PROZESSBESCHREIBUNG eraSURE® plus
ISO 9001 / 27001 zertifizierte und BSI IT-Grundschutz konforme Datenlöschung

VERSION 25.07 (Juli 2025)

1. **Bestandsaufnahme der zur Abholung angemeldeten Systeme**
   Die Bestandsaufnahme wird im vier Augen Prinzip durch einen Vertreter des Kunden und des Spediteurs vorgenommen. Die Erfassung der Geräte erfolgt beim Kunden, mittels einer mobilen Datenerfassungsstation, vor Ort. Nach der vollständigen Erfassung werden die Systeme entweder in verschließbare Rollcontainer bzw. verplombbare Kisten verpackt oder auf einen verplombbaren LKW verladen. Neben der Inventarisierung der Geräte können Bemerkungen für den Transportauftrag erfasst werden. Die Plombennummer wird auf dem Frachtbrief hinterlegt. Die Kunde muss im Rahmen seiner Mitwirkungspflicht den Transportauftrag und die Verplombung der Ware abschließend prüfen. Die Quittierung der Übergabe erfolgt anschließend zusammen mit dem Spediteur direkt auf der Datenerfassungsstation. In dem seltenen Fall, dass ein Problem mit dem Datenerfassungsstation auftritt, wird die Übergabe durch Unterzeichnung der Versandpapiere bestätigt.
   Im Anschluss erhält der Kunde einen Nachweis mit allen erfassten Geräten inkl. Bearbeitungsnummer, Seriennummer, Hersteller und Geräteklasse per email übermittelt.

2. **Transport der Geräte zum Technologie- und Servicezentrum**
   Die CHG-MERIDIAN AG setzt ausgewählte Spediteure für den verplombten, GPS-überwachten und geschützten Transport in stoßsicheren Behältern und luftgefederten LKW ein. Die Geräte werden auf direktem Weg zum CHG Technologie- und Servicezentrum, Wasserweg 2, 64521 Groß-Gerau, Deutschland, transportiert.
   Eine Auflistung der derzeit eingesetzten Subunternehmer findet sich unter https://www.chg-meridian.de/eraSURE_Subunternehmer.

3. **Wareneingang und Erfassung der Geräte bei CHG-MERIDIAN**
   Nach Überprüfung der Plombennummer werden die Geräte direkt in den Sicherheitsbereich gebracht und mittels Soll/Ist-Vergleich als Lagereingang gebucht. Werden Unstimmigkeiten bei der Plombennummer oder beim Vergleich festgestellt, wird sofort ein mehrstufiger Eskalationsprozess eingeleitet. Entpacken und Erfassen der einzelnen Geräte erfolgt auf Basis der Geräteseriennummer. Erfasste Geräte erhalten ein Barcode Label mit einer eindeutigen CHG Stock-ID und der Geräteseriennummer.

4. **Vorbereitung des Löschvorgangs**
   Jeder Prüfplatz hat eine eigene Identifikationsnummer. Der Barcode des Gerätelabels und die Prüfplatznummer werden an einer Konsole per Barcodeleser eingelesen und angemeldet. Die Anmeldung erstellt einen Datenbankeintrag, der die Anmeldung autorisiert. Damit ist gewährleistet, dass jederzeit nachvollziehbar ist, welche Geräte an welcher Prüfstation bearbeitet wurden.

CHG-MERIDIAN AG
Franz-Beer-Straße 111
88250 Weingarten
Deutschland

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

Vorstand
Dr. Mathias Wagner (Vorsitzender)
Ulrich Bergmann
Daniel Welzer

Aufsichtsratsvorsitzender
Jürgen Mossakowski
Registergericht
Ulm HRB 551857

5. Optische Überprüfung der zu löschenden Geräte

Ein Mitarbeiter überprüft die Geräte, insoweit dies technisch möglich ist, öffnet er hierzu das Gehäuse. Dies erfolgt in Abhängigkeit der Gehäusebauart und dem üblichen Verwendungszweck. Verklebte, vernietete oder anderweitig verschlossene und/oder nicht für eine Öffnung vorgesehene Gehäuse bleiben ungeöffnet. Durch die Überprüfung wird soweit sichergestellt, dass sich keine nicht angeschlossenen, als Raid konfigurierte oder sonstige nicht erreichbare Datenträger im Gerät befinden.
Zudem werden CD- und Disketten-Laufwerke, Steckplätze für Sim- und Speicherkarten auf entsprechende Medien überprüft.
Gefundene Medien werden, wenn nicht anders mit dem Auftraggeber vereinbart, sicher verwahrt und nach Ziffer 11 der Zerstörung zugeführt.

