eraSURE® plus PROCESS DESCRIPTION

eraSURE® plus PROCESS DESCRIPTION

ISO 9001/27001 e BSI IT

Versione 25.07 (luglio 2025)

- **Elenco dei beni registrati per il reso**
  L'inventario viene effettuato secondo il principio del doppio controllo da un rappresentante del cliente e dell'azienda di trasporti. I beni vengono registrati in loco presso la sede del cliente utilizzando un terminale mobile per l'acquisizione dati. Una volta completata la registrazione, i beni vengono imballati in contenitori su ruote chiudibili a chiave o in scatole chiudibili a chiave oppure caricati su un camion chiudibile a chiave. Oltre all'inventario dei beni, è possibile registrare anche eventuali commenti relativi all'ordine di trasporto. Il numero del sigillo viene riportato sul documento di spedizione. Nell'ambito del suo dovere di collaborazione, il cliente deve verificare l'ordine di trasporto e la sigillatura dei beni. La consegna viene quindi confermata insieme al vettore direttamente sul terminale di raccolta dati. Nel raro caso di un malfunzionamento del terminale dati, la consegna verrà confermata mediante la firma dei documenti di spedizione. Il cliente riceve quindi un'e-mail con tutti i beni registrati, inclusi il numero dell'ordine di trasporto, il numero di serie, il produttore e la classe di beni.
- **Trasporto dei dispositivi presso il Technology & Service Center**
  CHG-MERIDIAN AG si avvale di corrieri autorizzati per il trasporto sigillato, monitorato tramite GPS e sicuro in contenitori antiurto e autocarri con sospensioni pneumatiche. I beni vengono trasportati direttamente al CHG Technology and Service Center, Wasserweg 2, 64521 Groß-Gerau, Germania. Un elenco dei subappaltatori attualmente approvati è disponibile all'indirizzo **https://www.chg-meridian.de/eraSURE_subcontractors**
- **Ricezione e documentazione dei beni da parte di CHG-MERIDIAN**
  Dopo aver verificato il numero di sigillo, i beni vengono trasferiti direttamente nell'area protetta e registrati come beni in entrata con un confronto tra dati effettivi e previsti. Se si riscontrano discrepanze nel numero di sigillo o nel confronto, viene avviata immediatamente una procedura di escalation a più livelli. Il disimballaggio e la registrazione dei singoli beni avvengono in base al numero di serie dei beni. Ai beni documentati viene applicata un'etichetta con codice a barre contenente un chiaro ID di magazzino CHG e il numero di serie del bene.
- **Preparazione per il processo di cancellazione**
  Ogni stazione di collaudo dedicata ha un proprio numero di identificazione. Il codice a barre riportato sull'etichetta del bene e il numero della stazione di collaudo vengono scansionati su una console tramite un lettore di codici a barre e registrati. La registrazione crea una voce nel database che autorizza la registrazione. Ciò garantisce che sia sempre possibile risalire a quali beni siano stati trattati in quale stazione di collaudo.

- **Controllo visivo degli asset oggetto di cancellazione**
  Un addetto verifica le apparecchiature; se tecnicamente possibile, apre l'involucro per eseguire questa procedura. Ciò avviene a seconda del tipo di involucro e della normale destinazione d'uso. Gli involucri che sono incollati, rivettati o sigillati in altro modo e/o non destinati ad essere aperti rimangono chiusi. La verifica garantisce che all'interno delle apparecchiature non siano presenti supporti dati scollegati, configurati in RAID o comunque inaccessibili. Inoltre, si controlla la presenza dei relativi supporti nei lettori CD e floppy disk, negli slot per schede SIM e schede di memoria.Salvo diversamente concordato con il cliente, eventuali supporti rinvenuti saranno conservati in modo sicuro e distrutti in conformità con l'articolo 11.
- **Avvio del sistema e connessione di rete**

Il sistema da configurare (ad eccezione dei dispositivi di stampa) viene avviato utilizzando un supporto di avvio adeguato. Successivamente viene avviato il software che gestisce lo svolgimento delle fasi successive del processo. Solo a condizione che la registrazione, come descritto al punto 4, sia andata a buon fine, il processo proseguirà. In caso contrario, verrà visualizzato un messaggio di errore dettagliato.

