Information Security Management System
Password Policy & Procedure

Document no. JMBGRP/ISMS/Pol-PW

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The policy document is to manage logical access to its technology infrastructure through a password-based authentication process to protect its information.	
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 “12. Reference to ISO 27001:2022”	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Document reviewed. Modifications done in Section: “Scope, Policy Statement, Procedure, Responsibilities, Metrics, Exceptions, Disclaimer”	

Contents

Purpose

JMBGRP controls logical access to its technology infrastructure through a password-based authentication process to protect its information / business data / application services / network devices / operating systems and software from unauthorized or illegal access.

The Password Policy shall ensure that security is established and maintained when the employees or third parties access the information and information systems of JMBGRP on a need-to-know basis or otherwise.

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

- All JMBGRP's information technology resources shall have appropriate password controls in place to protect IT / Information assets from unauthorized or illegal access.
- Password controls shall include managing password complexity, periodicity (90 days) and length which shall be enforceable by the system.
- There shall be implementation of a formal process for password management to employees and concerned third parties.
- Employees shall be trained on the creation & use of strong passwords. Passwords shall not be shared.
- Default passwords, provided by the vendor for systems, network devices, applications shall be changed.
- Password complexity features shall be enabled where ever permitted by technology , else a suitable tool or password complexity manager shall be deployed to enforce password complexity.
- JMBGRP shall adopt Identity and Access Management Technologies which shall help in the management of not only logical access but also password management.
- Sharing of passwords shall merit disciplinary action.

Procedure

1.1 The procedure on Password Policy shall address the aspects as listed below

1.1.1 Authentication

1.1.2 User Categories

1.1.3 Password Management

1.1.4 Password Standards

1.2 **Authentication**

1.2.1 For the majority of systems used at JMBGRP the company, authentication using a user ID and secure password (in accordance with the steps included in this document) shall be sufficient. In exceptional cases, for example remote access to sensitive Company systems via the Internet, secure two-factor authentication (e.g. user ID and token) shall be deployed.

1.2.2 It is good to have (Not Mandatory) to supply users with the same user ID on all internal systems by adopting a convention for formulating user IDs (e.g. SAP user ID).

1.3 **User Categories**

1.3.1 **Individual User IDs (Desktops and Laptops)**

1.3.1.1 All users (except as provided for below) must have unique individual user IDs. This includes use of e-mail, applications, system management and access administration.

1.3.2 **Group IDs**

1.3.2.1 Group or Generic ID's shall only be used in exceptional circumstances where the allocation of individual IDs would be impractical, for example several users within a shift or across shifts working on the same workstation and on the same tasks. The rules shown below shall be applied:

1.3.2.1.1 Use of Group IDs must be strictly limited. When issued all user activity shall be logged.

1.3.2.1.2 Group IDs must not be used with data that is assessed as Critical or Confidential.

1.3.2.1.3 Permission for their use must be given by the local Information Security Officer or IT Manager / HoD.

1.3.2.1.4 A named person (e.g. the group leader or shift foreman) must be recorded for each Group ID. This person shall be responsible for the following:-

1.3.2.1.4.1 Ensuring that only the correct people are given details of the ID.

1.3.2.1.4.2 Ensuring that anyone given the ID and password is aware of company Information Security policy.

1.3.2.1.4.3 Taking appropriate action in the event of any misuse of the ID, including assisting any investigation as to who may have used the ID at a particular time.

1.3.2.1.4.4 Withdrawing rights to use the ID and changing passwords as required.

1.3.3 System User IDs – Network Infrastructure Equipment and Application IDs

User IDs supplied by the vendor, or without which the system cannot operate effectively, e.g. super users or privilege, systems administrators. If there is no requirement to log into them then access shall be prevented (e.g. by disabling the user ID or scrambling the password). Default passwords of system User Ids shall be changed upon commissioning.

1.3.4 Guest IDs

Guest IDs shall be disabled unless there is a business requirement for them.

1.4 Password Management

1.4.1 Password communication

1.4.1.1 Passwords shall be communicated by telephone, sealed letter, secure electronic mail or SMS message. Passwords may not be left with another person nor left on the user's desk.

