Information Security Management System Framework

Document No. - JMBGRP/ISMS/Apex_02

Version_v1.2

Document Details

Classification	Internal	
Released date	28.08.2018	
Description	This document explains the steps and describes how J.M. BAXI GROUP (JMBGRP) has fulfilled the requirements of Information Security Management System	
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 " 19. References to ISO 27001:2022"	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Reviewed & no changes	

Contents

Information Security Management System: Framework

1 Introduction

1.1 This document explains the steps and describes how J.M. BAXI GROUP (JMBGRP) has fulfilled the requirements of Information Security Management System as listed in ISO/IEC 27001:2013 Standard.

2 Responsibilities

2.1 This document shall refer to Information Security Policies and wherever required any other JMBGRP organizational document.

3 Context of the JMBGRP

3.1 J.M Baxi Group (hereinafter referred to as JMBGRP) to provide support services mainly to Shipping logistics.

3.2 The ISMS coordinates Information Security Policies, Procedures, and other relevant documents. It provides for transparency, efficiency, management, and control of JMBGRP's long-term security requirements. The ISMS provides the roadmap to achieve and maintain the required security level to protect JMBGRP's information resources.

3.3 JMBGRP understands the sensitivity of its business and wish to ensure compliance to all legal and regulatory requirements in addition to meet its organization mission related with information security. Following are the basic issues for JMBGRP Information Security Management System framework.

External Issue

The Identified External Issues are as follows:

4.1 Legal and Regulatory Compliance

4.2 Cross Border Data Transfer

4.3 Contractual Obligations & Consumer Satisfaction

4.4 Market Competition

4.5 Technology Changes

4.6 Issues of Cultural, Religious, Ethnic Group

4.7 IPR Issues

4.8 Privacy Issues

4.9 Piracy Issues

4.10 Vendors & Special Interest Groups

5 Internal Issue

The Identified Internal Issues are as follows:

5.1 Employees Information

5.2 Local Culture

5.3 Protection of Idea/IPR

5.4 Frequent change in employment

5.5 Change in Technical Environment

5.6 Security Vs. Ease of Business

6 Understanding the Need and Expectation of Interested Parties

6.1 JMBGRP business is supported by Information Security infrastructure and IT is an enabler for achieving the intended organizations Information Security objectives. Following are identified as the interested parties which are relevant for JMBGRP Information Security Management system

6.1 a) Relevant Interested Parties	6.1 b)Requirements of these parties
Senior Management	Assurance that all Information Security Risks are identified and mitigated to accepted Risk level
Customers	JMBGRP systems are up and running, secure their information
Regulators: Ministry of Information and Technology	Information gathering, sharing with different parties and confidentiality to be managed under the controls of IT ministry guidelines
Regulators: Indian Computer Emergency Response Team	Meet Cyber Security Reporting and update requirements.
Employees	JMBGRP protects all relevant information of its employees , provide good working culture with less stringent security features
Suppliers	JMBGRP protect and enforce the information Security with its suppliers' information and IPR
Special Groups	JMBGRP meets and mitigate their information security concerns

7 Scope of ISMS

7.1 With Reference to point 4 and 6 above JMBGRP include following in the scope of ISMS the purpose of ISO/IEC 27001:2013;

Physical Scope of ISMS

a) All JMBGRP companies' locations are functioning under the umbrella of JMBGRP information security management systems irrespective of the business segment they operate.

Logical and Information scope of the ISMS shall include

a) All information stored on Servers (in premises or cloud) and Systems available on these sites, irrespective of the origin, destination or association of this information.

b) All logical access to this information irrespective of the origin, termination or association of these accesses.

c) All network infrastructure available at these locations irrespective of what information they are carrying.

d) All users of these locations having access to information and information processing and Security facilities, Infrastructure and supporting utilities who include along with employees, any contractors, third parties, Supplier, visitor and any other human being in any capacity.

8 Information Security Management System

8.1 JMBGRP's information, information systems and data contents are fundamental for its daily operations and effective service provision. Hence, JMBGRP shall design and implement adequate security policies, procedures and controls to protect confidentiality maintain integrity and ensure availability of all information stored, processed and transmitted through its information systems.

