# Information Security Management System
## Training Policy & Procedure

Document no. JMBGRP/ISMS/Pol-TR

Version no. v1.2

**Document details**

| | | |
|---|---|---|
| **Classification** | Internal | |
| **Released date** | 28.08.2018 | |
| **Description** | The purpose of this policy to ensure information security needs to be imbibed in the organization's culture for successful implementation, sustenance, and continual improvement of the information security best practices. | |
| **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 " Reference" | |
| v1.3 | 16.10.2024 | Manish Jaiswal (Group CTO) | Modifications done in Section: "Scope, Policy Statement, Procedure, Responsibilities" | |

# Contents

## Purpose

JMBGRP recognizes that information security needs to be imbibed in the organization's culture for successful implementation, sustenance, and continual improvement of the information security best practices. This policy seeks to achieve this purpose.

## Scope

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

## Policy Statement

- All employees of JMBGRP, contractors and third-party users shall be imparted appropriate information security awareness training and shall be regularly updated with the organizational information security policies and procedures relevant for their job function.
- Information security training shall be imparted at the time of induction to all new employees and also on periodic basis, which shall be at least once in a year.
- The training content shall be updated taking into consideration the information security incidents, the changes in the business, contractual, legal or regulatory requirements. The identified group/HR/ Training Department/Corporate Communications which is responsible for coordination and implementation of Information Security shall be responsible for updation and creation of the training content.
- Evaluation of the employees shall be done on a periodic basis (once a year) through quizzes/training sessions conducted on line or offline by the identified group/HR/ Training Department/Corporate Communications.
- The records thereof shall be maintained by the HR/ Training Department for the number of trainings conducted, average attendance, number of users (employees) who have attended/not attended the sessions and training score obtained by each individual.

## Procedure

1.1 **Training Audience:**

The training audience for Information security training shall be identified under the following four categories:

1.1.1 **Users of Information Assets:** This category includes all employees and third parties who have access to JMBGRP's information, computing facilities and network. Wherever relevant and required, employees & third-party personnel who have access to the information assets of JMBGRP shall undergo training/briefing in information security as mentioned in the JMBGRP's policies and procedures with emphasis on Code of Conduct and Acceptable Usage of Assets.

1.1.2 **Business/Department Heads:** The personnel in this category shall be trained on:

1121 Information security Do's and Don'ts for users of information assets in the daily work routine.

1122 Management of information security i.e. ensuring compliance with information security policies, procedures and guidelines.

1123 Emphasis on Information Asset Classification, Risk Assessment, and Incident Reporting.

1.1.3 **Support Teams:** This category includes the IT department. The personnel under this category shall be trained with special emphasis on:

1131 Information security as a user of information assets in the daily work routine.

1132 Monitoring of IT systems and network for possible security threats.

1133 The security configurations for information systems with reference to threats and vulnerabilities.

1134 New threats and vulnerabilities for information systems.

1135 Incident response handling for IT incidents (Refer to Incident Management Procedure).

1136 Investigating the exceptional, abnormal incidents.

1137 Damage containment/control mechanisms.

1138 Business Continuity Planning & Management.

1139 Any other special training need because of changes in network, applications etc. apart from Information Security Policies and Procedures of JMBGRP.

1.1.4 **Administration Department:** The personnel under this category shall be trained on:

1141 Maintaining the physical security posture at the desired level.

1142 Incident response handling for Non-IT incidents.

1143 Ensuring compliance to the standard operating procedures on waste disposal, visitor management, snail mail, firefighting, access card and physical security.

1.1.5 Third Parties : The personnel under this category shall be trained on:

1151 Code of Conduct.

1152 Acceptable Usage of Information Assets.

1153 Any special information security requirement as per the engagement.

1.2 **Timing and Periodicity:**

1.2.1 Information security training shall be carried out for new employees as a part of the induction training program. It is the responsibility of the concerned HOD to ensure that this happens in coordination with the HR/ Training Department.

1.2.2 HR/ Training Department shall prepare an information security training calendar and organize information security training sessions in coordination with the IT Team.

1.2.3 Every employee shall undergo information security training at least once a year. This can be done through conventional training session wherever possible or through other means like loading of training sessions on the Intranet or visual reiteration tools.

1.2.4 All employees and third-party personnel working in JMBGRP shall be made aware of the procedure for reporting security incidents (IT and Non-IT).

1.2.5 Visual reiteration tools on Information Security like posters, wallpapers, screen-savers, flash-films, and periodic newsletters shall be deployed to imprint the Information security do's and don'ts on the minds of all employees.

1.3 **Contents of Information Security Training:**

The information security training shall include:

1.3.1 **Why is information security needed?**

1311 Definition of information assets;

1312 Explanation regarding the impact of loss/theft/damage of information asset.

1313 Implications of non-compliance with the information security policies and Procedures.

1.3.2 **How is information security implemented?**

1321 Framework of the Information Security Management System (ISMS) within JMBGRP.

1322 The information security policies, procedures and guidelines adopted by JMBGRP.

1.3.3 **How to access information security policies and procedures?**

1331 The location where the employees would be able to access the information security.

1332 Where and how the employees can obtain additional information.

1.3.4 **Employee Responsibilities:**

1341 The responsibilities of the employees in protecting the information assets as listed in the employee code of conduct.

1342 The disciplinary actions which can be taken against the employee in case of violations to the ISMS framework.

1.3.5 **Learning from Incidents:**

1351 To share experiences and learning from various IT and Non-IT incidents.

1352 The information security training content shall be regularly updated by the IS Team based on the learning from information security incidents, new risks to information security, changes to the business, contractual, legal and regulatory requirements, changes to organization structure, technology etc.

1.4 **Methodology and Tools:**

Some of the ways in which training shall be provided are:

1.4.1 **Instructional workshops:**

1411 Training in the form of instructional workshops shall be provided to all groups of users on a periodic basis as mentioned above, which shall be organized by the HR/ training department in coordination with the Security In-charge as per business need or during induction of new employees.

1.4.2 **Intranet:**

1421 The information security policies, procedures and guidelines shall be made available on the HRMS for easy accessibility and reference. Facilities like “key word” search etc. are recommended. Regular updates shall be made available on the intranet.

1.4.3 **Visual Reiteration Tools:**

1431 In order to reinforce the need for InfoSec discipline, subtle but effective visual reiteration tools shall be employed. These shall include:

1.4.3.1.1 Posters

1.4.3.1.2 Wallpapers

1.4.3.1.3 Screensavers

1.4.3.1.4 Handbooks

1.4.4 **Mailers:**

1441 Periodic e-mailers (InfoSec newsletters) shall be sent by the IS Team highlighting the need and importance of information security. The period is recommended to be monthly.

1442 In addition to the above, audiovisual films on Information Security are recommended to be shown to employees at regular intervals. This shall be organized by the IS Team.

1.4.5 **Measuring Training Effectiveness:**

1451 Surveys shall be conducted by the IT Team on periodic basis to check the awareness amongst the users about information security and the effectiveness of the various tools used for imparting training.

1452 Quizzes shall be administered by the IT Team for this purpose along with other survey tools.

1453 Periodic audits shall also provide inputs in terms of the user awareness levels.

## Responsibilities

The responsibility lies with the following personnel:

- HR/ Training department:
  - Establish the training calendar.
  - Create & update the training content.
  - Organize/Impart the training in coordination with the IS Team.
  - Conduct Surveys on effectiveness of the training.
  - Maintain the records of attendance of the training.
  - Reiterate the awareness through alternate means in an ongoing manner.
- HOD:
  - To ensure that the team members are made available for training as per schedule promulgated by HR/ Training department.
- IT Team:
  - To periodically audit the records and the effectiveness of the training, and coordinate with the HR/ Training department for preparation and delivery of training content. Report to be provided for Information Security Organization.

## Enforcement:

- This policy and procedure is applicable for all the employees 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 in accordance with the disciplinary action process as laid down in the Code of Conduct.
- 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 document at any time as

per its discretion.

## Metrics

- The metrics shall be measured on a quarterly basis and reported. The points include as given below, but not restricted to.
    - No of trainings conducted for various user departments.
    - No of new joiners who have gone through the induction vis-à-vis the no of employees who have joined in the particular month.
    - No of employees who have completed the annual refresher trainings along with % passed.
    - Average score of employees in the information security trainings.
    - Logs of the Intranet site to monitor how many employees have accessed policies/ content.
    - Data indicating reduction in business risk, if any specific campaigns were undertaken for the purpose
    - Indications from audits on awareness levels of employees before and after trainings.

## 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 this Security Policy and Procedures shall be allowed at the time of implementation of this policy and procedures or at the time of making any updation to this document or after implementation on an ad-hoc basis as per business or a specific and a peculiar manifestation of circumstances which shall be of temporary or permanent in nature.
- All exception requests shall be submitted by respective HODs/ Security In-charges. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester.
- The 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 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.
- For any clarifications related to this Acceptable usage policy and procedure document with respect to its interpretation, applicability and implementation, please raise a request in Ticketing Tool.

## References:

- Controls: A.5.9, A.5.10, A.7.10,