![CHG]

PROCESS DESCRIPTION
DATA ERASURE

CHG-MERIDIAN TECHNOLOGY AND SERVICE
CENTER SKIEN

Efficient Technology Management®

PROCESS DESCRIPTION DATA ERASURE

CHG-MERIDIAN is a market leader in end-of-life management. As an independent financial advisor and technology manager, the company, based in Weingarten in Germany, offers customized business concepts for the efficient management of investments in technology. Secure data erasure forms part of Managed Desktop Solutions (MDS), a package of services that enables companies to reduce their customers' costs over the full IT lifecycle.

CHG-MERIDIAN's MDS customers include companies that are required to conform to the highest standards of data security, such as banks, public authorities, or companies in the healthcare sector. They benefit from lower overall costs, increased process efficiency, strong data security and secu-rity

of investment, as well as from intelligent reporting tools for managing their ICT asset estate.

The erasure process is NSM-certified. This standard does not certify the transport step. The process is designed for PCs, notebooks, servers, and disk subsystems. It also covers the SSD and flash memory that can be found in smartphones or solid-state hard drives.
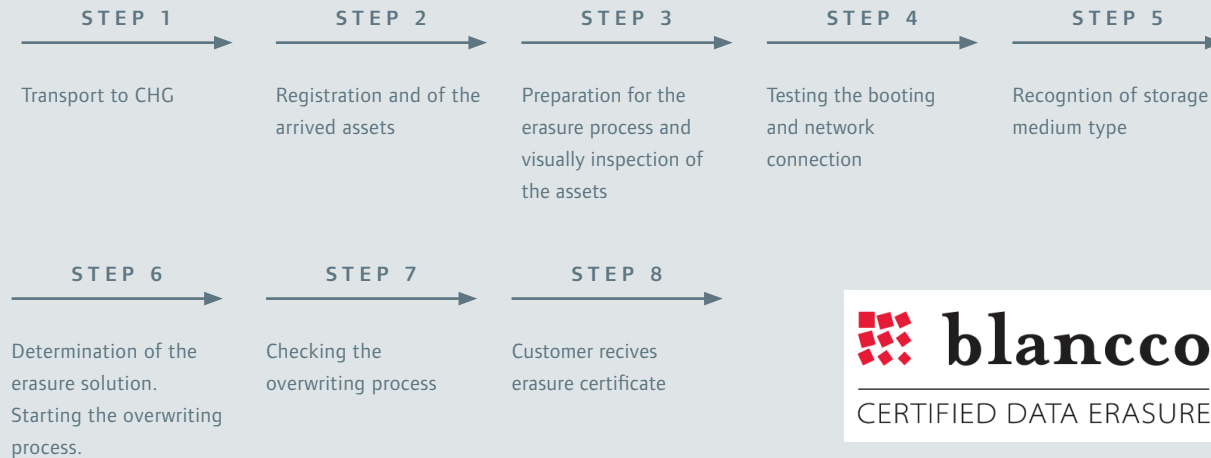
CHG Meridian Technology and Service Center Skien has obtained ISO Certificate

NS-EN ISO 14001:2015 and NS-EN ISO 9001:2015 which guards every step in the deletion process.

Management System
Certificate

To certify conformity with // Godkjent overensstemmelse med
the Management System Requirements of // Styringssystemkravene i henhold til

NS-EN ISO 9001:2015
NS-EN ISO 14001:2015

awarded // tildelt

CHG
CHG Meridian Skien AS
Rødmyrlia 20, 3735 Skien

Manufacturing/supplying following products/services:
for produksjon/leveranse av følgende produkter/tjenester:

Formidler og foredler brukt datautstyr
på en bærekraftig måte

Certificate No // Sertifikat nr.:
1259

First issued 14001 // Utstedt første gang: 2013-12-30
First issued 9001 // Utstedt første gang: 2014-10-08
Valid until // Gyldig til: 2019-12-30
Issued // Utstedt: 2017-01-03
Audit: Annual // Oppfølging: Årlig

Managing Director // Daglig leder   Lead Auditor // Revisjonsleder

Kiwa Teknologisk Institutt
Sertifisering as
Kabelgaten 2, 0580 Oslo

kiwa

_____ ISO CERTIFICATE

PROCESS STEPS

ERASURE PROCESS

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
Transport to CHG	Registration and of the arrived assets	Preparation for the erasure process and visually inspection of the assets	Testing the booting and network connection	Recogntion of storage medium type

STEP 6	STEP 7	STEP 8
Determination of the erasure solution. Starting the overwriting process.	Checking the overwriting process	Customer recives erasure certificate

blancco
CERTIFIED DATA ERASURE

1. Transport of the assets to the Technology and Service Center

If the customer asks CHG-MERIDIAN SKIEN to transport the assets, the assets are collected either by a freight forwarder or by CHG-MERIDIAN SKIEN staff. The assets are then transported to the CHG Technology and Service Center SKIEN. Otherwise, the customer takes the assets to the CHG Technology and Service Center.

