauthorized wireless access and threats.

3.5.1 Wireless Network Security Implementation

- **Corporate Wireless Network Security:**

  - WPA3-Enterprise authentication with 802.1X authentication for all corporate wireless networks
  - Certificate-based authentication for corporate devices accessing wireless networks
  - Network Access Control (NAC) integration for device compliance verification
  - Corporate wireless network segregation from guest and public networks
  - Wireless network monitoring and intrusion detection capabilities

3.5.2 Wireless Security Monitoring Implementation

- **Wireless Intrusion Detection and Prevention:**
  - Wireless intrusion detection system (WIDS) sensors shall be deployed throughout all facilities with **[Coverage Percentage, e.g., 95%]** coverage
  - WIDS shall monitor all wireless frequencies including 2.4GHz, 5GHz, and **[Additional Frequencies, e.g., 6GHz]** for comprehensive threat detection
  - Baseline inventory of authorized wireless access points shall be established including MAC addresses, locations, SSIDs, and security configurations
  - Automated alerts shall be configured for detection of unauthorized access points, evil twin attacks, wireless deauthentication attacks, and rogue devices
  - Security Operations Center shall monitor wireless security dashboard continuously with investigation of alerts within **[Duration, e.g., 15 minutes]** of detection
- **Wireless Security Assessment and Validation:**
  - Daily wireless site surveys shall be performed to identify unauthorized access points, signal interference, and coverage gaps
  - Weekly vulnerability scans of all authorized wireless access points shall be conducted using **[Scanning Tools, e.g., Nessus, OpenVAS]**
  - Daily review of wireless access logs shall identify suspicious connection patterns, failed authentication attempts, and data exfiltration indicators
  - Monthly wireless penetration testing shall validate security controls and identify configuration weaknesses
  - Quarterly review of wireless security architecture shall update detection rules based on emerging threat intelligence
- **Wireless Incident Response and Remediation:**
  - Confirmed rogue access points shall trigger immediate containment by blocking the device and investigating potential data compromise
  - Incident Response Team shall coordinate wireless security incident response with appro-

priate escalation and notification procedures
  - Wireless monitoring logs and incident documentation shall be maintained for minimum **[Retention Period, e.g., 3 years]** for audit compliance
  - Monthly wireless device inventory updates shall remove decommissioned devices from monitoring systems and security baselines
  - Weekly wireless security reports shall include threat detection statistics, vulnerability findings, and remediation status
- **Wireless Security Performance Metrics:**
  - Monthly wireless security metrics shall include mean time to detection (MTTD) and mean time to response (MTTR) for threats
  - Quarterly wireless security assessments shall be reviewed by the Information Security Officer with approval for monitoring procedure changes
  - Wireless security monitoring effectiveness shall be measured through penetration testing results and threat detection capabilities
  - Continuous improvement of wireless security controls based on threat intelligence and industry best practices

3.6 Guest Network Security

Guest network infrastructure shall provide secure visitor access while maintaining complete isolation from corporate networks and sensitive data.

3.6.1 Guest Network Isolation and Security Implementation

- **Guest Network Infrastructure Requirements:**
  - Dedicated guest network infrastructure with complete Layer 2 and Layer 3 isolation from corporate networks containing ePHI and sensitive business data
  - Guest network VLAN configuration with no routing to corporate VLANs and dedicated internet gateway with NAT
  - Separate physical or logical infrastructure components to prevent any potential cross-contamination with corporate resources
  - Guest network equipment shall be managed and monitored independently from corporate network infrastructure
  - Geographic and logical separation of guest network components from production systems
- **Guest Network Access Controls:**

  - Guest network access controls requiring **[Authentication Method, e.g., sponsored access, SMS verification]** for connection approval
  - Time-limited guest credentials valid for **[Duration, e.g., 8 hours]** with automatic expiration and termination
  - Visitor information collection and identity verification by reception or security staff prior to access provisioning
  - Guest access request approval through **[Guest Management System]** with business justification and access duration specification
  - Automated provisioning of guest credentials with specified time limits, bandwidth restrictions, and content filtering policies
- **Guest Network Traffic Management:**
  - Content filtering configuration blocking access to malicious websites, social media, streaming services, and inappropriate content
  - Bandwidth limiting for guest users with maximum **[Bandwidth Limit, e.g., 10 Mbps per device]** and total **[Total Bandwidth, e.g., 100 Mbps]**
  - Quality of service (QoS) policies to prevent guest traffic from impacting corporate network performance
  - Traffic shaping and rate limiting to ensure fair usage and prevent network abuse
  - Deep packet inspection (DPI) capabilities for enhanced security monitoring and threat detection
- **Guest Network Monitoring and Logging:**
  - Continuous monitoring of guest network traffic for malicious activity, data exfiltration attempts, and policy violations by the Security Operations Center
  - Comprehensive logging of all guest network connections including device MAC addresses, connection times, data usage, and visited websites
  - Daily review of guest network logs by network administrators to identify security events, policy violations, and system performance issues
  - Real-time alerting and automated response capabilities for suspicious guest network activities
  - Integration with SIEM systems for correlation with other security events and threat intelligence
- **Guest Network Security Validation:**
  - Investigation and response to guest network security alerts within **[Duration, e.g., 30 minutes]** including device isolation if necessary

  - Automatic termination of guest access upon credential expiration and removal of device associations from access control systems
  - Weekly guest network penetration testing to verify isolation effectiveness and identify potential security gaps
  - Monthly guest network security reports including usage statistics, security events, and compliance metrics reviewed by the Information Security Officer
  - Quarterly guest network security assessment and update of isolation controls based on risk assessment findings by the Network Security Manager
- **Guest Network Compliance and Retention:**
  - Maintenance of guest network access logs for minimum **[Retention Period, e.g., 1 year]** for security incident investigation and compliance requirements
  - Documentation of guest network policies, procedures, and security controls for audit and compliance purposes
  - Regular compliance assessments to ensure guest network implementation meets regulatory requirements
  - Incident response procedures specific to guest network security events and policy violations
  - Integration with organizational privacy and data protection requirements for guest network usage data

3.7 Network Access Control and Remote Access

Comprehensive network access controls shall ensure authorized access to network resources while preventing unauthorized access and maintaining security monitoring.

3.7.1 Network Access Control Implementation

- **Network Access Control (NAC) Systems:**
  - Automated device discovery and classification for all devices connecting to corporate networks
  - Device compliance verification including security patch status, antivirus updates, and configuration compliance
  - Dynamic VLAN assignment based on device type, user role, and compliance status
  - Quarantine network for non-compliant devices with limited access and remediation capabilities

  - Integration with identity management systems for user-based access policies

3.7.2 Remote Access Security

- **VPN and Remote Access Controls:**
  - Multi-factor authentication required for all remote access connections
  - End-to-end encryption for all remote access sessions using approved protocols
  - Remote access session monitoring and logging for security analysis
  - Time-limited remote access sessions with automatic disconnection
  - Device compliance verification for remote access endpoints

3.8 Network Performance and Capacity Management

Network performance monitoring shall ensure adequate capacity and optimal performance while maintaining security monitoring capabilities.

3.8.1 Network Performance Monitoring

- **Performance Monitoring Implementation:**
  - Real-time network performance monitoring including bandwidth utilization, latency, and packet loss
  - Capacity planning and forecasting based on historical usage patterns and business growth
  - Quality of Service (QoS) implementation to prioritize critical business traffic
  - Network optimization and traffic engineering to ensure optimal performance
  - Performance alerting and notification for capacity or performance issues

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Network Security Manager	Develop network security policies, oversee network security architecture, manage network security controls, and coordinate network security incident response.
Network Engineers	Design and maintain secure network architecture, implement network security controls, configure network devices, and monitor network security events.
Security Operations Center (SOC)	Monitor network security events 24/7, analyze network security alerts, coordinate network incident response, and provide network security monitoring.
Information Security Officer	Oversee network security program, approve network security policies, review network security assessments, and ensure regulatory compliance.
Managed Security Service Provider (MSSP)	Provide 24/7 network security monitoring, threat analysis, incident response capabilities, and network security expertise.
System Administrators	Configure network security settings on systems, implement network access controls, and maintain network security compliance.
Wireless Network Administrator	Manage wireless network infrastructure, implement wireless security controls, monitor wireless networks, and respond to wireless security incidents.
Firewall Administrators	Configure and maintain firewall rules, monitor firewall logs, implement firewall changes, and ensure firewall compliance.

Role	Responsibility
Cloud Engineers	Implement cloud network security controls, configure VPC security, manage cloud network services, and ensure cloud network compliance.
All Engineering Staff	Follow network security policies, implement network security controls in their areas, report network security issues, and participate in network security training.

Secure Coding and Testing Policy (ENG-POL-005)

1. Objective

The objective of this policy is to establish comprehensive secure coding standards and testing requirements for all software development activities at **[Company Name]**. This policy ensures that security controls are integrated into coding practices and testing processes to prevent vulnerabilities, protect electronic Protected Health Information (ePHI), and maintain compliance with HIPAA, HITECH, and SOC 2 requirements. By implementing standardized secure coding practices and rigorous security testing, **[Company Name]** minimizes security risks and ensures applications are resilient against common attack vectors.

2. Scope

This policy applies to all **[Company Name]** workforce members involved in software development and testing activities, including developers, architects, testers, security engineers, and quality assurance team members. 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 secure coding practices for all programming languages and frameworks used by **[Company Name]**, as well as all security testing methodologies including static analysis, dynamic testing, and penetration testing across all development environments.

3. Policy

[Company Name] shall implement comprehensive secure coding standards and rigorous security testing processes to ensure that all applications and systems are developed with appropriate security safeguards and thoroughly validated against security vulnerabilities.

3.1 Secure Coding Standards

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

3.1.1 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

3.1.2 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

3.2 Code Review and Static Analysis

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

3.2.1 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 shall 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

3.2.2 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 shall 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 shall require a formal risk acceptance document to be signed by the Information Owner and the Security Officer.
    * Vulnerability remediation shall be verified through re-testing.

3.3 Dynamic Testing and Security Assessment

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

3.3.1 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

3.3.2 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.

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Security Officer	Develop secure coding policies, coordinate security testing programs, provide security guidance, and ensure compliance with security standards and regulations.
Development Team Lead	Ensure team compliance with secure coding practices, coordinate security reviews, manage security training for developers, and implement security tools and processes within the team.
Software Developers	Follow secure coding standards, participate in code reviews, use security testing tools, remediate identified vulnerabilities, and complete required security training.
Security Engineers	Perform security assessments, conduct penetration testing, review security architecture, provide security guidance to development teams, and maintain security testing tools.
Quality Assurance Team	Execute security test cases, validate security controls, coordinate dynamic testing activities, verify vulnerability remediation, and ensure security requirements are met.
DevOps Engineers	Integrate security testing tools into CI/CD pipelines, manage security scanning automation, maintain security tool configurations, and ensure continuous security validation.
Architecture Team	Define secure coding patterns and standards, conduct security design reviews, establish security guidelines for development teams, and provide architectural security guidance.
All Workforce Members	Report security vulnerabilities and concerns, follow established security procedures, complete required training, and support security initiatives within their respective roles.

Third-Party Component Management Policy (ENG-POL-006)

1. Objective

The objective of this policy is to establish comprehensive requirements for the secure management of third-party libraries, frameworks, components, and DevOps tools throughout the software development lifecycle at **[Company Name]**. This policy ensures that third-party dependencies are properly assessed, monitored, and maintained to minimize security risks, protect electronic Protected Health Information (ePHI), and maintain compliance with HIPAA, HITECH, and SOC 2 requirements. By implementing rigorous third-party component governance and DevOps security practices, **[Company Name]** reduces supply chain risks and ensures the integrity of its development and deployment processes.

2. Scope

This policy applies to all **[Company Name]** workforce members involved in software development, infrastructure management, and DevOps activities, including developers, architects, DevOps engineers, security engineers, and system administrators. It encompasses all third-party components including open source libraries, commercial software components, frameworks, APIs, infrastructure-as-code templates, CI/CD tools, and development dependencies. This policy covers the entire lifecycle of third-party component management from selection and assessment through deployment, monitoring, and retirement across all development environments and production systems.

3. Policy

[Company Name] shall implement comprehensive governance and security controls for all third-party components used in software development and deployment processes to ensure supply chain security, minimize vulnerabilities, and maintain the integrity of systems and data.

3.1 Third-Party Component Management

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

3.1.1 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

3.1.2 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

3.1.3 Component Lifecycle Management

- **Component Selection Criteria:**
  - Security track record and vulnerability history assessment
  - Community or vendor support quality and responsiveness evaluation
  - License compatibility and legal compliance verification
  - Technical compatibility and performance impact analysis
  - Maintenance status and long-term viability assessment

- **Approval and Documentation:**
  - Formal approval process for new third-party components
  - Security assessment documentation for approved components
  - Dependency mapping and architecture impact analysis
  - Risk assessment and mitigation strategies documentation
  - Business justification and alternative analysis
- **Monitoring and Maintenance:**
  - Continuous monitoring of component security status and vulnerabilities
  - Regular updates and patches applied according to risk prioritization
  - End-of-life tracking and replacement planning for obsolete components
  - Performance monitoring and impact assessment for component updates
  - Documentation maintenance for component inventory and dependencies

3.2 DevOps and CI/CD Security

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

3.2.1 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

3.2.2 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

3.2.3 Build and Deployment Security

- **Secure Build Practices:**
  - Containerized and isolated build environments
  - Cryptographic signing of build artifacts and container images
  - Scan artifacts for vulnerabilities before deployment
  - Immutable artifact storage and retention policies
  - Provenance tracking for all build components and dependencies
- **Deployment Controls:**
  - Automated security scanning before production deployment
  - Configuration validation against security baselines
  - Rollback procedures for security incidents
  - Blue-green or canary deployment strategies for risk mitigation
  - Post-deployment security verification and monitoring

3.3 Supply Chain Risk Management

Comprehensive assessment and mitigation of supply chain risks associated with third-party components and vendors.

3.3.1 Vendor Risk Assessment

- **Security Due Diligence:**
  - Vendor security questionnaires and assessment programs

  - Third-party security certifications and compliance verification
  - Vendor incident response capabilities and procedures evaluation
  - Data handling and privacy practices assessment
  - Business continuity and disaster recovery planning verification
- **Contractual Security Requirements:**
  - Security requirements included in vendor contracts and agreements
  - Right to audit and security assessment clauses
  - Incident notification and response requirements
  - Data protection and confidentiality obligations
  - Compliance with regulatory requirements (HIPAA, SOC 2)

3.3.2 Software Supply Chain Security

- **Component Verification:**
  - Digital signature verification for commercial software components
  - Checksum validation for downloaded open source components
  - Source code review for critical or high-risk components
  - Build-from-source procedures for security-critical dependencies
  - Supply chain attack detection and prevention measures
- **Software Bill of Materials (SBOM):**
  - Generation and maintenance of SBOM for all applications
  - Component tracking including version, license, and vulnerability status
  - SBOM sharing with security teams and stakeholders
  - Integration with vulnerability management and incident response processes
  - Compliance with emerging SBOM regulations and standards

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Security Officer	Develop third-party component policies, oversee supply chain risk management, coordinate vendor security assessments, and ensure compliance with security standards.
Development Team Lead	Ensure team compliance with component management practices, coordinate security reviews of dependencies, and maintain approved component lists for their teams.
Software Developers	Follow component selection guidelines, use approved third-party libraries, report security vulnerabilities in dependencies, and participate in component security reviews.
DevOps Engineers	Implement secure CI/CD pipelines, manage secrets and credentials, maintain security tools integration, configure build security controls, and ensure infrastructure security.
Security Engineers	Perform security assessments of third-party components, maintain vulnerability databases, conduct supply chain risk assessments, and provide security guidance for component selection.
Architecture Team	Define component selection criteria, establish security standards for third-party integration, review high-risk component decisions, and provide architectural guidance for dependencies.
Legal/Compli Team	Review license compliance, assess contractual security requirements with vendors, ensure regulatory compliance, and manage legal aspects of third-party relationships.
Procurement Team	Include security requirements in vendor selection, coordinate vendor security assessments, maintain vendor risk registers, and ensure contractual security obligations.
All Workforce Members	Report security vulnerabilities and concerns related to third-party components, follow established procedures, complete required training, and support security initiatives.

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

See Annex: Control Mapping

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

See Annex: Glossary

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 shall create a remediation plan (e.g., wait for a patched version) or formally document a risk acceptance rationale.

Step	Who	What
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

See Annex: Control Mapping

7. Definitions

See Annex: Glossary

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

See Annex: Control Mapping

7. Definitions

See Annex: Glossary

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.
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.

Step	Who	What
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

See Annex: Control Mapping

7. Definitions

See Annex: Glossary

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.

Automated Privileged Access Management Procedure (ENG-PROC-006)

1. Purpose

The purpose of this procedure is to implement automated privileged access management using role-based access control (RBAC) and just-in-time (JIT) access, replacing manual quarterly reviews with continuous monitoring and exception-based access validation.

2. Scope

This procedure applies to all privileged access to production infrastructure, cloud services, and critical systems through automated identity and access management systems integrated with HR data and organizational roles.

3. Overview

This procedure leverages automated RBAC systems, just-in-time access controls, and exception-based monitoring to ensure privileged access is appropriately managed without manual quarterly disruptions. The approach emphasizes automation, self-service access requests, and anomaly detection over manual attestation processes.

4. Procedure

Step	Who	What
1	IT Operations Team	Configure identity management system to automatically synchronize employee data including role, department, manager, and employment status from HR systems. Enable real-time updates for role changes and terminations.

Step	Who	What
2	Security Officer	Define standard privileged access roles based on job functions and map each role to specific cloud resources and permission sets using infrastructure as code.
3	Platform Engineer	Configure automated role assignment based on HR data and job function. Implement rules that automatically grant appropriate privileged access when employees are hired or change roles.
4	IT Operations Team	Implement group-based access control where privileged permissions are assigned to groups rather than individual users based on organizational status.
5	Platform Engineer	Configure cloud-native JIT access solutions to provide temporary elevated access with automatic expiration. Set default access duration to **[Duration, e.g., 4-8 hours]**.
6	DevOps Engineer	Implement self-service portal where engineers can request temporary privileged access with business justification and automated approval workflows.

Step	Who	What
7	Security Officer	Configure emergency break-glass access procedures for critical system outages with automatic expiration within **[Duration, e.g., 2-4 hours]**.
8	Platform Engineer	Configure session recording and monitoring for all privileged access sessions with automated analysis of privileged activities.
9	Security Officer	Configure cloud-native access analytics tools to continuously monitor privileged access patterns with machine learning-based anomaly detection.
10	IT Operations Team	Configure real-time alerting for privileged access anomalies and integrate alerts with security monitoring systems.
11	Platform Engineer	Implement automated monthly validation of privileged access assignments against current HR data and generate exception reports.

Step	Who	What
12	Security Officer	Conduct targeted access reviews only for high-risk exceptions identified by automated monitoring rather than comprehensive quarterly reviews.
13	Security Officer	Conduct and document a quarterly privileged access review covering all privileged accounts and sessions, with sign-off by system owners and the Security Officer.

5. Standards Compliance

See Annex: Control Mapping

7. Definitions

See Annex: Glossary

8. Responsibilities

Role	Responsibility
Security Officer	Define RBAC policies, configure anomaly detection rules, oversee JIT access procedures, and review high-risk access exceptions.
IT Operations Team	Configure and maintain identity management systems, monitor access analytics, respond to access anomalies, and manage automated provisioning.

Role	Responsibility
Platform Engineer	Implement JIT access systems, configure cloud access controls, manage service account automation, and optimize privilege assignments.
DevOps Engineer	Integrate access controls into CI/CD pipelines, manage service account lifecycle, implement session recording, and automate credential rotation.
Managers	Approve exception-based access requests, validate access during role changes, and support incident response access procedures.

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

1. Objective

The objective of this policy is to establish practical requirements for implementing encryption and key management using cloud-native services and automated tools at **[Company Name]**. This policy ensures that sensitive information, particularly electronic Protected Health Information (ePHI), is protected through appropriate cloud-managed encryption technologies while maintaining compliance with HIPAA, HITECH, and SOC 2 requirements in a cost-effective manner.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, and third parties who handle, process, store, or transmit encrypted information. It encompasses all cloud-based information systems, applications, and data storage containing sensitive data. This policy covers cloud-native encryption services, automated key management, and data protection across cloud platforms including AWS, Azure, and Google Cloud Platform.

3. Policy

- **[Company Name]** shall implement cloud-native encryption controls to protect the confidentiality, integrity, and authenticity of sensitive information using automated, managed services that reduce operational complexity while maintaining security and compliance.

3.1 Cloud-Native Encryption Requirements

Encryption shall be implemented using cloud provider managed services for all sensitive information based on data classification levels and regulatory requirements.

3.1.1 Mandatory Encryption Implementations

The following data types and scenarios require encryption using cloud-managed services:

3.1.1.1 Electronic Protected Health Information (ePHI) Encryption

At Rest: AWS S3 Server-Side Encryption, Azure Storage Service Encryption, or GCP encryption at rest using AES-256 shall be implemented for all ePHI storage. **In Transit**: TLS 1.2 or higher automatically managed by cloud load balancers and API gateways shall be implemented for all

ePHI transmission. **Database**: AWS RDS/Aurora encryption, Azure SQL Database Transparent Data Encryption, or GCP Cloud SQL encryption shall be implemented for all databases containing ePHI.

3.1.1.2 Application and System Data Encryption

Application Secrets: AWS Secrets Manager, Azure Key Vault, or GCP Secret Manager shall be used for API keys, passwords, and connection strings. **Configuration Data**: Cloud-native parameter stores with automatic encryption (AWS Systems Manager Parameter Store, Azure App Configuration) shall be implemented. **File Storage**: Automatic encryption for cloud file storage (AWS EFS, Azure Files, GCP Filestore) shall be enabled. **Backup and Archives**: Cloud backup services with automatic encryption (AWS Backup, Azure Backup, GCP Cloud Storage) shall be implemented.

3.1.2 Cloud-Native Encryption Standards

Only cloud provider default encryption implementations and approved algorithms shall be used:

3.1.2.1 Approved Cloud Encryption Services

AWS: KMS-managed keys, S3 encryption, RDS encryption, EBS encryption shall be implemented. **Azure**: Key Vault, Storage Service Encryption, SQL Database TDE, Disk Encryption shall be implemented. **GCP**: Cloud KMS, default encryption at rest, Cloud SQL encryption shall be implemented.

3.1.2.2 Approved Algorithms

AES-256 for symmetric encryption (cloud provider default) shall be used. RSA-3072 or ECC-256 for asymmetric encryption (cloud provider managed) shall be implemented. SHA-256 for hashing and digital signatures (cloud provider managed) shall be used.

3.1.2.3 Prohibited Implementations

Custom encryption implementations without Security Officer approval shall be prohibited. Encryption using deprecated algorithms (DES, 3DES, MD5, SHA-1) shall be prohibited. Unmanaged encryption keys or self-implemented key management shall be prohibited. SSL/TLS versions below 1.2 shall be prohibited.

3.2 Cloud-Managed Key Management

Cryptographic keys shall be managed using cloud provider key management services with automated lifecycle management and minimal manual intervention.

3.2.1 Key Management Principles

3.2.1.1 Cloud-Native Implementation

Cloud provider key management services (AWS KMS, Azure Key Vault, GCP Cloud KMS) shall be used as the primary key management solution.

3.2.1.2 Customer-Managed Encryption Keys

Customer-Managed Encryption Keys (CMEK) shall be implemented for ePHI and sensitive data to maintain control over encryption keys.

3.2.1.3 Automated Lifecycle Management

Automatic key rotation, backup, and lifecycle management provided by cloud services shall be leveraged.

3.2.1.4 Access Control

Key access shall be restricted using cloud IAM policies and service-specific permissions according to least privilege principles.

3.2.2 Cloud Key Management Implementation

3.2.2.1 AWS Key Management Service Implementation

AWS-managed keys shall be used for standard encryption requirements. Customer-Managed Keys (CMK) shall be implemented for ePHI and sensitive data. Automatic key rotation shall be enabled where supported. Cross-region key replication shall be configured for disaster recovery.

3.2.2.2 Azure Key Vault Implementation

Azure-managed keys shall be used for standard encryption requirements. Customer-managed keys shall be implemented for ePHI and sensitive data. Key auto-rotation and versioning shall be enabled.

Geo-redundant backup shall be configured for key availability.

3.2.2.3 Google Cloud Key Management Service Implementation

Google-managed encryption keys shall be used for standard requirements. Customer-managed encryption keys (CMEK) shall be implemented for sensitive data. Automatic key rotation and version management shall be enabled. Multi-region key replication shall be configured for availability.

3.2.3 Access Control and Monitoring

3.2.3.1 IAM Integration

Key access shall be controlled through cloud IAM roles and policies.

3.2.3.2 Multi-Factor Authentication

Multi-factor authentication shall be required for key management console access.

3.2.3.3 Automated Monitoring

Cloud-native monitoring and alerting for key usage, access, and lifecycle events shall be implemented.

3.2.3.4 Audit Logging

Automatic audit trail through cloud logging services (CloudTrail, Azure Monitor, Cloud Audit Logs) shall be maintained.

3.2.4 Cloud-Native Key Management Implementation

- **Cloud Key Management Service Setup:**
  - AWS KMS shall be configured for primary cloud environment with customer-managed keys (CMK) for ePHI and sensitive data encryption with automatic key rotation enabled
  - Azure Key Vault shall be configured for multi-cloud environments with customer-managed keys, appropriate access policies, and soft-delete protection enabled
  - GCP Cloud KMS shall be configured for GCP workloads with customer-managed encryption keys (CMEK), appropriate IAM bindings, and automatic rotation schedules

  - Key usage policies, access controls, and rotation schedules shall be defined and approved to meet HIPAA and HITRUST requirements
- **Automated Key Generation and Management:**
  - Infrastructure as Code (IaC) shall define key management resources using Terraform, CloudFormation, or ARM templates including key policies, rotation schedules, and access controls in version-controlled infrastructure code
  - Applications shall be configured to use cloud key management APIs for encryption operations with proper error handling and fallback mechanisms for service unavailability
  - Cross-region key replication shall be configured for disaster recovery ensuring replicated keys maintain the same access policies and rotation schedules as primary keys
  - Automatic key rotation shall be enabled for supported key types with application logic implemented to handle key rotation events without service interruption
- **Application-Level Encryption Integration:**
  - Cloud provider SDKs and APIs shall be integrated for encryption operations within applications using envelope encryption patterns for large data objects and direct encryption for smaller data elements
  - Database systems shall be configured to use cloud-managed transparent data encryption (TDE) with customer-managed keys ensuring ePHI database fields use appropriate encryption methods
  - Cloud storage services shall be configured to use customer-managed keys for automatic encryption at rest including all storage tiers for backup and archive storage
  - Applications shall retrieve encryption keys and secrets from cloud secret management services rather than embedded credentials
- **Monitoring and Compliance Automation:**
  - Comprehensive audit logging shall be enabled for all key management operations using cloud provider audit services with log retention according to compliance requirements
  - Automated monitoring and alerting shall be configured for key usage anomalies, failed encryption operations, and unauthorized access attempts with integration to existing security monitoring systems
  - Automated compliance reporting shall be established for key management activities with monthly reports on key usage, rotation status, and access patterns for audit and compliance purposes
  - Key management service performance and latency impact shall be monitored with automated scaling and failover mechanisms for high-availability operations

- **Key Recovery and Disaster Response:**
  - Automated backup of key metadata and access policies shall be configured to secure storage with cross-region replication for disaster recovery scenarios
  - Key recovery procedures shall be documented and tested for disaster scenarios ensuring recovery procedures can restore key access within **[Timeframe, e.g., 4 hours]** to meet business continuity requirements
  - Emergency access procedures shall be configured for key management services during outages with break-glass access controls that maintain audit trails and security controls
  - Quarterly testing of key management service failover and recovery procedures shall be conducted with documented results and procedure updates based on findings
- **Cost Optimization and Management:**
  - Key management service usage and costs shall be monitored through cloud billing and cost management tools with identification of cost optimization opportunities through efficient key usage patterns
  - Appropriate caching strategies shall be implemented for key operations to reduce API call costs while maintaining security including data encryption keys (DEK) caching for high-volume operations
  - Key management service tiers and features shall be reviewed and optimized based on actual usage patterns and security requirements eliminating unused or redundant features
  - Automated lifecycle management shall be implemented for unused or expired keys with automatic deletion schedules for development and testing environments while preserving production keys according to retention policies

3.3 Application and Development Encryption

Encryption shall be integrated into application development using cloud-native services and secure coding practices.

3.3.1 Application-Level Encryption

3.3.1.1 Secrets Management

Cloud secrets management services (AWS Secrets Manager, Azure Key Vault, GCP Secret Manager) shall be used for application credentials.

3.3.1.2 API Security

TLS termination at cloud load balancers with automatic certificate management shall be implemented.

3.3.1.3 Data Processing

Cloud encryption APIs shall be used for data processing and storage operations.

3.3.1.4 Container Security

Encryption for container orchestration platforms (EKS, AKS, GKE) using cloud-managed keys shall be enabled.

3.3.2 Development and Deployment

3.3.2.1 Infrastructure as Code

Encryption configurations shall be defined in infrastructure code (Terraform, CloudFormation, ARM templates).

3.3.2.2 CI/CD Integration

Encryption validation and configuration checks shall be implemented in automated deployment pipelines.

3.3.2.3 Environment Parity

Encryption configurations shall be consistent across development, staging, and production environments.

3.3.2.4 Security Scanning

Cloud security scanning tools shall be used to validate encryption implementations.

3.4 Performance and Cost Optimization

Cloud-native encryption implementations shall be optimized for performance and cost-effectiveness.

3.4.1 Performance Optimization

3.4.1.1 Default Encryption

Cloud provider default encryption that provides minimal performance impact shall be leveraged.

3.4.1.2 Regional Deployment

Encryption services shall be deployed in regions close to data and applications to minimize latency.

3.4.1.3 Caching

Appropriate caching strategies for encrypted data and key operations shall be implemented.

3.4.1.4 Auto-Scaling

Cloud auto-scaling features shall be used to handle encryption processing loads.

3.4.2 Cost Management

3.4.2.1 Service Tier Selection

Appropriate cloud encryption service tiers shall be chosen based on usage requirements.

3.4.2.2 Key Usage Optimization

Key usage patterns shall be optimized to minimize cloud KMS API charges.

3.4.2.3 Storage Class Selection

Appropriate cloud storage classes for encrypted backup and archive data shall be used.

3.4.2.4 Regular Review

Quarterly reviews of encryption service costs and optimization opportunities shall be conducted.