8.2 Given the critical and competitive nature of the business for JMBGRP, protection of its information assets should be commensurate with its business value and risk.

8.3 The Information Security Framework of JMBGRP through the elements as explained herewith seeks to express the intent of JMBGRP and the required action it shall need to take, in order to effectively establish, maintain and sustain the Information Security paradigm in the Organization.

8.4 The purpose of this framework is also to ensure that due care is exercised in protecting the computing systems and related information assets of JMBGRP. "Due care" is defined as the cost-effective protection of information at a level appropriate to its value.

8.5 Information, regardless of its source and nature, is a valuable asset for JMBGRP. Its accuracy, availability, confidentiality, authenticity, integrity and reliability are essential to business to allow both, confidence in customers and the decisions, which are based upon it, and to engender good relationship with business associates and company representatives.

8.6 JMBGRP shall ensure that Information Assets; which includes, computing systems, network infrastructure equipment, software, applications, databases, and services offered by the Organization through its network infrastructure comprising of NTUs (Network Terminating Units), routers, switches, hubs, assets in paper and other media which are utilized by the Organization employees while discharging their duties, is protected from inappropriate access, disclosure, modification, or damage, thereby ensuring that Confidentiality, Integrity, Availability is maintained and sustained.

8.7 Also safeguarding supporting utilities like electrical supply, air-conditioning, (UPS) Uninterrupted Power Supply Systems, fire safety systems, cabling in premises, shall also called as Information asset as they contribute in maintaining the continuity of business operations

and maintaining the creation /transmission /storage /usage /processing /sharing /destruction of information within JMBGRP and its business associates and customers.

9 Terms and Definitions

9.1 Terms

The table below contains definitions of the terms used in this document:

Term	Definition
Availability	Ensuring that authorized users have access to information and associated assets wherever required.
Integrity	Ensuring that data is protected from accidental corruption or deliberate tampering.
Confidentiality	Ensuring that information is accessible only to those authorized to have access
Information Security Incident	An information security incident is indication by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Scope	A definition of exactly where the boundaries for the implementation of the controls for the purpose of. ISO27001:2013 implementation.
Security Coordinator	The department or team representative who is also the owner of the assets belonging to the department.
Business Information Security Officer	BISO is responsible for monitoring and driving compliance with the ISMS.
Control	In this International standard, the term ‘control’ is used as a synonym for ‘measure’ for protection.
Asset	Anything that has value to the organization
SOA	Documented statement describing the controls objectives and controls that are relevant and applicable to the organization’s ISMS.
Owner	The term ‘owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance use and security of the assets. The term ‘owner’ does not mean that the person actually has any property rights to the asset.

9.2 Abbreviations

The table below contains definitions of the abbreviations used in this document:

Abbreviation	Expansion
CISO	Chief Information Security Manager

BISO	Business Information Security Officer
ISC	Information Security Apex Committee
ISMS	Information Security Management System
RA	Risk Assessment
RT	Risk Treatment
SOA	Statement of Applicability
ISO	International Standard Organisation
IEC	International Electro-Technical Commission
PDCA	Plan-Do-Check-Act

10 Leadership

10.1 The Information Security Committee oversees JMBGRP ISMS. The management body is responsible for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the ISMS.

10.2 CISO is responsible for directing, coordinating, planning and organizing all information security of ISMS.

10.3 ISMS auditor is responsible for conducting internal audit of ISMS.

11 Leadership and Commitment

The commitment of Information Security Committee is documented in order to:

11.1 Establish and align to the Information Security Policy.

11.2 Ensure that Information Security objectives and plans are established.

11.3 Establish appropriate roles and responsibilities for Information Security from time to time.

11.4 Communicate to the organization the importance of meeting Information Security objectives and conform to the Information Security policy, its responsibilities under the law and the need for continual improvement.

