Information Security Management System
Access Control Policy & Procedure

Document no. JMBGRP/ISMS/Pol-AC

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The document showcases the policy to prevent organization's resources from unauthorized access while facilitating seamless and legitimate use of these resources	
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 "13. Reference to ISO 27001:2022"	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: "Procedure, Responsibilities, Metrics, Exceptions"	

Contents

Purpose

To protect an organization's resources from unauthorized access while facilitating seamless and legitimate use of these resources.

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.

Policy Statement

General Principles

- Systems may require more or less stringent controls than the stated standard, based on a Risk Assessment.
- Where access controls are different to this standard the reason for the differences must be documented.
- For each application or module, the business should nominate a System Owner who should undertake a risk assessment, specify access requirements, and monitor their overall implementation.
- Applications will be accessed via mechanisms that conform to Group standards and are consistent with the risk assessment.
- All access permissions will be granted in accordance with an approved process.
- Access to financial and sensitive data as identified in the Information Classification and Handling Policy should follow the principle of 'segregation of duties.
- The System Owner will conduct, at least annually, reviews of access permissions.
- Access to data has to be compliant with relevant legislation (including privacy laws).
- Security of data transferred from one system to another is the responsibility of the receiving System Owner.

Procedure

User Provisioning

All user IDs will be created, amended, and deleted in accordance with this procedure. This requires:

- Access requests will normally be raised by the user the user's manager and authorized by the System Owner.

- The IT Team making the change to access should be independent of the System Owner who authorizes the change – it is not acceptable for the same person to authorize the change and make the change on the system.
- System Owner should only change permissions with an authorized request. They should always ascertain the reason for the access request and details of any previous user IDs and permissions, so that these can be deleted at the same time as new ones are given.
- People who leave the organization and those who moved departments must be notified promptly to the System Owner by the HR Department so that access rights can be revoked at the appropriate time.
- Deletion of files for redundant user IDs - prior to a user leaving a department the manager must review the files owned by the user and arrange for them to be either deleted or transferred to new ownership, so that essential information is not lost.
- Redundant user IDs should not be reused. This is so that audited transactions can be traced back to a single individual.
- Whenever a new user ID is issued, the user should be given a statement that outlines the scope of the user's access authority and reminds them of their responsibilities as in the Acceptable Use Policy. Optionally, businesses may require users to acknowledge receipt and provide a declaration that they will be responsible for all transactions carried out in the system with the user ID and that the password will not be shared.
- A list of all the access rights assigned to a user must be maintained, so that in the event of the user leaving the company all the access rights can be removed efficiently.
- Access for external parties should be granted on a request, duly authorized by business, and assessed by System Owner. For major contracts, the external party should give an undertaking that it will indemnify J M Baxi Group (JMBGRP) for any loss/damage incurred as a consequence of misuse of the access granted to them.

Privilege management

The allocation and use of privileges should be restricted and controlled. This means:

- The use of privileges (e.g., system administrator) shall be granted only upon the authorization of the System Owner.
- The use of privileges for changes to business master data (such as parameters) shall only be granted to a restricted number of individuals.
- Appropriate emergency access accounts will be provided to enable support staff to apply emergency fixes. The use of these accounts will be logged, reviewed and emergency permissions revoked after use.

Reviewing Access Permissions

- System Owners should review at least quarterly all user IDs not used for more than 90 days (30 days for critical systems) to ensure that they are still appropriate.
- System Owners should review annually the permissions given to each access group that can access their data. For sensitive data this review may need to be performed more frequently.
- IT Team should review at least annually the membership of privileged access groups, such as System Administrator accounts in operating systems and databases.

User Password Management

- All user-level and system-level passwords must conform to the guidelines described below
- Passwords are used for various purposes at JMBGRP. Some of the more common uses include system user level accounts, web accounts, email accounts, screen saver protection, voicemail password, server, and local router logins.
- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed once a quarter.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed once a month.
- Passwords must not be inserted into email messages or other forms of electronic communication, hence should be communicated through other sources after ensuring proper identification.

Monitoring Security

Systems should be monitored for security incidents. Wherever technically possible, significant systems should incorporate real time alerts that notify the System Owner when there is a high volume of failed access attempts.

For logged information to be consistent and meaningful, all the servers and networking devices shall have their system clocks synchronized either manually by the system administrator or an automated process using a NTP server as reference.

Responsibilities

Data Owner - takes responsibility for the ownership of data and software on behalf of the business also known as Data Owners. For some applications the data and software will be entirely owned by a single System Owner. In other cases, ownership will be split between a number of System Owners.

System Owners. is a technical person, independent of the System Owner, responsible for operating access control mechanisms and maintaining the user IDs, access groups and security parameters etc.

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 right to alter or amend any clause in this procedure at any time as per its discretion.

Metrics

- The metrics shall be measured by the Security In-charge's office. The periodicity of reporting shall be
  quarterly.
- Following are the metrics to be measured:
  - Number of accesses which were given to JMBGRP network without carrying out of vendor risk assessment and/or without signing of confidentiality/non-disclosure agreements.

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 reasons 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 updation 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 to Ticketing Tool.

References

- ISO 27001:2022 - A.5.15, A.5.16, A.5.17, A.5.18