eraSURE® plus PROCESS DESCRIPTION
ISO 9001 / 27001 certified and BSI IT baseline compliant data erasure in accordance with component B1.15

VERSION 19.06 (June 2019)

1. Inventory of systems registered for collection

The documentation of equipment occurs on location by the client using a mobile data capture station. After complete documentation the systems are either packed into lockable roller containers or sealable boxes, or loaded onto a sealable truck.
The client shall receive verification of all documented equipment including reference number, serial number, manufacturer, asset class and seal number.

For remote locations with a small amount of returnable equipment, CHG-MERIDIAN may use a parcel service. The client shall receive a secure transport container (e.g. Rimova case) that can be locked. The client consigns the container with the hardware to the parcel service. CHG-MERIDIAN receives the shipment number and tracks the transport route of the container.

2. Transport of equipment to the Technology and Service Center

CHG-MERIDIAN AG uses selected carriers for sealed transport with GPS-tracked and protected transport of IT hardware in shockproof containers on air suspension trucks. The equipment is directly transported to the CHG Technology and Service Center.

3. Receipt of goods and documentation of equipment by CHG-MERIDIAN

After review of the seal number, the equipment is taken directly to the security area and recorded as incoming equipment with an actual/target comparison. Unpacking and recording of the individual equipment is based on the equipment serial number. Documented equipment receives a barcode label with a clear CHG stock ID and the equipment serial number.

4. Preparation of the erasure process

Each test station has its own identification number. The barcode on the equipment label and the test station number are scanned on a console using a barcode reader and registered. The registration creates a database entry that authorizes the registration.

5. Visual inspection of the equipment to be erased

Insofar as this is technically possible, an employee will inspect the equipment by opening the housing. This is dependent on the housing construction and the standard purpose of use. Housing that is glued or riveted closed, or otherwise sealed and/or not intended to be opened, shall remain unopened. This inspection ensures, as far as possible, that there are no unconnected, raid-configured or otherwise inaccessible data carriers in the equipment.

CD and disk drives, as well as slots for SIM and memory cards are also checked for relevant media.
Any media found is, unless otherwise agreed with the client, securely stored and destroyed in accordance with Clause 10.

6. Booting and network connection

The equipment to be processed (excluding printing systems) is launched with a suitable boot media. Then the software that will guide the processing is launched. The process is only continued after successful login as described in Clause 3.
In any other case there will be a detailed visual error message.

6.1. Pre-classification of printing systems

Where possible, when it comes to printing systems the status pages are printed out and attached to the equipment for further work steps.
The system reviews the registered equipment and reads the (core) characteristics such as manufacturer, model, serial number and counter readings. It is also determined whether it is possible to reset this device to factory settings and whether this has already been done.

6.2. Review and factory reset for printing systems

The equipment is reset to factory settings and any address books or configurations are deleted. This process is reviewed and identified in the system as a status.
If this reset to factory settings and associated erasure of address books and/or configurations is not possible then the erasure process must be viewed as unsuccessful and the system earmarked for destruction as outlined in Clause 10.

If the equipment has built-in exchangeable / removable storage media (mechanical hard drives, hybrid or SSD storage) then these are removed. These also receive a barcode label with a clear CHG stock ID that allows the storage media and the equipment to be clearly assigned to one another. The storage media to be processed is connected to a special test computer. Then the software that will guide the processing is launched. The process is only continued after successful login. In any other case there will be a detailed visual error message.
If the hard drive is locked with a device-specific password by the manufacturer or user, and this is not known to CHG or cannot be removed, then the hard drive will be destroyed as outlined in Clause 10.

7. Automatic recognition of the storage media type

A data carrier test automatically determines the storage media type. The data carrier test distinguishes between the following storage media types: Mechanical hard drive, SSD, hybrid and flash drives. The current technology does not allow secure erasure of hybrid hard drives, and they are therefore destroyed in accordance with Clause 10.

8. Erasure method

The client decides on the respective data protection needs and, based on this, the form of data erasure. For normal and higher protection needs the data carriers or equipment can be erased in accordance with BSI IT baseline protection B1.15. For the highest level of protection needs, the BSI IT baseline protection recommends complete destruction in accordance with DIN 66399.

7.1 Normal protection needs

For control programs a database query determines which type of erasure (mechanical / SSD / flash) must be implemented, and starts an appropriate erasure method.
A console monitors the client during erasure. All erasure incidents (defective sectors, progress messages, erasure logs etc.) are saved in a database.