6. Booten und Netzwerkverbindung

Das zu bearbeitende Gerät (ausgenommen Drucksysteme) wird mittels eines geeigneten Bootmediums gestartet. Danach wird die Software gestartet, die den Verlauf des weiteren Prozesses steuert. Nur unter der Voraussetzung einer erfolgreichen Anmeldung wie in Ziffer 4 beschrieben, wird der Prozess fortgesetzt. Andernfalls erfolgt eine detaillierte visuelle Fehlermeldung.

6.1 Vorqualifizierung von Drucksystemen

Bei Drucksystemen werden, sofern dies technisch möglich ist, die Statusseite(n) ausgedruckt und am Gerät für die weiteren Arbeitsschritte angebracht. Das System überprüft das angemeldete Gerät und liest die (Kern-) Merkmale wie Hersteller, Modell, Seriennummer und Zählerstände aus. Zudem wird ermittelt, ob für dieses Gerät ein Zurücksetzen auf Werkseinstellungen möglich ist und ob dies bereits durchgeführt wurde.

6.2 Prüfung und Werksreset bei Drucksystemen

Das Gerät wird auf Werkseinstellungen zurückgesetzt und eventuell vorhandene Adressbücher oder Konfigurationen gelöscht. Dieser Vorgang wird überprüft und im System als Status festgehalten. Ist dieses Zurücksetzen auf Werkseinstellungen und das dazugehörige Löschen von Adressbüchern und / oder Konfigurationen nicht erfolgreich möglich, muss der Löschvorgang als nicht erfolgreich angesehen werden und das System wird für die Zerstörung wie in Ziffer 11 beschrieben, vorgemerkt.
Sollte das Gerät über verbaute wechselbare / ausbaubare Speichermedien (mechanische Festplatte, Hybrid- oder SSD-Speicher) verfügen, werden diese ausgebaut. Diese erhalten ebenfalls einen Barcode Label mit einer eindeutigen CHG Stock-ID über die die Speichermedien und das Gerät eindeutig einander zugeordnet werden können. Das zu bearbeitende Speichermedium wird an einem speziellen Prüfcomputer angeschlossen. Danach wird die Software gestartet, die den Verlauf des weiteren Prozesses steuert. Nur unter der Voraussetzung einer erfolgreichen Anmeldung, wird der Prozess fortgesetzt; andernfalls erfolgt eine detaillierte visuelle Fehlermeldung.
Wurde die Festplatte durch den Hersteller oder Anwender mit einem gerätespezifischen Passwort versehen und ist dieses der CHG nicht bekannt bzw. ist nicht entfernbar, muss die Festplatte der Zerstörung, wie in Ziffer 11 aufgeführt, zugeführt werden.

CHG-MERIDIAN AG
Franz-Beer-Straße 111
88250 Weingarten
Deutschland

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

Vorstand
Dr. Mathias Wagner (Vorsitzender)
Ulrich Bergmann
Daniel Welzer

Aufsichtsratsvorsitzender
Jürgen Mossakowski
Registergericht
Ulm HRB 551857

7. Automatische Erkennung des Speichermedientyps

Eine Datenträgerprüfung ermittelt automatisch den Speichermedientyp. Die Datenträgerprüfung unterscheidet folgende Speichermedientypen: mechanische Festplatte, SSD-, Hybrid- und Flash-Speicher. Nach heutigem Stand der Technik sind Hybrid-Festplatten nicht sicher löschbar und werden der Zerstörung wie in Ziffer 11 aufgeführt zugeführt.

