©(ORGANISATION NAME)

DISPOSAL (data and asset) POLICY

Subject: Disposal (data and asset) Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 16	Authorised by:
Effective Date: June, 2024	Version 1.0	Next Review:

Author	Signature	Date
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this

document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

CONTENTS

1.0 OVERVIEW

Organisation's disposal policy ensures the secure and responsible handling of data and assets at the end of their lifecycle. By outlining clear procedures for data erasure and asset disposal, we minimise the risk of data breaches, protect sensitive information, and comply with relevant regulations. This policy covers the secure deletion of data from electronic devices, the physical destruction of storage media, and the environmentally friendly disposal of obsolete equipment. We prioritise data security and environmental sustainability in all disposal practices to maintain trust with our stakeholders and protect our Organisation's reputation.

1.1 RISKS ADDRESSED

The risks associated with insecure disposal of data and assets can be significant and far-reaching. Here are some of the major risks:

Reference	Description of Risk
SAFETag	Data breaches
SAFETag	Privacy violations
SAFETag	Identity theft
SAFETag	Intellectual property theft
SAFETag	Environmental hazard
SAFETag	Reputational damage
SAFETag	Unauthorised access

2.1 PURPOSE

The purpose of this policy is to provide guidelines for the proper or secure disposal of data and assets containing sensitive or confidential information. This policy aims to minimise the risk of unauthorised access, data breaches, identity theft, privacy violations, and ensure compliance with relevant laws and regulations.

1.2 OBJECTIVES

The objectives of this policy include:

- Ensuring that all sensitive information is securely erased or destroyed to prevent unauthorised access and data breaches.
- Meeting legal and regulatory requirements for data protection and disposal, such as GDPR, HIPAA, or other industry-specific regulations.
- Reducing the risk of data leakage or loss by implementing secure disposal practices for all assets.

- Optimising resource use by safely disposing of obsolete or unused assets, reducing storage costs and environmental impact.
- Minimising the environmental impact of disposal by recycling or disposing of assets in an environmentally friendly manner.
- Safeguarding the Organisation's reputation by ensuring that data and assets are disposed of responsibly, maintaining trust with customers, partners, and stakeholders.
- Reducing costs associated with storing and managing unused or obsolete assets by disposing of them in a timely and efficient manner.
- Educating employees about the importance of proper data and asset disposal to ensure compliance and reduce the risk of accidental data breaches.

1.3 SCOPE

This policy applies to all systems, people and processes that constitute the Organisation's information systems, including board members, directors, employees, suppliers and other third parties who handle or have access to the Organisation's data and assets.

1.4 RELATED DOCUMENTS

The following policies and procedures are relevant to this document:

- Data Classification Policy
- Information Security Policy
- Asset Management Policy

2. DATA CLASSIFICATION

2.1 DEFINITION OF DATA

Data is a fundamental component of information systems and plays a crucial role in decision-making processes, scientific research, business operations, and many other domains. Data can be raw (unprocessed) or processed, structured or unstructured, and can be generated from various sources, such as sensors, databases, transactions, social media, or user interactions.

2.2 DATA CLASSIFICATION

Data classification is the process of categorising data based on its level of sensitivity, criticality, or importance to an organisation. It helps organisations identify and protect their most valuable data assets while ensuring compliance with relevant regulations and industry standards.

Common data classification levels include:

- **Public/Unrestricted:** Data that can be freely shared with the public or external parties.
- **Internal/Confidential:** Data intended for internal use only and considered sensitive within the Organisation.
- **Restricted/Highly Confidential:** Data with strict access controls and handling procedures due to its criticality or legal requirements.

2.3 DATA REMANENCE

Data remanence, also known as data remnants or residual data, refers to the residual representation of data that remains on a storage medium or device even after the data has been deleted or the device has been erased. This residual data can potentially be recovered and accessed by unauthorised parties, posing a significant security risk.

Data remanence can occur for various reasons:

- Ineffective data erasure: Many standard deletion methods, such as file deletion or formatting a drive, do not actually remove the data from the storage medium. Instead, they simply remove the pointers or references to the data, leaving the actual data intact on the physical medium.
- Partial overwrites: In some cases, data may be partially overwritten during an update or modification process, leaving remnants of the original data on the storage medium.
- Remapping: Modern storage technologies, such as solid-state drives (SSDs), employ remapping techniques to extend the lifespan of the storage medium. These mechanisms can cause data remnants to be scattered across different physical locations on the drive, making complete erasure more challenging.
- Cached or temporary data: Operating systems, applications, and devices often create temporary or cached copies of data to improve performance or enable recovery in case of system failures. These temporary copies may inadvertently contain sensitive data remnants.

Data remanence poses significant risks, particularly when sensitive or confidential information is involved. If storage media or devices containing data remnants fall into the wrong hands, the residual data can be recovered and potentially misused, leading to data breaches, identity theft, intellectual property theft, or other security incidents.

