Information Security Management System
Data Backup Restore Policy

Document no. JMBGRP/ISMS/Pol-BR

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The document to define the requirement of necessary and applicable mechanisms for the purpose of backup and restoration of JMBGRP information assets	
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,	

Contents

Purpose

The policy seeks to define the requirement of necessary and applicable mechanisms for the purpose of backup and restoration of JMBGRP information assets so that information shall be protected from misuse, theft and loss and be available when required by authorized users.

Scope

This policy covers protection of any data that belongs to JMBGRP and applies to all users of information assets and facilities on behalf of JMBGRP.

Policy Statement

- Backup of all business data, related application systems and other business critical/confidential applications, wherein the frequency of backup operations and the procedures for recovery and restoration meets the need of the availability of data for the organization. The accepted level of availability should be maintained in case of a disaster or loss of data due to errors and omissions either advertent or inadvertent.
- Archiving of electronic data shall be in accordance with the business, legal and regulatory requirements. Archiving shall be done to ensure that stakeholders have easy access on a need-to-know basis of data / information.
- Data backup strategy and data recovery procedures shall be implemented to ensure that critical business data is never lost under any circumstances and is always available.
- Carriage/ transfer of any media within the premises of the JMBGRP or taking it outside the premises shall be done in a secure way.
- Regular process of media handling / back up / restoration and that of BCP / DR shall be done independent of each other; however, necessary protocols shall be followed in their individual execution.
- A suitable tool shall be deployed for endpoint back up.
- A suitable platform shall be deployed which will provide DR like back-up of the application servers and databases.
- Disposal of backup tapes shall be done in accordance with the environmental legislation prevailing in the country of operation. It shall be supervised to prevent any theft / unauthorized copying from occurring.

Procedure

- The data to be backed up shall come forth from the information assets captured in the Information Asset Listing Sheets of the various departments.
- This procedure shall address the following aspects as stated under and shall cover all aspects of Backup, Media Handling and Restoration as stated in the ensuing topics as mentioned in this procedure.
    - Application, Server, Router, Switches , Firewall and Appliances Backups
    - Desktop and Laptop backup

- External Media Backup
- Ad-hoc Backups
- Event or Calendar-based backup procedure
- Choice, Issue and Labeling of Media and Process
- Backup Register and Logs
- Media Handling Process
- Selecting an Off-site Storage Facility
- Contents of Off-site Storage
- Storage of Backup Media
- Media Rotation
- Restoration Drills
- Restoration of Backups in case of data loss

- Assignment of Responsibilities:
  - HOD IT (for Desktops, Laptops) shall assign the responsibility to a concern IT person for taking backup of desktop/laptop data.
  - There shall be fulltime custodian for managing backup media and who shall manage the circulation of the media as well.
- Initiation:
  - The initiator (Business Groups and Infrastructure Team) shall initiate a request for backup. The request shall include application details, server details, frequency, time of backup, data to be backed up for the department/application etc. Backup request form shall be used for the purpose and shall include detailed backup plan and procedures for each application, which shall be documented by initiator.
- Backup procedures shall provide the following information:
  - Application Back Up:
    - Files, applications including databases to be backed up (SECRET, CONFIDENTIAL)
    - Apart from the above-mentioned point, information assets in hard format such as, but not restricted to vendor agreements, paper licenses and any other documents not necessarily in CRITICAL or SECRET or CONFIDENTIAL category, but which are required from an availability perspective; shall be digitized with smart search for ease of reference and retrieval of information, and stored on either a portal with restricted access or a server with folder level protection.
    - IT (backup) Administrator assigned and authentication details.
    - Inventory of backup media including the location of their storage and contents.
    - Record of blank (unused), discarded and destroyed media in a manner that complete history of media usage is available.
    - The request shall be sent to the HOD who shall assign the backup activity to the IT Team member.
    - Any changes made to system, which affects regular backup, shall be intimated to IT team backup initiator.

- A suitable platform shall be deployed for backing up application configuration, OS, databases which also offers DR in the box capability.

