

SOC 2 Compliance Policies & Procedures

openaccesspolicies.org

Table of Contents

Access Control Policies

- Access Control Policy (AC-POL-001)
- Network Acceptable Use Policy (AC-POL-002)
- Remote Work Policy (AC-POL-003)

Access Control Procedures

- Acceptable Use Policy Violation Investigation Procedure (AC-PROC-001)
- Bring Your Own Device (BYOD) Onboarding Procedure (AC-PROC-002)
- User Access Review Procedure (AC-PROC-003)
- Access Control Management Procedure (AC-PROC-004)

Engineering Policies

- Secure Software Development Policy (ENG-POL-001)
- Change Control Policy (ENG-POL-002)
- Infrastructure Security Policy (ENG-POL-003)

Engineering Procedures

- Application Security Testing Procedure (ENG-PROC-001)
- Third-Party Component Security Review Procedure (ENG-PROC-002)
- Standard Change Management Procedure (ENG-PROC-003)
- Emergency Change Management Procedure (ENG-PROC-004)
- System Hardening and Baselining Procedure (ENG-PROC-005)
- Privileged Infrastructure Access Review Procedure (ENG-PROC-006)

ISMS Supplements

- Schedule of Security Procedures (ISMS-SUP-001)
- ISMS High-Level RACI Chart (ISMS-SUP-002)

Operational Policies

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

- Mobile Device Policy (BYOD) (OP-POL-002)
- Data Retention and Disposal Policy (OP-POL-003)
- Human Resources Security Policy (OP-POL-004)
- Acceptable Software and Browser Extension Policy (OP-POL-005)

Operational Procedures

- Cryptographic Key Lifecycle Management Procedure (OP-PROC-001)
- Mobile Device Onboarding and Security Configuration Procedure (OP-PROC-002)
- Lost or Stolen Mobile Device Response Procedure (OP-PROC-003)
- Secure Media Disposal and Sanitization Procedure (OP-PROC-004)
- Legal Hold Procedure (OP-PROC-005)
- Workforce Screening and Background Check Procedure (OP-PROC-006)
- Employee Onboarding and Offboarding Security Procedure (OP-PROC-007)
- Security Policy Sanction Procedure (OP-PROC-008)

Resilience Policies

- Incident Response Policy (RES-POL-001)

Resilience Procedures

- Incident Response Plan (IRP) ([RES-PROC-001])
- Data Breach Risk Assessment Procedure ([RES-PROC-002])
- Post-Incident Review Procedure ([RES-PROC-003])

Security Policies

- Information Security Policy (SEC-POL-001)
- Password Policy (SEC-POL-002)
- Risk Management Policy (SEC-POL-003)
- Data Classification and Handling Policy (SEC-POL-004)
- Vendor and Third-Party Risk Management Policy (SEC-POL-005)
- Physical Security Policy (SEC-POL-006)
- AI Acceptable Use Policy (SEC-POL-007)
- Vulnerability Management Policy (SEC-POL-008)

Security Procedures

- Information Security Committee Charter Procedure (SEC-PROC-001)
- Internal Audit Procedure (SEC-PROC-002)
- Password Policy Exception Procedure (SEC-PROC-003)
- Risk Assessment Procedure (SEC-PROC-004)
- Vendor Risk Assessment and Onboarding Procedure (SEC-PROC-005)
- Facility Access Management Procedure (SEC-PROC-006)
- AI Tool Risk Assessment and Approval Procedure (SEC-PROC-007)
- Vulnerability Management Procedure (SEC-PROC-008)
- Vulnerability Management Exception Procedure (SEC-PROC-009)

Access Control Policy (AC-POL-001)

1. Objective

The objective of this policy is to define requirements for managing access to **[Company Name]**'s information systems and data based on SOC 2 requirements. This policy ensures access is granted using least privilege principles, protecting company and customer information while maintaining practical implementation.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, and vendors who require access to company information systems or data. This includes applications, servers, databases, network devices, cloud services, and physical facilities where company information is accessed or stored.

3. Policy

Access to all **[Company Name]** information systems and data shall be managed through a documented process that is consistently applied.

3.1 Least Privilege Principle

All access rights shall be granted based on least privilege. Workforce members shall receive only the minimum access necessary to perform their job responsibilities.

3.2 User Access Lifecycle Management

Access rights shall be managed throughout the user's employment lifecycle.

- **Provisioning:** Access for new workforce members shall be requested by their manager through the IT service request process. Access shall be based on job role and documented responsibilities.
- **Modification:** When workforce members change roles, their manager shall request access modifications. Previous access no longer needed shall be revoked.
- **Deprovisioning:** Upon termination, all system and facility access shall be revoked within **[Number, e.g., 24]** hours. For involuntary terminations, access shall be revoked immediately when possible.

3.3 Access Reviews

Regular access reviews shall be conducted to ensure access rights remain appropriate.

- Access to systems containing sensitive or confidential data shall be reviewed quarterly by system owners or managers.
- All other user access shall be reviewed annually.
- Reviews shall require documented approval from designated managers. Failure to complete reviews within [Number, e.g., 14] days shall result in escalation to the [Role Title, e.g., IT Manager/Security Officer].
- Review results and any access modifications shall be documented.

3.4 Privileged Access Management

Administrative accounts require additional controls due to their elevated risk.

- Administrative access shall be granted on a limited, as-needed basis with documented business justification.
- Workforce members with administrative privileges shall use separate accounts for administrative tasks and standard accounts for daily activities.
- Multi-Factor Authentication (MFA) is mandatory for all administrative accounts.
- Administrative activities shall be logged and monitored.

3.5 System Access Controls

Logical access to systems shall be secured through proper authentication and session management.

- **Unique Identification:** Every user shall have a unique user ID. Shared accounts are prohibited.
- **Authentication:** Access requires unique user ID and strong password as defined in the Password Policy (SEC-POL-002). MFA is required for sensitive systems.
- **Session Timeouts:** Systems shall automatically terminate inactive sessions after [Duration, e.g., 15 minutes] for sensitive systems and [Duration, e.g., 30 minutes] for other systems.
- **Network Security:** Corporate networks shall be segmented with appropriate access controls between network zones.

3.6 Third-Party Access

Third parties require security review before receiving access to company systems or data.

- All third parties shall undergo security assessment before access is granted.
- Third-party access shall be limited to specific systems and data required for their function.
- Access shall be time-bound and automatically expire upon contract termination.
- Third-party activities shall be monitored and logged.

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	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.2, 3.3	SOC 2 Trust Services Criteria	CC6.2 - Prior to issuing system credentials...
3.2, 3.6	SOC 2 Trust Services Criteria	CC6.3 - Authorization, modification, and removal of access...

5. Definitions

- **Least Privilege:** The security principle of restricting access rights for users to the minimum permissions needed to perform their work.
- **Privileged Account:** A user account with elevated permissions, such as administrator or system accounts.
- **Multi-Factor Authentication (MFA):** An authentication method requiring two or more verification factors to gain access.
- **System Owner:** The individual responsible for a specific system or application, typically a manager or technical lead.

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Own, review, and update this policy annually. Monitor access controls and ensure compliance with policy requirements.
IT Department	Implement and manage technical access controls. Process access requests and conduct access provisioning, modification, and deprovisioning.
Managers / System Owners	Request and approve access for their teams. Conduct periodic access reviews and ensure team members follow access policies.
All Workforce Members	Follow access control requirements, use only assigned accounts, and report unauthorized access or suspicious activity.

Network Acceptable Use Policy (AC-POL-002)

1. Objective

The objective of this policy is to establish acceptable use rules for **[Company Name]**'s network and internet access that meet SOC 2 requirements while maintaining practical implementation. This policy protects company information resources and ensures a secure, productive work environment.

2. Scope

This policy applies to all **[Company Name]** workforce members and anyone granted access to company network and information systems. It covers all network resources including internet access, email, cloud services, and devices connected to the corporate network.

3. Policy

All use of **[Company Name]**'s network resources must be conducted in a secure, professional manner that supports business objectives.

3.1 General Use and Ownership

- **Company Property:** All network infrastructure, systems, and data are the property of **[Company Name]**.
- **Monitoring:** Network traffic may be monitored for security threats and policy compliance in accordance with applicable laws.
- **Business Purpose:** Network resources are provided for business activities. Limited personal use is permitted if it does not interfere with work performance or violate company policies.

3.2 Security Requirements

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

- **Credentials:** Account credentials must not be shared. Each user must use only their assigned accounts.
- **Malicious Software:** Introducing malicious software is prohibited. Exercise caution with email attachments and links from unknown sources.
- **Security Incidents:** Report suspected security incidents, unauthorized access, or vulnerabilities immediately to the **[Role Title, e.g., IT Manager/Security Officer]**.

- **Data Protection:** Transmission of sensitive company data must use approved, encrypted methods.

3.3 Prohibited Activities

The following activities are prohibited when using company network resources:

- **Illegal Activities:** Any activity that violates local, state, or federal law, including harassment, copyright infringement, or fraud.
- **Circumventing Security:** Attempting to bypass or disable security controls such as firewalls or content filters.
- **Unauthorized Access:** Accessing systems, data, or accounts without explicit authorization.
- **Disruptive Behavior:** Activities that could disrupt network services or degrade performance for other users.
- **Unauthorized Data Transfer:** Using unapproved file-sharing services or transferring company data to personal cloud storage accounts.
- **Inappropriate Content:** Accessing, downloading, or distributing content that violates company professional conduct standards.

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	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.2, 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:** Company-owned or managed hardware and software providing network connectivity and services, including internet connections, wireless access points, and communication platforms.
- **Sensitive Data:** Any company information requiring protection, including customer data, financial information, and proprietary business information.

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Own, review, and update this policy annually. Monitor network activity for security and compliance purposes.
IT Department	Implement technical controls to enforce this policy. Investigate and respond to security incidents.
Managers	Ensure team members understand and follow this policy. Address policy violations in consultation with IT and HR.
All Workforce Members	Comply with this policy and use network resources responsibly. Report violations or security concerns immediately.

Remote Work Policy (AC-POL-003)

1. Objective

The objective of this policy is to establish security requirements for remote access to **[Company Name]**'s information systems that meet SOC 2 requirements while enabling workforce productivity. This policy ensures the protection of company data and systems when accessed from locations outside corporate offices.

2. Scope

This policy applies to all **[Company Name]** workforce members who work remotely, either full-time, part-time, or occasionally. It covers work from any location outside designated corporate offices, 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 securely to protect company information and systems from unauthorized access or disclosure.

3.1 Secure Network Connectivity

Workforce members must use secure network connections for all remote work.

- **VPN Requirement:** All access to internal company systems and sensitive data must use the company-approved Virtual Private Network (VPN).
- **Secure Networks:** Public or untrusted Wi-Fi networks may not be used for accessing sensitive company data. When using public networks for general tasks, VPN is mandatory.
- **Home Network Security:** Home wireless networks must be secured with strong encryption (WPA2 or better) and complex, unique passwords.

3.2 Device Security Requirements

Any device used to access company resources remotely must meet comprehensive security standards:

- **Encryption:** Full-disk encryption must be enabled on all devices.

- **Access Control:** Devices must be protected with strong passwords or biometric controls and configured to automatically lock after [Number, e.g., 15] minutes of inactivity.
- **Malware Protection:** Company-approved anti-malware software must be installed and kept current.
- **Updates:** Operating systems and applications must be kept up-to-date with security patches.

3.3 Data Handling and Physical Security

Workforce members must protect both digital and physical security when working remotely.

- **Data Storage:** Sensitive company data may not be stored locally on personal devices. All sensitive data must be accessed through company-managed systems or cloud platforms.
- **Physical Privacy:** Take measures to prevent unauthorized viewing of screens in public or shared spaces, including use of privacy screens when appropriate.
- **Information Privacy:** Confidential information must not be discussed where conversations can be overheard.
- **Document Security:** Printed documents containing sensitive information must be handled securely and properly destroyed when no longer needed.
- **Asset Protection:** Company equipment must be physically secured and never left unattended in vehicles or public locations. Loss or theft must be reported to the [Role Title, e.g., IT Manager/Security Officer] within [Number, e.g., 24] hours.

3.4 Personal Device Use

Use of personal devices for company work requires adherence to security requirements:

- **Registration:** Personal devices must be registered with the IT Department before accessing company resources.
- **Security Software:** Required security software must be installed and maintained on personal devices.
- **Data Removal:** Upon employment termination, all company data and applications must be securely removed from personal devices.

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	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.1, 3.2	SOC 2 Trust Services Criteria	CC6.6 - The entity implements logical access security measures for assets...
3.3	SOC 2 Trust Services Criteria	CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software.

5. Definitions

- **Remote Work:** Work performed for **[Company Name]** from locations outside designated corporate offices.
- **Virtual Private Network (VPN):** A secure, encrypted connection over a public network to access company systems.
- **Company-Provided Equipment:** Hardware owned by **[Company Name]** and issued to workforce members.
- **Sensitive Data:** Company information requiring protection, including customer data, financial information, and proprietary business information.

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Own, review, and update this policy annually. Monitor remote access for compliance and security issues.
IT Department	Maintain VPN and remote access technologies. Assist workforce members with secure device configuration.

Role	Responsibility
Managers	Ensure team members understand and follow this policy. Report security concerns to the [Role Title, e.g., IT Manager/Security Officer] .
All Workforce Members	Follow this policy when working remotely. Secure remote work environments and company assets. Report security incidents or lost/stolen devices immediately.

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

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

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

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

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

5. Standards Compliance

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

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2 Trust Services Criteria	CC6.8 - System Operations

6. Artifact(s)

A completed policy violation investigation report.

7. Definitions

N/A

8. Responsibilities

Clearly assign responsibility for various aspects of the procedure.

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

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

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

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

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2 Trust Services Criteria	CC6.4 - Physical Access

6. Artifact(s)

A completed and signed BYOD Registration and Consent form.

7. Definitions

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

8. Responsibilities

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

User Access Review Procedure (AC-PROC-003)

1. Purpose

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

2. Scope

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

3. Overview

This procedure describes the process for conducting quarterly access reviews to ensure users maintain only the access necessary for their current role. Regular reviews help maintain the principle of least privilege and support SOC 2 compliance.

4. Procedure

Step	Who	What
1	IT Manager/Security Officer	Generates user access reports for all systems and applications quarterly.
2	IT Manager/Security Officer	Reviews each user's access rights to verify they align with current job responsibilities.
3	Direct Manager	Attests whether access is still appropriate for each team member's current role.
4	IT Manager/Security Officer	Removes any unnecessary access rights identified during the review.
5	IT Manager/Security Officer	Documents the review results and stores as audit records.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security

6. Artifact(s)

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

7. Definitions

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

8. Responsibilities

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

Access Control Management Procedure (AC-PROC-004)

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

4.1 Access Provisioning/Modification

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

4.2 Access Revocation (Termination)

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

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
4.1, 4.2	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security

6. Artifact(s)

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

7. Definitions

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

8. Responsibilities

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

Secure Software Development Policy (ENG-POL-001)

1. Objective

The objective of this policy is to establish comprehensive security requirements for software development at **[Company Name]** that meet SOC 2 requirements while maintaining practical implementation. This policy ensures security controls are integrated into development processes to protect company information systems and maintain system security.

