Transmission Corporation of Andhra Pradesh Limited

DATA DELETION

AND

RETENTION POLICY

Confidentiality Statement

Document Control

Document Name	Data Deletion and Retention Policy
Document Reference Number	APTRANSCO/ISMS/DDRP/1.0
Classification	Internal
Version Number	D1.0
Date	25 – NOV-2024
Reviewed by	IT Wing / GICU Division
Approved by	

TABLE OF CONTENTS

1. INTRODUCTION 4
2. IMPORTANCE OF DATA DELETION AND RETENTION POLICY 4
3. KEY COMPONENTS OF A DATA DELETION AND RETENTION POLICY 5
4. BEST PRACTICES FOR DATA DELETION AND RETENTION 6
5. REGULATORY CONSIDERATIONS 6
6. ADVANCED CONSIDERATIONS 6
7. IMPLEMENTING A DATA DELETION AND RETENTION POLICY 7
8. CONCLUSION 7

1. Introduction

In today's digital age, organizations collect, store, and process vast amounts of data. Managing this data effectively is crucial for compliance, security, and operational efficiency. A well-defined data deletion and retention policy ensures that data is retained for the appropriate length of time and deleted securely when no longer needed. This policy helps in mitigating risks, ensuring compliance with various regulations, and maintaining customer trust.

Purpose

Clearly define the purpose of the policy and specify the types of data it covers, such as personal data, sensitive data, Organisation / business records, etc.

Scope

Identify the departments or individuals responsible for implementing the policy.This policy applies to all data, regardless of its format (electronic or physical), that is collected, stored, or processed by Soulpay, including data related to customers, employees, suppliers, and other stakeholders.

1.1. Data Categories

1.1 P**ersonal data**: Data that can identify individuals, including but not limited to names, addresses, contact information, and sensitive personal information.

1.2 **Financial data**: Data related to financial transactions, including payment information, invoices, and financial reports.

1.3. **Operational data**: Data used for the day-to-day operations of the organization, including emails, communication records, and project-related information.

1.4. **Legal/Compliance data**: Data required to meet legal and regulatory obligations, including contracts, tax records, and compliance reports.

1.2 Data Retention Periods

1.2.1. **Personal data**: Retained only as long as necessary to fulfill the purposes for which it was collected or as required by law. Once the retention period ends, personal data is securely deleted.

1.2.2. **Financial data**: Retained as required by applicable financial and tax regulations. Once the retention period ends, financial data is securely deleted.

1.2.3. O**perational data**: Retained for a reasonable period to support business operations. Once it is no longer needed, operational data is securely deleted.

1.2.4. **legal/compliance data**: Retained for the duration specified by applicable laws or regulations. Once the retention period ends, legal/compliance data is securely deleted.

2. Importance of Data Deletion and Retention Policy

1. **Compliance**: Various laws and regulations, such as GDPR, HIPAA, PCI DSS, and ISO 27001, mandate specific data retention and deletion practices. Non-compliance can lead to hefty fines and legal consequences.
2. **Data Security:** Retaining unnecessary data increases the risk of data breaches. Secure deletion minimizes this risk by ensuring that obsolete data is not accessible to unauthorized entities.
3. **Storage Management:** Efficient data retention policies help manage storage resources better, reducing costs associated with data storage.
4. **Operational Efficiency:** A clear policy helps in streamlining data management processes, making it easier for employees to access relevant data while reducing clutter from obsolete information.

3. Key Components of a Data Deletion and Retention Policy

1. **Data Classification**
   - **Sensitive Data**: Information that could cause harm if disclosed, such as personal data, financial information, and health records.
   - **Operational Data**: Data necessary for day-to-day operations, such as transaction logs and user activity records.
   - **Historical Data**: Data that has historical significance but is no longer actively used, such as old project files.
2. **Retention Periods**
   - **Regulatory Requirements**: Define retention periods based on regulatory requirements for different types of data.
   - **Business Needs**: Consider business needs and operational requirements when defining retention periods.
   - **Data Lifecycle Management**: Implement processes to manage data throughout its lifecycle, from creation to deletion.
3. **Deletion Procedures**
   - **Regular Deletion Cycles**: Establish regular deletion cycles (e.g., monthly, quarterly) to review and delete obsolete data.
   - **Secure Deletion Methods**: Utilize secure deletion methods, such as data wiping and shredding, to ensure that deleted data cannot be recovered.
   - **Automation**: Implement automation tools to facilitate regular and secure deletion processes.
4. **Roles and Responsibilities**
   - **Data Owners**: Individuals responsible for the data within their departments, ensuring compliance with retention policies.
   - **IT Department**: Manages the technical aspects of data retention and deletion, including automation and secure deletion tools.
   - **Compliance Officers**: Ensure that the organization adheres to regulatory requirements and conducts regular audits.
5. **Documentation and Monitoring**
   - **Policy Documentation**: Maintain comprehensive documentation of the data deletion and retention policy.

- **Monitoring and Auditing**: Regularly monitor compliance with the policy and conduct audits to ensure effectiveness.

4. Best Practices for Data Deletion and Retention

1. **Data Minimization**: Collect and retain only the necessary data to reduce the burden of managing and securing large volumes of information.
2. **Encryption**: Encrypt sensitive data both at rest and in transit to protect it during its retention period.
3. **Backup Management**: Implement policies for managing backups, including retention and secure deletion of outdated backups.
4. **Employee Training**: Educate employees on the importance of data retention and deletion policies, and train them on proper data handling procedures.
5. **Incident Response**: Develop an incident response plan that includes procedures for handling data breaches and ensuring that data deletion is part of the recovery process.

5. Regulatory Considerations

1. **GDPR**: The General Data Protection Regulation requires organizations to retain personal data only for as long as necessary and mandates the right to erasure (right to be forgotten) for individuals.
2. **HIPAA**: The Health Insurance Portability and Accountability Act mandates retention periods for medical records and requires secure disposal of patient information.
3. **ISO 27001:** The international standard for information security management systems (ISMS) includes requirements for data retention and secure disposal.

6. Advanced Considerations

For a truly comprehensive approach, consider these advanced aspects of data deletion and retention:

- **Data Anonymization and Pseudonymization:** Instead of deletion, organizations may choose to anonymize or pseudonymize data. This involves removing personally identifiable information (PII) or replacing it with non-identifiable substitutes. This allows for data retention for analytics or historical purposes while protecting privacy.
- **Legacy Data:** Organizations may have historical data stored on outdated systems. The policy should address the migration, deletion, or secure archiving of such data.
- **Data Backups and Archiving:** Data backups and archived data fall under the purview of the policy. Procedures for deleting backups after a specific period or securely archiving historical data should be defined.
- **Cloud Storage Considerations:** Cloud storage providers may have their own data deletion and retention policies. The organization's policy should align with or build upon these cloud-specific considerations

7. Implementing a Data Deletion and Retention Policy

1. **Policy Development**
   - Conduct a data inventory to identify all data types and their associated retention requirements.
   - Engage stakeholders from various departments to understand business needs and regulatory requirements.
   - Draft a comprehensive policy that includes retention periods, deletion procedures, and roles and responsibilities.
2. **Implementation**
   - Communicate the policy to all employees and provide necessary training.
   - Deploy necessary technical solutions for data classification, retention management, and secure deletion.
   - Establish a monitoring and auditing mechanism to ensure compliance with the policy.
3. **Review and Update**
   - Regularly review and update the policy to reflect changes in regulations, business processes, and technology.
   - Conduct periodic audits to assess the effectiveness of the policy and make improvements as needed.

8. Conclusion

A robust data deletion and retention policy is essential for managing the lifecycle of data within an organization. It ensures compliance with regulatory requirements, enhances data security, optimizes storage management, and improves operational efficiency. By implementing best practices and regularly reviewing the policy, organizations can effectively manage their data assets and mitigate risks associated with data retention and deletion