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Security Officer	Develop cloud encryption strategies, approve service configurations, and ensure compliance with cryptographic standards.
Cloud Engineering Team	Configure and deploy cloud-native encryption services according to approved standards and security requirements.
DevOps Team	Integrate encryption validation into CI/CD pipelines and maintain secure application secret management.
Development Team	Implement encryption requirements in application code using cloud encryption APIs and best practices.
IT Operations Team	Manage cloud encryption service accounts, access controls, and cost optimization strategies.
Compliance Team	Provide audit support and ensure encryption practices meet regulatory requirements.

Mobile Device Security Policy (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. 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. This unified policy addresses technical security controls, business usage guidelines, and Bring Your Own Device (BYOD) program requirements to provide a single source of truth for all mobile device security.

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 across all business environments and usage scenarios.

3. Policy

[Company Name] shall implement comprehensive mobile device security controls that balance workforce mobility and productivity needs with robust technical security, data protection, privacy rights, and regulatory compliance requirements.

Section A: Technical Security Requirements

3.1 Mobile Device Technical Security Framework

A comprehensive technical security framework shall be implemented to protect mobile devices and ensure consistent security posture across all device types and usage scenarios.

3.1.1 Device Security Classification and Technical Requirements

Technical Security Levels:

- **Level 1 - Basic Technical Security**: Standard encryption, basic MDM enrollment, passcode protection, and fundamental security configurations for email and basic business applications
- **Level 2 - Enhanced Technical Security**: Full disk encryption, advanced MDM with compliance monitoring, multi-factor authentication, and enhanced monitoring for internal systems and Confidential information
- **Level 3 - Maximum Technical Security**: Hardware-based encryption, advanced MDM with containerization, continuous monitoring, and dedicated business environments for ePHI and Restricted information

Technical Security Baseline Requirements:

- Operating system security baseline compliance with industry standards (CIS Benchmarks, NIST guidelines) shall be implemented for all managed devices
- Automatic security update installation with enterprise patch management integration shall be configured and maintained
- Endpoint detection and response (EDR) deployment shall be implemented where technically feasible for enhanced threat protection
- Network security controls including VPN enforcement and traffic filtering shall be deployed for secure remote connectivity
- Application security controls including sandboxing and runtime protection shall be implemented for business application protection

3.1.2 Approved Mobile Device Technical Specifications

Supported Device Types and Security Requirements:

- **iOS Devices**: iOS **[Version, e.g., 15.0]** or later with hardware-based Secure Enclave for encryption key management shall be required
- **Android Devices**: Android **[Version, e.g., 11.0]** or later with security patch level within **[Timeframe, e.g., 90 days]** and hardware-backed keystore shall be required
- **Windows Devices**: Windows **[Version, e.g., 10]** Pro or Enterprise with TPM 2.0 and BitLocker encryption capability shall be required
- **macOS Devices**: macOS **[Version, e.g., 12.0]** or later with T2 Security Chip or Apple Silicon secure boot shall be required

Prohibited Devices:

- Devices with modified firmware (jailbroken/rooted devices) shall be automatically blocked

from accessing organizational resources

- Devices running unsupported or end-of-life operating systems shall be prohibited from accessing company systems
- Devices with known critical vulnerabilities that are unpatched shall be blocked from system access
- Personal gaming devices or IoT devices shall be prohibited from accessing business information

3.2 Mobile Device Management (MDM) Technical Implementation

Comprehensive mobile device management systems shall provide centralized technical security control and monitoring for all enrolled devices.

3.2.1 MDM Platform Security Architecture

MDM Infrastructure Security:

- Redundant MDM server deployment with high availability and disaster recovery capabilities shall be implemented
- Secure certificate-based device enrollment with automated provisioning and validation shall be configured
- Encrypted communication channels between MDM servers and enrolled devices using TLS 1.3 or equivalent shall be maintained
- Integration with enterprise identity management systems for centralized authentication and authorization shall be established
- API security controls for MDM system integrations with rate limiting, authentication, and monitoring shall be implemented

MDM Enrollment Requirements:

- All devices shall be enrolled in MDM before accessing company information systems or data
- Device enrollment shall require management approval and IT verification before access is granted
- Users shall accept MDM terms and conditions including remote wipe capabilities as a condition of access
- Device compliance shall be verified before initial access is granted to organizational resources

3.2.2 Technical Security Policy Configuration

Device Security Configuration Management:

- Minimum passcode complexity enforcement: minimum 6-digit passcode with alphanumeric requirements for Level 2+ devices shall be implemented
- Automatic screen lock after **[Duration, e.g., 5 minutes]** of inactivity with immediate lock capability shall be configured
- Maximum failed unlock attempts configuration: **[Number, e.g., 10]** attempts before device wipe for Level 3 devices shall be enforced
- Automatic device encryption enforcement with hardware-backed key storage where available shall be implemented
- Bluetooth and Wi-Fi security restrictions including approved protocol versions and certificate validation shall be configured

Application and Data Security Controls:

- Application installation restrictions with approved application catalog enforcement shall be implemented
- Application sandboxing and data isolation with enterprise containerization for business applications shall be configured
- Data loss prevention (DLP) controls for copy/paste, file sharing, and screen capture activities shall be deployed
- Automatic application updates with security patch priority and emergency patching capabilities shall be maintained
- Mobile application management (MAM) integration with conditional access and data protection shall be implemented

3.3 Mobile Device Encryption and Cryptographic Controls

Comprehensive encryption and cryptographic controls shall protect data at rest and in transit on all mobile devices.

3.3.1 Device Encryption Requirements

Full Device Encryption:

- Full disk encryption shall be mandatory for all devices accessing company information using

hardware-accelerated encryption where available

- Hardware-based key storage utilizing device secure elements, TPM, or equivalent security hardware shall be implemented
- Encryption key management with automatic key rotation and secure key escrow for enterprise recovery shall be configured
- File-level encryption for additional protection of sensitive data files and databases shall be deployed where required
- Encrypted backup storage with separate encryption keys and secure backup validation shall be maintained

Cryptographic Implementation Standards:

- Advanced Encryption Standard (AES) 256-bit encryption for data at rest with approved cryptographic modules shall be implemented
- Elliptic Curve Cryptography (ECC) for key exchange and digital signatures with FIPS 140-2 Level 2 or higher validation shall be used
- SHA-256 or stronger hashing algorithms for data integrity validation and digital signatures shall be implemented
- Perfect Forward Secrecy (PFS) implementation for network communications shall be deployed where technically feasible
- Quantum-resistant cryptographic algorithms shall be considered for future-proofing where available

3.3.2 Data-in-Transit Protection

Network Communication Security:

- Transport Layer Security (TLS) 1.3 or equivalent for all network communications with certificate validation shall be implemented
- Certificate pinning for business applications to prevent man-in-the-middle attacks shall be deployed
- VPN requirement for access to internal systems with enterprise-grade VPN protocols (IPSec, WireGuard) shall be enforced
- Wi-Fi security enforcement with WPA3 or equivalent encryption and enterprise authentication shall be implemented
- Mobile network security with carrier-grade encryption and network access control integration shall be maintained

Section B: Business Usage and Data Handling

3.4 Mobile Device Business Usage Framework

A comprehensive business usage framework shall define appropriate mobile device usage scenarios and establish clear guidelines for business activities and data handling.

3.4.1 Business Access Classification and Usage Guidelines

Business Access Levels and Usage Scenarios:

- **Level 1 - Basic Business Access**: Email, calendar, contacts, and approved business communication applications with standard data protection
- **Level 2 - Standard Business Access**: Internal business applications, confidential information access, and collaborative tools with enhanced data protection
- **Level 3 - Restricted Business Access**: ePHI access, restricted information handling, and mission-critical applications with maximum data protection

Approved Business Usage Activities:

- Email access and business communication with approved email clients and security controls shall be permitted
- Calendar and scheduling management with corporate directory integration and meeting security shall be enabled
- Document access and collaboration using approved business applications with data protection controls shall be supported
- Business application usage including CRM, ERP, and industry-specific applications with appropriate security measures shall be authorized
- Video conferencing and communication tools with privacy protection and data handling controls shall be implemented

3.4.2 Business Data Handling and Classification

Data Classification and Handling Requirements:

- **Public Data**: General business information with standard mobile security controls shall be permitted
- **Internal Data**: Internal business information with enhanced mobile security and access logging shall be protected

- **Confidential Data**: Sensitive business information requiring advanced mobile security and monitoring shall be secured
- **Restricted Data**: ePHI and highly sensitive information requiring maximum mobile security and company-owned devices shall be protected

Business Data Protection Responsibilities:

- Data access shall be limited to authorized business purposes with audit logging and monitoring
- Data sharing and transmission shall use approved business channels with encryption and access controls
- Data storage and backup shall follow corporate data management policies with secure cloud storage integration
- Data retention and disposal shall be conducted in accordance with business records management and regulatory requirements
- Data incident reporting shall include immediate notification and response procedures

Section C: Bring Your Own Device (BYOD) Program

3.5 BYOD Program Management and Requirements

A comprehensive BYOD program shall enable personal device usage for business purposes while maintaining appropriate security controls and privacy protections.

3.5.1 BYOD Program Eligibility and Enrollment

BYOD Participation Requirements:

- Formal application and approval process with manager authorization and HR verification shall be required
- Device compatibility assessment with technical requirements validation and security evaluation shall be conducted
- Background check requirements for access to restricted information with periodic revalidation shall be completed
- Signed BYOD agreement acknowledging security policies, monitoring, and remote management capabilities shall be mandatory
- Annual device revalidation and security assessment with compliance verification and policy updates shall be performed

BYOD Device Approval Criteria:

- Current operating system with latest security patches and manufacturer support shall be required
- Compatibility with enterprise mobile device management (MDM) and security requirements shall be verified
- Hardware-based security features including encryption support and biometric authentication shall be validated
- Adequate storage capacity and performance for business applications and data protection shall be confirmed
- User agreement to security policy enforcement including remote wipe and monitoring capabilities shall be documented

3.5.2 BYOD Security and Privacy Framework

Business and Personal Data Separation:

- Containerization technology to separate business and personal data with distinct security policies shall be implemented
- Separate email profiles and application workspaces with independent security controls and backup procedures shall be maintained
- Personal application restrictions that could compromise business data security or introduce vulnerabilities shall be enforced
- Selective wipe capability for business data only with personal data protection and privacy preservation shall be configured
- Data loss prevention (DLP) controls for business information with user privacy protection shall be deployed

Privacy Protection and User Rights:

- Clear communication of monitoring capabilities and data access rights with transparent privacy practices shall be provided
- Limited monitoring scope to business-related activities with personal activity exclusion and privacy boundaries shall be maintained
- Data minimization principles for collected information with purpose limitation and retention controls shall be applied
- User consent and opt-out procedures for monitoring and data collection with alternative ar-

rangement options shall be established
- Secure disposal of personal information upon employment termination with privacy protection validation shall be ensured

Section D: User Responsibilities and Security Controls

3.6 User Responsibilities and Accountability

Clear user responsibilities and accountability measures shall ensure appropriate mobile device usage and compliance with business and security requirements.

3.6.1 Device Security and Maintenance Responsibilities

User Security Responsibilities:

- Current operating system and security patches shall be maintained with automated update enablement where possible
- Strong device authentication including passcodes, PINs, or biometric authentication with complexity requirements shall be used
- Lost, stolen, or compromised devices shall be reported promptly with immediate notification procedures
- Unauthorized applications or device security setting modifications that could compromise business data shall be avoided
- Required security training and awareness programs with competency validation and annual updates shall be completed

Device Maintenance and Care:

- Proper physical security including device storage, transportation, and protection from theft or unauthorized access shall be maintained
- Regular backup of personal data to prevent loss during business security procedures or device management shall be performed
- Compliance with device usage policies including acceptable use, location restrictions, and activity monitoring shall be maintained
- Cooperation with IT support for device troubleshooting, security updates, and compliance verification shall be provided
- Responsible disposal or return of devices following corporate procedures with data sanitization and asset management shall be ensured

3.6.2 Business Application and Data Usage

Application Usage Guidelines:

- Only approved business applications for accessing company information with version management and security validation shall be used
- Application security requirements including authentication, session management, and data protection shall be followed
- Application security issues or suspected malware shall be reported immediately with detailed incident information
- Business applications for personal purposes or mixing business and personal data within applications shall be avoided
- Application training and support programs with competency validation and ongoing education shall be completed

Data Handling and Protection:

- Company data shall be accessed only for authorized business purposes with appropriate justification and audit trails
- Confidential and restricted information shall be protected from unauthorized disclosure or access with appropriate security measures
- Approved data sharing and transmission methods with encryption and access controls shall be used
- Data retention and disposal requirements with secure deletion and sanitization procedures shall be followed
- Data security incidents or suspected breaches shall be reported immediately with detailed incident documentation

3.7 Mobile Application Security Framework

Comprehensive security controls shall be implemented for mobile applications to ensure secure application development, deployment, and operation.

3.7.1 Application Security Development and Testing

Secure Mobile Application Development:

- Secure coding practices for mobile applications with OWASP Mobile Top 10 compliance shall

be implemented

- Static application security testing (SAST) and dynamic application security testing (DAST) for all custom applications shall be conducted
- Third-party application security assessment with vendor security validation and penetration testing shall be performed
- Code signing and integrity verification for application deployment with certificate-based validation shall be implemented
- Application vulnerability scanning and management with automated patching and update procedures shall be maintained

Application Approval Process:

- All mobile applications shall be reviewed and approved before installation on devices accessing company information
- Security assessment of applications including code review and penetration testing shall be performed for high-risk applications
- Vendor security assessments for third-party applications shall be conducted before approval is granted
- Application risk classification and appropriate controls implementation shall be performed based on data sensitivity
- Regular application security updates and patch management shall be maintained to address security vulnerabilities

3.7.2 Application Runtime Security and Management

Runtime Security Controls:

- Runtime application self-protection (RASP) implementation for critical business applications shall be deployed
- Application sandboxing and isolation with inter-process communication restrictions shall be maintained
- Anti-tampering and reverse engineering protection for sensitive applications shall be implemented
- Application performance monitoring (APM) with security event correlation and alerting shall be configured
- Behavioral analysis and anomaly detection for application usage patterns and security events shall be implemented

Mobile Application Management (MAM) Technical Controls:

- Enterprise application containerization with separate cryptographic keys and data protection shall be implemented
- Application data isolation with per-application encryption and access controls shall be maintained
- Selective wipe capability for business applications and data with granular control shall be configured
- Application network isolation with VPN-per-app and traffic filtering capabilities shall be deployed
- Integration with enterprise identity providers for single sign-on (SSO) and conditional access shall be established

Section E: Monitoring and Incident Response

3.8 Mobile Device Monitoring and Threat Detection

Comprehensive monitoring and threat detection capabilities shall provide real-time visibility into mobile device security events and threats.

3.8.1 Device Security Monitoring

Continuous Compliance Monitoring:

- Real-time device compliance status monitoring with automated reporting and alerting shall be implemented
- Device health and security posture assessment with risk scoring and trending analysis shall be conducted
- Configuration drift detection with automatic remediation and policy enforcement shall be maintained
- Application inventory and unauthorized software detection with automatic removal capabilities shall be deployed
- Network behavior monitoring with anomaly detection and threat correlation shall be implemented

Mobile Threat Detection and Response:

- Mobile threat detection (MTD) platform integration with enterprise security operations center

(SOC) shall be established
- Malware and phishing detection with real-time threat intelligence and behavioral analysis shall be implemented
- Network-based threat detection with DNS filtering and traffic analysis shall be deployed
- Device behavior analysis with machine learning-based anomaly detection shall be configured
- Automated threat response with quarantine, remediation, and incident escalation procedures shall be implemented

3.8.2 Security Event Correlation and Analysis

Integration with Enterprise Security Systems:

- Security information and event management (SIEM) integration for mobile security events shall be established
- User and entity behavior analytics (UEBA) integration for cross-platform threat detection shall be implemented
- Threat intelligence platform integration for mobile threat indicators and attack patterns shall be configured
- Security orchestration and automated response (SOAR) integration for incident response automation shall be deployed
- Enterprise risk management integration for mobile security risk assessment and reporting shall be maintained

3.9 Mobile Device Incident Response and Recovery

Specialized incident response procedures shall address mobile device security events and ensure rapid recovery from security incidents.

3.9.1 Lost or Stolen Device Procedures

- All lost or stolen devices shall be reported to the IT Security Team immediately, and in no case later than **[Number, e.g., 1]** hour after discovery
- Remote location and tracking attempts shall be initiated immediately upon notification of device loss
- Remote lock and wipe procedures shall be executed according to established incident response protocols

- Access credential revocation and reset shall be performed immediately to prevent unauthorized access
- Law enforcement reporting shall be performed if required by organizational policy or regulatory requirements
- Incident documentation and lessons learned shall be completed for all device loss events

3.9.2 Mobile Security Incident Detection and Response

Incident Detection and Classification:

- Automated incident detection for mobile security events with severity classification and escalation shall be implemented
- Mobile-specific incident types including device theft, malware infection, data leakage, and policy violations shall be addressed
- Incident correlation across multiple mobile devices and enterprise systems for advanced threat detection shall be performed
- Forensic evidence collection procedures for mobile devices with legal admissibility requirements shall be established
- Chain of custody procedures for mobile device evidence with secure handling and documentation shall be maintained

Incident Response and Recovery Procedures:

- Remote device location and tracking capabilities with law enforcement coordination procedures shall be available
- Remote lock and wipe procedures with immediate containment and selective data removal shall be executable
- Device quarantine and network isolation with graduated response based on threat severity shall be implemented
- Incident communication procedures with affected users, management, and regulatory authorities shall be established
- Post-incident device restoration and re-enrollment procedures with security validation shall be defined

3.10 Device Lifecycle Security Management

Comprehensive lifecycle management shall ensure secure device onboarding, maintenance, and offboarding procedures.

3.10.1 Device Onboarding Security

Device Onboarding:

- Security assessment and approval process shall be completed before device access is granted
- MDM enrollment and configuration shall be performed according to established procedures
- User training on security requirements shall be provided before device activation
- Initial compliance verification shall be completed to ensure policy adherence
- Automated device enrollment with security validation and compliance verification shall be implemented

3.10.2 Device Offboarding and Data Sanitization

Device Offboarding:

- Complete data wipe and sanitization shall be performed for all device terminations using NIST 800-88 compliant data destruction procedures
- MDM unenrollment and access revocation shall be completed immediately upon employment termination
- Certificate and credential removal shall be performed to prevent unauthorized future access
- Device return procedures (company-owned devices) shall be followed according to organizational policy
- Exit interview and security debriefing shall be conducted to address security concerns

Section F: Training and Support

3.11 Mobile Device Security Training and Support

Comprehensive support and training programs shall ensure effective mobile device usage and security compliance for business activities.

3.11.1 User Training and Education

Mandatory Mobile Security Training:

- Initial mobile device security training for all users including policy overview, security requirements, and incident procedures shall be provided
- Annual security awareness updates covering emerging threats, policy changes, and best practices shall be delivered
- Role-specific training for users with access to restricted information including ePHI handling and compliance requirements shall be conducted
- BYOD program training covering personal device management, privacy rights, and security obligations shall be provided
- Incident response training including device theft reporting, security incident recognition, and response procedures shall be delivered

Ongoing Education and Support:

- Regular security awareness communications including threat alerts, policy updates, and best practice guidance shall be provided
- Self-service training resources including videos, documentation, and interactive learning modules shall be available
- Peer support programs and mobile security champions with advanced training and mentoring capabilities shall be established
- Feedback mechanisms for policy improvement and user experience enhancement with continuous program refinement shall be maintained
- Performance measurement and competency assessment with targeted improvement programs shall be implemented

3.11.2 Business Support Services

Technical Support and Troubleshooting:

- Help desk support for mobile device business usage including application issues, connectivity problems, and security concerns shall be provided
- Device enrollment assistance for BYOD program participants with guided setup and validation procedures shall be available
- Application installation and configuration support with security validation and user training shall be offered

- Password and authentication support including multi-factor authentication setup and troubleshooting shall be provided
- Device replacement and upgrade support with data migration and security configuration transfer shall be available

Business Process Integration:

- Mobile device integration with business workflows and process automation with user training and support shall be implemented
- Application rollout and adoption support with change management and user communication shall be provided
- Business continuity planning for mobile device dependencies with alternative access methods and recovery procedures shall be established
- Performance monitoring and optimization for business applications with user feedback and improvement initiatives shall be conducted
- Cost management and budgeting support for mobile device programs with usage tracking and optimization shall be provided

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Mobile Security Team	Overall mobile device security program management, technical control implementation, and policy coordination.
IT Security Team	Integration of mobile security with enterprise security controls, threat detection, and incident response coordination.
MDM Administrators	Configuration and maintenance of mobile device management systems, policy enforcement, and device lifecycle management.

Role	Responsibility
Mobile Program Manager	BYOD program management, business requirements alignment, and cross-functional coordination.
Human Resources	BYOD agreement management, employment law compliance, workforce training coordination, and privacy rights protection.
Business Unit Managers	Team mobile device usage approval, business requirement definition, user accountability, and security compliance oversight.
Privacy Officer	Privacy protection oversight, BYOD privacy rights implementation, and regulatory compliance coordination.
Legal Team	BYOD agreement development, regulatory compliance validation, liability management, and eDiscovery coordination.
Training and Development Team	Mobile security training delivery, user education programs, and competency assessment coordination.
IT Support Team	Business user support, device enrollment assistance, application support, and technical troubleshooting.
Security Operations Center (SOC)	24/7 monitoring of mobile security events, incident detection and response, and threat analysis.
Network Security Team	Implementation of network security controls for mobile devices, VPN management, and traffic monitoring.
Application Security Team	Mobile application security testing, approval, and runtime protection implementation.
System Administrators	Technical infrastructure support for mobile security systems, certificate management, and integration maintenance.
All Mobile Device Users	Compliance with mobile device security policies, security responsibility fulfillment, and incident reporting.

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

1. Objective

The objective of this policy is to establish practical, cloud-native data retention and disposal practices that meet regulatory requirements for electronic Protected Health Information (ePHI) and business data while leveraging automated technical controls to minimize administrative overhead.

2. Scope

This policy applies to all **[Company Name]** workforce members who create, process, or access company information in cloud environments and systems. It covers electronic information stored in cloud services, databases, applications, and backup systems, with focus on automated lifecycle management rather than manual governance processes.

3. Policy

- **[Company Name]** shall implement automated data retention and disposal practices using cloud-native services and technical controls to ensure regulatory compliance while minimizing manual administrative overhead.

3.1 Automated Data Retention Framework

Data retention shall be implemented through automated technical controls rather than manual governance processes, leveraging cloud service provider capabilities and application-level lifecycle management.

3.1.1 Cloud-Native Retention Implementation

- **Electronic Protected Health Information (ePHI):**
- **Database Retention**: Automated deletion based on configurable retention periods (minimum 6 years per HIPAA requirements)
- **Cloud Storage Lifecycle**: AWS S3 Lifecycle, Azure Blob Lifecycle, or GCP Object Lifecycle policies for automatic data tiering and deletion
- **Application Data**: Built-in retention logic within applications with automated background processing

- **Backup Retention**: Cloud backup services configured with automatic retention policy enforcement
- **Business and Operational Data:**
- **Application Logs**: Automated log rotation and retention (typically **[Duration, e.g., 1-2 years]**)
- **System Logs**: Cloud logging services with configurable retention periods
- **Development Data**: Automated cleanup of staging and development environments
- **Analytics Data**: Automated data lifecycle management within analytics platforms

3.1.2 Retention Period Configuration

Instead of complex retention schedules, use simplified categorization with automated enforcement:

- **Regulatory Data (ePHI and Compliance):**
- **Retention Period**: 6 years minimum (HIPAA requirement) shall be enforced for all ePHI and compliance-related data.
- **Implementation**: Database triggers, application logic, cloud storage policies shall be configured to automatically enforce retention requirements.
- **Monitoring**: Automated alerts for retention policy violations or failures shall be implemented to ensure compliance.
- **Business Data (Operational Records):**
- **Retention Period**: **[Duration, e.g., 3-7 years]** based on business requirements shall be established and enforced for operational records.
- **Implementation**: Application-level retention with cloud storage lifecycle policies shall be configured to manage business data lifecycle.
- **Monitoring**: Dashboard reporting on data lifecycle status shall be maintained to provide visibility into retention compliance.
- **System Data (Logs, Monitoring, Backups):**
- **Retention Period**: **[Duration, e.g., 1-2 years]** for operational needs shall be configured for system data.

- **Implementation**: Cloud service automatic retention and deletion shall be configured to manage system data lifecycle.
- **Monitoring**: Service-level monitoring and alerting shall be implemented to track system data retention compliance.

3.1.3 Legal Hold Automation

- **Technical Implementation**: Application flags or database fields shall be used to prevent automated deletion when legal holds are in effect.
- **Integration**: Legal hold status shall be integrated with automated retention systems to ensure proper data preservation.
- **Notification**: Automated alerts shall be generated when legal hold affects normal retention processes.
- **Release**: Automated restoration of normal retention policies shall occur upon legal hold release with appropriate approvals.

3.2 Cloud-Native Data Disposal

Data disposal shall leverage cloud provider certified deletion processes and automated technical controls rather than manual oversight.

3.2.1 Automated Disposal Triggers

- **Application Logic**: Built-in data lifecycle management shall be implemented within applications to automate disposal processes.
- **Cloud Storage Policies**: Automatic deletion through cloud provider lifecycle management shall be configured and maintained.
- **Database Maintenance**: Automated database cleanup jobs and archival processes shall be scheduled and monitored.
- **Backup Expiration**: Automatic backup deletion based on cloud service retention policies shall be implemented and verified.

3.2.2 Cloud Provider Disposal Methods

- **Amazon Web Services (AWS):**

- **S3 Object Deletion**: AWS's secure deletion processes with cryptographic erasure shall be leveraged for object storage data disposal.
- **EBS Volume Deletion**: AWS shall handle secure wiping per NIST SP 800-88 guidelines for block storage disposal.
- **RDS Deletion**: Automated secure deletion of database instances and snapshots shall be performed through AWS RDS services.
- **Backup Deletion**: AWS Backup shall automatically handle secure disposal of expired backups according to configured retention policies.
- **Microsoft Azure:**
- **Blob Storage Deletion**: Azure's certified secure deletion processes shall be utilized for blob storage data disposal.
- **Managed Disk Deletion**: Cryptographic erasure and physical overwriting shall be performed according to Azure security standards.
- **SQL Database Deletion**: Automated secure deletion of database resources shall be performed through Azure SQL services.
- **Azure Backup Deletion**: Automatic secure disposal shall be performed through Azure Recovery Services according to retention policies.
- **Google Cloud Platform (GCP):**
- **Cloud Storage Deletion**: Google's certified data destruction processes shall be utilized for cloud storage data disposal.
- **Persistent Disk Deletion**: Cryptographic erasure and secure overwriting shall be performed according to GCP security standards.
- **Cloud SQL Deletion**: Automated secure deletion of database instances shall be performed through Google Cloud SQL services.
- **Cloud Backup Deletion**: Automatic secure disposal shall be performed through Google Cloud backup services according to retention policies.

3.2.3 Disposal Verification

- **Cloud Provider Certifications**: SOC 2, ISO 27001, and other certifications shall be relied upon for disposal assurance and compliance verification.
- **Automated Logging**: Cloud service logs shall provide audit trail for deletion activities and disposal verification.
- **Compliance Reporting**: Automated reports shall be generated demonstrating disposal compliance and regulatory adherence.
- **Exception Monitoring**: Automated alerts shall be configured for disposal failures or anomalies requiring attention.

3.3 Application-Level Data Lifecycle Management

Applications shall implement built-in data lifecycle management to automate retention and disposal without manual intervention.

3.3.1 Database Lifecycle Management

- **Automated Archival**: Database jobs shall be implemented to move aging data to archive tables or storage tiers according to retention schedules.
- **Partition Management**: Date-based table partitioning shall be implemented for efficient lifecycle management and automated data removal.
- **Trigger-Based Deletion**: Database triggers shall be configured to enforce retention policies during normal operations.
- **Soft Deletion**: Application-level logical deletion with automated physical cleanup shall be implemented to manage data lifecycle.

3.3.2 File and Document Management

- **Metadata-Based Lifecycle**: File metadata shall drive automated retention and disposal decisions without manual intervention.
- **Version Control**: Automated cleanup of old file versions shall be performed based on retention requirements and business needs.
- **Integration with Cloud Storage**: Applications shall leverage cloud storage lifecycle policies for automated file management.
- **Automated Classification**: Applications shall automatically classify data for appropriate re-

tention treatment.

3.3.3 Development and Testing Data

- **Environment Refresh**: Automated refresh of development/staging environments with production data subset shall be performed according to established schedules.
- **Test Data Lifecycle**: Automated cleanup of synthetic and anonymized test data shall be implemented to manage development data retention.
- **Development Artifact Cleanup**: Automated deletion of old build artifacts and temporary files shall be performed to maintain system performance.
- **Database Anonymization**: Automated anonymization processes for development data retention shall be implemented to protect sensitive information.

3.4 Monitoring and Compliance Automation

Compliance monitoring shall be automated through technical controls and service-level monitoring rather than manual audits.

3.4.1 Automated Compliance Monitoring

- **Retention Policy Enforcement**: Automated monitoring of retention policy implementation and compliance shall be maintained to ensure policy adherence.
- **Disposal Verification**: Automated verification that data is being disposed according to policy requirements shall be performed for all disposal activities.
- **Exception Detection**: Automated detection and alerting for retention policy violations shall be implemented to provide immediate notification.
- **Regulatory Reporting**: Automated generation of compliance reports for HIPAA and other requirements shall be performed according to regulatory schedules.

3.4.2 Performance and Cost Optimization

- **Storage Cost Monitoring**: Automated monitoring of storage costs related to retention policies shall be implemented to optimize resource utilization.
- **Performance Impact Assessment**: Monitoring of retention policy impact on application performance shall be conducted to ensure system efficiency.

- **Optimization Recommendations**: Automated recommendations for retention policy optimization shall be generated based on performance metrics.
- **Resource Utilization**: Monitoring of compute and storage resources used for retention processing shall be performed to manage operational costs.

3.5 Emergency and Legal Hold Procedures

Streamlined procedures for emergency data preservation and legal hold requirements without complex governance overhead.

3.5.1 Emergency Data Preservation

- **Technical Implementation**: Database flags or API calls to suspend automated deletion shall be implemented for emergency situations.
- **Rapid Response**: Ability to preserve data within **[Timeframe, e.g., 2 hours]** of notification shall be maintained for urgent preservation requirements.
- **Documentation**: Automated logging of preservation actions and affected data shall be performed to create audit trails.
- **Coordination**: Clear escalation to Security Officer for emergency preservation requests shall be established for rapid response.

