TECHNICAL USER MANUAL

For Blancco Erasure Software v5.7.0.1

ABSTRACT

This document is based on "Guidelines for Preparation of User Manual v2.0", issued by the National Security Authority (NSM) and describes 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 5 v5.7.0.1 for secure data erasure, as well as User Manual for Blancco 5, v5.7.0.1.

This manual describes the following:

- release, reuse and the declassification or downgrading the security level of data storage media
- destruction

It is assumed that the data storage media addressed for erasure is handled in accordance with the current document on security regulations, Regulations on Information Security (Chapter 4).

TABLE OF CONTENTS

INTRODUCTION

Purpose and Scope

This Technical User Manual describes how to properly overwrite the classified information stored electronically on a computer media, using Blancco 5. The person who performs erasure services must have sufficient security clearance and be authorized in accordance with the storage medium's classification level.

Blancco 5 - Specifications

- This product can be used for the erasure of ATA (i.e. IDE, PATA, SATA, eSATA), SCSI, SAS, USB, Fibre Channel and FireWire drives of any size and with varying block sizes.
- 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.
- Blancco 5 is independent of any operating system on the storage medium, it can erase hidden files and remove HPA and DCO areas. It must be run on machines using x86 architecture.
- System requirements: see user manual (Appendix 1).

References and Notes

This Technical User Manual has been prepared based on the requirements described in Regulations 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 v5.7.0.1 (Appendix 1) describes the detailed and extended use.

Updates

The security Officer / security manager / operator is responsible for informing Blancco Oy Ltd. ("Blancco") about any need to update this document. Blancco will perform needed changes and deliver updated document to the appointed persons.

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 Storage Media

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

Requirements for Training

The leader of the organization is responsible for ensuring that the user is given the necessary training, so that the user can operate Blancco 5 in a secure and appropriate manner.

User Obligations

- 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 and its attachments.
- The 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 the operator / security officer / security manager until the user no longer has access to the relevant system.

Reporting of Security Breaches or Events

All personnel have a responsibility to protect security concerns in their work or business projects, and are obliged to contribute to the preventative security measures. Security breaches, potentially security-threatening events or evidence of an attempt to somehow breach security shall immediately be reported to the Security Officer / Data security manager. The company should implement measures and reporting as specified in the Regulations on security administration.

Reaction to Security Breaches or 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 also be punished accordingly.

DATA STORAGE MEDIA: REUSE, DECLASSIFICATION AND DOWNGRADING

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 the persons that have access to storage medium also have the necessary authorization to handle the classified information on it, and the storage media is overwritten at least once with Blancco 5 v5.7.0.1 (approved by NSM).

The storage 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 to store data classified as HEMMELIG. It is also not allowed to reuse the data storage media that has been used to store KONFIDENSIELT, HEMMELIG or STRENGT HEMMELIG information in an unclassified system.

The operator / 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. Table 1 on page 10 sets the conditions for the reuse and downgrading of storage media used for classified data. The security level declassification or downgrading rules for declassification or downgrading of the security level of the information are provided in the document *Regulations on Information Security* (Chapter 2, B and C). Any 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 5 v5.7.0.1 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.

Notes:

- Downgrading or reuse of data storage media classified LIMITED recommended only if Blancco 5, or another / other tools / methods approved by the NSM is used.
- Reuse of data storage media classified KONFIDENSIELT are allowed only if Blancco 5, or another / 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 strong magnetic field.

Overwriting as an Approved Method

After a storage medium has been erased with Blancco 5, 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 (data classification) of the storage media being processed (see table 1).

Requirements of Overwriting

Blancco 5 is able to overwrite all information from the computer where it is used. In practice this means that the entire disk is overwritten.

Thus, Blancco 5 is capable of overwriting:

- The entire user addressable space.
- Hidden ("hidden") areas of a drive such as the Host Protected Area (HPA) or Device Configuration Overlay (DCO).
- Unused fragments of sectors or blocks of data.
- Sectors or data blocks on disk that have been logically "deleted" i.e. using the usual (not approved) deletion method provided by an operating system.
- Sectors and blocks the system has marked as "not usable" (remapped sectors).

It is verified by the use of Blancco 5 that information is not stored in hidden files or directories, and residual information is not stored on the media. Samples are taken from the disk at the sector/block level to verify that data is removed (see also Appendix 1).

Overview of the re-use, declassification or downgrading the security level using the approved overwrite mechanism from Blancco 5.

	LIMITED Textual Information	KONFIDENSIELT	HEMMELIG
Reuse	1 x overwriting	7 x overwriting	NOT ALLOWED
Downgrading	Not recommended	NOT ALLOWED	NOT ALLOWED
Declassification	7 x overwriting	NOT ALLOWED	NOT ALLOWED

Table 1 - conditions for the reuse and downgrading of storage media

Reuse (definition)

Machine-readable storage medium classified as BEGRENSET or KONFIDENSIELT and used as part of 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 to access the information on it or the storage media is overwritten at least once with Blancco 5 v5.7.0.1 (approved by NSM).

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

Downgrading (definition)

The rules for downgrading information are provided in the Regulations on Information Security (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 either:

1. Re-classified
2. Removed using approved overwrite technique
   or
3. Removed by degaussing

Downgrading of storage media is not recommended. Downgrading where the overwriting is used can only be accepted for information classified BEGRENSET.

Degaussing

A degausser, is an instrument or machine that generates strong magnetic fields, which can distort the magnetic field of HDDs that apply this technology and therefore cause data to become unreadable. Only degaussers approved by NSM may be used.

USER DECLARATION

This statement applies to the use of Blancco 5 v5.7.0.1 for overwriting classified information in accordance with the Security Act and its regulations.

This declaration shall be dated and signed by the user. Two copies should be made: one to be retained by the user, and the other to be kept by the operating / safety manager / security manager.

****

By signing this user declaration, I confirm that:

A. I have read and understood the user documentation that I have received from my supervisor/Security Manager/ Data Security Manager.

B. I understand the obligations and responsibilities associated with using Blancco 5 v5.7.0.1 for use on 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:

Supervisor/Security Manager/ Data Security Manager:

Place / date:

Username:

User Signature:

APPENDICES

Appendix 1

Blancco 5 User Manual for version 5.7.0.1.