2. Receipt and documentation of assets at CHG-MERIDIAN

Upon arrival every asset is counted to make sure there is no inconstancy between the customers asset-list and received assets. Each case is given a unique identifier number which follows the assets throughout the erasure process.

3. Preparation of the erasure process

Every testing station uses EAN labels to register faults and other irregularities while the assets are erased by Blancco drive erasure. All codes registered by barcodes generates a database inquiry and gets logged into the Blancco data erasure software to easily generate certificates later..

The „certified data erasure" process is designed for PCs, notebooks, servers and disk subsystems (SAS and FC technologies) with IBM compatible BIOS, 80x86 processors, and appropriate periph-erals.

This procedure cannot be applied to computers with different hardware infrastructure. For this reason, variant types of computer are separated out at this point (if they haven't been already); where possible, their hard disks are removed, installed in a compatible computer and erased using soft-ware.

3.1 Visual inspection of PCs and servers

An employee opens the computer casing (except for laptops) and visually checks how many hard disks have been installed in the computer, to ensure that there are no hard disks in the computer that are unconnected, configured as RAIDs or otherwise inaccessible.

3.2 Checking of CD drives, diskette drives, and memory cards

The content of any removable drives is checked and any

data storage media removed. Unless agreed otherwise with the customer, any data storage media found is destroyed immedi-ately.

4. Booting and network connection

The computer system to be processed is started using a network cable /via pxe and then the Blancco controls the rest of the process. The process continues only if the computer is booting according to Blancco's requirements. Otherwise, manual erasure will be executed

5. Automatic recognition of storage medium type

Blancco automatically identifies the storage medium type. The data storage media test detects the following storage types: mechanical hard drives, SSD, hybrid drive, and flash memory.

6. Overwriting of storage medium

The IT-operator determines which type of erasure (mechanical or flash) to carry out and starts the appropriate erasure method.

REQUIREMENT FOR HIGHEST PROTECTION

Following an additional agreement, the contractor can be tasked with the destruction of the data storage media. CHG-MERIDIAN Skien uses a MAXXeGUARD Shredder which meets the following standards

1. EADMS: Level C and D in accordance with the standards of destruction of the European As-sociation for Data Media Security.
2. DIN 66399: Complies to level H-5 /H-6 for Hard Disks (magnetic), to level O-5 for optical da-ta carriers (CD, DVD) and to level E-4 for electronic data carriers (SSD, USB, memory cards)

7. Checking of the overwriting process

Following erasure there is an automatic check whether:

· there is an erasure log
· the erasure log shows error-free erasure runs.

If an error has occurred, the process is restarted after the error has been corrected, or the hard disk is separated out and classified as ‚Cannot be securely erased by overwri-ting, and then handled as specified:

· Mechanical hard disks are degaussed and subsequently shredded.
· SSD, hybrid drive and flash memory storage media are shredded.

8. Retrieval and distribution of erasure data

Following data erasure, the customer receives an email. The email confirms that the data has been erased successfully, and erasure certificates are included as a ZIP'ed PDF document. For single erasure certificates, the document name is the serial number of the asset in which the hard disk was originally installed.

The relevant data is stored on the CHG file server and can be retrieved at any time. The data erasure reports are retained for at least ten years following completion of the data erasure process.

____MAXXEGUARD SHREDDER

08/2018

DO YOU WANT FURTHER INFORMATION ABOUT CHG-MERIDIAN'S PROCESS AROUND DATA ERASURE? PLEASE CONTACT US AT sales.skien@chg-meridian.com

WE'RE THERE FOR YOU WORLDWIDE!

OUR PROMISE TO YOU: MAXIMUM WORKLOAD REDUCTION THROUGHOUT THE ENTIRE TECHNOLOGY LIFE CYCLE—FULLY INDEPENDENT FROM BANKS, MANUFACTURERS AND SERVICE PROVIDERS. WE CALL IT EFFICIENT TECHNOLOGY MANAGEMENT®

WWW.CHG-MERIDIAN.NO