GSTIN : 08AAWFR1181K1ZK
PAN : AAWFR1181K

Mob. : 9314070008

# RCA & CONSULTANT

Plot No. D-4, Lal Kothi, Jyoti Nagar, Jaipur 302004
E-mail : rcaconsultant77@gmail.com, rcaconsultant@yahoo.com

Document Control chart.

| Document Name | Data Backup, Retention and Purging Policy |
|---|---|
| Version | 1.0 |
| Created on | 24-06-2026 |
| Created by | Surendra Meena |
| Reviewed by | Ravindra Singh |
| Next Revision | 25-06-2027 |
| Document Approved by | Ravindra Singh |

Document Revision chart.

| Date | Version | Reviewed by | Changes |
|---|---|---|---|
| 25-06-2027 | 1.0 | Ravindra Singh (Director) | Create |

For RCA & CONSULTANT
Ravindra
Partner

**Data Backup, Retention and Purging Policy**

**1. Purpose**

A) The policy seeks to define the requirement of necessary and applicable mechanisms for the purpose of backup, restoration and media handling of (RCA AND CONSULTANT) information assets so that information shall be protected from misuse, theft and loss and be available when required by authorized users.
B) The purpose of this policy is to ensure efficient and secure access to the common drive for employees while minimizing impact on internet bandwidth and ensuring data integrity.

**2. Scope**

A) This procedure applies to all (RCA AND CONSULTANT) Company information stored by the IT Department, regardless of storage medium

**3. Execution Responsibility**

A) The Backup Management team is responsible for reviewing the backup and restoration procedures and responding to the escalations (if any) pertaining to the backup and restoration procedures.
B) Process Head is responsible for developing and reviewing the Company's information storage and backup plan.
C) Backup Management team should also be responsible for reviewing the logs of the backup and the reasons for failure (if any). The Backup Management team is responsible for implementing the Company information storage and backup plan.

**4. Policy Requirements**

A) Backup of all business data, related application systems and other business critical applications, wherein the frequency of backup operations and the procedures for recovery and restoration meets the need of the availability of data to business in case of a disaster or loss of data due to errors and omissions either advertent or inadvertent.
B) Archiving 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
C) Data backup strategy and data recovery procedures shall be implemented to ensure that critical business data is not lost under any circumstances and is always available.
D) Data Purging of all electronic data, images and any other information pertaining to client shall be carried out according to guidelines laid down by client as per defined periodicity of data.
E) **Access Control**: Access to the common drive will be granted based on the principle of least privilege, with access rights determined by the employee's role and responsibilities approved by Ops Head & ITSMT.
F) **Data Security**: Employees are responsible for maintaining the confidentiality and integrity of data stored on the common drive.
G) All sensitive or confidential information must be appropriately labelled, and access restricted to authorized personnel only.

For RCA & CONSULTANT

Partner

H) Deletion of data without proper approval is prohibited. Also, you will update, delete data only which is yours from common drive, if found that you are deleting data of someone else, ZTP will be applied.
I) **File Organization**: Employees are required to organize files in a logical and consistent manner to facilitate easy retrieval and minimize clutter.
J) Files should be named descriptively and include relevant dates or version numbers if applicable.
K) **Usage Guidelines**: The common drive is intended for storing and sharing work-related documents only. Personal files or non-work-related content are not permitted.
L) Employees must adhere to all relevant laws, regulations, and company policies when accessing or storing data on the common drive.
M) Data which is needed in the long run (older than 90 days & unwanted) should not be stored on common drive and should be deleted or with approval from SLA should be transferred to respective client.
N) **Bandwidth Management**: Editing or working on files simultaneously with multiple users in one file via the common drive is discouraged to prevent excessive strain on internet bandwidth.
O) Employees should copy and paste files to their local drive for editing, then upload the revised file back to the common drive upon completion.
P) Data Backup: It is the responsibility of individual employees to ensure that important files are backed up (to client location or to client repository) regularly to prevent data loss.
Q) The IT department will implement regular backups of the common drive, but employees should not rely solely on this backup for critical files, nor will this backup be responsible for providing deleted files or lost files.
R) **Prohibited Actions:** Uploading or storing malicious software, illegal content, or any material that violates company policies or applicable laws is strictly prohibited.
S) Any attempts to bypass security measures or access unauthorized areas of the common drive will result in disciplinary action.

**Common Drive Guidelines:**

A) Before working on a file, users should copy it to their local drive.
B) After completing work, users should upload the revised file back to the common drive and delete the local copy.
C) Data which is needed in the long run (older than 90 days & unwanted) should not be stored on common drive and should be deleted or with approval from SLA it should be transferred to respective client.
D) Deletion of data without proper approval is prohibited. Also, you will update, delete data only which is yours from common drive, if found that you are deleting data of someone else, ZTP will be applied.