- Server Backups:
  - A tool-based approach shall be deployed while backing up data from servers. This shall be scheduled based on the work schedule.
  - Backup Scheduling shall be related to business risk, frequency with which data and software is changed and the criticality of the system to business operations.
  - Based on criticality a full image back up shall also be taken using tools which provide DR in a Box features.
  - Systems software, application software, data, different logs and documentation shall be backed up on a regular basis, in accordance with back-up schedule as defined below.
  - As a minimum standard for SECRET or CONFIDENTIAL Servers:
    - Full daily back-up of data will be done as per business requirement.
    - Full weekly back-ups of all application data, including its configuration are taken.
    - Full monthly back-ups of all data, including operating system configuration files.
    - Consolidated backup shall be taken on a monthly basis for archival. Such archives shall be stored for a year or as per business need.
    - Yearly backup of all consolidated monthly tapes/media shall be taken and archived.
    - Time frame for the archival will be as per the regulatory and business requirements.
  - As a minimum standard for rest of the servers:
    - Full monthly back-ups of all data, including operating system configuration files and applications.
- Configuration back-up of Routers, Switch, and Firewalls to be taken on monthly basis, the configuration details history to be maintained and stored on a storage system with restricted access.
- Desktop and Laptop backup:
  - End User Computing Team shall provide a backup facility to users for backing up of SECRET and CONFIDENTIAL data stored on their desktops / laptops, and it shall be a tool-based process.
  - This shall be done through a scheduled backup routine which shall back data from the designated folders to the designated drive on a file server or will be done through a backup tool. The user will not be able to kill the process, the settings of which will not be accessing to the user as a result of hardening process applied.

- Once planned the portal for collaborative working is established then users shall backup all their SECRET/CRITICAL/CONFIDENTIAL data on this portal only.
- Access rights to these designated folders on file server or on the portal shall be manage by the Infrastructure Team.

- External Media Backup (Hard Disk/CD/DVD):
  - Users shall submit backup request to their Head of the Department.
  - After approval from Head of the Department, it shall be forwarded to the IT team therein.
  - The IT Team shall label and issue the media to the user / IT Helpdesk/Infrastructure Team to take the backup and shall update the media issue register (Refer to section: Issue and Labeling of Media).
  - User shall keep the media under their protection in a locked drawer preferably with Department Head after taking backup on it.
  - All important data on desktop/laptop / other systems which are moved to the Infrastructure Team as a part of decommissioning shall be backed up and the backup media shall be handed over to the concerned Department Head before it gets formatted.
  - IT shall provide a centralized back up tool for desktop and laptop users to back up their data in a protected manner.
- Ad-hoc Backups:
  - Backup of the complete operating system, including all applications and data shall be taken before and after any significant changes that may affect the operating system, system or application software. The changes may be the result of a system upgrade, a planned power outage or any other event that may put the system and data at risk.
  - All ad-hoc backup shall be initiated by the data owner, who shall send a formal request for backup of the same.
  - Based on the retention period specified in the backup request form and the classification level, the media shall be stored, erased or destroyed.
- Event or Calendar-based backup procedure:
  - Applications may require a backup based on occurrence of an event or a quarterly, end-of-month or end-of-year backup
    - Asset Owners with specific backup requirements driven by either events or the calendar shall provide written instructions to the IT team detailing those requirements with the associated retention requirements for the backup media.
    - IT team performs backup according to the written instructions from the Asset Owner.
    - Media produced, as a result of an Asset Owner request, shall be placed in secure on-site/off-site storage.
- Choice, Issue and Labeling of Media and Process:
  - Choice of backup media shall be guided by considerations of size of data to be backed up, requirements of backup software, speed of backup and

restoration, life of storage of the data, reliability requirement, efficiency and available technology.

