# Change Management Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives.*

### **S**ecurity boundary under scope

1. [List of applicable systems]

### References

1. ISO/IEC 27001:2022: 6.3, 8.1.c, A.5.3, A.5.7, A.7.8, A.7.13, A.8.19, A.8.29, A.8.32, A.8.33
2. NIST 800-53 rev. 5: AC-5, CA-9, CM-3, CM-3(2), CM-3(4), CM-4, CM-4(2), CM-5, CM-5(1), CM-5(5), CM-6, CM-8(1), MA-x, PE-16, SA-11, SA-11(2), SA-22, SI-1, SI-2, SI-2(2), SI-4(2), SI-5, SI-7, SI-7(1), SR-11(2)
3. CIS v8: 7.3, 7.4, 16.1, 16.12, 16.14
4. PCI DSS 4.0: 6.2.3, 6.3.3, 6.5.1, 6.5.2, 6.5.4, 9.5.1.3, 1.1.1
5. AICPA SOC 2 TSC: A1.2, CC3.4, CC5.1, CC5.2, CC6.3, CC7.1, CC8.1, PI1.1, PI1.3

## Document ownership

<(Choose from)>

* 1. Policy Owner:
     1. [Owner name] ([Owner email]), [Owner title]
  2. Information Security Officer:
     1. [Information officer name], ([Information officer email]), [Information officer title]
  3. System Owner(s):
     1. [System owner name], ([System owner email]), [System owner title]
  4. Process and Operational Owner(s)
     1. [process owner], ([process owner email]), [process owner title]
  5. System Administrator(s):
     1. [System admin name], ([System admin email]), [System admin title]
  6. Required Dissemination: <(Choose from)>
     1. IT Administrator
     2. Engineering
     3. Product Management
     4. Support
     5. Information Security Team
     6. [Organization name] Leadership Team
     7. Contractors
     8. Vendors
     9. Company Wide
     10. [Organization name] SIRT
  7. Optional Dissemination: <(Choose from)>
     1. IT Administrator
     2. Engineering
     3. Product Management
     4. Support
     5. Information Security Team
     6. [Organization name] Leadership Team
     7. Contractors
     8. Vendors
     9. Company Wide
     10. [Organization name] SIRT

## Purpose

The purpose of the Change Management Policy is to ensure that all changes to [Organization name]'s information systems, networks, applications, and related processes are managed in a controlled and systematic manner. This policy aims to minimize the risks associated with changes, including unintended service disruptions, security vulnerabilities, and compliance violations. By establishing a formal change management process, the organization seeks to maintain the integrity, availability, and security of its IT environment while enabling continuous improvement and adaptation to business needs.

## Scope

This policy applies to all personnel, including employees, contractors, vendors, and third-party service providers, involved in requesting, reviewing, approving, or implementing changes to [Organization Name]'s information systems and related infrastructure. The scope of this policy covers:

* Changes in development, staging, testing, and production environments.
* Modifications to networks, system components, processes, and system design.
* Code deployments and software updates.
* Threat modeling and risk analysis related to proposed changes.
* Installation and maintenance of system components.