8. Löschmethodik

Der Auftraggeber entscheidet über den jeweiligen Schutzbedarf der Daten und somit der Form der Datenlöschung. Bei normalem und höherem Schutzbedarf können die Datenträger bzw. Geräte nach BSI IT-Grundschutz B1.15 einer Löschung unterzogen werden. Bei höchsten Schutzbedarf empfiehlt der BSI IT-Grundschutz die vollständige Zerstörung nach DIN 66399.

7.1 Normaler Schutzbedarf

Dem Steuerprogramm wird durch eine Datenbankabfrage mitgeteilt, welche Art der Löschung (mechanisch / SSD / Flash) durchgeführt werden muss und startet eine entsprechende Löschmethode.
Eine Konsole überwacht den Client während der Löschung. Alle Löschvorfälle (defekte Sektoren, Fortschrittsnachrichten, Löschprotokoll usw.) werden in einer Datenbank gespeichert.

7.2 Höherer Schutzbedarf

Der Löschvorgang erfolgt wie in Ziffer 7.1 aufgeführt, unter Berücksichtigung der nachfolgend beschriebenen Hinweise:
Je nach Verschlüsselungsart und Implementierung von Löschbefehlen der SSD-, Hybrid oder Flash-Speicher durch die jeweiligen Hersteller bestehen nach erfolgter Löschung nachfolgend genannte Restrisiken einer Wiederherstellung von Daten oder Datenfragmenten:
Wenn eine SSD keine Verschlüsselung aufweist, werden die an sie übergebenen Daten im Klartext in den Speichermodulen gespeichert. Löschbefehle in SSDs, die eine rückstandsfreie Löschung solcher Inhalte garantieren sollen, sind nicht immer ausreichend vertrauenswürdig. Somit muss damit gerechnet werden, dass SSDs auch nach Anwendung von ATA-Löschbefehlen noch Daten enthalten. Ein Angreifer könnte sich dies zunutze machen, indem er die Speichermodule aus dem Gerät entfernt und mit einer externen Elektronik ausliest.
Bei der Hardwareverschlüsselung werden die Nutzdaten des Benutzers von der SSD selbst vor Ablage mit einem in der Hardware der SSD generierten und auf der SSD abgelegten privaten Schlüssel verschlüsselt. Die Löschung beginnt damit, dass der Schlüssel gelöscht wird. Daten, die nach einer Löschung auf der SSD verbleiben, sind dann für einen Angreifer wertlos, da er sie nur mit sehr hohem Aufwand entschlüsseln kann. Notwendig wäre ein Nachbau des Entschlüsselungsmechanismus der SSD und ein Brute-Force-Angriff zur Ermittlung des Schlüssels.

- Bei der Softwareverschlüsselung wird die Verschlüsselung von dem Gerät bewerkstelligt, in das die SSD eingebaut ist. Der Schlüssel wird vom Verschlüsselungsprogramm auf dem Gerät erzeugt und auch dort abgelegt. Daten, die nach einer Löschung auf der SSD verbleiben, könnten bei Kenntnis des Verschlüsselungsprogramms und des Schlüssels gelesen werden. Notwendig wäre hier, den Entschlüsselungsmechanismus des Geräteprogramms nachzubauen und den Schlüssel aus dem Rechnerspeicher zu lesen.

CHG-MERIDIAN AG
Franz-Beer-Straße 111
88250 Weingarten
Deutschland

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

Vorstand
Dr. Mathias Wagner (Vorsitzender)
Ulrich Bergmann
Daniel Welzer

Aufsichtsratsvorsitzender
Jürgen Mossakowski
Registergericht
Ulm HRB 551857

7.3 Höchster Schutzbedarf

Ist der höchste Schutzbedarf erforderlich, ist in einer zusätzlichen Vereinbarung der Auftragnehmer mit der Zerstörung nach Ziffer 11 der entsprechenden Datenträger oder Systeme zu beauftragen.

9. Prüfung des Löschergebnisses

Nach der Löschung erfolgt eine automatische Überprüfung ob:

- ein Löschprotokoll vorhanden ist
- das Löschprotokoll fehlerfreie Löschvorgänge ausweist

Im Falle eines aufgetretenen Fehlers wird der Prozess nach Fehlerbehebung neu gestartet oder der Datenträger als „nicht sicher zu löschen" aussortiert und gemäß Ziffer 11 weiter behandelt.