CHG-MERIDIAN AG
Franz-Beer-Strasse 111
88250 Weingarten
Germany

Tel +49 751 503-0
Fax +49 751 503-66
info@chg-meridian.com
www.chg-meridian.com

Board of Management
Dr. Mathias Wagner (Chairman of the Board)
Frank Kottmann, Joachim Schulz, Oliver Schorer

Chairman of the Supervisory Board
Jürgen Mossakowski
Court of Registration
Ulm HRB 551857

7.2 Higher protection needs

The erasure process occurs as outlined in Clause 7.1, under consideration of the notes described below

Depending on the encryption type and implementation of erasure instructions by the SSD, hybrid or flash storage units of respective manufacturers there may be the residual risks listed below that data or data fragments can be restored after erasure has taken place:

- If an SSD is not encrypted then the data moved to it will be saved in plain text in the storage modules. Erasure instructions in SSDs that aim to guarantee complete erasure of such content are not always adequately reliable. Thus it needs to be expected that SSDs will still contain data after application of ATA erasure instructions. An attacker could make use of this by removing the storage module from the device and reading it with an external electronic device.
- In the case of hardware encryption the user data is encrypted before storage by the SSD itself with a private key generated in the hardware of the SSD and stored on the SSD. The erasure begins with erasure of this key. Any data that remains on the SSD after erasure is worthless to an attacker as it can only be decrypted with a lot of effort. It would be necessary to replicate the decryption mechanism of the SSD and carry out a brute force attack to determine the key.
- In software encryption the encryption is managed by the device that the SSD is integrated into. The key is created by the encryption program on the device and stored there. Data that remains on the SSD after erasure could be read using knowledge of the encryption program and the key. To do this it would be necessary to replicate the decryption mechanism of the device program and read the key from the computer memory.

7.3 Highest protection needs

If the highest level of protection needs is required then an additional agreement with the client is required for destruction of the respective data carriers or systems in accordance with Clause 10.

9. Audit of the erasure result

After erasure there is an automatic check that:

- an erasure log exists
- the erasure log shows error-free erasure

In the event that an error occurred, the process will be restarted after troubleshooting or the data carrier will be set aside as “not secure for erasure” and processed in accordance with Clause 10.

10. Documentation of the erasure process

The erasure log will be made available to the client after completed erasure and audit in accordance with Clause 11.
There is at least one backup, which is kept in a different physical location.

11. Special treatment of non-rewritable storage media and printing systems

Storage media that emerge from this process as “not secure for erasure” or cause an error in the process are treated by the employee handling the equipment (e.g. reconnected, formatted, configured in the BIOS, installed into a different PC) to attempt successful completion of the erasure process starting with Clause 3.
If this is not possible, e.g. due to a hardware defect or other access restrictions, or it is commissioned as such, the storage media will be removed if possible. If removal is not possible, the complete device will undergo the following process.

- Mechanical hard drives will be degaussed and then shredded after a waiting period of 6 weeks.
- SSD, hybrid and flash storage media will be stored in a sealed aluminum box.
- These stored storage media are shredded at short, regular intervals by a certified specialist disposal firm (in accordance with DIN 66399, protection class 2, security level E4) and the residual particles then thermally destroyed.
- The disposal occurs according to the “four eyes” principle and is confirmed with a signature from both sides.

If desired by the client, non-erasable storage media can instead be returned.

All physical storage media to be erased is stored in the security area. After removal it is recorded in the CHG-MERIDIAN warehouse system and receives a reference number (Stock ID). This is linked to the original serial number of the device, so that allocation is always possible.

If the client wants all storage media that is “not secure for erasure” to be sent back, the storage media will be sent back to them in a separate order in sealed transport container. The client will receive a list via email of all the storage media being returned and the seal number. Shipment to the client will be carried out by a parcel service.

12. Retrieval and dispatch of erasure information

If the client uses TESMA® then the erasure information can always be retrieved via TESMA® in the “End of Life” module under “Erasure log search”, viewed as a PDF and downloaded. If the client doesn’t use TESMA® then CHG-MERIDIAN shall send the client the erasure information or logs by email or by posting a CD. The document name is generally the serial number of the device that the hard drive came from.
If required and in individual cases, a client that uses TESMA® can retrospectively request logs via email or CD. The data is saved on the CHG-MERIDIAN file server and can be retrieved at any time. The erasure logs are stored for at least two years after implementation of the erasure process.