All changes, regardless of size or complexity, must follow the procedures outlined in this policy to ensure consistency, accountability, and security across the organization’s IT landscape.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], **[owner title]** | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | **Executive Team** | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | **Executive Team** | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], **[Information officer title]** | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner],  **Operational owner title]** |  |
| Information Systems Administrators | **System Administrators** | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], **[HR title]** | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users | **End Users** | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | **[provider type]** | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
  2. Management has reviewed and approved this policy.
  3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
  4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
  2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. **Change Management**:
     1. The process of managing changes to systems, applications, or infrastructure in a structured and systematic manner to minimize the impact on services and ensure proper documentation and authorization.
  2. **Development Environment**:
     1. A computing environment used by developers to write and test code. This environment is typically isolated from staging and production environments.
  3. **Stage Environment**:
     1. An intermediate environment where applications or systems are tested before being deployed to production. This environment closely mimics the production environment to ensure accuracy in testing.
  4. **Test Environment**:
     1. A controlled environment where testing of applications, systems, or components is conducted. This environment is used to validate changes and ensure they meet requirements without affecting the production environment.
  5. **Production Environment**:
     1. The live environment where systems and applications are available for end users. Changes to this environment are carefully controlled and monitored to ensure stability and availability.
  6. **Version Control System (VCS)**:
     1. A tool that helps track changes to code or documents over time. It allows multiple developers to work on the same project concurrently while maintaining a history of changes.
  7. **Change Control Process**:
     1. A formal process that ensures changes are proposed, reviewed, approved, and implemented in a controlled manner. This process helps to manage risks and ensures proper documentation.
  8. **Segregation of Duties (SoD)**:
     1. A security principle that ensures no single individual has control over all aspects of any critical process. It reduces the risk of fraud and error by distributing tasks and associated privileges among multiple individuals.
  9. **Threat Modeling**:
     1. A structured approach to identifying and evaluating potential security threats to a system. It involves analyzing the system architecture, identifying potential threats, and implementing measures to mitigate those threats.
  10. **Impact Analysis**:
      1. The assessment of the potential consequences of a change on systems and operations. It helps in understanding the risks associated with the change and planning for mitigation strategies.
  11. **Rollback Plan**:
      1. A predefined strategy for reverting a system to its previous state in case a change leads to unintended consequences or system failure. It ensures business continuity and minimizes downtime.
  12. **Patch Management**:
      1. The process of identifying, acquiring, testing, and applying patches to software and systems. It is essential for maintaining security and functionality by addressing known vulnerabilities.
  13. **Maintenance Window**:
      1. A scheduled period during which routine maintenance activities are performed on systems or networks. It is planned to minimize impact on business operations and ensure that services remain available.
  14. **Automated Testing**:
      1. The use of software tools to execute tests on code or applications automatically. It helps in quickly identifying defects and verifying that changes meet the required standards and functionality.
  15. **Change Request**:
      1. A formal proposal for a change to a system, application, or process. It includes details about the proposed change, its justification, and potential impacts.
  16. **Deployment Pipeline**:
      1. A series of automated steps that code changes go through before being deployed to production. It includes stages such as building, testing, and deploying code to ensure quality and reliability.

## Policy

#### Change Management in Development, Stage, Test, and Production Environments

##### Development Environment:

* + - 1. Development teams shall use version control systems to manage code changes.
      2. All changes in the development environment shall be documented and tracked.
      3. Periodic reviews of the development environment are required to ensure compliance with security policies.

##### Stage Environment:

* + - 1. Changes shall be tested in the stage environment before moving to production.
      2. Access to the stage environment shall be restricted to authorized personnel only.

##### Test Environment:

* + - 1. All testing activities shall be performed in a controlled and isolated test environment.
      2. Test data shall be sanitized to prevent exposure to sensitive information.
      3. Detailed test plans and results shall be documented and reviewed.

##### Production Environment:

* + - 1. Changes to the production environment shall follow a strict change control process.
      2. Only approved changes shall be deployed to the production environment.
      3. Emergency changes shall be documented and reviewed post-implementation.

#### System Change Management

##### Networks:

* + - 1. Network changes, including configurations and hardware modifications, shall be reviewed and approved by the network security team.
      2. Network change requests shall include an impact analysis and a rollback plan.

##### System Components and Processes:

* + - 1. Changes to system components and processes shall undergo thorough testing and validation.
      2. All changes shall be documented, including the rationale and expected outcomes.

##### System Design:

* + - 1. Design changes shall be evaluated for security implications and compliance with architectural standards.
      2. A formal review process involving key stakeholders shall be conducted for all design changes.

##### Code Deployments:

* + - 1. Code deployments shall follow a structured deployment pipeline with automated testing and validation stages.
      2. Deployment logs shall be maintained and monitored for anomalies.

#### Segregation of Duties

* + 1. Requests for changes and the approval of those changes shall not be performed by the same individual.
    2. The change requestor shall document the change requirements and submit them for approval.
    3. An independent review and approval process shall be conducted by authorized personnel who are not involved in the request or implementation of the change.

#### Threat Modeling and Analysis

* + 1. Threat modeling and analysis shall be integrated into the change management process to identify potential security risks associated with proposed changes.
    2. All significant changes shall undergo a threat modeling exercise to evaluate and mitigate risks.
    3. The results of threat modeling activities shall be documented and reviewed by the security team.

#### Installation and Maintenance

##### Installation

* + - 1. All new system components shall be assessed for security impact prior to installation
      2. New components must be independently reviewed and approved by a separate, qualified approver prior to their deployment
      3. Installation of new system components shall only be completed by approved, competent personnel

##### Maintenance:

* + - 1. Maintenance activities shall be scheduled and documented.
      2. Maintenance windows shall be planned to minimize disruption to business operations.

##### System/Software Updates and Patches:

* + - 1. System and software updates and patches shall follow the established change management process.
      2. Updates shall be tested in non-production environments before deployment to production.
      3. Update logs and documentation shall be maintained for audit purposes.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
  2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
  3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
     1. Policies
     2. Procedures
     3. Standards
     4. Documentation
     5. Regulations
     6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
  2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
     1. The Information Security Officer
     2. Officer of the [Organization name] Leadership Team
  3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |