VERSION 22.11 (November 2022)

1. Inventory of assets registered for collection
The inventory is carried out according to the dual control principle by a representative of the client and the transport company. The assets are captured on site at the client's location using a mobile data capture terminal. After complete capturing, the assets are either packed into lockable roll containers or lockable boxes or loaded onto a lockable truck. In addition to the inventory of the assets, comments on the transport order can also be recorded. The seal number is recorded on the shipping document. As part of his duty to cooperate, the client must finally check the transport order and the sealing of the assets. The handover is then acknowledged together with the carrier directly at the data collection terminal. In the rare case of an issue with the data terminal the handover will be acknowledged by signing the shipping documents.
The client then receives an e-mail with all registered assets including transport order number, serial number, manufacturer and assets class.

2. Transport of assets to the Technology and Service Center
CHG-MERIDIAN AG uses approved carriers for the sealed, GPS-monitored and secure transportation in shock-proof containers and air-suspended trucks. The assets are directly transported to the CHG Technology and Service Center, Wasserweg 2, 64521 Groß-Gerau, Germany. A listing of the currently approved subcontractors can be found at https://www.chg-meridian.de/eraSURE_subcontractors.

3. Receipt and documentation of assets by CHG-MERIDIAN
After review of the seal number, the assets are moved directly to the secure area and recorded as incoming assets with an actual/target comparison. If discrepancies are found in the seal number or in the comparison, a multi-stage escalation process is started immediately. Unpacking and recording of the individual assets is based on the assets serial number. Documented assets receives a barcode label with a clear CHG stock ID and the assets serial number.

4. Preparation of the erasure process
Each dedicated test station has its own identification number. The barcode on the assets label and the test station number are scanned on a console using a barcode terminal and registered. The registration creates a database entry that authorizes the registration. This ensures that it is always possible to trace which assets were processed at which test station.

5. Visual inspection of the assets to be erased
An employee checks the assets; if technically possible, he opens the housing for this procedure. This is done depending on the type of housing and the usual purpose of use. Cases that are glued, riveted or otherwise sealed and/or not intended for opening remain unopened. The check ensures to the extent that there are no unconnected data media, data media configured as Raid or other inaccessible data media in the assets. In addition, CD and floppy disk drives, slots for Sim and memory cards are checked for corresponding media.
Unless otherwise agreed with the client, any media found will be stored securely and destroyed in accordance with Clause 11.

6. Booting and network connection
The assets to be processed (except printing assets) is started by using a suitable boot medium. Then the software is started, which controls the course of the further process. Only under the condition of a successful registration as described in Clause 4, the process will be continued. Otherwise, a detailed visual error message is displayed.

6.1. Pre-classification of printing assets
In the case of printing assets, if technically possible, the status page(s) are printed out and attached to the assets for further work steps. The software checks the registered assets and reads out the (core) characteristics such as manufacturer, model, serial number and meter readings. It also determines whether a factory reset is possible for this asset and whether this has already been performed.

6.2. Review and factory reset for printing assets
The assets is reset to factory settings and any existing address books or configurations are deleted. This process is checked and recorded in the software as a status. If this reset to factory settings and the associated deletion of address books and / or configurations is not possible successfully, the deletion process must be considered unsuccessful and the printer is marked for destruction as described in Clause 11.
If the assets has built-in exchangeable / removable storage media (mechanical hard disk, hybrid or SSD storage), these will be removed. These also receive a barcode label with a unique CHG stock ID via which the storage media and the assets can be clearly assigned to each other. The storage medium to be processed is connected to a dedicated test station. Then the software is started, which controls the further process. Only on the condition of a successful connection between the asset and the test station, the process continues; otherwise, a detailed visual error message is displayed.
If the storage media was provided with a assets-specific password by the manufacturer or user and this is not known to CHG or cannot be removed, the hard disk must be sent for destruction as outlined in Clause 11.

7. Automatic recognition of the storage media type
A data medium check performed by the data erasure software automatically determines the storage medium type. The data media check distinguishes between the following storage media types: mechanical hard disk, SSD, hybrid and flash memory. According to the current industry standard software erasure tools, hybrid hard disks cannot be safely erased and are subject to destruction as listed in Clause 11.

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 medium or assets 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
The control software is instructed by a database query which type of erasure (mechanical / SSD / Flash) must be performed, and starts an appropriate erasure method. A console monitors the client during erasure. All erasure events (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, Ulrich Bergmann, 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 assets and reading it with an external electronic assets.
- 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 the case of software encryption, the encryption is managed by the assets that the SSD is integrated into. The key is created by the encryption software on the assets and stored there. Data that remains on the SSD after erasure could be read using knowledge of the encryption software and the key. To do this it would be necessary to replicate the decryption mechanism of the assets software 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 medium or assets in accordance with Clause 11.

9. Audit of the erasure result

After the erasure, an automatic check is performed whether:

- an erasure log exists
- the erasure log records error-free data erasure

In the event of an error occurring, the process is restarted after the error has been corrected. If the data erasure still fails or the data medium is flaged as "not safe to delete" it will be handled in accordance with Clause 11.

10. Documentation of the erasure process

The erasure log will be made available to the client accordingly after successful erasure and verification in accordance with clause 9.
There is at least one backup that is stored at another physical location.

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

Storage media that emerge from the process as “not secure for erasure” or cause an error in the process are treated by the employee handling the assets in such a way (e.g. reconnected, formatted, configured in the BIOS, installed into a different PC) to attempt successful completion of the erasure process starting with Clause 4.

If this is not possible, e.g. due to a hardware defect or other access restrictions, or if so instructed in accordance with the agreement, the storage medium will be removed as far as possible. After removal, all storage media are recorded in CHG-MERIDIAN's warehouse system with an unique stock ID. This id is linked to the original serial number of the assets so that it can be tracked at any time. If removal is not possible, the complete assets is subjected to the following process.

- Mechanical hard disks are degaussed and stored in a sealed aluminum box
- SSD, hybrid and flash storage media are stored in a sealed aluminum box
- Assets are stored in a separate secured area
- The storage media and assets stored in this way are shredded at short regular intervals by a certified specialist disposal company (in accordance with DIN 66399 protection class 2, security level E5).
- The shredding is carried out according to dual control principle and is confirmed by both parties with a signature. A listing of the approved subcontractors can be found at https://www.chg-meridian.de/eraSURE_subcontractors.
- All our subcontractors are approved in line with our supplier management policy

At the request of the client, non-erasable storage media can also be returned.

12. Retrieval and dispatch of erasure information

If the client uses tesma, it can access the erasure information at any time, viewed as a PDF document and download it. If the client does not use tesma then CHG-MERIDIAN will send the erasure information or logs to the client by email. The document name is always the serial number of the assets from which the hard disk originates. The data is stored on the CHG-MERIDIAN file server and can be retrieved at any time. The eraSURE reports are retained for at least two years after the data deletion has been performed.