**ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE**

# Claims Testing Application Form
### Form Number ADPC0033

| Section 1 – Applicant Information |
|---|

Company Name: Extreme Protocol Solutions
Address: 10 River Road, Suite 101, Uxbridge, MA 01569 (USA)

General Contact
Name: Brian Therrien, ITAD Sales Director
Phone: 508-278-3600 Ext.115
Mobile: 508-422-6916
E-Mail: btherrien@extremeprotocol.com

| Section 2 – Applicant Software Information |
|---|

Manufacturer                Extreme Protocol Solutions
Version of software        XErase – Enterprise Data Erasure V12

**Background (Explanation of the company and software)**

Based in the United States, Extreme Protocol Solutions is an industry leader in software solutions for overwriting of both magnetic and solid-state media. This product has been in use by corporate and industrial clients. Extreme Protocol (EPS) has been in business since 1999 and its engineering team have over twenty years of expertise in storage and hard drive engineering.

**Technical / physical architecture of claims test applicant software.**

Extreme Protocol Solutions Inc. software/ product called XErase Enterprise Data Erasure, when used in accordance with User Manual V12.0 will overwrite/destroy data on both Magnetic Media (Hard Disk Drives) and Solid-State Media (SSD) to protect from a forensic attack equivalent to test level 2 of the ADISA threat matrix.

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

XErase Enterprise Data Erasure V12 Manual provides concise and detailed guidance for software operation across all deployment platforms.

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

EPS has varied solutions for direct connected erasure. At time of testing EPS will provide hardware and software to facilitate erasures using the various deployment methods indicated in the physical architecture claim section.

EPS will provide 2 media samples for each of the following media types; magnetic media, and SSD media. These are:

1. Micron 2.5 SSD  Model: MTFDDAK256TBN
2. SanDisk Lightening Enterprise Class SSD  Model No: LB406M
3. Dell Enterprise  Model number ST91000642SS
4. WD Scorpio Blue / 500GB / WD5000BPVT / SATA / Electromechanical Drive

ADISA Threat Matrix

| Risk Level | Threat Actor and Compromise Methods | Test Level |
| --- | --- | --- |
| 1<br><br>(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<br><br>(Low) | Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks. | 1 |
| 3<br><br>(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<br><br>(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<br><br>(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 |

Extreme Protocol Solutions Inc. software/ product called XErase Enterprise Data Erasure, when used in accordance with User Manual V12.0 will overwrite data / destroy data carrying media on the hardware sample within this test to protect from a forensic attack equivalent to test level 2 of the ADISA threat matrix.

Specifically, the NIST 800-88 Rev1 Purge Erasure Method will perform the functions supported by each individual drive.  These include Block Erase, Block Overwrite and Cryptographic Erasure.

Additionally, the 3x Wrt/Vfy – DoD Sanitize performed on a hard drive will apply a pattern, it's compliment and finally a repeating random block of data to all accessible blocks of the media making any previous data unrecoverable.

Erasure methods can be selected by using the Wrench/Screwdriver Button in XErase and selecting the appropriate method prior to the start of each test.

Claim Technical Contact at applicant.

Name:   Brent Burkholder, VP of Engineering
Phone:  508-278-3600, Ext. 113
Mobile: 774-287-6257
E-Mail: bburk@extremeprotocol.com

**Acceptance**

I, <u>Roger D. Gagnon</u> of <u>Extreme Protocol Solutions Inc.</u> 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 <u>Extreme Protocol Solutions Inc.</u>
SIGNED:
NAME: Roger D. Gagnon
TITLE:  President and CEO
DATE:  01/28/2018

Claim Accepted by:

Signed on behalf of University of South Wales          Signed on behalf of ADISA

SIGNED:                                                SIGNED:
NAME:    Andrew Blyth                                  NAME:   Steve Mellings
TITLE:    Professor                                    TITLE:    Director
DATE:    30.01.2018                                    DATE:    30.01.2018