2. Scope

This policy applies to all **[Company Name]** workforce members involved in software development, including developers, testers, and DevOps personnel. It covers all software development projects including new applications, system modifications, and third-party integrations across all environments (development, testing, production).

3. Policy

[Company Name] implements comprehensive security controls in software development processes to meet SOC 2 requirements while maintaining practical implementation.

3.1 Secure Development Process

All software development follows a comprehensive secure development process appropriate for the company's operations.

- **Security Requirements:** Security requirements shall be identified and documented for applications that handle sensitive data.
- **Code Reviews:** All code changes shall be reviewed by at least one qualified team member before deployment to production.
- **Testing:** Security testing shall be performed on applications before production deployment, including vulnerability scanning where technically feasible.
- **Deployment:** Production deployments shall follow documented procedures that include security configuration validation.

3.2 Secure Coding Standards

Development teams shall follow secure coding practices to prevent common vulnerabilities.

- **Input Validation:** All user inputs shall be validated and sanitized before processing.
- **Authentication:** Strong authentication mechanisms shall be implemented, including multi-factor authentication where appropriate.
- **Authorization:** Access controls shall be implemented based on user roles and least privilege principles.
- **Error Handling:** Error messages shall not reveal sensitive system information.
- **Data Protection:** Sensitive data shall be encrypted in transit and at rest using approved cryptographic methods.

3.3 Code Review Process

A documented code review process shall be followed for all production code changes.

- All code changes shall require approval from at least one peer reviewer before merging.
- Code reviews shall include security considerations and follow documented guidelines.
- Review approvals and any identified issues shall be documented in the version control system.

3.4 Security Testing

Security testing shall be performed to identify vulnerabilities before production deployment.

- Vulnerability scanning shall be conducted on applications and infrastructure where technically feasible.
- Security issues identified during testing shall be documented, prioritized, and remediated before production deployment.
- Testing results shall be reviewed and approved by appropriate personnel.

3.5 Third-Party Components

Use of third-party libraries and components shall be managed securely.

- Third-party components shall be evaluated for known security vulnerabilities before use.
- Third-party components shall be kept up-to-date with security patches.
- An inventory of third-party components shall be maintained for security tracking purposes.

3.6 Security Training

Development team members receive comprehensive security training appropriate to their roles.

- New team members shall receive secure coding training within [Number, e.g., 90] days of starting.
- Annual security training updates shall be provided to all development team members.
- Training completion shall be tracked and documented.
- 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.

3.4 Dynamic Testing and Security Assessment

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

3.4.1 Dynamic Application Security Testing (DAST)

Automated Security Scanning:

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

Interactive Application Security Testing (IAST):

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

3.4.2 Penetration Testing Requirements

Internal Penetration Testing:

- Applications handling Confidential data shall undergo annual penetration testing
- Testing shall be performed by qualified internal security team members or approved third parties
- Testing scope shall include application logic, authentication, authorization, and data protection
- Network-level testing shall validate infrastructure security controls
- Social engineering testing shall assess human factors in application security

External Penetration Testing:

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

3.5 Third-Party Component Management

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

3.5.1 Dependency Scanning and Management

Automated Dependency Scanning:

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

- Dependency inventory shall be maintained for all applications and systems

Vendor Component Assessment:

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

3.5.2 Open Source Security Management

Open Source Governance:

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

Vulnerability Response:

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

3.6 DevOps and CI/CD Security

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

3.6.1 Secure CI/CD Pipeline

Pipeline Security Controls:

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

Infrastructure as Code (IaC) Security:

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

3.6.2 Secrets Management

Credential Protection:

- Application secrets, API keys, and credentials shall never be stored in source code
- Dedicated secrets management systems shall be used for all sensitive credentials
- Secrets shall be encrypted at rest and in transit
- Regular rotation of secrets and credentials
- Audit logging for all secrets access and usage

Environment Separation:

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

3.7 Security Training and Awareness

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

3.7.1 Developer Security Training

Initial Training Requirements:

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

Ongoing Training and Awareness:

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

3.7.2 Security Champions Program

Security Champion Selection:

- Designated security champions within each development team
- Additional security training and certification for champions
- Regular security champion meetings and knowledge sharing
- Champion responsibility for promoting security within their teams
- Recognition and incentives for effective security championship

4. Standards Compliance

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

Policy Section	Standard/Framework	Control Reference
All	SOC 2 Trust Services Criteria	CC8.1 - System Development
3.3, 3.4	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
3.2	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security

5. Definitions

Code Review: The systematic examination of source code by peers to identify defects and security vulnerabilities before deployment.

Secure Coding: Programming practices that prevent common security vulnerabilities and implement appropriate security controls.

Third-Party Component: External software libraries, frameworks, or modules used in application development.

Vulnerability Scanning: Automated process of identifying security weaknesses in applications and systems.

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Develop and maintain secure development policies. Oversee security testing and ensure compliance with security standards.
Development Team Lead	Ensure team compliance with secure development practices. Coordinate code reviews and manage security training for the team.
Software Developers	Follow secure coding standards, participate in code reviews, and complete required security training.
All Development Team Members	Report security vulnerabilities, follow established procedures, and support security initiatives.

Change Control Policy (ENG-POL-002)

1. Objective

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

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.

1. Objective

The objective of this policy is to establish a comprehensive change management process for **[Company Name]**'s production systems that meets SOC 2 requirements while maintaining practical implementation. This policy ensures changes are properly authorized, tested, and documented to maintain system stability and security.

2. Scope

This policy applies to all workforce members involved in making changes to production systems, applications, and infrastructure. This includes all code changes, system configurations, and database modifications that affect production environments.

3. Policy

All changes to production environments shall follow a documented process to ensure system stability, security, and auditability.

3.1 Standard Change Process

All non-emergency changes shall follow this process:

- **Planning:** Changes shall be planned and documented with business justification and technical requirements.

- **Development:** Code and configuration changes shall be developed in non-production environments.
- **Review:** All changes shall be reviewed and approved by at least one qualified team member before production deployment.
- **Testing:** Changes shall be tested to verify functionality and identify potential issues before production deployment.
- **Approval:** Production deployment shall require documented approval from authorized personnel.
- **Documentation:** All changes shall be documented with details of what was changed, who approved it, and when it was deployed.

3.2 Emergency Changes

Emergency changes to resolve critical issues may follow an expedited process but require:

- **Authorization:** Emergency changes require approval from the [Role Title, e.g., Engineering Lead] and [Role Title, e.g., IT Manager/Security Officer].
- **Review:** Peer review is still required but may be expedited to address the emergency.
- **Documentation:** Emergency changes shall be fully documented within [Number, e.g., 24] hours of deployment.
- **Follow-up:** A review of emergency changes shall be conducted within [Number, e.g., 3] business days to identify process improvements.

3.3 Change Documentation

All changes shall be properly documented and tracked:

- **Change Records:** Each change shall have a record that includes description, justification, approver, and deployment date.
- **Version Control:** Code changes shall be managed through version control systems with appropriate branching and review processes.
- **Audit Trail:** Change documentation shall be maintained for audit purposes and compliance review.

3.4 Production Access Controls

Access to production systems shall be controlled and monitored:

- **Restricted Access:** Production system access shall be limited to authorized personnel only.
- **Privileged Access:** Administrative access to production systems shall require additional approval and monitoring.
- **Access Logging:** All production system access and changes shall be logged for security monitoring.

3.5 Change Communication

Relevant stakeholders shall be notified of changes that may impact operations:

- **Internal Notification:** Team members shall be notified of upcoming production changes through established communication channels.
- **Impact Assessment:** Changes with potential customer impact shall be communicated to appropriate stakeholders in advance.

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	SOC 2 Trust Services Criteria	CC8.1 - The entity designs, develops, and implements controls over change management.

5. Definitions

- **Change:** Any modification to production code, system configurations, or database content.
- **Production Environment:** The live environment that serves [Company Name]’s customers and processes real data.
- **Emergency Change:** A modification required to resolve a critical production issue or security vulnerability.

6. Responsibilities

Role	Responsibility
Development Team	Develop, test, and document changes in accordance with this policy. Conduct peer reviews.
IT Manager/Security Officer	Review changes for security implications and approve emergency changes.
Engineering Lead	Provide approval for production changes and authorize emergency changes.

Infrastructure Security Policy (ENG-POL-003)

1. Objective

The objective of this policy is to establish security requirements for the design, implementation, operation, and maintenance of **[Company Name]**'s IT infrastructure. This policy ensures that all infrastructure components including cloud services, networks, servers, databases, and supporting systems are configured and managed with appropriate security controls to protect the confidentiality and integrity of information systems while maintaining SOC 2 compliance.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, and third parties involved in the design, deployment, configuration, or management of IT infrastructure. It encompasses all infrastructure components including cloud platforms, virtual machines, databases, networks, storage systems, backup infrastructure, monitoring systems, and security tools. This policy covers production, staging, and development environments.

3. Policy

[Company Name] shall implement layered security controls across all infrastructure components to ensure protection against threats and maintain SOC 2 compliance.

3.1 Infrastructure Security Framework

A security framework shall be implemented across all infrastructure components to ensure consistent security posture.

- Network security controls including firewalls, security groups, and access control lists
- Identity and access management (IAM) with role-based access control and least privilege
- Data protection through encryption at rest and in transit
- Logging and monitoring integration across infrastructure components
- Incident response capabilities with recovery procedures

3.2 System Security and Hardening

Infrastructure systems shall be configured according to security baselines and maintained with current security updates.

- Security baselines for operating systems and platforms shall be documented and implemented

- Removal of unnecessary services, protocols, and software components
- Vulnerability scanning shall be conducted at least quarterly for production systems
- Patch management shall be performed according to defined timeframes
- Network segmentation for different security zones

3.3 Access Control and Authentication

Infrastructure access shall be controlled through formal processes implementing least privilege principles.

- Multi-factor authentication (MFA) required for all administrative access
- Role-based access control (RBAC) with predefined roles and permissions
- Quarterly access reviews for administrative and privileged accounts
- Immediate access revocation upon role changes or employment termination
- Audit logging for all infrastructure access and changes

3.4 Data Protection and Encryption

Data protection controls shall ensure the confidentiality and integrity of information within the infrastructure.

- Encryption at rest for all sensitive data storage including databases and file systems
- Encryption in transit using TLS 1.2 or higher for all network communications
- Secure key management using cloud-native key management services
- Regular key rotation according to defined schedules
- Backup data encryption for all backup media and archives

3.5 Infrastructure Management and Change Control

Infrastructure deployments and changes shall be managed through documented processes to maintain security and stability.

- All infrastructure changes shall be documented, tested, and approved before implementation
- Version control shall be used for infrastructure code and configuration management
- Security scanning of infrastructure templates and configurations
- Automated deployment pipelines with security validation
- Change tracking and rollback capabilities for configuration modifications

3.6 Backup and Recovery

Backup and recovery capabilities shall ensure business continuity and data protection.

- Regular automated backups for all critical systems and data
- Encryption of all backup data at rest and in transit
- Geographic distribution of backups for disaster recovery
- Backup integrity validation shall be performed at least quarterly for critical systems
- Documented backup and recovery procedures with defined recovery time objectives

3.7 Monitoring and Incident Response

Infrastructure monitoring shall provide threat detection and support incident response activities.

- Continuous monitoring of infrastructure components and services
- Centralized log collection and analysis with appropriate retention periods
- Automated threat detection and alerting capabilities
- Integration with organizational incident response procedures
- Evidence preservation capabilities for infrastructure incidents

4. Standards Compliance

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

Policy Section	Standard/Framework	Control Reference
3.1, 3.3	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.2	SOC 2 Trust Services Criteria	CC6.6 - Network Security
3.4	SOC 2 Trust Services Criteria	CC6.7 - Data Transmission
3.6	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
3.7	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
3.5	SOC 2 Trust Services Criteria	CC8.1 - Change Management

5. Definitions

Encryption at Rest: Protection of data stored on disk or other storage media through cryptographic methods.

Encryption in Transit: Protection of data while being transmitted between systems through cryptographic methods.

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

Multi-Factor Authentication (MFA): Authentication method requiring two or more verification factors to gain access.

Role-Based Access Control (RBAC): Method of restricting system access based on the roles of individual users within an organization.

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Develop infrastructure security policies, implement security controls, monitor infrastructure security, and coordinate incident response.
IT Department	Design and implement secure infrastructure, manage security configurations, ensure compliance with security policies, and maintain system hardening.
All Workforce Members	Follow infrastructure security policies, report security issues, and participate in security training related to infrastructure usage.

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 that process or store sensitive customer data.

3. Overview

This procedure outlines the security testing requirements for applications, including automated security scans integrated into the development process and periodic security assessments to identify and remediate vulnerabilities.

4. Procedure

4.1 Automated Security Testing

Step	Who	What
1	Development Team	Integrates automated security scanning tools into the development pipeline to check code for common vulnerabilities.
2	Development Team	Reviews security scan reports and addresses high-severity findings before production deployment.
3	Development Team	Documents remediation efforts and tracks resolution of identified security issues.

4.2 Security Assessments

Step	Who	What
1	IT Manager/Security Officer	Conducts or arranges annual security assessments for applications handling sensitive data.
2	IT Manager/Security Officer	Reviews assessment findings and prioritizes remediation based on risk level.
3	Development Team	Implements remediation plan for identified vulnerabilities within established timeframes.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
4.1 - 4.2	SOC 2 Trust Services Criteria	CC7.1 - System Operations

6. Artifact(s)

Security scan reports and annual security assessment documentation with remediation tracking.

7. Definitions

Security Scanning: Automated tools that analyze application code or running applications to identify potential security vulnerabilities.

Security Assessment: Comprehensive evaluation of application security including testing and review of security controls.

8. Responsibilities

Role	Responsibility
Development Team	Implements security scanning, reviews findings, and remediates identified vulnerabilities.

Role	Responsibility
IT Manager/Security Officer	Manages security assessments and provides guidance on vulnerability remediation priorities.

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 creates a remediation plan (e.g., wait for a patched version) or formally document a risk acceptance rationale.
5	Development Team Lead	Based on the review and any remediation plan, formally approves or denies the use of the component in the project documentation or ticket.

5. Standards Compliance

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

6. Artifact(s)

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

7. Definitions

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

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

8. Responsibilities

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

Standard Change Management Procedure (ENG-PROC-003)

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

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

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

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2 Trust Services Criteria	CC8.1 - Change Management

6. Artifact(s)

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

7. Definitions

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

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

8. Responsibilities

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

Role	Responsibility
Engineering Lead	Provides final authorization for the change to be deployed to production.

Emergency Change Management Procedure (ENG-PROC-004)

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

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

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2 Trust Services Criteria	CC8.1 - Change Management

6. Artifact(s)

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

7. Definitions

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

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

8. Responsibilities

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

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

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

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

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

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

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
2, 4	CIS Controls	Control 4, 5

6. Artifact(s)

A compliance scan report confirming adherence to the security baseline.

7. Definitions

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

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

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

8. Responsibilities

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

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

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

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

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

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security

6. Artifact(s)

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

7. Definitions

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

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

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

8. Responsibilities

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

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

Schedule of Security Procedures (ISMS-SUP-001)

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

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

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

Procedure (Code)	Primary Owner	Description
Internal Audit Procedure (SEC-PROC-002)	Head of Internal Audit	Outlines the process for planning, conducting, and reporting on annual internal audits of the Information Security Management System.
Risk Assessment Procedure (SEC-PROC-004)	Security Officer	Establishes a systematic process for conducting risk assessments annually and on an ad-hoc basis when significant changes occur.