3.5.2 Simplified Legal Hold

- **Technical Hold**: Application-level flags to prevent automated deletion of specific data sets shall be implemented for legal hold requirements.
- **Automated Notification**: System notifications when legal hold affects normal data lifecycle shall be generated to inform stakeholders.
- **Impact Assessment**: Automated reporting on storage and cost impact of legal holds shall be provided for management review.
- **Release Process**: Streamlined process for releasing legal holds and resuming normal lifecycle shall be maintained for efficient operations.

3.6 Vendor and Service Provider Management

Simplified approach to third-party data disposal leveraging cloud provider certifications and automated processes.

3.6.1 Cloud Provider Reliance

- **Certification Acceptance**: Major cloud provider (AWS, Azure, GCP) disposal certifications shall be accepted as sufficient assurance for data destruction.
- **Contract Terms**: Standard cloud provider terms for data disposal and destruction shall be incorporated into service agreements.
- **Audit Reports**: Annual review of cloud provider SOC 2 and security certification reports shall be performed to verify disposal capabilities.
- **Service Level Agreements**: Cloud provider SLAs for disposal timelines and assurance shall be relied upon for compliance verification.

3.6.2 Specialized Disposal Services

For rare cases requiring specialized disposal:

- **Pre-Approved Vendors**: A short list of certified disposal vendors for edge cases shall be maintained for specialized requirements.
- **Simplified Assessment**: Basic vendor qualification process focused on certifications shall be implemented for vendor evaluation.
- **Automated Documentation**: Electronic certificates of destruction and audit trails shall be obtained for all specialized disposal activities.
- **Cost Management**: Focus on cost-effective disposal for limited specialized requirements shall be maintained to optimize expenses.

4. Responsibilities

4.1 Security Officer

- **Policy Oversight**: Review and approve automated data retention configurations and procedures shall be performed to ensure policy compliance.
- **Compliance Monitoring**: Automated systems that maintain regulatory compliance (HIPAA, HITRUST, SOC 2) shall be ensured through oversight activities.
- **Legal Hold Coordination**: Primary contact for legal hold requests and coordination of technical implementation shall be served to manage legal requirements.
- **Exception Management**: Exceptions to automated retention policies shall be reviewed and approved to maintain security standards.
- **Vendor Management**: Cloud provider disposal certifications and specialized disposal vendor

relationships shall be overseen to ensure compliance.

4.2 Platform Engineering Team

- **Technical Implementation**: Cloud-native retention and disposal systems shall be configured and maintained to support organizational requirements.
- **Automation Development**: Automated data lifecycle management within applications shall be developed and maintained for operational efficiency.
- **Cloud Service Configuration**: Cloud storage lifecycle policies and retention rules shall be set up and maintained according to policy requirements.
- **Monitoring Implementation**: Automated monitoring and alerting for retention policy compliance shall be implemented to ensure ongoing adherence.
- **Integration Management**: Retention systems shall be ensured to integrate properly with applications and cloud services for seamless operation.

4.3 Development Team

- **Application Lifecycle**: Data retention and disposal logic shall be built into application design and development to ensure policy compliance.
- **Database Management**: Automated database cleanup, archival, and retention procedures shall be implemented to manage data lifecycle.
- **Testing and Validation**: Data lifecycle functionality shall be tested during application development and deployment to verify proper operation.
- **Documentation**: Application-level retention and disposal implementations shall be documented for maintenance and compliance purposes.
- **Performance Optimization**: Retention processes shall be ensured not to negatively impact application performance through proper design.

4.4 DevOps Team

- **Infrastructure Automation**: Infrastructure-level retention and disposal processes shall be automated to ensure consistent policy implementation.
- **Backup Management**: Automated backup retention and disposal through cloud services shall be configured to manage backup lifecycle.
- **Environment Management**: Automated cleanup of development and staging environments shall be implemented to maintain operational efficiency.

- **Cost Optimization**: Storage costs related to data retention policies shall be monitored and optimized for financial efficiency.
- **Deployment Integration**: Retention configurations shall be ensured to be part of automated deployment processes for consistent implementation.

4.5 Legal Team

- **Retention Requirements**: Minimum retention periods based on regulatory and business requirements shall be defined to ensure compliance.
- **Legal Hold Requests**: Legal hold procedures shall be initiated and coordinated with Security Officer for technical implementation.
- **Regulatory Compliance**: Retention practices shall be ensured to meet evolving legal and regulatory requirements through ongoing review.
- **Disposal Authorization**: Disposal of data when legal hold requirements are lifted shall be approved by authorized legal personnel.
- **Contract Terms**: Cloud provider and vendor disposal terms in service agreements shall be reviewed for compliance assurance.

4.6 Compliance Team

- **Regulatory Mapping**: Retention requirements to specific regulatory frameworks (HIPAA, HITRUST, SOC 2) shall be mapped to ensure comprehensive compliance.
- **Audit Support**: Automated retention reports and evidence for internal and external audits shall be provided for compliance verification.
- **Policy Updates**: Policy updates based on regulatory changes or compliance findings shall be recommended to maintain current compliance.
- **Risk Assessment**: Risks related to automated retention and disposal processes shall be assessed to identify potential compliance issues.
- **Training Coordination**: Training on retention requirements for relevant team members shall be coordinated to ensure proper implementation.

5. Standards Compliance

See Annex: Control Mapping

6. Definitions

See Annex: Glossary

7. Related Policies and Procedures

This policy shall be implemented in conjunction with the following organizational policies:

- **Data Classification and Handling Policy (SEC-POL-001)**: Defines data sensitivity levels for retention classification
- **Encryption and Key Management Policy (OP-POL-001)**: Addresses cryptographic erasure and key lifecycle for disposal
- **Infrastructure Security Policy (ENG-POL-003)**: Covers cloud infrastructure retention and disposal capabilities
- **Incident Response Policy (SEC-POL-006)**: Addresses data preservation during security incidents
- **Business Continuity and Disaster Recovery Policy (RES-POL-001)**: Covers backup retention and recovery requirements
- **Supporting Procedures:**
- **Automated Data Lifecycle Implementation Procedure (OP-PROC-004)**: Technical implementation of automated retention and disposal
- **Legal Hold Management Procedure (OP-PROC-005)**: Streamlined legal hold procedures for technical teams
- **Cloud Data Lifecycle Configuration Procedure**: Configuration of cloud provider retention services

Workforce 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 shall 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

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Human Resources Department	Owns, reviews, and updates this policy annually. Manages screening, onboarding, termination processes, and administers the sanction policy with management.
Security Officer / Team	Advises on security aspects of HR processes, including background checks and termination procedures. Participates in investigations of security policy violations.
Managers	Ensures direct reports complete required security training, promptly notifies HR of terminations, and participates in sanction enforcement.
All Workforce Members	Comply with all information security policies and report suspected 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 shall 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 shall 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

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

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.

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 mandates 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 mandated 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 mandated. Access is denied until the device meets all security mandates.

5. Standards Compliance

See Annex: Control Mapping

6. Artifact(s)

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

7. Definitions

See Annex: Glossary

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 shall 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 mandated 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

See Annex: Control Mapping

6. Artifact(s)

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

7. Definitions

See Annex: Glossary

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 mandated 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 required.
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

See Annex: Control Mapping

6. Artifact(s)

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

7. Definitions

See Annex: Glossary

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.

Role	Responsibility
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

See Annex: Control Mapping

6. Artifact(s)

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

7. Definitions

See Annex: Glossary

8. Responsibilities

Role	Responsibility
Legal Team	Responsible for identifying the need for a legal hold, issuing notices, tracking compliance, and releasing the hold.
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 mandated 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 mandates for adverse action.
7	Human Resources (HR)	Documents the completed background check in the candidate's confidential personnel file.

5. Standards Compliance

See Annex: Control Mapping

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

See Annex: Glossary

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

See Annex: Control Mapping

6. Artifact(s)

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

7. Definitions

See Annex: Glossary

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 shall 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

See Annex: Control Mapping

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

See Annex: Glossary

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.

Role	Responsibility
Human Resources (HR)	Responsible for ensuring the sanction process is fair, consistent, and legally compliant, and for maintaining official records.

Incident Response Framework and Team Management Policy (RES-POL-001)

1. Objective

The objective of this policy is to establish the foundational framework and team management structure for **[Company Name]**'s incident response program. This policy defines the overall incident response lifecycle, establishes incident classification criteria, creates the organizational structure for incident response team management, and ensures post-incident learning and improvement processes. By implementing a comprehensive incident response framework with clearly defined roles, responsibilities, and governance structures, **[Company Name]** ensures coordinated and effective response to security incidents while protecting electronic Protected Health Information (ePHI), maintaining regulatory compliance with HIPAA, HITECH, and SOC 2 requirements, and enabling continuous improvement of security capabilities.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, third parties, and business associates involved in incident response planning, team management, or improvement activities. It encompasses the governance structure for all types of security incidents including data breaches, malware infections, unauthorized access, denial of service attacks, and physical security breaches. This policy establishes the framework that is implemented through the Security Event Detection and Monitoring Policy (RES-POL-003) and Incident Communication and Regulatory Compliance Policy (RES-POL-004), covering all information systems, applications, networks, devices, and data owned, operated, or managed by **[Company Name]**.

3. Policy

[Company Name] shall maintain a comprehensive incident response framework that establishes clear governance structures, team management processes, and continuous improvement mechanisms to ensure effective coordination of all incident response activities across the organization, implemented through specialized policies for detection and monitoring (RES-POL-003) and communication and compliance (RES-POL-004).

3.1 Incident Response Framework

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

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) shall be performed to maintain current readiness.
  - Establishment and maintenance of a designated Incident Response Team (IRT) with clearly defined roles and responsibilities shall be implemented.
  - Annual training and simulation exercises (e.g., tabletop exercises) for the IRT shall be conducted to ensure readiness, with outcomes documented for improvement tracking.
  - Deployment and maintenance of tools and technologies mandated for incident detection, analysis, and response shall be performed.
  - Maintenance of secure, out-of-band communication channels for the IRT shall be ensured for emergency communications.
  - At least annual testing of incident response capabilities shall be conducted, with results documented and used to drive improvements.
- **2. Detection and Analysis:**
  - Continuous monitoring of information systems to detect security events shall be implemented and maintained.
  - Initial triage of detected events to determine if a potential incident has occurred shall be performed promptly.
  - Formal declaration of an incident and activation of the Incident Response Team (IRT) shall be executed according to established procedures.
  - Initial impact and severity assessment to classify the incident according to the criteria in section 3.1.2 shall be completed.
  - Establishment of a secure repository for evidence collection and chain of custody documentation shall be performed.
  - Prioritization of response activities based on the incident classification shall be imple-

mented.

- **3. Containment, Eradication, and Recovery:**
  - Execution of containment strategies to prevent the incident from spreading and to minimize further damage shall be performed immediately.
  - Identification of the root cause and all affected systems shall be completed through systematic investigation.
  - Eradication of the threat (e.g., removing malware, disabling breached accounts, patching vulnerabilities) shall be performed.
  - Systematic recovery of affected systems and data from trusted sources shall be executed.
  - Validation that systems are clean and secure before returning them to production shall be performed.
  - Enhanced monitoring of recovered systems to ensure the threat has been fully removed shall be implemented.
- **4. Post-Incident Activity:**
  - Incident documentation and reporting shall be completed according to organizational standards.
  - Lessons learned analysis and improvement recommendations shall be developed and implemented.
  - Incident response plan updates shall be performed based on lessons learned.
  - Stakeholder communication and follow-up shall be conducted as required.
  - Legal and regulatory compliance activities shall be completed according to applicable requirements.

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 shall be classified as Critical.
  - Active compromise of critical systems affecting business operations shall be classified as Critical.
  - Widespread malware infection or ransomware attack shall be classified as Critical.
  - Suspected nation-state or advanced persistent threat (APT) activity shall be classified as Critical.

  - Physical security breach affecting critical assets shall be classified as Critical.
  - Response Time: Immediate response shall be required (within 15 minutes).
- **High (P2) - Urgent Response Required:**
  - Unauthorized access to sensitive systems or data shall be classified as High.
  - Malware infection on critical systems shall be classified as High.
  - Denial of service attacks affecting business operations shall be classified as High.
  - Suspected insider threat activity shall be classified as High.
  - Social engineering attacks targeting executives or privileged users shall be classified as High.
  - Response Time: Response shall be required within 1 hour.
- **Medium (P3) - Standard Response Required:**
  - Unsuccessful attack attempts against critical systems shall be classified as Medium.
  - Malware infection on non-critical systems shall be classified as Medium.
  - Policy violations with potential security impact shall be classified as Medium.
  - Suspicious network activity or anomalous behavior shall be classified as Medium.
  - Physical security violations in non-critical areas shall be classified as Medium.
  - Response Time: Response shall be required within 4 hours.
- **Low (P4) - Routine Response Required:**
  - Security policy violations without immediate risk shall be classified as Low.
  - Failed login attempts within normal thresholds shall be classified as Low.
  - Spam or phishing emails reported by users shall be classified as Low.
  - Minor physical security issues shall be classified as Low.
  - Security awareness training opportunities shall be classified as Low.
  - Response Time: Response shall be required 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 shall be maintained.

  - Communication with executive leadership and external stakeholders shall be performed.
  - Resource allocation and escalation decisions shall be made as required.
  - Post-incident review and improvement oversight shall be provided.
- **Security Analyst:**
  - Technical investigation and analysis shall be conducted.
  - Evidence collection and preservation shall be performed.
  - Malware analysis and threat intelligence gathering shall be executed.
  - System forensics and artifact examination shall be performed.
- **System Administrator:**
  - System containment and isolation procedures shall be executed.
  - System restoration and recovery activities shall be performed.
  - Network security controls implementation shall be conducted.
  - Infrastructure monitoring and maintenance shall be provided.
- **Privacy Officer:**
  - HIPAA breach assessment and notification requirements shall be managed.
  - Regulatory compliance coordination shall be performed.
  - Patient notification and communication shall be conducted as required.
  - Risk assessment for privacy violations shall be performed.
- **Legal Counsel:**
  - Legal implications assessment and guidance shall be provided.
  - Law enforcement coordination and communication shall be managed.
  - Litigation hold and evidence preservation requirements shall be addressed.
  - Regulatory notification and compliance support shall be provided.
- **Communications Lead:**
  - Internal and external communication coordination shall be performed.
  - Media relations and public communications shall be managed.
  - Customer and stakeholder notification shall be conducted.
  - Crisis communication management shall be provided.

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 shall be engaged as needed.
- Facilities manager for physical security incidents shall be involved when required.

- Third-party forensics and investigation specialists shall be engaged for complex incidents.
- Public relations and crisis communication experts shall be involved for high-visibility incidents.
- External legal counsel and regulatory specialists shall be engaged as circumstances require.
- Business unit leaders and system owners shall be involved based on affected systems and operations.

3.3 Security Event Detection and Monitoring

All security event detection, monitoring, and initial reporting activities shall be implemented as defined in the Security Event Detection and Monitoring Policy (RES-POL-003). This includes automated detection systems, manual observation methods, event reporting procedures, and triage processes that determine when incident response activities should be activated.

3.4 Incident Response Procedures and Compliance

All incident response procedures, stakeholder communication, and regulatory compliance activities shall be implemented as defined in the Incident Communication and Regulatory Compliance Policy (RES-POL-004). This includes standardized response procedures, containment and recovery activities, HIPAA breach notification requirements, and comprehensive communication protocols with internal and external stakeholders.

3.5 Post-Incident Activities and Organizational Learning

Comprehensive post-incident activities shall ensure organizational learning and continuous improvement of the incident response framework.

3.7.1 Incident Documentation

- **Incident Report Contents:**
  - Complete timeline of incident detection, response, and recovery shall be documented.
  - Root cause analysis and contributing factors shall be identified and documented.
  - Impact assessment including affected systems and data shall be completed.
  - Response effectiveness evaluation and lessons learned shall be documented.
  - Recommendations for security improvements and process enhancements shall be provided.

3.7.2 Lessons Learned and Improvement

- **Post-Incident Review:**
  - Formal review meeting within **[Timeframe, e.g., 2 weeks]** of incident closure shall be conducted.
  - Analysis of response effectiveness and areas for improvement shall be performed.
  - Review of incident response plan adequacy and updates needed shall be completed.
  - Evaluation of team performance and training requirements shall be conducted.
  - Assessment of detection capabilities and monitoring effectiveness shall be performed.
- **Process Improvement:**
  - Incident response procedures shall be updated based on lessons learned.
  - Additional security controls to prevent similar incidents shall be implemented.
  - Monitoring and detection capabilities shall be enhanced as needed.
  - Training and awareness programs shall be improved based on findings.
  - Business continuity and disaster recovery plans shall be updated as required.

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Security Officer	Incident response framework and policies shall be developed, incident response team structure shall be maintained, incident response program shall be overseen, and compliance with regulatory requirements shall be ensured.

Role	Responsibility
Incident Commander	Incident response activities shall be led, team efforts shall be coordinated, critical response decisions shall be made, stakeholder communication shall be managed, and effective incident management shall be ensured.
IT Security Team	Incident response framework implementation shall be supported, technical expertise to incident response team shall be provided, incident response tools and capabilities shall be maintained, and team training shall be participated in.
Privacy Officer	Coordination with incident response team on privacy-related incidents shall be performed, HIPAA compliance activities shall be supported, and incident response training and exercises shall be participated in.
Legal Counsel	Legal guidance for incident response framework shall be provided, incident response team during legal matters shall be supported, and incident response planning and training shall be participated in.
Executive Leadership	Strategic guidance and resources for incident response program shall be provided, incident response team authority shall be supported, and organizational commitment to incident response capabilities shall be ensured.

Role	Responsibility
Human Resources	Incident response team with workforce-related incidents shall be supported, coordination with legal team on personnel matters shall be performed, and incident response training programs shall be participated in.
All Workforce Members	Incident response procedures shall be understood, incident response training shall be participated in, incident response activities shall be supported when requested, and incident response policies and procedures shall be followed.

Business Continuity Management Policy (RES-POL-002)

1. Objective

The objective of this policy is to establish a comprehensive business continuity management framework for **[Company Name]** that ensures the continuation of critical business operations and essential services during disruptions. This policy focuses on business process continuity, stakeholder communication, alternative operating procedures, and organizational resilience while technical disaster recovery capabilities are addressed in the Disaster Recovery and Technical Operations Policy (RES-POL-005). By implementing structured business continuity capabilities including business impact analysis, emergency response procedures, and alternative operations, **[Company Name]** maintains essential service delivery to patients and customers, protects electronic Protected Health Information (ePHI), meets regulatory obligations under HIPAA, HITECH, and SOC 2, and minimizes business impact during various types of disruptions.

2. Scope

This policy applies to all **[Company Name]** workforce members, business units, facilities, business processes, and third-party service providers that support critical business operations. It encompasses business continuity planning and response for all types of disruptions including natural disasters, pandemics, civil emergencies, supply chain disruptions, workforce shortages, and other events that could impact business operations. This policy covers business process continuity, stakeholder management, emergency communications, alternative work arrangements, and vendor continuity management, while technical system recovery is addressed through the Disaster Recovery and Technical Operations Policy (RES-POL-005).

3. Policy

[Company Name] shall maintain comprehensive business continuity management capabilities that enable the organization to continue critical business operations during disruptions through alternative procedures, emergency response coordination, and stakeholder management, with technical system recovery addressed through the Disaster Recovery and Technical Operations Policy (RES-POL-005).

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 shall be the highest priority in all emergency situations.
  - Emergency evacuation and safety procedures shall take precedence over business operations.
  - Clear communication channels and emergency coordination procedures shall be maintained at all times.
- **Essential Services Continuity:**
  - Critical business functions shall be identified and prioritized for continuity during disruptions.
  - Minimum service levels shall be defined for essential operations to ensure baseline service delivery.
  - Alternative methods and resources shall be available to maintain critical services during emergencies.
  - Patient care and safety functions shall 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 according to regulatory requirements.
  - 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 throughout disruptions.
  - Multiple communication channels shall be available for redundancy to ensure reliable communications.

  - Regular updates shall be provided during extended disruptions to maintain stakeholder awareness.
  - Post-incident communication shall address lessons learned and improvements implemented.

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, shall 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 Technical Disaster Recovery Integration

All technical disaster recovery planning, data backup and recovery systems, IT infrastructure recovery, and system restoration procedures shall be implemented as defined in the Disaster Recovery and Technical Operations Policy (RES-POL-005). This includes comprehensive IT disaster recovery strategy, backup systems management, system recovery procedures, and technical performance monitoring that supports the business continuity requirements defined in this policy.

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

3.6 Business Recovery and Restoration

Systematic business recovery procedures shall guide the restoration of normal business operations following emergency situations, with technical system recovery coordinated through RES-POL-005.

3.6.1 Business Recovery Procedures

- **Operational Damage Assessment:**
  - Comprehensive assessment of facilities, equipment, and business capabilities
  - Safety inspection and clearance for facility reoccupancy and operations
  - Business process and service capability evaluation and validation
  - Workforce accountability and fitness for duty assessment
  - Vendor and supply chain impact assessment and alternative sourcing
- **Phased Business Recovery Approach:**
  - **Phase 1**: Life safety and immediate emergency response coordination
  - **Phase 2**: Critical business process restoration and essential service resumption
  - **Phase 3**: Full operational capability restoration and normal service levels
  - **Phase 4**: Normal operations resumption and lessons learned integration
  - Business process dependencies mapping and coordinated restoration

3.6.2 Post-Incident Review and Improvement

Following any activation of the business continuity plan, a formal post-incident review shall be conducted to ensure organizational learning and improvement.

- **Comprehensive Business Impact Analysis:**
  - Formal Post-Incident Report detailing business impact, response effectiveness, and operational lessons learned
  - Business process performance analysis and service level achievement assessment
  - Financial impact assessment and cost analysis of business disruption and response
  - Stakeholder feedback collection and satisfaction analysis
  - Regulatory compliance validation and business requirement fulfillment
- **Business Process Improvement Implementation:**
  - All business findings and lessons learned shall be documented and prioritized
  - Business improvement action items shall be assigned owners and due dates and tracked to completion
  - Business continuity plans and procedures shall be updated based on approved improvements
  - Business training programs and workforce development based on lessons learned
  - Vendor relationships and service agreements modifications and improvements
  - Integration of business process improvements with technical disaster recovery enhancements

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

The following roles and responsibilities apply specifically to business continuity management functions, with technical disaster recovery responsibilities defined in RES-POL-005.

Role	Responsibility
Executive Leadership	Provide strategic direction and resources for business continuity program, approve business operational plans and resource allocation, and communicate with external stakeholders during business emergencies.
Business Continuity Manager	Develop and maintain business continuity plans, coordinate business impact analysis and testing, manage business emergency response activities, and ensure business operational compliance.
Business Unit Leaders	Implement business unit specific continuity plans, coordinate business process restoration, manage departmental business communications, and support workforce business needs.
Emergency Operations Team	Coordinate business emergency response activities, manage emergency operations center for business functions, communicate with business stakeholders, and ensure workforce safety and business operations.
Human Resources	Manage workforce accountability and business communications, coordinate with families, support workforce welfare during business disruptions, and maintain emergency contact information.
Legal and Compliance	Ensure regulatory compliance during business emergencies, manage legal implications of business incidents, coordinate with business authorities, and handle business insurance claims.

Role	Responsibility
Communications Team	Manage external business communications, coordinate with media and customers, handle business crisis communications, and maintain business stakeholder relationships.
Facilities Management	Maintain business facility emergency systems, coordinate with emergency services for business facilities, assess business facility damage, and manage alternate business facility arrangements.
All Workforce Members	Follow business emergency procedures, participate in business continuity training and drills, report business safety concerns, and support business recovery efforts as assigned.

Security Event Detection and Monitoring Policy (RES-POL-003)

1. Objective

The objective of this policy is to establish comprehensive requirements for the detection, monitoring, and initial reporting of security events and incidents within **[Company Name]**'s information systems and infrastructure. This policy ensures that security events are identified promptly through both automated and manual detection methods, properly reported through established channels, and appropriately triaged to determine if incident response procedures should be activated. By implementing robust detection and monitoring capabilities, **[Company Name]** can minimize the time between incident occurrence and detection, reducing potential impact on operations and 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, contractors, third parties, and business associates who may detect, observe, or report potential security events or incidents. It encompasses all information systems, applications, networks, devices, and infrastructure components owned, operated, or managed by **[Company Name]**, including cloud services, mobile devices, and third-party systems that process company data. This policy covers all detection methods including automated security tools, manual observation, and workforce reporting, as well as the initial triage and reporting procedures that determine whether formal incident response should be activated.

3. Policy

[Company Name] shall implement comprehensive security event detection and monitoring capabilities across all information systems and infrastructure components to ensure early identification of potential security incidents and enable rapid activation of incident response procedures as defined in the Incident Response Framework & Team Management Policy (RES-POL-001).

3.1 Security Event Detection Framework

Multiple detection methods shall be employed to identify potential security incidents as early as possible across all organizational systems and infrastructure.

3.1.1 Automated Detection Systems

- **Security Information and Event Management (SIEM):**
  - Centralized log collection and correlation from all critical systems
  - Real-time analysis and alerting for security events and anomalies
  - Custom rules and signatures for organization-specific threats
  - Integration with threat intelligence feeds for enhanced detection
  - Automated escalation procedures for high-priority alerts
- **Intrusion Detection and Prevention Systems (IDS/IPS):**
  - Network-based detection for suspicious traffic patterns and known attack signatures
  - Host-based detection for system-level compromises and malicious activity
  - Behavioral analysis and machine learning for advanced threat detection
  - Automated blocking and containment for confirmed threats
  - Integration with network security infrastructure and response systems
- **Endpoint Detection and Response (EDR):**
  - Continuous monitoring of all endpoints including workstations, servers, and mobile devices
  - Real-time detection of malware, suspicious processes, and unauthorized changes
  - Behavioral analysis and anomaly detection for advanced persistent threats
  - Automated isolation and containment capabilities for compromised endpoints
  - Forensic data collection and analysis for incident investigation
- **Data Loss Prevention (DLP):**
  - Monitoring of data access, transmission, and storage activities
  - Detection of unauthorized data exfiltration attempts and policy violations
  - Content inspection and classification for sensitive data protection
  - Integration with email, web, and network security systems
  - Automated blocking and quarantine of suspicious data activities
- **Additional Automated Detection Tools:**
  - Antivirus and anti-malware system notifications and alerts
  - Network anomaly detection and behavioral analysis systems
  - File integrity monitoring and system change detection tools
  - Cloud security posture management (CSPM) and configuration monitoring
  - Application security monitoring and runtime protection systems

3.1.2 Detection Coverage Requirements

- **System Coverage:**
  - All production systems processing ePHI or Confidential data shall have continuous monitoring
  - Critical infrastructure components shall have redundant detection capabilities
  - Cloud services shall be monitored through native and third-party security tools
  - Network perimeter and internal segments shall have comprehensive coverage
  - Remote access and VPN connections shall be continuously monitored
- **Event Categories:**
  - Unauthorized access attempts and authentication failures
  - Privilege escalation and administrative access activities
  - Data access violations and unauthorized data movement
  - Malware infections and suspicious file activities
  - Network intrusions and communication anomalies
  - System configuration changes and unauthorized modifications
  - Performance anomalies that may indicate security compromise

3.2 Manual Detection and Observation

Workforce members shall be trained and empowered to identify and report potential security events through observation and awareness.

3.2.1 Workforce-Based Detection

- **Security Awareness and Training:**
  - Annual security awareness training including incident recognition and reporting
  - Regular updates on current threat landscape and attack techniques
  - Specialized training for IT and security personnel on advanced threat detection
  - Simulated phishing and social engineering exercises to test detection capabilities
  - Recognition and incentive programs for effective security event reporting
- **Observation-Based Detection Methods:**
  - Workforce member reports of suspicious emails, phone calls, or social engineering attempts
  - System administrator observation of anomalous system behavior or performance
  - Physical security observations including unauthorized access attempts or suspicious indi-

viduals
  - Customer or partner reports of potential compromise or suspicious communications
  - Third-party security service provider notifications and threat intelligence

3.2.2 Proactive Security Monitoring

- **Security Team Activities:**
  - Proactive threat hunting and security monitoring activities
  - Regular analysis of security logs and system behavior patterns
  - Vulnerability assessment and penetration testing activities
  - Dark web monitoring for indicators of organizational compromise
  - Threat intelligence research and analysis for organization-specific risks
- **System Administrator Monitoring:**
  - Regular review of system logs and security events
  - Monitoring of system performance and capacity metrics for anomalies
  - Configuration change monitoring and unauthorized modification detection
  - User activity monitoring and access pattern analysis
  - Integration with automated tools for manual validation and investigation

3.3 Security Event Reporting and Triage

Comprehensive reporting procedures shall ensure that all potential security events are properly documented and triaged for appropriate response.

3.3.1 Incident Reporting Channels

- **Primary Reporting Methods:**
  - 24/7 security hotline: **[Phone Number]** for immediate verbal reporting
  - Email reporting: **[Email Address]** for detailed written reports
  - Online incident reporting portal: **[URL]** for structured reporting and tracking
  - In-person reporting to Security Officer, IT Management, or designated incident response personnel
- **Reporting Channel Requirements:**
  - Multiple redundant channels available 24/7 for continuous availability
  - Secure communication methods to protect sensitive incident information
  - Integration with incident tracking and management systems

  - Automated acknowledgment and case number assignment for all reports
  - Escalation procedures for high-priority or urgent security events

3.3.2 Reporting Requirements and Procedures

- **Mandatory Reporting Timelines:**
  - All suspected security incidents shall be reported within **[Timeframe, e.g., 2 hours]** of discovery
  - Initial reports may be verbal with written follow-up mandated within **[Timeframe, e.g., 24 hours]**
  - Critical incidents involving ePHI or system compromise require immediate reporting
  - Workforce members shall not delay reporting while gathering additional information
  - No investigation or remediation attempts shall be made prior to reporting
- **Report Content Requirements:**
  - Date, time, and method of incident discovery
  - Description of observed events, symptoms, or indicators
  - Affected systems, applications, or data categories
  - Potential impact assessment and scope of compromise
  - Actions taken prior to reporting (if any)
  - Contact information for the reporting individual
  - Any relevant evidence or supporting documentation

3.3.3 Event Triage and Classification

- **Initial Triage Process:**
  - Immediate assessment of reported events to determine validity and priority
  - Classification of events according to incident severity criteria
  - Determination of whether formal incident response procedures should be activated
  - Assignment of incident response team members based on event type and severity
  - Coordination with Incident Response Framework & Team Management Policy (RES-POL-001)
- **Event Classification Criteria:**
  - **Critical:** Events involving ePHI compromise, widespread system compromise, or immediate threat to operations
  - **High:** Events involving Confidential data access, targeted attacks, or significant system

compromise
  - **Medium:** Events involving suspicious activity, minor system compromise, or potential policy violations
  - **Low:** Events involving general security alerts, routine monitoring findings, or minor security issues
  - **Informational:** Events requiring documentation but not requiring active response

3.4 Detection System Management and Maintenance

Continuous management and optimization of detection systems shall ensure effective coverage and minimal false positives.

