Secure Disposal of Sensitive Information

BITS Technology Group Pty Ltd

Action	Name	Title
Prepared By	Muhammad Nauman Mustafa	Cyber Security Engineer
Reviewed By	Esther Mangelsdorf	General Manager
Approved By	Bernard Mangelsdorf	Chief Executive Officer

Version	Date	Description of Change	Updated By
1.0	10 May 2025	Initial Policy Creation	Muhammad

1. Purpose

This policy outlines the procedures for the secure disposal of physical and digital media that contain sensitive, private, or confidential information. The goal is to prevent unauthorized access, data breaches, and ensure compliance with data protection regulations.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who handle or manage sensitive information in any form—physical or digital—on behalf of the organization..

3. Responsibility

- Service Department: Ensure secure disposal tools and services are available and maintain records of destruction.
- Employees: Follow disposal procedures and report any incidents of improper disposal.
- Management: Provide training and enforce compliance with this policy.

4. Physical Document Disposal

- All physical documents and records containing sensitive, private, or confidential information must be securely destroyed when no longer needed.
- Destruction must be carried out using a cross-cut document shredder.

5. Digital Media Disposal

- All computer devices and external storage media (e.g., USB drives, external hard drives, CDs, DVDs, backup tapes) that have stored sensitive data must be disposed of securely.
- Acceptable methods include (in case of device has to be disposed of):
    - Use of a certified external service provider specializing in secure media destruction (refer to Documents - Hardware Disposal).
- If devices are to be reused, sold, or donated:
    - All storage media must be removed or securely wiped using non-recoverable data destruction methods such as Kill Disk.
    - Verification of data destruction must be performed and documented.

6. Compliance

This policy will be reviewed annually or upon significant changes to relevant laws, regulations, or organizational practices.

This policy must be readily available to all the relevant employees. It will be accessible through the company's document management portal, and during onboarding sessions. Employees are encouraged to review the policy regularly and stay informed about any updates as compliance to this policy is mandatory.