Information Security Management System Compliance, Audit & Sustenance Policy & Procedure

Document No. - JMBGRP/ISMS/Apex_03

Version_v1.2

Document Details

Classification	Internal	
Released date	28.08.2018	
Description	The policy document addresses aspects of sustenance; audit and compliance required to be adhered to and fulfilled with respect to Information Security Policies and Procedure.	
Custodian	Corporate IT dept.	
Approved by	Manish Jaiswal (Group CTO)	
Owner	Corporate IT dept.	

Distribution List

Name
To JMBGRP Employees Only
Third Party and Auditors: On Need basis

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 Reference to ISO 27001:2022	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: “Scope, Policy Statement, Procedure”	

Contents

Purpose

This policy addresses aspects of sustenance; audit and compliance required to be adhered to and fulfilled with respect to J.M Baxi Group (hereinafter referred as JMBGRP) Information Security Policies and Procedure.

The audit component of the document shall seek to provide the specific and overall, Health Status of the organization against the various domains and the commitment of the organization in terms of implementation effectiveness.

Scope

This policy applies to all employees;)Business owners, custodians, system administrators, software developers and users of information).

The policy also applies to other stakeholders such as outsourcing partners, consultants and trainees, Contractors, Service providers etc.

Policy Statement

- JMBGRP has instituted a comprehensive set of Information Security Policies and Procedures to protect the confidentiality, integrity and availability of its information assets.
- In order to ensure that policy deployment and implementation stays consistent with planned outcomes, JMBGRP shall establish a sustenance, audit and a compliance mechanism to ensure continual improvement of ISMS takes place.
- The policy covers the following areas.
    - Sustenance
    - Audit
    - Compliance
- Audit
    - The Internal Audit Team shall be responsible for conducting audits as per the published schedule every year in coordination with the Security In-charge.
    - External audits shall be conducted if the organization seeks to be certified and wishes to bring an independent review of the smooth functionality of the defined processes.
    - The audit approach could be by way of a desktop review and or process review.
    - All new facilities of JMBGRP which manage information shall also be audited post them getting commissioned.
    - Those involved in implementation shall not be allowed to conduct the audit.
    - Independence of an auditor shall be ensured in any audit activity.
- Compliance
    - Compliance at the group level shall be ensured by the Security In-Charge as per the outcome of the audit, ensuring implementation effectiveness through the controls deployed and submissions towards regulatory requirements if any.
    - Compliance at IT functional level shall be the responsibility of the Security In-Charge through the Positive Assurance Report mechanism.
    - Use or creation of Intellectual Property within JMBGRP shall be in accordance to the regulatory and legislative norms.
    - Use of approved and licensed tools shall be necessary for the purpose of

conducting audits, monitoring of implementation and sustenance activities and ensuring compliance in accordance within the regulatory landscape.

- Dashboards, reports and corrective action plans shall be deployed as means of communication to the Apex Committee and to the rest of the employees on a need-to-know basis.
- The Security In-Charge shall be responsible for defining the periodicity of audit, monitoring and review of metrics to ensure their relevance and adequacy; and submission of Compliance Reports to the Apex Committee.
- Any exception to this policy shall be managed by a formal process.

Procedure

The procedure section has been divided into three sections namely:-

1.1 Sustenance

1.1.1 The sustenance activity shall be carried out at the IT functional level. The Security In-Charge shall be overall responsible and will be supported by the respective PO's across all the locations under the purview of the Security In-Charge.

1.1.2 The starting point of the sustenance activity shall emerge from the Information Asset Listing Classification (IAC) Activity, followed by the Risk Assessment and Risk Treatment Plan (RARTP) for a location including the capture of any specific threats and vulnerabilities captured for a department.

1.1.3 Based on the outcome of the IAC and RARTP, the Security In-Charge will have the dashboard of the critical processes by department based on the classification of information assets and the associated risks which will be mitigated.

1.1.4 Each Process Owners as the case may be will submit the action plan for the mitigation of risks affecting their own departments for management sanction and approval based on prioritization of the Risk Impact Rating.

1.1.5 Each Process Owners shall provide the Security In-charge and the Corporate Security In-charge with a Positive Assurance Report covering aspects of legal compliance based on applicable legislation; the activity should be conducted once every six months (as per regulatory requirement).

1.1.6 The Security In-Charge shall have an overall action plan for the location on the prioritized Risk Impact Rating in descending order.

1.1.7 The action plan shall be monitored by the Security In-Charge on a monthly basis and the Security In-Charge shall intervene any executive action or any threats or vulnerabilities are not addressed in the previous risk assessment. The support and assistance of the Security In-Charge shall be sought for if necessary.