**5. SOP for Data Backup**

A) A file server with an allocated space for the identified users shall be created.
B) If any external parties are to be involved for data back up or recovery, then adequate care shall be taken to protect the information assets of RCA AND CONSULTANT given to these agencies.
C) Carriage/ transfer of any media within the premises of the RCA AND CONSULTANT or taking it outside the premises shall be done in a secure way.
D) 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.

For RCA & CONSULTANT
Ravindra Pawan Chaudhary
Partner

E) Adequate security shall be provided to the area (onsite and offsite) which shall house back up media and sitting norms shall be adhered to.
F) 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.

**6. SOP for Data Retention / Purging Data Identification**

A) **Classification:** All data stored within IT systems must be classified according to its type, sensitivity, and requirements.
B) **Retention Schedule:** Establish a retention schedule for each data type, ensuring it does not exceed 90 days unless legally required.
C) **Review:** System Administrators should review stored data at regular intervals to identify data approaching the end of its retention period. Notification and Approval
D) **Internal Notification:** Notify the data owner and relevant department heads when data is due for purging.
E) **Approval:** Obtain written approval from the data owner and Compliance Officer before proceeding with the purge.

**Documentation and Reporting**

A) **Record Keeping:** Maintain detailed records of the purging activity, including the data type, date of purging, methods used, and personnel involved.
B) **Reporting:** Submit a purging report to the Compliance Officer and IT Director for review and record-keeping. Audit and Compliance
C) **Periodic Audits:** The RCA AND CONSULTANT Internal Compliance Officer will conduct audits every three months to ensure adherence to the SOP.
D) **Non-Compliance:** Any instances of non-compliance should be documented, and corrective actions must be taken immediately.

| Process Name | Retention Period | Purging frequency |
|---|---|---|
| DMS collection process | 90 Days | Quarterly |

**7. Exceptions**

A) 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.
B) 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 temporary or permanent in nature.
C) All exceptions during implementation shall be submitted by the person responsible for implementation concerned. These shall be submitted through an Exception Form and sign-off on the same shall be maintained including ad-hoc requests. Backup, Restoration and Media Handling Policy CLASS 1.
D) RCA AND CONSULTANT shall also list parameters to ensure that before acquiring new applications or other software and hardware, the set of applicable policies and guidelines shall be matched with the available security mechanisms of the product to ensure that the product has the necessary features. If not, then exceptions shall be approved before

For RCA & CONSULTANT
Ravindra Pawan Chaudhary
Partner

acquiring the desired product. Similarly, while developing new applications, the necessary security policies and guidelines must be incorporated in the application or exceptions shall be obtained for the same from the Information Security Team.

**8. Violations & Disciplinary Action**

A) In case of violations by stakeholders, the actions to be taken have been mentioned in the RCA AND CONSULTANT's Code of Conduct.
B) The Organization shall always protect the interests of its stakeholders through the adherence to Information Security Policies and the applicable legislation and through the administrative mechanism established coupled with the Information Security Policies, RCA AND CONSULTANT shall control the occurrence of violations by individuals.
C) Violations by the third party shall also come under the purview of the Information Security Framework and action shall be taken accordingly.

**9. Disclaimer**

A) RCA AND CONSULTANT 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, CDS, 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 RCA AND CONSULTANT.
B) The information security policy and procedure document is meant to be published on the intranet of RCA AND CONSULTANT and/or any other forum as decided by the management of RCA AND CONSULTANT. Anything not specifically stated in this information security policy and procedure document shall not be considered as implied in any manner.
C) For any clarifications related to this information security policy and procedure document with respect to its interpretation, applicability and implementation, please write to (Defined Email ID)

**10. Policy Review**

A) This policy shall be reviewed every 12 months by authorized IT / Operations personnel and any changes to procedures or new guidelines shall be recorded in document revision chart for this document.

**11. Reviewer & Monitor Staircase and SPOC Details: -**

| SR.No. | Name of SPOC | Staircase |
|---|---|---|
| 1. | Team Leader | L1 |
| 2. | Process Head | L2 |
| 3. | Director of (RCA AND CONSULTANT) | L3 |

Approved by Management

Ravindra Singh

Director (RCA AND CONSULTANT)

For RCA & CONSULTANT

Ravindra

Partner

Prepared by

Surendra Meena

Process Head

For RCA & CONSULTANT

Ravindra

Partner