Change Management and Control PolicyContents

[1 Introduction 3](#_Toc279662605)

[2 Scope 3](#_Toc279662606)

[3 Purpose 3](#_Toc279662607)

[4 References and definitions 4](#_Toc279662608)

[4.1 Normative references 4](#_Toc279662609)

[4.2 Definitions and abbreviations 4](#_Toc279662610)

[4.2.1 Audit trail 4](#_Toc279662611)

[4.2.2 Information resources 4](#_Toc279662612)

[4.2.3 Abbreviations 4](#_Toc279662613)

[5 Policy 5](#_Toc279662614)

[5.1 Preamble 5](#_Toc279662615)

[5.1.2 Operational Procedures 5](#_Toc279662616)

[5.1.3 Documented Change 5](#_Toc279662617)

[5.1.4 Risk Management 6](#_Toc279662618)

[5.1.5 Change Classification 6](#_Toc279662619)

[5.1.6 Testing 6](#_Toc279662620)

[5.1.7 Changes affecting SLA‘s 6](#_Toc279662621)

[5.1.8 Version control 6](#_Toc279662622)

[5.1.9 Approval 6](#_Toc279662623)

[5.1.10 Communicating changes 6](#_Toc279662624)

[5.1.11 Implementation 6](#_Toc279662625)

[5.1.12 Fall back 7](#_Toc279662626)

[5.1.13 Documentation 7](#_Toc279662627)

[5.1.14 Business Continuity Plans (BCP) 7](#_Toc279662628)

[5.1.15 Emergency Changes 7](#_Toc279662629)

[5.1.16 Change Monitoring 7](#_Toc279662630)

[6 Roles and Responsibilities 8](#_Toc279662631)

[7 Compliance 10](#_Toc279662632)

[8 IT Governance Value statement 10](#_Toc279662633)

[9 Policy Access Considerations 10](#_Toc279662634)

# Introduction

#### IS gains discipline and quality control through operational change management. Its success will be determined by its governance and established policies and processes. Using formalized governance and regulations to manage operational change results in a more disciplined and efficient infrastructure. This formalization necessitates communication, the recording of critical process processes and people responsibilities, and, when applicable, the alignment of automation technologies. Where change management is lacking, it is the responsibility of IS's senior management to offer the leadership and vision necessary to kick-start the process. IS organizations may exhibit improved agility in responding predictably and consistently to changing business needs by creating procedures and rules.

#### The management of Walpita Enterprises Pvt Ltd recognizes the importance of change management and control, as well as the dangers associated with inadequate change management and control, and has developed this Change Management and Control Policy to meet the opportunities and risks.

# Scope

#### This policy applies to everyone who interacts with the company's network or uses its information resources. It includes data networks, LAN servers, and personal computers (stand-alone or network-enabled) at company offices and production-related locations where these systems are under the company's jurisdiction and/or ownership, as well as any personal computers, laptops, mobile devices, and servers authorised to access the company's data networks. This policy applies to all employees.

# Purpose

#### The goal of this strategy is to define managerial direction as well as high-level change management and control objectives. This policy will guarantee that change management and control techniques are used in order to reduce risks such as:

* Information that has been damaged and/or lost;
* Computer performance that has been interrupted and/or impaired;
* Productivity losses;
* Rreputational harm.

# References and definitions

## Normative references

#### The following papers include provisions that, by virtue of their inclusion in the text, constitute policy requirements. The editions listed were valid at the time of publication. All standards and specifications are subject to change, therefore parties to agreements based on this policy should look into using the most recent editions of the papers indicated below.

* Information Security Policy (overall)
* Information Security - Systems Development and Maintenance Policy
* Information Security - Business Continuity Management
* Information Security - Physical Asset Classification and Control Policy
* Information Security – Change Control Procedure

## Definitions and abbreviations

### Audit trail

#### A record or set of records that allows the processing carried out by a computer system to be precisely recognized as well as the validity of such modifications to be verified.

### Information resources

#### All data, information, including the technology, software, personnel, and procedures that go into storing, processing, and distributing it. Data networks, servers, PCs, storage media, printers, photo copiers, fax machines, supporting equipment, fall-back equipment, and backup media are all examples of this.

