Information Security Organization Policy

Document No. - JMBGRP/ISMS/Apex_01
Version_v1.2

Document Details

Classification	Internal	
Released date	28.08.2018	
Description	The policy document to provide the necessary organization to adequately direct, support and guide J.M Baxi Group (JMBGRP) to establish Information Security in line with business/legal/regulatory needs	
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 "13. Reference to ISO 27001:2022"	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: 4,5,10	

Contents

Information Security Organization Policy

1. Objective

The purpose of this policy is to provide the necessary organization to adequately direct, support and guide J.M Baxi Group (JMBGRP) to establish Information Security in line with business/legal/regulatory needs.

2. Scope

This policy is applicable to all corporate offices and all locations of JMBGRP.

3. Policy

3.1 Information security is a business responsibility shared by all employees and third parties of JMBGRP. A management framework shall be established to initiate and control the implementation of information security within the organization.

3.2 An Information Security Organization Structure shall be established comprising of all the identified business groups and senior management personnel of the Organization.

3.3 Roles and Responsibilities shall be clearly defined and communicated to the identified functionaries of the Information Security Organization.

3.4 The management shall ensure that the ISMS (Information Security Management System) policies and procedures are reviewed at planned intervals or if significant changes occur to ensure that policies are suitable to current business environment and are effective and ensure adequacy in the establishment, maintenance and sustenance of Information Security in the organization.

3.5 The management shall ensure that requisite support to be provided in terms of manpower and resource for the execution of ISMS in the Organization. So also there shall be formal process of authorization comprising of the identified groups when new information processing facilities are started.

3.6 The Information Security Organization shall ensure that in pursuant with the requirements of Information Security confidentiality agreements with relevant clauses protecting the interests of the Organization shall be developed.

3.7 Contact with special interest groups (wherever possible) to get updates on industry best practices in process optimization and on mitigation modalities for new threats and vulnerabilities identified and reported by these agencies.

3.8 The policies and procedures so developed as a part of the ISMS along with the controls selected for mitigation of identified risks shall be reviewed independently by the Internal Audit Department of the Organization or through the identified third party with a predefined periodicity or when there is any change to the business environment on account of regulatory changes or otherwise.

3.9 Commissioning of new information processing facilities shall be done only after the approval from the identified members of the Information Security Organization.

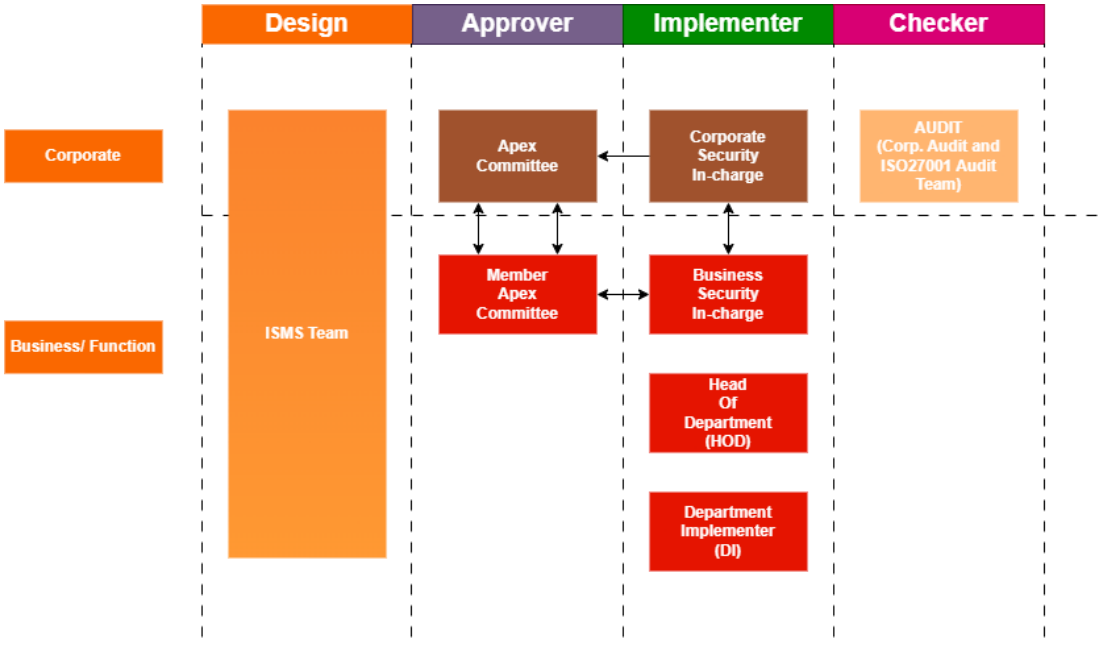
3.10 At all times, no designation in the Information Security Organization of the Organization shall be left unfilled.