3.4.1 System Configuration and Tuning

- **Detection Rule Management:**
  - Regular review and optimization of detection rules and signatures
  - Custom rule development for organization-specific threats and environments
  - False positive analysis and rule tuning to improve detection accuracy
  - Integration of threat intelligence feeds for enhanced detection capabilities
  - Documentation of all custom rules and configuration changes
- **Performance Monitoring:**
  - Continuous monitoring of detection system performance and availability
  - Capacity planning and resource allocation for detection infrastructure
  - Redundancy and failover capabilities for critical detection systems
  - Regular testing of detection capabilities and response procedures
  - Integration with overall system monitoring and alerting infrastructure

3.4.2 Continuous Improvement

- **Detection Effectiveness Assessment:**
  - Regular analysis of detection system effectiveness and coverage gaps
  - Metrics tracking including mean time to detection (MTTD) and false positive rates
  - Comparison with industry benchmarks and best practices
  - Integration of lessons learned from incident response activities
  - Continuous improvement based on emerging threats and attack techniques
- **Technology Updates and Enhancement:**

- Regular updates to detection system software and signatures
- Evaluation and integration of new detection technologies and capabilities
- Coordination with vendor support and threat intelligence providers
- Testing and validation of system updates in non-production environments
- Documentation of all changes and their impact on detection capabilities

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Security Officer	Develop detection and monitoring policies, oversee detection system implementation, coordinate with incident response team, and ensure compliance with regulatory requirements.
IT Security Team	Implement and manage detection systems, analyze security events and alerts, perform threat hunting activities, and coordinate event triage and escalation.
Security Analysts	Monitor security events and alerts, perform initial triage and investigation, escalate incidents to response team, and maintain detection system rules and configurations.
System Administrators	Monitor system performance and behavior, report suspicious activities, support detection system implementation, and coordinate with security team on event investigation.
SOC Team	Provide 24/7 monitoring and analysis of security events, perform initial incident triage, coordinate escalation procedures, and maintain situational awareness of security posture.

Role	Responsibility
Network Administrators	Monitor network traffic and behavior, implement network-based detection systems, support security event investigation, and coordinate network-related incident response activities.
All Workforce Members	Report suspected security events promptly, participate in security awareness training, follow established reporting procedures, and cooperate with security event investigations.

Incident Communication and Regulatory Compliance Policy (RES-POL-004)

1. Objective

The objective of this policy is to establish comprehensive requirements for incident response procedures, communication protocols, and regulatory compliance activities during security incidents at **[Company Name]**. This policy ensures that security incidents are handled through standardized response procedures, appropriate stakeholders are notified in a timely manner, and all regulatory and legal obligations are met throughout the incident lifecycle. By implementing structured communication and compliance processes, **[Company Name]** maintains transparency with stakeholders, meets regulatory notification requirements, and preserves legal and regulatory standing while effectively managing incident response activities in coordination with the Incident Response Framework & Team Management Policy (RES-POL-001).

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, third parties, and business associates involved in incident response activities, stakeholder communications, or regulatory compliance processes. It encompasses all types of security incidents including data breaches, system compromises, malware infections, and other events that require formal response procedures. This policy covers communication with internal stakeholders, external parties including customers and vendors, regulatory bodies, law enforcement, and the media, as well as all regulatory notification and compliance requirements under HIPAA, HITECH, state data breach laws, and other applicable regulations.

3. Policy

[Company Name] shall implement comprehensive incident response procedures and communication protocols that ensure effective incident management, appropriate stakeholder notification, and full compliance with all regulatory and legal requirements throughout the incident response lifecycle.

3.1 Incident Response Procedures

Standardized procedures shall be followed for responding to different types of security incidents once they have been detected and triaged through the Security Event Detection and Monitoring Policy (RES-POL-003).

3.1.1 Initial Response Procedures

- **Incident Verification and Classification:**
  - Confirm that a security incident has actually occurred based on detection and monitoring activities
  - Gather comprehensive information about the scope, impact, and affected systems
  - Classify the incident according to established severity criteria from RES-POL-001
  - Activate appropriate incident response procedures based on classification
  - Notify relevant incident response team members as defined in RES-POL-001
- **Evidence Preservation and Documentation:**
  - Preserve all relevant digital and physical evidence in its original state
  - Document all actions taken, decisions made, and timeline of events
  - Maintain strict chain of custody procedures for all evidence
  - Take system snapshots or forensic images before making changes
  - Collect network traffic captures, log files, and other relevant artifacts
  - Establish secure evidence repository with access controls and audit logging

3.1.2 Containment Procedures

- **Short-term Containment:**
  - Isolate affected systems from the network to prevent lateral movement
  - Disable compromised user accounts and force password changes
  - Block malicious IP addresses, domains, and communication channels
  - Implement temporary firewall rules and access controls to prevent spread
  - Preserve system state and evidence while implementing containment measures
  - Coordinate containment activities with system owners and administrators
- **Long-term Containment:**
  - Rebuild compromised systems from known clean backups or baseline images
  - Implement enhanced monitoring and logging on affected and related systems
  - Apply all relevant security patches and configuration hardening measures

  - Conduct comprehensive security validation before system restoration
  - Monitor for signs of persistent compromise or reinfection
  - Update security controls and detection capabilities based on incident findings

3.1.3 Eradication and Recovery Procedures

- **Threat Eradication:**
  - Remove all malware, malicious artifacts, and unauthorized access from systems
  - Close security vulnerabilities and configuration weaknesses that enabled the incident
  - Improve security controls and detection capabilities to prevent recurrence
  - Validate that all traces of compromise have been completely eliminated
  - Conduct comprehensive security assessment of all remediated systems
  - Document all eradication activities and validation procedures
- **System Recovery and Restoration:**
  - Restore systems and data from verified clean backups
  - Implement additional security monitoring and protective controls
  - Gradually restore full system functionality with continuous monitoring
  - Conduct comprehensive user acceptance testing and functionality validation
  - Monitor systems continuously for signs of compromise or instability
  - Coordinate recovery activities with business units and stakeholders

3.2 Regulatory and Legal Compliance

Incident response procedures shall ensure compliance with all applicable legal and regulatory mandates throughout the incident lifecycle.

3.2.1 HIPAA Breach Notification Requirements

- **Breach Assessment and Determination:**
  - Conduct formal assessment to determine whether incident constitutes a HIPAA breach
  - Evaluate the probability that electronic Protected Health Information (ePHI) has been compromised
  - Assess the risk of harm to affected individuals based on incident specifics
  - Document the breach assessment decision, rationale, and supporting evidence
  - Coordinate assessment with Privacy Officer, Legal Counsel, and incident response team
- **HIPAA Notification Timelines and Requirements:**

  - **Individual Notification:** Within **60 days** of breach discovery for all affected individuals
  - **HHS Notification:** Within **60 days** of breach discovery through HHS breach notification portal
  - **Media Notification:** Within **60 days** if breach affects **500 or more individuals** in a state/jurisdiction
  - **Immediate HHS Notification:** Within **60 days** if breach affects **500 or more individuals** nationwide
  - **Annual Summary:** Submit summary of smaller breaches (less than 500 individuals) annually to HHS
- **Notification Content Requirements:**
  - Description of what happened and when the breach occurred
  - Types of information that were involved in the breach
  - Steps individuals should take to protect themselves from potential harm
  - What **[Company Name]** is doing to investigate, mitigate, and prevent future occurrences
  - Contact information for individuals to ask questions or get additional information

3.2.2 Additional Regulatory and Legal Requirements

- **State Data Breach Notification Laws:**
  - Identify applicable state notification requirements based on affected individual residency
  - Comply with varying state timelines, notification methods, and content requirements
  - Coordinate notifications with state attorneys general as required by state law
  - Maintain documentation of all state notification activities and compliance
- **Federal and Industry-Specific Requirements:**
  - **SEC Notification:** Material cybersecurity incidents for public companies (if applicable)
  - **Financial Industry Notifications:** Banking, credit, or financial service requirements (if applicable)
  - **Professional Licensing Board Notifications:** Healthcare or professional service requirements (if applicable)
  - **Insurance Carrier Notification:** Cyber insurance claim procedures and requirements
  - **Law Enforcement Coordination:** FBI, Secret Service, or other federal agency reporting as appropriate

3.2.3 Legal Hold and Evidence Management

- **Litigation Hold Procedures:**
  - Implement litigation hold for all relevant documents and electronic information
  - Preserve all incident-related communications, logs, and documentation
  - Coordinate with Legal Counsel on scope and duration of preservation requirements
  - Train incident response team on legal hold obligations and procedures
  - Document all preservation activities and ensure compliance with legal requirements
- **Law Enforcement Coordination:**
  - Coordinate with appropriate law enforcement agencies for criminal incidents
  - Provide evidence and support for law enforcement investigations
  - Balance operational recovery needs with law enforcement evidence preservation
  - Maintain chain of custody for evidence provided to law enforcement
  - Document all law enforcement interactions and coordination activities

3.3 Communication and Coordination

Effective communication shall be maintained with all stakeholders throughout the incident response process.

3.3.1 Internal Communications

- **Executive Leadership Reporting:**
  - Immediate notification to CEO and Executive Leadership for Critical and High severity incidents
  - Regular status updates throughout incident response with timeline and impact assessment
  - Final incident report with comprehensive analysis, lessons learned, and recommendations
  - Board of Directors notification for significant incidents affecting organizational reputation or compliance
  - Coordination with legal counsel on all executive communications
- **Workforce Communications:**
  - Information sharing on need-to-know basis to protect investigation integrity
  - General security awareness messages as appropriate to enhance organizational security posture

  - Post-incident training and awareness updates incorporating lessons learned
  - Recognition programs for effective incident reporting and response activities
  - Clear communication channels for questions and concerns from workforce members

3.3.2 External Communications

- **Customer and Client Communications:**
  - Timely notification of customers and clients potentially affected by security incidents
  - Clear, accurate explanation of incident impact and potential risks
  - Regular updates on investigation progress and remediation efforts
  - Dedicated communication channels and contact information for questions and concerns
  - Coordination with customer success and account management teams
- **Vendor and Business Associate Communications:**
  - Notification of business associates and vendors as required by contracts and regulations
  - Coordination with third-party service providers for incident response and recovery activities
  - Information sharing with industry partners and threat intelligence communities
  - Coordination with insurance carriers and coverage providers for claim processing
  - Vendor assistance coordination for specialized incident response services

3.3.3 Media and Public Communications

- **Media Relations:**
  - Designation of authorized spokesperson for all media interactions
  - Coordination with public relations team and external communications specialists
  - Preparation of consistent messaging and talking points for media inquiries
  - Proactive media outreach for significant incidents requiring public notification
  - Monitoring of media coverage and social media for accuracy and sentiment
- **Regulatory Communications:**
  - Formal notifications to regulatory bodies as required by law and regulation
  - Coordination with regulatory affairs team for ongoing compliance activities
  - Response to regulatory inquiries and investigation requests
  - Documentation of all regulatory communications and interactions
  - Legal counsel review of all regulatory communications before submission

3.4 Post-Incident Activities and Lessons Learned

Comprehensive post-incident activities shall ensure organizational learning, process improvement, and enhanced security posture.

3.4.1 Incident Documentation and Reporting

- **Comprehensive Incident Report Contents:**
  - Complete chronological timeline of incident detection, response, and recovery activities
  - Detailed root cause analysis and identification of all contributing factors
  - Comprehensive impact assessment including affected systems, data, and stakeholders
  - Evaluation of response effectiveness and identification of lessons learned
  - Specific recommendations for security improvements and process enhancements
  - Financial impact assessment and cost analysis of incident and response

3.4.2 Lessons Learned and Continuous Improvement

- **Post-Incident Review Process:**
  - Formal lessons learned meeting within **[Timeframe, e.g., 2 weeks]** of incident closure
  - Analysis of response effectiveness with focus on communication and compliance activities
  - Review of incident response plan adequacy and identification of needed updates
  - Evaluation of team performance and identification of additional training requirements
  - Assessment of detection capabilities and monitoring effectiveness for future improvements
- **Process and Security Improvement Implementation:**
  - Update incident response procedures based on lessons learned and best practices
  - Implement additional security controls to prevent similar incidents
  - Enhance monitoring and detection capabilities based on incident findings
  - Improve training and awareness programs incorporating new threats and techniques
  - Update business continuity and disaster recovery plans based on incident impact
  - Share lessons learned with industry peers and professional communities

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Incident Commander	Lead incident response activities, coordinate communication efforts, make critical response decisions, and ensure compliance with all regulatory requirements.
Privacy Officer	Assess HIPAA breach requirements, coordinate breach notifications, manage patient communications, ensure privacy compliance, and oversee regulatory notification activities.
Legal Counsel	Provide legal guidance throughout incident response, coordinate law enforcement relations, manage litigation holds, ensure regulatory compliance, and review external communications.
Communicati Team	Manage internal and external communications, coordinate media relations, support crisis communications, develop messaging, and maintain stakeholder relationships.
Security Officer	Oversee incident response procedures, ensure policy compliance, coordinate with regulatory bodies, manage incident documentation, and drive continuous improvement initiatives.
Compliance Team	Ensure regulatory notification compliance, coordinate with regulatory affairs, manage compliance documentation, support audit activities, and maintain regulatory relationships.
IT Security Team	Implement technical response procedures, conduct forensic analysis, coordinate system recovery, preserve evidence integrity, and support compliance activities.
Executive Leadership	Provide strategic guidance and resources, approve major response decisions, coordinate with board and stakeholders, and ensure organizational commitment to improvement.

Role	Responsibility
All Workforce Members	Follow incident response procedures, support communication efforts, cooperate with investigations, maintain confidentiality, and participate in post-incident improvement activities.

Disaster Recovery and Technical Operations Policy (RES-POL-005)

1. Objective

The objective of this policy is to establish comprehensive technical disaster recovery requirements for **[Company Name]**'s information systems, infrastructure, and technology operations. This policy ensures that critical IT systems and data can be rapidly restored following disasters, disruptions, or system failures while maintaining the integrity and availability of electronic Protected Health Information (ePHI) and other sensitive data. By implementing robust disaster recovery capabilities including data backup, system redundancy, and technical recovery procedures, **[Company Name]** minimizes technology-related business impact, ensures rapid restoration of IT services, and maintains compliance with HIPAA, HITECH, and SOC 2 technical safeguard requirements in coordination with the Business Continuity Management Policy (RES-POL-002).

2. Scope

This policy applies to all **[Company Name]** IT personnel, system administrators, cloud engineers, and third-party service providers involved in the design, implementation, operation, or maintenance of disaster recovery systems and procedures. It encompasses all information systems, applications, databases, infrastructure components, and technology assets that support critical business operations including production systems, development environments, network infrastructure, cloud services, and data storage systems. This policy covers technical recovery procedures for all types of disasters including natural disasters, cyber attacks, equipment failures, data corruption, and other events that could impact the availability or integrity of technology systems and data.

3. Policy

[Company Name] shall implement comprehensive technical disaster recovery capabilities that enable rapid restoration of IT systems and data following disasters or disruptions, ensuring minimal impact on business operations and maintaining the security and integrity of all technology assets and information.

3.1 Disaster Recovery Planning and Strategy

Comprehensive disaster recovery plans shall be developed for all critical information systems and infrastructure components to ensure rapid and effective technical recovery.

3.1.1 IT Disaster Recovery Strategy

- **Primary Data Center Protection:**
  - Redundant systems and infrastructure components with automatic failover capabilities
  - Uninterruptible Power Supply (UPS) systems with minimum **[Duration, e.g., 30 minutes]** runtime capacity
  - Backup generator systems with minimum **[Duration, e.g., 72 hours]** fuel supply and automatic transfer
  - Advanced fire suppression systems and comprehensive environmental monitoring
  - Physical security controls including access management and surveillance systems
  - Network redundancy with multiple internet service providers and diverse routing paths
- **Secondary Site Operations:**
  - Geographically separated backup data center located minimum **[Distance, e.g., 100+ miles]** from primary site
  - Real-time data replication for all critical systems and databases
  - Standby infrastructure capable of supporting minimum **[Percentage, e.g., 80%]** of production capacity
  - Alternative network connectivity and communication systems with redundant paths
  - Pre-positioned equipment and supplies for extended operations up to **[Duration, e.g., 30 days]**
  - Automated failover procedures for critical applications and services
- **Cloud-Based Recovery Infrastructure:**
  - Cloud infrastructure for scalable and elastic recovery capabilities
  - Hybrid cloud strategy combining on-premises and cloud resources for optimal resilience
  - Multi-cloud approach to avoid single vendor dependency and geographic concentration
  - Infrastructure-as-Code (IaC) templates for rapid environment provisioning
  - Automated failover and recovery procedures using cloud-native capabilities
  - Data sovereignty and regulatory compliance validation in all cloud environments

3.1.2 System Classification and Recovery Requirements

- **Critical Systems (Tier 1):**
  - Recovery Time Objective (RTO): **[Duration, e.g., 4 hours]** maximum downtime
  - Recovery Point Objective (RPO): **[Duration, e.g., 15 minutes]** maximum data loss
  - 24/7 monitoring and immediate response capabilities

  - Real-time replication and automated failover
  - Dedicated disaster recovery infrastructure and personnel
- **Important Systems (Tier 2):**
  - Recovery Time Objective (RTO): **[Duration, e.g., 24 hours]** maximum downtime
  - Recovery Point Objective (RPO): **[Duration, e.g., 1 hour]** maximum data loss
  - Business hours monitoring with 4-hour response time
  - Near-real-time replication and semi-automated recovery
  - Shared disaster recovery infrastructure with priority allocation
- **Standard Systems (Tier 3):**
  - Recovery Time Objective (RTO): **[Duration, e.g., 72 hours]** maximum downtime
  - Recovery Point Objective (RPO): **[Duration, e.g., 4 hours]** maximum data loss
  - Scheduled monitoring with next business day response
  - Daily backup and manual recovery procedures
  - Standard disaster recovery infrastructure and procedures

3.2 Data Backup and Recovery Systems

Comprehensive data backup and recovery systems shall ensure the protection and rapid restoration of all critical information and systems.

3.2.1 Backup Strategy and Implementation

- **3-2-1 Backup Rule Implementation:**
  - **3 copies** of all critical data maintained at all times
  - **2 different media types** for backup storage (disk, tape, cloud)
  - **1 offsite location** geographically separated from production systems
  - Additional air-gapped backup for ransomware protection and compliance
- **Backup Frequency and Retention:**
  - **Real-time replication** for Tier 1 critical systems and databases
  - **Hourly incremental backups** for Tier 2 important systems
  - **Daily full backups** for all production systems with synthetic full backup capabilities
  - **Weekly full system backups** with long-term retention for compliance
  - **Monthly archive backups** for historical data and regulatory compliance
  - **Retention policies** aligned with business requirements and regulatory mandates
- **Backup Encryption and Security:**

  - All backup data encrypted at rest using AES-256 or equivalent encryption
  - Encryption key management through dedicated key management systems
  - Backup data transmission encrypted using TLS 1.3 or equivalent protocols
  - Access controls and audit logging for all backup systems and operations
  - Backup media secured with physical and logical access controls

3.2.2 Backup Testing and Validation

- **Regular Backup Validation:**
  - **Daily automated validation** of backup completion and integrity
  - **Weekly restore testing** for critical system backups and databases
  - **Monthly comprehensive restore testing** for all backup systems
  - **Quarterly disaster recovery testing** with full system restoration
  - **Annual comprehensive validation** of all backup and recovery procedures
- **Backup Integrity and Monitoring:**
  - Automated backup monitoring and alerting for failures or anomalies
  - Backup integrity validation using checksums and hash verification
  - Regular analysis of backup performance metrics and trends
  - Automated notification of backup failures with immediate escalation
  - Documentation of all backup validation activities and results

3.3 System Recovery and Restoration Procedures

Systematic technical recovery procedures shall guide the restoration of IT systems and services following disasters or disruptions.

3.3.1 Recovery Activation and Procedures

- **Disaster Declaration and Activation:**
  - Formal disaster declaration process with clear activation criteria
  - Technical assessment of system impact and recovery requirements
  - Activation of appropriate recovery procedures based on system classification
  - Coordination with Business Continuity Management team as defined in RES-POL-002
  - Documentation of all activation decisions and technical assessments
- **Recovery Sequence and Prioritization:**
  - **Phase 1**: Critical infrastructure and network connectivity restoration

  - **Phase 2**: Core business systems and databases recovery
  - **Phase 3**: Supporting applications and services restoration
  - **Phase 4**: Complete system functionality and performance validation
  - Dependencies mapping and coordinated recovery of interconnected systems

3.3.2 Technical Recovery Procedures

- **Infrastructure Recovery:**
  - Network connectivity and communication systems restoration
  - Server and compute infrastructure recovery using automated procedures
  - Storage systems and database recovery with integrity validation
  - Security systems and monitoring infrastructure restoration
  - Load balancing and performance optimization configuration
- **Application and Data Recovery:**
  - Application restoration using automated deployment procedures
  - Database recovery with point-in-time restoration capabilities
  - Data integrity validation and consistency checking
  - Application configuration and customization restoration
  - User access and authentication systems recovery
- **Recovery Validation and Testing:**
  - Comprehensive system functionality testing and validation
  - Performance testing and capacity validation
  - Security controls validation and vulnerability assessment
  - User acceptance testing and business process validation
  - Documentation of all recovery activities and validation results

3.4 Cloud Disaster Recovery and Hybrid Operations

Specialized disaster recovery procedures shall address cloud-based systems and hybrid infrastructure environments.

3.4.1 Cloud-Based Disaster Recovery

- **Cloud Infrastructure Recovery:**
  - Multi-region cloud deployment for geographic redundancy
  - Automated cloud resource provisioning using Infrastructure-as-Code

  - Cloud-native backup and recovery services integration
  - Cross-cloud replication for vendor diversification
  - Elastic scaling for disaster recovery capacity management
- **Hybrid Cloud Recovery:**
  - Seamless failover between on-premises and cloud environments
  - Data synchronization and replication across hybrid infrastructure
  - Network connectivity and VPN recovery for hybrid operations
  - Identity and access management integration across environments
  - Consistent security policy enforcement in hybrid recovery scenarios

3.4.2 Container and Microservices Recovery

- **Containerized Application Recovery:**
  - Container orchestration platform disaster recovery procedures
  - Container image backup and restoration processes
  - Persistent volume backup and recovery for stateful applications
  - Service mesh and networking recovery procedures
  - Container security and policy restoration
- **Database and Storage Recovery:**
  - Database cluster recovery and replication management
  - Distributed storage system recovery and data consistency validation
  - Message queue and event streaming system recovery
  - API gateway and service discovery recovery procedures
  - Data pipeline and ETL process recovery and validation

3.5 Recovery Monitoring and Performance Management

Comprehensive monitoring and performance management shall ensure effective disaster recovery operations and continuous improvement.

3.5.1 Recovery Monitoring and Metrics

- **Key Performance Indicators (KPIs):**
  - Recovery Time Objective (RTO) achievement and measurement
  - Recovery Point Objective (RPO) achievement and data loss assessment
  - System availability and uptime metrics during recovery

  - Recovery procedure execution time and efficiency metrics
  - Resource utilization and capacity metrics during recovery operations
- **Real-time Monitoring and Alerting:**
  - Continuous monitoring of disaster recovery infrastructure and systems
  - Automated alerting for recovery procedure failures or delays
  - Performance monitoring and capacity management during recovery
  - Security monitoring and threat detection during recovery operations
  - Integration with SIEM systems for comprehensive security monitoring

3.5.2 Post-Recovery Analysis and Improvement

- **Recovery Assessment and Analysis:**
  - Comprehensive technical analysis of recovery procedure effectiveness
  - Performance metrics analysis and comparison with objectives
  - Root cause analysis of any recovery failures or delays
  - Cost analysis and resource utilization assessment
  - Technology infrastructure and procedure improvement recommendations
- **Continuous Improvement Implementation:**
  - Regular updates to disaster recovery procedures based on lessons learned
  - Technology infrastructure improvements and capacity enhancements
  - Automation enhancement and procedure optimization
  - Staff training and skill development for improved recovery capabilities
  - Integration of new technologies and best practices

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
IT Recovery Team Lead	Lead technical disaster recovery activities, coordinate system restoration efforts, manage recovery team resources, and ensure adherence to recovery procedures and timelines.
System Administrators	Implement system recovery procedures, restore servers and infrastructure, validate system functionality, monitor recovery progress, and document recovery activities.
Database Administrators	Perform database recovery procedures, validate data integrity, coordinate database replication, manage backup restoration, and ensure database security during recovery.
Network Engineers	Restore network connectivity and infrastructure, configure failover systems, validate network performance, coordinate with ISPs and vendors, and ensure network security.
Cloud Engineers	Manage cloud-based disaster recovery, coordinate multi-cloud operations, implement automated recovery procedures, manage cloud resource scaling, and ensure cloud security compliance.
Security Engineers	Validate security controls during recovery, monitor for security threats, ensure compliance with security policies, coordinate security incident response, and maintain audit trails.
DevOps Engineers	Implement automated recovery procedures, manage CI/CD pipeline recovery, coordinate application deployment, manage containerized recovery, and maintain infrastructure automation.
IT Management	Provide strategic direction for recovery efforts, coordinate with business units, manage vendor relationships, ensure resource allocation, and communicate recovery status.
All IT Personnel	Follow disaster recovery procedures, participate in recovery testing and training, report technical issues, support recovery efforts as assigned, and maintain recovery documentation.

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	Who	What
1	Security Team	Conduct annual incident response training and exercises.
2	Security Team	Maintain and test incident response tools and systems.
3	All Personnel	Report suspected incidents to the Security Team immediately.
4	Security Analyst	Triage and classify incoming alerts and reports to determine if an incident has occurred.

Step	Who	What
5	Incident Commander	Activate the Incident Response Team (IRT) for confirmed incidents.
6	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	Incident Commander	Conduct a post-incident review (lessons learned) meeting.
10	Incident Commander	Complete and file a formal Incident Report.

5. Standards Compliance

See Annex: Control Mapping

7. Definitions

See Annex: Glossary

8. Responsibilities

Role	Responsibility
Incident Commander	Leads and coordinates the overall incident response effort.

Role	Responsibility
Security Analyst	Performs initial triage, analysis, and technical investigation of incidents.
Privacy Officer	Assesses incidents for potential data breach notification mandates, 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 mandated 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

See Annex: Control Mapping

6. Artifact(s)

A completed and signed HIPAA Breach Risk Assessment form.

7. Definitions

See Annex: Glossary

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

See Annex: Control Mapping

6. Artifact(s)

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

7. Definitions

See Annex: Glossary

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

See Annex: Control Mapping

6. Artifact(s)

A formally approved Business Impact Analysis (BIA) Report.

7. Definitions

See Annex: Glossary

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 mandated 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

See Annex: Control Mapping

7. Definitions

See Annex: Glossary

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 mandated 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

See Annex: Control Mapping

6. Artifact(s)

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

7. Definitions

See Annex: Glossary

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.

Role	Responsibility
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 mandates 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 mandated 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

See Annex: Control Mapping

6. Artifact(s)

- A completed annual test plan.
- A post-exercise report with lessons learned for each test conducted.

7. Definitions

See Annex: Glossary

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 review cadence is defined in the IAM Policy (AC-POL-001) for standard access and the Privileged Access Management Policy (AC-POL-004) for privileged access. See AC-POL-001 and AC-POL-004 for authoritative requirements.
- 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.

3.10.1 Threat Intelligence and Security Information Sharing Implementation

- **[Company Name]** shall implement comprehensive threat intelligence and security information sharing processes as follows:

- **Healthcare-Specific Threat Intelligence:** Subscriptions to healthcare-specific threat intelligence feeds including **[Threat Feeds, e.g., HHS HCCIC, FBI IC3, MS-ISAC]** shall be maintained to receive current threat information relevant to the healthcare sector.
- **Automated Threat Indicator Ingestion:** Automated ingestion of threat indicators including IoCs, TTPs, and vulnerability information shall be configured into **[Threat Intelligence Platform]** for systematic processing and analysis.
- **Internal Security Data Collection:** Internal security data from SIEM, IDS/IPS, endpoint detection, and vulnerability scanners shall be collected and analyzed for threat pattern identification.
- **Daily Threat Analysis:** Daily analysis of threat intelligence feeds shall be performed to identify threats relevant to healthcare sector and organizational infrastructure, with correlation to internal security events.
- **Security Monitoring Integration:** Threat intelligence indicators shall be integrated into security monitoring tools for automated detection and alerting capabilities.
- **Proactive Threat Hunting:** Weekly proactive threat hunting using intelligence-driven hypotheses shall be conducted to identify advanced persistent threats and sophisticated attack activities.
- **Intelligence Briefings:** Weekly threat intelligence briefings shall be generated for security teams including emerging threats, attack trends, and recommended countermeasures.
- **External Information Sharing:** Sanitized threat indicators shall be shared with **[Sharing Partners, e.g., HC3, industry peers]** through secure information sharing platforms, subject to approval processes to protect sensitive organizational information.
- **Incident Response Intelligence:** Threat intelligence shall be leveraged during incident response to understand attacker tactics, techniques, and procedures (TTPs), with analysis of security incidents to extract new threat intelligence.
- **Vulnerability Prioritization:** Vulnerability remediation shall be prioritized based on threat intelligence indicating active exploitation in healthcare sector.
- **Security Control Updates:** Security controls and monitoring rules shall be updated based on threat intelligence findings and emerging attack techniques.
- **Documentation and Retention:** Threat intelligence records and sharing documentation shall

be maintained for minimum **[Retention Period, e.g., 2 years]** for audit compliance purposes.

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

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.
Information Owners	Classify information assets, approve access requests, and ensure appropriate handling of sensitive data.

Role	Responsibility
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.
Threat Intelligence Analyst	Collect, analyze, and disseminate threat intelligence. Correlate external threats with internal security events and generate intelligence briefings.
Security Operations Center	Integrate threat intelligence into monitoring tools and respond to intelligence-driven alerts and detections.
Threat Hunting Team	Conduct proactive threat hunting using intelligence-driven hypotheses to identify advanced threats and attack activities.
Incident Response Team	Leverage threat intelligence during incident response and analyze incidents to extract new threat intelligence.
Vulnerability Management Team	Prioritize vulnerability remediation based on threat intelligence indicating active exploitation patterns.
Security Architecture Team	Update security controls and monitoring rules based on threat intelligence findings and emerging attack techniques.

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

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

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.