1.1.8 Security In-Charge will prepare the metrics which is apart from the implementation plan for the deployment of controls shall form a part of the sustenance activity, help for which shall be provided by the Security In-Charge.

1.1.9 Metrics shall be identified based on the outcome of the Risk Assessment, and the monitoring of which will act as a preventive control.

1.1.10 Action points from the previous audits and Corrective Action Plans will also form a part of the sustenance process.

1.1.11 The Security In-Charge shall take a formal approval from the Apex Committee in writing for the execution of the implementation plans.

1.2 Audit

1.2.1 The Security In-Charge shall publish the audit calendar at the beginning of the fiscal year for all the locations in scope.

1.2.2 Internal audit should be conducted once in a year.

1.2.3 The identified members of the Internal Audit Team, by the Apex committee shall be responsible for conducting the audits.

1.2.4 The Internal Audit Team shall be equipped with the necessary skills to perform Information Security Audits, through training or derived knowledge of ISO 27001:2022.

1.2.5 External Audits shall be carried out every year through an independent third party.

1.2.6 The auditee should be briefed on the audit procedure to be adopted and the scope of the audit.

1.2.7 Segregation of duties shall be maintained when audits are being conducted. The auditor shall not be allowed to audit his/her own department.

1.2.8 The audit will comprise of 3 types of audits namely:-

1.2.8.1 Management System Audit for Information Security as per the Framework for the sustenance activity conducted and against compliance to the ISMS Policies and Procedures

1.2.8.2 Technical Compliance Audit for the IT Infrastructure and Supporting Utilities.

1.2.8.3 Identified Critical Third Parties

1.2.9 Management System Audit

1.2.9.1 The first component of this will comprise of Management Review. This will comprise of the review of the framework and the activities by the Apex Committee, Chief Information Security Officer, Information Security Manager and respective Process Owner / Functional Head, in terms of their commitment to the initiative in intent and spirit. Corresponding records, metrics and the inputs received from respective process owners, as specified in the relevant policies and procedures shall be checked, but will not be restricted to.

1.2.9.2 The inputs to the Management Review Meeting shall also comprise of action points from the previous Management review, which include:-

1.2.9.2.1 Changes that could affect ISMS.

1.2.9.2.2 Closure of the audit findings (Corrective actions) along with the planned closure dates.

1.2.9.2.3 Recommendations for improvement if any;

1.2.9.2.4 Minutes / output of the previous Apex Committee Meeting

1.2.9.3 The output of the Management Review Meeting shall include but not limited to:-

1.2.9.3.1 Reconciling the planned closure dates for the completion of corrective actions along with responsibility with the current status of the closure of the audit findings.

1.2.9.3.2 Modifications of policies and procedures to respond to internal and external events impacting ISMS, due to changes in the Business requirement, Technological environment, Legal and regulatory environment, levels of risk and risk acceptance.

1.2.9.4 The second component of this shall comprise of the adherence to practices as laid down in the policies and procedures at an operational level under the Security In-Charge.

1.2.9.5 Interactions/ interviews shall be conducted to check for awareness levels, compliance to the framework, the As a part of this activity, adherence against the selected metrics from the ISMS Policies and Procedures and controls deployed as an outcome of the Risk Treatment Plan. Corresponding records and evidence shall be checked as well.

1.2.9.6 The auditor shall be assisted in the audit process through the Points of Audit, Records to be maintained and Metrics as documented under each Policy of the ISMS, however audit action shall not be restricted to them in totality.

1.2.9.7 Over and above the preceding two points, the information assets in hard/paper format shall be audited for their entire lifecycle management comprising of creation, classification, storage modification, distribution, and disposal.

1.2.9.8 All auditor and auditee conflicts shall be resolved within 15 days from the closure of the audit.

1.2.9.9 Escalation / Interventions, if necessary, shall be taken to the Security In-Charge followed by the Security In-Charge.

1.2.9.10 The verdict of the Apex Committee shall be considered to be final and binding on all the parties concerned.

1.2.9.11 If there is a conflict between the external auditor and the auditee, then the Security In-Charge shall make a representation on behalf of JMBGRP to the Lead Auditor of the external auditing agency. Resolution of the conflict shall be based on the outcome of the appeal received and accepted by JMBGRP.

1.2.9.12 The internal audit report should consist of :-

1.2.9.12.1 Total Findings Raised (from previous audit report) – The total number of findings shall include Non – conformity, Observations, opportunity for Improvement and Noteworthy Effort.

1.2.9.13 The auditor shall classify the findings as follows:-

1.2.9.13.1 Non–Conformity - A systematic failure or significant deficiency - either as a single incident or a combination of a number of similar incidents - in part of the Information Security Management System (ISMS), or the lack of implementation of such a part, governed by applicable ISO27001:2022 standards and/or Information Security Policies of the organization.

