**Change Management Policy for Workflow and IT Software Changes**

**I. Purpose**

The purpose of this policy is to provide a structured approach for managing changes to workflows and IT software systems within the organization. It ensures that all changes are effectively planned, tested, approved, communicated, and implemented with minimal disruption to business operations. This policy aims to mitigate risks, maintain service continuity, and ensure compliance with regulatory and organizational standards.

**II. Scope**

This policy applies to all workflow and IT software changes within the organization, including:

* Modifications to business processes or workflows.
* Updates, patches, or upgrades to IT software.
* Implementation of new software systems or tools.
* Changes to system configurations or infrastructure.
* Decommissioning of legacy systems or workflows.

It applies to all employees, contractors, and third-party vendors involved in initiating, approving, or executing changes.

**III. Key Definitions**

* **Change Request (CR)**: A formal proposal for a modification to a workflow or IT software.
* **Change Advisory Board (CAB)**: A group of stakeholders responsible for reviewing and approving significant change requests.
* **Change Owner**: The person responsible for planning, coordinating, and executing a change.
* **Emergency Change**: A change that must be implemented immediately due to an urgent issue (e.g., security vulnerability, critical system failure).

**IV. Change Categories**

1. **Standard Changes**:
   * Pre-approved, low-risk changes that follow a repeatable process.
   * Do not require CAB approval but must be logged and documented.
2. **Normal Changes**:
   * Non-urgent changes that may impact systems, workflows, or business operations.
   * Require formal assessment, testing, and CAB approval before implementation.
3. **Emergency Changes**:
   * Changes that must be implemented urgently to address critical incidents, security risks, or system failures.
   * Can bypass the normal approval process but must be reviewed retrospectively by the CAB.

**V. Roles and Responsibilities**

1. **Change Initiator**:
   * Submits a formal Change Request (CR) with a detailed description of the proposed change.
   * Provides justification, risk assessment, and potential impact analysis.
2. **Change Owner**:
   * Assigned by management to oversee the planning, testing, and execution of the change.
   * Coordinates with relevant stakeholders, ensures testing is completed, and oversees the implementation.
3. **Change Advisory Board (CAB)**:
   * Reviews and approves Normal and Emergency Change Requests.
   * Evaluates the potential risks, benefits, and impacts of each change.
   * Consists of representatives from key departments such as IT, Operations, Security, Compliance, and Business Units.
4. **IT Operations/Support Team**:
   * Assists in the technical implementation of IT software changes.
   * Ensures that systems are properly backed up before changes and that contingency plans are in place.
5. **End Users**:
   * Affected by changes to workflows or software systems.
   * Should be notified of upcoming changes and provided with appropriate training or support materials, if necessary.

**VI. Change Request Process**

1. **Submission of Change Request**:
   * The Change Initiator submits a CR via the organization’s Change Management System (CMS).
   * The CR must include a clear description, rationale, risk assessment, impact analysis, and a rollback plan.
2. **Initial Review**:
   * The Change Owner conducts an initial review of the CR to determine its feasibility and categorize the change (Standard, Normal, Emergency).
   * The Change Owner may consult subject matter experts for technical feasibility and risk assessments.
3. **Approval Process**:
   * **For Standard Changes**: Changes proceed without CAB approval but must follow pre-approved procedures.
   * **For Normal Changes**: The CAB reviews the CR, assesses risks, and either approves, rejects, or requests modifications.
   * **For Emergency Changes**: Immediate implementation is authorized by the Change Owner, with retrospective CAB review.
4. **Testing and Validation**:
   * All Normal and Emergency Changes must be tested in a non-production environment where possible.
   * Affected teams (IT, operations, end users) must validate the change to ensure it works as intended and does not disrupt other systems.
5. **Implementation**:
   * Changes are scheduled for implementation at a time that minimizes business disruption (e.g., off-peak hours).
   * The Change Owner coordinates with all stakeholders to execute the change.
   * A rollback plan must be ready in case the change causes unintended issues.
6. **Post-Implementation Review**:
   * After the change is implemented, a review is conducted to assess its success.
   * Issues or deviations from the plan are documented, and corrective actions are taken if necessary.
   * The CR is formally closed once the change is verified to be successful.

**VII. Communication**

1. **Pre-Change Communication**:
   * Stakeholders, including end users, must be notified of planned changes in advance.
   * Relevant training, documentation, or FAQs must be provided to assist with any new workflows or software features.
2. **Post-Change Communication**:
   * After successful implementation, all stakeholders are informed that the change is complete.
   * Any known issues, updates, or additional steps for end users should be communicated clearly.

**VIII. Risk and Impact Assessment**

All change requests must include a thorough risk and impact assessment. This assessment should cover:

* **Business Impact**: How the change will affect operations, workflows, or revenue.
* **Technical Impact**: Potential effects on systems, integrations, and performance.
* **User Impact**: How the change will affect end users, including training and support needs.
* **Security Impact**: Any implications for data security, privacy, or regulatory compliance.
* **Rollback Plan**: A documented process for reverting to the previous state if the change fails.

**IX. Emergency Change Procedures**

In the event of a critical issue requiring an Emergency Change:

1. The Change Owner must document the reason for the emergency and submit the CR post-implementation.
2. The Emergency Change must be reviewed by the CAB within 24 hours of implementation for approval and documentation.

**X. Monitoring and Compliance**

1. **Audit and Monitoring**:
   * All changes will be tracked and logged in the Change Management System.
   * Regular audits will be conducted to ensure compliance with the policy.
2. **Non-Compliance**:
   * Any unauthorized changes or deviations from the process must be reported to management.
   * Non-compliance will be addressed through corrective actions, which may include disciplinary measures.

**XI. Review and Amendment**

This policy will be reviewed annually to ensure its effectiveness and alignment with organizational and regulatory requirements. Changes to the policy must be approved by senior management and communicated to all employees.

This Change Management Policy provides a clear framework for managing workflow and IT software changes, minimizing risks, and ensuring smooth transitions.

4o