3.2.1 Penetration Testing and Vulnerability Assessment Implementation

- **[Company Name]** shall implement comprehensive penetration testing and vulnerability assessment processes as follows:
- **Annual Penetration Testing Plan:** The Information Security Officer shall develop an annual penetration testing plan identifying scope, methodology, timeline, and resource requirements for comprehensive security assessment.
- **Third-Party Testing Providers:** Qualified third-party penetration testing vendors with **[Required Certifications, e.g., CISSP, CEH, OSCP]** and healthcare industry experience shall be engaged for testing activities.
- **Testing Methodology:** Penetration testing shall include:
  - Pre-testing reconnaissance shall be conducted to identify external-facing systems, network ranges, and application attack surfaces.
  - Automated vulnerability scanning using **[Scanning Tools, e.g., Nessus, Qualys, OpenVAS]** shall be performed across all in-scope systems.
  - Network penetration testing shall be conducted including external perimeter testing, internal network lateral movement, and wireless network security assessment.
  - Web application security testing using **[Testing Methodology, e.g., OWASP Testing Guide]** shall be performed for all applications handling sensitive data.

  - Social engineering assessment shall be conducted including phishing simulation, physical security testing, and employee security awareness validation.
  - Cloud infrastructure security testing shall be performed including IAM controls, storage security, network configurations, and container security.

- **Vulnerability Documentation:** All identified vulnerabilities shall be documented with risk ratings using **[Risk Rating System, e.g., CVSS v3.1]** and exploitation evidence.
- **Remediation Requirements:** Critical and high-risk vulnerabilities shall be remediated within **[Duration, e.g., 30 days]** of testing completion, medium-risk vulnerabilities within **[Duration, e.g., 90 days]**, and low-risk vulnerabilities within **[Duration, e.g., 180 days]**.
- **Validation Testing:** Validation testing shall be conducted to confirm successful remediation of all critical and high-risk vulnerabilities.
- **Quarterly Vulnerability Assessments:** Automated vulnerability assessments shall be conducted quarterly with monthly scan result reviews for ongoing security validation.
- **Targeted Testing:** Penetration testing shall be performed within **[Duration, e.g., 30 days]** of significant system changes, new application deployments, or security incidents.
- Risk identification shall consider internal and external threats, including but not limited to:
  - Cybersecurity threats (malware, phishing, unauthorized access) shall be identified and assessed for organizational impact.
  - Natural disasters and environmental hazards shall be evaluated for their potential impact on information systems and business operations.
  - Human error and insider threats shall be considered as potential sources of information security risks.
  - Technology failures and system outages shall be assessed for their impact on data availability and business continuity.
  - Regulatory and compliance changes shall be monitored and evaluated for their impact on organizational risk posture.
  - Third-party and vendor risks shall be identified and assessed as part of the comprehensive risk management program.

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) shall be quantified where possible to support risk-based decision making.
  - Operational impact (service disruption, productivity loss) shall be assessed for its effect on business operations and service delivery.
  - Reputational impact (customer trust, market confidence) shall be evaluated for its potential long-term consequences to organizational standing.
  - Regulatory impact (compliance violations, sanctions) shall be assessed for potential legal and regulatory consequences.
  - Patient safety and privacy implications shall be evaluated for their impact on healthcare delivery and regulatory compliance.
- Likelihood assessment shall consider:
  - Threat actor capabilities and motivations shall be evaluated based on available threat intelligence and industry analysis.
  - Asset vulnerabilities and exposure shall be assessed through vulnerability scanning and security assessments.
  - Effectiveness of existing controls shall be evaluated through testing, monitoring, and audit activities.
  - Historical incident data and industry trends shall be analyzed to inform likelihood assessments and improve accuracy.
- 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 shall be documented with clear justification and approval.
  - **Avoid:** Eliminate the risk by discontinuing or modifying activities shall be considered when risks exceed organizational tolerance.
  - **Mitigate:** Implement controls to reduce likelihood or impact shall be the primary approach for managing significant risks.
  - **Transfer:** Share or transfer risk through insurance, contracts, or outsourcing shall be utilized where appropriate and cost-effective.
- 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 shall be clearly defined with measurable objectives and outcomes.
  - Responsible parties and timelines shall be assigned to ensure accountability and timely implementation.
  - Resource requirements and budget allocations shall be identified and approved through appropriate organizational processes.
  - Success criteria and monitoring measures shall be established to evaluate the effectiveness of risk treatment activities.
- 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 shall be reported to provide situational awareness to stakeholders.
  - Status of risk treatment activities shall be communicated to track progress and identify issues requiring attention.
  - Emerging threats and vulnerabilities shall be shared to enable proactive risk management and response planning.
  - Recommendations for risk mitigation shall be provided to support evidence-based decision making.
  - Compliance and regulatory implications shall be communicated to ensure awareness of legal and regulatory requirements.

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	HITRUST CSF v11.2.0	17.a - Risk Management Program
3.1	HITRUST CSF v11.2.0	17.b - Risk Management Framework
3.2, 3.3	HITRUST CSF v11.2.0	17.c - Risk Assessment Process
3.2.1	HITRUST CSF v11.2.0	07.a - Vulnerability Management

Policy Section	Standard/Framework	Control Reference
3.2.1	HITRUST CSF v11.2.0	07.b - Vulnerability Assessment
3.2.1	HITRUST CSF v11.2.0	07.c - Vulnerability Remediation
3.2.1	HITRUST CSF v11.2.0	08.b - Network Security Testing
3.4, 3.5	HITRUST CSF v11.2.0	17.d - Risk Treatment
3.6	HITRUST CSF v11.2.0	17.e - Risk Monitoring and Review
3.7	HITRUST CSF v11.2.0	14.b - Third Party Risk Assessment
3.8	HITRUST CSF v11.2.0	16.b - Business Impact Analysis
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
3.2.1	HIPAA Security Rule	45 CFR § 164.308(a)(8) - Evaluation
All	SOC 2 Trust Services Criteria	CC3.1 - Risk Assessment Process
3.2, 3.3	SOC 2 Trust Services Criteria	CC3.2 - Risk Identification
3.4, 3.5	SOC 2 Trust Services Criteria	CC3.3 - Risk Mitigation
3.6	SOC 2 Trust Services Criteria	CC3.4 - Risk Assessment Updates

Policy Section	Standard/Framework	Control Reference
3.2.1	SOC 2 Trust Services Criteria	CC7.1 - System Security
3.2.1	SOC 2 Trust Services Criteria	CC8.1 - Change Management
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
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
3.2.1	NIST SP 800-115	Technical Guide to Information Security Testing

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. Oversee penetration testing and vulnerability assessment programs.
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.

Role	Responsibility
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.
Audit and Compliance Team	Validate risk assessment processes and control effectiveness. Ensure regulatory compliance requirements are addressed.
Third-Party Testing Vendors	Conduct comprehensive penetration testing and vulnerability assessments according to defined methodologies and healthcare industry standards.
System Administrators	Remediate identified vulnerabilities within specified timeframes based on risk level and impact assessment.

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 shall be required for public information.
- Standard backup and archival procedures shall be applied to public information.
- Public information may be stored on standard business systems without additional security controls.
- Public information can be transmitted via standard email or file sharing without encryption requirements.

3.3.2 Internal Information

- Access shall be restricted to authorized **[Company Name]** workforce members.
- Internal information shall be password-protected when stored on portable devices.
- Internal information shall be transmitted via secure channels (encrypted email, secure file transfer).
- Internal information shall be stored on company-approved systems with appropriate access controls.
- Internal information shall be covered by confidentiality agreements for third-party access.

3.3.3 Confidential Information

- Access shall be granted only on a need-to-know basis with formal approval.
- Confidential information shall be encrypted when stored on laptops, mobile devices, or removable media.
- Confidential information shall be transmitted only via encrypted channels (secure email, VPN, HTTPS).
- Confidential information shall be stored on hardened systems with enhanced access controls and audit logging.
- Systems containing confidential information shall be protected by multi-factor authentication for system access.
- Non-Disclosure Agreements (NDAs) shall be required for third-party access to confidential information.

- Confidential information must be clearly labeled or marked to indicate classification level.

3.3.4 Restricted Information

- Access shall be granted only to specifically authorized individuals with documented business justification.
- Restricted information shall be encrypted at rest using **[Encryption Standard, e.g., AES-256]** or equivalent.
- Restricted information shall be encrypted in transit using **[Protocol, e.g., TLS 1.3]** or equivalent.
- Restricted information shall be stored only on systems specifically approved for Restricted data.
- Systems containing restricted information shall be protected by multi-factor authentication and privileged access controls.
- All access to restricted information shall be logged and monitored for unauthorized activity.
- Business Associate Agreements (BAAs) shall be required for third-party handling of restricted information.
- Restricted information must be clearly labeled and handled according to regulatory requirements.
- Restricted information shall be 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 to ePHI shall be limited to workforce members whose job functions require ePHI to perform their duties
- Minimum necessary standard shall be applied to all ePHI access, use, and disclosure
- All ePHI access shall be logged with user identification, date/time, and specific information accessed
- ePHI shall be transmitted only via HIPAA-compliant secure methods
- Regular audits shall be conducted to verify appropriate ePHI access and usage
- Breach notification procedures shall be 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 shall require encryption and compliance with security standards
- Access reviews shall follow the cadence defined in AC-POL-001 (IAM) for standard access and AC-POL-004 (PAM) for privileged access
- 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 shall be performed according to NIST SP 800-88 guidelines.
  - Physical documents: Cross-cut shredding or incineration shall be performed to prevent information recovery.
  - Optical media: Physical destruction shall be performed to ensure complete data 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

3.11 Portable Media Security Management

Comprehensive security controls shall be implemented for portable media and digital storage devices containing or potentially containing sensitive information throughout their lifecycle.

3.11.1 Media Classification and Inventory

- Media inventory entries shall be created in **[Asset Management System]** with unique identifiers, content classification, encryption status, and assigned custodians
- All media shall be appropriately labeled indicating classification level (Public, Internal, Confidential, Restricted) and handling requirements
- Media classification shall follow the same framework as other information assets with the highest classification determining overall media handling requirements
- Physical inventory verification shall be conducted monthly comparing actual media location with inventory system records
- Missing, damaged, or compromised media shall be reported immediately to the Information Security Officer with incident response initiation

3.11.2 Media Encryption and Protection

- All media containing Confidential or Restricted data shall be encrypted using **[Approved Encryption Standards, e.g., AES-256]** with organization-managed keys

- Encryption implementation shall be verified and data accessibility tested before initial use or distribution
- Media storage shall be in appropriate secure locations based on classification: locked cabinet (Internal), safe (Confidential), or vault (Restricted)
- Tamper-evident packaging with chain of custody documentation shall be used for media transportation
- Continuous custody shall be maintained during transport or bonded courier services with tracking and signature confirmation utilized

3.11.3 Media Reuse and Sanitization

- Secure data sanitization using **[NIST SP 800-88]** compliant methods shall be performed before media reassignment
- Sanitization methods shall be documented with verification of data removal and approval for reuse recorded in asset management system
- Media custodians shall verify package integrity, validate chain of custody documentation, and test media accessibility upon receipt
- Reuse approval shall require Information Security Officer verification of complete data sanitization

3.11.4 Media Disposal and Destruction

- End-of-life media shall use certified destruction services with certificate of destruction for all Confidential and Restricted media
- Media containing ePHI shall ensure destruction methods meet HIPAA requirements with detailed destruction certificates obtained
- Destruction certificates and inventory records shall be maintained for minimum **[Retention Period, e.g., 7 years]** for audit and regulatory compliance
- Disposal personnel shall be vetted and bonded for handling sensitive media destruction
- Physical destruction methods shall render data unrecoverable using industry-recognized standards

3.11.5 Media Security Monitoring and Assessment

- Monthly media inventory reports shall be reviewed by the Information Security Officer with investigation of discrepancies or unauthorized usage

- Quarterly assessment of media security controls shall be conducted with procedure updates based on risk assessment findings
- Media handling violations shall be reported through the incident response process with appropriate corrective actions
- Annual media security training shall be provided to all personnel handling portable media
- Compliance audits shall verify adherence to media handling requirements and regulatory obligations

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Information Owners	Classify information assets, approve access requests, conduct periodic classification reviews, and ensure appropriate handling.
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.

Role	Responsibility
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 practical, risk-based requirements for managing security risks associated with vendors and third-party service providers, with focus on regulatory compliance for electronic Protected Health Information (ePHI) while maintaining operational efficiency.

2. Scope

This policy applies to all **[Company Name]** workforce members involved in vendor selection and management. It covers external parties that access company data or systems, with streamlined procedures based on actual risk levels rather than comprehensive assessment requirements for all vendors.

3. Policy

- **[Company Name]** shall implement a streamlined, risk-based vendor management approach that focuses resources on high-risk vendors while maintaining regulatory compliance through practical assessment and monitoring procedures.

3.1 Simplified Vendor Risk Tiers

Vendors shall be classified into three practical risk tiers with appropriate assessment requirements for each tier.

3.1.1 Risk-Based Vendor Classification

- **Tier 1 - Critical Risk (ePHI and Core Infrastructure):**
  - Cloud service providers (AWS, Azure, GCP)
  - Vendors with direct ePHI access (healthcare APIs, patient communication tools)
  - Core infrastructure providers (identity management, security tools)
  - Development and deployment platform providers
- **Tier 2 - Business Risk (Internal Data and Business-Critical Services):**
  - Business applications with internal data access (CRM, HR systems, financial tools) shall be included in this risk tier.

  - Communication and collaboration platforms (Slack, email providers) shall be classified as business risk tier.
  - Backup and disaster recovery services shall be evaluated under business risk assessment requirements.
  - Legal and professional services with confidential data access shall be subject to business risk tier controls.
- **Tier 3 - Standard Risk (Limited Access and Commodity Services):**
  - Marketing and analytics tools with minimal data access shall be included in the standard risk tier.
  - Development tools and services without production data shall be classified as standard risk.
  - Office productivity tools and subscriptions shall be subject to standard risk assessment requirements.
  - Professional services without data access shall be evaluated under standard risk tier controls.

3.1.2 Streamlined Assessment Requirements

- **Tier 1 - Critical Risk Assessment:**
- **Security Certification**: SOC 2 Type II, ISO 27001, or equivalent certification required
- **Business Associate Agreement**: Required for any ePHI access
- **Financial Stability**: Basic financial stability verification
- **Security Contact**: Established security contact and incident notification procedures
- **Insurance**: Cyber liability insurance verification ($**[Amount, e.g., 5-10 million]** minimum)
- **Tier 2 - Business Risk Assessment:**
- **Basic Security Review**: Security questionnaire or self-attestation shall be conducted to assess basic security posture.
- **Contract Terms**: Standard security clauses shall be included in service agreement to establish security expectations.
- **Data Protection**: Basic data protection and incident notification requirements shall be documented in contractual terms.

- **Insurance**: General liability and professional insurance verification shall be performed to ensure adequate coverage.
- **Tier 3 - Standard Risk Assessment:**
- **Service Agreement**: Standard terms of service with basic security provisions shall be reviewed and accepted.
- **Privacy Policy**: Review of vendor privacy policy and data handling practices shall be conducted to ensure alignment with organizational requirements.
- **Minimal Due Diligence**: Basic vendor legitimacy and reputation verification shall be performed through public sources and references.

3.2 Automated Vendor Risk Assessment

Leverage automated tools and vendor risk assessment platforms to streamline the evaluation process.

3.2.1 Third-Party Risk Assessment Platforms

- **Vendor Risk Management Tools**: Platforms like SecurityScorecard, BitSight, or UpGuard shall be used for automated vendor security ratings.
- **Questionnaire Automation**: Shared security questionnaire databases and automated assessment tools shall be leveraged to streamline evaluation processes.
- **Continuous Monitoring**: Automated monitoring of vendor security posture and incident notifications shall be implemented for ongoing risk visibility.
- **Compliance Databases**: Compliance databases shall be used to verify vendor certifications and attestations.

3.2.2 Cloud Provider Security Posture

- **Shared Responsibility Model**: Cloud provider vs. customer security responsibilities shall be understood and documented.
- **Compliance Center**: Regular review of cloud provider compliance center documentation and certifications shall be conducted.
- **Service Health**: Cloud provider service health dashboards and security advisories shall be monitored continuously.

- **Configuration Reviews**: Quarterly review of cloud service security configurations and settings shall be performed.

3.3 Business Associate Agreements and Practical Contract Terms

Focus contract negotiations on essential security requirements rather than comprehensive security clauses for all vendors.

3.3.1 ePHI Business Associate Agreements

For Tier 1 vendors with ePHI access:

- **Standard BAA Template**: Use standardized BAA template covering HIPAA requirements
- **Incident Notification**: **[Timeframe, e.g., 24-hour]** incident notification requirement
- **Data Return**: Secure data return or destruction upon contract termination
- **Audit Rights**: Right to review security practices and compliance evidence
- **Subcontractor Requirements**: Flow-down of BAA requirements to subcontractors

3.3.2 Standard Security Contract Provisions

For Tier 2 vendors:

- **Data Protection**: Basic data protection and confidentiality requirements
- **Incident Notification**: **[Timeframe, e.g., 72-hour]** security incident notification
- **Insurance**: Professional liability and cyber insurance requirements
- **Data Location**: Geographic data storage and processing restrictions
- **Termination**: Data return requirements upon contract termination

3.3.3 Commodity Service Agreements

For Tier 3 vendors:

- **Terms of Service**: Accept standard vendor terms of service with privacy policy review
- **Data Minimization**: Limit data shared to necessary business purposes only
- **Account Security**: Require multi-factor authentication and strong password policies
- **Access Controls**: Implement role-based access controls within vendor systems

3.4 Ongoing Vendor Monitoring

Implement practical, automated monitoring focused on high-risk vendors while maintaining awareness of vendor security posture.

3.4.1 Tier 1 Vendor Monitoring

- **Annual Certification Review**: Review updated SOC 2 reports and security certifications
- **Security Scorecard Monitoring**: Continuous monitoring through vendor risk assessment platforms
- **Incident Notifications**: Active monitoring of vendor security incidents and advisories
- **Contract Performance**: Annual review of contract compliance and service performance
- **Access Review**: Quarterly review of vendor access and permissions

3.4.2 Tier 2 and 3 Vendor Monitoring

- **Contract Renewal Review**: Security assessment during contract renewal cycle
- **Incident Awareness**: Monitor for significant security incidents affecting vendor services
- **Access Management**: Annual review of vendor access and account permissions
- **Cost and Performance**: Monitor vendor performance and cost optimization opportunities

3.5 Vendor Access Management

Implement practical access controls that balance security with operational efficiency.

3.5.1 Access Provisioning

- **Business Justification**: Clear business justification required for vendor access requests
- **Least Privilege**: Limit vendor access to minimum necessary for contracted services
- **Time-Limited Access**: Implement time-limited access for temporary or project-based vendors
- **Multi-Factor Authentication**: Require MFA for all vendor access to critical systems
- **Single Sign-On**: Use SSO integration where available to centralize access management

3.5.2 Access Monitoring and Review

- **Automated Logging**: Log vendor access activities through existing security monitoring tools

- **Regular Access Review**: **[Frequency, e.g., Quarterly]** review of active vendor accounts and permissions
- **Prompt Deprovisioning**: Immediate access revocation upon contract termination or project completion
- **Exception Reporting**: Automated alerts for unusual vendor access patterns or failed authentication attempts

3.6 Cloud-Native Vendor Security

Leverage cloud provider security capabilities to monitor and control vendor access to cloud resources.

3.6.1 Cloud Provider Selection

- **Major Cloud Providers**: Prefer major cloud providers (AWS, Azure, GCP) with comprehensive compliance certifications
- **Shared Responsibility**: Clearly understand and document shared responsibility model
- **Security Center**: Use cloud provider security centers for continuous compliance monitoring
- **Cost Optimization**: Balance security requirements with cost-effective service selection

3.6.2 Cloud Service Monitoring

- **Service Health Monitoring**: Monitor cloud provider service health and security advisory notifications
- **Configuration Management**: Use cloud-native tools to monitor and enforce security configurations
- **Access Analytics**: Leverage cloud provider access analytics and unusual activity detection
- **Compliance Dashboards**: Use cloud provider compliance dashboards for ongoing attestation evidence

3.7 Incident Response and Vendor Coordination

Establish practical procedures for coordinating security incidents involving vendor services.

3.7.1 Vendor Incident Notification

- **Notification Procedures**: Clear procedures for vendors to report security incidents affecting **[Company Name]** data
- **Response Coordination**: Designated Security Officer as primary contact for vendor incident coordination
- **Impact Assessment**: Rapid assessment of vendor incident impact on company operations and data
- **Communication**: Internal communication procedures for vendor-related security incidents

3.7.2 Vendor Support During Incidents

- **Technical Coordination**: Coordinate with vendors during security incidents affecting their services
- **Evidence Collection**: Coordinate evidence collection and forensic activities with vendor support
- **Recovery Planning**: Coordinate service recovery and business continuity with vendor teams
- **Lessons Learned**: Document lessons learned from vendor incidents for future risk assessment

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, 3.4	HITRUST CSF v11.2.0	14.a - Third Party Assurance Policy
3.1, 3.4	HITRUST CSF v11.2.0	14.b - Third Party Risk Assessment
3.3	HITRUST CSF v11.2.0	14.c - Third Party Service Agreements
3.5	HITRUST CSF v11.2.0	14.d - Third Party Access Management
3.4	HITRUST CSF v11.2.0	14.e - Third Party Monitoring

Policy Section	Standard/Framework	Control Reference
3.3.1	HIPAA Security Rule	45 CFR § 164.314(a)(1) - Business Associate Contracts
3.3.1	HIPAA Security Rule	45 CFR § 164.314(a)(2) - Business Associate Safeguards
3.1	HIPAA Security Rule	45 CFR § 164.308(a)(1)(ii)(A) - Risk Assessment
3.5	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Information Access Management
3.7	HIPAA Security Rule	45 CFR § 164.308(a)(6) - Security Incident Procedures
All	SOC 2 Trust Services Criteria	CC9.1 - Vendor Management
3.1, 3.4	SOC 2 Trust Services Criteria	CC9.2 - Vendor Risk Assessment
3.3	SOC 2 Trust Services Criteria	CC9.3 - Vendor Agreements

5. Definitions

- **Business Associate Agreement (BAA):** A written contract between a covered entity and a business associate required by HIPAA for any ePHI access.
- **Cloud Service Provider:** A company that offers network services, infrastructure, or business applications in the cloud (e.g., AWS, Azure, GCP).
- **Risk Tier:** Classification system for vendors based on data access and business criticality (Tier 1-Critical, Tier 2-Business, Tier 3-Standard).
- **Security Scorecard:** Automated security rating system that continuously monitors vendor security posture using external security indicators.
- **Single Sign-On (SSO):** Authentication system that allows users to access multiple vendor systems with one set of credentials.

- **Vendor Risk Assessment:** Streamlined evaluation process appropriate to vendor risk tier and data access requirements.

6. Responsibilities

Role	Responsibility
Security Officer	Classify vendors into appropriate risk tiers, manage relationships with critical risk vendors, ensure BAA execution for ePHI access vendors, and serve as primary contact for vendor security incidents.
Business Owners	Select appropriate vendors based on business requirements, provide business justification for vendor engagement, monitor vendor service delivery, and manage vendor costs within approved budgets.
IT Operations Team	Implement technical integrations with vendor systems, provision and manage vendor access through SSO systems, configure vendor systems according to security requirements, and provide technical support during vendor incidents.
Legal/Contracts Team	Negotiate contract terms and security provisions, execute Business Associate Agreements, review vendor contracts for compliance issues, and manage contract termination procedures.
Finance Team	Conduct financial stability assessments for Tier 1 vendors, verify vendor insurance coverage, monitor vendor costs and optimization opportunities, and include vendor management costs in budget planning.

Role	Responsibility
Development Team	Implement secure API integrations with vendor services, ensure data minimization in vendor integrations, implement application-level security controls, and document vendor integrations and security implementations.

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 access reviews following the cadence defined in AC-POL-001 (IAM) and AC-POL-004 (PAM)
  - 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

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

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 Governance and Coordination Framework Policy (SEC-POL-007)

1. Objective

The objective of this policy is to establish the comprehensive governance framework and coordination requirements for Artificial Intelligence (AI) and Machine Learning (ML) technologies at **[Company Name]**. This policy provides the overarching framework for AI governance and coordinates the specialized requirements defined in SEC-POL-012 (AI Development and Deployment Security Policy) and SEC-POL-013 (AI Ethics and Compliance Policy). This framework ensures that AI tools and systems are governed holistically with appropriate security, ethical, and compliance controls while enabling innovation and productivity improvements through responsible AI adoption that protects confidentiality, integrity, and availability of company information, particularly electronic Protected Health Information (ePHI).

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, third parties, and business associates who use, develop, deploy, govern, or manage AI and ML technologies on behalf of the organization. It encompasses all AI applications including generative AI tools, machine learning models, automated decision-making systems, and AI-powered business applications. This policy provides the governance framework for both internally developed AI systems and third-party AI services, regardless of deployment model, and coordinates the technical security requirements (SEC-POL-012) with ethics and compliance requirements (SEC-POL-013) across all use cases.

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
All	HITRUST CSF v11.2.0	01.d - Information Security Governance
3.1	HITRUST CSF v11.2.0	01.e - Information Handling Requirements
3.2	HITRUST CSF v11.2.0	19.a - Data Protection and Privacy Policy
3.3	HITRUST CSF v11.2.0	13.b - Information Security Awareness
3.4	HITRUST CSF v11.2.0	12.b - Audit Logging Requirements
3.5	HITRUST CSF v11.2.0	17.f - Emerging Technology Risk
3.2.1	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Information Access Management
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

Policy Section	Standard/Framework	Control Reference
3.1	SOC 2 Trust Services Criteria	CC2.1 - Communication and Information
3.5	SOC 2 Trust Services Criteria	CC8.1 - System Development
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.
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.

Role	Responsibility
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 shall 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

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

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.

Audit Logging Framework and Coordination Policy (SEC-POL-009)

1. Objective

The objective of this policy is to establish the comprehensive audit logging framework and coordination requirements for **[Company Name]**'s information systems to ensure security events are captured, protected, and analyzed in support of incident detection, forensic analysis, and regulatory compliance. This policy provides the overarching framework for audit logging and coordinates the specialized logging requirements defined in SEC-POL-010 (Authentication and Network Audit Logging Policy) and SEC-POL-011 (Data Access and Compliance Audit Logging Policy). This framework ensures that appropriate audit trails are maintained to support the confidentiality, integrity, and availability of information assets and electronic Protected Health Information (ePHI) in compliance with HIPAA, HITECH, SOC 2, and HITRUST CSF v11.2.0 requirements.

2. Scope

This policy applies to all **[Company Name]** information systems, applications, network devices, security tools, and cloud services that process, store, or transmit company information or ePHI. This includes all production, staging, development, and administrative systems, as well as any third-party systems that process company data. All workforce members, contractors, and third parties with access to company systems are subject to the monitoring and logging requirements defined in this policy and its associated specialized policies SEC-POL-010 and SEC-POL-011.

3. Policy

- **[Company Name]** shall implement comprehensive audit logging and monitoring capabilities across all information systems through a coordinated framework that integrates authentication and network security logging (SEC-POL-010) with data access and compliance logging (SEC-POL-011) to provide early detection of security incidents, support forensic analysis, and maintain compliance with regulatory requirements.

3.1 Audit Logging Framework Architecture

The audit logging framework shall provide comprehensive coverage across all system domains through specialized policies while maintaining centralized coordination and analysis capabilities.

3.1.1 Policy Integration and Coordination

- **Specialized Logging Domains:**
  - **SEC-POL-010 (Authentication and Network Audit Logging Policy)**: Comprehensive logging for user authentication, authorization, network security events, and system security activities
  - **SEC-POL-011 (Data Access and Compliance Audit Logging Policy)**: Detailed logging for data access, ePHI handling, privacy controls, and regulatory compliance activities
  - Cross-policy coordination through common session identifiers, correlation mechanisms, and shared infrastructure
  - Unified incident response integration combining evidence from authentication, network, and data access domains
- **Framework Coordination Requirements:**
  - Common log format standards and metadata requirements across all logging domains
  - Shared centralized logging infrastructure with integrated Security Information and Event Management (SIEM) platform
  - Coordinated retention policies and storage requirements aligned with regulatory and business needs
  - Integrated monitoring and alerting capabilities combining events from authentication, network, and data access domains
  - Unified reporting and compliance validation across all audit logging domains

3.1.2 Comprehensive Event Coverage

The audit logging framework shall ensure comprehensive coverage of all security-relevant events through specialized logging domains:

- **Authentication and Network Events (SEC-POL-010):**
  - User authentication, authorization, and session management events
  - Network security events, traffic analysis, and communication monitoring
  - System security events, infrastructure monitoring, and privilege management
  - Integration with identity management systems and network security appliances
- **Data Access and Compliance Events (SEC-POL-011):**
  - Electronic Protected Health Information (ePHI) and sensitive data access events
  - Regulatory compliance activities including HIPAA, SOC 2, and privacy regulation requirements

  - Data protection and privacy controls implementation and monitoring
  - Data lifecycle management including retention, disposal, and privacy rights fulfillment

3.2 Centralized Log Management Framework

Comprehensive log management processes shall ensure the integrity, availability, and appropriate retention of audit information across all logging domains.

3.2.1 Unified Log Collection and Storage

- **Centralized Infrastructure Requirements:**
  - All systems shall forward security-relevant logs to centralized Security Information and Event Management (SIEM) system supporting both SEC-POL-010 and SEC-POL-011 requirements
  - Log transmission shall use encrypted channels (TLS 1.3 or equivalent) to protect log data in transit
  - Redundant log collection paths shall be implemented for critical systems across all logging domains
  - Real-time log forwarding required for security events classified as Critical or High priority
  - Backup log storage at local systems for minimum **[Duration, e.g., 7 days]** to ensure continuity during network outages
- **Integrated Storage and Retention:**
  - Security audit logs shall be retained for minimum **[Duration, e.g., 7 years]** to support regulatory compliance across all domains
  - ePHI access logs shall be retained for minimum **[Duration, e.g., 6 years]** per HIPAA requirements as detailed in SEC-POL-011
  - Authentication and network logs shall be retained per SEC-POL-010 requirements with coordination for incident investigation
  - Archive logs shall be stored in immutable storage systems where technically feasible
  - Legal hold procedures shall supersede standard retention periods when litigation is anticipated

3.2.2 Cross-Domain Event Correlation

- **Event Integration and Analysis:**

  - Automated correlation of authentication events from SEC-POL-010 with data access events from SEC-POL-011
  - Session identifier and transaction correlation across all logging domains
  - Timeline reconstruction capabilities integrating evidence from authentication, network, and data access logs
  - Behavioral analysis combining user authentication patterns with data access activities
  - Threat intelligence integration across all event types and logging domains

3.3 Log Protection and Integrity Framework

Audit logs across all domains shall be protected against unauthorized access, modification, and deletion to maintain their evidentiary value through coordinated security controls.

