Data Erasure process description – CHG-MERIDIAN UK

ISO 9001 / ISO 27001 certified and compliant data erasure process

1. Transport of equipment to the processing centre

The equipment is transported by the customer to the designated CHG-MERIDIAN UK processing facility or to an approved partner facility, Tier 1, at the customer's own expense and risk.

At the customer's request, CHG-MERIDIAN can arrange secure collection and transport via an approved logistics partner under a separate agreement.

Following receipt and inspection, the customer will receive confirmation of the number of units accepted.

2. Receipt and documentation of assets

Unpacking and recording of each asset is based on the serial number.

Tier1 endeavours to capture the serial and asset number for each device. Where this information is missing or cannot be identified, the asset will still proceed through the Blancco erasure process and the relevant details will be captured and updated during the testing phase.

Each documented asset is assigned a unique identifier, typically via barcode labelling, ensuring full traceability throughout the process.

3. Preparation of the erasure process

The asset barcode is scanned and registered within the Blancco system, creating a database entry and ensuring full traceability throughout the process.

The barcode is directly linked to the Blancco erasure report. The technician performing the process is also identified within the report through their initials, providing clear accountability and auditability for each processed asset.

4. Visual inspection of assets

An operator inspects each asset and, where technically possible, opens the device to identify all data-bearing components.

This ensures that no hidden or additional storage media are missed. Removable media such as SIM cards, CDs or memory cards are also checked.

CHG-MERIDIAN UK Limited
65 High Street,
Egham, Surrey
TW20 9EY, UK

Any media found is securely stored and processed in line with the destruction procedure if required.

5. Booting and system access

Assets are started using a secure boot environment. The erasure software is then initiated to control the process.

Only successfully registered assets proceed further. If registration fails, the process is stopped and flagged for review.

5.1 Pre-classification of printing devices

Where applicable, status pages are printed and attached to the device. Key information such as manufacturer, model and serial number is recorded.

5.2 Reset of printing systems

Printing devices are reset to factory settings, and any stored data such as address books or configurations is deleted.

If this is not possible, the device is marked for secure destruction.

6. Identification of storage media

The erasure software automatically identifies the type of storage media, including HDD, SSD, hybrid and flash memory.

This ensures the correct erasure method is selected based on the media type.

7. Erasure method

The client determines the required level of data protection and the corresponding erasure approach.

For standard and higher protection requirements, data erasure is performed using certified software solutions, including Blancco, which is widely recognised and compliant with international and UK standards.

Blancco enables secure overwriting of data across different storage media types and generates a tamper-proof audit trail for each erasure process, including detailed reporting and verification logs.

The process is managed and monitored throughout, ensuring:

- the correct erasure method is applied based on media type
- all erasure events are recorded
- full traceability and reporting is maintained

For the highest protection requirements, data carriers are physically destroyed in accordance with DIN 66399 standards.

8. Audit of the erasure result

After completion, an automated check verifies that:

- an erasure log exists
- the erasure has been completed successfully without errors

If errors occur, the process is repeated or escalated to destruction if required.

9. Documentation of the erasure process

Erasure reports are made available to the customer following completion and verification.

These reports include full details of the process and are securely stored, with backups maintained in separate locations.

10. Treatment of non-erasable media

Storage media that cannot be securely erased are removed where possible and recorded within the system.

They are securely stored and then destroyed by certified partners such as Tier 1, in line with DIN 66399 requirements.

All destruction activities follow strict control procedures and are fully documented.

11. Access to erasure information

Customers can access erasure reports and certificates at any time via tesma or receive them directly from CHG-MERIDIAN.

All documentation is retained in line with compliance requirements and can be retrieved when needed.

CHG-MERIDIAN UK Limited
65 High Street,
Egham, Surrey
TW20 9EY, UK