OPD_Change Management and Control Policy

Document Details

Document Path	http://192.168.1.102:9073/Mindshare/5gpal/policies/OPD_Change Management and Control Process
Document Version	1.3
Document Date	January 31st, 2017
Document Status	Final
Circulation Type	Internal
Circulation List	All@ 5G

Revision History

Ver No. & Date	Added/ Revised By	Content Added/ Changed	Reviewed/ Approved By	App. Date	Broadcast Date	Effective Date
1.0 / March 1 2007	5G PG	As part of Quality Process Manual	Sumitra Seshan	Mar 27, 2007	Mar 28, 2007	Apr 1, 2007
1.1/October 22nd 2012	Jai Srinivasan	Separated from Quality Process manual – content changed	Sumitra Seshan	October 30th, 2012	October 31st, 2012	October 31st, 2012
1.2/April 4th 2015	Jai Srinivasan	Content updated	Sumitra Seshan	April 14th 2015	April 14th 2015	April 15th 2015
1.3/January 31, 2017	5G PG	Logo changed	Sumitra Seshan	Feb 15, 2017	Feb 15, 2017	Feb 15, 2017

Table of Contents

1. Introduction

Adopting formal and standard policies for operation change management, delivers a disciplined and efficient infrastructure, thereby ensuring an efficient organization. The Change Management and Control Policy of 5G (herein '5G' refers to Fifth Generation Technologies India (P) Ltd., 5G Automatika Ltd., 5G Energy Ltd., 5G Technologies Ltd.), has been developed keeping in mind the necessity for 5G to demonstrate its agility in responding to business and environmental changes in a predictable and reliable manner.

2. Objective

This policy applies to all 5G employees who are working within the company's network environment or utilizing IT resources. It covers data networks, servers and personal computers and Laptops and mobile devices that are authorized to access company's data networks. No employee is exempt from this policy.

Change Management and Control Process in *5G* has been formulated to ensure that 5G efficiently manages and mitigates the risks associated with the

- Information being corrupted and/or destroyed;
- Computer Performance being disrupted and/or degraded;
- Productivity losses being incurred; and
- Damage (if any) to the image of 5G brand.

3. Change Management and Control Process

i. Change Control Process shall be in place to control changes to all critical company information resources (such as Hardware, Software, Documentation, Organizational Policies and Processes).

ii. Change Request may occur in many forms

    a. oral or written;

    b. externally or internally initiated (eg. Could be client initiated or initiated within the organization in order to align with the external business needs)

    c. legally mandated or optional (eg. Introduction of a new tax by the government)

iii. The Change Management Process shall include following steps:

    - Logging of Change Requests;

- Impact Assessment
- Estimating the Cost of Impact;
- Authorization of associated costs due to the change (authorization shall be sought from clients in case of Requirement/Scope changes that are related to project development);
- Develop an Approach Plan for implementing the change;
- Change testing in isolated environment;
- User testing and approval;
- Implementation and release planning;
- Documentation.

3.1.1 Change Request Log

- A Change request log (process template/Change Request Log) is maintained in central repository of 5G, to keep track of the change requests. All change requests shall be logged whether approved or rejected on a tracker system. Each entry in the log contains a Change Request Number, a brief description of the change requested, the effect of the change, the status of the change request and key dates. Change requests received from a client shall be tracked within the respective project repository.
- This tracker will capture all the necessary documentation related to this change request. No single person shall make changes to the production information systems without the approval of authorized personnel.

3.1.2 Change Classification

The change requests will be initially categorized as (a) Project related Change Request (b) Product related Change Requests (c) IT Infrastructure or Organization related Change Requests. However, all change requests need to be prioritized based on benefits, urgency, effort required and potential impact on the project or organization.

Project Related Change Requests:
  - A change request can be classified as minor if the total effort involved in implementing it does not exceed two person-days. This change will be absorbed as part of the project effort and will be accommodated within the planned estimate.
  - If the impact is more than two days then the effort estimate has to be re-negotiated and revised. The change in the schedule/effort has to be communicated to and

approved by the client.

- o Major changes in the scope/requirement needs formal approval from the client since it would have severe impact on the development effort.

In case of product development related change requests, any new feature that the customer wants are documented and maintained as a wish list for the next version of the product. By doing so, it is ensured that the customer feedbacks are not lost and that they get incorporated in the Market requirement document for the product's subsequent releases. These requests are prioritized and finalized as part of the Product Release Management process.

In case of IT security, environment or infrastructure changes, the users can log their requests directly onto the Issue Tracker which is monitored regularly by the IT System Administrator.

3.1.3 Impact Assessment

All change requests shall go through Impact Assessment and Analysis. This exercise shall try to address the following questions:

- o Is the Change necessary? in this release?
- o What other groups, resources shall be impacted by the change? How will dependencies be impacted?
- o Is there a more effective and preferred change to the one that has been proposed?
- o What documentation must be produced to document the change properly?
- o How and when can the change best be made with the least negative impact?

3.1.4 Approval Process

All changes shall be taken up for implementation only after approval. Change Requests that have impact on (a) Cost (b) Schedule (c) Effort (d) Information Infrastructure and Security shall go through a formal approval and acceptance process that is governed by the overall organization's structure and policies. In case of client projects, Change Requests forms are sent to the client for their approval, only after which the requests are taken for development and implementation.

3.1.5 Testing

Changes shall be tested in an isolated, controlled test environment (where such an environment is feasible) prior to implementation in the production environment, in order to minimize the impact on regular business operations and security. Please refer to section related to Quality in the Process Manual of 5G.

3.1.6 Version Control

All changes related to software shall be controlled using version control. Older versions shall be retained in accordance with 5G's overall configuration management policies.

3.1.7 Communicating changes

All users who shall be significantly impacted by the changes shall be kept informed formally.

3.1.8 Implementation

Implementing the changes shall be undertaken only after appropriate testing and approval by all stakeholders. All major changes shall be treated as new initiatives and a request for initiating a new project in 5G's intranet tool (Mindshare) will be initiated by appropriate authorized personnel.

3.1.9 Documentation

- Change Request Templates are maintained in the respective Project Repositories for future references, knowledge transfer etc. as per 5G's Configuration Management Policies.

4. Roles and Responsibilities

Role	Responsibilities
Change Control Board	o Responsible for providing oversight and inputs to the information security policies of the organization o Approval of Change Requests o Periodic review of Information Security Audits to ensure that necessary Information Security Controls are implemented properly and complied with as per 5G's Information Security Policy.
Compliance Officer	o Along with the IT System Administrator is responsible for overseeing the implementation of Security Policies as defined in the overall Information Security and Management Policy of the Organization. o Perform compliance audits against the standard policies and file a monthly report to the CCB. o Coordinate overall communication strategy with respect to changes. o Process Owner and internal champion of the Change Management Process. o Coordinates the Implementation of Change Process for the organization.

Role	Responsibilities
IT or System Administrator	o Overall responsible for developing and implementation of Security Policies as per the direction of the Executive Management and to keep up the changes to the industry standards and environment needs. o Monitor Change Requests related to IT Systems and Processes regularly. o Perform Impact Assessment. o Sought approval for changes. o Implement IT/System changes as per IT Security Policies and Processes. o Establish and implement the necessary standards and procedures that conform to the Information Security policy. o Communicate the changes and closure of requests regularly to the CCB. o Coordinate the communication and awareness exercise with respect to changes within the organization. o In case of Emergency has direct access to the CEO and Executive board of the organization for escalation purposes.

- End of Document -