3. SECURE DATA AND ASSET DISPOSAL

The disposal of data and assets refers to the secure and permanent removal or destruction of electronic data, physical documents, and hardware assets that are no longer needed or have reached the end of their useful life within an Organisation.

3.1 DATA DISPOSAL

Data disposal involves the permanent and irreversible erasure or destruction of electronic data stored on various media, such as hard drives, solid-state drives (SSDs), tapes, CDs, DVDs, and other storage devices. This process ensures that sensitive or confidential information cannot be accessed or recovered by unauthorised individuals or entities.

The following must be taken into consideration:

a. All electronic data containing sensitive or confidential information must be securely wiped or overwritten using industry-standard data erasure methods before disposal of the storage media.
b. Physical documents containing sensitive or confidential information must be shredded or otherwise rendered unreadable before disposal.
c. Data disposal must be carried out in a manner that ensures the complete destruction of the data, making it unrecoverable.

3.2 ASSET DISPOSAL

Asset disposal refers to the secure removal and disposal of hardware assets, such as computers, servers, printers, mobile devices, and other equipment that may contain sensitive data or intellectual property. This process ensures that confidential information stored on these devices is securely erased or destroyed before the assets are recycled or disposed of.

The following must be taken into consideration:

a. All assets containing data storage components (e.g., computers, servers, mobile devices, removable media) must be securely wiped or overwritten before disposal.
b. Asset disposal must be coordinated with the IT department to ensure proper data sanitization and asset tracking.
c. Assets containing sensitive or confidential information must be disposed of through Authorised channels or vendors that provide secure asset disposal services.

3.3 METHODS FOR DATA AND ASSET DISPOSAL

The following are common methods for data and asset disposal:

- Data erasure or wiping: Using specialised software or hardware tools to overwrite data on storage media multiple times, making it unrecoverable.
- Degaussing: Applying a strong magnetic field to storage media, effectively erasing, or scrambling the data stored on magnetic media like hard drives and tapes.

- Physical destruction: Physically destroying the storage media and asset through shredding, crushing, or disintegration, rendering the data unrecoverable.
- Data sanitization: Securely erasing or overwriting data stored on the asset's storage media using approved data erasure methods.
- Secure recycling or disposal: Working with trusted third-party vendors or Organisations that specialise in secure asset disposal and recycling, ensuring proper data sanitization and environmentally disposal practices.

The disposal of data and assets is a critical aspect of information security and data protection. It helps Organisations maintain compliance with data privacy regulations, protect sensitive information from unauthorised access or misuse, and mitigate the risks associated with data breaches and cyber threats.

3.4 PROCEDURES FOR IDENTIFYING DATA AND ASSETS REQUIRING DISPOSAL

a. Asset Inventory Review: Regularly review the Organisation's asset inventory to identify assets that have reached the end of their useful life or are no longer needed. Consider factors such as asset age, obsolescence, maintenance costs, and Organisational changes that may necessitate asset disposal.

b. Data Retention and Disposition Policies: Implement and follow data retention and disposition policies that define the lifecycle of data, including when data should be disposed of or archived.
   Review data repositories, backups, and storage systems to identify data that has reached the end of its retention period and is eligible for disposal.

c. Data Classification and Risk Assessment: Conduct data classification exercises to identify sensitive or confidential data that requires secure disposal.
   Assess the potential risks associated with retaining or improper disposing of sensitive data.

d. Business Process Reviews: Review business processes and workflows to identify potential sources of data or assets that may require disposal. Involve stakeholders from various departments (e.g., IT, finance, human resources, legal) to ensure comprehensive identification.

e. Regulatory and Compliance Requirements: Monitor and adhere to relevant industry regulations, data protection laws, and compliance requirements that may mandate the secure disposal of certain types of data or assets.

f. Change Management Processes: Integrate asset and data disposal considerations into the Organisation's change management processes, such as system upgrades, office relocations, or Organisational restructuring. Ensure that data and assets are properly identified and disposed of during these changes.

g. Employee Reporting and Feedback: Encourage employees to report assets or data that they believe should be considered for disposal.
Establish channels for employees to provide feedback and report potential risks or concerns related to data and asset disposal.

h. Regular Audits and Assessments: Conduct regular audits and assessments to identify any data or assets that may have been overlooked or require disposal due to changing circumstances.

4. PROCEDURES FOR SECURE DATA AND ASSET DISPOSAL

4.1 STEP-BY-STEP PROCEDURES FOR SECURE DATA DISPOSAL

- Identify and classify the data to be disposed of (e.g., sensitive, confidential, or public).
- Determine the appropriate disposal method based on the data classification and applicable regulations (e.g., secure wiping, degaussing, physical destruction).
- Obtain approval from the relevant authority (e.g., data owner, information security team) for data disposal.
- Ensure that the data is stored securely, and access is restricted during the disposal process.
- Use approved and secure data erasure tools or methods to render the data unrecoverable.
- Verify the successful disposal of the data through auditing and testing.
- Document the data disposal process, including the date, method used, and the personnel involved.
- Dispose of any physical media or documents containing the data in a secure manner (e.g., shredding, incineration).

