Information Security Management System
Change Management Policy & Procedure

Document no. JMBGRP/ISMS/Pol-CH

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The policy document provides a means to initiate, evaluate and implement a change request for IT infrastructure and applications	
Custodian	Corporate IT dept.	
Approved by	Manish Jaiswal (Group CTO)	
Owner	Corporate IT Dept.	

Distribution list

Name
To all locations of JMB group.

Version History

Version no.	**Version date**	**Approved by**	**Comments**	**Signature**
v1.0	28.08.2018	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	10.01.2019	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	08.02.2020	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	11.02.2021	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.1	25.03.2022	Manish Jaiswal (Group CTO)	Logo changes done in this policy	
v1.2	18.08.2023	Manish Jaiswal (Group CTO)	Document reviewed. Modification done to "21. Reference to ISO 27001:2022"	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: "3,4,6,7,8"	

Contents

1. Purpose

1.1. Change Management Policy provides a means to initiate, evaluate and implement a change request for IT infrastructure and applications.

2. Scope

This policy applies to the following:

- All Locations of J.M Baxi Group
- All Employees, contract workers and vendors of J.M Baxi Group

3. Policy Statement

3.1. The End user may initiate a Change Request through request form or ticketing management system after approval from department head.

3.2. JMBGRP shall employ a formal mechanism to capture change requests emerging from the business groups and the technology groups.

3.3. All changes before getting executed shall be formally approved by concerned stakeholders from business and technology groups.

3.4. The Change Requests shall be dealt with in terms of their importance and impact on the business.

3.5. All change requests made and closed in the affirmative or those which have been denied / delayed or escalated shall be documented in a pre-prescribed format and detail. Records of the change requests shall be maintained by the process owner for audit purposes.

3.6. No changes to the information systems shall be made without valid and authorized change control approval in place.

3.7. A formal review of all changes made to JMBGRP's information systems and infrastructure shall be conducted.

4. Procedure

4.1. Changes to the existing system / process may be required because of technological or business changes.

4.2. Listed below are examples of technological changes, but not restricted to:

4.2.1. New technology application roll out.

4.2.2. New equipment / server roll out.

4.2.3. Migration of applications from one existing commissioned server to another existing server.

4.2.4. Server version upgrade, hardware / software

4.2.5. Changes to firewall rules.

4.2.6. Network device / Server configuration changes

4.2.7. Services to be started and stopped.

4.2.8. Patch updates for critical servers

4.2.9. Commissioning and decommissioning of equipment.

4.2.10. Computer system validations and updates

4.3. Listed below are examples of business changes, but not restricted to:

4.3.1. New business applications roll out.

4.3.2. Request for modification to applications due to errors.

4.3.3. Development of new modules as per business requirement.

4.4. Listed below are examples of business changes, but not restricted to:

4.4.1. New business applications roll out.

4.4.2. Request for modification to applications due to errors.

4.4.3. Development of new modules as per business requirement.

4.5. Type of changes:

4.5.1. **Scheduled Change:** Formal notification received, reviewed and approved by the review process in advance of the change being made.

4.5.2. **Emergency Change:** These are changes which need to be made as soon as possible to avoid any loss to business. Instances where emergency changes may be required, however not limited to, are

4.5.2.1. System failure

4.5.2.2. Major security vulnerability

4.5.3. **Routine Changes**: These changes should be done on a should be examine and done within 3 to 6 months depending upon the criticality by the concerned process own

4.6. Change Management Process:

4.6.1. Change Request

4.6.2. Change management controls apply to various areas mentioned in the scope above. Since the changes could be initiated either from business users or infrastructure users, the process is bifurcated. The application change management process is described under the same.

4.6.3. When a user/system administrator requires a change to be made, a formal change request procedure should be followed.

4.6.4. The Change Management Form should be used to record all activities for the change management process. The user requesting the changes should fill in the form and get it approved by the Department Head.

4.6.5. The change request should contain the following details:

4.6.5.1. Description of change: The details regarding the changes including configuration changes, installation of additional components and system restart requirements.

4.6.5.2. Change objective or reason for change: There should be a clear justification for the change. This could include new business requirements, product feature enhancements and problem rectification.

4.6.5.3. Users/Applications/Services affected during/post the change: List of the users and department who will be affected because of the change.

4.6.5.4. Alternate Solution, if any, should be provided. If there are alternate solutions which could achieve the same benefits, these should be documented.

4.6.5.5. All application functionality related changes should be logged/approved through the E-mail and Change Management Form.

4.6.5.6. For all IT infrastructure related changes, the Head-IT or his nominee (IT Managers) along with the concerned personnel should perform the Feasibility analysis of the change and record it in the Change Management Form.