1.4.1.2 Password must be communicated separately from the user ID. E.g. user ID and instructions may be sent by e-mail or a letter; the initial password can be communicated by telephone or SMS-message.

1.4.1.3 When passwords are required to be couriered, then these passwords shall be sealed in an envelope and the sealed envelope shall be placed in another envelope. Recipient shall call or write to confirm the receipt of the password and shall destroy the same after memorizing. A record shall be maintained by IT Helpdesk where passwords have been couriered.

1.4.2 Change passwords after first use

Where passwords are initially selected or reset by Security Administrators, force or tell users to change them at the next logon (where technically possible). This shall be applicable across applications, infrastructure devices and end user systems.

1.4.3 **Password reset procedure.**

IT Help Desk or Security Administrators shall reset passwords. In these cases, the caller's identity shall be verified by one of the following methods:

1.4.3.1 The user sends a request for password reset to the Service Desk from the personal e-Mail account.

1.4.3.2 The caller visits a Service Desk to authenticate in person by showing an identity card.

1.4.3.3 Use personal information, such as date of birth, joining date or home address to validate the user if this information is available to Service Desk staff.

1.4.3.4 Verify the users full name, telephone number, location, e-mail address and PC reference number with information stored about the user (e.g. equipment database). Then call the user back on the number stored in the database or Company directory. If the user is away from their normal office base and cannot be called back on their registered number, then the Service Desk may still reset the password, but must follow this up with a telephone call back to the requestor later that day (or the following morning for out of hours requests) to check that the password reset request was valid.

1.4.3.5 If the IT Help Desk is suspicious about the request, contact the user's Line Manager / Head or an IT contact person of the caller's department.

1.4.4 **Access to another person's user ID**

1.4.4.1 IT Help desk or Security Administrators shall not reset a password for a user ID that does not belong to the user making the request. In emergency situations, where there would be a significant adverse impact on the organization, passwords may be reset upon the receipt of written (or e-mail) authorization by HOD which explains the reason for access. Access shall only be granted for a short period to retrieve/copy the required information after which access shall be withdrawn. The owner of the user ID shall subsequently be informed of the circumstances. A record of all such cases shall be maintained vide the Ticketing Took

1.4.5 **Storage of Critical Passwords**

1.4.5.1 Critical system accounts and passwords shall be stored securely by the System Owner, situation (e.g. administrator is not available at site). This shall be applicable for all systems which are not domain. This includes the UNIX environment and also those servers on Windows and which are classified as critical.

1.5 **Password Standards**

The following section describes the settings which shall be enforced.

1.5.1 **End User Systems an End User Application Access:**

1.5.1.1 At least eight characters minimum password length.

1.5.1.2 Passwords to be a combination of letters, numbers and special characters.

1.5.1.3 Password complexity to specify the number of times each password component should appear in the construction of a complex password and also the case of alphabets.

1.5.1.4 Apply a password dictionary and/or other checks to prevent users from selecting passwords that can be easily guessed.

1.5.1.5 Password change to be enforced or a reminder sent on or before 90 days, or more frequently if this shall be deemed necessary by the Data Owner.

1.5.1.6 Prevent quick re-use of passwords. Keep a history of at least 5 passwords.

1.5.1.7 Prevent users from changing passwords more frequently than once every 24 hours.

1.5.1.8 Allow users to select and change their own passwords.

1.5.1.9 Require verification of password changes, i.e. double input of the new password.

1.5.1.10 Stored passwords and passwords in transport shall be encrypted.

1.5.1.11 While browsing always select – " do not remember password"

1.5.1.12 Passwords must not be displayed in logs or printed output or stuck on pin boards.

1.5.1.13 Selectively deploy Single Sign On to eliminate password necklace syndrome.

1.5.1.14 Passwords for any kind of access shall not get transmitted in clear text.

1.5.1.15 In-case of any breach, passwords shall be reset through helpdesk.

1.5.1.16 IT Helpdesk shall not share desktop and laptop passwords with the end users.

1.5.2 **Network Devices and Application and Database Administration:**

1.5.2.1 Passwords in databases shall be stored in a secured manner.

1.5.2.2 Passwords for all system administrators and privilege users shall be 12 characters with complexity assigned.

1.5.2.3 Password complexity shall be maintained by way of inclusion of alphabets, numerals, special characters.

1.5.2.4 Password complexity to specify the number of times each password component should appear in the construction of a complex password and also the case of alphabets.