Procedure (Code)	Primary Owner	Description
Incident Response Plan (IRP) ([RES-PROC-001])	Security Team	Provides actionable steps for responding to incidents, including conducting annual training and simulation exercises.
Cryptographic Key Lifecycle Management Procedure (OP-PROC-001)	Security Engineering Team	Provides technical steps for the secure lifecycle of cryptographic keys, including their annual rotation.
Application Security Testing Procedure (ENG-PROC-001)	Security Team	Details the process for conducting security testing, including annual penetration tests for applications handling sensitive data.

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

Procedure (Code)	Primary Owner	Description
Password Policy Exception Procedure (SEC-PROC-003)	Security Officer	Provides a formal process for requesting, reviewing, and documenting exceptions to the Password Policy.
Vendor Risk Assessment and Onboarding Procedure (SEC-PROC-005)	Security Team	Details the process for assessing a new vendor's security posture before engagement.
AI Tool Risk Assessment and Approval Procedure (SEC-PROC-007)	AI Governance Committee	Defines the process for performing a risk assessment on new AI tools before they are approved for use.

Procedure (Code)	Primary Owner	Description
Vulnerability Management Procedure (SEC-PROC-008)	Security Team	Describes the continuous workflow for identifying, prioritizing, remediating, and verifying system vulnerabilities.
Vulnerability Management Exception Procedure (SEC-PROC-009)	Security Officer	Outlines the process for formally requesting and documenting an exception to a vulnerability remediation Service Level Agreement (SLA).
Acceptable Use Policy Violation Investigation Procedure (AC-PROC-001)	Security Officer	Defines the process for investigating and responding to reported violations of the acceptable use policy.
Bring Your Own Device (BYOD) Onboarding Procedure (AC-PROC-002)	IT Department	Establishes the process for registering and securing a personally-owned device for access to company resources.
Access Control Management Procedure (AC-PROC-004)	IT Department	Defines the process for managing the lifecycle of user access, including provisioning, modification, and revocation.
Data Breach Risk Assessment Procedure ([RES-PROC-002])	Privacy Officer	Guides the formal risk assessment required to determine if an incident qualifies as a notifiable breach.
Post-Incident Review Procedure ([RES-PROC-003])	Incident Commander	Outlines the process for conducting a formal ‘lessons learned’ review after a significant incident is resolved.
Mobile Device Onboarding and Security Configuration Procedure (OP-PROC-002)	IT Security Team	Details the steps for enrolling a mobile device in the MDM system and ensuring it meets security requirements.
Lost or Stolen Mobile Device Response Procedure (OP-PROC-003)	IT Security Team	Provides the immediate steps to take when a mobile device used for company business is reported lost or stolen.

Procedure (Code)	Primary Owner	Description
Secure Media Disposal and Sanitization Procedure (OP-PROC-004)	IT Team	Provides instructions for securely destroying or sanitizing media that is at the end of its lifecycle.
Legal Hold Procedure (OP-PROC-005)	Legal Team	Outlines the steps for issuing, tracking, and releasing a legal hold on information relevant to legal matters.
Workforce Screening and Background Check Procedure (OP-PROC-006)	Human Resources (HR)	Outlines the formal process for conducting required background checks on all candidates for employment.
Employee Onboarding and Offboarding Security Procedure (OP-PROC-007)	Human Resources (HR)	Provides a formal checklist to ensure all security tasks are completed during employee onboarding and termination.
Security Policy Sanction Procedure (OP-PROC-008)	Manager & HR	Describes the process for documenting security policy violations and applying appropriate disciplinary actions.
Third-Party Component Security Review Procedure (ENG-PROC-002)	Development Team Lead	Defines the steps for reviewing and approving the use of new third-party software components.
Standard Change Management Procedure (ENG-PROC-003)	Engineering Lead	Details the process for managing a standard, non-emergency change to a production application or configuration.
Emergency Change Management Procedure (ENG-PROC-004)	Engineering & Security Teams	Outlines the expedited process for authorizing and deploying an emergency change to resolve a critical issue.
System Hardening and Baselining Procedure (ENG-PROC-005)	Security Team	Describes the process for applying security baselines to new systems and verifying their ongoing compliance.

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

RACI Definitions:

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

Consolidated Roles for a ~50-Person Company:

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

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

ISMS HIGH-LEVEL RACI CHART (ISMS-SUP-002)

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

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

1. Objective

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

2. Scope

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

3. Policy

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

3.1 Encryption Requirements

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

Confidential Data Requirements:

- Data at rest: Encrypted using AES-256 or equivalent approved algorithm
- Data in transit: Encrypted using TLS 1.2 or higher with strong cipher suite configuration
- Mobile devices and removable media: Full device/media encryption mandatory
- Database encryption for sensitive data fields using transparent data encryption (TDE) or column-level encryption
- Email encryption for messages containing sensitive data
- Backup encryption for all backup media and archives

Authentication Credentials:

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

3.2 Encryption Standards and Algorithms

Only cryptographically strong, industry-standard algorithms and protocols approved by the **[Role Title, e.g., IT Manager/Security Officer]** shall be used.

Approved Symmetric Encryption Algorithms:

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

Approved Asymmetric Encryption Algorithms:

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

Approved Hash Functions:

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

Prohibited Algorithms:

- DES, 3DES, MD5, SHA-1, RC4, RSA keys shorter than 3072 bits, SSL v2/v3, TLS 1.0/1.1

3.3 Key Management Framework

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

Key Management Principles:

- Separation of duties for key management roles and responsibilities
- Least privilege access to cryptographic keys
- Secure key generation using approved cryptographically secure random number generators
- Keys stored separately from the data they protect
- Multi-factor authentication required for access to key management systems

Key Rotation and Lifecycle:

- Data encryption keys: Annually or after encrypting **[Amount, e.g., 1TB]** of data

- SSL/TLS certificates: Annually or as required by Certificate Authority
- Authentication keys (e.g., API keys): Every **[Duration, e.g., 6 months]**
- Emergency key rotation upon suspected compromise or security incidents

Key Destruction:

- Cryptographic keys shall be securely destroyed when no longer required
- Secure deletion methods (cryptographic erasure, overwriting with random data)
- All key destruction activities logged and auditable

3.4 Digital Certificates and PKI

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

- Certificate requests shall be validated and approved through a documented process
- Certificate revocation capabilities shall be maintained through Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP)
- Automated monitoring shall ensure expired or revoked certificates are removed from systems

3.5 Cloud Encryption

All use of cloud services must adhere to cryptographic requirements defined in the Infrastructure Security Policy (ENG-POL-003).

- Customer-managed encryption keys (CMEK) shall be used for production data stores containing Confidential data
- Cloud provider encryption services and configurations shall be reviewed and approved before use
- Company-controlled key management services shall be the standard for all cloud-based encryption

3.6 Monitoring and Performance

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

- Encryption overhead shall be measured and optimized
- Cryptographic failures and misconfigurations shall be logged and trigger automated alerts
- Key management system access and activity logs shall be monitored for suspicious activity
- Annual review of cryptographic standards shall be conducted to maintain current security practices

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, 3.3	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.4, 3.5	SOC 2 Trust Services Criteria	CC6.6 - Other Controls to Achieve Logical Access Security
3.3	SOC 2 Trust Services Criteria	CC6.8 - Restricts Access to Encrypted Data

5. Definitions

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

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

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

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

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

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

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Develop encryption policies, oversee key management program, and ensure compliance with cryptographic standards.
IT Department	Implement encryption technologies, manage key management systems, configure encryption systems, and monitor cryptographic controls.
Application Developers	Implement application-level encryption using approved cryptographic libraries and follow secure coding practices.
All Workforce Members	Use encryption tools as required, protect credentials, and report suspected encryption failures or key compromises.

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

1. Objective

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

2. Scope

This policy applies to all [Company Name] workforce members, including employees, contractors, temporary staff, and third parties who use mobile devices to access company information systems, email, applications, or data. It covers all mobile computing devices including smartphones, tablets, laptops, 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).

3. Policy

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

3.1 Mobile Device Requirements

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

Standard Access Devices: Devices with access to email and internal business systems

- Mobile device management (MDM) enrollment required
- Passcode/PIN protection mandatory (minimum [Number, e.g., 6 digits])
- Multi-factor authentication required for business applications
- Device encryption mandatory
- Automatic screen lock after [Duration, e.g., 5 minutes] of inactivity

Confidential Access Devices: Devices with access to Confidential information

- Company-owned devices preferred

- Enhanced MDM enrollment with compliance monitoring
- Hardware-based encryption required
- Continuous compliance monitoring
- Application containerization for business data separation

3.2 Acceptable Mobile Devices

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

Approved Device Types:

- Smartphones running current iOS or Android versions with security patches within [Timeframe, e.g., 90 days]
- Tablets running current iPadOS or Android versions with security patches within [Timeframe, e.g., 90 days]
- Laptops running current Windows, macOS, or approved Linux distributions with latest security updates

Prohibited Devices:

- Devices with modified firmware (jailbroken/rooted devices) - automatically blocked by MDM
- Devices running unsupported or end-of-life operating systems
- Devices with known critical vulnerabilities that are unpatched

3.3 Mobile Device Management (MDM)

All mobile devices accessing company information shall be enrolled in the [Company Name] Mobile Device Management system.

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

MDM Security Policies:

- Minimum passcode/password complexity requirements
- Automatic screen lock after defined inactivity period
- Maximum failed unlock attempts before device lock/wipe
- Automatic device encryption enforcement

- Approved application catalog with pre-approved business applications
- VPN requirements for accessing internal systems
- Prohibition of unsecured Wi-Fi networks for business use

3.4 Bring Your Own Device (BYOD) Program

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

- BYOD participation shall require a formal application and approval process
- Device compatibility assessment and security evaluation are required
- A signed BYOD agreement is mandatory, including consent to security policies and remote wipe capabilities
- Annual device revalidation and security assessment

BYOD Security Requirements:

- Current operating system with latest security patches
- Strong device passcode/biometric authentication
- Automatic screen lock configuration
- Full device encryption enabled
- Remote wipe capability acceptance
- Separation of business and personal data through containerization
- Business applications and data contained within managed workspace
- Selective wipe capability for business data only

3.5 Security Controls and Monitoring

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

- Multi-factor authentication required for all business applications
- Full device encryption mandatory for all devices accessing company information
- Data-in-transit encryption using approved protocols (TLS 1.2 or higher)
- Continuous device compliance monitoring through MDM
- Anomalous behavior detection and alerting
- Integration with security monitoring systems

3.6 Incident Response and Device Management

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

Lost or Stolen Device Procedures:

- All lost or stolen devices must be reported to the **[Role Title, e.g., IT Manager/Security Officer]** immediately
- Remote location and tracking attempts where technically feasible
- Remote lock and wipe procedures
- Access credential revocation and reset
- Incident documentation and lessons learned

Device Lifecycle Management:

- Security assessment and approval process for new devices
- MDM enrollment and configuration
- User training on security requirements
- Regular compliance monitoring and reporting
- Complete data wipe and sanitization upon device retirement
- MDM unenrollment and access revocation

4. Standards Compliance

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

Policy Section	Standard/Framework	Control Reference
3.3, 3.5	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.5	SOC 2 Trust Services Criteria	CC6.7 - Data Transmission
3.6	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
3.3, 3.4	SOC 2 Trust Services Criteria	CC6.3 - Access Management

5. Definitions

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

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

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

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

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

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Develop mobile security policies, manage MDM systems, monitor device compliance, and respond to mobile security incidents.
IT Department	Assist with device enrollment, provide technical support, manage device lifecycle, and maintain MDM configurations.
Human Resources	Integrate mobile security requirements into employment agreements, conduct security training, and manage BYOD program participation.
All Workforce Members	Comply with mobile security requirements, maintain device security configurations, promptly report security incidents, and participate in security training.

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

1. Objective

The objective of this policy is to establish requirements for the retention, archival, and secure disposal of **[Company Name]**'s information assets throughout their lifecycle. This policy ensures that information is retained for appropriate periods to meet business and legal requirements while ensuring secure disposal when information is no longer needed, in compliance with SOC 2 requirements.

2. Scope

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

3. Policy

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

3.1 Data Retention Framework

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

3.1.1 Data Retention Schedule

The **[Role Title, e.g., IT Manager/Security Officer]** shall develop and maintain a formal Data Retention Schedule. This schedule shall be reviewed annually and categorize data types with specific retention periods for each. Examples of categories include:

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

3.1.2 Backup and Archive Retention

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

3.2 Legal Hold and Litigation Support

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

3.2 Legal Hold and Litigation Support

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

3.2.1 Legal Hold Procedures

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

3.2.2 eDiscovery Support

- Information systems shall be capable of identifying, preserving, and producing relevant information
- Search and collection capabilities shall be maintained for electronic information
- Chain of custody procedures shall be followed for all collected information

3.3 Data Disposal Framework

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

3.3.1 Disposal Triggers

Information disposal shall be triggered by:

- Expiration of defined retention periods
- Completion of business processes requiring the information
- System decommissioning or migration activities

- Employee termination (personal information only)
- Contract termination with appropriate notice periods
- Legal hold release after litigation conclusion

3.3.2 Disposal Classification Requirements

Disposal methods shall correspond to information sensitivity levels:

Public Information:

- Standard deletion or disposal methods acceptable
- Standard recycling procedures for physical media

Internal Information:

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

Confidential Information:

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

3.4 Secure Disposal Methods

3.4 Secure Disposal Methods

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

3.4.1 Electronic Media Disposal

Hard Disk Drives and SSDs:

- Software-based secure deletion using approved methods
- Cryptographic erasure where full disk encryption is implemented
- Physical destruction for Confidential information or failed drives

Removable Media:

- Physical destruction for all Confidential information
- Secure overwriting for reusable media containing less sensitive information

Mobile Devices:

- Factory reset combined with encryption
- Physical destruction of storage components for Confidential information
- Remote wipe verification for lost or stolen devices

3.4.2 Physical Document Disposal

- Cross-cut shredding with particle size [**Size, e.g., 4mm x 32mm**] or smaller
- Secure destruction for confidential documents
- Witnessed destruction for Confidential information

3.4.3 Cloud Data Disposal

- Cryptographic erasure using customer-managed encryption keys
- Verification of data deletion from all storage tiers and backups
- Certificate of deletion from cloud service providers

3.5 Disposal Documentation and Verification

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

3.5.1 Documentation Requirements

Disposal records shall include:

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

3.6 Third-Party Disposal Services

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

3.6.1 Vendor Requirements

- Security assessment and approval before engagement
- Appropriate certifications (e.g., NAID AAA, R2, e-Stewards)
- Insurance coverage for data breaches

- Signed confidentiality and security agreements

3.6.2 Vendor Oversight

- Validation of certificates of destruction
- Performance monitoring and contract compliance reviews

3.7 Data Retention Governance

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

- The [Role Title, e.g., IT Manager/Security Officer] shall be responsible for program oversight
- Annual review and approval of the Data Retention Schedule and this policy
- Training programs for workforce members
- Compliance monitoring and reporting

3.8 Monitoring and Compliance

Regular monitoring shall ensure adherence to retention and disposal requirements.