- All backup media shall be issued by the IT Administrator, who shall also update the media issue register on issue, return and disposal of media.
- The media issue register shall include the details like type of media, issued to whom, date of issue, date of return, expected life span, date of disposal etc.
- All backup media shall be labeled by the IT Administrator to include the following details:
    - Date of issue of media. (This label shall be tamperproof).
    - Type of Backup (Full / Incremental / Differential).
    - Media identifier / Set Number.
    - Date and Time of Backup.
    - Reference to machine whose data is backed up (Server/Applications/ Databases/ Desktops/Laptops).
    - Location (Onsite / Offsite).
    - Classification: The classification of backup media shall be in accordance with Information Asset Security Classification Policy and Procedure.
    - The IT administration team shall schedule the backups as per the backup request.
    - Backup process shall run (either automatically through scheduled tasks configured in the OS systems or by use of dedicated backup software or manually). The IT Administrator shall put in the correct labeled tape before the backup commences.
    - After the backup is complete, the IT Administrator shall remove the tape from the tape drive and put in tape for the next scheduled backup. The IT Administrator shall check the label of the tape before inserting it. Alternatively dedicated storage boxes shall also be used.
    - Backup failure reports shall be automatically sent through emails to the respective application owners/data owner and IT Administrator(s).
    - Backup media shall be replaced on the basis of number of writes permissible by media manufacturer only.
    - The duration of the backups which are to be kept in the repository shall be based upon regulatory and business requirements.

- Backup Register and Logs:
    - A register of the backups, including the verification of their success and failures shall be maintained at the location where restoration activity was carried out with the details as under.
        - Date and time of backup (start time and end time).
        - Type of backup (Incremental / Full/Differential).
        - The label of the tape/CD/DVD/Hard disk used.

- The details of offsite / onsite storage of media.
- Details of movement of the tape (if stored offsite).
- Date of movement.
- Courier Company used.
- Whether backup completed successfully.
- Reasons for unsuccessful backup (if any).

▪ Automatic logs shall be generated which show the status of the backups taken.

- These status logs shall be sent to the application owners in case of applications and to HODs in case of failure of the identified desktops and laptops by the IT Administrator indicating the success/failure of critical server's (SECRET, CRITICAL, CONFIDENTIAL) backup and failure of GENERAL servers as may be applicable.
- All the backup logs shall be archived by the IT Administrator on a dedicated system with restricted access.

o Media Handling Process:

▪ The media handling process shall cover aspects related to access, movement, handling storage, and movement of media. This shall include onsite and offsite process and shall include aspects of testing and restoration.

▪ Media Handling Points:

- Backup media shall not be exposed to excessive heat, light, moisture, dust, high magnetic fields, static electricity etc.
- Surface of CDs/ DVDs shall be prevented from scratches.
- Hard disks shall not be exposed to mechanical jerks or vibrations.
- Antistatic packaging shall be used during transport for tapes and hard disks.
- Agreement with the courier company with clear instructions for handling shall be provided and there shall be a preferred courier for this purpose.
- In case of a third-party facility being used then the list of personnel, who manage the process, from the company's side and that of personnel from the service provider's side shall be maintained.
- The periodicity of transfer of media and the mode shall be decided by JMBGRP and adhered to by the service provider.
- If the media is being handled in-house then the IT Administrator shall assign a person from the team to do the task.

o Selecting an Off-site Storage Facility

▪ The off-site storage facility shall be at least 15 kilometers (9.32 miles) from the facility and not be located within the same flood plain, tectonically unstable area, or other area of significant shared physical or environmental risk.

- The off-site storage facility shall not be located in an area that would be inaccessible due to blocked streets or damaged bridges in the event of a natural disaster or civil unrest.
- The off-site storage facility shall either have an alternate source of backup power or be on a different power grid than the facility.
- The off-site storage facility shall be accessible by at least three entirely different routes to disaster recovery site and to the facility.
- Off-site storage facilities must provide physical and environmental security that is compliant with the requirements of the companies Physical and Environmental Policy for Information Security.