10. Dokumentation des Löschvorgangs

Das Löschprotokoll wird dem Auftraggeber nach erfolgreicher Löschung und Überprüfung gemäß Ziffer 9. entsprechend zur Verfügung gestellt.
Es existiert mindestens ein Backup, das an einer anderen physikalischen Lokation vorgehalten wird.

11. Spezielle Behandlung nicht überschreibbarer Speichermedien und Drucksystemen

Speichermedien, die als „nicht sicher zu löschen" aus dem Prozess hervorgehen oder im Prozess einen Fehler verursachen, werden von dem mit dem Gerät arbeitenden Mitarbeiter so behandelt (z.B. neu angeschlossen, formatiert, im Bios konfiguriert, in einen anderen PC eingebaut usw.), dass sie den Löschprozess, beginnend bei Ziffer 4, erfolgreich durchlaufen können.
Ist dies, z.B. aufgrund eines Hardwaredefektes oder sonstiger Zugriffsbeschränkungen, nicht möglich oder gemäß Vereinbarung so beauftragt wird das Speichermedium soweit möglich ausgebaut. Alle Speichermedien werden nach dem Ausbauen im Lagersystem der CHG-MERIDIAN erfasst und erhalten ebenfalls eine Bearbeitungsnummer (Stock-ID). Diese wird mit der ursprünglichen Seriennummer des Gerätes verknüpft, so dass jederzeit eine Zuordnung möglich ist. Ist ein Ausbau nicht möglich, wird das komplette Gerät dem nachfolgenden Prozess unterzogen.

- Mechanische Festplatten werden degaussert und in einer versiegelten Aluminiumbox verwahrt
- SSD-, Hybrid- und Flash-Speichermedien werden in einer versiegelten Aluminiumbox verwahrt
- Geräte werden in einem separaten Bereich verwahrt
- Die so verwahrten Speichermedien und Geräte werden in kurzen regelmäßigen Abständen von einem zertifizierten Entsorgungsfachbetrieb (nach DIN 66399 Schutzklasse 2, Sicherheitsstufe E5) geschreddert.
- Die Entsorgung erfolgt nach dem „Vier Augen" Prinzip und wird von beiden Seiten mit Unterschrift bestätigt.

CHG-MERIDIAN AG
Franz-Beer-Straße 111
88250 Weingarten
Deutschland

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

Vorstand
Dr. Mathias Wagner (Vorsitzender)
Ulrich Bergmann
Daniel Welzer

Aufsichtsratsvorsitzender
Jürgen Mossakowski
Registergericht
Ulm HRB 551857

- Eine Auflistung der derzeit eingesetzten Subunternehmer findet sich unter https://www.chg-meridian.de/eraSURE_Subunternehmer.
- Alle unsere Unterauftragnehmer werden gemäß unserer Richtlinie zum Lieferanten-Management zugelassen

Auf Wunsch des Auftraggebers, können nicht löschbare Speichermedien auch zurückgegeben werden.

12. Abruf und Versand von Löschinformationen

Sofern der Auftragnehmer tesma nutzt, kann er die Löschinformationen jederzeit über tesma abrufen, als PDF-Dokument anzeigen lassen und herunterladen. Sofern der Auftraggeber tesma nicht nutzt, wird CHG-MERIDIAN dem Auftragnehmer die Löschinformationen bzw. –protokolle per Email zusenden. Der Dokumentenname ist grundsätzlich die Seriennummer des Gerätes, aus dem die Festplatte stammt. Die Daten werden auf dem File-Server der CHG-MERIDIAN gespeichert und sind jederzeit abrufbar. Die Löschberichte werden nach Durchführung der Löschungsroutine mindestens zwei Jahre aufbewahrt.

CHG-MERIDIAN AG
Franz-Beer-Straße 111
88250 Weingarten
Deutschland

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

Vorstand
Dr. Mathias Wagner (Vorsitzender)
Ulrich Bergmann
Daniel Welzer

Aufsichtsratsvorsitzender
Jürgen Mossakowski
Registergericht
Ulm HRB 551857