1.2.9.13.2 Observation - An isolated or sporadic lapse in the content or implementation of procedures or records which could reasonably lead to a systematic failure or significant deficiency of the Information Security Management System (ISMS) if not corrected.

1.2.9.13.3 Opportunity for improvement - An opportunity for improvement is the suggestion by the auditor for aligning existing practices / process to other industry best practice. An opportunity for improvement may be accepted by the management at their discretion.

1.2.9.13.4 Noteworthy effort - A noteworthy effort is a positive finding. A noteworthy effort can be an improvement compared to the previous audit, or processes that perform better than expected, e.g. best practice

1.2.9.14 The Security In-Charge shall ensure that the arranged in the report number wise in the internal Audit Report file.

1.2.9.15 For all Non – Conformances and observations raised during the audit function head shall perform root cause analysis and prepare CA (Corrective Action).

1.2.9.16 Submission of a consolidated CA shall be responsibility of the ISM and which will be submitted to the Security In-Charge within 25 days from the completion of the audit and acceptance of the observations and non-conformances.

1.2.9.17 Security In-Charge shall take approvals from the Apex Committee for any capex / opex / resources which might be required for adequate closure of the audit findings.

1.2.9.18 The consolidated findings of the Audits shall be reported to the Apex Committee by the Security In-Charge along with the planned steps at an organizational level and Security In-Charge level.

1.2.9.19 The Security In-Charge shall provide a final organization wide CA (Corrective Action) along with their status and planned closure dates to the Apex Committee for discussion and concurrence.

1.2.10 Technical Systems Audit

1.2.10.1 Network Devices and Applications shall be rated based on their criticality to business.

1.2.10.2 It is recommended that any critical device shall be audited twice a year and accordingly, others shall be audited thereafter. However, every year the network devices shall be audited.

1.2.10.3 As regards the critical applications having multiple modules, these shall be audited in keeping with their scale of deployment.

1.2.10.4 The technical systems audit be done for the network infrastructure and supporting utilities. This will comprise of Network Devices (Core Routers, Core Switches, Servers, Web Applications (Internal Facing and External Facing) Firewalls, IDS, IPS, Desktops, and Laptops.

1.2.10.5 The periodicity of web application testing shall be according to Network Security policy and Procedure and System Acquisition, Development and Maintenance Policy and Procedure.

1.2.10.6 Identified critical business applications shall be audited for their access control management.

1.2.10.7 At the time of conducting technical audit (External) the following shall be adhered to:

1.2.10.7.1 A documented process and a plan shall be provided by the auditor to the Auditee clearly stating the duration /nature and methodology which is going to be applied.

1.2.10.7.2 The audit tools as used for conducting technical audit shall have controlled. These shall remain resided on dedicated systems or in the custody of the Head of Audit. The Reports generated by the tools shall be securely archived as per business and or regulatory requirements in case of internal audit. In case of external auditors, they shall provide the details of tools which shall be used for the assessment.

1.2.10.7.3 Tools which are being used currently or those which shall be used for information system audits and the data generated through these tools shall be protected and kept separate from operational environment to prevent any possible misuse or compromise.

1.2.10.7.4 The auditors shall ensure that they preserve the integrity of production data and shall not inadvertently delete or overwrite or modify this data and hence shall ask for 'read only' access.

1.2.10.7.5 Access to systems shall be provided through the prevailing access rights Mechanism with the necessary approvals.

1.2.10.7.6 All access by Auditors shall be logged and monitored as evidence.

1.2.10.7.7 Upon conclusion of the audit, all access rights shall be removed with prior approval from concerned authority.

1.2.10.7.8 The auditor shall also check the CA (Corrective Action)of the previous audit for compliance.

1.2.10.7.9 All points as other mentioned under the Management Review Audit shall remain applicable for the Technical Systems Audit.

1.3 Audit of Third Parties

1.3.1 These shall be conducted once every year for the identified Critical Third Parties .The audit template for conducting these audits is available in the Third-Party Security Policy and Procedure. The third-party audits shall comprise of Information Security Processes in existence and also audit the Technology Systems of the auditee.

1.3.2 As an adjunct methodology the Security In-Charge shall conduct specific surveys to check understanding of the employees on various aspects of information security through Web Based surveys which shall be communicated to the Apex Committee.

1.3.3 Reports from all audits so carried out shall be stored in a secure manner and shall be released on a need-to-know basis.