- **Pre-classificazione delle stampanti**
  Nel caso di stampanti, se tecnicamente possibile, le pagine di stato vengono stampate e allegate agli asset per le fasi successive del processo. Il software verifica i dispositivi registrati e rileva le caratteristiche (principali) quali produttore, modello, numero di serie e letture dei contatori. Determina inoltre se per quel dispositivo è possibile eseguire un ripristino alle impostazioni di fabbrica e se tale operazione è già stata effettuata.
- **Controllo e reset alle impostazioni di fabbrica per stampanti**
  Il dispositivo viene ripristinato alle impostazioni di fabbrica e tutte le rubriche o le configurazioni esistenti vengono cancellate. Questo processo viene verificato e registrato nel software come stato. Se il ripristino alle impostazioni di fabbrica e la conseguente cancellazione delle rubriche e/o delle configurazioni non possono essere completati con successo, il processo di cancellazione deve essere considerato fallito e la stampante viene contrassegnata per la distruzione come descritto nell'articolo 11. Se il dispositivo dispone di supporti di memorizzazione integrati sostituibili/rimovibili (disco rigido meccanico, memoria ibrida o SSD), questi vengono rimossi. Anche questi ricevono un'etichetta con codice a barre con un ID di magazzino CHG univoco, tramite il quale il supporto di memorizzazione e il dispositivo possono essere chiaramente associati l'uno all'altro. Il supporto di memorizzazione da elaborare viene collegato a una stazione di test dedicata. Quindi viene avviato il software, che controlla l'ulteriore processo. Solo a condizione che la connessione tra il bene e la stazione di test abbia esito positivo, il processo prosegue; in caso contrario, viene visualizzato un messaggio di errore dettagliato. Se il supporto di memorizzazione è stato dotato di una password specifica per il bene da parte del produttore o dell'utente e questa non è nota a CHG o non può essere rimossa, il disco rigido deve essere inviata alla distruzione come indicato nell'articolo 11.
- **Riconoscimento automatico del tipo di supporto di memorizzazione**
  Il cliente stabilisce le proprie esigenze in materia di protezione dei dati e, sulla base di ciò, la modalità di cancellazione dei dati. Per esigenze di protezione normali o superiori, i supporti dati o le risorse possono essere cancellati in conformità con la norma BSI IT Baseline Protection B1.15. Per le esigenze di protezione più elevate, la norma BSI IT Baseline Protection raccomanda la distruzione completa in conformità con la norma DIN 66399.
- **Normali esigenze di protezione**
  Il software di controllo riceve da una query del database le istruzioni relative al tipo di cancellazione (meccanica / SSD / Flash) da eseguire e avvia il metodo di cancellazione appropriato. Una console monitora il dispositivo durante la cancellazione. Tutti gli eventi relativi alla cancellazione (settori difettosi, messaggi di avanzamento, registri di cancellazione ecc.) vengono salvati in un database.
- **Elevate esigenze di protezione**
  Il processo di cancellazione avviene secondo quanto descritto nell'articolo 7.1, tenendo conto delle note riportate di seguito. A seconda del tipo di crittografia e dell'attuazione delle istruzioni di cancellazione da parte delle unità di archiviazione SSD, ibride o flash dei rispettivi produttori, potrebbero sussistere i rischi residui elencati di seguito, ovvero che i dati o frammenti di dati possano essere recuperati dopo che la cancellazione è stata effettuata:
    - Se un SSD non è crittografato, i dati trasferiti su di esso verranno salvati in chiaro nei moduli di memoria. Le istruzioni di cancellazione presenti negli SSD, volte a garantire la cancellazione completa di tali contenuti, non sono sempre sufficientemente affidabili. È quindi lecito aspettarsi che gli SSD continuino a contenere dati anche dopo

l'applicazione delle istruzioni di cancellazione ATA. Un malintenzionato potrebbe approfittarne rimuovendo il modulo di archiviazione dal dispositivo e leggendo il suo contenuto con un dispositivo elettronico esterno.