11.5 Provide sufficient resources to develop, implement, operate and maintain the ISMS.

11.6 Decide the criteria for accepting risks and the acceptable level of risk.

11.7 Ensure that the internal ISMS audits are conducted.

11.8 Conduct management reviews of the ISMS

12 Policies

Following set of Policies has been approved by Information Security Committee to make sure that it is appropriate, includes framework for setting ISMS objectives, shows management commitment to satisfy applicable requirements and ensures continual improvement.

12.1 JMBGRP ISMS Framework
12.2 JMBGRP ISMS Organization Policy and Procedure
12.3 JMBGRP ISMS Risk Management Methodology
12.4 JMBGRP ISMS Sustenance Policy & Procedure

13 Organizational Roles, Responsibilities and Authorities

13.1 JMBGRP has defined roles and described the responsibilities and authorities in JMBGRP Information Security Organizational Policy. Performance reported to the top management in form of matrix and reports described in "JMBGRP ISMS Organization Policy and Procedure."

14 Planning

14.1 Addressing Risk and Opportunities:

General Requirements

a) JMBGRP have planned its Information Security Management System & ensures that each information security project achieve its intended outcome, prevent or reduce any undesired effects and support the achievement of overall continual improvement. JMBGRP ISMS Framework documents the planning aspect of Information Security Program.

Information Security Risk Assessment

a) JMBGRP have adopted a comprehensive Risk assessment methodology. The methodology is asset-based methodology and comply the requirements of ISO 27001 and ISO 31000 risk management standards. The process of Risk Assessment documented as 'JMBGRP ISMS Risk Management Methodology'. The result documented in Risk Assessment as part of overall Risk Assessment and Treatment Sheet. JMBGRP also ensures that, Risk is owned by the Risk owner or Asset Owner himself as any risk to asset will affect the asset owner.

Information Security Risk Treatment

a) JMBGRP compare the results of Information Security Risk obtained as a result of Risk Assessment exercise and decide if it has to be treated or acted upon as an opportunity. The Process of Risk treatment documented in JMBGRP ISMS Risk Management Methodology and the result of risk treatment has documented in Risk Assessment and Treatment Sheet. The controls required to mitigate risks are documented and presented for approval to management. Once approved, action plans are charted for

their implementation. A Statement of Applicability with reference to ISO/IEC 27001:2013 - list of controls is prepared to check if any relevant controls are missed.

14.2 Information Security Objective and Planning for their achievement

a) JMBGRP ensures SMART (Specific, Measurable, Achievable, Realistic and Time-bound) objectives are drawn for Information Security. Objectives are reviewed and changed when required. JMBGRP also ensure that, plan to achieve this objective shall identify Action, Resources, Responsibility, Timelines and Metrics for measurement.

15 Support

15.1 Resources

a) JMBGRP ensures that the 'relevant resources' are available.

15.2 Competency

a) JMBGRP ensures that resources required shall have relevant competency. A competency matrix shall be prepared for the roles required for JMBGRP ISMS Organization Policy and Procedure.
b) JMBGRP declare that competency matrix shall be drawn for JMBGRP Information Security committee. In the organizational member if any designation has been included, the competency requirement crafted by HR and the manager shall be considered as sufficient. The competency for operation processes shall be defined and documented by respective managers in consultation with HR/SMEs.

15.3 Awareness

a) JMBGRP ensures that all personnel in JMBGRP including Employees, Contractors, Suppliers, Third Parties and Visitors are aware about the JMBGRP ISMS Policies and Procedures, Acceptable Usage for their roles and responsibilities. Various modes of awareness including classroom sessions, online training modules and other communications like E mailers, Wall Papers, and Posters may be used to achieve the objective of security awareness.

15.4 Communication

a) JMBGRP shall have a communication plan, which shall include what to communicate, when to communicate, with whom to communicate, who communicate and what shall be the mode of communication.

16 Documented Information

a. General

i. JMBGRP shall identify all documented information for ISO/IEC 27001:2013 standard and any other legal or contractual requirements for the effectiveness of ISMS.

b. Control of Documented information

i. JMBGRP shall ensure that documented information is available to authorized persons when required, is adequately protected from loss of Confidentiality, Integrity and Availability. This shall be achieved by putting controls on Distribution, Access, Retrieval, Use, Storage and Preservation, Changes, Retention and Disposition.

ii. All Documents shall be latest and relevant and unwanted copies shall be taken out from circulation and archived.

iii. Records shall be maintained as per regulatory or business requirements.

