Change Management Policy

DOCUMENT CLASSIFICATION	Internal
VERISON	1.0
DATE	
DOCUMENT AUTHOR	Ayaz Sabir
DOCUMENT OWNER	

REVISION HISTORY

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES

DISTRIBUTION LIST

NAME	SUMMARY OF CHANGE

APPROVAL

NAME	POSITION	SIGN

Contents

1. Introduction

In today's dynamic technological and business environment, change is constant and inevitable. While change is essential for growth, innovation, and adaptation, poorly managed changes can introduce significant risks to an organization's information security, operational stability, and compliance posture. Unauthorized, untested, or inadequately documented changes can lead to system outages, data breaches, service disruptions, and non-compliance with regulatory requirements.

This Change Management Policy establishes a structured and controlled approach to managing all changes within the organization's information systems, services, and processes. It is designed to minimize the risks associated with changes, ensure the integrity and availability of information assets, and maintain the confidentiality of sensitive data. By implementing a robust change management framework, the organization aims to facilitate necessary changes efficiently while preserving the security and stability of its operations, aligning with the principles and controls set forth in ISO/IEC 27001:2022, particularly Annex A 8.32.

2. Purpose

The primary purpose of this Change Management Policy is to establish a systematic and controlled process for managing all changes to the organization's information systems, services, and processes. This policy aims to:

- **Minimize Risk:** Reduce the likelihood and impact of information security incidents, operational disruptions, and data integrity issues caused by uncontrolled or poorly managed changes.
- **Ensure Stability and Reliability:** Maintain the stability, reliability, and performance of information systems and services by ensuring that all changes are properly planned, tested, and implemented.

- **Protect Information Assets:** Safeguard confidentiality, integrity, and availability of information assets throughout the change lifecycle.
- **Ensure Compliance:** Facilitate compliance with relevant legal, regulatory, and contractual obligations, as well as internal organizational policies and standards, including ISO/IEC 27001:2022, specifically Annex A Control 8.32.
- **Improve Efficiency:** Streamline the change process, making it more efficient and effective while ensuring that security considerations are integrated at every stage.
- **Enhance Accountability:** Define clear roles and responsibilities for all personnel involved in the change management process, promoting accountability and transparency.
- **Facilitate Communication:** Ensure effective communication and coordination among all stakeholders affected by or involved in changes.
- **Support Business Objectives:** Enable the organization to adapt to new business requirements and technological advancements in a secure and controlled manner.

3. Scope

This Change Management Policy applies to all changes that could impact on the confidentiality, integrity, or availability of the organization's information and associated assets. This includes, but is not limited to, changes to:

- **Information Systems:** Hardware, software, operating systems, applications, databases, and network devices.
- **Services:** IT services, business services, and cloud services.
- **Processes:** Business processes, operational procedures, and information security processes.
- **Configurations:** System configurations, security settings, and network configurations.
- **Data Structures:** Database schemas, data models, and data storage

mechanisms.

- **Physical Environment:** Changes to physical security controls, data centers, and server rooms that could impact information security.
- **Organizational Structure:** Changes in roles, responsibilities, or reporting lines that affect information security management.

This policy applies to all personnel involved in initiating, planning, approving, implementing, testing, or reviewing changes, including:

- All Employees (full-time, part-time, temporary)
- Contractors and Consultants
- Third-Party Service Providers (where their changes impact the organization’s information assets)
- Management and Leadership

The policy covers all stages of the change lifecycle, from initiation and planning to implementation, review, and closure. It applies to both planned and emergency changes. While the policy provides a framework, specific detailed procedures for different types of changes will be documented separately and referenced herein.

4. Policy Statements

This section outlines the mandatory principles and practices for managing changes within the organization, aligning with ISO/IEC 27001:2022 requirements. These statements provide clear management direction and support for all activities related to secure change management.

4.1 General Principles for Change Management

All changes to the organization’s information systems, services, and processes must adhere to the following general principles. These principles ensure that changes are introduced in a controlled, secure, and systematic manner, minimizing risks and maintaining the integrity of information assets:

- **Minimizing Disruption:** Changes should be planned and implemented in a way that minimizes disruption to business operations and services. This includes scheduling changes during off-peak hours and having robust rollback plans.
- **Risk Assessment:** Every change must undergo a thorough risk assessment to identify potential impacts on information security (confidentiality, integrity, availability), operational stability, and compliance. Changes with higher risks require more rigorous review and approval processes.
- **Authorization:** All changes must be formally authorized before implementation. The level of authorization required will depend on the criticality and potential impact of the change.
- **Documentation:** All changes, including their justification, scope, risk assessment, implementation plan, testing results, and approval, must be thoroughly documented. This documentation is crucial for audit trails, troubleshooting, and future reference.
- **Testing:** Changes must be adequately tested in a non-production environment that closely mirrors the production environment before deployment. Testing should verify functionality, security, and compatibility.
- **Communication:** Effective communication is vital throughout the change lifecycle. All affected stakeholders must be informed about planned changes, potential impacts, and implementation schedules.
- **Back-out/Rollback Pan:** A clear and tested back-out or rollback plan must be in place for every change. This plan should enable the restoration of the system or service to its pre-change state in case of unforeseen issues or failures.
- **Segregation of Duties:** Where possible, segregation of duties should be maintained within the change management process to prevent a single individual from having control over all stages of a change.
- **Security by Design:** Security considerations must be integrated into the design and planning of all changes from the outset, rather than being an afterthought.
- **Continuous Improvement:** The change management process itself should be

regularly reviewed and improved based on lessons learned from change implementations, incidents, and audits.

4.2 Change Management Process (ISO 27001:2022 Annex A 8.32)

As per ISO 27001:2022 Annex A 8.32, changes to information and other associated assets shall be controlled. This section outlines the structured process for managing changes, ensuring that all modifications are systematically planned, assessed, approved, implemented, and reviewed to minimize risks and maintain information security.

4.2.1 Change Request and Initiation

All proposed changes, regardless of their size or complexity, must be formally initiated through a documented change request. This request should include:

- **Change Identifier:** A unique reference number for tracking.
- **Requester Information:** Name, department, and contact details of the person requesting the change.
- **Description of Change:** A clear and concise description of the proposed change.
- **Justification/Reason:** The business need or problem that the change aims to address.
- **Expected Outcome:** The desired results or benefits of the change.
- **Affected Assets:** Identification of all information systems, services, processes, or data that will be impacted by the change.
- **Urgency/Priority:** The criticality and timeline for the change.

4.2.2 Change Assessment and Planning

Once a change request is initiated, it must undergo a comprehensive assessment and detailed planning phase. This involves:

- **Impact Assessment:** Evaluating the potential impact of the change on confidentiality, integrity, and availability of information, operational stability, system performance, and compliance requirements. This includes identifying dependencies and potential conflicts with other systems or processes.
- **Risk Assessment:** Conducting a formal risk assessment to identify and evaluate potential threats and vulnerabilities associated with the change. This assessment should quantify the likelihood and impact of identified risks and propose mitigation strategies.
- **Technical Design:** Developing a detailed technical design for the change, including architecture diagrams, configuration changes, and code modifications.
- **Implementation Plan:** Creating a step-by-step plan for implementing the change, including timelines, resources required, and responsible personnel. This plan must include a clear communication strategy for all affected stakeholders.
- **Testing Plan:** Developing a comprehensive testing plan that outlines the types of tests to be performed (e.g., functional, security, performance, regression), test environments, test data, and expected results. Testing must verify that the change achieves its intended purpose without introducing new vulnerabilities or negatively impacting existing functionality.
- **Back-out Plan:** Defining a clear and tested back-out or rollback plan to restore the system or service to its pre-change state in case of failure or unforeseen issues during implementation or post-implementation.

4.2.3 Change Approval

All changes must be formally approved by authorized personnel before implementation. The approval process will be tiered based on the assessed risk and impact of the change:

- **Low-Risk Changes:** May be approved by the immediate manager or team leader.
- **Medium-Risk Changes:** Require approval from the Change Advisory Board (CAB) or a designated change manager.
- **High-Risk Changes:** Require approval from senior management or the Information Security Steering Committee, in addition to CAB approval.

Approval will be granted only after a thorough review of the change request, impact assessment, risk assessment, implementation plan, and testing plan. All approvals must be documented.

4.2.4 Change Implementation

Changes must be implemented according to the approved implementation plan. Key considerations during this phase include:

- **Scheduled Windows:** Changes should ideally be implemented during predefined maintenance windows to minimize disruption to business operations.
- **Trained Personnel:** Only authorized and adequately trained personnel should implement changes.
- **Monitoring:** Continuous monitoring of systems and services during and immediately after implementation to detect any anomalies or issues.
- **Documentation Updates:** All relevant documentation (e.g., system configurations, network diagrams, user manuals) must be updated to reflect the implemented change.

4.2.5 Change Review and Closure

After implementation, each change must undergo a post-implementation review to verify its success and effectiveness. This includes:

- **Verification:** Confirming that the change was implemented as planned and achieved its intended objectives.
- **Performance Monitoring:** Assessing the impact of the change on system performance and stability.
- **Security Review:** Verifying that the change did not introduce any new security vulnerabilities or compromise existing security controls.
- **Lessons Learned:** Documenting any lessons learned from the change process, including successes, challenges, and areas for improvement. These lessons will be used to refine the change management process.
- **Formal Closure:** Formally close the change request once all post-implementation reviews are complete and the change is deemed successful and

stable. This includes achieving all relevant documentation.

4.3 Emergency Changes

Emergency changes are those that must be implemented immediately to resolve a critical incident (e.g., security breach, system outage) or to address an urgent business requirement that cannot wait for the standard change management process. While speed is critical, emergency changes must still be managed with appropriate controls to minimize risks.

- **Definition:** An emergency change is an unplanned change that is required to restore a critical service, resolve a security vulnerability, or address a critical business need that, if not addressed immediately, would result in significant negative impact to the organization.

- **Authorization:** Emergency changes may bypass some steps of the standard change management process (e.g., pre-approval by CAB). However, they must be authorized by a designated authority (e.g., senior IT manager, Information Security Officer) before implementation. Post-implementation review and formal approval are mandatory.

- **Process for Emergency Changes:**
  - **Identification:** A critical incident or urgent business need is identified that necessitates an emergency change.
  - **Immediate Action:** Designated personnel take immediate action to implement the necessary change to mitigate the critical issue.
  - **Minimal Documentation:** Initial documentation may be minimal, focusing on the problem, the solution implemented, and the impact.
  - **Post-Implementation Review:** As soon as the emergency is resolved, a full post-implementation review must be conducted. This review will include a detailed risk assessment, impact analysis, and thorough documentation of the change, including justification for its emergency nature, implementation steps, and verification of effectiveness.
  - **Formal Approval:** The emergency change must be formally approved by the relevant authorities (e.g., CAB, senior management) retrospectively.

  - **Lessons Learned:** A lesson learned session must be conducted to identify the root cause of the emergency, evaluate the effectiveness of the emergency change process, and implement preventative measures to avoid similar emergencies in the future.

- **Risk Mitigation:** Even in emergency situations, efforts must be made to minimize risks. This includes:
  - Using pre-approved emergency procedures where available.
  - Implementing changes with the least possible impact.
  - Ensuring that only authorized and skilled personnel perform the changes.
  - Maintaining clear communication channels during the emergency.
  - Having a rollback plan in case the emergency change introduces new issues.

4.4 Roles and Responsibilities within Change Management

Clear definition of roles and responsibilities is crucial for the effective and secure operation of the change management process. Each role has specific duties to ensure that changes are managed in a controlled and secure manner.

Change Initiator:

- Identifies the need for a change and submits a formal change request.
- Provides a clear description and justification for the proposed change.
- Collaborates with relevant teams during the assessment and planning phases.

Change Manager:

- Oversee the entire change management process.
- Ensures adherence to this policy and associated procedures.
- Facilitates change meetings (e.g., CAB meetings).
- Monitors the progress of changes and ensures timely completion.
- Maintains the change management of documentation and records.

Change Advisory Board (CAB):

- Composed of representatives from IT, information security, business units, and other relevant stakeholders.
- Reviews and assesses proposed changes, particularly medium and high-risk changes.
- Provides recommendations for approval or rejection based on impact, risk, and resource availability.
- Ensure that changes align with business objectives and security requirements.

Information Security Officer (ISO) / CISO:

- Reviews of all changes for potential information security risks and impacts.
- Ensure that security controls are integrated into change designs and implementations.
- Provides guidance on security best practices throughout the change lifecycle.
- Approves changes with significant security implications.

System Owners / Business Process Owners:

- Responsible for the information systems or business processes affected by the change.

- Participate in the impact assessment and risk assessment of changes related to their assets.
- Provide input on business requirements and operational impacts.
- Approve changes that affect their systems or processes.

Implementation Teams / Technical Teams:

- Develop and execute the technical implementation plans for approved changes.
- Conduct thorough testing of changes in non-production environments.
- Ensure that changes are implemented according to documented procedures and within scheduled windows.
- Provide support during and after the change implementation.

Testing Teams / Quality Assurance (QA):

- Develop and execute test plans to verify the functionality, performance, and security of changes.
- Report any defects or issues identified during testing.
- Ensure that changes meet the defined quality standards before deployment to production.

All Personnel:

- Adhere to the change management policy and procedures.
- Report any unauthorized changes or deviations from approved changes.
- Participate in training and awareness programs related to change management.

5. Roles and Responsibilities

Effective change management relies on clearly defined roles and responsibilities to ensure accountability and efficient execution throughout the change lifecycle. All individuals involved in the change process, from initiation to closure, must understand their specific duties and how they contribute to maintaining the security and stability of the organization's information assets. Detailed responsibilities for key roles within the change management process are outlined in Section 4.4 of this policy. This section provides a high-level overview of the collective responsibility for changing management.

- **Senior Management:** Responsible for providing strategic direction, approving the Change Management Policy, allocating necessary resources, and ensuring that change management is integrated into the organization's overall information security and operational frameworks.

- **Information Security Officer (ISO) / CISO:** Accountable for overseeing the security aspects of change management, ensuring that security risks are adequately assessed and mitigated, and that changes comply with information security policies and standards.

- **Change Manager:** Responsible for the day-to-day operation and coordination of the change management process, ensuring adherence to the policy, facilitating communication, and maintaining accurate change records.

- **Change Advisory Board (CAB):** Responsible for reviewing, assessing, and approving significant changes, providing expert advice, and ensuring that changes are aligned with business objectives and risk appetite.

- **System and Business Process Owners:** Responsible for understanding the impact of changes on their respective systems and processes, participating in risk assessments, and providing necessary approvals.

- **All Personnel:** Every individual within the organization who initiates, implements, or is affected by a change has a responsibility to understand and adhere to this policy. This includes the following established procedures, reporting issues, and participating in training and awareness programs.

6. Compliance and Enforcement

Adherence to this Change Management Policy is mandatory for all individuals and entities within its scope. Compliance will be regularly monitored, and any non- compliance will be addressed through appropriate enforcement mechanisms. The following outlines our approach to ensuring compliance:

- **Monitoring and Auditing:** Regular monitoring and auditing activities will be conducted to assess adherence to this policy and the effectiveness of the change management process. This includes:
    - **Review of Change Records:** Periodic review of change requests, approvals, implementation plans, test results, and post-implementation reviews to ensure completeness and adherence to procedures.
    - **Internal Audits:** Scheduled internal audits to verify compliance with policy requirements and identify areas for improvement in the change management process.
    - **Security Reviews:** Specific security reviews of changes to ensure that security controls are not compromised and new vulnerabilities are not introduced.
- **Reporting and Investigation:**
    - All identified or suspected deviations from this policy, or any unauthorized changes, must be reported immediately to the Change Manager or Information Security Officer.
    - All reports will be investigated promptly and thoroughly to determine the root cause of non-compliance and implement corrective actions.
- **Training and Awareness:** Mandatory training will be provided for all personnel involved in the change management process, covering the principles, procedures, and their specific roles and responsibilities outlined in this policy. Awareness campaigns will reinforce the importance of controlled change management for information security.
- **Non-Compliance:**

  - Any instances of non-compliance with this policy will be investigated and addressed in accordance with the organization’s disciplinary procedures.
  - Depending on the severity and frequency of non-compliance, disciplinary actions may range from mandatory re-training and formal warnings to suspension or termination of employment, in accordance with the organization’s human resources policies and applicable labor laws.
  - Violations that result in legal penalties, regulatory fines, or significant financial or reputational damages to the organization may also lead to legal action.

- **Continuous Improvement:** The effectiveness of this policy and the overall change management process will be continuously evaluated. Feedback from monitoring activities, incident investigations, and audits will be used to refine and improve the policy, associated procedures, and training programs. This commitment to continuous improvement ensures that our changing management practices remain robust and adaptable to evolving threats and organizational needs.

7. Policy Review

This Change Management Policy will be reviewed at least annually, or more frequently if significant changes occur in the organization’s information systems, business processes, technological landscape, legal or regulatory requirements, or in response to major security incidents. The review process will involve:

- **Assessment of Effectiveness:** Evaluating the policy’s effectiveness in managing changes securely and achieving its stated objectives.
- **Feedback Integration:** Incorporating feedback from all relevant stakeholders, including employees, management, IT, and information security personnel.
- **Alignment with Standards:** Ensuring continued alignment with ISO/IEC 27001:2022 (specifically Annex A Control 8.32) and other relevant security standards and best practices.

- **Updates and Revisions:** Making necessary updates and revisions to the policy document to reflect changes in change management practices, emerging threats, organizational structure, and operational processes. All revisions will be formally approved and communicated to all relevant personnel.
- **Lessons Learned:** Integrating lessons learned from actual incidents, near misses, and audits to continuously improve the policy and associated guidelines.

8. Definitions

- **Change:** Any modification, addition, or removal of an item that could influence information security, operational stability, or compliance. This includes changes to hardware, software, networks, processes, and documentation.
- **Change Management:** The process of controlling changes to an information system or service, including the identification, documentation, assessment, approval, implementation, and review of changes.
- **Change Request (CR):** A formal document or record used to initiate a proposed change.
- **Change Advisory Board (CAB):** A group of individuals responsible for reviewing, assessing, and approving changes, particularly those with significant impact or risk.
- **Emergency Change:** An unplanned change that must be implemented immediately to resolve a critical incident or address an urgent business requirement.
- **Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity:** The property of safeguarding the accuracy and completeness of assets.
- **Availability:** The property of being accessible and usable upon demand by an authorized entity.

9. References

- **ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements**
- **ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security control**