Change Management Process (Updated)

1. Purpose

The Change Management Process (CMP) ensures that changes to FinalForms' systems, services, and infrastructure are managed efficiently with minimal disruption to clients, users, and business operations. This process applies to all standard and emergency changes, ensuring consistency, accountability, and communication throughout the lifecycle of each change.

2. Scope

This CMP applies to:

- **Software updates and enhancements**
- **Infrastructure changes** (including network, server, or database changes)
- **Security updates** (related to risk management and cybersecurity)
- **Operational changes** (related to internal workflows and processes)
- **Policy changes** (affecting service-level agreements or client-facing policies)

3. Roles and Responsibilities

- **Change Requestor**: The individual or team proposing a change.
- **Change Manager**: Responsible for overseeing the entire change process, ensuring compliance with procedures.
- **Change Review Board (CRB)**: A group of designated stakeholders, including representatives from IT, Operations, Security, and Executive Management, who review, approve, or reject changes.
- **Technical Teams (Development, Engineers, etc.)**: Execute changes and report on progress.
- **Business Continuity Team**: Handles emergency changes and ensures that services are restored quickly if a critical failure occurs.

4. Change Categories

1. **Standard Changes**:
    - Planned, low-risk changes that follow an established process and do not require immediate action.
    - Examples: routine software patches, minor feature enhancements, UI/UX improvements.
2. **Emergency Changes**:
    - Unplanned, high-priority changes that must be implemented immediately to resolve an outage, security breach, or critical issue.
    - Examples: security vulnerability fixes, critical bug patches, restoring access to critical data.

5. Change Process Flow

5.1 Standard Change Process

1. **Initiation**:

    - The Change Requestor submits a formal Change Request (CR), providing details such as purpose, scope, potential impact, timeline, and risk assessment.
2. **Risk and Impact Assessment**:
    - The Change Manager, with input from technical teams, assesses the potential risks and impacts, categorizing the change as low, medium, or high risk.
3. **Approval by CRB**:
    - The CRB reviews the CR, considering the assessment. High-risk changes may require more detailed discussions or revisions.
4. **Scheduling**:
    - Once approved, the change is scheduled for implementation. The timing must align with internal or client needs and minimize disruption.
5. **Testing**:
    - Changes undergo testing in a staging or development environment to ensure functionality without disrupting live operations.
6. **Implementation**:
    - The change is deployed according to the approved schedule. The technical team executes the change, following predefined steps.
7. **Validation**:
    - Post-change validation ensures that the change was successful and did not negatively impact other systems or services.
8. **Documentation**:
    - All details of the change (including the outcomes) are documented for audit and future reference.
9. **Communication**:
    - Internal teams and external stakeholders are notified of the change and any relevant information (e.g., updates or new features).

5.2 Emergency Change Process

1. **Identification**:
    - Emergency changes are triggered by urgent situations such as service outages, security incidents, or critical failures that impact users or business continuity.
2. **Immediate Escalation**:
    - The Change Manager or designated member of the Business Continuity Team is immediately notified and begins the emergency change process.
3. **Approval**:
    - Given the urgency, emergency changes bypass the standard CRB process. Instead, approval is provided by a designated executive or senior leader (e.g., CTO or CSO).
4. **Rapid Implementation**:
    - The technical team implements the change immediately. Testing may be limited depending on the nature of the emergency, with the focus on resolving the issue as quickly as possible.
5. **Post-Implementation Review (PIR)**:
    - After resolution, a formal review is conducted to assess the effectiveness of the emergency change and identify areas for improvement. Documentation is completed after the change.
6. **Rollback/Mitigation**:
    - Emergency changes must have a rollback or mitigation plan in case the change fails or introduces new issues.

6. Risk and Impact Assessment

- **Low Risk**: Minimal potential for system or operational disruption, no direct impact on clients or users.
- **Medium Risk**: Potential for moderate disruption, affecting non-critical systems or functions.
- **High Risk**: Significant potential for service interruption or data loss, with direct impacts on clients or users. High-risk changes undergo thorough testing and review before implementation.

7. Communication Plan

- **Internal Communication**:
    - For all changes, internal teams are informed in advance through email notifications, including details on timing, impact, and necessary steps.
- **Client/External Communication**:
    - For changes impacting clients, notifications are sent via email or the support portal, including information on expected downtime (if any) and key updates. Emergency changes are communicated immediately after resolution.

8. Documentation and Auditing

All changes, including emergency changes, must be documented. This documentation includes:

- Change Request forms (for standard changes)
- Risk assessments and approvals
- Test results (if applicable)
- Post-Implementation Review (PIR) reports
- Rollback plans (if applicable)

Audits are conducted periodically to ensure that changes were implemented as approved and that appropriate procedures were followed.

9. Rollback and Recovery

- **Standard Changes**: Each change must include a rollback plan, allowing systems to revert to the previous state if the change fails or causes issues.
- **Emergency Changes**: A rollback or mitigation strategy is required to restore critical services if the emergency change is unsuccessful.

10. Training and User Awareness

For changes that impact users, training materials or guides are prepared and distributed prior to the change. If the change is complex or highly impactful, live training or walkthroughs may be conducted.

11. Continuous Improvement

The CMP is reviewed annually to ensure its effectiveness. Feedback from the Post-Implementation Review (PIR) of both standard and emergency changes is used to refine and improve the process.

FINALFORMS

This CMP outlines a structured, transparent approach to managing changes within FinalForms, ensuring that all updates, from minor fixes to emergency patches, are implemented with minimal disruption to clients and internal operations.