17 Operation

a. Operation Planning and control

i. Please refer to set of JMBGRP ISMS Information Security Policies and Procedures, Support Policies and Procedures and IT Policies and Procedures.

b. Information Security Risk Assessment

i. JMBGRP-ISMS follow an asset-based risk assessment approach. The IT department maintains its own inventory of assets as part of their documentations.

ii. Please refer to Information Security Risk Management Methodology and Risk Assessment & Treatment Sheet.

c. Information Security Risk Treatment

i. A risk treatment plan is created based on the outcome of the risk assessment carried out in the organization and is documented as part of the Risk Assessment Sheet available in the repository.

ii. Please refer to Information Security Risk Management Methodology and Risk Assessment & Treatment Sheet.

d. Performance Evaluations

i. JMBGRP has developed a matrix to ensure the effectiveness of applied controls and overall effectiveness of ISMS. The Matrix shall consist of parameters to be

measured, method and units for monitoring, measurements, analysis and evaluation, frequency, responsibility and reporting of matrix.

ii. JMBGRP ensures ISMS performance shall be evaluated on defined intervals and on management directives through developed metrics.

e. Monitoring, measurement, analysis and evaluation

i. All security incidents need to be reported and acted upon as required by Security Incident Response Procedure.

ii. Monthly reports with key security metrics that project the security posture of the organization are provided to the management.

iii. The Information Security Committee shall convene every year to review the status of the implementation of the JMBGRP-ISMS.

iv. ISWG Shall meet at least every quarter for ISMS Discussions.

v. The improvements and new measures implemented will be adequately communicated to the appropriate personnel.

vi. The security policies, procedures and standards will be updated based on the requirements immediately or in phased manner based on case to case.

vii. The identified improvements in the ISMS will be implemented by the organization. In cases where the timelines can't be met, an exception will be raised, and justifications will be provided and documented.

f. Internal Audits

i. JMBGRP shall ensure that internal audits are conducted at regular intervals and should conform to ISO/IEC 27001:2013 standard and other identified and defined organizational requirements.

ii. JMBGRP shall ensure that Audit criteria and scope are well defined, Auditors competency is matched, results of audits are reported to management and documented information relevant to audit process is maintained. (Refer to JMBGRP ISMS Sustenance Policy & Procedure)

g. Management Reviews

i. JMBGRP shall ensure that management review happens half yearly at ISC level. The ISO/IEC 27001:2013 Information Security committee shall review to ensure its continuing suitability, adequacy and effectiveness.

ii. The management review shall include:

1. Action form previous reviews
2. Changes in external and internal issues
3. Feedback from nonconformities and corrective actions
4. Input from monitoring and measurement results
5. Inputs from internal and external audits
6. Inputs from Information Security Objective fulfillments
7. Feedback from interested parties.
8. Results of risk assessment and risk treatment
9. Opportunities for continuous improvement

h. Management review output shall include decisions on improvements and changes.

i. The review proceedings shall be documented in form of minutes and circulated to all attendees.

18 ISMS Improvement

18.1 Nonconformity and corrective actions

i. To ensure that continual improvement takes place, Internal Audits are conducted periodically, an Incident response procedure is in place to ensure that the effectiveness of the JMBGRP-ISMS is continually evaluated. Vulnerability scans are conducted periodically, and vulnerabilities are reported to the appropriate personnel.

ii. The JMBGRP Information Security Committee reviews on a regular basis, the security assessments and recommendations from the audit teams. ISM will highlight the key findings of vulnerability assessments. Specifically, the following roles and responsibilities are central to the assessment of corrective actions.

18.2 Continual Improvement

iii. JMBGRP shall continually improve the suitability, adequacy and effectiveness of the information security management system.

19 Reference

ISO 27001: 2022 Clause 4 to Clause 10