

IT122 - Change Management Policy

|  |  |
| --- | --- |
| Status | Final |
| Version | 1.03 |
| Classification | Confidential |
| Owner | Razvan Anghelidi, Directory of IT |
| Address | 1705 Tech Avenue, Unit 3, Mississauga, ON, L4W 0A2, Canada |

*Statement of Confidentiality: This document and supporting materials contain confidential and proprietary business information of Signifi Solutions Inc. These materials may be printed or photocopied for use internally and must not be shared with other parties.*

[Document Control iii](#_Toc38473295)

[Purpose 4](#_Toc38473296)

[Scope 5](#_Toc38473297)

[Policy Statement 5](#_Toc38473298)

[Enforcement 5](#_Toc38473299)

[Revision History 9](#_Toc38473300)

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Signifi Solutions Inc (from now on, Signifi). The information contained in this document is proprietary to Signifi and may not be used or disclosed except as expressly authorized in writing by Signifi.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

|  |  |  |
| --- | --- | --- |
| APPROVER(S) | TITLE/DEPARTMENT | APPROVED DATE |
| Shamira Jaffer | CEO | December 23rd, 2021 |
| Shamira Jaffer | CEO | December 7th, 2020 |
| Shamira Jaffer | CEO | June 1st, 2020 |
|  |  |  |
|  |  |  |

## Document Sensitivity Level

Confidential

Introduction

**Overview**

Change management is the process of controlling the creation and introduction of changes into the IT environment to minimize service disruptions. Change management is responsible for:  
• Logging changes;  
• Assessing the impact, cost, benefits, and risk of requested changes;  
• Providing approval or rejection;  
• Overseeing the change implementation;  
• Monitoring and reporting the status of change; and   
• Closing change requests and conducting post-implementation reviews.

Signifi can realize the following benefits:  
• More efficient use of IT resources and better alignment with organizational priorities;  
• Reduction of operational risks and increases in business productivity as a result of fewer business disruptions and improvements in change implementation turnaround;  
• Better alignment and communication between IT and the business units, and also between internal IT groups;  
• Reductions in the number of changes that have to be backed out, and a better ability to back out changes when required;  
• Provides an audit trail for all changes;  
• Helps to initiate the communication with the user community;

Overall improvements in the quality of IT services, ultimately leading to increases in user satisfaction and an enhanced business perception and image of the IT department.

Purpose

The Change Management Policy is in place to ensure that all changes to Signifi’s Business Applications and IT Infrastructure are managed carefully and in a consistent manner by all teams. This policy will help the IT associates manage change effectively to achieve the desired results. Please note that this policy is intended to make sure that changes have their intended impact while avoiding unintended consequences.

Scope

This policy applies to all users which include but not limited to employees, associates, contractors, part-time and temporary workers, trainees, service providers, and those employed by others to perform work at hosted or outsourced sites, or who have been granted access to Signifi information or systems. This policy applies to all Signifi resources owned, leased, or supported by Signifi, or any outside entity that has signed a Vendor Access Agreement with Signifi.

Policy Statement

Change Management Governance

IT Change Management Committee

The IT Change Management Committee’s (CMC) role is to facilitate the adoption of new or improved processes and/or procedures across the Information Technology Department. The Committee will oversee the development and deployment of change management methodologies and procedures to guide the adoption process.

Information Technology Change Management Committee shall meet at least once a year to review the policy and procedures ensuring they address the needs of the IT Department. The Change Management committee is made up of IT Management and includes the Chief Information Officer, Vice-President, Information Technology or other IT representatives when needed. The Chief Information Officer is the owner of the Change Management Policy and is responsible for approving all updates and changes to the policy.

IT Change Review Committee

The role of the IT Change Review Committee (CRC) is to review and approve all IT production environment changes. The CRC will review scheduled and implemented changes on a weekly basis providing final IT approval and feedback if necessary. The CRC will help enforce the Change Management policy and procedures and make recommendations for updating the policy or procedures.

The CRC is made up of IT Management representatives from teams that are potentially involved in, or will be impacted by, a production environment change.