### Abbreviations

* **PC:**   Personal Computer
* **BCP:** Business Continuity Plan
* **SLA:** Service Level Agreement

# Policy

## Preamble

#### A rigorous change control procedure must be used to manage and implement changes to information resources. The control process ensures that proposed changes are evaluated, authorized, tested, implemented, and released in a controlled way, as well as that the status of each proposed change is tracked.

#### In order to fulfil this policy, the following statements shall be adhered to:

### Operational Procedures

#### The change management process must be formalized and recorded. To control changes to all important business information resources, a change control methodology must be in place (such as hardware, software, system documentation and operating procedures). Management roles and procedures must be included in this defined process. Operational and application change control methods should be linked wherever possible.At a minimum the change control process should include the following phases:

* Logged Change Requests;
* Identification, prioritisation and initiation of change;
* Proper authorisation of change;
* Requirements analysis;
* Inter-dependency and compliance analysis;
* Impact Assessment;
* Change approach;
* Change testing;
* User acceptance testing and approval;
* Implementation and release planning;
* Documentation;
* Change monitoring;
* Defined responsibilities and authorities of all users and IT personnel;
* Emergency change classification parameters.

### Documented Change

#### On an uniform and central system, all change requests must be documented, whether granted or refused. All modification requests must be approved, and the outcomes must be recorded.

#### At all times, a documented audit trail including relevant information must be kept at the Business Unit Level. Change request paperwork, change authorisation, and the change's outcome should all be included. Without the permission of other authorized people, no one individual should be allowed to make modifications to production information systems.

### Risk Management

#### For all modifications, a risk assessment must be completed, followed by an impact assessment based on the outcome.

#### The possible influence on other information resources as well as any financial consequences must be included in the impact evaluation. Compliance with legal requirements and standards should be considered in the impact assessment when relevant.

### Change Classification

#### All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.

### Testing

#### Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made. (For more information see **System Development Life Cycle** [1]).

### Changes affecting SLA‘s

#### It is necessary to consider the impact of the change on present SLAs. Changes to the SLA must be governed by a structured change procedure that includes, where applicable, contractual amendments.[2].

### Version control

#### Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies. (For more information see **System Development Life Cycle** [3 ])

### Approval

#### Prior to implementation, all changes must be approved. Changes will be approved based on formal acceptance criteria, such as a change request from an authorised user, an effect assessment, and a test of the proposed changes.

### Communicating changes

#### All users who will be significantly impacted by a change must be notified. The change must be approved by the user representative. Users will be needed to make submissions and provide feedback prior to the modification being accepted.

### Implementation

#### Only after thorough testing and approval by stakeholders can implementation begin. All significant modifications must be handled as a new system implementation and documented as a project. Major modifications will be categorized based on the time and effort required to develop and implement them.plementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes. (For more information see **System Development Life Cycle** [4])

### Fall back

#### Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

### Documentation

#### Documentation for information resources must be updated after each modification, and old documentation must be stored or disposed of according to the documentation and data retention regulations.

#### The documenting of information resources is used for reference in a variety of circumstances, including the expansion of current information resources and guaranteeing proper knowledge transfer in the event that the original developer and/or development house are unavailable. As a result, it's critical that the documentation for information resources is full, accurate, and up to date with the newest modifications. On completion of each change, policies and procedures impacted by software changes must be modified.

### Business Continuity Plans (BCP)

#### Changes to business continuity plans must be updated and controlled through the change control process. BCP documentation must be thorough, accurate, and readily available in order for business continuity plans to be effective. BCP documentation serves as a road map for minimizing disruption to important business activities and facilitating their speedy recovery in the event of a disaster.

### Emergency Changes

#### Specific protocols must be in place to provide adequate control, permission, and recording of emergency adjustments. For defining modifications as Emergency changes, specific parameters will be developed as a standard.

### Change Monitoring

#### After all modifications have been deployed out to the production environment, they will be monitored. Deviations from design specs and test findings will be documented and forwarded to the solution owner for approval.