4.2 STEP-BY-STEP PROCEDURE FOR SECURE ASSET DISPOSAL:

- Identify the assets to be disposed of (e.g., computers, servers, mobile devices, storage media).
- Determine if the assets contain sensitive or confidential data.

- Obtain approval from the relevant authority (e.g., asset owner, IT department) for asset disposal.
- Securely backup and migrate any necessary data from the assets to be disposed of.
- Use approved and secure data erasure tools or methods to wipe or overwrite the data on the assets.
- Verify the successful data erasure through auditing and testing.
- Document the asset disposal process, including the date, method used, and the personnel involved.
- Disassemble or physically destroy the assets to prevent unauthorised access or reuse.
- Dispose of the assets through authorised channels or vendors that provide secure asset disposal services.

4.3 BENEFITS OF SECURE DATA AND ASSETS DISPOSAL

The benefits of secure data and assets disposal include the following:

- Data Protection: Secure disposal methods, such as data erasure, degaussing, or physical destruction, ensure that sensitive information is rendered unrecoverable, protecting against data breaches and unauthorised access.
- Compliance Assurance: Adhering to secure disposal practices helps Organisations maintain compliance with relevant regulations and industry standards, avoiding costly penalties and legal issues.
- Reputation and Trust: By demonstrating a commitment to data protection and secure disposal practices, Organisations can enhance their reputation, build customer trust, and maintain positive business relationships.
- Intellectual Property Protection: Secure disposal of assets and data safeguards an Organisation's intellectual property, trade secrets, and proprietary information, protecting its competitive advantage and business interests.
- Risk Mitigation: Effective disposal practices mitigate the risks associated with data breaches, cyber-attacks, and legal liabilities, reducing the potential for financial losses, operational disruptions, and reputational damage.
- Environmental Responsibility: Proper disposal of electronic assets and media devices can contribute to an Organisation's sustainability efforts and reduce environmental impact through responsible recycling and disposal practices.

4.4 ESTABLISHED GUIDELINES FOR SECURE DATA AND ASSETS DISPOSAL

1. Data Classification and Inventory:
   - Implement a data classification policy and maintain an up-to-date inventory of all data and assets containing sensitive or confidential information.
   - Clearly identify the data and assets that require secure disposal based on their classification level.
2. Access Controls:
   - Restrict access to data and assets scheduled for disposal to Authorised personnel only, preventing unauthorised access or tampering.
3. Data Sanitization:
   - Use approved and secure data sanitization methods to permanently remove or overwrite data from storage media before disposal or reuse.
   - Common methods include secure data wiping/overwriting, degaussing (for magnetic media), and cryptographic erasure.
4. Physical Destruction:
   - For assets or media that cannot be securely sanitised, physically destroy them through shredding, crushing, or disintegration to render the data unrecoverable.
   - Ensure proper handling and disposal of any resulting debris or waste materials.
5. Chain of Custody:
   - Establish a documented chain of custody processes to track and account for the movement and handling of assets and data throughout the disposal process, from collection to final destruction.
6. Verification:
   - Verify the successful erasure of data through auditing, testing, or obtaining certificates of destruction from Authorised disposal vendors.
7. Vendor Management:
   - If outsourcing disposal services, thoroughly vet and monitor third-party vendors to ensure they follow industry standards and your organisation's disposal requirements.
   - Obtain certificates of destruction and maintain audit trails for all outsourced disposal activities.
8. Secure Storage and Transportation:
   - Ensure that assets and data awaiting disposal are securely stored and access is restricted to Authorised personnel only, preventing unauthorised access or tampering.

- Implement secure transportation procedures for assets and data being moved to disposal facilities.

9. Environmental:
   - Consider environmentally responsible disposal methods, such as recycling or sending electronic waste to certified e-waste facilities for proper handling and disposal.
   - Comply with applicable environmental regulations and best practices.
10. Policy and Procedure Documentation:
    - Develop and maintain comprehensive policies and procedures for data and asset disposal.
    - Regularly review and update these policies and procedures to align with changing regulations and industry best practices.
11. Employee Training and Awareness:
    - Provide regular training and awareness programs for employees and contractors on secure disposal practices, emphasising the importance of data protection and their roles and responsibilities.
    - Ensure that all personnel involved in the disposal process are adequately trained and follow established procedures.
12. Disposal Logs and Records:
    - Maintain detailed logs and records of all disposal activities, including dates, methods used, personnel involved, and verification details.
13. Auditing and Monitoring:
    - Implement auditing and monitoring processes to verify the effectiveness of disposal practices, identify areas for improvement, and ensure compliance with policies and regulations.
    - Conduct regular audits and assessments of disposal activities and maintain detailed records for audit trails.

