canvas
share in graphic detail

Change Management

Canvas GFX Inc.

April 12, 2024

Table of Contents

Change Management

A formal change management policy governs changes to the applications and supporting infrastructure and aid in minimizing the impact that changes have on organization processes and systems.

Canvas GFX Inc. Change Management Policy

1.0 Purpose

This policy aims to establish management direction and high-level objectives for the change management process. In addition, this policy guides the implementation of changes to reduce the impact on other tasks/projects as well as to mitigate associated risks such as:

- Information being corrupted and/or destroyed
- Adverse impact on other organizational processes
- Computer performance being disrupted and/or degraded
- Productivity losses being incurred

2.0 Scope

This policy applies to all IT systems and applications managed by Canvas GFX Inc. that store, process or transmit information, including network and computer hardware, software and applications, mobile devices and telecommunication systems. In addition, it applies to all business units that operate within Canvas GFX Inc.’s network environment or utilizes its information resources.

3.0 Policy

Changes to information resources shall be managed and executed according to a formal change control process. The change control process will ensure that the proposed changes are reviewed, authorized, tested, implemented and released in a controlled manner, and the status of each proposed change is monitored. To fulfill this policy, the following statements shall be adhered to:

- Canvas GFX Inc. shall consider developing, documenting and maintaining a current baseline configuration standard of the information systems and their components.
- The baseline configuration of the information systems shall be updated:
  - As an integral part of the information system component installation or updates.
  - As a result of defined circumstances.
- All change requests must be entered into the ticketing system, and all approvals, scheduling, comments and implementation details will be recorded as part of the ticket.
- Changes to the information system shall be authorized, documented and controlled using a formal change control procedure.
- Changes in the configuration of the information systems shall be monitored.
- Test, validate and document changes to the information system prior to implementing the proposed changes.
- Automatic tools shall be employed (wherever possible) to initiate changes/change requests, notify the appropriate approval authority and record the approval and implementation details.
- Changes that can not follow the regular process because of their urgency (such as service outages) shall be considered emergency changes and require immediate priority.
- Changes that are normal administrative functions or processes within a system can be classified as standard changes.
- Changes affecting customers shall be formally communicated to them before the change implementation.
- Development/test environments are separate from production environments, with access control in place to enforce separation.
- Duties shall be separated between personnel assigned to the development/test environments and those assigned to the production environment.
- Production data shall not be used for testing or development.
- A risk assessment should be undertaken where personal information is necessary to be used for testing purposes. Appropriate technical and organizational measures shall be implemented to minimize the

identified risks.
- Test data and accounts are removed before a production system becomes active.
- Change control procedures related to implementing security patches and software modifications are documented.

3.1 Change Initiation and Impact Analysis

All changes, both scheduled and unscheduled, shall be documented, classified into and tracked:

- Low impact: affects < 1% of individuals
- Medium impact: affects between 1% and 5% of individuals
- High impact: affects > 5% individuals

The documentation must identify the scope of the change, areas affected, back-out process, test plan, communication plan and the planned deployment date.

Business and technical risks (including the potential impact on performance and security) and costs must be formally considered part of the impact assessment and documented in the change record before submitting for approval. In addition, an implementation plan detailing all the stages required to successfully manage the change (including a test plan and roll-back strategy) shall be developed as part of this phase.

3.2 Change Approval and Implementation

Changes shall be approved formally prior to commencing the change or development and prior to implementing the fully-tested change into the live environment.

Impact across the organization and involvement of representatives from other business units will be considered depending on the impact on other business services.

3.3 Post-Implementation Review

A post-implementation review shall be performed to evaluate whether the desired result has been achieved. In the event that a change does not perform as expected or causes issues to one or more areas of the production environment, the attendees of the change meeting will determine if the change should be removed and the production environment returned to its prior stable state.

3.4 Denials

The Business Owner or Change Advisory Board (CAB) or their designee may deny a scheduled or unscheduled change for reasons including, but not limited to:

- Inadequate change planning or unit testing
- Lack of stakeholder acceptance (where applicable)
- System integration or interoperability concerns
- Missing or deficient roll-back plans
- Security implications and risks
- Timing of the change negatively impacts key business processes
- Timeframes do not align with resource scheduling (e.g., late-night, weekends, holidays or special events)

3.5 Emergency Changes

Changes that can not follow the normal process because of their urgency (such as service outages) shall be considered emergency changes because they require immediate attention and must be implemented quickly to avoid disruption.

Approvals shall be obtained for such changes in the form of a discussion with a relevant service manager. Such changes shall be assessed and formally approved retrospectively. In addition, such changes shall be discussed during the periodic Business Owner or CAB meetings for analysis of lessons learned, root cause, impact and status.

3.6 Standard Changes and Patching

Standard changes (also called “routine changes”) tend to be pre-authorized changes that are considered to have little to no risk associated with them. These changes (for example, applying security patches) are already pre-approved by IT Management, so they can be executed by creating a ticket without following the change management approval workflow.

All systems shall be patched and updated on a documented, regular and timely schedule. Common Vulnerability Scoring System (CVSS) is recommended to be used to aid in setting patching guidelines.

The organization must identify systems affected by announced software or firmware flaws, including potential vulnerabilities resulting from these flaws. Security-relevant patches, service packs, hotfixes and anti-virus signatures should be reported to designated personnel.

During security assessments, continuous monitoring, incident response activities, and system error handling, flaws discovered should be addressed.

Policy Version History

Version	Status	Summary of Changes	Last Updated On	Approved By	Published By
1	Published	removed PCI section	2024-04-12 8:28:08AM		John Yee