4.6.6. Feasibility analysis should be carried out based on the following parameters:

4.6.6.1. Need for change: The objective of the change should be evaluated to check if it is in accordance with the business requirements.

4.6.6.2. Impact of change: The impact of the change on the overall network and systems should be identified.

4.6.6.3. Priority of change: The criticality of the changes should be evaluated. The priority will determine if the change needs to be done immediately or can be implemented at a later time.

4.7. Change evaluation and approval

4.7.1. The approval authorities for the changes should be segregated from the requestor to avoid a conflict among the duties of the individual.

4.7.2. The change requests are analyzed for identifying the:

4.7.2.1. Feasibility.

4.7.2.2. Priority of the change based on the impact, nature, type and time required for implementation impact of the change on the existing control setup.

4.7.3. The approval authorities should determine whether the changes compromise the security controls implemented for the information system / hardware. In such cases, approval should be obtained from the Departmental head (DH) / Information Security Manager prior to initiating the change resolution and Carrying out the Risk Assessment.

4.7.4. All changes to IT infrastructure will have to be approved by the Head-IT in concurrence with respective IT Manager. The Change Management Ticketing Tool will be maintained for all changes. The CR number provided in the form will serve as the primary key for the audit logs. The reference number will be unique and will be taken in succession after the last CR from the Change Management Ticketing Tool.

4.7.5. The Department Head will ensure that the details on the person responsible for implementing the changes will be updated in the Change Management form, along with the criticality of the change.

4.7.6. The resolution timeframes for the changes will be decided by the Department Head and updated in the Change Management Register.

4.7.7. Roll Back plan should be part of CR.

4.8. Change Impact Analysis

4.8.1. The request for change should be approved by the Head–IT based on the business requirement, process improvement or to enhance the security of the environment. The approval should be recorded in the Change Management Form.

4.8.2. Once the change has been approved, IT team consisting of the administrators, operational personnel and third-party vendors (if any), should prepare a detailed implementation plan consisting of the following details

4.8.2.1. Time and resource requirements: The time and resource (in terms of people or additional software/hardware, commercials) requirements for implementing the change should be identified and documented.

4.8.2.2. Pre-requisites: If there are pre-requisites including completion of day end activities or taking a full backup that need to completed, before the change can be done, these should be documented.

4.8.2.3. Downtime requirements: If the change involves system downtime, then it is preferred to be scheduled during non-business hours. Arrangements should be made for availability of the system

personnel and specific users required to implement and verify the change.

4.8.2.4. Implementation Steps: The steps that need to be executed to implement the change and the personnel responsible for executing the steps should be documented in detail.

4.8.2.5. Test Plan: The procedure for testing the change should be documented. The team responsible for implementing the change should consult with the end users while creating the test plan.

4.8.2.6. Roll Back Plan: There should be a documented roll back plan for restoring the system to the original state. The time and the resources required to implement the rollback should also be documented.

4.8.2.7. The Business/Application owner should inform the user and the IT team about the change to be implemented.

4.8.2.8. A mail should be sent to all the users and the IT team briefing them about the changes to be applied and the downtime requirements.

4.9. Change Testing

4.9.1. The team responsible for implementation should make the change on a test system as per the implementation plan and confirm functionality of the system to the Head– IT.

4.9.1.1. Any deviations from the implementation plan should be documented in the Change Management Form.

4.9.2. The team responsible for implementation should test the roll back plan in the staging environment.

4.9.3. Once the tests are confirmed, the Head – IT should approve the implementation of the change on the production systems.

4.9.3.1. There may be cases where testing is not required or is not feasible. Such cases should be documented in the change request form.

4.10. Change Implementation

4.10.1. The team responsible for implementation should perform the changes on the production system in accordance with the implementation plan.

4.10.2. The team responsible for implementation should submit a post implementation report containing details of actual steps done during implementation. This should include all details pertaining to the following:

4.10.2.1. Time and resources

4.10.2.2. Implementation steps involved.

4.10.2.3. Test plan results

4.10.2.4. Justification for deviation (if any) from the plan

4.10.3. The configuration document of the IT asset affected by the change should be updated accordingly after the successful change implementation.

4.11. Change Monitoring & Verification

4.11.1. Once the change has been implemented, the change should be monitored for a few days to ensure that the change has not affected the regular business operations.

4.11.1.1. The Change should be reviewed for effectiveness based on the following parameters Changes achieving the desired objective: The Head-IT along with the Department Head should evaluate if the objectives defined in the original change request have been met.

4.11.1.2. Adherence to the implementation plan: The Head-IT should evaluate if all the steps that were proposed in the implementation plan have been followed and if the time and effort estimates were appropriate.

4.12. Change Rollback

4.12.1. If the change is not successful, then the change applied should be rolled back as per the roll back plan documented.