- Regular audits of disposal activities and documentation
- Exception reporting and corrective action procedures
- Annual training on retention and disposal requirements

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	SOC 2 Trust Services Criteria	CC6.5 - Data Disposal
3.7	SOC 2 Trust Services Criteria	CC2.1 - Communication and Information

5. Definitions

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

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

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

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

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

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

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

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

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

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Develop and maintain retention schedules, oversee disposal activities, coordinate legal holds, and ensure compliance with retention policies.
Legal Team	Establish legal retention requirements, issue legal hold notices, support eDiscovery activities, and ensure compliance with legal obligations.
IT Department	Implement secure disposal technologies, verify disposal completion, manage disposal vendors, and ensure security of disposal processes.

Role	Responsibility
Information Owners	Determine business retention requirements, approve disposal activities, participate in retention reviews, and ensure appropriate information handling.
All Workforce Members	Comply with retention requirements, participate in legal holds, properly dispose of information, and report retention violations.

Human Resources Security Policy (OP-POL-004)

1. Objective

The objective of this policy is to define the security requirements and procedures that govern the lifecycle of all **[Company Name]** workforce members. This policy ensures that individuals with access to sensitive company information 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 **[Role Title, e.g., IT Manager/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 (AC-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 (AC-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 **[Role Title, e.g., IT Manager/Security Officer]**.

4. Standards Compliance

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

Policy		
Section	Standard/Framework	Control Reference
3.1, 3.2	SOC 2 Trust Services Criteria	CC2.1 - The entity establishes and communicates the importance of integrity and ethical values...
3.1, 3.2	SOC 2 Trust Services Criteria	CC2.2 - The entity establishes oversight responsibilities and governance processes...

5. Definitions

- **Workforce Member:** All employees, contractors, and temporary staff working for **[Company Name]**.
- **Background Check:** A process of verifying the identity and credentials of a candidate for employment, which may include criminal history, employment verification, and other checks as permitted by law.
- **Sanction:** A penalty or disciplinary action imposed for violating a rule or policy.

6. Responsibilities

Role	Responsibility
Human Resources Department	Own, review, and update this policy annually. Manage the screening, onboarding, and termination processes. Administer the sanction policy in consultation with management.

Role	Responsibility
IT Manager/Security Officer	Advise on the security aspects of HR processes, including background checks and termination procedures. Participate in the investigation of security policy violations.
Managers	Ensure their direct reports complete all required security training. Promptly notify HR of all terminations. Participate in the enforcement of the sanction policy.

All Workforce Members | Comply with all information security policies. Report any suspected policy violations to their manager or the **[Role Title, e.g., IT Manager/Security Officer]**. 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 are trustworthy, properly trained, and managed in a way that minimizes insider risk and upholds the company's commitment to security and compliance. 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 are trustworthy, properly trained, and managed in a way that minimizes insider risk and upholds the company's commitment to security and compliance. New workforce members must be documented prior to access.

3.4 Policy Enforcement

Security policy violations may result in disciplinary action to ensure consistent compliance.

- **Sanctions:** Disciplinary actions may include warnings, additional training, suspension, or termination depending on violation severity.
- **Documentation:** All policy violations and sanctions shall be documented by Human Resources in consultation with the workforce member's manager and **[Role Title, e.g., IT Manager/Security Officer]**. Ensure secure separation when workforce members leave the company.
- **Notification:** Managers must immediately notify Human Resources and IT of any termination.
- **Access Revocation:** All system and facility access must be revoked promptly upon termination as defined in the Access Control Policy (AC-POL-001).
- **Asset Return:** Departing workforce members must return all company property including devices, access badges, and documents.

- **Exit Process:** Human Resources will conduct exit procedures and remind departing individuals of confidentiality obligations. complete security onboarding to understand their responsibilities.
- **Confidentiality Agreements:** All workforce members must sign confidentiality agreements as a condition of employment.
- **Security Training:** New workforce members must complete security awareness training within [Number, e.g., 30] days of starting.
- **Access Provisioning:** System access will be provisioned according to the Access Control Policy (AC-POL-001) based on job role and least privilege principles. yment shall undergo appropriate screening before receiving access to company information systems.
- **Background Checks:** All job offers are contingent upon successful completion of background checks conducted by an approved third-party provider.
- **Scope:** Standard background checks include identity verification, criminal history, and employment verification, in accordance with applicable laws.
- **Review Process:** Adverse findings will be reviewed by Human Resources and the [Role Title, e.g., IT Manager/Security Officer] to determine employment eligibility. Name]** shall implement procedures to ensure workforce security throughout the employment lifecycle.

The objective of this policy is to define essential security requirements for managing [Company Name] workforce members throughout their employment lifecycle. This policy ensures that individuals with access to company information are trustworthy, properly trained, and managed to minimize insider risk while meeting SOC 2 requirements.

2. Scope

This policy applies to all [Company Name] workforce members, including employees, contractors, and temporary staff. It covers all stages of employment from pre-employment screening through termination.

Human Resources Security Policy (OP-POL-004) parent: Operational Policies nav_order: 4 — ### 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 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

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

Policy		
Section	Standard/Framework	Control Reference
3.1, 3.2	SOC 2 Trust Services Criteria	CC2.1 - The entity establishes and communicates the importance of integrity and ethical values...
3.1, 3.2	SOC 2 Trust Services Criteria	CC2.2 - The entity establishes oversight responsibilities and governance processes...

5. Definitions

- **Workforce Member:** All employees, contractors, and temporary staff working for [Company Name].
- **Background Check:** The process of verifying identity and credentials of employment candidates, including criminal history and employment verification as permitted by law.

6. Responsibilities

Role	Responsibility
Human Resources	Own, review, and update this policy annually. Manage screening, onboarding, and termination processes. Document and administer policy violations.
IT Manager/Security Officer	Advise on security aspects of HR processes. Participate in policy violation investigations. Ensure access is properly provisioned and revoked.
Managers	Ensure team members complete required security training. Notify HR of terminations promptly. Support policy enforcement activities.
All Workforce Members	Comply with security policies and report suspected violations to management or the [Role Title, e.g., IT Manager/Security Officer].

5. Definitions

- **Workforce Member:** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for [Company Name], is under the direct control of the company,

whether or not they are paid by the company.

- **Background Check:** A process of verifying the identity and credentials of a candidate for employment, which may include criminal history, employment verification, and other checks as permitted by law.
- **Sanction:** A penalty or disciplinary action imposed for violating a rule or policy.

6. Responsibilities

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

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

parent: Operational Policies nav_order: 5 —

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., Secret or Confidential data) must be explicitly approved and listed on the company's official **Software Allowlist**. Any software not on this list is implicitly denied.
- **Blocklist (for Prohibited Software):** Certain categories of software are explicitly prohibited and are maintained on a **Software Blocklist**.

3.2 Software Approval Process

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

- **Request Submission:** A request must be submitted via an IT support ticket, detailing the software's name, purpose, and a justification for its business use.

- **Security Review:** The Security Team will conduct a risk assessment of the requested software. The assessment will consider the software's function, the data it will access, its vendor's reputation, and any known vulnerabilities.
- **Approval or Denial:** Based on the risk assessment, the Security Team will either approve or deny the request. Approved software will be added to the Software Allowlist. The decision will be documented in the IT ticket.

3.3 Prohibited Software Categories

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

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

3.4 Browser Extension Security

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

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

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

3.5 Auditing and Enforcement

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

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

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

Policy		
Section	Standard/Framework	Control Reference
All	SOC 2 Trust Services Criteria	CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software.
3.5	SOC 2 Trust Services Criteria	CC7.1 - The entity uses detection and monitoring procedures to identify changes that are indicative of a control failure.

5. Definitions

- **Endpoint:** Any company-owned or managed computing device, such as a laptop or workstation.
- **Software Allowlist:** An official, centrally managed list of all software and browser extensions that have been vetted and are approved for installation on company endpoints.

- **Software Blocklist:** An official list of specific software applications or categories that are explicitly forbidden from being installed on company endpoints.
- **Shadow IT:** Technology, software, or services used inside an organization without explicit organizational approval.

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	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.
All Workforce Members	Comply with this policy at all times. Request approval for new software as required and refrain from installing prohibited software.

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

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

4.1 Key Generation

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

4.2 Key Distribution

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

4.3 Key Storage

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

4.4 Key Rotation

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

4.5 Key Destruction

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

5. Standards Compliance

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

Procedure Step(s)	Standard/Framework	Control Reference
4.1-4.5	SOC 2 Trust Services Criteria	CC6.7 - Data Transmission

6. Artifact(s)

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

7. Definitions

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

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

8. Responsibilities

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

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

1. Purpose

To detail the steps for enrolling a new or personal device in the Mobile Device Management (MDM) system and ensuring it meets all security configuration 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

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

Procedure Step(s)	Standard/Framework	Control Reference
1-7	SOC 2 Trust Services Criteria	CC6.7 - Data Transmission

6. Artifact(s)

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

7. Definitions

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

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

8. Responsibilities

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

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

1. Purpose

To provide the immediate steps a user and the IT Security Team 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

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

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2 Trust Services Criteria	CC6.4 - Physical Access

6. Artifact(s)

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

7. Definitions

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

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

8. Responsibilities

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

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

1. Purpose

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

2. Scope

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

3. Overview

This procedure outlines the 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

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

Procedure Step(s)	Standard/Framework	Control Reference
4.1-4.2	SOC 2 Trust Services Criteria	CC6.5 - Data Protection
4.1	NIST	SP 800-88

6. Artifact(s)

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

7. Definitions

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

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

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

8. Responsibilities

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

Legal Hold Procedure (OP-PROC-005)

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

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

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

5. Standards Compliance

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

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

6. Artifact(s)

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

7. Definitions

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

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

8. Responsibilities

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

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

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

1. Purpose

To outline the formal process for conducting 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

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

Procedure Step(s)	Standard/Framework	Control Reference
1-7	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security

6. Artifact(s)

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

7. Definitions

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

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

8. Responsibilities

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

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

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

4.1 Onboarding

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

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

4.2 Offboarding

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

5. Standards Compliance

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

Procedure Step(s)	Standard/Framework	Control Reference
4.1-4.2	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security

6. Artifact(s)

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

7. Definitions

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

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

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

8. Responsibilities

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

Security Policy Sanction Procedure (OP-PROC-008)

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

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

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

5. Standards Compliance

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

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2 Trust Services Criteria	CC1.2 - Management Oversight

6. Artifact(s)

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

7. Definitions

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

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

8. Responsibilities

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

Incident Response Policy (RES-POL-001)

1. Objective

This policy establishes a comprehensive incident response framework for **[Company Name]** to effectively detect, respond to, contain, and recover from information security incidents. The policy ensures that security incidents are handled in a coordinated, timely, and effective manner to minimize impact on business operations, protect sensitive data, maintain regulatory compliance with SOC 2 requirements, and preserve evidence for potential legal proceedings.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, third parties, and business associates who may detect, report, or respond to information security incidents. It encompasses all information systems, applications, networks, devices, and data owned, operated, or managed by **[Company Name]**, including cloud services, mobile devices, and third-party systems. This policy covers all types of security incidents including data breaches, malware infections, unauthorized access, denial of service attacks, and physical security breaches.

3. Policy

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

3.1 Incident Response Framework

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

3.1.1 Incident Response Team

The IT Manager/Security Officer leads incident response activities with support from relevant personnel:

- **Incident Commander:** IT Manager/Security Officer responsible for overall incident coordination
- **Technical Response:** IT Department personnel for technical investigation and remediation
- **Communications:** Designated personnel for internal and external communications
- **Legal/Compliance:** Legal counsel and compliance officers for regulatory requirements

- **Business Continuity:** Business unit leaders for operational impact assessment

3.1.1 Incident Response Lifecycle

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

1. Preparation:

- Development and at least annual review of the Incident Response Plan (IRP).
- Establishment and maintenance of a designated Incident Response Team (IRT) with clearly defined roles and responsibilities.
- Annual training and simulation exercises (e.g., tabletop exercises) for the IRT to ensure readiness, with outcomes documented for improvement tracking.
- Deployment and maintenance of tools and technologies mandated for incident detection, analysis, and response.

3.1.2 Incident Response Process

The incident response process follows a structured four-phase approach:

1. Preparation:

- Maintenance of incident response procedures and contact information
- Training and awareness for incident response team members
- Regular testing of incident response capabilities with documented results

2. Detection and Analysis:

- Continuous monitoring of information systems to detect security events
- Initial triage to determine if a potential incident has occurred
- Formal incident declaration and activation of the incident response team
- Impact and severity assessment to classify the incident
- Evidence collection and chain of custody documentation

3. Containment, Eradication, and Recovery:

- Execution of containment strategies to prevent incident spread
- Identification of root cause and all affected systems
- Eradication of the threat (removing malware, disabling accounts, patching vulnerabilities)
- Systematic recovery of affected systems from trusted sources

- Validation that systems are clean before returning to production

4. Post-Incident Activity:

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

3.1.3 Incident Classification

All incidents are classified based on severity and potential impact:

Critical (P1) - Response within 15 minutes:

- Confirmed data breach involving confidential data
- Active compromise of critical systems affecting operations
- Widespread malware infection or ransomware attack
- Physical security breach affecting critical assets

High (P2) - Response within 1 hour:

- Unauthorized access to sensitive systems or data
- Malware infection on critical systems
- Denial of service attacks affecting operations
- Suspected insider threat activity

Medium (P3) - Response within 4 hours:

- Unsuccessful attack attempts against critical systems
- Malware infection on non-critical systems
- Policy violations with potential security impact
- Suspicious network activity or anomalous behavior

Low (P4) - Response within 24 hours:

- Security policy violations without immediate risk
- Failed login attempts within normal thresholds
- Spam or phishing emails reported by users
- Minor physical security issues

3.2 Incident Response Team

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

3.2.1 Core Team Members

Incident Commander:

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

Security Analyst:

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

System Administrator:

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

Legal Counsel:

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

Communications Lead:

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

3.2.2 Extended Team Members

3.2 Incident Detection and Reporting

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

3.2.1 Detection Methods

Automated Detection:

- Security monitoring system alerts and notifications
- Intrusion detection and prevention system alerts
- Antivirus and anti-malware system notifications
- Network anomaly detection and behavioral analysis
- File integrity monitoring and system change detection

Manual Detection:

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

3.2.2 Incident Reporting Procedures

Immediate Reporting Channels:

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

Reporting Requirements:

- All suspected incidents are reported within 2 hours of discovery
- Initial reports may be verbal with written follow-up within 24 hours
- Reports include all available information about the incident
- Workforce members do not investigate incidents independently

3.3 Incident Response Procedures

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

3.3.1 Initial Response Procedures

Incident Verification:

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

Evidence Preservation:

- Preserve all relevant evidence in its original state
- Maintain proper chain of custody documentation
- Create forensic images of affected systems when appropriate
- Secure physical evidence and access logs
- Document all actions taken and decisions made
- Maintain chain of custody for digital and physical evidence
- Take system snapshots or images before making changes
- Collect network traffic captures and log files

3.4.2 Containment Procedures

3.3.2 Containment Procedures

Short-term Containment:

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

Long-term Containment:

- Rebuild compromised systems from clean backups
- Apply security patches and configuration hardening
- Conduct security validation before system restoration

3.3.3 Eradication and Recovery Procedures

Threat Eradication:

- Remove malware and malicious artifacts from systems
- Close security vulnerabilities that enabled the incident

- Validate that all traces of compromise have been eliminated

System Recovery:

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

3.4 Regulatory and Legal Compliance

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

3.4.1 Breach Notification Requirements

When incidents involve potential data breaches:

- Determine whether incident constitutes a data breach under applicable laws
- Assess the risk of harm to affected individuals
- Document the breach assessment decision and rationale
- Comply with applicable notification timelines and requirements
- Coordinate with legal counsel for regulatory notifications

3.5 Communication and Coordination

Effective communication is maintained throughout the incident response process.