By following these established guidelines, Organisations can effectively mitigate the risks associated with improper data and asset disposal.

5. MOBILE DEVICE MANAGEMENT (MDM) SOLUTION

Mobile Device Management (MDM) is a solution that allows Organisations to securely manage, and control mobile devices used by employees, contractors, or other authorised users. MDM provides a centralised platform for managing and securing a wide range of mobile devices, including smartphones, tablets, and other portable devices.

5.1 BENEFITS OF MOBILE DEVICE MANAGEMENT

Having a Mobile Device Management (MDM) solution operating in an Organisation provides several benefits:

1. Enhanced Data Security and Privacy:
   - MDM enables Organisations to enforce security policies, such as device encryption, password requirements, and remote wipe capabilities, protecting sensitive data on mobile devices.
   - It helps prevent data leaks by controlling app installations, network access, and content sharing from managed devices.
2. Centralised Device Management:
   - MDM allows Organisations to maintain an accurate inventory of mobile devices, track their locations, and manage their lifecycle from deployment to retirement.
   - MDM enables remote device management, including locking, wiping, or locating lost or stolen devices, protecting sensitive data and assets.
   - It facilitates remote configuration, software updates, and app distribution, ensuring devices are up-to-date and consistently configured.
3. Increased Productivity and Efficiency:
   - By enforcing standardised configurations and enabling centralised app distribution, MDM streamlines mobile device provisioning and management, reducing IT overhead.
   - It ensures that employees have access to the necessary apps and resources on their mobile devices, enhancing productivity and mobility.
   - MDM solutions can separate personal and corporate data and apps, enabling secure bring-your-own-device (BYOD) policies and reducing the need for dedicated corporate devices.
4. Cost Savings and Risk Mitigation:
   - Effective mobile device management through MDM can reduce the costs associated with data breaches, regulatory fines, and legal liabilities.
   - It helps mitigate risks related to lost or stolen devices, unauthorised access, and malware infections, which can result in significant financial and reputational damage.
   - MDM enables better control over mobile device expenses and usage, optimising resource allocation and reducing unnecessary costs.
5. Integration and Unified Management:
   - MDM solutions often integrate with other security and management platforms, such as identity and access management (IAM), unified endpoint management (UEM), and mobile threat defence (MTD).

6. RECOMMENDATIONS/ADVISORY ON DISPOSAL (DATA AND ASSET)

Organisations with 1 – 5 Employees	Organisations with 6 – 20 Employees	Organisations with more than 20 Employees
• Physical documents should be destroyed using a document shredder. • Use a hard drive shredder or degausser to physically destroy storage media (hard drives, SSDs, USB drives). • Before disposing of devices, use cloud backup solutions (OneDrive, Google Drive etc.) to securely back up critical data off-site. • Devices to be disposed of should be physically destroyed. i.e., punctured. • Maintain an inventory of all devices/assets. • Conduct regular training for employees on importance of data security and secure data and assets disposal. • Use Find My Device (Android) built in features to remotely locate, lock and	• Physical documents should be destroyed using a document shredder. • Use a hard drive shredder or degausser to physically destroy storage media (hard drives, SSDs, USB drives). • Ensure device formatting before disposal. • Devices to be disposed of should be physically destroyed. i.e., punctured • Maintain an inventory of all devices/assets. • Implement on-premises backup solutions like network-attached storage (NAS) devices or local server backups to securely backup critical data before disposal. • Adopt cloud-based Mobile Device Management (MDM) solutions: Services like Microsoft Intune, ManageEngine MDM or On-Premises MDM solutions like Microsoft Endpoint Manager or VMware Workspace One • Conduct regular training for employees on importance of data	• Deploy a company-wide device management solution. • Maintain an inventory of all devices/assets. • Implement on-premises backup solutions like network-attached storage (NAS) or Cloud cack-up solutions to securely backup critical data before disposal. • Outsource asset disposal and data destruction to certified third -party service providers who specialised in secure data destruction. • Adopt cloud-based Mobile Device Management (MDM) solutions: Services like Microsoft Intune, ManageEngine MDM OR On-Premises MDM solutions like Microsoft System Center Configuration Manager (SCCM) or Cisco Meraki Systems Manager • Conduct regular training for employees on importance of data security and secure data and assets disposal.

erase data from lost or stolen devices. • Adopt cloud-based Mobile Device Management (MDM) solutions: Services like Microsoft Intune, ManageEngine MDM.	security and secure data and assets disposal	

If you have any questions about the above policy, please contact the IT Manager or Head of IT.