- Contents of Off-site Storage:
  - Secure off-site storage shall contain the following:
    - Removable media containing backup data.
    - Copy of the current inventory of the backup media that are both on-site and in off-site storage.
    - Copies of all procedures addressing backup, restoration, and reconstitution of data storage.
    - Copy of log reflecting introduction and removal of contents of off-site storage.
- Storage of Backup Media:
  - The steps for offsite and onsite storage have been provided below:
    - All backup media containing backup of CRITICAL/CONFIDENTIAL Servers, Network Devices shall be stored offsite and or onsite. For any other backup, storage location shall be decided by the data/ information owner.
    - Backups shall be retained as required by business, legal and statutory requirements.
    - Temperature/Relative humidity shall be maintained as per manufacturer's recommendations.
    - The storage container shall be made of fireproof material and shall have combination locking mechanisms.
    - Different categories of media shall be segregated in the storage location for ease of locating.
    - The place where media is being stored shall not be in the basement of any building as there could be risk of flood.
    - The place where backup media is being stored shall be devoid of any windows and if they happen to be there, then the same shall be sealed and comprise of toughened glass to prevent any natural elements intruding into the area.
    - For onsite backup there shall be two custodians for the keys to the backup vault.

- When backup media is being sent to an offsite location then the same shall be done in a container, which is fireproof, weather proof and tamper proof.
- Two keys of the above-mentioned container shall be with the IT Administrator and one set shall be with the offsite service provider.
- Access list of personnel who will manage the process or will have access to media, shall be maintained by the service provider and JMBGRP and reviewed once in three months or when changes occurs to the designated team by the Information Security Team.
- After every transfer of media to a third-party location there shall be communication via mail to the IT administrator.
- The audit of the offsite backup facility shall be conducted by the IT Team at least once in 6 months.
- There shall be biometric access mechanism coupled with RFID Access to the media storage room.
- The access to authorized personnel shall be time bound and any access beyond working hours shall be with the authorization of the HOD and the security desk shall be informed.

- Media Rotation:
  - The rotation of the media shall be informed by the respective application owners to the IT (Backup and restoration) Team in writing for every quarter. Any change to this schedule shall also be done in writing and informed to the IT team. The rotation data of media shall also be maintained by the Information Security Team.
- Restoration Drills:
  - Restoration shall be scheduled at least once a quarter for CRITICAL/CONFIDENTIAL data by the respective IT Administrators. The result shall be communicated in writing by the IT Head to the respective application owners/HODs. The IT administrator shall select a tape at random basis for restoration drill of or as requested by the concerned application owner and HOD.
  - A log of restoration drills shall be maintained by IT Administrator to include the following details:
    - Tape Identification Number (if applicable).
    - Date and time of drill.
    - Whether restoration completed successfully.
    - Whether the process owner has verified the restored data.
    - Details of review by the IT Team.
    - Reasons for unsuccessful restoration (if applicable).
    - Corrective Actions if any.
  - After the restoration drill is completed successfully, the media shall be safely returned to its original location.

- In case of failure in restoration, the IT Administrator shall inform the application owner/Information Security Team citing reasons of failure and the nature of the intervention required. The Infrastructure Head along with the concerned manager with ISO/ HOD oversight and IT Administrators shall decide on corrective action.
- The IT Administrator shall log the incident and shall update the media issue register (if required) and inform the Information Security Team.
- The restoration drill for backups taken by user on the external media shall be user's responsibility.

- Restoration of Backups in case of data loss:
  - Desktops/ Laptops:
    - In case of data loss, the user shall check the centralized file server for restoration and prepare a request.
    - User request shall contain details about the data to be restored, the reasons for restoration etc. and approval of their HOD.
    - The user's Head of the Department shall approve this request after verifying the need for restoration and checking whether the user is authorized to have access to the data.
    - The user shall then submit this completed form to IT Administrator.
    - The IT Administrator shall restore the required data from the onsite or offsite backup media.
    - After the restoration, the IT Administrator shall safely return the media to the original location.
    - IT Administrator shall maintain a log containing details about the date and time of restoration, label of the backup media, location of storage etc. These details shall be filled in the restoration form and filed in restoration register.
    - During restart of the machine in case of recovery procedure for a hard-disk crash, only safe mode shall be used for restart. Disks shall be scanned and then the system shall be shut down and the system booted in a normal mode.
  - Servers:
    - The IT Team shall decide on the tape to be used for restoration. The tape, as far as possible, shall be the most recent successfully backed up tape.
    - Recovery procedures as defined by application owners shall ensure the relevant files are restored in order to ensure full application functionality is restored.
    - Restoration is being done on a standby machine and then transferred to the live machine. Restoration directly on a live machine shall be treated as an exception and a written approval from Head of IT/HOD shall be taken.