3.3.1 Unified Access Controls

- **Framework-Wide Access Management:**
  - Role-based access control with principle of least privilege across all logging domains
  - Separate administrative accounts for log system management with multi-factor authentication
  - Coordinated access reviews for all log system administrators across SEC-POL-010 and SEC-POL-011 domains
  - Cross-domain access logging and monitoring for administrative activities
  - Integration with identity management systems for centralized access control

3.3.2 Integrated Integrity Protection

- **Cross-Domain Integrity Controls:**
  - Cryptographic hashing (SHA-256 or stronger) for log file integrity verification across all domains
  - Digital signatures for critical audit logs using approved PKI infrastructure
  - Tamper detection mechanisms with automated alerting for all log sources
  - Write-once storage technologies for immutable log preservation
  - Coordinated integrity verification procedures and reporting across authentication, network, and data access logs

3.4 Coordinated Monitoring and Analysis Framework

Continuous monitoring and analysis of audit logs shall provide early detection of security incidents through integrated analysis across all logging domains.

3.4.1 Unified Real-Time Monitoring

- **Integrated Monitoring Capabilities:**
  - 24/7 automated monitoring of all security-relevant log sources from SEC-POL-010 and SEC-POL-011 domains
  - Real-time correlation of events across authentication, network, and data access domains
  - Machine learning and behavioral analysis for cross-domain anomaly detection
  - Threat intelligence integration for all event types and logging domains
  - Automated response capabilities for predefined security scenarios across all domains

3.4.2 Comprehensive Analysis and Reporting

- **Framework-Wide Analysis:**
  - Daily review of high-priority security alerts and events from all logging domains
  - Weekly trend analysis and security metrics reporting across authentication, network, and data access activities
  - Monthly comprehensive security posture assessment integrating all audit log sources
  - Quarterly log analysis program effectiveness review across all specialized logging policies
  - Annual audit log retention and disposal review coordinated across all domains
- **Integrated Compliance Reporting:**
  - Automated generation of compliance reports combining evidence from SEC-POL-010 and SEC-POL-011
  - Executive dashboard with key security metrics from all logging domains
  - Unified regulatory reporting supporting HIPAA, SOC 2, and HITRUST requirements
  - Cross-domain exception reports for policy violations and security events
  - Coordinated audit evidence collection and presentation

3.5 Integrated Incident Response Framework

Audit logs from all domains shall provide comprehensive support for security incident detection, investigation, and response activities through coordinated evidence collection and analysis.

3.5.1 Cross-Domain Incident Detection

- **Unified Detection Capabilities:**
  - Automated correlation rules combining authentication events from SEC-POL-010 with data access events from SEC-POL-011
  - Baseline deviation detection across user authentication, network behavior, and data access patterns
  - Advanced persistent threat (APT) detection through cross-domain log analysis
  - Insider threat detection through integrated privilege, authentication, and data access monitoring
  - Integration with external threat intelligence sources across all logging domains

3.5.2 Coordinated Response Support

- **Integrated Evidence Collection:**
  - Rapid log search and analysis capabilities across authentication, network, and data access domains
  - Automated evidence collection and preservation procedures coordinating SEC-POL-010 and SEC-POL-011 sources
  - Timeline reconstruction capabilities integrating all logging domains for comprehensive incident analysis
  - Chain of custody procedures for multi-domain log-based evidence
  - Integration with legal hold and eDiscovery processes across all audit log sources

3.6 Performance and Capacity Management Framework

Log management systems shall be monitored and maintained to ensure adequate performance and capacity across all logging domains.

3.6.1 Unified Performance Monitoring

- **Framework-Wide Performance Metrics:**
  - Real-time monitoring of log ingestion rates and processing delays across all domains
  - Storage capacity monitoring with automated alerting for space constraints
  - System performance metrics for search and analysis capabilities across SEC-POL-010 and SEC-POL-011 requirements

  - Network bandwidth utilization for log transmission from all sources
  - Regular performance testing and optimization procedures for integrated logging infrastructure

3.6.2 Coordinated Capacity Planning

- **Integrated Capacity Management:**
  - Annual capacity planning based on business growth and data volume projections across all logging domains
  - Scalability testing for peak load scenarios including authentication surges and data access patterns
  - Archive and disposal procedures for managing storage growth across all log types
  - Cost optimization through data lifecycle management coordinated across SEC-POL-010 and SEC-POL-011 requirements
  - Disaster recovery planning for log management systems supporting all specialized logging domains

4. Standards Compliance

See Annex: Control Mapping

4.2 Policy Coordination References

This framework policy coordinates with specialized logging policies to ensure comprehensive compliance coverage:

- **SEC-POL-010**: Authentication and network security logging requirements including identity management, network communications, and system security events
- **SEC-POL-011**: Data access and compliance logging requirements including ePHI handling, privacy controls, and regulatory compliance activities
- **Cross-Policy Compliance**: Integrated compliance reporting and evidence collection across all logging domains

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Security Officer	Overall responsibility for audit logging framework coordination and integration of SEC-POL-010 and SEC-POL-011 requirements.
IT Security Team	Implementation and daily management of centralized logging infrastructure supporting all specialized logging domains.
System Administrators	Configuration of unified log forwarding and maintenance of shared logging infrastructure across all domains.
Compliance Team	Coordination of compliance requirements across authentication, network, and data access logging domains.
Incident Response Team	Utilization of integrated audit logs from all domains for comprehensive incident investigation and evidence collection.
Legal Team	Legal hold procedures and retention requirement coordination across all logging domains.
Privacy Officer	Coordination of privacy and ePHI logging requirements between framework and specialized policies.
All Workforce Members	Compliance with coordinated logging policies and prompt reporting of suspected security events across all domains.

Authentication and Network Audit Logging Policy (SEC-POL-010)

1. Objective

The objective of this policy is to establish comprehensive audit logging requirements for authentication, authorization, and network security events within **[Company Name]**'s information systems. This policy ensures that user access activities, network communications, and system security events are comprehensively captured, monitored, and analyzed to support incident detection, forensic analysis, and regulatory compliance. This policy focuses specifically on identity management, network security, and system-level security events while coordinating with data access logging requirements defined in SEC-POL-011.

2. Scope

This policy applies to all **[Company Name]** authentication systems, identity management platforms, network devices, security appliances, and infrastructure components that manage user access or network communications. This includes all identity providers, authentication services, network firewalls, VPN systems, intrusion detection systems, and security tools across production, staging, development, and administrative environments. All workforce members, contractors, and third parties with system access are subject to the authentication and network logging requirements defined in this policy.

3. Policy

- **[Company Name]** shall implement comprehensive audit logging and monitoring capabilities for all authentication, authorization, and network security events to provide early detection of unauthorized access attempts, support forensic analysis, and maintain compliance with regulatory requirements as defined in SEC-POL-009.

3.1 Authentication and Authorization Logging

All identity management and authentication systems shall generate detailed audit logs for security-relevant events to provide comprehensive accountability and support incident investigation.

3.1.1 Authentication Event Logging

The following authentication and authorization events shall be logged by all applicable systems:

3.1.1.1 User Authentication Events

Successful and failed user authentication attempts shall be logged with source IP address and user agent information. Account lockout events due to failed authentication attempts or security policy violations shall be logged. Password changes, resets, and expiration events shall be logged with administrative approval tracking. Multi-factor authentication events including setup, usage, and failure scenarios shall be logged. Single sign-on (SSO) authentication events and cross-system authentication propagation shall be logged. Service account and API key authentication events shall be logged with application context.

3.1.1.2 Authorization and Privilege Events

Account creation, modification, deletion, and privilege changes shall be logged with administrative approval tracking. Role assignments and group membership changes shall be logged with effective permission modifications. Privilege escalation and administrative access activities shall be logged with justification and approval documentation. Session establishment, termination, and timeout events shall be logged with session duration and activity tracking. Delegation of administrative privileges and proxy authentication events shall be logged. Emergency access activations and break-glass procedure usage shall be logged.

3.1.1.3 Identity Management System Events

Identity provider configuration changes and federation relationship modifications shall be logged. Authentication policy changes and security parameter modifications shall be logged. Certificate and key management activities for authentication infrastructure shall be logged. Directory service modifications and schema changes affecting user access shall be logged. Integration configuration changes with connected applications and services shall be logged. Backup and recovery operations for identity management systems shall be logged.

3.1.2 Authentication Log Content Standards

All authentication audit log entries shall contain the following minimum information:

3.1.2.1 Temporal and Session Information

Precise timestamp synchronized with authoritative time source (NTP) shall be recorded with millisecond precision. Time zone information shall be included for accurate correlation across geo-

graphic locations. Session identification and correlation identifiers shall be maintained for multi-system authentication flows. Event sequence numbers shall be maintained for authentication session ordering and completeness validation.

3.1.2.2 Identity and Source Context

User identification (username, user ID, email address, or service account identifier) shall be recorded. Source system, IP address, geographic location, and network segment information shall be captured. User agent information, device fingerprinting, and client system identification shall be logged. Authentication method used (password, MFA, certificate, biometric, etc.) shall be documented. Identity provider or authentication service processing the request shall be identified. Referring application or service requesting authentication shall be recorded.

3.1.2.3 Authentication Event Details

Authentication event type and category classification (login, logout, privilege escalation, etc.) shall be documented. Success or failure status shall be recorded with detailed error codes and failure reasons. Risk assessment and fraud detection scores shall be included where available. Policy violations detected during authentication process shall be logged. Security context and privilege level granted or requested shall be documented. Conditional access policy evaluation results and applied restrictions shall be recorded.

3.2 Network Security Event Logging

Comprehensive network security logging shall capture network communications, security events, and traffic patterns to support threat detection and investigation.

3.2.1 Network Communication Logging

- **Network Traffic and Access Events:**
  - Firewall rule evaluations with allow/deny decisions and rule matching information
  - Network connection establishment and termination events with duration and data transfer metrics
  - VPN connections and remote access activities with endpoint information and tunnel characteristics
  - Network access control (NAC) decisions and device compliance validation events

  - Wireless network connections and authentication events with device and location information
  - Network segmentation boundary crossings and micro-segmentation policy enforcement
- **Security Appliance Events:**
  - Intrusion detection and prevention system alerts with attack signature and severity information
  - Web application firewall (WAF) events including blocked requests and security policy violations
  - Data loss prevention (DLP) system alerts with data classification and transfer attempt details
  - Anti-malware and antivirus detection events with threat classification and response actions
  - Network behavior analysis anomalies and baseline deviation alerts
  - Security orchestration and automated response (SOAR) actions and playbook executions
- **Network Infrastructure Events:**
  - Network device configuration changes and administrative access activities
  - Routing table modifications and network topology changes
  - Network service availability and performance threshold violations
  - DNS query logging for security analysis and threat detection
  - Certificate validation events for secure communications
  - Network time protocol (NTP) synchronization events and time source validation

3.2.2 Network Log Content Standards

All network security audit log entries shall contain the following minimum information:

- **Network Communication Context:**
  - Source and destination IP addresses, ports, and protocol information
  - Network zone or segment classification for both source and destination
  - VLAN information and network policy context
  - Bandwidth utilization and data transfer metrics
  - Communication duration and session state information
  - Quality of service (QoS) classification and priority handling
- **Security and Policy Context:**
  - Security policy rule or signature that triggered the event

  - Risk assessment and threat intelligence correlation results
  - Geolocation information for source and destination addresses
  - Network device or security appliance generating the event
  - Administrative action or automatic response taken
  - Integration with threat intelligence feeds and reputation services

3.3 System Security Event Logging

System-level security events shall be comprehensively logged to provide visibility into infrastructure security and system integrity.

3.3.1 System Security Events

- **System and Service Security Events:**
  - System startup, shutdown, and configuration changes with administrator identification
  - Critical system process and service status changes with impact assessment
  - Security software installation, updates, and configuration modifications
  - System resource utilization anomalies and performance threshold violations
  - Kernel and operating system security events including privilege escalation attempts
  - Container and virtualization security events including escape attempts and resource violations
- **Infrastructure Security Events:**
  - Cloud infrastructure configuration changes and resource provisioning activities
  - Infrastructure-as-code deployment events and automation system activities
  - Backup and recovery operations with data integrity validation results
  - Encryption and key management activities with key lifecycle events
  - Certificate management events including issuance, renewal, and revocation
  - Compliance scanning results and configuration drift detection events

3.3.2 Integration with Data Access Logging

This policy coordinates with SEC-POL-011 (Data Access and Compliance Audit Logging Policy) to ensure comprehensive coverage:

- **Coordination Points:**
  - Authentication events shall include session identifiers for correlation with data access

events logged under SEC-POL-011
  - Network communication logs shall provide context for data transmission events captured under SEC-POL-011
  - System security events shall include references to data processing activities subject to SEC-POL-011 requirements
  - Cross-policy event correlation shall be maintained through common session and transaction identifiers
- **Scope Boundaries:**
  - This policy focuses on user authentication, network communications, and system security events
  - SEC-POL-011 addresses data access, modification, ePHI handling, and regulatory compliance events
  - Shared logging infrastructure and retention requirements are coordinated between both policies
  - Incident response procedures integrate events from both authentication/network and data access domains

3.4 Log Management and Monitoring

Authentication and network security logs shall be managed with appropriate collection, storage, and monitoring procedures coordinated with overall audit logging requirements.

3.4.1 Centralized Log Collection

- **Authentication Log Aggregation:**
  - All authentication systems shall forward security logs to centralized Security Information and Event Management (SIEM) system with real-time transmission
  - Identity provider logs shall be integrated including SAML assertions, OAuth token events, and federation activities
  - Multi-factor authentication system logs shall be centrally collected including hardware token, mobile app, and biometric events
  - Log transmission shall use encrypted channels (TLS 1.3 or equivalent) with mutual authentication
  - Redundant log collection paths shall be implemented for critical authentication infrastructure

- **Network Security Log Integration:**
  - Network device logs shall be forwarded to centralized logging platform using standardized formats (syslog, SNMP, etc.)
  - Security appliance logs shall be integrated including firewall, IPS, WAF, and DLP system events
  - Cloud network security logs shall be collected from AWS VPC Flow Logs, Azure Network Security Group logs, and GCP VPC Flow Logs
  - Network monitoring tools shall provide log integration including network behavior analysis and traffic analytics
  - Real-time log forwarding required for security events classified as Critical or High priority

3.4.2 Automated Monitoring and Analysis

- **Real-Time Authentication Monitoring:**
  - 24/7 automated monitoring of authentication failures and brute force attack patterns
  - Behavioral analysis for unusual authentication patterns including impossible travel and off-hours access
  - Automated correlation of authentication events across multiple systems and applications
  - Integration with threat intelligence feeds for known malicious IP addresses and attack patterns
  - Automated response capabilities for account lockouts and suspicious authentication activities
- **Network Security Event Analysis:**
  - Continuous monitoring of network traffic patterns and anomaly detection
  - Automated analysis of security appliance alerts with false positive reduction
  - Real-time correlation of network events with authentication activities
  - Threat hunting capabilities using network communication patterns and indicators
  - Integration with external threat intelligence for IP reputation and domain analysis

3.4.3 Authentication and Network Monitoring Implementation

- **Cloud-Native Authentication Analytics:**
  - AWS CloudTrail integration for API authentication and authorization events with automated analysis of admin access patterns, unusual API usage, and cross-account activities
  - Azure Active Directory logs integration for user authentication, conditional access, and

risk detection events with automated correlation of sign-in patterns and anomaly detection
  - Google Cloud Identity and Access Management (IAM) audit logs for authentication and authorization events with automated analysis of service account usage and privilege escalation
  - Multi-cloud authentication event correlation for federated identity scenarios with standardized event formatting and cross-platform analysis
- **Network Security Analytics and Correlation:**
  - AWS VPC Flow Logs analysis with automated threat detection including botnet communication, data exfiltration patterns, and lateral movement detection
  - Azure Network Security Group logs correlation with security events including automated blocking of malicious traffic and threat intelligence integration
  - Google Cloud VPC Flow Logs integration with security analytics including machine learning-based anomaly detection and automated incident creation
  - Cross-cloud network security event correlation with standardized threat classification and automated response capabilities
- **Managed Security Service Provider (MSSP) Integration for Authentication and Network Events:**
  - MSSP 24/7 monitoring of authentication events including failed login analysis, privilege escalation detection, and account compromise indicators
  - Network security event analysis by MSSP including traffic pattern analysis, threat hunting, and incident correlation with authentication activities
  - Automated escalation of critical authentication and network security events to internal security team with detailed analysis and recommended response actions
  - Integration of MSSP analysis with internal incident response procedures including evidence collection and containment recommendations

3.5 Incident Response Integration

Authentication and network audit logs shall provide comprehensive support for security incident detection, investigation, and response activities.

3.5.1 Authentication Incident Detection

- **Detection Capabilities:**

  - Automated correlation rules for authentication-based attack patterns including credential stuffing, password spraying, and account takeover attempts
  - Baseline deviation detection for user authentication behavior including unusual locations, devices, and access patterns
  - Privilege escalation detection through authentication and authorization monitoring
  - Insider threat detection through authentication pattern analysis and privilege usage monitoring
  - Integration with external threat intelligence for known compromised credentials and attack indicators
- **Response Support:**
  - Rapid authentication log search and analysis capabilities for incident investigation
  - Automated evidence collection for authentication-related security incidents
  - Timeline reconstruction capabilities for user access and authentication events
  - Integration with identity management systems for rapid account response and containment
  - Chain of custody procedures for authentication log-based evidence

3.5.2 Network Security Incident Response

- **Network Incident Detection:**
  - Automated correlation of network traffic patterns with known attack signatures
  - Lateral movement detection through network communication analysis
  - Data exfiltration detection through network traffic pattern analysis
  - Command and control communication detection through DNS and network flow analysis
  - Network-based insider threat detection through traffic pattern and access analysis
- **Response Capabilities:**
  - Network-based incident containment through automated traffic blocking and isolation
  - Network forensics capabilities for incident investigation and evidence collection
  - Integration with network security appliances for automated response and containment
  - Coordination with authentication systems for network-based account response
  - Network traffic capture and analysis for detailed incident investigation

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Security Officer	Overall responsibility for authentication and network audit logging program coordination with SEC-POL-011 requirements.
Identity and Access Management Team	Implementation and management of authentication logging systems, user access monitoring, and identity security events.
Network Security Team	Configuration and management of network security logging, traffic analysis, and network-based threat detection.
System Administrators	Configuration of authentication system logging, network device log forwarding, and maintenance of logging infrastructure.
Security Operations Center (SOC)	24/7 monitoring of authentication and network security events, alert analysis, and incident escalation.
Incident Response Team	Utilization of authentication and network logs for incident investigation, evidence collection, and forensic analysis.
Compliance Team	Regular audit of authentication and network logging practices and coordination with SEC-POL-011 compliance requirements.
All Workforce Members	Compliance with authentication and network logging policies and prompt reporting of suspected security events.

Data Access and Compliance Audit Logging Policy (SEC-POL-011)

1. Objective

The objective of this policy is to establish comprehensive audit logging requirements for data access, modification, and regulatory compliance activities within **[Company Name]**'s information systems. This policy ensures that access to electronic Protected Health Information (ePHI), sensitive data, and compliance-related activities are comprehensively captured, monitored, and analyzed to support regulatory compliance, data protection, and forensic analysis. This policy focuses specifically on data handling, privacy protection, and compliance reporting while coordinating with authentication and network logging requirements defined in SEC-POL-010.

2. Scope

This policy applies to all **[Company Name]** information systems, applications, databases, and services that process, store, or transmit sensitive data, ePHI, or compliance-related information. This includes all production databases, data processing applications, data analytics platforms, backup systems, and data transmission services across all environments. All workforce members, contractors, and third parties with access to sensitive data are subject to the data access and compliance logging requirements defined in this policy.

3. Policy

- **[Company Name]** shall implement comprehensive audit logging and monitoring capabilities for all data access, modification, and compliance activities to ensure regulatory compliance, data protection, and forensic analysis capabilities as defined in SEC-POL-009 and coordinated with authentication and network logging requirements in SEC-POL-010.

3.1 Data Access and Modification Logging

All systems processing sensitive data shall generate detailed audit logs for data-related security events to provide comprehensive accountability and support regulatory compliance.

3.1.1 Data Access Event Logging

The following data access and modification events shall be logged by all applicable systems:

- **Electronic Protected Health Information (ePHI) Access:**

  - All access to ePHI including read, view, print, and export activities with patient identifier correlation
  - ePHI query activities including database searches, report generation, and data analytics operations
  - ePHI modification events including create, update, delete, and merge operations with before/after values where feasible
  - ePHI transmission activities including email, file transfer, API calls, and system-to-system communications
  - Bulk ePHI operations including batch processing, data migration, and system integration activities
  - ePHI backup and recovery operations including data restoration and archive access
- **Sensitive Data Handling Events:**
  - Access to personally identifiable information (PII), financial data, and other classified data categories
  - Data classification and labeling activities including sensitivity assessment and protection application
  - Data encryption and decryption activities with key usage tracking and access justification
  - Data sharing and collaboration activities including external partner access and third-party data processing
  - Data retention and disposal activities including automated purging and manual data destruction
  - Data loss prevention (DLP) policy violations and data leakage prevention actions
- **Database and Application Data Events:**
  - Database query execution including SELECT, INSERT, UPDATE, and DELETE operations with query details
  - Stored procedure and function executions with parameter values and execution results
  - Database schema modifications including table alterations, index changes, and permission modifications
  - Application-level data access including user interface interactions and API-based data operations
  - Data export and import operations including file downloads, uploads, and bulk data transfers
  - Data synchronization and replication activities including cross-system data consistency operations

3.1.2 Data Event Log Content Standards

All data access audit log entries shall contain the following minimum information:

- **Data Context and Classification:**
  - Data classification level (Public, Internal, Confidential, Restricted, ePHI) and handling requirements
  - Specific data elements or fields accessed with field-level granularity where technically feasible
  - Patient identifiers or subject identifiers for ePHI and PII access tracking
  - Data volume or record count for bulk operations and batch processing activities
  - Data retention requirements and regulatory classification affecting the accessed information
  - Business justification or workflow context for data access activities
- **Access Details and Metadata:**
  - User identification with role, department, and business justification for data access
  - Application or system component facilitating the data access with version and configuration information
  - SQL queries, API calls, or specific operations performed on the data
  - Success or failure status with detailed error codes and data validation results
  - Data transformation or processing activities performed during access
  - Integration with authentication events from SEC-POL-010 through session correlation identifiers

3.2 Compliance and Regulatory Logging

Comprehensive compliance logging shall capture activities required for regulatory compliance and audit support.

3.2.1 HIPAA Compliance Logging

- **HIPAA Security Rule Compliance Events:**
  - Administrative safeguards implementation including security officer activities and workforce training records
  - Physical safeguards validation including facility access controls and workstation security measures

  - Technical safeguards operation including access controls, audit controls, and transmission security
  - Risk assessment and security incident activities related to ePHI protection and breach prevention
  - Business associate agreement compliance monitoring including third-party access and data processing activities
  - Minimum necessary rule compliance tracking including access justification and data minimization activities
- **HIPAA Privacy Rule Compliance Events:**
  - Patient consent and authorization activities including consent capture, modification, and withdrawal
  - Notice of Privacy Practices distribution and acknowledgment tracking
  - Patient rights exercised including access requests, amendment requests, and accounting of disclosures
  - Uses and disclosures of ePHI including purpose, recipient, and authorization basis
  - Complaints and privacy-related inquiries including investigation and resolution activities
  - Marketing and fundraising communications including opt-out preferences and consent management

3.2.2 SOC 2 and Industry Compliance Logging

- **SOC 2 Trust Services Criteria Compliance:**
  - Security controls operation including logical access, system monitoring, and change management activities
  - Availability controls validation including system monitoring, backup operations, and disaster recovery testing
  - Confidentiality controls implementation including data classification, encryption, and access restrictions
  - Processing integrity controls including system monitoring, data validation, and error handling
  - Privacy controls operation including notice, choice, access, and accountability requirements
- **Industry-Specific Compliance Events:**
  - HITRUST CSF control implementation and validation activities including assessment preparation and remediation tracking

  - Payment Card Industry (PCI) compliance activities if applicable including cardholder data protection and network security
  - State privacy law compliance including CCPA, GDPR, and other applicable privacy regulations
  - Industry-specific reporting requirements including regulatory submissions and compliance certifications
  - Third-party audit and assessment activities including external auditor access and evidence provision

3.3 Data Protection and Privacy Logging

Comprehensive data protection logging shall ensure privacy controls and data handling compliance.

3.3.1 Privacy Controls Logging

- **Data Subject Rights Management:**
  - Data subject access requests including request receipt, processing, and fulfillment activities
  - Right to rectification requests including data correction and validation procedures
  - Right to erasure (right to be forgotten) requests including data deletion and verification procedures
  - Data portability requests including data extraction and format conversion activities
  - Consent management activities including consent capture, withdrawal, and preference management
  - Privacy preference and opt-out management including marketing communications and data processing restrictions
- **Data Processing and Transfer Events:**
  - Cross-border data transfers including adequacy determinations and safeguard implementations
  - Data processing purpose changes including notice provision and consent management
  - Third-party data sharing activities including data sharing agreements and purpose limitations
  - Data minimization activities including automated data reduction and retention policy enforcement
  - Pseudonymization and anonymization activities including privacy-enhancing technology

implementation
  - Data breach detection and notification activities including breach assessment and regulatory reporting

3.3.2 Data Lifecycle Management Logging

- **Data Retention and Disposal:**
  - Automated data retention policy enforcement including retention schedule application and data aging
  - Data disposal activities including secure deletion, media destruction, and disposal certification
  - Legal hold implementation including litigation hold application and data preservation
  - Archive and backup data management including long-term storage and retrieval activities
  - Data migration and system decommissioning activities including data transfer and legacy system retirement
  - Data quality and integrity validation including data validation, cleansing, and error correction

3.4 Compliance Monitoring and Reporting

Data access and compliance logs shall be continuously monitored and analyzed to ensure regulatory compliance and data protection.

3.4.1 Real-Time Compliance Monitoring

- **Automated Compliance Monitoring:**
  - 24/7 automated monitoring of ePHI access patterns and policy compliance
  - Real-time detection of data access policy violations and unauthorized data handling
  - Automated correlation of data access events with authentication activities from SEC-POL-010
  - Behavioral analysis for unusual data access patterns including bulk downloads and off-hours access
  - Integration with data loss prevention (DLP) systems for real-time data protection
  - Automated response capabilities for high-risk data access scenarios
- **Compliance Alert Management:**

  - Severity-based compliance alert classification (Critical, High, Medium, Low) with automated escalation
  - Real-time alerting for ePHI access violations and privacy rule breaches
  - Automated notification for data subject rights requests and regulatory compliance deadlines
  - Integration with incident response procedures for compliance violations
  - Automated reporting to Privacy Officer and Compliance Team for regulatory events

3.4.2 Compliance Reporting and Analytics

- **Regulatory Compliance Reporting:**
  - Automated generation of HIPAA compliance reports including ePHI access summaries and security incident reports
  - SOC 2 compliance evidence collection including control operation documentation and exception reporting
  - HITRUST CSF assessment support including control evidence and implementation documentation
  - Privacy regulation compliance reporting including data processing activities and data subject rights fulfillment
  - Breach notification support including incident documentation and regulatory filing assistance
- **Data Analytics and Insights:**
  - ePHI access pattern analysis including user behavior analytics and anomaly detection
  - Data processing trend analysis including volume patterns and compliance metrics
  - Privacy rights request analysis including request patterns and fulfillment metrics
  - Compliance program effectiveness measurement including policy violation trends and remediation success
  - Executive dashboard with key compliance metrics and regulatory status indicators

3.4.3 Data Access and Compliance Monitoring Implementation

- **Cloud-Native Data Analytics and Compliance:**
  - AWS CloudTrail data events for S3 bucket access with automated ePHI access pattern analysis and compliance monitoring
  - AWS CloudWatch for database activity monitoring with automated detection of unusual

data access patterns and bulk operations
  - Azure SQL Database auditing for ePHI access tracking with automated compliance reporting and privacy controls monitoring
  - Google Cloud Audit Logs for BigQuery and Cloud SQL with automated data access analysis and regulatory compliance validation
  - Cross-cloud data access correlation with standardized compliance event classification and automated regulatory reporting
- **Database Activity Monitoring (DAM) and Data Security:**
  - Real-time database activity monitoring for all ePHI and sensitive data access with automated policy enforcement and compliance validation
  - Automated SQL query analysis for data access pattern detection including bulk operations, unusual queries, and privilege escalation attempts
  - Database security policy enforcement including access controls, encryption validation, and data masking compliance
  - Integration with data loss prevention (DLP) systems for real-time data protection and compliance monitoring
  - Automated evidence collection for SOC 2 and HIPAA audits including data access reports and control operation documentation
- **Privacy and Compliance Management Integration:**
  - Automated HIPAA compliance monitoring including ePHI access tracking, minimum necessary rule compliance, and business associate oversight
  - Privacy rights management including automated data subject request processing, consent management, and privacy preference enforcement
  - Regulatory reporting automation including breach notification assistance, compliance reporting, and audit evidence collection
  - Integration with privacy management platforms including OneTrust, TrustArc, or similar solutions for comprehensive privacy program management
  - Automated compliance dashboard including key performance indicators, regulatory deadlines, and compliance status tracking

3.5 Integration with Authentication and Network Logging

This policy coordinates with SEC-POL-010 (Authentication and Network Audit Logging Policy) to ensure comprehensive security and compliance coverage.

3.5.1 Cross-Policy Coordination

- **Event Correlation and Integration:**
  - Data access events shall include session identifiers for correlation with authentication events from SEC-POL-010
  - Database connections and API calls shall be correlated with network communication logs from SEC-POL-010
  - User data access patterns shall be analyzed in context of authentication behavior and network activity
  - Compliance violations shall trigger coordinated review of authentication, network, and data access logs
  - Incident response procedures shall integrate evidence from both authentication/network and data access domains
- **Shared Infrastructure and Standards:**
  - Common log management infrastructure shared with SEC-POL-010 for centralized analysis and correlation
  - Consistent log format standards and retention policies coordinated between authentication, network, and data logging
  - Integrated monitoring and alerting platforms combining authentication, network, and data access security events
  - Unified incident response procedures incorporating evidence from all logging domains
  - Coordinated compliance reporting combining authentication controls with data protection requirements

3.6 Incident Response and Forensics Support

Data access and compliance logs shall provide comprehensive support for security incident investigation and regulatory compliance validation.