1.5.2.5 Passwords shall be changed every 90 days.

1.5.2.6 Password history rule will be – last 5 passwords.

1.5.2.7 Allow users to select and change their own passwords.

1.5.2.8 Require verification of password changes, i.e. double input of the new password.

1.5.2.9 Stored passwords and passwords in transport shall be encrypted.

1.5.2.10 While browsing always select – " do not remember password."

1.5.2.11 Passwords must not be displayed in logs or printed output or stuck on pin boards.

1.5.2.12 Passwords of systems not on domain shall be written down in front of their Group Leader and sealed in an envelope and stored in a fireproof cabinet.

1.5.2.13 In case of any breach, passwords shall be reset through helpdesk.

1.5.2.14 IT Helpdesk shall not share desktop and laptop passwords with the end users.

1.5.3 **Secure Logon Procedures**

1.5.3.1 Disable the user ID after 5 unsuccessful logon attempts so that it cannot be accessed until resumed by a Security Administrator. Where there are

technical or business reasons why this is not enforced, compensating controls shall be introduced, such as an increasing time delay before further logon attempts are allowed. With every failed logging attempt, the next attempt shall get delayed in the sequence of 5, 10, 20, 30, 60 minutes. The same shall be deployed for all server and network device access and also application database access.

1.5.3.2 Minimize displayed information regarding reasons for logon failures. For example, do not display "incorrect password" because this implies that the user ID is correct.

1.5.3.3 Passwords must not be displayed on the screen when being entered or changed.

1.5.3.4 All user IDs on applications, end user systems which have not been used for more than 30 days shall be disabled. All IDs having root access, administrator access if not used for 15 days, then they shall be disabled. All Power Users/Privilege Users whose IDs shall not be used for 30 days shall be deleted.

1.5.3.5 The user ID can be reactivated through a written request to the respective Group Leaders by the IT Infrastructure Team Members and to IT Helpdesk by the rest of the employees post approval from their respective HOD.

1.5.3.6 In cases of known absence on account of sabbatical, health grounds, transfer, the IDS shall be disabled and passwords reset on the same day, the request is received from the concerned HOD.

1.5.3.7 Display sufficient details of the last successful logon and subsequent failures so that a user shall identify unauthorized use or attempted use of the ID.

1.5.4 **Reference**

1.5.4.1 Access Policy and Procedure shall be reviewed in conjunction with this document.

Responsibilities

The responsibility for implementing this procedure lies with the following personnel:

- System / Application Administrator:
  - Allocate one-time/new or separate passwords as required by the individual applications.
  - Reset password after identity verification.
  - Log password reset requests.
  - Implement password security controls.

  - Implement two factor authentications for Privileged IDs.
  - Review Log of password retrieval of privileged ids from the sealed envelopes.
  - Review of password reset logs.
  - Approve retrieval of privileged id password from the sealed envelopes.
- IT Helpdesk:
  - Review the password reset request.
  - Provide new passwords.
  - Provide MIS to InfoSec Team about the number of passwords reset requests received every month.

Enforcement:

- This policy and procedure is applicable for all the employees and contractors 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 by the Head IT – Network Infrastructure and Head IT for-Application Management Windows and UNIX respectively. And provided to the Head GIS and Security In-charge.
- The periodicity of reporting shall be once in a quarter.
- The metrics to be monitored are as given under:
  - Number of weak passwords found.
  - Number of unsuccessful logon attempts recorded.
  - Number of passwords reset done for users.
  - Maximum number of password resets done per user.
  - Number of time the sealed envelope was accessed to gain privileged ID passwords.
  - Number of default passwords detected on systems / network devices and applications.
  - Number of exceptions provided in the password policy implementation.

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 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 shall 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.

- Identified IT team 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 on Ticketing Tool

References:

- Control : A.5.17,