Responsibilities

- After successful test restoration, the restoration shall be carried out on the actual server.
- While restoring the files and directories, it shall be ensured that access permissions are not changed or corrected after restoration is complete.
- IT Administrator shall maintain a log containing details about the date and time of restoration, label of the backup media, location of storage etc. These details shall be filled in the restoration form and filed in Restoration register.
- The IT Administrator shall inform the Infrastructure Team about the data loss on the server. The Information Security Team shall also be informed to log the incident.

▪ Outdated Media Formats:

- The IT Administrator shall convert the existing backups to the new formats if required. This shall be applicable in case of old floppies and tapes from legacy systems if any.

▪ Disposal:

- There shall be a formal mechanism for the execution of the disposal process.
- With approval from the concerned department/ application owner /information security team/ IT Team, the data on the media shall be erased completely before disposal.
- It shall be ensured by the IT Administrator that the media is completely unreadable before discarding it.
- The hard disk media shall be degaussed or physically destroyed, while the tapes shall be crushed/ cut into multiple pieces or degaussed under supervision of the personnel from IT Team.
- Disposal records shall be maintained for audit purpose by IT Team

- The Media Issue Register shall be updated accordingly if the tapes are being incinerated/ destroyed through a third party with NDA to protect from violations. A supervisor from the side of JMBGRP shall be present at the time when JMBGRPs' media is being destroyed at the external party's premises.

The responsibility for implementing this policy is with the following personnel:

IT Administrator and Team:

- Label and issue the media.
- Review the status logs of the backup activity.
- Inform the application owners/HOD whenever there is a failure of data backup.
- Ensure proper configuration of the backup system.

- Backup data in accordance with the schedule.
- Maintain / Review restoration drill schedules and execute the same.
- Restore data whenever requested and take a sign off from the requester of successful restoration.
- Maintain accounting of issued media.
- Assign the responsibilities of backup to the IT Administrator.
- Review the backup request and assign the task to IT Administrator.
- Random review of the backup/restoration logs and media. Review media issue register.
- Approve direct restoration on live server in case of data loss.
- Approve disposal of media.
- Manage offsite backup process.
- Ensure Information Security Team Audits the backup process on-site and offsite.

HOD, application owners and Users as the case may be:

- Give information to IT Team about the data to be backed up, the frequency of backups etc. taking into consideration the criticality of information.
- Ensure backups are taken for their business-critical data.
- Request restoration in case of loss to data.
- Record the incident in case of loss of data on the server/desktop /laptop and restoration failure.
- Employees and third parties of JMBGRP are expected to ensure backup of CRITICAL and CONFIDENTIAL business data and adhere to this procedure. Non-compliance to this could result in disciplinary action as per the code of conduct of the organization.
- While restoring the files and directories, it shall be ensured that access permissions are not changed after restoration is complete.

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

Metrics

- Metrics shall be measured by IT Team and shall be reported to respective HODs every quarter.
- The periodicity of reporting shall be once in a quarter and shall include, but not limited to:
    - Number of times restoration has failed for Critical and Confidential assets.
    - Number of times data was lost on account of back up not being taken.
    - Number of times media was lost on account of it not being entered into the register before removal.
    - Number of times back up media was lost in transit/damaged/stolen.
    - Media wise issues during the backup procedure.
    - Number of times scheduled back up and restoration has not happened.
    - Media destroyed without any record.

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 updating 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 in Ticketing Tool.

References

ISO 27001:2022 - A.8.13