3.5.1 Internal Communications

- Immediate notification to executive leadership for Critical incidents
- Regular status updates throughout incident response
- Final incident report with lessons learned and recommendations
- Need-to-know basis for incident details

3.5.2 External Communications

- Timely notification of customers potentially affected by incidents
- Coordination with third-party service providers for response activities
- Notification of business partners and vendors as required
- Coordination with insurance carriers and coverage providers

3.6 Post-Incident Activities

Comprehensive post-incident activities ensure organizational learning and improvement.

3.6.1 Incident Documentation

Incident Report Contents:

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

3.6.2 Lessons Learned and Improvement

- Formal review meeting within 2 weeks of incident closure
- Analysis of response effectiveness and areas for improvement
- Update incident response procedures based on lessons learned
- Implement additional security controls to prevent similar incidents
- Enhance monitoring and detection capabilities
- Update business continuity and disaster recovery plans

4. Standards Compliance

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

Policy Section	Standard/Framework	Control Reference
All	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
3.4, 3.6	SOC 2 Trust Services Criteria	CC7.2 - Controls Monitor Effectiveness
3.7	SOC 2 Trust Services Criteria	CC2.1 - Communication and Information
All	NIST Cybersecurity Framework	RS.RP - Response Planning
3.4	NIST Cybersecurity Framework	RS.CO - Communications
3.7	NIST Cybersecurity Framework	RC.IM - Improvements

5. Definitions

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

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

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

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

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

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

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

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Lead incident response activities, coordinate team communications, ensure regulatory compliance, and approve major response decisions.
IT Security Team	Detect and analyze security incidents, perform technical investigations, implement containment measures, and conduct system recovery.
Legal Counsel	Provide legal guidance, coordinate law enforcement relations, manage litigation holds, and ensure regulatory compliance.

Role	Responsibility
System Administrators	Implement technical containment measures, perform system restoration, maintain evidence integrity, and support forensic activities.
All Workforce Members	Report suspected incidents promptly, cooperate with investigations, follow incident response procedures, and participate in post-incident training.

4. Standards and Controls

This policy maps to the following regulatory and compliance frameworks:

Section	Framework	Control
3.1	SOC 2 Trust Services Criteria	CC7.4 - Response to System Disruptions
3.2	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
3.3	SOC 2 Trust Services Criteria	CC7.2 - System Monitoring
3.4	SOC 2 Trust Services Criteria	CC1.4 - Regulatory Compliance

5. Definitions

Incident: Any actual or suspected compromise of information security that may result in unauthorized access, use, disclosure, modification, or destruction of information.

Incident Commander: Individual responsible for overall coordination and management of incident response activities.

Incident Response Team: Group of individuals responsible for responding to information security incidents.

Threat Actor: Individual or group responsible for an incident or attack against an organization.

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Lead incident response activities, coordinate team communications, ensure regulatory compliance, and approve major response decisions.
IT Security Team	Detect and analyze security incidents, perform technical investigations, implement containment measures, and conduct system recovery.
Legal Counsel	Provide legal guidance, coordinate law enforcement relations, manage litigation holds, and ensure regulatory compliance.
System Administrators	Implement technical containment measures, perform system restoration, maintain evidence integrity, and support forensic activities.
All Workforce Members	Report suspected incidents promptly, cooperate with investigations, follow incident response procedures, and participate in post-incident training.

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

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

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

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

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-10	SOC 2 Trust Services Criteria	CC7.3 - Risk Monitoring

6. Artifact(s)

A completed Incident Report for each declared incident.

7. Definitions

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

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

8. Responsibilities

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

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

1. Purpose

To guide the Security Officer and Incident Response Team through the formal risk assessment process to determine if a security incident qualifies as a notifiable data breach requiring customer and regulatory notification.

2. Scope

This procedure applies to any security incident involving the potential compromise of sensitive customer or company data.

3. Overview

This procedure details the steps for conducting a formal risk assessment to determine the probability that sensitive data has been compromised and whether breach notification requirements apply.

4. Procedure

Step	Who	What
1	Security Officer / IRT	Determine if the security incident involves sensitive customer data or confidential company information.
2	Security Officer / IRT	Assess the probability that sensitive data has been compromised by evaluating the following factors: - The nature and extent of the data involved. - The unauthorized person who accessed the data or to whom it was disclosed. - Whether the data was actually acquired or viewed. - The extent to which the risk to the data has been mitigated.
3	Security Officer	Document the complete risk assessment findings and the final rationale for the determination (i.e., whether it constitutes a notifiable breach) on the Data Breach Risk Assessment form.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-3	SOC 2 Trust Services Criteria	CC7.3 - Risk Monitoring

6. Artifact(s)

A completed and signed Data Breach Risk Assessment form.

7. Definitions

Sensitive Data: Customer information, financial data, personal information, or confidential business information that requires protection under applicable regulations or contractual obligations.

Data Breach: The unauthorized acquisition, access, use, or disclosure of sensitive data that compromises the security, confidentiality, or integrity of the information.

8. Responsibilities

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

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

1. Purpose

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

2. Scope

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

3. Overview

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

4. Procedure

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

5. Standards Compliance

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

6. Artifact(s)

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

7. Definitions

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

8. Responsibilities

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

Information Security Policy (SEC-POL-001)

Information Security Policy (SEC-POL-001)

1. Objective

This policy establishes **[Company Name]**'s Information Security Management System (ISMS) to achieve SOC 2 compliance. This policy defines comprehensive security controls to protect the confidentiality and integrity of company information assets while maintaining practical implementation.

2. Scope

This policy applies to all **[Company Name]** workforce members, including employees, contractors, and temporary staff. It encompasses all company information assets, systems, and data, whether stored on-premises, in cloud services, or accessed remotely. This policy also applies to third parties and vendors who access company systems or data.

3. Policy

[Company Name] is committed to implementing comprehensive information security controls that meet SOC 2 Common Criteria requirements.

3.1 Security Governance and Management

[Company Name] establishes effective security governance.

- An **[Role Title, e.g., IT Manager/Security Officer]** is designated with responsibility for information security. This role may be combined with other IT responsibilities as appropriate.
- Security roles and responsibilities are documented and communicated to all workforce members.
- Information security is integrated into business processes and system changes through documented procedures.

3.2 Risk Management

[Company Name] implements a comprehensive risk management approach focused on SOC 2 requirements.

- An annual risk assessment is conducted to identify security risks to company systems and data.
- High and medium risks are documented and addressed with appropriate controls.
- A risk register is maintained to track identified risks and mitigation efforts.

3.3 Access Control

Access to company systems and data is controlled through formal processes that implement least privilege principles.

- All users have unique user accounts and are authenticated before accessing company systems.
- Multi-factor authentication (MFA) is implemented for all systems containing sensitive data.
- User access is reviewed quarterly for critical systems and annually for all other systems.
- Privileged access is monitored and restricted to authorized personnel only.

3.4 Security Awareness and Training

All workforce members receive security awareness training to understand their security responsibilities.

- New workforce members complete security awareness training within [Number, e.g., 30] days of hire.
- Annual refresher training is provided to all workforce members.
- Training completion is tracked and documented.

3.5 Incident Response

[Company Name] maintains effective incident response capabilities to address security incidents.

- Documented procedures are in place for incident detection, analysis, and response.
- Incidents are classified by severity and handled according to appropriate response procedures.
- All incidents are documented and tracked through resolution.
- A designated incident response team is available to coordinate incident response activities.

3.6 System Monitoring

Continuous monitoring is implemented to detect security threats and anomalous activities.

- Security logs are collected from all critical systems and applications.
- Automated monitoring tools provide real-time alerting for security events.
- Log reviews are conducted regularly to identify potential security issues.

3.7 Data Protection

Company and customer data is protected through comprehensive data protection measures.

- Data classification standards define handling requirements for different data types.
- Encryption is implemented for data in transit and at rest for all sensitive data.
- Data retention and disposal procedures ensure proper data lifecycle management.
- Regular backups are performed and tested to ensure data recoverability.

3.7 Business Continuity

Critical business functions shall be protected through continuity planning.

- Critical systems and data shall be identified and documented.
- Backup procedures shall be implemented and tested at least annually.
- Recovery procedures shall be documented and available to key personnel.

3.8 Vendor Management

Third-party vendors are evaluated and managed to ensure they meet **[Company Name]**'s security requirements.

- Vendor risk assessments are conducted before onboarding new vendors.
- Contracts with vendors include appropriate security requirements and data protection clauses.
- Vendor security practices are reviewed annually.

3.9 Change Management

Changes to systems and applications are managed through formal change control processes.

- Change requests are documented and approved before implementation.
- Testing procedures verify that changes do not introduce security vulnerabilities.
- Emergency changes are documented and reviewed post-implementation.

3.10 Compliance

[Company Name] maintains compliance with applicable regulations and standards, with primary focus on SOC 2 requirements.

- Regular audits and assessments are conducted to verify compliance.
- Compliance gaps are documented and addressed through corrective action plans.

- Management receives regular reports on compliance status.

4. Roles and Responsibilities

Chief Executive Officer (CEO)

- Provides executive leadership and accountability for the overall ISMS.
- Allocates appropriate resources for security initiatives.
- Demonstrates commitment to security through leadership actions.

Chief Information Security Officer (CISO)

- Manages the day-to-day operations of the ISMS.
- Develops and maintains security policies and procedures.
- Conducts security risk assessments and implements controls.
- Reports security metrics and incidents to executive management.

IT Personnel

- Implement and maintain technical security controls.
- Monitor systems for security events and respond to incidents.
- Ensure systems are configured according to security standards.

All Workforce Members

- Follow security policies and procedures in their daily work.
- Report suspected security incidents promptly.
- Complete required security training.
- Protect company and customer information according to data handling requirements.

5. Policy Review and Updates

This policy is reviewed annually and updated as needed to ensure continued effectiveness and compliance with changing business requirements and regulatory standards.

- The CISO leads the annual policy review process.
- Updates are approved by executive management before implementation.
- All workforce members are notified of policy changes and receive updated training as required.

6. Non-Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Non-compliance incidents are investigated and documented according to company HR policies.

6. Responsibilities

Role	Responsibility
Executive Leadership	Provide support and resources for the information security program. Approve security policies and ensure accountability.
IT Manager/Security Officer	Develop, implement, and maintain security policies and procedures. Oversee security operations and incident response.
IT Department	Implement technical security controls and support security operations.
Human Resources	Integrate security requirements into hiring processes and manage workforce security training.
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 and conduct required access reviews.

Password Policy (SEC-POL-002)

1. Objective

The objective of this policy is to establish comprehensive standards for password creation, management, and protection that meet SOC 2 requirements while maintaining practical implementation. Strong password management is essential for preventing unauthorized access to company systems and protecting sensitive data.

2. Scope

This policy applies to all **[Company Name]** workforce members and any third party that requires access to company systems, applications, or 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 requirements. Exceptions must be documented and approved by the **[Role Title, e.g., IT Manager/Security Officer]**.

3.1 Password Requirements

All user passwords must meet these comprehensive standards:

- **Length:** Minimum twelve (12) characters for standard user accounts. Minimum sixteen (16) characters for accounts with administrative privileges.
- **Complexity:** Passwords must contain characters from at least three (3) of the following categories:
 - Uppercase letters (A-Z)
 - Lowercase letters (a-z)
 - Numbers (0-9)
 - Special characters (e.g., !@#\$%^&*())
- **Prohibited Content:** Passwords must not contain:
 - Company names or variations
 - Usernames or personal information
 - Dictionary words or common patterns (e.g., “password”, “qwerty”)

- Consecutive or repeating characters

3.2 Password Management

- **Password Age:** User passwords must be changed at least every [Number, e.g., 90] days.
- **Password History:** Systems must prevent reuse of the previous [Number, e.g., 5] passwords.
- **Account Lockout:** User accounts must be automatically locked for [Duration, e.g., 30 minutes] after [Number, e.g., 5] consecutive failed login attempts.

3.3 Multi-Factor Authentication (MFA)

MFA is required for all workforce members and must be implemented on:

- All systems containing sensitive or confidential data
- Remote access to company networks (e.g., VPN)
- Administrative accounts and privileged access
- Cloud-based business applications and services

Approved MFA methods include authenticator applications, hardware tokens, or biometric identifiers. SMS-based MFA is discouraged for sensitive systems.

3.4 Password Protection

- Passwords must never be shared, written down, or stored in plain text
- Use of a company-approved password manager is strongly encouraged
- Passwords must not be transmitted via email or instant messaging
- Systems must store passwords using strong, salted hashing algorithms

3.5 Password Resets and Initial Passwords

- New accounts must receive randomly generated, temporary passwords
- Users must change temporary passwords upon first login
- Password reset requests must be verified through a secure process
- Service account passwords must be unique and rotated at least annually

4. Standards and Controls

This policy maps to the following regulatory and compliance frameworks:

Section	Framework	Control
3.1, 3.2, 3.4	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.3, 3.5	SOC 2 Trust Services Criteria	CC6.2 - User Access Authentication
3.3	SOC 2 Trust Services Criteria	CC6.3 - User Access Authorization

5. Definitions

- **Multi-Factor Authentication (MFA):** An authentication method that requires two or more verification factors to gain access to a resource.
- **Strong Password:** A password that meets the length and complexity requirements defined in this policy.
- **Workforce Member:** All employees, contractors, and temporary staff working for [Company Name].
- **Service Account:** A non-interactive account used by applications or services to access systems and data.

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Own, review, and update this policy annually. Monitor password-related security and ensure technical controls are implemented.
IT Department	Implement and maintain password policy enforcement across all systems. Manage the password reset process and system configurations.

Role	Responsibility
All Workforce Members	Follow password requirements for all company accounts. Protect credentials and report any suspected compromise immediately.

Risk Management Policy (SEC-POL-003)

1. Objective

The objective of this policy is to establish a comprehensive risk management framework for **[Company Name]** that meets SOC 2 requirements while maintaining practical implementation. This policy ensures that information security risks are systematically identified, assessed, and managed to protect company information assets and maintain business operations.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, and third parties. It encompasses all company information assets, systems, and processes, including cloud services and remote work environments.

3. Policy

[Company Name] implements a comprehensive risk management process that meets SOC 2 Common Criteria requirements.

3.1 Risk Management Framework

[Company Name] establishes an effective risk management process.

- Risk management shall follow a cycle of identification, assessment, treatment, and monitoring.
- Risk management activities shall be documented consistently.
- The framework shall be reviewed annually and updated as needed.
- Risk considerations shall be integrated into system changes and vendor decisions.

3.2 Risk Identification

[Company Name] shall identify information security risks through regular assessment and monitoring.

- A comprehensive risk assessment shall be conducted annually and when significant system changes occur.
- Risk identification shall consider common threats including:
 - Cybersecurity threats (malware, phishing, unauthorized access)

- System failures and outages
- Human error and insider threats
- Natural disasters and environmental hazards
- Third-party and vendor risks

3.3 Risk Assessment

All identified risks shall be analyzed to determine their potential impact and likelihood.