- Nel caso della crittografia hardware, i dati dell'utente vengono crittografati prima dell'archiviazione dallo stesso SSD utilizzando una chiave privata generata nell'hardware dell'SSD e memorizzata su di esso. La cancellazione inizia con la rimozione di questa chiave. Qualsiasi dato che rimane sull'SSD dopo la cancellazione è privo di valore per un aggressore, poiché può essere decrittografato solo con un grande sforzo. Sarebbe necessario replicare il meccanismo di decrittografia dell'SSD ed eseguire una forzatura per determinare la chiave.
- Nel caso della crittografia software, la crittografia è gestita dai dispositivi in cui l'SSD è integrato. La chiave viene generata dal software di crittografia presente sui dispositivi e lì memorizzata. I dati che rimangono sull'SSD dopo la cancellazione potrebbero essere letti sfruttando la conoscenza del software di crittografia e della chiave. Per farlo, sarebbe necessario riprodurre il meccanismo di decrittografia del software dei dispositivi e leggere la chiave dalla memoria del computer.

- **Massime esigenze di protezione**
  Qualora sia richiesto il massimo livello di protezione, è necessario stipulare un accordo aggiuntivo con il cliente per la distruzione dei rispettivi supporti dati o beni in conformità con l'articolo 11.
- **Verifica del risultato della cancellazione**
  Dopo la cancellazione, viene eseguito un controllo automatico per verificare se:
  - esiste un registro delle cancellazioni
  - Il registro delle cancellazioni registra le operazioni di cancellazione dei dati eseguite senza errori

  In caso di errore, il processo viene riavviato una volta corretto l'errore. Se la cancellazione dei dati continua a non andare a buon fine o se il supporto dati viene contrassegnato come non sicuro da cancellare, verrà gestito in conformità con l'articolo 11.
- **Documentazione del processo di cancellazione**
  Il registro delle operazioni di cancellazione sarà messo a disposizione del cliente al termine della cancellazione e della verifica, in conformità con l'articolo 9. È presente almeno un backup archiviato in un'altra sede fisica.
- **Trattamento speciale dei supporti di memorizzazione non riscrivibili e stampanti**
  I supporti di memorizzazione che risultano dal processo come «non idonei alla cancellazione» o che causano un errore nel processo vengono trattati dal dipendente incaricato della gestione delle risorse in modo tale (ad es. ricollegati, formattati, configurati nel BIOS, installati su un altro PC) da tentare il completamento con successo del processo di cancellazione a partire dall'articolo 4. Se ciò non è possibile, ad esempio a causa di un difetto hardware o di altre restrizioni di accesso, o se così indicato in conformità con il contratto, il supporto di memorizzazione verrà rimosso per quanto possibile.
  Dopo la rimozione, tutti i supporti di memorizzazione vengono registrati nel sistema di magazzino di CHG-MERIDIAN con un ID di magazzino univoco. Questo ID è collegato al numero di serie originale dei beni in modo che possa essere tracciato in qualsiasi momento. Se la rimozione non è possibile, l'intero bene viene sottoposto al seguente processo.
  - I dischi rigidi meccanici vengono smagnetizzati e conservati in una scatola di alluminio sigillata
  - I supporti di archiviazione SSD, ibridi e flash sono conservati in una scatola di alluminio sigillata
  - I beni sono conservati in un'area separata e protetta

- 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
- Tutti i nostri subappaltatori sono approvati in conformità con la nostra politica di gestione dei fornitori

Su richiesta del cliente, è possibile restituire anche supporti di memorizzazione non cancellabili.

- **Recupero e invio delle informazioni relative alla cancellazione**
  Se il cliente utilizza tesma, può accedere in qualsiasi momento alle informazioni relative alla cancellazione, visualizzarle come documento PDF e scaricarle. Se il cliente non utilizza tesma, CHG-MERIDIAN invierà le informazioni relative alla cancellazione o i registri al cliente tramite e-mail. Il nome del documento corrisponde sempre al numero di serie delle apparecchiature da cui proviene il disco rigido. I dati vengono archiviati sul file server CHGfile server di CHG-MERIDIAN e possono essere recuperati in qualsiasi momento. I report eraSURE vengono conservati per almeno due anni dopo l'esecuzione della cancellazione dei dati.