3.6.1 Data Breach Investigation Support

- **Breach Detection and Analysis:**
  - Automated detection of potential data breaches through data access pattern analysis
  - Evidence collection for breach notification requirements including affected data identification and access timeline reconstruction
  - Integration with breach response procedures including impact assessment and notifica-

tion requirements
  - Forensic analysis capabilities for data access incidents including timeline reconstruction and evidence preservation
  - Coordination with legal and compliance teams for breach response and regulatory notification
- **Compliance Investigation Support:**
  - Rapid search and analysis capabilities for compliance investigations and audit support
  - Evidence collection for regulatory inquiries including data access documentation and control operation evidence
  - Timeline reconstruction for compliance violations including user activity and system behavior analysis
  - Integration with legal hold procedures for litigation and regulatory investigation support
  - Chain of custody procedures for compliance-related evidence and audit documentation

4. Standards Compliance

See Annex: Control Mapping

5. Definitions

See Annex: Glossary

6. Responsibilities

Role	Responsibility
Privacy Officer	Overall responsibility for data access and compliance audit logging program and coordination with SEC-POL-010 requirements.
Data Protection Team	Implementation and management of data access logging systems, privacy controls monitoring, and compliance event analysis.
Database Administrators	Configuration of database activity monitoring, data access logging, and maintenance of data logging infrastructure.

Role	Responsibility
Compliance Team	Regular audit of data access and compliance logging practices, regulatory reporting, and audit evidence collection.
Security Operations Center (SOC)	24/7 monitoring of data access security events, compliance violations, and privacy-related incident escalation.
Incident Response Team	Utilization of data access logs for breach investigation, evidence collection, and regulatory notification support.
Legal Team	Legal hold procedures, regulatory compliance guidance, and coordination with privacy and data protection requirements.
All Workforce Members	Compliance with data access and privacy logging policies and prompt reporting of suspected data security events.

AI Development and Deployment Security Policy (SEC-POL-012)

1. Objective

The objective of this policy is to establish comprehensive security requirements for the development, deployment, and operation of Artificial Intelligence (AI) and Machine Learning (ML) technologies at **[Company Name]**. This policy ensures that AI systems are developed with appropriate security controls, deployed through secure processes, and operated with robust security measures to protect the confidentiality, integrity, and availability of company information and electronic Protected Health Information (ePHI). This policy focuses specifically on technical security requirements for AI development lifecycles, deployment security, and operational security while coordinating with AI ethics and compliance requirements defined in SEC-POL-013.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, and third parties involved in the development, deployment, configuration, or technical management of AI and ML technologies. It encompasses all AI development activities including model creation, training, validation, deployment, and maintenance. This policy covers both internally developed AI systems and the technical integration of third-party AI services, regardless of deployment model (cloud-based, on-premises, or hybrid), and applies to all technical aspects of AI system security including infrastructure, data pipelines, model protection, and operational monitoring.

3. Policy

- **[Company Name]** shall implement comprehensive security controls throughout the AI development and deployment lifecycle to ensure AI systems are developed, deployed, and operated securely while protecting sensitive information and maintaining system integrity as coordinated with AI ethics and compliance requirements in SEC-POL-013.

3.1 AI Development Security Framework

Secure development practices shall be integrated throughout the AI development lifecycle to ensure AI systems are built with appropriate security controls and protections.

3.1.1 Secure AI Development Lifecycle

- **Security-by-Design Principles:**
  - Security requirements shall be integrated into AI development lifecycle from initial design through deployment and maintenance
  - Threat modeling shall be conducted for all AI systems during the design phase to identify security risks and mitigation strategies
  - Code review and security testing shall be mandatory for all AI applications and model implementations
  - Vulnerability assessment of AI frameworks, libraries, and dependencies shall be performed before integration
  - Secure coding practices shall be applied to all AI model development and implementation activities
- **AI Development Environment Security:**
  - Isolated development environments with restricted network access for AI model training and experimentation
  - Version control and change management for AI systems including models, training data, and configuration files
  - Secure development workstations with endpoint protection and monitoring for AI developers
  - Access controls and authentication for AI development tools, platforms, and repositories
  - Development environment monitoring and logging for security events and policy compliance

3.1.2 AI Model Security and Protection

- **Model Intellectual Property Protection:**
  - Protection of AI models as intellectual property and trade secrets with appropriate classification and handling
  - Secure storage and versioning of AI models with encryption and access controls
  - Model watermarking and fingerprinting to detect unauthorized use or distribution
  - Secure backup and recovery procedures for AI models and related intellectual property
  - Legal protection measures including confidentiality agreements for AI model access
- **Adversarial Attack Prevention:**
  - Adversarial attack testing during AI model development and validation phases

  - Input validation and sanitization to prevent adversarial inputs and prompt injection attacks
  - Model robustness testing against various attack vectors including poisoning, evasion, and extraction
  - Defensive mechanisms including adversarial training and input monitoring
  - Regular security assessments of AI models for emerging attack techniques

3.2 AI Data Security and Protection

Comprehensive data security controls shall protect AI training data, model inputs, and outputs throughout the AI system lifecycle.

3.2.1 AI Training Data Security

- **Training Dataset Protection:**
  - Encryption of all AI training datasets containing sensitive information using approved encryption algorithms
  - Secure data pipelines for AI model training with authenticated and encrypted data transmission
  - Data lineage tracking and documentation for all AI datasets including source, transformations, and usage
  - Access controls and monitoring for AI training data with role-based permissions and audit logging
  - Secure data preparation environments with isolation from production systems
- **Training Data Lifecycle Management:**
  - Data quality and integrity assessments for AI training datasets with validation and verification procedures
  - Secure deletion of training data when no longer needed in accordance with data retention policies
  - Data versioning and change management for training datasets with immutable storage where feasible
  - Regular data refresh and update procedures for AI training datasets with security validation
  - Backup and recovery procedures for critical AI training data with appropriate security controls

3.2.2 AI System Data Protection

- **Real-Time Data Security:**
  - Encryption of all data at rest and in transit for AI systems processing sensitive information
  - Real-time data protection for AI system inputs and outputs with data loss prevention controls
  - Input validation and sanitization to prevent data injection attacks and model manipulation
  - Output filtering and validation to prevent data leakage and unauthorized information disclosure
  - Data masking and tokenization for sensitive data used in AI system testing and development
- **AI Data Monitoring and Logging:**
  - Comprehensive monitoring and logging of all AI system data interactions and processing activities
  - Data access logging for AI systems handling ePHI and other sensitive information
  - Anomaly detection for unusual data access patterns or volume in AI systems
  - Integration with data loss prevention (DLP) systems for AI-generated content and outputs
  - Incident detection and alerting for AI data security events and policy violations

3.3 AI Infrastructure and Platform Security

Robust infrastructure security controls shall protect AI systems, platforms, and supporting infrastructure from security threats.

3.3.1 AI Platform Security

- **AI Infrastructure Hardening:**
  - Security baselines and hardening standards for AI development and deployment platforms
  - Container security for AI workloads including image scanning, runtime protection, and network policies
  - Cloud security configurations for AI services including identity management, network controls, and monitoring
  - GPU and specialized hardware security for AI compute resources with firmware validation and monitoring

  - Infrastructure as code (IaC) security for AI platform deployments with configuration management and drift detection
- **AI Service Security Controls:**
  - API security controls for AI service integrations including authentication, authorization, and rate limiting
  - Service mesh security for AI microservices with mutual TLS and network segmentation
  - Load balancer and gateway security for AI service endpoints with SSL/TLS termination and monitoring
  - Database security for AI metadata and result storage with encryption and access controls
  - Message queue security for AI processing pipelines with encryption and access management

3.3.2 AI System Access Controls

- **Authentication and Authorization:**
  - Multi-factor authentication required for all AI system access including development, deployment, and operational access
  - Role-based access control (RBAC) for AI systems and platforms with principle of least privilege
  - Privileged access management (PAM) for AI system administration with session monitoring and recording
  - Service account management for AI system integrations with automated credential rotation
  - API key and token management for AI service access with secure storage and rotation
- **Access Monitoring and Management:**
  - Regular access reviews and recertification for AI system users with automated workflow and approval
  - Just-in-time (JIT) access for temporary AI system administration and emergency access
  - Access attempt monitoring and alerting for failed authentication and unauthorized access attempts
  - Session management and timeout controls for AI system access with automatic logout procedures
  - Integration with identity and access management (IAM) systems for centralized access control

3.4 AI Deployment and Operations Security

Secure deployment practices and operational security controls shall ensure AI systems are deployed and operated with appropriate security measures.

3.4.1 Secure AI Deployment

- **Deployment Pipeline Security:**
  - Secure CI/CD pipelines for AI model deployment with automated security testing and validation
  - Model validation and testing procedures before production deployment including security and performance testing
  - Staged deployment approach with security validation at each stage including development, staging, and production
  - Automated rollback procedures for AI model failures or security issues with rapid recovery capabilities
  - Deployment approval gates for production AI systems with security team validation and sign-off
- **AI Model Deployment Controls:**
  - Model signing and integrity verification for deployment processes to prevent tampering and unauthorized modifications
  - Canary deployment and A/B testing for new AI models with gradual rollout and monitoring
  - Environment promotion controls with security validation between development, staging, and production
  - Configuration management for AI model deployment with version control and change tracking
  - Deployment monitoring and alerting for AI model deployment failures and security events

3.4.2 AI Operations Security

- **Continuous Security Monitoring:**
  - Real-time monitoring of AI system performance, security events, and anomalous behavior
  - Behavioral analysis and anomaly detection for AI system operations with automated alerting

  - Security event correlation for AI systems with integration to Security Operations Center (SOC)
  - Threat detection and response capabilities specific to AI systems and attack vectors
  - Integration with security information and event management (SIEM) systems for centralized monitoring
- **AI System Maintenance Security:**
  - Patch management for AI frameworks, libraries, and dependencies with security priority assessment
  - Regular security assessments and penetration testing of AI systems and infrastructure
  - Model retraining and update procedures with security validation and approval processes
  - Performance monitoring and capacity management for AI systems with security impact assessment
  - Incident response procedures specific to AI security events with specialized response capabilities

3.5 AI Security Monitoring and Incident Response

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

3.5.1 AI Security Monitoring

- **Model Performance and Security Monitoring:**
  - Continuous monitoring of AI model accuracy, performance, and drift with security impact assessment
  - Input and output monitoring for AI systems to detect adversarial attacks and anomalous behavior
  - Model behavior analysis to identify potential security issues, bias, or performance degradation
  - User interaction monitoring for AI systems with pattern analysis and anomaly detection
  - Integration with application performance monitoring (APM) tools for comprehensive AI system visibility
- **AI Security Metrics and Alerting:**
  - Key security indicators (KSIs) for AI system security including attack detection, access violations, and performance anomalies

  - Automated alerting for AI security events with severity classification and escalation procedures
  - Security dashboard and reporting for AI systems with executive visibility and compliance tracking
  - Trend analysis and reporting for AI security metrics with proactive risk identification
  - Integration with business intelligence and reporting tools for AI security insights

3.5.2 AI Incident Response

- **AI-Specific Incident Response:**
  - Specialized incident response procedures for AI security events including model compromise, data breaches, and adversarial attacks
  - AI incident classification and severity assessment with specialized response teams and procedures
  - Evidence collection and forensic analysis for AI security incidents with model and data preservation
  - Containment and mitigation procedures for AI security incidents with rapid response capabilities
  - Recovery and restoration procedures for AI systems with business continuity considerations
- **AI Incident Coordination:**
  - Integration with organizational incident response procedures including communication and escalation
  - Coordination with AI ethics and compliance teams for incidents involving bias, fairness, or regulatory issues
  - Legal and regulatory notification procedures for AI incidents with compliance team coordination
  - Post-incident review and improvement for AI security events with lessons learned integration
  - Cross-functional incident response training including AI-specific scenarios and tabletop exercises

3.6 Third-Party AI Service Security

Security controls for third-party AI services shall ensure appropriate security standards and protections for external AI integrations.

3.6.1 AI Vendor Security Assessment

- **Vendor Security Evaluation:**
  - Comprehensive security assessment of third-party AI vendors including infrastructure, data protection, and compliance
  - Security questionnaires and audits for AI service providers with documented security controls validation
  - Penetration testing and security validation of third-party AI services where feasible
  - Geographic data location restrictions and data sovereignty requirements for AI service providers
  - Service level agreements (SLAs) including security requirements, incident response, and breach notification

3.6.2 AI Service Integration Security

- **Secure Integration Practices:**
  - API security controls for third-party AI service integrations including authentication, encryption, and monitoring
  - Data minimization and protection for information sent to third-party AI services
  - Output validation and filtering for third-party AI service responses with security and content filtering
  - Network security controls for AI service communications including VPN, firewall, and monitoring
  - Contract and legal protections for AI service usage including data protection and liability clauses

3.7 Coordination with AI Ethics and Compliance

This policy coordinates with SEC-POL-013 (AI Ethics and Compliance Policy) to ensure comprehensive coverage of AI security, ethics, and compliance requirements.

3.7.1 Policy Integration Points

- **Cross-Policy Coordination:**
  - Security requirements shall support ethical AI principles and compliance obligations defined in SEC-POL-013
  - Technical security controls shall enable audit trails and monitoring required for AI governance and compliance
  - Incident response procedures shall coordinate with ethics and compliance teams for comprehensive AI incident management
  - Development security processes shall integrate bias testing and fairness validation requirements from SEC-POL-013
  - Vendor security assessments shall include ethical AI and compliance evaluation criteria from SEC-POL-013

4. Standards Compliance

This AI Development and Deployment Security Policy aligns with and supports compliance requirements from multiple regulatory frameworks while coordinating with AI ethics and compliance requirements in SEC-POL-013.

4.1 Regulatory Compliance Mapping

Policy Section	Standard/Framework	Control Reference
3.1	HITRUST CSF v11.2.0	09.b - System Development Controls
3.1	HITRUST CSF v11.2.0	06.a - Configuration Management Policy
3.2	HITRUST CSF v11.2.0	19.a - Data Protection and Privacy Policy
3.2	HITRUST CSF v11.2.0	09.a - Data Protection Policy
3.3	HITRUST CSF v11.2.0	08.a - Network Protection Policy
3.3	HITRUST CSF v11.2.0	11.a - Access Control Policy

Policy Section	Standard/Framework	Control Reference
3.4	HITRUST CSF v11.2.0	06.b - Change Management
3.5	HITRUST CSF v11.2.0	15.a - Incident Response Policy
3.5	HITRUST CSF v11.2.0	12.c - Log Monitoring
3.6	HITRUST CSF v11.2.0	14.a - Third Party Assurance
3.2	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Information Access Management
3.2	HIPAA Security Rule	45 CFR § 164.312(a)(2)(iv) - Encryption and Decryption
3.5	HIPAA Security Rule	45 CFR § 164.312(b) - Audit Controls
3.6	HIPAA Security Rule	45 CFR § 164.314(a)(1) - Business Associate Contracts
3.1, 3.4	SOC 2 Trust Services Criteria	CC8.1 - System Development
3.3	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.2	SOC 2 Trust Services Criteria	CC6.7 - Data Transmission and Disposal
3.5	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
3.1	NIST Cybersecurity Framework	PR.PT - Protective Technology
3.2	NIST Cybersecurity Framework	PR.DS - Data Security
3.5	NIST Cybersecurity Framework	DE.CM - Security Continuous Monitoring
3.5	NIST Cybersecurity Framework	RS.RP - Response Planning

5. Definitions

- **Adversarial Attack:** Deliberate attempts to manipulate AI systems through crafted inputs designed to cause incorrect outputs or behavior.

- **AI Development Lifecycle:** The complete process of developing AI systems from initial design through deployment and maintenance.
- **API Security:** Security controls and measures applied to Application Programming Interfaces to protect data and functionality.
- **Model Drift:** Degradation in AI model performance over time due to changes in underlying data patterns or distributions.
- **Model Signing:** Cryptographic process to verify the integrity and authenticity of AI models.
- **Prompt Injection:** Attack technique where malicious inputs are designed to manipulate AI system behavior through crafted prompts.
- **Training Data Poisoning:** Attack where malicious data is introduced into training datasets to compromise AI model behavior.

6. Responsibilities

Role	Responsibility
AI Security Team	Implementation and management of AI security controls, AI system security monitoring, and coordination with SEC-POL-013 requirements.
Data Scientists/AI Engineers	Development of secure AI systems, implementation of security controls in AI development, and coordination with AI ethics requirements.
DevOps/MLOps Engineers	Secure deployment and operations of AI systems, CI/CD pipeline security, and infrastructure protection for AI platforms.
IT Security Team	Integration of AI security with enterprise security controls, incident response for AI security events, and vendor security assessments.
System Administrators	Configuration and maintenance of secure AI infrastructure, access control management, and monitoring of AI system security.

Role	Responsibility
Security Operations Center (SOC)	24/7 monitoring of AI security events, incident detection and response, and coordination with AI development teams.
Compliance Team	Coordination of AI security compliance requirements with SEC-POL-013 and regulatory validation of AI security controls.
All AI Development Staff	Implementation of secure development practices, compliance with AI security policies, and coordination with AI ethics and compliance teams.

AI Ethics and Compliance Policy (SEC-POL-013)

1. Objective

The objective of this policy is to establish comprehensive ethical guidelines and regulatory compliance requirements for the use of Artificial Intelligence (AI) and Machine Learning (ML) technologies at **[Company Name]**. This policy ensures that AI systems are developed, deployed, and used in accordance with ethical principles, regulatory requirements, and responsible AI practices while protecting individual rights, preventing bias and discrimination, and maintaining transparency and accountability. This policy focuses specifically on AI governance, ethical principles, regulatory compliance, and acceptable use guidelines while coordinating with technical security requirements defined in SEC-POL-012.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, third parties, and business associates who use, evaluate, approve, or govern AI and ML technologies on behalf of the organization. It encompasses all AI applications including generative AI tools, machine learning models, automated decision-making systems, and AI-powered business applications regardless of their technical implementation. This policy covers AI governance, risk assessment, ethical evaluation, regulatory compliance, and acceptable use across all business functions including healthcare, administrative, and operational activities.

3. Policy

- **[Company Name]** shall implement comprehensive AI governance, ethical guidelines, and compliance controls to ensure responsible, fair, and compliant use of AI technologies while protecting individual rights, preventing discrimination, and maintaining regulatory compliance as coordinated with technical security requirements in SEC-POL-012.

3.1 AI Governance and Risk Management Framework

A formal AI governance structure shall be established to oversee the ethical evaluation, compliance assessment, approval, and monitoring of AI technologies across the organization.

3.1.1 AI Governance Committee Structure

- **Committee Composition and Leadership:**
  - AI Governance Committee comprising representatives from Security, Privacy, Legal, Clinical, IT, Business units, and external ethics expertise
  - Designated AI Ethics Officer responsible for ethical AI oversight, compliance coordination, and organizational ethics leadership
  - Patient Advocate or Patient Representative for healthcare-related AI governance decisions
  - External Ethics Advisor or AI Ethics Consultant for independent perspective and specialized expertise
  - Executive Sponsor from senior leadership for strategic direction and resource allocation
- **Governance Committee Responsibilities:**
  - Strategic oversight of AI initiatives and alignment with organizational values and mission
  - Approval of new AI tools and applications based on ethical, compliance, and risk assessments
  - Policy development and maintenance for AI ethics, compliance, and acceptable use
  - Cross-functional coordination for AI incidents involving ethics, bias, or regulatory compliance
  - Annual review and update of AI governance policies, procedures, and risk appetite

3.1.2 AI Risk Assessment and Classification

- **Comprehensive AI Risk Assessment Process:**
  - Mandatory risk assessment for all new AI tools, significant changes to existing AI systems, and periodic review of deployed systems
  - Multi-dimensional risk evaluation including ethical implications, regulatory compliance, bias potential, and individual impact
  - Stakeholder impact assessment including patients, employees, customers, and communities affected by AI decisions
  - Data sensitivity analysis with specific focus on ePHI, PII, and other protected information categories
  - The completed risk assessment must be submitted to and formally approved by the AI Governance Committee prior to deployment
- **AI Risk Classification Framework:**
  - **High Risk**: AI systems making automated decisions affecting individuals, processing

ePHI or Restricted data, or having significant ethical implications
  - **Medium Risk**: AI systems providing recommendations influencing human decisions, processing Confidential data, or affecting business-critical functions
  - **Low Risk**: AI systems for content assistance, processing only Public or Internal data, with limited individual or business impact
  - **Regulatory Risk**: Additional classification for AI systems subject to FDA approval, clinical validation, or other regulatory oversight
  - Risk classification determines approval authority, monitoring requirements, and compliance obligations

3.2 AI Ethics and Fairness Framework

Comprehensive ethical principles and fairness measures shall guide AI development, deployment, and usage to ensure responsible and equitable outcomes.

3.2.1 Ethical AI Principles

- **Fairness and Non-Discrimination:**
  - Commitment to preventing algorithmic bias and discrimination based on protected characteristics including race, gender, age, disability, and other legally protected categories
  - Regular bias testing and fairness evaluation for AI systems affecting hiring, promotion, patient care, or other individual decisions
  - Diverse and representative training data and validation datasets to minimize algorithmic bias and ensure equitable outcomes
  - Ongoing monitoring of AI system outcomes for disparate impact on protected groups with corrective action procedures
  - Documentation and reporting of fairness measures, bias testing results, and remediation activities
- **Transparency and Explainability:**
  - Clear documentation and communication of AI system capabilities, limitations, decision-making processes, and potential risks
  - Explainable AI (XAI) requirements for systems making decisions affecting individuals with understandable reasoning and justification
  - User notification and disclosure when individuals are interacting with AI systems or AI-generated content

  - Model interpretability measures for critical business and clinical decisions with accessible explanations
  - Regular communication about AI system changes, updates, and performance to affected stakeholders

3.2.2 Human Oversight and Control

- **Human-in-the-Loop Requirements:**
  - Mandatory human review and approval for AI-generated decisions affecting individuals including employment, healthcare, and financial decisions
  - Override capabilities and escalation procedures for all automated AI decisions with clear human authority
  - Training and competency requirements for workforce members supervising AI systems and making AI-assisted decisions
  - Clear escalation procedures for AI system malfunctions, unexpected outcomes, or ethical concerns
  - Regular validation of AI system performance, accuracy, and alignment with intended outcomes and ethical principles
- **Individual Rights and Agency:**
  - Right to human review for individuals affected by automated AI decisions with accessible appeal processes
  - Right to explanation for AI-generated decisions affecting individuals with clear and understandable reasoning
  - Opt-out procedures for individuals who prefer human-only decision-making where technically and operationally feasible
  - Consent and notification requirements for AI system involvement in healthcare delivery and patient care
  - Protection of individual autonomy and decision-making authority in AI-assisted processes

3.3 Regulatory Compliance and Data Protection

Comprehensive compliance controls shall ensure AI systems meet all applicable regulatory requirements and protect individual privacy and data rights.

3.3.1 Healthcare and Clinical AI Compliance

- **Clinical AI Regulatory Requirements:**
  - FDA approval or validation through appropriate regulatory processes for AI clinical decision support tools and medical devices
  - Clinical evidence and validation requirements for AI systems providing diagnostic, therapeutic, or clinical recommendations
  - Medical ethics and professional standards compliance for AI systems involved in patient care delivery
  - Patient safety monitoring and adverse event reporting for AI systems with clinical applications
  - Integration with clinical governance and quality assurance programs for AI-enabled healthcare delivery
- **HIPAA and ePHI Protection:**
  - Strict prohibition of ePHI processing in unauthorized AI systems without Business Associate Agreements (BAAs) and appropriate safeguards
  - De-identification requirements for healthcare data used in AI model training in accordance with HIPAA Privacy Rule standards (45 CFR § 164.514)
  - Safe Harbor method or Expert Determination for ePHI de-identification with documented methodology and validation
  - Re-identification prohibition and controls to prevent unauthorized linkage of de-identified data to individuals
  - Minimum necessary rule compliance for AI systems accessing ePHI with purpose limitation and data minimization

3.3.2 Privacy and Data Protection Compliance

- **Privacy Rights and Data Subject Rights:**
  - Individual rights implementation including access, rectification, erasure, and portability for AI systems processing personal data
  - Consent management and preference systems for AI data processing with granular control and easy withdrawal
  - Privacy impact assessments (PIAs) for AI applications processing personal data with risk mitigation measures
  - Cross-border data transfer restrictions and data localization requirements for AI services

and data processing
  - Privacy by design principles integration into AI system development and deployment processes
- **Data Minimization and Purpose Limitation:**
  - Data minimization principles for all AI training and inference data ensuring only necessary data is collected and used
  - Purpose limitation and use restriction controls preventing AI data use beyond authorized purposes
  - Data retention and disposal requirements for AI systems with automated enforcement and compliance monitoring
  - Secondary use controls and governance for AI data repurposing with ethical review and approval
  - Anonymization and pseudonymization requirements for AI data processing with privacy protection validation

3.4 AI Acceptable Use and Guidelines

Specific guidelines shall govern the appropriate and ethical use of AI technologies by workforce members across different business functions and roles.

3.4.1 General Acceptable Use Guidelines

- **Permitted AI Use Cases and Applications:**
  - Content creation assistance for marketing, documentation, and communications with human review and validation
  - Code generation and software development assistance with security review and intellectual property compliance
  - Data analysis and business intelligence support with data protection and privacy compliance
  - Process automation and workflow optimization with human oversight and quality assurance
  - Research and information gathering for business purposes with accuracy validation and source attribution
- **Prohibited AI Use Cases and Activities:**
  - Clinical diagnosis or treatment recommendations without appropriate medical oversight,

validation, and regulatory compliance
  - Automated decision-making for hiring, firing, promotion, or performance evaluation without human review and appeal processes
  - Processing of ePHI through unauthorized AI systems without BAAs and appropriate safeguards
  - Generation of misleading, false, or deceptive content including deepfakes, misinformation, or fraudulent materials
  - Circumvention of security controls, policy violations, or unauthorized access through AI assistance

3.4.2 Role-Specific AI Guidelines and Requirements

- **Healthcare and Clinical Staff:**
  - AI clinical decision support tools must be FDA-approved, clinically validated, or approved through institutional review processes
  - Mandatory human clinician review and validation for all AI-generated clinical recommendations and decisions
  - Patient consent and disclosure requirements for AI system involvement in care delivery with clear opt-out procedures
  - Documentation of AI system use in patient medical records with decision rationale and human oversight
  - Compliance with medical ethics, professional standards, and institutional clinical governance policies
- **Software Development Teams:**
  - Code review and security testing requirements for all AI-generated code before production deployment
  - Intellectual property review and clearance for AI-generated content and code with legal compliance validation
  - Security vulnerability assessment of AI-generated code with penetration testing and security scanning
  - Documentation of AI tool usage in development processes with audit trail and accountability measures
  - Compliance with secure development lifecycle requirements and integration with SEC-POL-012 technical controls
- **Business and Administrative Functions:**

  - Data privacy review and approval for AI applications processing personal information or sensitive data
  - Accuracy validation and fact-checking for AI-generated business documents, reports, and communications
  - Human review and approval for AI-assisted decision-making processes affecting individuals or business operations
  - Compliance with regulatory requirements for automated processing and algorithmic decision-making
  - Documentation and audit trail for AI system use in business processes with accountability and oversight

3.5 Third-Party AI Service Governance

Comprehensive governance controls shall ensure third-party AI services meet ethical, compliance, and contractual requirements.

3.5.1 AI Vendor Ethics and Compliance Assessment

- **Vendor Ethics Evaluation:**
  - Comprehensive assessment of third-party AI vendor ethical practices, governance frameworks, and responsible AI commitments
  - Review of vendor AI development practices including bias testing, fairness validation, and transparency measures
  - Evaluation of vendor data handling practices, privacy protection, and individual rights implementation
  - Assessment of vendor compliance with applicable regulations including healthcare, privacy, and AI-specific requirements
  - Due diligence review of vendor AI ethics policies, incident response procedures, and accountability measures

3.5.2 AI Service Contracts and Agreements

- **Contractual Requirements and Protections:**
  - Business Associate Agreements (BAAs) for AI services processing ePHI with HIPAA compliance and breach notification requirements

  - Data processing agreements with privacy protection, individual rights implementation, and compliance validation
  - Intellectual property protection and confidentiality agreements for AI service usage and data processing
  - Liability and indemnification clauses for AI-related risks including bias, discrimination, and compliance violations
  - Service level agreements including ethical AI requirements, transparency obligations, and audit rights

3.6 AI Training and Awareness Program

Comprehensive training and awareness programs shall ensure workforce members understand AI ethics, compliance requirements, and responsible use practices.

3.6.1 AI Ethics Training Requirements

- **General AI Ethics Awareness:**
  - Annual mandatory training for all workforce members on AI ethics principles, bias prevention, and responsible use practices
  - Role-specific training for AI system users including ethical decision-making and bias recognition
  - Ethics and fairness awareness training for managers and decision-makers using AI-assisted tools
  - Privacy and compliance training for workforce members handling AI systems processing personal data
  - Regular updates on emerging AI ethics issues, regulatory changes, and policy modifications
- **Specialized Ethics Training Programs:**
  - Advanced ethics training for AI Governance Committee members including ethical frameworks and decision-making models
  - Clinical ethics training for healthcare staff using AI decision support tools with patient safety and care quality focus
  - Legal and compliance training for AI oversight roles including regulatory requirements and liability issues
  - Leadership training on AI ethics governance, organizational culture, and stakeholder

communication
  - Train-the-trainer programs for internal AI ethics champions and subject matter experts

3.6.2 AI Ethics Competency and Culture

- **Ethics Competency Assessment and Development:**
  - Regular assessment of workforce AI ethics literacy and competency with targeted improvement programs
  - Certification requirements for critical AI system users including ethics knowledge validation
  - Continuing education and professional development for AI ethics and responsible AI practices
  - Knowledge sharing and best practices documentation for AI ethics implementation and lessons learned
  - Performance evaluation integration of AI ethics compliance and responsible use practices
- **Organizational AI Ethics Culture:**
  - Clear communication of organizational AI ethics values, principles, and expectations from leadership
  - Recognition and reward programs for exemplary AI ethics practices and responsible innovation
  - Open reporting and discussion culture for AI ethics concerns without fear of retaliation
  - Regular organizational assessment of AI ethics culture and continuous improvement initiatives
  - External engagement and thought leadership in AI ethics and responsible AI development

3.7 Coordination with AI Development and Security

This policy coordinates with SEC-POL-012 (AI Development and Deployment Security Policy) to ensure comprehensive coverage of AI ethics, compliance, and technical security requirements.

3.7.1 Cross-Policy Integration and Coordination

- **Ethics and Security Integration:**
  - Technical security controls shall support and enable ethical AI principles and compliance requirements

- Ethics review and approval processes shall coordinate with security assessments and technical validation
- Incident response procedures shall integrate ethics and compliance considerations with technical security response
- Governance and oversight activities shall coordinate ethics compliance with security and technical requirements
- Training and awareness programs shall integrate ethics education with security and technical competency development

4. Standards Compliance

This AI Ethics and Compliance Policy aligns with and supports compliance requirements from multiple regulatory frameworks while coordinating with technical security requirements in SEC-POL-012.

