ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Claims Testing Application Form

Form Number ADPC00025

Section 1 – Applicant Information

Company Name: Blancco Technology Group
Address: Länsikatu 15, 80110, Joensuu, Finland

General Contact
Name: Jonathan Brew
Phone:
Mobile: +358 44 7388002
E-Mail: jonathan.brew@blanccotechgroup.com

Section 2 – Applicant Software Information

Manufacturer: Blancco
Version of software: 5.10.1

Background (Explanation of the company and software)

Blancco Technology Group is a leading, global provider of mobile device diagnostics and secure data erasure solutions. We help our clients' customers test, diagnose, repair and repurpose IT devices with the most proven and certified software. The company is headquartered in Alpharetta, GA, United States, with a distributed workforce and customer base across the globe. Blancco, a division of Blancco Technology Group, is the global de facto standard in certified data erasure. We provide thousands of organizations with an absolute line of defense against costly security breaches, as well as verification of regulatory compliance through a 100% tamper-proof audit trail.

Blancco 5 is an erasure solution for x86-based tablets, desktops, laptops, servers and storage environments that provides total peace of mind with fully comprehensive post-erasure reports. It is a flexible yet robust solution with the very latest hardware support and cutting-edge, patented SSD erasure capabilities. The feature rich software can be controlled locally or remotely, offers high-speed erasure of high volumes of drives simultaneously, offers RAID dismantling and direct access to the underlying physical drives as well as automated detection and unlocking of freeze locked drives.

Technical / physical architecture of claims test applicant software.

The software performs a series of steps to enable the secure repurposing of SSDs. Depending on the capability of the drive being erased, the software will apply multiple different techniques, accessing the best available erasure process for a given device and determining the success of said process based on the visible results and security enhanced commands. Techniques include writing data to the SSD, totaling the full capacity of the device; partial verification of successful actions; drive issued sanitization commands and a full verification of the entire logical surface of the device.

Best practice usage guide for usage of software being tested. (Please enclose any manuals)

Manual enclosed detailing full operational instructions.

Host Information for claims test applicant software to run on. To be shipped by test claimant.

Minimum System Requirements
* x86 architecture machine
* 1 GB RAM memory in most cases (erasing servers with 2+ drives requires more RAM)
* CD-drive or a CD-compatible drive for CD-booting
* USB-port for exporting / saving reports locally and/or USB-booting
* SVGA display and VESA compatible video card for graphical user interface
* SAS storage controller (for erasing SAS SSDs)

Section 3 – Test Hardware Information

Device 1

Solid State Storage Device chip set of device.

Manufacturer:	Hewlett Packard	Controller:	
Model:	ProLiant SSD/MO0200FCTRN	NAND Chipset	
Capacity:	200 GB	Drive serial no.	40338572

Device 2

Solid State Storage Device chip set of device.

Manufacturer:	Hewlett Packard	Controller:	
Model:	ProLiant SSD/ EO0400FBRWA	NAND Chipset	
Capacity:	400 GB	Drive serial no.	40032672

ADISA Threat Matrix

Risk Level	Threat Actor and Compromise Methods	Test Level
1 (Very Low)	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilising freeware, OS tools and COTS products.	1
2 (Low)	Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	1
3 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising COTS products.	2
4 (High)	Commercial data recovery and computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising both COTS and bespoke utilities.	2
5 (Very High)	Government-sponsored organisations or an organisation with unlimited resources and unlimited time capable of using advanced techniques to mount all types of software and hardware attacks to recover sanitised data.	3

Section 4 – The Claim

Blancco Technology Group's software, Blancco 5, when using the erasure standard "Blancco SSD Erasure" and in accordance with BLANCCO 5 User Manual for version 5.10.1, will remove all available data on the SSD samples within this test to protect from a forensic attack equivalent up to and including Test Level 2 of the ADISA threat matrix.

Claim Technical Contact at applicant.

Name: Blancco Support
Phone: _____
Mobile: _____
E-Mail: support@blancco.com

Acceptance

I, Jonathan Brew of Blancco Technology Group, confirm that the information outlined in this document is an accurate and true reflection of the claims made by our product wishing to undergo the ADISA testing method.

Signed on behalf of Blancco Technology Group
SIGNED:
NAME: Jonathan Brew
TITLE: Research Manager
DATE: 23/06/2016

Claim Accepted by:

Signed on behalf of University of South Wales
SIGNED:
NAME: Andrew Blyth
TITLE: Professor
DATE:

Signed on behalf of ADISA
SIGNED:
NAME: Steve Mellings
TITLE: Director
DATE: