Information Security Management System

Data Retention/ Storage & Disposal of Media, Records Policy

Document No. – JMBGRP/ISMS/Pol-DRSDM

Version_v1.1

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The information availability, its storage and safe disposing mechanism	
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	
v1.0	25.03.2022	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.1	18.08.2023	Manish Jaiswal (Group CTO)	Document reviewed. Modification done to "15.Reference to ISO 27001:2022"	
v1.2	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: "Content, Policy"	

Contents

1. Purpose

Organizational data is information that supports the mission of J M Baxi Group (JMBGRP). It is a vital asset and is owned by the Organization. Organizational data is considered essential, and its quality and security must be ensured to comply with legal, regulatory, and administrative requirements. Authorization to access organizational data varies according to its sensitivity (the need for care or caution in handling). This administrative policy sets forth the organization's standards with regards to the handling of confidential organizational data.

2. Scope

To establish policy for the safeguarding of restricted and confidential data relating to customer, client and JMBGRP IT personnel that is created, received, maintained or transmitted by the Organization. This policy is intended to ensure that the information is uniformly used and disclosed only in accordance with all organization policies and applicable laws and standards. A combination of physical security, personnel security, and system security mechanisms are used to achieve this standard.

3. Policy

Data Collection

3.1 Users should collect only the minimum necessary organizational/confidential information required to perform organization business.

3.2 Department heads must ensure that all decisions regarding the collection and use of organizational data are in compliance with the law and with organization policy and procedure.

Data Access

3.3 Only authorized users may access, or attempt to access, confidential information.

3.4 Authorization for access to confidential data comes from the department head and is typically made in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other official authority.

3.5 Where access to confidential data has been authorized, use of such data shall be limited to the purpose required to perform organization business.

3.6 Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

3.7 Notification of a user's termination or removal of authorized access to confidential information must be conveyed immediately in written or verbally to the JMBGRP IT department.

Data Handling and Data Transfer

3.8 Restricted & confidential information must not be transferred by any method to persons who are not authorized to access that information. Users must ensure that adequate security measures are in place at each destination when restricted & confidential data is transferred from one location to another.

3.9 Restricted & confidential data must be protected from unintended access by unauthorized users. Users must not leave restricted & confidential information unattended and accessible.

3.10 Restricted & confidential information must not be taken off-premises unless the user is authorized to do so. Restricted & Secret data should not be transmitted through electronic messaging even to other authorized users unless security methods are employed.

3.11 Physical protection from theft, loss, or damage must be utilized for mobile devices that can be easily moved such as a PDA, thumb drive or laptop.

Storage of Confidential Data

3.12 Physical protection must be employed for all devices storing confidential data. This shall include physical access controls that limit physical access and viewing, if open to public view. When not directly in use, office, lab, and suite doors must be locked and any easily transportable devices should be secured in locked cabinets or drawers.

3.13 Users of laptop and other mobile computing devices need to be particularly vigilant and take appropriate steps to ensure the physical security of mobile devices at all times, but particularly when traveling or working away from the Organization.

3.14 IT Managed servers; storing confidential information shall be regularly scanned for vulnerabilities, patched, and backed-up.

3.15 Systems (hardware and software) designed to store and transfer confidential records require enhanced security protections and must be closely monitored.

3.16 It is strongly recommended that important organizational data to be backed up on servers or other systems in offices or laboratories. Organizational data (including word documents, spreadsheets and Access databases) that is created on a PC or similar system should also be stored on a network drive hosted on an IT managed server.

3.17 Electronic media storing restricted/confidential data must be protected by password security. To the extent possible, these devices must employ encryption methods.

Data Retention and Disposal of Media, Records

Archiving

3.18 Organizational records, including confidential information records, which are not being used for active organization business, may be archived until retention requirements have been met.

3.19 Departments determine the criteria for inactive record status in their areas, based on need for the records and available storage space and public records law.

3.20 Storage areas for inactive records must be physically secure and environmentally controlled, to protect the records from unauthorized access and damage or loss from temperature fluctuations, fire, water damage, pests, and other hazards.

Record Disposal

3.21 The proper destruction of records is essential to creating a credible records management program. Records containing restricted/confidential data shall only be destroyed in the ordinary course of business; no records that are currently involved in, or have open investigations, audits, or litigation pending shall be destroyed or otherwise discarded.

3.22 No primary records of any type belonging to JMBGRP may be destroyed until they have met retention requirements established by JMBGRP policies and public records law.

3.23 When retention requirements have been met, records must be either immediately destroyed or placed in secure locations as described in this section for controlled destruction later.

3.24 The authorized methods of destruction for non-electronic records are burning where authorized or shredding.

3.25 Organizational data are in compliance with the law and with organization policy and procedure.

4. Point of Contact

'Security In-charge', JMBGRP.

5. Execution Responsibility

JMBGRP IT shall have execution responsibility of this policy.

6. Supervisory Personnel

JMBGRP IT employee who has supervisory responsibilities and whose job responsibilities include the maintenance of or use of confidential data is responsible for implementing and ensuring compliance with this policy and initiating corrective action if needed. In implementing this policy, each supervisor is responsible for the following:

5.1 Communicating this policy to personnel under their supervision.

5.2 Ensuring that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect organizational data.

5.3 Providing education and training in data management principles to employees under their supervision.

7. User Responsibilities

Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. All data users are expected to:

6.1 Access organizational/confidential data only in their conduct of organization business.

6.2 Request only the minimum necessary confidential/confidential information necessary to perform organization business.

6.3 Respect the confidentiality and privacy of individuals whose records they may access.

6.4 Observe any ethical restrictions that apply to data to which they have access.

6.5 Know and abide by applicable laws or policies with respect to access, use, or disclosure of information.

8. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9. Violations & Disciplinary Action

Compliance with this data protection policy is the responsibility of all JMBGRP Users. Users suspected of violating these policies may be temporarily denied access to JMBGRP's information technology resources during investigation of an alleged abuse. Violations can also be subject to prosecution by state authorities.

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 floppy diskettes, hard disks, USB Drives, Pen Drives, Memory Cards, CD's, DVD's), 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 are 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 document with respect to its interpretation, applicability and implementation, please raise a request to Ticketing Tool.

11. Metrics

11.1 The metrics shall be measured by the 'Business Information Security Officer'.

11.2 The periodicity of reporting shall be quarterly.

11.2.1 Following are the metrics to be measured:

11.2.1.1 Number of incidences of unauthorized access of information.

11.2.1.2 Data loss or theft incidences recorded.

11.2.1.3 Number of disposal of media recorded.

12. Exceptions

No exceptions.

13. Reference to ISO 27001:2022

Control Objectives:A.7.10