1.4 Compliance

1.4.1 Identification of Applicable Legislation:

1.4.1.1 Through JMBGRP's Legal department, the Security In-Charge shall be provided with inputs on the applicable legislations, amendments, new rulings, notices in the gazette, promulgation of new laws, by laws, acts which shall have a bearing on JMBGRP's Information Security Posture.

1.4.1.2 The Security In-Charge shall propagate the relevant aspects of applicable legislations to the rest of the information security Organization on a need to know and act basis.

1.4.2 Protection of Intellectual Property Rights:

1.4.2.1 JMBGRP shall always ensure that Information assets; which it has procured, developed, modified; adhere to the legislative, contractual and regulatory requirements, and does not contravene any of the applicable Intellectual Property Rights Laws.

1.4.2.2 JMBGRP shall also protect its information assets when it gets into agreements with third parties through a clear mention of the applicable clauses in the contracts; which shall safeguard JMBGRP's interests in the light of any violation caused by the external party.

1.4.2.3 No unauthorized software, freeware, sharewares shall be used on any of the information systems of JMBGRP.

1.4.3 Protection of Organizational Records:

1.4.3.1 All records as mandated by statutory/legal/regulatory authorities, to whom JMBGRP is responsible for compliance, shall be protected from advertent or inadvertent damage through natural or manmade causes.

1.4.3.2 JMBGRP shall ensure that there is no misappropriation, falsification of records or their confidentiality, integrity and availability is not compromised in any manner during their lifecycle from creation to destruction.

1.4.3.3 The retention limit of statutory records shall be as mandated by the applicable legislation. However, for business records/documents, the Security In-Charge's and or HODs shall determine the retention limit.

1.4.4 Data Protection and Privacy:

1.4.4.1 JMBGRP shall always seek to protect the privacy of the personal information of its customers, employees and third parties with whom JMBGRP has signed an agreement. Divulging of facts shall only be done in keeping with statutory / contractual / regulatory / legal requirements.

1.4.4.2 Privacy protection shall be done with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the privacy, and protect it against risks such as unauthorized access, destruction, use, modification, disclosure or loss throughout the whole of its life cycle.

1.4.5 Prevention of Misuse of Information Assets:

1.4.5.1 All identified information assets of JMBGRP shall be productively used for official purposes only. Any unauthorized use of information assets shall be dealt with a disciplinary action. This shall be done as per the Acceptable Use Policy and Procedure. This shall also cover the distribution and usage of the Digital Signatures and Certificates.

1.4.6 Regulation of Cryptographic Controls:

1.4.6.1 Cryptographic controls when deployed shall adhere to the legal requirements as per applicable legislation in India and that of countries outside India, where JMBGRP maintains operations.

Enforcement

- Any employee found to have violated this procedure shall be subjected to disciplinary action as per JMBGRP Code of Conduct Procedure.
- Management's interpretation of the clauses in this procedure shall be final and binding. Management reserves the rights to alter or amend any clause in this procedure at any time as per its discretion.

Metrics

- The metric shall be measured by the Security In-Charge with support from Process Owners, the metrics to be reported to the Head-IT once in a quarter.
- The metrics to be monitored are as given under:
  - Number of internal audits done per department internally.
  - Number of Non-conformances received during internal audit by various departments.
  - Number of external audits done through an external agency.
  - Number of Non-Conformances received in the audit done by the external agency.
  - Reduction in the number of non-conformances through the implementation of the corrective action plan.
  - Number of Non-Conformances not closed from internal audit.
  - Number of Non-Conformances not closed from external audit.
  - Number of auditee and auditor conflicts in internal audit.
  - Number of repeats Non-Conformances in external and internal audit.
  - Number of non-conformances for the points of audit and metrics as mentioned under each procedure.

Exceptions

- 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 reason existing at any point of time.
- Exceptions to the Information Security Policy and Procedures may have to be allowed at the time of implementation of these policies and procedures or at the time of making any updating to this document or after implementation on an ad hoc basis based on business or a specific and a peculiar manifestation of circumstances which could be of temporary or permanent in nature.
- All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through an Exception Form and sign-off on the same shall be maintained including ad-hoc requests.
- Security In-Charge shall review all exceptions, as the case may be, every year for validity and continuity.

Disclaimer

- JMBGRP reserves all rights and is the exclusive owner of all intellectual property rights over this Backup, Restoration and Media Handling 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 Backup and Restoration 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 Backup and Restoration policy and procedure document shall not be considered as implied in any manner.
- For any clarifications related to this Backup and Restoration policy and procedure document with respect to its interpretation, applicability and implementation, please raise a request in Ticketing Tool.
-

References

- Clause: 4.2.3 – Monitor and Review the ISMS
- Clause 6 – Internal ISMS Audit
- Clause 7 – Management Review of ISMS