blancco

CERTIFIED DATA ERASURE

TECHNICAL USER MANUAL

For Blancco Erasure Software v4.10 HMG

Author

Juha Levo / Quality Manager / Blancco Ltd.

ID 138

VERSION HISTORY

DATE	VERSION	DESCRIPTION	AUTHOR
2011-12-14	0.1	First draft	Juha Levo
20011-12-21	0.2	Second draft for internal inspection purposes	Juha Levo
2011-01-02	1.0	First published version	Juha Levo
2011-01-23	2.0	Second published version	Juha Levo
2011-01-27	3.0	Third published version	Juha Levo

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 Blancco Erasure Software (BES) v4.10 HMG for secure data erasure, as well as User Manual for Blancco Erasure Software, v4.10 HMG (Appendix 1) for further details.

This user manual describes the following

- release, reuse and the 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].

DEFINITIONS

BES	Blancco Erasure Software
NSM	Nasjonal sikkerhetsmyndighet

TABLE OF CONTENTS

INTRODUCTION

Purpose and Scope

Technical User Manual describes how to properly overwrite the classified information stored electronically on a computer media, using Blancco Erasure Software version 4.10 HMG.
It is assumed that the person who performs this service has a sufficient security clearance and is authorized in accordance with the storage medium's classification level.

Specifications for the use of Blancco Erasure Software v4.10 HMG

- This product can be used for the erasure of PATA (a.k.a. ATA/IDE), SATA, SCSI, SAS and USB drives with no limit on the size of the hard disk.
- Blancco Erasure Software treats storage medium as physical devices, not logical disks. The benefit of this approach is, that the erasure process can circumvent limitations set by computer BIOS. As Blancco Erasure Software is independent of any operating system on the storage medium, it can erase hidden files and remove HPA and DCO areas.
- System requirements: see user manual (Appendix 1).

References and notes

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

- Act of 20 March 1998 on protective security services (Norway’s law concerning security) and regulations
- This technical user manual for secure data deletion
- Blancco Erasure Software User Manual for v4.10 HMG (Appendix 1) describes the detailed and extended use.

Updating

Head of IT / Security Officer / Security Manager is responsible for informing Blancco Oy Ltd. (“Blancco”) about any needs to update this document. Blancco will perform needed changes and deliver updated document to the appointed persons.

Version Control of Manual

Version control of this Technical User Manual is handled by Blancco’s Document Management System. Unique ID number of this document can be seen in the front 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 the authorization

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

Requirements for training

The organization's leader shall ensure that the user is given the necessary training, so that the user can operate Blancco Erasure Software in a secure manner.

User obligation

All personnel with access to the use of Blancco Erasure Software in connection with classified hardware, are required to familiarize themselves with and follow the instructions in this manual with attachments.

User shall sign a statement (see Chapter "User Policy") that she/he has become familiarized with the current user documentation before being granted access to the Blancco 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 preventive security service. Security breaches and security-threatening events or attempt 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 willfully 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 medium 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 persons that have access to storage medium are authorized for the information on it and the storage media is overwritten at least once with Blancco Erasure Software v4.10 HMG (approved by NSM). Medium'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 allowed 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 1 on page 11 sets the frame conditions for reuse and downgrading of classified data storage media system approved 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 re-classification if all information is - or was - stored on the media are:

A.

Deleted or re-classified using Blancco Erasure Software v4.10 HMG 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.

- Downgrading or reuse of data storage media classified BEGRENSETrecommended only if Blancco Erasure Software v4.10 HMG, or other / other tools / methods approved by the NSM is used.
- Reuse of data storage media classified KONFIDENSIELT are allowed only if Blancco Erasure Software v4.10 HMG, or other / other tools / methods approved by the NSM is used.
- Reuse of data storage media classified HEMMELIG is not allowed.

Overwriting and degaussing

There are two methods that can be used in 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 to 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 Blancco Erasure Software v4.10 HMG, the information that was on the media cannot, in practice, be reconstructed. The number of times information must be overwritten depends on the grading requirements (see table 1 on page 10).

Requirements of Overwriting

Blancco Erasure Software v4.10 HMG is able to overwrite all information from the computer where it is used. In practice this means that the entire disk is overwritten. Thus overwriting 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 is "deleted" by the usual (not approved) deletion
- sectors and blocks the system has marked as "not usable" (similar to "bad sectors" in MS-DOS)

It is verified by the use of Blancco Erasure Software v4.10 HMG 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 down to sector/block level (see also Appendix 1).

Overview of the re-use, declassification or downgrading the security level using approved overwrite by using Blancco Erasure Software v4.10 HMG:

Table 1

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

Reuse (definition):

Machine-readable storage medium 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 medium are authorized for the information on it or the storage media is overwritten at least once with Blancco Erasure Software v4.10 HMG (approved by NSM).
Medium's original markings shall be retained unless higher classified information is stored on the media.

Downgrading (definition):
Rules for Downgrading information provided in the Regulations relating information Chapter 2, B and C. A data storage medium may only be re-classified if all information is - or was - stored on the media is:

a. re-classified or
b. removed using approved overwrite technique, or by the use of degaussing.

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

Degausser

Degausser, is an instrument or machine that generates strong magnetic fields, which can make the information unusable. Only degaussers approved by NSM may be used.

USER DECLARATION

1. This statement applies to the use of Blancco Erasure Software v4.10 HMG by overwriting of classified information in accordance with the Security Act and its 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 Blancco Erasure Software v4.10 HMG 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 Safety Act and Regulations, as well as other Norwegian law.

Company:
Place / date:
Title:
Name:
User Signature:

APPENDIX

APPENDIX 1
Blancco Erasure Software User Manual for v4.10 HMG