If there is an urgent need to implement a change ahead of a regularly scheduled CRC meeting, an IT manager may approve the change on behalf of the CRC as long as additional requirements are met. The approval should be communicated to the rest of the committee and the change reviewed at the next CRC meeting. Urgent changes require approval from a Business VP or delegate as well as an IT Director. In addition, the ticket should indicate the business impact to revenue or cost (in dollars), member satisfaction, brand image or government/regulatory compliance if the implementation is delayed.

|  |  |
| --- | --- |
| Change Management | The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation. |
| Change | * Any implementation of new functionality * Any interruption of service * Any repair of existing functionality * Any removal of existing functionality * Execution of any process or tool deemed to introduce material risk to the production environment |
| Standard Change | A scheduled change where formal notification is received, reviewed, and approved by the review process in advance of the change being made. |
| Emergency Change | An immediate, unscheduled change that is performed when responding to an imminent or sudden critical system failure. These changes are documented and reviewed after the emergency is over. |
| Routine Change | A low risk, pre-approved change that is regularly performed and has been implemented as a Standard Change at least once. |
| Urgent Change | A scheduled change that urgently needs to be implemented prior to the next CRC meeting. |

Each IT Team must follow the Change Management (CM) policy and process that will meet all of the following requirements:

* All changes to the IT production environment, including changes to operating systems, hardware, firmware, networks, and business applications are subject to the CM Policy and must follow the CM Procedures.
* All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) are subject to Change Management Policy and must follow the CM procedures.
* All CM requests must be submitted in accordance with CM procedures. CM request tickets must be submitted at least two business days prior to the CRC meeting in order to give the approving IT manager and the CRC enough time to review the request, identify risks, and make a decision to allow or delay the request.
* Appropriate notification must be sent out to impacted users, groups and/or stakeholders for each scheduled change or unscheduled, emergency change.
* The individual assigned to a CM ticket is responsible for tracking the status and work progress of the change, updating the CM ticket appropriately.
* Changes must be tested in all cases before implementing in production. If testing cannot be conducted due to a technical constraint, sufficient justification must be provided with the CM request.
* Applicable test plans and results require sign-off from the appropriate stakeholders.
* CM requests must have appropriate level of approval prior to implementation. IT approval must come from the IT Manager responsible for supporting the impacted environment. Business approval for Standard changes must come from a supervisor or manager responsible for the area impacted.
* All planned changes must be scheduled for implementation to avoid conflicts with business process and resources.
* Changes must have a fallback (roll-back) plan. If such measures cannot be taken due to technical constraints, sufficient justification must be provided with the CM request.
* All changes will be maintained in the IT Management module of QuickBase. The changes are recorded in the Change Requests table and must contain at least the following fields:

1. Date of submission and date of change
2. Owner and custodian contact information
3. Description of the change
4. Level of risk/impact to the production environment
5. Reason for the change
6. Length of downtime required
7. Who has tested the change?
8. Who will be implementing the change?
9. Indication of success or failure

* Any supporting documentation such as detailed implementation and rollback plans and approvals should be either directly attached to the CM ticket or the ticket should reference the specific document location. An applicable Test Evidence Template must be directly attached to the ticket.
* If a change approved by the CRC is canceled, rescheduled, has to be rolled back or otherwise does not go as planned, all appropriate stakeholders need to be notified including the CRC. A review of the associated CM request is to take place at the next CRC meeting where it can be decided if any additional follow up actions are necessary.

This Change Management policy is part of the Information Security policy, and as such, any deliberate violation is subject to the enforcement clause indicated below.

Enforcement

All instances of non-compliance will be reviewed by the department director. The department director, with the assistance of the Human Resources department has the authority to impose disciplinary actions, up to and including termination of employment or contractual agreement.

Update

This policy and all supporting documentation will be reviewed and updated annually or upon material changes to Signifi business rules, technology processes, organizational goals, or information security objectives to ensure its continuing suitability, adequacy, and effectiveness.

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | SUMMARY OF CHANGE | CHANGED BY |
| 1.0 | 2020-05-06 | First version | Muhammad Nasir |
| 1.01 | 2020-05-12 | Update template, minor changes | Razvan Anghelidi |
| 1.02 | 2020-05-29 | Minor updates | Razvan Anghelidi |
| 1.03 | 2020-12-04 | Annual review | Razvan Anghelidi |
| 1.04 | 2021-12-12 | Annual review | Hadeel Alzuhairi |