Technical User Manual for Enterprise Erase LAN

Tabernus Enterprise Erase LAN 5.3

Monday, January 27, 2014

Summary

Based on “Guidelines for Preparation of User Manual v2.0”, issued by the National Security Authority (NSM), this document describes how to handle the classified data storage media addressed for erasure (for reuse or downgrading).

Document ID: 20140127T1511

Version History

DATE	VERSION	DESCRIPTION	AUTHOR
2013-10-29	0.1	First draft	Thomas Reid
2013-10-30	0.2	Second daft for internal review	Thomas Reid
2013-11-12	0.3	Internal Review Submission	Daniel Dyer
2013-11-20	1.0	Internal Review Submission	Daniel Dyer
2013-01-20	1.1	Third Draft for External Review	Thomas Reid

Abstract

This document is based on “Guidelines for Preparation of User Manual v2.0”, issued by the National Security Authority (NSM).

The purpose of this technical user manual is to describe how to handle the classified data storage media addressed for erasure (for reuse or downgrading).

This technical user manual is based on the use of Tabernus Enterprise Erase 5.3 for secure data erasure, as well as Enterprise Erase – LAN Users Guide Version 5.3.2.1 (Appendix 1) for further details.

This user manual describes the following

- Release, reuse and declassification or downgrading of the security level of data storage media
- Destruction

It is assumed that the data storage media addressed for erasure is handled in accordance to the current document security regulations [Regulations on Information Security, chapter 4].

Contents

Introduction

Purpose and Scope

Technical User Manual describes how to properly overwrite the classified information stored electronically on a computer media, using Tabernus Enterprise Erase LAN 5.3. It is assumed that the person who performs this service has a sufficient security clearance and is authorised in accordance with the storage medium's classification level.

Specification for the use of Tabernus Enterprise Erase LAN 5.3

- This product can be used for the erasure of ATA/IDE, SATA, SAS, FC, USB and Firewire drives with no limit on the size of the hard disk.
- Tabernus Enterprise Erase treats the storage media as physical devices rather than logical disks. The benefit of this approach is, that the erasure process can circumvent limitations set by particular computer BIOS or operating system. As Tabernus Enterprise works independently from any file system on the target media, it is able to erase hidden files and remove HPA and DCO areas.

References and Notes

This Technical User Manual has been prepared based on the requirements described on information security § 5-26.

- Act of 20 March 1988 on protective security services (Norway's law concerning security) and regulations
- This technical user manual for secure data deletion
- Enterprise Erase – LAN Users Guide Version 5.3.2.1 (Appendix 1) describes the detailed and extended use of the software.

Updating this Manual

Head of IT / Security Officer / Security Manager is responsible for informing Tabernus Europe Ltd. ("Tabernus") about any requirement to update this document. Tabernus will perform the required changes and deliver the updated document to the appointed person.

Version Control of Manual

Version control of this Technical User Manual is handled by Tabernus' document management system. A unique ID of this document can be seen at the bottom of each page.

Responsibility and Organization

Security Organization

The security organization of <entity> is:

The Entity's leader:	NNNN
Head of IT:	NNNN
Security Officer:	NNNN
Security Manager:	NNNN

Access to Data Storage Media in Accordance with Authorization

Head of IT / Security Officer / Security Manager in the organisation shall verify the individual user's security clearance and ensure that they have signed a confidentiality agreement.

Requirements for Training

The organisation's leader shall ensure that the user is given the necessary training, so that the user can operate Tabernus Enterprise Erase in a secure manner.

User Obligation

All personnel with access to the use of Tabernus Enterprise Erase in connection with classified hardware, are required to familiarise themselves with and follow the instructions in the manual with attachments.

User shall sign a statement (see 'User Declaration') that he/she has become familiarised with the current user documentation before being granted access to the Tabernus Erasure Software.

The declaration shall be kept by Head of IT / Security Officer / Security Manager until the user no longer has access to the relevant system.

Reporting of Security Breaches and Security Threatening Events

All personnel have a responsibility to protect the security concerns in their work or business projects, and are obliged to contribute to the preventative security service. Security breaches and security threatening events or attempts to such shall immediately be reported to the Security Officer / Security manager. The company implements measures and reporting as specified in the Regulations on security administration.

Reactions to Security Breaches and Security Threatening Events

Any person who wilfully or negligently violates the provisions prescribed by law, regulation or this procedure may be punished by fines or imprisonment, see Security Act. An accomplice may be punished accordingly.

Reuse, Declassification and Downgrading of Data Storage Media

Reuse

Machine-readable storage media classified BEGRENSET or KONFIDENSIELT used in an information system, can be reused in another regulated information system of at least the same security level, if person that have access to storage medium are authorised for the information on it and the storage media is overwritten at least once with Tabernus Enterprise Erase LAN 5.3 (approved by NSM). Media's original security level shall be retained unless a higher classified information is stored on the media.

