RenovaTech – Data Destruction Policy

Version: 1.0
Last Updated: November 2025
Location: Victoria, Australia

1. Purpose

The purpose of this Data Destruction Policy is to outline RenovaTech's commitment to secure, compliant, and fully auditable data destruction processes. This policy ensures that all data-bearing devices handled by RenovaTech are sanitised or destroyed in accordance with Australian laws and industry best practices.

2. Scope

This policy applies to:

- All data-bearing IT assets received from clients
- All RenovaTech employees, technicians, and contractors
- All secure transport, storage, destruction, refurbishment, and recycling activities
- All facilities, equipment, and tools used in the destruction process

Devices covered include (but are not limited to): laptops, desktops, servers, hard drives, SSDs, mobile devices, tablets, network equipment, storage appliances, and removable media.

3. Compliance Standards

RenovaTech complies with all relevant data protection and destruction standards, including:

- **Privacy Act 1988 (Cth)**
- **Australian Privacy Principles (APPs)**
- **NIST Special Publication 800-88 – Guidelines for Media Sanitisation**
- **AS/NZS 5377:2013 – E-Waste Management Standard**
- **Environment Protection Act 2017 (VIC)** (for materials disposal)

These standards guide all technical, procedural, and administrative controls within our data destruction processes.

4. Approved Data Destruction Methods

4.1 Software-Based Data Erasure

Where devices are functional, RenovaTech uses certified data wiping tools such as:

- Blancco
- KillDisk
- Active@ Wipe
- Or equivalent industry-standard software

These tools meet or exceed **NIST 800-88 Clear/Purge** requirements.

The process includes:

- Overwriting existing data with secure wipe patterns
- Verification of wipe completion
- Logging of device identifiers (e.g., serial numbers)
- Issuing a Certificate of Data Destruction to the client

4.2 Physical Destruction

Physical destruction is used when:

- A device is non-functional
- Software wiping fails
- A client requests full physical destruction
- Destruction is required by law or contract

Accepted destruction methods include:

- Hard drive shredding
- Crushing or disintegration
- Degaussing (for magnetic media)

Physical destruction renders the device and its stored data permanently unrecoverable.

4.3 Verification Procedures

After software wiping or physical destruction:

- A technician verifies that the destruction process is complete
- Device identifiers (serial numbers, asset tags) are confirmed
- All actions are logged in the destruction record
- The destruction report is prepared for the client

5. Chain of Custody Controls

RenovaTech maintains a secure, documented chain of custody for all data-bearing devices:

- Devices are tagged upon collection
- Asset details are logged (model, type, serial number where available)
- Transport containers are locked or sealed
- Movement is tracked from pickup to destruction
- Devices are checked in upon arrival at the facility
- Discrepancies are escalated immediately

A complete audit trail is maintained for every asset.

6. Secure Storage Requirements

Before destruction or wiping occurs, all devices are stored in secure, controlled areas:

- Restricted-access rooms
- CCTV-monitored zones
- Locked cages for sensitive devices
- Alarm-protected facilities
- Optional tamper-evident seals for high-security assets

Only authorised staff may enter secured storage areas.

7. Staff Security Requirements

All RenovaTech personnel involved in handling data-bearing devices must:

- Hold a valid police background check
- Sign confidentiality and non-disclosure agreements
- Complete training in secure handling, chain of custody, and destruction procedures
- Follow internal security policies at all times

Staff are prohibited from accessing, viewing, or attempting to recover client data.

8. Documentation & Reporting

Upon completion of the destruction process, RenovaTech provides clients with:

- Certificate of Data Destruction

- List of devices processed, including serial numbers where available
- Destruction method used (wipe / shred / crush / degauss)
- Name of technician responsible
- Date and time of destruction
- Supporting logs (if required for audits)

All documentation is retained in accordance with regulatory and internal retention requirements.

9. Incident Response

In the event of a suspected or confirmed issue involving a data-bearing asset, such as:

- Unlogged assets
- Transport delays
- Broken seals
- Potential tampering
- Storage irregularities

RenovaTech will:

1. Immediately secure and isolate affected assets
2. Notify the Security & Compliance team
3. Conduct a full internal investigation
4. Document all findings and corrective actions
5. Inform the client where required by law or contract

10. Review & Continuous Improvement

This policy is reviewed:

- Annually
- When legal or regulatory requirements change
- When RenovaTech expands operations
- When new technologies or industry standards emerge

Feedback is encouraged to continually strengthen data security practices.

11. Contact Information

For questions regarding this Data Destruction Policy or to request supporting documentation:

RenovaTech – Data Security Office
Email: security@renovatech.com.au
Phone: 1300 RENOVA
Victoria, Australia