# Roles and Responsibilities

|  |  |
| --- | --- |
| **ROLE** | **FUNCTIONAL RESPONSIBILITIES** |
| Members of the Board | 1. Members of the Board are responsible for ensuring that the required information security procedures are implemented and followed in accordance with this policy. |
| Information Security Manager | 1. With input from interest groups and subsidiaries, develop and revise an information security strategy, policy, and standards for change management and control. 2. Facilitate and coordinate the necessary countermeasures to modify management and control initiatives, as well as assess and evaluate policies and standards; 3. Establish security requirements for change management and control directives, as well as approval of change management and control standards and change control/version control products; Coordinate the entire change management communication and awareness strategy. 4. Acts as the change management and control advocate in the organization; 5. Provide technical input into service needs and, if applicable, coordinate affected adjustments to SLAs. 6. Create and coordinate relevant interest group forums to represent, feedback on, implement, and track change management and control activities; and 7. For change management, coordinate the deployment of new or additional security controls. |
| Operations Manager | * With input from all stakeholders, implement, maintain, and update the change management and control strategy, baselines, standards, rules, and procedures. * On behalf of Walpita Enterprises Pvt Ltd, approve and authorise change management and control measures. * Ensure that all application owners are aware of the necessary change management and control policies, standards, processes, and guidelines. * Ensure that any changes to policy, standards, or procedures are reported to the appropriate owners and management forums. * Appoint the required representation to the interest groups and other forums for Information Security Management relating to change management and control that each organization has established; * Establish and revise a change management and control strategy, policy, and standards for information security; * Facilitate and coordinate within each organization the essential change management and control initiatives; * Change management and control rules and standards are reported and evaluated. * Co-ordinate the deployment of new or additional security controls for change management and control; Co-ordinate the overall communication and awareness strategy for change management and control * Review the efficacy of the change management and control plan and put in place corrective controls if deficiencies are found; * Regularly provide updates on change management and control projects, as well as the appropriate application; * Evaluate and recommend improvements to change management/version control systems; and Coordinate awareness campaigns and rollouts in each firm to effectively communicate change management and control mitigation solutions. * Establish and put in place the appropriate standards and procedures in accordance with the Information Security policy. * Responsible for approving, authorizing, monitoring, and enforcing change management initiatives and related security controls across all Walpita companies and divisions; Ensure that all solution owners are aware of change management and control policies, standards, processes, and guidelines. * Ensure that this policy is followed and that any variations are reported to the Information Manager. |
| IT Service Provider | * Shall follow all of this policy's change management and control statements. |
| Solution Owners | * All information security rules, standards, and processes for change management and control must be followed, and any deviations must be reported. |

*Table 1 Roles and Responsibilities*

# Compliance

#### Any person who violates the requirements of this policy or any amendments thereto will be liable to appropriate disciplinary or legal action in line with the Walpita Enterprises Pvt Ltd Disciplinary Code and Procedures. Legal, regulatory, and statutory obligations must be met by the company's information security policies, standards, procedures, and guidelines.

# IT Governance Value statement

#### Changes that have a significant impact on the financial process must be assessed and reported on on a quarterly basis. Upgrades or replacements of financial systems will necessitate fresh certification. The consequence is that Sarbanes-Oxley compliance is contingent on the operational systems and processes you implement.

# Policy Access Considerations

#### Access to this policy shall be granted to:

* All IT personnel
* Business Unit Management teams
* Executive Directors

**References**

1. [online] Available at: <https://performancelabus.com/software-testing-importance-sdlc/>
2. Lts.lehigh.edu. 2021. *Systems Development Life Cycle and Change Management | Library & Technology Services*. [online] Available at: <https://lts.lehigh.edu/services/explanation/systems-development-life-cycle>
3. Atlassian. 2021. *What is version control | Atlassian Git Tutorial*. [online] Available at: <https://www.atlassian.com/git/tutorials/what-is-version-control>
4. Study.com. 2021. [online] Available at: <https://study.com/academy/lesson/implementation-coding-phase-in-sdlc.html>