3.11 The review of ISMS shall be as per the standard agenda as mentioned in the Framework Document.

3.12 There shall not be any absenteeism during the quarterly review of the ISMS.

4. Procedure

4.1. Every member in the information security organization structure shall discharge the roles allocated to them as per this procedure.



5. Roles and Responsibilities

5.1 Apex Committee [CXO Level Designates]

Composition: The APEX Committee shall include the COO, Corporate Security In-charge, Business Security In-charge, Head HR, and Head-Finance, Admin.

Details of Duties and Responsibilities:

The APEX Committee shall be responsible for the following:

a) Promote Information security through commitment and adequate resources

b) Enterprise Level Ownership of Information Security

c) Approve: Enterprise level information security policies and changes and Initiatives recommended by businesses

d) Review : Major information security incidents and Information security status

e) Allocation of roles & responsibilities of Project Organization

5.2 Chief Information Security Officer

Roles and Responsibilities

The Chief Information Security Officer (SECURITY IN-CHARGE) is having the overall responsibility for implementation and maintenance of ISMS for Organization and shall report to the APEX Committee. SECURITY IN-CHARGE shall be responsible for below mentioned:

a) Custodian of Information Security Management System for Organization.

b) Shall be having ownership implementation of Information security within JMBGRP.

c) Shall coordinate corporate wide information security initiatives.

d) Enhancement of Information Security

5.3 Business Security In-charge

Roles and Responsibilities

a) Shall have ownership of implementation of Information Security at the business level / location level, here at JMBGRP.

b) Provide Positive Assurance Report

c) Support for internal audits

d) Closure of non-conformances

5.4 Department Head

Roles and Responsibilities

a) Shall have ownership of implementation of information security within the department.
b) Shall provide positive assurance.
c) Shall be responsible for closure of audit non-conformances.
d) Representative of Department Head; Implementation of the procedures within the department.

5.5 Department Implementer

Roles and Responsibilities

a) Assist respective HOD in implementation and compliance of information security within the department.
b) Responsible for classifying assets.
c) Responsible for maintenance of records.
d) Provide positive assurance report for information security.
e) Support for Internal Audits.
f) Closure of non-compliance.

6. Enforcement

6.1 This procedure is applicable for all the employees and third parties of the company who have access to and use the information assets and IT assets as listed in the Information Asset List which have been created for all the business groups. Any violation shall be dealt in accordance with the disciplinary action process as laid down in the Code of Conduct Procedure.

6.2 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 it-team discretion.

7. Metrics

The metrics shall be measured by respective department.

The department implementer shall be responsible for measurement of appropriate metrics relevant to their department & security implementation to ensure the effectiveness implemented security controls and for doing an analysis for scope of improvement. Any change in Organization structure shall be reported to APEX committee and Chief Information Security Officer for review.

7.1 The periodicity of reporting shall be once in 90 days.

7.2 Metrics shall be reviewed by HOD of respective department periodically (as decided by respective department) and action plan for improvement of ISMS control shall be made.

7.3 The metrics to be monitored are as given under:

a) Number of changes in the organization structure every six months.

b) Number of unassigned positions as per Org Structure

c) Number of review meetings conducted.

d) Number of points from the MOMs which have not been resolved.

e) Increase / Decrease in Non-Compliances month over month.

8. Exceptions

8.1 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 reason existing at any point of time.

8.2 Exceptions to the Information Security Policy and Procedures may 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.

8.3 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.

8.4 The respective department HOD or Department Implementer shall review all exceptions, as the case may be, every year for validity and continuity.

8.5 JMBGRP shall also list parameters to ensure that before acquiring new applications or other software and hardware, the set of applicable policies and guidelines shall be matched with the available security mechanisms of the product to ensure that the product has the necessary features. If not, then exceptions shall be approved before acquiring the desired product. Similarly, while developing new applications, the necessary security policies and guidelines have to be incorporated in the application or exceptions shall be obtained for the same from the Information Security Team.

9. Violations & Disciplinary Action

9.1 Any employee or third party found to have violated this policy and procedure shall be subjected to disciplinary action as per the Code of Conduct of the JMBGRP.

9.2 JMBGRP Management interpretation of the clauses in this policy and procedure shall be final and binding on all the stakeholders. Management reserves the rights to alter or amend any

clause in this procedure at any time as per it-team discretion.

10. Disclaimer

10.1 JMBGRP reserves all rights and is the exclusive owner of all intellectual property rights over this information security policy and procedure document. This information security policy and procedure 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, , Memory Cards, CDS, DVD's) or any other media, and/or captured or transmitted through by any means (electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior written consent from the Information Security Team of JMBGRP. The information security 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 information security policy and procedure document shall not be considered as implied in any manner.

10.2 For any clarifications related to this information security policy and procedure document with respect to it-team interpretation, applicability and implementation, please raise a request in Ticketing Tool.

11. Reference to ISO 27001:2022

Clause 5, Control Objective: A.6.1