- Impact assessment shall consider financial, operational, and reputational consequences.
- Likelihood assessment shall consider threat capabilities, system vulnerabilities, and existing controls.
- Risk levels shall be categorized as **High**, **Medium**, or **Low** using documented criteria.

3.4 Risk Treatment

[Company Name] shall implement appropriate responses to identified risks based on their level and business impact.

- Risk treatment options include:
 - **Accept:** Monitor risks within acceptable tolerance levels
 - **Avoid:** Eliminate risk by discontinuing or modifying activities
 - **Mitigate:** Implement controls to reduce likelihood or impact
 - **Transfer:** Share risk through insurance or contracts
- High risks shall be addressed with priority and escalated to management.
- Risk treatment plans shall include specific actions, responsible parties, timelines, and success criteria.

3.5 Risk Monitoring and Review

[Company Name] shall monitor risks and the effectiveness of risk treatments on an ongoing basis.

- A risk register shall be maintained to track identified risks, assessments, treatments, and current status.
- Risk levels shall be reviewed quarterly for high risks and annually for medium and low risks.
- Risk status reports shall be provided to management quarterly.

- The annual risk assessment shall validate identified risks and assess program effectiveness.

3.6 Risk Communication

Risk information shall be communicated effectively to support informed decision-making.

- Risk reports shall be provided to management in a clear, actionable format.
- Critical risks shall be escalated immediately to appropriate management levels.
- Risk communication shall include current risk status, treatment progress, and recommendations for improvement.

3.7 Third-Party Risk Management

Risks from third-party vendors and service providers shall be assessed and managed.

- Security assessments shall be conducted before engaging third parties with access to company systems or data.
- Contracts shall include appropriate security requirements and risk allocation provisions.
- Third-party security performance shall be monitored through regular reviews and assessments.

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	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

5. Definitions

Inherent Risk: The level of risk that exists before any controls or mitigation measures are applied.

Residual Risk: The level of risk that remains after controls and mitigation measures have been implemented.

Risk Assessment: The process of identifying, analyzing, and evaluating information security risks.

Risk Register: A document that records identified risks, their assessments, treatments, and current status.

Risk Treatment: The process of selecting and implementing measures to modify risk.

6. Responsibilities

Role	Responsibility
Executive Leadership	Provide support for risk management activities and approve risk treatment decisions for high-level risks.
IT Manager/Security Officer	Own, implement, and maintain the risk management process. Conduct risk assessments and manage the risk register.
IT Department	Support risk assessment activities and implement technical risk controls.
All Workforce Members	Participate in risk identification and report security concerns or incidents.
Managers	Support risk assessment activities within their areas of responsibility and implement assigned risk treatments.

5. Definitions

Business Impact Assessment (BIA): Analysis to identify and evaluate potential impacts resulting from business disruption.

Inherent Risk: The level of risk that exists before any controls or mitigation measures are applied.

Key Risk Indicators (KRIs): Metrics that provide early warning signals of increasing risk exposure.

Residual Risk: The level of risk remaining after controls and mitigation measures have been applied.

Risk Appetite: The level of risk that an organization is willing to accept in pursuit of its objectives.

Risk Assessment: The systematic process of identifying, analyzing, and evaluating risks.

Risk Register: A document that records identified risks, their analysis, and risk response plans.

Risk Tolerance: The acceptable level of variation around risk appetite.

Threat Intelligence: Information about current and emerging security threats and vulnerabilities.

6. Responsibilities

Role	Responsibility
Executive Leadership	Formally document, approve, and annually review the company's risk appetite and tolerance levels. Approve risk treatment strategies for high-risk items. Provide resources for risk management activities.
Security Officer	Own and maintain the risk management program. Conduct risk assessments and coordinate risk treatment activities. Report risk status to leadership.
Information Security Committee	Review and approve risk management policies and procedures. Oversee high-risk treatment decisions and resource allocation.
Risk Management Team	Support risk assessment activities, maintain the risk register, and monitor risk treatment effectiveness.
IT Department	Identify technical risks and vulnerabilities. Implement technical risk controls and participate in risk assessments.

Role	Responsibility
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.

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 and business value. This policy ensures that appropriate security controls are applied consistently across all information types to meet SOC 2 requirements and protect against unauthorized disclosure.

2. Scope

This policy applies to all **[Company Name]** workforce members, including employees, contractors, 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. 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 and integrity.

3.1 Information Classification Framework

[Company Name] shall use a three-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
- Standard business handling requirements

Internal: Information intended for use within **[Company Name]** that should not be disclosed to external parties without authorization.

- Examples: Internal policies, business communications, system documentation, employee contact information
- Requires 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, customer data, strategic plans, proprietary technology, authentication credentials
- Requires enhanced security controls, encryption, audit logging, and formal access approval

3.2 Information Classification Responsibilities

Information classification shall be assigned by designated information owners and applied consistently throughout the information lifecycle.

- Information owners are responsible for the initial classification of data, approving access requests, and ensuring data is handled according to this policy.
- Classification shall be assigned at the time of creation and documented appropriately.
- 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 annually.

3.3 Handling Requirements by Classification Level

Specific security controls shall be implemented based on information classification levels.

3.3.1 Public Information

- Standard business handling requirements
- May be stored on company systems and transmitted via standard business channels
- Standard backup and archival procedures apply

3.3.2 Internal Information

- Access restricted to authorized **[Company Name]** workforce members
- Password-protected when stored on portable devices
- Transmitted via secure channels (encrypted email, secure file transfer)
- Stored on company-approved systems with appropriate access controls
- Covered by confidentiality agreements for third-party access

3.3.3 Confidential Information

- Access granted only on a need-to-know basis with formal approval
- Encrypted when stored on laptops, mobile devices, or removable media using **[Encryption Standard, e.g., AES-256]**
- Transmitted only via encrypted channels (secure email, VPN, HTTPS)

- Stored on secure systems with enhanced access controls and audit logging
- Protected by multi-factor authentication for system access
- All access logged and monitored for unauthorized activity
- Requires appropriate agreements for third-party access
- Must be clearly labeled to indicate classification level
- Subject to data loss prevention (DLP) monitoring and controls

3.4 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 when feasible
- Email communications containing Confidential information shall include classification indicators
- Physical documents shall be marked with classification levels when appropriate
- Storage media shall be labeled with the highest classification level of contained information

3.5 Information Storage and Access Controls

Storage requirements shall be implemented based on information classification levels.

- All information systems shall maintain access control lists restricting access based on classification and business need
- Confidential information shall be stored only on systems with appropriate security controls
- Cloud storage of Confidential information requires encryption and compliance with security standards
- Regular access reviews shall be conducted annually for Confidential information
- Automated tools shall be used where feasible to enforce classification-based access controls

3.6 Information Transmission and Sharing

Information transmission methods shall align with classification requirements.

- Public and Internal information may be transmitted via standard business communication channels
- Confidential information shall be encrypted during transmission using approved encryption methods
- File sharing services shall be approved for specific classification levels and configured with appropriate security settings

- Email systems shall include capabilities to prevent unauthorized transmission of sensitive information

3.7 Information Retention and Disposal

Information shall be retained according to business requirements and then securely disposed of when no longer needed.

- Retention schedules shall be established for each information type considering business and legal requirements
- Secure disposal methods shall be used for all Confidential information:
 - Electronic media: Cryptographic erasure or physical destruction
 - Physical documents: Cross-cut shredding or secure destruction
- Disposal activities shall be documented for Confidential information
- Third-party disposal services shall provide certificates of destruction

3.8 Mobile Device and Remote Access

Appropriate controls shall apply to information access via mobile devices and remote locations.

- Mobile devices accessing Confidential 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 approved security requirements
- Lost or stolen devices shall be reported immediately and remotely wiped if containing sensitive information

4. Standards Compliance

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

Policy Section	Standard/Framework	Control Reference
All	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security
3.5, 3.6	SOC 2 Trust Services Criteria	CC6.7 - Data Transmission
3.7	SOC 2 Trust Services Criteria	CC6.5 - Data Disposal

5. Definitions

Data Loss Prevention (DLP): Technology and processes designed to detect and prevent unauthorized transmission of sensitive information.

Information Owner: The person responsible for the business content and context of information, including classification and access decisions.

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

6. Responsibilities

Role	Responsibility
Information Owners	Classify information assets, approve access requests, conduct periodic classification reviews, and ensure appropriate handling.
IT Manager/Security Officer	Develop and maintain classification policies, monitor compliance, and investigate classification violations.
IT Department	Implement technical controls for each classification level and provide secure storage and transmission capabilities.
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 and approve access requests within their authority.

Vendor and Third-Party Risk Management Policy (SEC-POL-005)

1. Objective

The objective of this policy is to establish requirements for assessing, managing, and monitoring security risks associated with vendors and third-party service providers. This policy ensures that [Company Name] maintains appropriate oversight of external parties who access, process, store, or transmit company information while maintaining SOC 2 compliance.

2. Scope

This policy applies to all [Company Name] workforce members involved in vendor selection, contract negotiation, or ongoing vendor management. It encompasses all external parties including vendors, service providers, consultants, and contractors that have access to [Company Name] information systems, data, or facilities. This policy covers the entire vendor lifecycle from initial assessment through contract termination.

3. Policy

[Company Name] shall implement a vendor risk management program to ensure that all third-party relationships meet security and compliance requirements.

3.1 Vendor Classification and Risk Assessment

All vendors shall be classified based on their risk level and subject to appropriate due diligence and ongoing monitoring.

3.1.1 Vendor Risk Classification

Vendors shall be classified into risk categories based on the following factors:

- Type and sensitivity of data accessed (Confidential, Internal, Public)
- Level of system access required (network, applications, databases, privileged access)
- Business criticality and financial impact
- Duration and scope of engagement

Risk Classifications:

- **High Risk:** Vendors with access to Confidential data or critical systems; cloud service providers; vendors with privileged access
- **Medium Risk:** Vendors with access to Internal data or providing business-critical services

- **Low Risk:** Vendors with limited access to Internal data or no direct system access; vendors providing non-critical services

3.1.2 Pre-Engagement Risk Assessment

Prior to engaging any vendor, appropriate risk assessment shall be conducted based on the vendor's risk classification.

High-Risk Vendor Requirements:

- Comprehensive security questionnaire
- Security assessment report (SOC 2, ISO 27001, or equivalent)
- Financial stability assessment
- Reference checks with existing customers
- Cyber insurance verification

Medium-Risk Vendor Requirements:

- Standard security questionnaire
- Third-party assessment report or self-attestation
- Financial stability review
- Reference checks
- Insurance verification

Low-Risk Vendor Requirements:

- Comprehensive security questionnaire or assessment
- General insurance verification

3.2 Contractual Security Requirements

All vendor contracts shall include appropriate security provisions based on the vendor's risk level and data access requirements.

3.2.1 Standard Security Contract Provisions

All vendor contracts shall include security provisions appropriate to the risk level:

Essential Security Clauses:

- Data protection and confidentiality requirements
- Incident notification and response procedures with defined timeframes
- Right to audit and conduct security assessments when appropriate

- Personnel security requirements for vendor staff
- Insurance and liability provisions
- Compliance with applicable laws and regulations
- Requirement for secure data return or destruction upon contract termination

Additional High-Risk Vendor Clauses:

- Specific security control requirements (encryption, access controls, logging)
- Regular security reporting requirements
- Breach notification procedures with specific timelines
- Subcontractor approval and oversight requirements
- Business continuity and disaster recovery provisions
- Right to terminate for security violations

3.3 Vendor Security Monitoring and Ongoing Assessment

Ongoing monitoring shall be conducted to ensure vendors maintain appropriate security posture throughout the engagement lifecycle.

3.3.1 Continuous Monitoring Requirements

- Annual security questionnaire updates for High-risk vendors
- Review of updated security certifications and assessment reports
- Monitoring of vendor security incidents and breach notifications
- Performance and service level monitoring
- Compliance with contractual security requirements

3.3.2 Periodic Assessments

- High-Risk vendors: Annual security assessment
- Medium-Risk vendors: Assessment every two years or upon contract renewal
- Low-Risk vendors: Assessment upon contract renewal

3.3.3 Vendor Security Incident Management

- Vendors shall notify **[Company Name]** of security incidents within contractually specified timeframes
- **[Company Name]** shall assess the impact of vendor incidents on company operations and data
- Incident response coordination with vendors shall follow documented procedures

3.4 Vendor Access Management

Access granted to vendors shall be controlled and monitored in accordance with the principle of least privilege.

3.4.1 Access Provisioning

- Vendor access requests shall be formally approved by the business owner and **[Role Title, e.g., IT Manager/Security Officer]**
- Access shall be limited to the minimum necessary to perform contracted services
- Vendor personnel shall be individually identified and authenticated
- Multi-factor authentication shall be required for High-risk vendor access

3.4.2 Access Monitoring and Review

- All vendor access shall be logged and monitored for inappropriate activity
- Annual access reviews shall be conducted for all vendors with system access
- Access shall be promptly revoked upon contract termination or personnel changes

3.5 Vendor Onboarding and Offboarding

Formal processes shall be established for vendor onboarding and offboarding to ensure security requirements are met.

3.5.1 Vendor Onboarding Process

1. Risk assessment and classification
2. Security questionnaire and documentation review
3. Contract negotiation including security provisions
4. Security orientation (if required)
5. Access provisioning and testing
6. Ongoing monitoring setup

3.5.2 Vendor Offboarding Process

1. Access revocation and account deactivation
2. Data return or secure destruction verification
3. Equipment and credential return
4. Final security assessment and documentation
5. Contract closure and relationship termination

3.6 Cloud Service Provider Management

Cloud service providers shall be subject to enhanced security requirements due to the sensitivity of data and critical nature of services.

3.6.1 Cloud Provider Requirements

3.6.1 Cloud Provider Requirements

- SOC 2 Type II certification or equivalent (ISO 27001)
- Data encryption at rest and in transit
- Geographic data location controls where required
- Incident response and breach notification procedures
- Business continuity and disaster recovery capabilities
- Regular security assessments and vulnerability testing

3.6.2 Cloud Service Monitoring

- Regular review of service provider security posture and certifications
- Monitoring of provider security advisories and incident notifications
- Assessment of configuration changes and security updates

3.7 Subcontractor Risk Management

Vendors shall be required to manage risks associated with their subcontractors and ensure equivalent security standards.

- Vendors shall obtain written approval before engaging subcontractors for services involving [Company Name] data
- Subcontractors shall be subject to the same security requirements as primary vendors
- Vendors shall maintain oversight of subcontractor security practices
- Notification requirements for subcontractor changes or incidents

4. Standards Compliance

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

Policy Section	Standard/Framework	Control Reference
All	SOC 2 Trust Services Criteria	CC9.1 - Vendor Management
3.1, 3.3	SOC 2 Trust Services Criteria	CC9.2 - Vendor Risk Assessment

Policy Section	Standard/Framework	Control Reference
3.2	SOC 2 Trust Services Criteria	CC9.3 - Vendor Agreements

5. Definitions

Cloud Service Provider: A company that offers network services, infrastructure, or business applications in the cloud.

Due Diligence: The investigation or exercise of care that a reasonable business is expected to take before entering into an agreement or contract.