4.1 Regulatory Compliance Mapping

Policy Section	Standard/Framework	Control Reference
3.1	HITRUST CSF v11.2.0	01.d - Information Security Governance
3.1	HITRUST CSF v11.2.0	01.e - Information Handling Requirements
3.2	HITRUST CSF v11.2.0	13.b - Information Security Awareness
3.3	HITRUST CSF v11.2.0	19.a - Data Protection and Privacy Policy
3.3	HITRUST CSF v11.2.0	19.d - Privacy Controls
3.5	HITRUST CSF v11.2.0	14.a - Third Party Assurance
3.6	HITRUST CSF v11.2.0	13.a - Information Security Education
3.3	HIPAA Security Rule	45 CFR § 164.308(a)(4) - Information Access Management

Policy Section	Standard/Framework	Control Reference
3.3	HIPAA Privacy Rule	45 CFR § 164.502(b) - Minimum Necessary Standard
3.3	HIPAA Privacy Rule	45 CFR § 164.514 - De-identification
3.5	HIPAA Security Rule	45 CFR § 164.314(a)(1) - Business Associate Contracts
3.3	HIPAA Privacy Rule	45 CFR § 164.522 - Rights to Request Privacy Protection
3.1, 3.2	SOC 2 Trust Services Criteria	CC2.1 - Communication and Information
3.3	SOC 2 Trust Services Criteria	PI1.1 - Privacy Notice and Communication
3.3	SOC 2 Trust Services Criteria	PI1.2 - Privacy Choice and Consent
3.3	SOC 2 Trust Services Criteria	PI1.3 - Privacy Collection
3.2	NIST AI Risk Management Framework	AI risk management and governance
3.2	NIST Privacy Framework	GV.PO - Governance and Privacy Objectives

5. Definitions

- **Algorithmic Bias:** Systematic prejudice in AI systems that results in unfair treatment of certain groups or individuals based on protected characteristics.
- **Artificial Intelligence (AI):** Computer systems that can perform tasks typically requiring human intelligence, including learning, reasoning, and perception.
- **De-identification:** Process of removing personal identifiers from data to protect individual privacy in accordance with regulatory standards.

- **Explainable AI (XAI):** AI systems designed to provide understandable explanations for their decisions and recommendations to affected individuals.
- **Human-in-the-Loop:** AI system design requiring human oversight, review, and decision-making authority for automated processes.
- **Privacy Impact Assessment (PIA):** Systematic assessment of privacy risks and mitigation measures for systems processing personal data.
- **Responsible AI:** Approach to AI development and deployment emphasizing ethical principles, fairness, transparency, and accountability.

6. Responsibilities

Role	Responsibility
AI Ethics Officer	Overall responsibility for AI ethics program, governance coordination, and integration with SEC-POL-012 technical requirements.
AI Governance Committee	Approval of AI implementations, ethics and compliance review, policy decisions, and strategic guidance for responsible AI initiatives.
Privacy Officer	AI privacy compliance oversight, ePHI protection validation, privacy impact assessments, and coordination with technical security controls.
Legal and Compliance Team	Regulatory compliance validation, contract review for AI services, legal risk assessment, and coordination with technical implementation teams.
Clinical Leadership	Healthcare AI governance, clinical validation requirements, patient safety oversight, and coordination with technical security measures.
Business Unit Leaders	Team compliance with AI ethics policies, business requirement validation, responsible AI culture development, and coordination with technical teams.

Role	Responsibility
Training and Development Team	AI ethics education program delivery, competency assessment, and coordination with technical training requirements.
All Workforce Members	Compliance with AI ethics and acceptable use policies, responsible AI practices, and coordination with technical security requirements.

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

See Annex: Control Mapping

6. Artifact(s)

Signed and dated meeting minutes are stored in the company’s document management system.

7. Definitions

See Annex: Glossary

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

See Annex: Control Mapping

6. Artifact(s)

A final internal audit report and a corrective action tracking log.

7. Definitions

See Annex: Glossary

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

See Annex: Control Mapping

6. Artifact(s)

A completed and approved Password Policy Exception Request form.

7. Definitions

See Annex: Glossary

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

See Annex: Control Mapping

6. Artifact(s)

An updated Risk Register and a formal Risk Assessment Report.

7. Definitions

See Annex: Glossary

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

See Annex: Control Mapping

6. Artifact(s)

A completed Vendor Risk Assessment Report.

7. Definitions

See Annex: Glossary

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/Security 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/Security Team	Conducts and documents annual 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

See Annex: Control Mapping

6. Artifact(s)

A completed access request form and an access review log.

7. Definitions

See Annex: Glossary

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

See Annex: Control Mapping

6. Artifact(s)

A completed AI Risk Assessment and Approval Form.

7. Definitions

See Annex: Glossary

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

See Annex: Control Mapping

6. Artifact(s)

An entry in the vulnerability tracking system showing the lifecycle of a vulnerability from discovery to verified remediation.

7. Definitions

See Annex: Glossary

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

See Annex: Control Mapping

6. Artifact(s)

A completed and approved Exception Request Form documented in the risk register.

7. Definitions

See Annex: Glossary

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.

Op Proc 009

Software and Extension Approval Procedure (OP-PROC-009)

1. Purpose

To define the formal process for requesting, assessing, and approving new software, applications, and browser extensions for use on company-managed endpoints, ensuring they are secure and have a valid business justification.

2. Scope

This procedure applies to all workforce members who wish to install new software and to the Security and IT teams responsible for the review, approval, and management of that software.

3. Overview

This procedure outlines the streamlined, ticket-based workflow for managing new software requests. It ensures that all requests are formally documented, subject to a security risk assessment, and that the outcome is recorded in a central system, creating an auditable trail of all software approvals.

4. Procedure

Step	Who	What
1	Workfor Mem- ber	Submits a “New Software Request” ticket via the IT helpdesk system. The request shall include the software/extension name, a link to its official source, and a clear business justification.
2	Security Team	Receives and reviews the ticket. Conducts a risk assessment based on the software’s function, the data it accesses, its permissions, vendor reputation, and any known vulnerabilities.
3	Security Team	Based on the assessment, formally approves or denies the request within the ticket, providing a brief rationale for the decision.

4 | IT Department | If approved, adds the software to the official

Software Allowlist and, if necessary, assists the user with a secure installation. |

5. Standards Compliance

See Annex: Control Mapping

6. Artifact(s)

A completed IT helpdesk ticket that documents the initial request, the security team's risk assessment notes, and the final, documented approval or denial.

7. Definitions

See Annex: Glossary

8. Responsibilities

Role	Responsibility
Workforce Member	Initiates the approval process by submitting a complete and accurate request ticket.
Security Team	Performs the risk assessment for all new software requests and makes the final decision on approval or denial.
IT Department	Manages the official Software Allowlist and assists with the deployment of approved software.

Op Proc 009

Software and Extension Approval Procedure (OP-PROC-009)

1. Purpose

To define the formal process for requesting, assessing, and approving new software, applications, and browser extensions for use on company-managed endpoints, ensuring they are secure and have a valid business justification.

2. Scope

This procedure applies to all workforce members who wish to install new software and to the Security and IT teams responsible for the review, approval, and management of that software.

3. Overview

This procedure outlines the streamlined, ticket-based workflow for managing new software requests. It ensures that all requests are formally documented, subject to a security risk assessment, and that the outcome is recorded in a central system, creating an auditable trail of all software approvals.

4. Procedure

Step	Who	What
1	Workfor Mem- ber	Submits a “New Software Request” ticket via the IT helpdesk system. The request shall include the software/extension name, a link to its official source, and a clear business justification.
2	Security Team	Receives and reviews the ticket. Conducts a risk assessment based on the software’s function, the data it accesses, its permissions, vendor reputation, and any known vulnerabilities.
3	Security Team	Based on the assessment, formally approves or denies the request within the ticket, providing a brief rationale for the decision.

4 | IT Department | If approved, adds the software to the official

Software Allowlist and, if necessary, assists the user with a secure installation. |

5. Standards Compliance

See Annex: Control Mapping

6. Artifact(s)

A completed IT helpdesk ticket that documents the initial request, the security team's risk assessment notes, and the final, documented approval or denial.

7. Definitions

See Annex: Glossary

8. Responsibilities

Role	Responsibility
Workforce Member	Initiates the approval process by submitting a complete and accurate request ticket.
Security Team	Performs the risk assessment for all new software requests and makes the final decision on approval or denial.
IT Department	Manages the official Software Allowlist and assists with the deployment of approved software.

Annex: Glossary

This annex consolidates and standardizes definitions used across the ISMS policy and procedure set. Individual documents should reference this annex instead of including their own glossary sections.

How to use:

- When a term is needed in a document, link to this annex section using a relative link.
- Keep terms plain, vendor-neutral, and adaptable.

Terms

- Access Review: A periodic or event-driven evaluation of user entitlements to verify they remain appropriate for role and business need.
- Account Lifecycle: The end-to-end process of user account creation, modification, review, and termination aligned with employment status and role changes.
- Audit Logging Framework: The coordinated system of policies, procedures, and technologies that support logging across domains (authentication/network, data access, etc.).
- Authentication Event: A security event related to verifying the identity of a user, device, or service attempting to access a system or resource.
- Authorization Event: A security event related to granting or denying access permissions to authenticated entities based on their privileges and roles.
- Business Associate Agreement (BAA): A HIPAA-required contract between a covered entity and a business associate defining permitted uses/disclosures of ePHI and safeguards.
- BYOD (Bring Your Own Device): A practice that allows workforce members to use personal devices for work-related purposes subject to security controls.
- Clean Desk Policy: Practice requiring sensitive materials to be secured when workspaces are unattended.
- Cloud Service Provider: A third-party organization providing cloud computing services, including infrastructure, platforms, or software.
- Cross-Domain Correlation: The process of analyzing and linking related events across authentication, network, and data access logging domains.
- Data Lifecycle Management: Managing data from creation through retention, archiving, and secure destruction.
- Data Loss Prevention (DLP): Technology and processes that detect and prevent unauthorized transmission or use of sensitive data.

- Electronic Protected Health Information (ePHI): Individually identifiable health information that is created, stored, transmitted, or maintained electronically.
- Environmental Controls: Systems and procedures designed to protect against environmental hazards such as fire, flood, temperature extremes, and power failures.
- Event Integration: The technical capability to combine and analyze security events from multiple specialized logging domains.
- Identity and Access Management (IAM): Policies, processes, and technologies used to manage digital identities and control access to resources based on user roles and responsibilities.
- Information Owner: Individual with authority and responsibility for specific information, including establishing handling requirements and approving access.
- 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 principle of restricting access rights to the minimum permissions needed to perform work.
- Mobile Device Management (MDM): Software that enables an organization to secure, monitor, and manage mobile devices used for business purposes.
- Multi-Factor Authentication (MFA): A security process requiring two or more authentication factors (e.g., password plus token/biometric) for access verification.
- Network Flow: A sequence of packets from a source to a destination that share common characteristics such as IP addresses, ports, and protocols.
- Privileged Access: Elevated administrative or system-level access that can modify configurations, security settings, or data beyond standard user capabilities.
- Privilege Escalation: Gaining elevated access permissions beyond those initially granted to a user or service account.
- Remote Lock: Administrative action that remotely makes a device inaccessible.
- Remote Wipe: Administrative action that remotely deletes data from a device.
- Risk Assessment: The process of identifying vulnerabilities and threats to information assets and determining the risk posed by those threats.
- Role-Based Access Control (RBAC): A method of restricting access based on user roles aligned to job functions.
- Security Incident: Any event that could result in unauthorized access, disclosure, modification, or destruction of information assets.
- Security Information and Event Management (SIEM): Technology providing real-time analysis and correlation of security alerts and events from multiple sources.

- Session Correlation: Linking related authentication and access events across multiple systems using session identifiers.
- System Owner: The individual or group responsible for the procurement, development, operation, and maintenance of an information system.
- Tailgating: Unauthorized access gained by following an authorized person through a controlled physical access point.
- Threat Intelligence: Information about current and potential security threats used to enhance detection and response.
- User Agent: Information about the client software, operating system, and device characteristics used for requests such as authentication.
- Visitor Management System: Automated system for registering, tracking, and managing facility visitors.
- SOC 2 Report: A report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy.
- Physical Security Perimeter: The physical boundary around facilities, systems, or areas requiring protection.
- Follow-Me Printing: Secure printing requiring user authentication at the printer before documents are released.

Annex: Control Mapping

This annex consolidates all regulatory and framework mappings referenced across the policy and procedure set. Individual documents should replace embedded mapping tables with a pointer to this annex.

How to use:

- Use the framework sections below to see which document(s) implement each control.
- Section/step references point to the exact clause in the implementing policy/procedure.

Mappings by Framework

HITRUST CSF v11.2.0

01.g — Information Security Management Program Review

Implementing Document	Section/Steps
SEC-PROC-002 Internal Audit Procedure	1-6
RES-PROC-003 Post-Incident Review Procedure	3
RES-PROC-007 BCDR Testing and Exercise Procedure	4

02.b — Information Security Roles and Responsibilities

Implementing Document	Section/Steps
OP-PROC-006 Workforce Screening and Background Check Procedure	1-7

03.b — Media Handling; 03.c — Secure Media Disposal

Implementing Document	Section/Steps
OP-POL-003 Data Retention and Disposal Policy	3.4 (03.b), 3.2 (03.c)

Implementing Document	Section/Steps
OP-PROC-004 Secure Media Disposal and Sanitization Procedure	4.1 (NIST SP 800-88), 4.1-4.2

04.a–04.f — Mobile Device Security

Implementing Document	Section/Steps
OP-POL-002 Mobile Device Security Policy	Section A (04.a), 3.2 (04.b), 3.2, 3.6 (04.c), 3.3 (04.d), 3.7 (04.e), 3.8 (04.f)
OP-PROC-002 Mobile Device Onboarding and Security Configuration Procedure	1-7 (04.b)
OP-PROC-003 Lost or Stolen Mobile Device Response Procedure	1-5 (04.f)

05.a–05.b — Wireless Network Security

Implementing Document	Section/Steps
ENG-POL-004 Network Security Policy	3.5 (05.a, 05.b)

06.a–06.d — Configuration and Change Control

Implementing Document	Section/Steps
ENG-POL-002 Change Control Policy	All (06.a); 3.1, 3.2 (06.b); 3.3 (06.c); 3.4 (06.d)
ENG-POL-003 Cloud and Core Infrastructure Security Policy	All (06.a); 3.4 (06.a)

Implementing Document	Section/Steps
ENG-PROC-003 Standard Change Management Procedure	1-6 (12.a + SDLC)
ENG-PROC-004 Emergency Change Management Procedure	1-5 (12.a)

06.e — Secure Development

Implementing Document	Section/Steps
ENG-POL-001 Secure Software Development Lifecycle (SDLC) Policy	3.1
ENG-POL-005 Secure Coding and Testing Policy	3.1, 3.2
ENG-POL-006 Third-Party Component Management Policy	3.2

07.a–07.d — Vulnerability Management

Implementing Document	Section/Steps
ENG-POL-001 SDLC Policy	All (07.a)
ENG-POL-005 Secure Coding and Testing Policy	3.1 (07.b); 3.2, 3.3 (07.c); 3.2.2 (07.d)
ENG-POL-006 Third-Party Component Management Policy	3.1.1 (07.b); 3.1.2 (07.d)
ENG-PROC-001 Application Security Testing Procedure	4.1-4.3 (07.a); 4.1 (07.b); 4.2 (07.c); 4.3 (07.d)
ENG-PROC-002 Third-Party Component Security Review Procedure	1-5 (07.a); 2-3 (07.d)
ENG-PROC-003 Standard Change Management Procedure	2-4 (07.b); 5 (07.c)

Implementing Document	Section/Steps
ENG-PROC-004 Emergency Change Management Procedure	3 (07.b)

08.a–08.h — Network Protection

Implementing Document	Section/Steps
ENG-POL-003 Cloud and Core Infrastructure Security Policy	3.1 (08.a)
ENG-POL-004 Network Security Policy	All (08.a); 3.1 (08.b); 3.2 (08.c); 3.7 (08.d); 3.3 (08.e); 3.4 (08.g); 3.1.1 (08.f, 08.h)

09.a–09.b — Data Protection and Cryptography

Implementing Document	Section/Steps
ENG-POL-003 Cloud and Core Infrastructure Security Policy	3.3 (09.a); 3.5 (09.b)
OP-POL-001 Encryption and Key Management Policy	All (09.a, 09.b, 09.c)

10.c — Password Protection Systems

Implementing Document	Section/Steps
SEC-PROC-003 Password Policy Exception Procedure	1-3

11.a — Access Control Policy

Implementing Document	Section/Steps
ENG-POL-003 Cloud and Core Infrastructure Security Policy	3.2
ENG-POL-004 Network Security Policy	3.6
SEC-POL-001 Information Security Policy	3.4

12.a–12.f — Audit Logging and Monitoring

Implementing Document	Section/Steps
RES-POL-003 Security Event Detection and Monitoring Policy	3.1 (12.a); 3.1.1 (12.d); 3.4 (12.c)
ENG-POL-004 Network Security Policy	3.2, 3.6 (12.a)
ENG-POL-003 Cloud and Core Infrastructure Security Policy	3.7 (12.b)
SEC-PROC-002 Internal Audit Procedure	1-6 (12.f)
ENG-PROC-003 Standard Change Management Procedure	1-6 (12.a)
ENG-PROC-004 Emergency Change Management Procedure	1-5 (12.a)

13.a–13.e — Education, Training and Awareness; Disciplinary

Implementing Document	Section/Steps
ENG-POL-001 SDLC Policy	3.4 (13.a)
OP-PROC-006 Workforce Screening and Background Check Procedure	4-5 (13.b); 1-7 (02.b)
OP-PROC-008 Security Policy Sanction Procedure	1-6 (13.e); 2-3 (13.b); 4-5 (13.d)

Implementing Document	Section/Steps
OP-POL-004 Workforce Security Policy	All (13.a–13.e)

14.a–14.g — Third Party Assurance and Supplier Management

Implementing Document	Section/Steps
SEC-PROC-005 Vendor Risk Assessment and Onboarding Procedure	1-6 (14.b); 2-4 (14.f); 3 (14.a); 5-6 (14.c)
ENG-POL-006 Third-Party Component Management Policy	3.3 (14.a); 3.1 (14.g)
ENG-PROC-002 Third-Party Component Security Review Procedure	3-4 (14.f)

15.a–15.g — Incident Response

Implementing Document	Section/Steps
RES-POL-001 Incident Response Framework and Team Management Policy	All (15.a); 3.1, 3.2 (15.b); 3.1.2 (15.c); 3.5 (15.g)
RES-POL-003 Security Event Detection and Monitoring Policy	3.3 (15.c)
RES-POL-004 Incident Communication and Regulatory Compliance Policy	All (15.d); 3.2 (15.e); 3.3 (15.f); 3.4 (15.g); 3.1 (15.c)
ENG-PROC-004 Emergency Change Management Procedure	1-5 (15.a); 5 (15.f)
RES-PROC-001 Incident Response Plan (IRP)	1-10 (15.a); 3-5 (15.b); 6-8 (15.c); 7 (15.d); 8 (15.e); 9-10 (15.f, 15.g)
RES-PROC-002 HIPAA Breach Risk Assessment Procedure	1-3 (15.b, 15.f)

Implementing Document	Section/Steps
RES-PROC-003 Post-Incident Review Procedure	1-4 (15.f, 15.g)

16.a–16.i — Business Continuity and Disaster Recovery

Implementing Document	Section/Steps
RES-POL-002 Business Continuity Management Policy	3.1–3.6 (16.a–16.f)
RES-POL-005 Disaster Recovery and Technical Operations Policy	All (16.c); 3.1 (16.g); 3.2 (16.h); 3.3 (16.i); 3.5 (12.d)
RES-PROC-004 Business Impact Analysis (BIA) Procedure	1-4 (16.b, 16.c, 16.a)
RES-PROC-005 IT Disaster Recovery Plan (DRP)	1-8 (16.g, 16.c, 16.e)
RES-PROC-006 Business Continuity Plan (BCP)	1-5 (16.d, 16.f, 16.a, 16.c)
RES-PROC-007 BCDR Testing and Exercise Procedure	1-4 (16.e, 16.a, 16.d)

17.a–17.e — Risk Management

Implementing Document	Section/Steps
SEC-PROC-004 Risk Assessment Procedure	1-6 (17.c); 1-2 (17.b); 3-4 (17.d); 5-6 (17.e)
SEC-POL-001 Information Security Policy	3.2 (17.a)
SEC-PROC-003 Password Policy Exception Procedure	2 (17.c)

19.e — Data Retention Requirements; 19.g — Privacy Impact Assessment

Implementing Document	Section/Steps
OP-POL-003 Data Retention and Disposal Policy	3.1, 3.2 (19.e)
RES-PROC-002 HIPAA Breach Risk Assessment Procedure	2-3 (19.g)

SOC 2 Trust Services Criteria

CC6.1 — Logical Access Security

Implementing Document	Section/Steps
SEC-POL-001 Information Security Policy	3.4
OP-PROC-002 Mobile Device Onboarding Procedure	1-7
OP-POL-002 Mobile Device Security Policy	Section A
ENG-POL-003 Cloud and Core Infrastructure Security Policy	All
ENG-POL-004 Network Security Policy	All
SEC-PROC-003 Password Policy Exception Procedure	1-3

CC6.6 — Network Security; CC6.7 — Data Transmission; CC6.8 — System Security

Implementing Document	Section/Steps
ENG-POL-004 Network Security Policy	3.1 (CC6.6); All (CC6.7)
ENG-POL-003 Cloud and Core Infrastructure Security Policy	3.3 (CC6.7)
OP-POL-001 Encryption and Key Management Policy	3.2, 3.2.4 (CC6.8)
ENG-POL-005 Secure Coding and Testing Policy	3.1 (CC6.8)

CC7.1–CC7.2 — System Monitoring

Implementing Document	Section/Steps
RES-POL-003 Security Event Detection and Monitoring Policy	All (CC7.1); 3.1.1 (CC7.2)
ENG-POL-003 Cloud and Core Infrastructure Security Policy	3.7 (CC7.1)
ENG-POL-004 Network Security Policy	3.2, 3.6 (CC7.2); 3.2, 3.3 (CC7.1)
SEC-PROC-008/009 Vulnerability Management (Std/Exception) Procedures	1-6 (CC7.1)
RES-PROC-001 Incident Response Plan (IRP)	1-10 (CC7.1, CC7.2)

CC8.1 — Change Management

Implementing Document	Section/Steps
ENG-POL-001 SDLC Policy	All
ENG-POL-002 Change Control Policy	All
ENG-POL-003 Cloud and Core Infrastructure Security Policy	3.4
ENG-POL-004 Network Security Policy	3.4
ENG-PROC-001 AppSec Testing Procedure	4.1-4.3
ENG-PROC-003 Standard Change Management Procedure	1-6
ENG-PROC-004 Emergency Change Management Procedure	1-5

A1.1–A1.3 — Availability

Implementing Document	Section/Steps
RES-POL-002 Business Continuity Management Policy	3.1, 3.4 (A1.1); 3.3, 3.4 (A1.2); 3.5 (A1.3)
RES-POL-005 Disaster Recovery and Technical Operations Policy	All (A1.1); 3.1 (A1.2); 3.5 (A1.3)
RES-PROC-004/006/007 BIA/BCP/BCDR Tests	1-4/1-5/1-4

PI1.1–PI1.2 — Processing Integrity (from OP-POL-002)

Implementing Document	Section/Steps
OP-POL-002 Mobile Device Security Policy	3.5 (PI1.1, PI1.2)

CC2.1–CC2.2 — Communication and Information

Implementing Document	Section/Steps
SEC-POL-001 Information Security Policy	3.1 (CC2.1)
RES-POL-001 Incident Response Framework	3.5 (CC2.1)
RES-POL-004 Incident Communication and Regulatory Compliance Policy	3.3 (CC2.1); 3.4 (CC2.2)
SEC-PROC-001 InfoSec Committee Charter Procedure	1-5 (CC2.1)
OP-POL-004 Workforce Security Policy	3.1, 3.2 (CC2.1, CC2.2)

HIPAA Security Rule (45 CFR § 164)

§ 164.308(a)(1) — Security Management Process

Implementing Document	Section/Steps
SEC-POL-008 Vulnerability Management Policy	All
ENG-POL-003 Cloud and Core Infrastructure Security Policy	All
ENG-POL-005 Secure Coding and Testing Policy	All
ENG-POL-006 Third-Party Component Management Policy	All

§ 164.308(a)(2) — Assigned Security Responsibility; (a)(3) — Workforce Security; (a)(4) — Information Access Management; (a)(5) — Security Awareness and Training; (a)(6) — Security Incident Procedures; (a)(7) — Contingency Plan; (a)(8) — Evaluation

Implementing Document	Section/Steps
SEC-POL-001 Information Security Policy	3.1 (a)(2); 3.4 (a)(4); 3.5 (a)(5); 3.6 (a)(6); 3.7 (a)(7); 3.9 (a)(8)
OP-POL-004 Workforce Security Policy	All (a)(3)
OP-PROC-006 Workforce Screening Procedure	1-7 (a)(3)
RES-POL-001 Incident Response Framework	All (a)(6)
RES-PROC-001 Incident Response Plan	1-10 (a)(6)
RES-POL-002/RES-POL-005 BCM/DR	As mapped (a)(7)
ENG-POL-001 SDLC Policy	3.4 (a)(5)
ENG-PROC-001 AppSec Testing Procedure	4.1-4.3 (a)(8)

§ 164.310(d)(2)(i) — Media Disposal

Implementing Document	Section/Steps
OP-PROC-004 Secure Media Disposal and Sanitization Procedure	4.1-4.2

§ 164.312 — Technical Safeguards

Implementing Document	Section/Steps
Access Control (a)(1), (a)(2)(i), (a)(2)(iv)	ENG-POL-005 3.1 (a)(1); ENG-POL-005 3.1.1 (a)(2)(i); OP-POL-001 3.1.1, 3.2.4 (a)(2)(iv); ENG-POL-003 3.3 (a)(2)(iv)
Audit Controls (b)	ENG-POL-003 3.7; ENG-POL-004 3.2, 3.5, 3.6; RES-POL-003 3.1; RES-POL-004 3.2.3; ENG/RES Procedures as mapped
Integrity (c)(1)	ENG-POL-002 3.1, 3.2; ENG-PROC-003 1-6
Transmission Security (e)(1), (e)(2)(ii)	OP-POL-001 3.1.1, 3.2.4; ENG-POL-003 3.3; ENG-POL-004 3.5, 3.6
Business Associate (164.314(a)(1))	ENG-POL-006 3.3

HIPAA Breach Notification Rule — § 164.400–414

Implementing Document	Section/Steps
RES-POL-004 Incident Communication and Regulatory Compliance Policy	3.2.1
RES-PROC-002 HIPAA Breach Risk Assessment Procedure	1-3

NIST Cybersecurity Framework (CSF)

PR.AC — Identity Management and Access Control

Implementing Document	Section/Steps
ENG-POL-003 Cloud and Core Infrastructure Security Policy	All
ENG-POL-004 Network Security Policy	All
OP-POL-002 Mobile Device Security Policy	3.2

PR.DS — Data Security; PR.IP-1 — Baseline Security; PR.PT — Protective Technology; PR.AT-1 — Awareness & Training

Implementing Document	Section/Steps
ENG-POL-003 Cloud and Core Infrastructure Security Policy	3.3 (PR.DS); 3.5 (PR.PT)
ENG-POL-005 Secure Coding and Testing Policy	All (PR.IP-1)
ENG-POL-001 SDLC Policy	All (PR.IP-1); 3.4 (PR.AT-1)
OP-POL-002 Mobile Device Security Policy	3.11 (PR.AT)

DE.CM — Security Continuous Monitoring; DE.AE — Anomalies and Events

Implementing Document	Section/Steps
ENG-POL-003 Cloud and Core Infrastructure Security Policy	3.7 (DE.CM, DE.AE)
ENG-POL-004 Network Security Policy	3.2 (DE.CM); 3.2, 3.3 (DE.AE)
RES-POL-003 Security Event Detection and Monitoring Policy	All (DE.CM); 3.1 (DE.AE)

RS.MI — Mitigation; RS.CO — Communications; RS.RP — Response Planning; RC.IM — Improvements; RC.RP — Recovery Planning; RC.CO — Recovery Communications

Implementing Document	Section/Steps
ENG-POL-003 Cloud and Core Infrastructure Security Policy	3.7 (RS.MI)
RES-POL-003 Security Event Detection and Monitoring Policy	3.3 (RS.CO)
RES-POL-004 Incident Communication and Regulatory Compliance Policy	All (RS.CO); 3.1 (RS.RP); 3.4 (RC.IM)
RES-POL-002/RES-POL-005 BCM/DR	All (RC.RP); 3.3 (RC.CO); 3.5 (RC.IM)
RES-PROC-001/004/005/006/007 IRP/BIA/DRP/BCP/BCDR Tests	As mapped

---

ISO/IEC 27001:2013

A.17.1 — Information Security Aspects of Business Continuity Management

Implementing Document	Section/Steps
RES-POL-002 Business Continuity Management Policy	3.1, 3.2
RES-PROC-007 BCDR Testing and Exercise Procedure	1-4 (verify/review)

A.17.1.1 — Planning Information Security Continuity; A.17.1.3 — Verify, Review and Evaluate

Implementing Document	Section/Steps
RES-POL-002 Business Continuity Management Policy	3.2, 3.3 (A.17.1.1); 3.5 (A.17.1.3)

Other Referenced Frameworks and Standards

CIS Controls — Control 4, 5

Implementing Document	Section/Steps
ENG-POL-003 Cloud and Core Infrastructure Security Policy	3.1.2

OWASP SAMM; OWASP Top 10

Implementing Document	Section/Steps
ENG-POL-001 SDLC Policy	All (OWASP SAMM)
ENG-POL-005 Secure Coding and Testing Policy	3.1 (OWASP Top 10)

NIST SP 800-88 — Media Sanitization

Implementing Document	Section/Steps
OP-PROC-004 Secure Media Disposal and Sanitization Procedure	4.1

NIST SP 800-34 Rev. 1 — Business Process Contingency Planning

Implementing Document	Section/Steps
RES-POL-002 Business Continuity Management Policy	3.4, 3.5

NIST SP 800-161 — Supply Chain Risk Management; NIST SP 800-218 — SSDF

Implementing Document	Section/Steps
ENG-POL-006 Third-Party Component Management Policy	3.1 (800-161); 3.2 (800-218)