CLAIMS TESTING APPLICATION FORM

FORM NUMBER: ADPC158

SECTION 1 – APPLICANT INFORMATION

Company Name: toolhouse DV-Systeme GmbH

Address: Türltorstr. 16 - 20, 85276 Pfaffenhofen an der Ilm, Germany

General Contact

Name: Sandro Leinzinger

Phone: +49 8441 5044 59

Mobile:

E-Mail: sle@toolhouse.de

SECTION 2 – APPLICANT SOFTWARE INFORMATION

Manufacturer: toolhouse Entwicklungs KG

Version of software: toolstar®testLX with shredderLX-module 5.83

Version of user manual: inbuilt manual- and help-function

Algorithm to be used: Overwrite plus Enhanced Secure Erase

Please describe the means of deployment for your software/hardware product:

The software must be written to a usb drive which is then bootable on the target PC. After booting, the software is started automatically.

Please list the equipment you are intending to ship to execute the test, or the means to access/download your software tool:

None

SECTION 3 – MEDIA WHICH YOUR PRODUCT IS TO BE TESTED ON

1 x SSD

ADISA THREAT MATRIX

TEST LEVEL	THREAT ACTOR	COMPROMISE METHODS	SANITISATION METHOD
1	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilizing freeware, COTS and OS tools.	Keyboard attacks from a motivated individual or professional organisation. Typical attack may be the use of open-source forensic tools or commercial tools.	Aligned to Clear
2	Commercial data recovery and computer forensics organisation able to mount invasive/destructive software and hardware attack, utilising both COTS and bespoke hardware and software.	Laboratory attacks from commercial data recovery experts or specialist forensic scientists. Typical attack may be the use of advanced data recovery software, Chip Readers and protocol decoders. Typical attack would involve analysis of individual hardware components as well as protocol structures.	Aligned to Purge
3	Government-sponsored organisations using advanced techniques to mount all types of software and hardware attacks with unlimited time and resources to recover sanitised data.	An attack agent of unknown capability and unlimited resource. Typical attacks would involve taking theoretical data recovery techniques and making them an actual capability.	Aligned to Destroy

CLAIMS TESTING APPLICATION FORM

SECTION 4 – THE CLAIM

toolstar®testLX with shredderLX-module 5.83, when used in accordance with inbuilt manual- and help-function will overwrite all user data on sample device using algorithm Overwrite plus Enhanced Secure Erase such that no user data can be recovered using forensic techniques aligned with ADISA test level 2.

I, Sandro Leinzinger of toolhouse DV-Systeme GmbH confirm that:

- the product submitted for testing is an automated solution for data sanitisation of the media listed within this document.
- that ownership of any code used within the software is understood and that there are no known ownership disputes.
- that the I have the authority to submit the product for testing and will disclose to laboratory if I am not the developer or owner of the product being submitted.
- that the use of any licenses shared with the laboratory does not contravene any existing software usage licence agreements.

I agree to abide by the ADISA Brand Guidelines when referring to this testing process.

SIGNED: S. Leinzinger

NAME: Sandro Leinzinger

TITLE: Head of Engineering

DATE: 27.09.2022

ACCEPTANCE

Claim Accepted by:

ADISA Research Centre

SIGNED: P. B. Turner

NAME: Dr Phil Turner

TITLE: Director of Technology

DATE: 20.10.2022