Service Level Agreement (SLA): A contract between a service provider and customer that defines the level of service expected.

Subcontractor: An entity engaged by a vendor to perform functions or activities on behalf of the vendor.

Vendor Risk Assessment: The process of evaluating the potential risks associated with engaging a third-party vendor.

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Develop vendor security requirements, conduct risk assessments, and monitor vendor security compliance.
Legal/Contracts Team	Negotiate security contract provisions, ensure legal compliance, and manage contract lifecycle.
Business Owners	Define business requirements, approve vendor selections, and monitor service delivery performance.

Role	Responsibility
IT Department	Implement technical controls for vendor access, monitor vendor system activity, and manage vendor integrations.
All Workforce Members	Report vendor security concerns, comply with vendor interaction policies, and protect company information shared with vendors.

Physical Security Policy (SEC-POL-006)

1. Objective

The objective of this policy is to establish 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 and integrity of information assets in compliance with 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, and temporary workspaces 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.

3. Policy

[Company Name] shall implement layered physical security controls appropriate to the cloud-based operating model while ensuring 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.

- Electronic badge access systems shall be implemented for 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 periodic access reviews
- CCTV surveillance systems covering entry/exit points and sensitive areas
- Video retention for minimum **[Duration, e.g., 90 days]** with secure storage

3.2 Remote Work Environment Security

Remote work environments meet comprehensive security requirements to protect company information.

- Dedicated workspace with privacy measures to prevent unauthorized access to company information
- Secure storage for company equipment when not in use
- Physical security of devices and materials in temporary work environments
- Prohibition of accessing Confidential information in public spaces
- Privacy screens required when working on sensitive information in shared spaces

3.3 Equipment and Asset Protection

All company equipment and physical assets shall be protected against theft, damage, and unauthorized access throughout their lifecycle.

- 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
- Secure provisioning process with pre-configured security settings
- Regular physical inventory audits
- Secure decommissioning with verified data destruction
- Return procedures for workforce member separation or equipment refresh

3.4 Removable Media and Storage Security

Removable media and storage devices shall be handled securely to prevent unauthorized access or disclosure.

- 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
- Physical destruction required for all media containing Confidential information
- Certified disposal vendors with appropriate security clearances
- Secure overwriting followed by physical destruction for solid-state media

3.5 Cloud Provider Physical Security Oversight

[Company Name] shall validate the physical security controls implemented by cloud service

providers to ensure appropriate protection of company data and systems.

- 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
- Annual review of cloud providers' security certifications and audit reports
- Validation of physical security controls through review of third-party assessments
- Contractual agreements including physical security standards and incident notification requirements

3.6 Physical Document and Information Security

Physical documents and printed materials containing sensitive information shall be protected throughout their lifecycle.

- Classification and marking of all physical documents based on sensitivity levels
- Locked storage for documents containing Confidential information
- Clean desk policy requiring secure storage of sensitive documents when unattended
- Controlled access to document storage areas with access logging
- Secure printing controls with user authentication at printer before document release
- Secure disposal procedures for printed materials and documents

4. Standards Compliance

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

Policy Section	Standard/Framework	Control Reference
3.1, 3.2	SOC 2 Trust Services Criteria	CC6.4 - Physical Access Controls
3.5	SOC 2 Trust Services Criteria	CC9.1 - Vendor Management

5. Definitions

Clean Desk Policy: Security practice requiring sensitive materials to be secured when workspaces are unattended.

Multi-Factor Authentication: Security process requiring two or more authentication factors for access verification.

Physical Security Perimeter: Physical boundary around facilities, systems, or areas requiring protection.

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Develop physical security policies, oversee facility security measures, coordinate with cloud providers on physical security requirements, and manage physical security incidents.
Facilities Management	Implement and maintain physical security controls, manage visitor access, coordinate with security vendors, and ensure compliance with physical security procedures.
IT Department	Manage equipment security controls, implement device encryption and tracking, coordinate secure disposal, and maintain physical asset inventory.
All Workforce Members	Follow physical security procedures, protect company equipment, report security incidents or concerns, and comply with clean desk and visitor escort requirements.

Clean Desk Policy: Security practice requiring sensitive materials to be secured when workspaces are unattended.

Cloud Service Provider: Third-party organization providing cloud computing services including infrastructure, platforms, or software.

Environmental Controls: Systems and procedures designed to protect against environmental hazards such as fire, flood, temperature extremes, and power failures.

Follow-Me Printing: Secure printing system requiring user authentication at the printer before documents are released.

Multi-Factor Authentication: Security process requiring two or more authentication factors for access verification.

Physical Security Perimeter: Physical boundary around facilities, systems, or areas requiring protection.

Tailgating: Unauthorized access gained by following an authorized person through a controlled access point.

Visitor Management System: Automated system for registering, tracking, and managing facility visitors.

6. Responsibilities

Role	Responsibility
Security Officer	Develop physical security policies, oversee security system implementation, coordinate with facilities management, and ensure compliance with security standards.
Facilities Management	Maintain physical security systems, manage environmental controls, coordinate building security, and ensure compliance with safety regulations.
IT Security Team	Secure IT equipment and infrastructure, coordinate physical and logical security measures, and monitor security events.
Human Resources	Manage badge access provisioning, conduct background checks, coordinate visitor management, and integrate security into HR processes.

Role	Responsibility
Reception/Administrative Staff	Manage visitor registration and badging, monitor lobby areas, enforce visitor policies, and coordinate with security team.
Cloud Security Team	Assess cloud provider physical security controls, monitor cloud security compliance, and coordinate cloud security requirements.
All Workforce Members	Comply with physical security policies, secure workspaces and equipment, challenge unauthorized individuals, and report security incidents.
Managers/Supervisors	Ensure team compliance with physical security policies, approve visitor access, support emergency procedures, and manage physical asset inventory.
Remote Workers	Implement home office security measures, protect company equipment, follow secure work practices, and report security concerns.

AI Acceptable Use Policy (SEC-POL-007)

1. Objective

This policy establishes comprehensive guidelines for the acceptable and secure use of Artificial Intelligence (AI) and Machine Learning (ML) technologies at **[Company Name]**. The policy ensures that AI tools and systems are used responsibly, ethically, and securely while protecting the confidentiality and integrity of company information. This policy addresses the unique risks associated with AI technologies including data privacy, bias, transparency, and regulatory compliance with SOC 2 requirements while enabling innovation and productivity improvements through responsible AI adoption.

2. Scope

This policy applies to all **[Company Name]** workforce members, contractors, third parties, and business associates who use, develop, deploy, or manage AI and ML technologies on behalf of the organization. It encompasses all AI applications including generative AI tools, machine learning models, automated decision-making systems, and AI-powered business applications. This policy covers both internally developed AI systems and third-party AI services, regardless of deployment model, and applies to all business operations and administrative functions.

3. Policy

[Company Name] implements 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 oversees the evaluation, approval, deployment, and monitoring of AI technologies across the organization.

3.1.1 AI Governance Committee

The IT Manager/Security Officer maintains oversight of AI initiatives including:

- Evaluation and approval of AI technologies and use cases
- Regular review of AI risks and ethical considerations
- Development of AI policies and procedures

- Monitoring compliance with AI governance requirements
- Coordination with business units on AI implementations

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

3.1.2 AI Risk Assessment

All AI technologies require a documented risk assessment before implementation, including:

- Data sensitivity analysis to identify confidential information usage
- Security assessment of the AI tool and vendor
- Business impact and risk evaluation
- Privacy considerations for personal data processing

Risk Categories:

- **High Risk:** AI systems processing confidential data or making automated business decisions
- **Medium Risk:** AI systems processing internal data or providing business functions
- **Low Risk:** AI systems processing only public data with limited business impact

3.2 Data Protection and Privacy

AI systems implement comprehensive data protection measures to safeguard sensitive information and ensure privacy compliance.

3.2.1 Data Handling Requirements

- Confidential data usage in third-party AI systems requires approval and appropriate vendor agreements
- Data minimization principles apply to all AI training and inference data
- Encryption required for data at rest and in transit for systems handling confidential data
- Access to AI systems handling sensitive data must be logged and reviewed quarterly

3.2.2 Third-Party AI Service Usage

- The IT Manager/Security Officer maintains an inventory of approved AI services
- Vendor assessment includes data handling practices, security controls, and compliance certifications
- Contractual requirements address data protection, privacy, and compliance obligations
- 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 3.3 Ethical AI Use

AI systems are implemented with appropriate ethical considerations and human oversight.

3.3.1 Ethical Principles

- AI systems are monitored for bias and discriminatory outcomes
- Documentation of AI system capabilities, limitations, and decision-making processes
- User notification when interacting with AI systems or AI-generated content
- Human review required for AI-generated decisions affecting business operations

3.3.2 Human Oversight and Control

- Override capabilities for all automated AI decisions
- Training for workforce members supervising AI systems
- Clear escalation procedures for AI system issues or unexpected outcomes
- Regular validation of AI system performance and accuracy

3.4 AI Security Controls

Comprehensive security controls protect AI systems from threats and ensure system integrity.

3.4.1 AI System Security

- Role-based access control for all AI systems and platforms
- Multi-factor authentication required for AI system access
- Regular access reviews and recertification for AI system users

- API security controls for AI service integrations
- Protection of AI models as intellectual property

3.4.2 AI Data Security

- Encryption of AI training datasets containing sensitive information
- Secure data pipelines for AI model training and validation
- Monitoring and logging of all AI system interactions
- Data loss prevention controls for AI-generated content
- Incident response procedures for AI data security issues

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

3.5 AI Development and Deployment

AI systems follow secure development and deployment practices.

3.5.1 Development Standards

- Secure coding practices for AI system development
- Version control and change management for AI models
- Testing and validation procedures for AI systems
- Documentation requirements for AI system functionality
- Code review processes for AI-generated content

3.5.2 Deployment Controls

- Staged deployment approach for new AI systems
- Performance monitoring and alerting for production AI systems
- Rollback procedures for AI system issues
- Regular updates and patch management for AI platforms

3.6 Acceptable Use Guidelines

Clear guidelines define appropriate and inappropriate AI usage across the organization.

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:

- Automated decision-making for hiring, firing, or promotion without human review
- Processing of confidential data through unauthorized AI systems
- Generation of misleading, false, or deceptive content
- Circumvention of security controls or policy violations

3.6.2 Role-Specific Guidelines

Software Development Teams:

- Code review required for all AI-generated code before production deployment
- Security testing of AI-generated code for vulnerabilities
- Documentation of AI tool usage in development processes

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

3.7 Training and Awareness

All workforce members receive appropriate training on AI policies, risks, and best practices.

3.7.1 AI Training Requirements

- Annual training for all workforce members on AI acceptable use policies
- Role-specific training for users of AI systems and tools
- Privacy and security training for AI applications handling sensitive data
- Regular updates on new AI technologies and policy changes
- 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** |

4. Standards and Controls

This policy maps to the following regulatory and compliance frameworks:

Section	Framework	Control
3.2	SOC 2 Trust Services Criteria	CC6.7 - Data Transmission and Disposal
3.1	SOC 2 Trust Services Criteria	CC2.1 - Communication and Information
3.5	SOC 2 Trust Services Criteria	CC8.1 - System Development
All	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security

5. Definitions

Artificial Intelligence (AI): Computer systems that can perform tasks typically requiring human intelligence, including learning, reasoning, and perception.

Machine Learning (ML): Subset of AI that enables systems to learn and improve from data without explicit programming.

Algorithm Bias: Systematic prejudice in AI systems that results in unfair treatment of certain groups or individuals.

Explainable AI (XAI): AI systems designed to provide understandable explanations for their decisions and recommendations.

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Develop AI governance policies, oversee AI security controls, conduct AI risk assessments, and ensure compliance with AI requirements.
IT Department	Implement AI security controls, monitor AI system security, respond to AI security incidents, and maintain AI security infrastructure.
Data Scientists/AI Engineers	Develop secure and ethical AI systems, implement bias testing, document AI model limitations, and ensure model validation and monitoring.
Business Unit Leaders	Ensure team compliance with AI policies, approve AI tool usage, provide business requirements for AI systems, and support AI governance activities.
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)

Vulnerability Management Policy (SEC-POL-008)

1. Objective

This policy establishes a systematic and continuous process for identifying, prioritizing, remediating, and verifying security vulnerabilities across all of **[Company Name]**'s information assets. The policy ensures that risks to the confidentiality and integrity of data 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 servers, workstations, network devices, applications (both internally developed and third-party), and cloud infrastructure.

3. Policy

[Company Name] implements and maintains a comprehensive vulnerability management program that covers the full lifecycle of vulnerability identification, assessment, remediation, and verification.

3.1 Vulnerability Management Lifecycle

The program follows a continuous four-phase lifecycle:

1. Discovery: Vulnerabilities are identified through multiple methods:

- **Automated Scanning:** Regular 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 are assigned a severity rating using the Common Vulnerability Scoring System (CVSS) version 3.x, enhanced with contextual factors:

- **Asset Criticality:** Based on business importance and data sensitivity
- **Exploitability:** Likelihood of successful exploitation
- **Network Exposure:** Internal vs. external accessibility
- **Threat Intelligence:** Active exploitation in the wild

3. Remediation: Vulnerabilities are remediated by the responsible asset owner within defined timeframes based on severity rating. Remediation may include applying vendor patches, implementing configuration changes, or deploying compensating controls. All remediation activities follow the Change Control Policy (ENG-POL-002).

4. Verification: After remediation, the IT Manager/Security Officer performs verification scans to confirm successful resolution. All verification results are documented in the vulnerability tracking system.

3.2 Vulnerability Scanning

To ensure comprehensive vulnerability discovery, the following scanning schedule is maintained:

- **External Scans:** Unauthenticated scans of all internet-facing systems performed at least weekly
- **Internal Scans:** Authenticated scans of all internal production systems and workstations performed at least monthly
- **Application Scans:** Dynamic and/or static analysis of in-house developed applications performed prior to major releases
- **Scan Result Processing:** All vulnerability scan results are automatically ingested into a centralized tracking system with review within 1 business day

3.3 Remediation Timeframes

Vulnerabilities must be remediated within the following timeframes based on severity:

Severity	CVSS Score	Remediation Timeframe
Critical	9.0 - 10.0	7 days
High	7.0 - 8.9	30 days
Medium	4.0 - 6.9	90 days
Low	0.1 - 3.9	180 days

3.4 Exception Management

When vulnerabilities cannot be remediated within standard timeframes, a formal exception process applies:

- **Request:** Asset owners submit formal exception requests including business justification, risk analysis, and proposed compensating controls
- **Approval:** Exception requests require approval from the asset owner's manager and IT Manager/Security Officer. Critical or High severity vulnerabilities require additional senior management approval
- **Documentation:** All approved exceptions are documented in a centralized risk register
- **Duration:** Approved exceptions are temporary and reviewed quarterly

3.5 Compensating Controls

When remediation is not feasible, documented and testable compensating controls may be implemented to reduce the likelihood or impact of vulnerability exploitation. Compensating controls must be approved through the exception management process.

4. Standards and Controls

This policy maps to the following regulatory and compliance frameworks:

Section	Framework	Control
3.1	SOC 2 Trust Services Criteria	CC7.1 - System Monitoring
3.2	SOC 2 Trust Services Criteria	CC7.2 - System Monitoring
3.3	SOC 2 Trust Services Criteria	CC7.3 - Evaluation and Response
All	SOC 2 Trust Services Criteria	CC6.1 - Logical Access Security

5. Definitions

Common Vulnerability Scoring System (CVSS): Industry standard framework for rating the severity of security vulnerabilities.

Compensating Control: Security measure implemented to provide alternative protection when primary controls cannot be applied.

Penetration Testing: Authorized simulated cyber attack to evaluate system security.

Vulnerability: Weakness in a system that could be exploited to compromise security.

Zero-Day Vulnerability: Previously unknown vulnerability for which no patch is available.

6. Responsibilities

Role	Responsibility
IT Manager/Security Officer	Oversee vulnerability management program, approve remediation plans, coordinate with asset owners, and ensure compliance with remediation timeframes.
IT Department	Perform vulnerability scans, maintain scanning infrastructure, track vulnerabilities in central system, and verify successful remediation.
System Administrators	Implement vulnerability remediation, apply patches and updates, deploy compensating controls, and maintain system security configurations.
Asset Owners	Approve remediation plans for their systems, coordinate remediation activities, submit exception requests when needed, and ensure business continuity during remediation.
All Workforce Members	Report suspected vulnerabilities, comply with patch management procedures, and support vulnerability remediation activities as required.

Information Security Committee Charter Procedure (SEC-PROC-001)

1. Purpose

To define the operating rules, membership, authority, and responsibilities of the Information Security Committee.

2. Scope

This procedure applies to the Information Security Committee and all personnel involved in the governance of the Information Security Management System (ISMS).

3. Overview

This procedure outlines the process for scheduling and conducting Information Security Committee meetings, setting agendas, documenting minutes, and managing policy changes to ensure effective oversight of the company's security posture.

4. Procedure

Step	Who	What
1	Committee Chair	Schedules quarterly meetings and distributes the agenda to all committee members at least one week prior.
2	Committee Members	Attend scheduled meetings, participate in discussions, and vote on proposed policy changes.
3	Committee Secretary	Records detailed meeting minutes, including key decisions, action items, and voting results.
4	Committee Secretary	Distributes the signed and dated meeting minutes to all members within five business days of the meeting.
5	Policy/Procedure Owner	Submits proposed changes to policies or procedures to the Committee Chair for agenda inclusion.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2 Trust Services Criteria	CC2.1 - Communication Objectives

6. Artifact(s)

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

7. Definitions

ISMS: Information Security Management System.

8. Responsibilities

Role	Responsibility
Committee Chair	Presides over meetings, sets the agenda, and ensures procedures are followed.
Committee Members	Attend meetings, provide input, and vote on security-related matters.
Committee Secretary	Documents and distributes meeting minutes and maintains committee records.

Internal Audit Procedure (SEC-PROC-002)

1. Purpose

To outline the process for planning, conducting, and reporting on annual internal audits of the Information Security Management System (ISMS).

2. Scope

This procedure applies to all internal audits of the ISMS, including all systems, processes, and controls that fall under its scope.

3. Overview

This procedure details the end-to-end process for the annual internal audit of the ISMS. It covers the creation of an audit plan, the execution of audit fieldwork, the documentation of findings, the generation of a formal report, and the tracking of corrective actions through to resolution.

4. Procedure

Step	Who	What
1	Head of Internal Audit	Develops and documents an annual internal audit plan, including scope, objectives, and resources.
2	Internal Auditor(s)	Conducts audit fieldwork by gathering and analyzing evidence to assess control effectiveness.
3	Internal Auditor(s)	Documents all findings, including non-conformities, observations, and opportunities for improvement.
4	Head of Internal Audit	Creates and distributes a formal audit report detailing the scope, findings, and recommendations.
5	Management/Process Owners	Develops and implements corrective action plans for identified findings.
6	Head of Internal Audit	Tracks the status of all corrective actions to completion in a tracking log.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2 Trust Services Criteria	CC6.6 - System Monitoring

6. Artifact(s)

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

7. Definitions

ISMS: Information Security Management System.

8. Responsibilities

Role	Responsibility
Head of Internal Audit	Oversees the entire audit process, from planning to reporting and tracking.
Internal Auditor(s)	Executes the audit plan, documents findings, and assists in report creation.
Management/Process Owners	Responsible for implementing corrective actions to address audit findings.

Password Policy Exception Procedure (SEC-PROC-003)

1. Purpose

To provide a formal process for requesting, reviewing, and documenting exceptions to the Password Policy.

2. Scope

This procedure applies to all personnel and systems within the organization when a deviation from the established Password Policy is required.

3. Overview

This procedure outlines the steps for submitting, evaluating, and documenting requests for exceptions to the company's Password Policy. It ensures that any deviation is subject to a formal risk assessment and approval by the Security Officer, and that all approved exceptions are tracked.

4. Procedure

Step	Who	What
1	User or System Owner	Submits a formal Password Policy Exception Request form, including a detailed justification and any proposed compensating controls.
2	Security Officer	Conducts a risk assessment of the request to evaluate potential security impacts and formally approves or denies the request in writing.
3	Security Officer	Documents all approved exceptions, including the justification, risk assessment, and expiration date, in a central tracking log.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-3	SOC 2 Trust Services Criteria	CC6.8 - System Operations

6. Artifact(s)

A completed and approved Password Policy Exception Request form.

7. Definitions

N/A

8. Responsibilities

Role	Responsibility
User/System Owner	Initiates the exception request and provides all necessary information and justification.
Security Officer	Performs a risk assessment, makes the final decision on the exception request, and maintains all documentation.

Risk Assessment Procedure (SEC-PROC-004)

1. Purpose

To establish a systematic process for conducting annual and ad-hoc risk assessments to identify, analyze, and evaluate risks to the organization's information assets.

2. Scope

This procedure applies to all information assets and processes within the scope of the Information Security Management System (ISMS). Risk assessments are performed annually and on an ad-hoc basis when significant changes occur.

3. Overview

This procedure details the methodology for conducting risk assessments. It covers the identification of assets, threats, and vulnerabilities; the analysis of likelihood and impact; the calculation of risk levels; and the documentation of results in the risk register and a formal report.

4. Procedure

Step	Who	What
1	Risk Assessment Team	Identifies and documents critical information assets and their owners.
2	Risk Assessment Team	Identifies potential threats and vulnerabilities associated with each asset.
3	Risk Assessment Team	Analyzes the likelihood of a threat exploiting a vulnerability and the potential impact to the organization.
4	Risk Assessment Team	Calculates the overall risk level for each identified threat/vulnerability pair based on predefined risk criteria.

Step	Who	What
5	Risk Assessment Team	Documents the results of the assessment, including identified risks, risk levels, and recommended treatments, in the risk register.
6	Security Officer	Compiles a formal Risk Assessment Report summarizing the key findings and recommendations for management review.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2 Trust Services Criteria	CC3.2 - Risk Assessment

6. Artifact(s)

An updated Risk Register and a formal Risk Assessment Report.

7. Definitions

Risk Register: A log of identified risks, their characteristics, and their status.

8. Responsibilities

Role	Responsibility
Risk Assessment Team	Conducts the risk assessment activities as outlined in this procedure.
Security Officer	Oversees the risk assessment process and is responsible for the final report.
Asset Owners	Provide necessary information about their assets for the risk assessment.

Vendor Risk Assessment and Onboarding Procedure (SEC-PROC-005)

1. Purpose

To detail the process for assessing a new vendor's security posture before engagement to ensure they meet the company's security requirements.

2. Scope

This procedure applies to all new vendors that will handle, store, process, or transmit company data, or will be connected to the company's network or systems.

3. Overview

This procedure outlines the steps for conducting due diligence on prospective vendors. It includes initiating the request, classifying the vendor's risk level, performing a security assessment tailored to that risk level, and obtaining formal approval before a contract is signed.

4. Procedure

Step	Who	What
1	Business Owner	Initiates a new vendor request and provides details about the services and data involved.
2	Security Team	Classifies the vendor's inherent risk level (e.g., High, Medium, Low) based on the nature of the service and data access.
3	Security Team	Performs due diligence activities based on the risk level. This may include sending security questionnaires, reviewing SOC 2 reports, or conducting technical calls.
4	Security Team	Documents the findings in a Vendor Risk Assessment Report and provides a recommendation.
5	Business Owner/Manager	Reviews the assessment report and formally approves or denies the vendor engagement.
6	Legal/Procurement	Executes the contract only after receiving formal approval from the security review.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2 Trust Services Criteria	CC1.2 - Management Oversight

6. Artifact(s)

A completed Vendor Risk Assessment Report.

7. Definitions

SOC 2 Report: A report on controls at a service organization relevant to security, processing integrity, confidentiality, or privacy.

8. Responsibilities

Role	Responsibility
Business Owner	Initiates the vendor request and acts as the primary point of contact for the vendor relationship.
Security Team	Conducts the risk classification and due diligence assessment and produces the final report.
Management	Provides final approval for vendor engagement based on the risk assessment findings.

Facility Access Management Procedure (SEC-PROC-006)

1. Purpose

To describe the process for provisioning, reviewing, and revoking physical access to company facilities to ensure a secure physical environment.

2. Scope

This procedure applies to all employees, contractors, and visitors requiring access to company-controlled facilities.

3. Overview

This procedure outlines the standardized steps for managing physical access. It covers the issuance of access badges for new personnel, the process for registering and escorting visitors, and the requirement for regular reviews of access rights to ensure they remain appropriate.

4. Procedure

Step	Who	What
1	Hiring Manager/HR	Submits a facility access request form for a new employee or contractor.
2	Facilities/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 quarterly reviews of all physical access permissions to ensure they are still required and appropriate.
5	Manager/HR	Notifies the Facilities/Security Team immediately upon termination of an employee or contractor to revoke physical access.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2 Trust Services Criteria	CC6.4 - Physical Access

6. Artifact(s)

A completed access request form and an access review log.

7. Definitions

N/A

8. Responsibilities

Role	Responsibility
Hiring Manager/HR	Initiates and approves access requests for new personnel and reports terminations promptly.
Facilities/Security Team	Manages the physical access control system, issues badges, conducts access reviews, and manages visitor logs.
Employee/Host	Responsible for their assigned access badge and for escorting any visitors they host.

AI Tool Risk Assessment and Approval Procedure (SEC-PROC-007)

1. Purpose

To define the formal process for submitting a new AI tool for consideration and for the AI Governance Committee to perform a risk assessment to ensure its use aligns with company policies and risk appetite.

2. Scope

This procedure applies to all employees and contractors who wish to use a new Artificial Intelligence (AI) tool for business purposes, especially those that may process sensitive or confidential company or customer data.

3. Overview

This procedure outlines the workflow for the review and approval of new AI tools. It details the submission process for an employee, the required information for the request, and the steps the AI Governance Committee takes to conduct a thorough risk assessment before formally approving or denying its use.

4. Procedure

Step	Who	What
1	Employee/Req	Submits an “AI Tool Risk Assessment and Approval Form” to the AI Governance Committee.
2	Employee/Req	Provides all required information, including the tool’s purpose, data sensitivity, privacy impact, and vendor documentation.
3	AI Governance Committee	Reviews the submission and conducts a risk assessment, considering factors like data security, privacy, compliance, and operational impact.
4	AI Governance Committee	Formally approves or denies the request in writing, documenting the rationale for the decision and any conditions for use.

Step	Who	What
5	AI Governance Committee	Maintains a register of all approved and denied AI tools.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-5	SOC 2	CC2.1
1-5	NIST AI Risk Management Framework	Entire Framework

6. Artifact(s)

A completed AI Risk Assessment and Approval Form.

7. Definitions

AI: Artificial Intelligence.

8. Responsibilities

Role	Responsibility
Employee/Requester	Initiates the review process and provides complete and accurate information about the proposed AI tool.
AI Governance Committee	Conducts the risk assessment, makes the final approval decision, and maintains records of all assessments.

Vulnerability Management Procedure (SEC-PROC-008)

1. Purpose

To describe the workflow for identifying, prioritizing, remediating, and verifying vulnerabilities across the organization's systems and applications.

2. Scope

This procedure applies to all company-owned or managed systems, networks, and applications. It covers the entire lifecycle of a vulnerability from discovery to closure.

3. Overview

This procedure outlines the systematic process for managing vulnerabilities. It begins with the discovery of vulnerabilities through various means, followed by prioritization based on risk. It then details the assignment of remediation tasks to asset owners, the remediation process itself, and the final verification by the Security Team to confirm the fix.

4. Procedure

Step	Who	What
1	Security Team	Discovers vulnerabilities through automated scans, penetration tests, and other sources.
2	Security Team	Prioritizes identified vulnerabilities using CVSS scores and contextual business risk factors.
3	Security Team	Assigns prioritized findings to the appropriate asset owners for remediation, including defined Service Level Agreements (SLAs).
4	Asset Owner	Performs remediation actions to fix the vulnerability within the specified SLA.
5	Security Team	Performs verification scans or other tests to confirm that the vulnerability has been successfully remediated.
6	Security Team	Closes the finding in the vulnerability tracking system upon successful verification.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2 Trust Services Criteria	CC1.2 - Management Oversight

6. Artifact(s)

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

7. Definitions

CVSS: Common Vulnerability Scoring System. A standard for assessing the severity of computer system security vulnerabilities. **SLA:** Service Level Agreement. A commitment between a service provider and a client.

8. Responsibilities

Role	Responsibility
Security Team	Responsible for discovering, prioritizing, assigning, and verifying vulnerabilities.
Asset Owner	Responsible for remediating identified vulnerabilities on their assigned assets within the defined SLAs.

Vulnerability Management Exception Procedure (SEC-PROC-009)

1. Purpose

To outline the process for formally requesting, approving, and documenting an exception to a remediation Service Level Agreement (SLA) for an identified vulnerability.

2. Scope

This procedure applies when an asset owner cannot remediate a vulnerability within the timeframe defined in the Vulnerability Management Policy and requires a formal exception.

3. Overview

This procedure provides a structured pathway for managing situations where immediate vulnerability remediation is not feasible. It details the steps for an asset owner to request an exception, the multi-level approval workflow based on vulnerability severity, and the requirement to document approved exceptions in the risk register for regular review.

4. Procedure

Step	Who	What
1	Asset Owner	Submits a formal Exception Request Form, including a detailed justification, risk analysis, and any compensating controls in place.
2	Asset Owner's Manager	Reviews the request for business validity and approves or denies it.
3	Security Officer	Reviews the request for security implications and approves or denies it.
4	CTO	For Critical or High-risk vulnerabilities, provides the final layer of approval.
5	Security Team	Documents the approved exception, including its expiration date, in the risk register.
6	Security Team	Reviews all active exceptions on a quarterly basis to ensure they are still valid and necessary.

5. Standards Compliance

Procedure Step(s)	Standard/Framework	Control Reference
1-6	SOC 2 Trust Services Criteria	CC7.1 - Risk Mitigation

6. Artifact(s)

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

7. Definitions

SLA: Service Level Agreement. **CTO:** Chief Technology Officer.

8. Responsibilities

Role	Responsibility
Asset Owner	Initiates the exception request and provides all necessary justification and documentation.
Asset Owner's Manager	Provides the initial business approval for the exception request.
Security Officer	Provides security approval and ensures proper documentation in the risk register.
CTO	Provides final approval for exceptions related to high-impact vulnerabilities.