It is not allowed to reuse the data storage media that has been used for HEMMELIG data. It is also not permitted to reuse the data storage media that has been used to KONFIDENSIELT, HEMMELIG or STRENGT HEMMELIG information in an unclassified system. Head of IT / Security Officer / Security Manager is responsible for ensuring that the necessary procedures and measures in connection with the instructions for the reuse of media, are attached and completed. The table on page 8 sets the frame conditions for reuse and downgrading of classified data storage for a lower classification level.

Security Level Declassification or Downgrading

Rules for declassification or downgrading of the security level of the information is provided in the Regulations relating information security chapter 2, B and C.

A classified data storage medium may only be considered as approved for reuse or declassification if all data that is/was stored on the media are:

A. Deleted or declassified using Tabernus Enterprise Erase LAN 5.3 as described in this instruction with attachments (approved by NSM), or by use of degausser (see section on "Degaussing Media").
B. Deleted or declassified using another eraser approved by NSM.

Downgrading or reuse of data storage media classified BEGRENSET recommended only if Tabernus Enterprise Erase LAN 5.3, or other tools or methods approved by NSM are used.

Reuse of data storage media classified KONFIDENSIELT are allowed only if Tabernus Enterprise Erase LAN 5.3, or other tools or methods approved by NSM are used.

Reuse of data storage media classified HEMMELIG is not allowed.

Overwriting and Degaussing

There are two methods that can be used in the re-use and re-classification of magnetic data storage media:

- Overwriting
- Degaussing

Overwriting of magnetic storage media is a procedure to remove classified information from the media. Degaussing is a method to make information inaccessible on a magnetic data storage medium by exposing it to a varying magnetic field.

Overwriting as an Approved Method

After a storage medium has been erased with Tabernus Enterprise Erase LAN 5.3, the information that was on the media cannot, in practise, be reconstructed. The number of times information must be overwritten depends on the grading requirements (see table on page 8).

Requirements of Overwriting

Tabernus Enterprise Erase LAN 5.3 is able to overwrite all information from the computer where it is used. In practise this means that the entire disk is overwritten. Thus overwriting all regular files and

- Hidden ("hidden") files and directories
- Unused fragments of sectors or blocks of data that is seized of stored files
- Sectors or data blocks on disk that have been "deleted" by usual (not approved) deletions
- Sectors and blocks the file system has marked as "not usable" (as the software is filesystem independent)

It is verified by the use of Tabernus Enterprise Erase LAN 5.3 that

- Information is not stored in hidden files or directories, and that
- Residual information is not stored on the media. Samples are taken of the disk information content at sector/block level.

Table 1 - Re-use, declassification or downgrading the security level using approved overwrite by using Tabernus Enterprise Erase LAN 5.3

	BEGRENSET Textual information	KONFIDENSIELT	HEMMELIG
Reuse	1x overwriting	7x overwriting	NOT ALLOWED
Downgrading	Not applicable	NOT ALLOWED	NOT ALLOWED
Declassification	7x overwriting	NOT ALLOWED	NOT ALLOWED

Reuse Definition

Machine-readable storage media classified BEGRENSET or KONFIDENSIELT used in an information system, can be reused in another information system at the same or higher classification level, if all persons that have access to storage media are authorized for the information on it or the storage media is overwritten at least once with Tabernus Enterprise Erase LAN 5.3 (approved by NSM).

The media's original markings shall be retained unless higher classified information is stored on the media.

Downgrading Definition

Rules for declassification or downgrading of the security level of the information is provided in the Regulations relating information security chapter 2, B and C.

A classified data storage medium may only be considered as approved for reuse or re-classification if all data that is/was stored on the media are:

A. Deleted or re-classified using Tabernus Enterprise Erase LAN 5.3 as described in this instruction with attachments (approved by NSM), or by use of degausser (see section "Degausser").
B. Deleted or re-classified using another eraser approved by NSM.
C. All information held on the drive has been reclassified by the owner of the information.

Downgrading of storage media is not recommended. Copy instead its re-classified information onto a medium with the appropriate classification level, and consider the possibility of reusing the original storage medium for other purposes.

Downgrading where overwriting is used can only be accepted for information classified BEGRENSET.

Degaussing Media

A degausser is an instrument or machine that generates a strong magnetic field, which can make any information unusable. Only degaussers approved by the NSM may be used.

User Declaration

1. This statement applies to the use of Tabernus Enterprise Erase LAN 5.3 for overwriting classified information in accordance with the Security Act and it's regulations.
2. This declaration shall be dated and signed in duplicate by the user. One copy is retained by the user, and the other kept by the Head of IT / Security Officer / Security Manager.

By signing this user declaration, I confirm that:

A. I have read and understood the user documentation that I have received from Head of IT / Security Officer / Security Manager.
B. I understand the obligations and responsibilities associated with using Tabernus Enterprise Erase LAN 5.3 for classified storage media.
C. I am aware of the criminal penalties it may have for me personally if I do not act in accordance with the Security Act and Regulations, as well as other Norwegian law.

Company:

Location:

Date:

User Name (Printed):

User Signature:

Appendix

Appendix 1

Tabernus Enterprise Erase – LAN Users Guide