4.12.2. After the implementation of the rollback plan, the system should be verified by the IT Manager.

4.12.3. The IT Manager should maintain records of the changes and the rollback activity.

4.12.4. Post Implementation Review

4.12.5. The IT Manager along with the Head - IT is responsible for carrying out post implementation review to ensure that the desired changes have taken effect and there is no unexpected behavior.

4.13. Emergency Change

4.13.1. Emergency changes (e.g., system, breakdown, priority security patches etc.) should be carried out only under exceptional circumstances. Such changes should be carried out as necessary on receiving verbal approvals (Followed by proper approval later) from the Head–IT.

4.13.2. The emergency changes should be ratified as per the normal change management process defined above.

4.13.3. The following steps should be taken to ensure integrity of the computer systems during such situations:

4.13.3.1. The emergency changes should be allowed only to resolve production problems.

4.13.3.2. The IT Manager should document the approved changes and report them to the IT Head.

4.13.4. The person responsible for implementing the change should submit a post- implementation report to the IT Head. This should include all details of the change including the following:

4.13.4.1. Reason for change

4.13.4.2. Implementation steps involved.

4.13.4.3. Test plan results

4.13.5. All emergency changes should be reviewed by the Head-IT. If the changes do not meet the desired objective, the Head-IT should inform the IT team to perform a rollback of the change.

4.13.6. Records of rejected change requests should also be maintained. In such cases, the reason for the rejection of the change request should also be mentioned as a record.

4.13.7. The System and Network change management process flow should be in accordance with the procedure.

4.13.8. Measurement Metrics – Change Management (quarterly) should be sent to IT Team.

4.14. Changes in Secure system architecture and engineering principles

4.14.1. Identify proposed changes to the system architecture or engineering.

4.14.2. Document and categorize proposed changes.

4.14.3. Conduct an impact assessment to determine potential effects on security architecture.

4.14.4. Review proposed changes by security experts to ensure alignment with secure system architecture principles.

4.14.5. Evaluate proposed changes against established security standards and guidelines.

4.14.6. Obtain approval from relevant stakeholders

4.14.7. Implement approved changes following organizational change management procedures.

4.14.8. Conduct thorough testing and validation of implemented changes.

4.14.9. Document all changes, including security considerations and risk assessments.

4.14.10. Monitor implemented changes for effectiveness and potential security risks.

4.14.11. Conduct periodic reviews and adjustments as needed.

4.14.12. Provide training and awareness programs to relevant personnel.

4.14.13. Establish procedures for incident response related to changes in system architecture or engineering.

5. Enforcement

5.1. This policy and procedure is applicable for all the employees and contractors of the company who have access to and use the information assets and IT assets as listed in the Information Asset Classification sheet which have been created for all the departments. Any violation shall be dealt with in accordance with the disciplinary action process as laid down in the Code of Conduct.

5.2. Violations by the vendors shall also come under the purview of the Information Security Framework and action shall be taken accordingly.

5.3. Management's interpretation of the clauses in this procedure shall be final and binding. Management reserves the right to alter or amend any clause in this document at any time as per its discretion.

6. Metrics

6.1. The metrics shall be measured by the IT Team and reported to Security In-charge/Head-IT on a quarterly basis.

6.2. The metrics to be measured are given as under but not restricted to

6.3. No of cases unresolved.

6.4. No of changes done but not recorded.

6.5. No of emergencies handled.

6.6. No of changes carried out.

6.7. Number of changes not rolled back after expiry.

7. Exceptions

7.1. Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the information owner. These may arise, for example, because

of local circumstances, conditions or legal reasons existing at any point of time.

7.2. Exceptions to this Policy and Procedures shall have to be allowed at the time of implementation of this policy and procedures or at the time of making any updating to this document or after implementation on an ad-hoc basis as per business or a specific and a peculiar manifestation of circumstances which could be of temporary or permanent in nature.

7.3. Any exceptions during implementation shall be submitted by the HODs responsible for the particular vendor. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester.

7.4. The Security In-charge shall review all exceptions, as the case may be, every year for validity and continuity.

8. Disclaimer

8.1. JMBGRP reserves all rights and is the exclusive owner of all intellectual property rights over this Acceptable usage Policy and Procedures document. This document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (such as hard disks, USB Drives, Pen Drives, Memory Cards, CDS, DVD's), and/or captured or transmitted through by any means (such as electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior consent from the Apex Committee. The Acceptable usage policy and procedure document is meant to be published on the intranet of JMBGRP and/or any other forum as decided by the management of JMBGRP. Anything not specifically stated in this Acceptable usage policy and procedure document shall not be considered as implied in any manner.

8.2. For any clarifications related to this Acceptable usage policy and procedure document with respect to its interpretation, applicability and implementation, please raise the request in Ticketing Tool.

9. References:

Control Objectives: 8.27, 8.32