ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

# Claims Testing Application Form

## Form Number ADPC0012

### Section 1 – Applicant Information

Company Name: **ITRenew Inc.**
Address: 8356 Central Avenue, Newark, CA 9560

General Contact
Name: Matt Mickelson
Phone: 001 408 799 4118
Mobile: 001 408 799 4118
E-Mail: matt.m@itrenew.com

### Section 2 – Applicant Software Information

Manufacturer **ITRenew Inc.**
Version of software **Teraware v2.15**

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

The Teraware platform discovers the target device and capabilities to formulate a multi-stage, forensic-level, sanitization protocol for a solid state device.
Stage 1 - Teraware determines if the target drive supports back-end AES encryption. If so, Teraware will initiate the CRYPTOGRPAHIC_ERASE command to delete the key between the NAND controller and the NAND components. This first step quickly obfuscates the user data making it unavailable.
Stage 2 - Teraware applies the PRNG_OVERWRITE process to the logical capacity. This process is measuring the devices ability to handle host I/O and collect medium statistics that contribute to final disposition decision making.
Stage 3 - Teraware employs a method to issue a BLOCK_ERASE cycle to each of the physical NAND blocks effectively eliminating all previously written data to the physical medium. This step disregards the defect error registers and will address all physical blocks on the NAND chips.
Stage 4 - Teraware performs a DEVICE_ISSUED_OVERWRITE command that will write a designated pattern to all physical NAND blocks using a program cycle. If the drive does not offer self-issued overwrites, then Teraware shall issue a LOGICAL_OVERWRITE command to cover the logical user capacity.
Stage 5 - Verification. Teraware performs a VERIFICATION process on the logical capacity to ensure sanitization of this area is exhaustive.

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

***TW_Appliance_Users_Guide_v1.0.pdf***

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

1x Teraware Appliance (contains the application, database, and deployment system)
1x Dell DCS 2100 server w/LSI SAS 9211-4i HBA + Qlogic 4Gb FC HBA (processing station)
1x FC T-Card adapter, SFP, and fibre cable
Teraware User Guide
Setup doc

## Section 3 – Test Hardware Information

| VENDER | FAMILY | MODEL | CAPACITY | INTERFACE | RISK LEVEL | TEST LEVEL | CERT LISTING NAME |
|---|---|---|---|---|---|---|---|
| EMC | Clariion CX SSD | Z16IFE3B-200/520UC-EMC | 200GB | FC-SSD | 1,2,3,4 | 2 | EMC Clariion CX SSD 200GB FC-SSD |
| HP | ProLiant SSD | MO0200FCTRN | 200GB | SAS-SSD | 1,2,3,4 | 2 | HP ProLiant SSD 200GB SAS-SSD |
| HP | ProLiant SSD | EO0400FBRWA | 400GB | SAS-SSD | 1,2,3,4 | 2 | HP ProLiant SSD 400GB SAS-SSD |
| Intel | 320 Series | SSDSA2BW160G3D | 160GB | SATA-SSD | 1,2 | 1 | Intel 320 Series 160GB SATA-SSD |
| Intel | 320 Series | SSDSA2BW160G3L | 160GB | SATA-SSD | 1,2 | 1 | (Dell) Intel 320 Series 160GB SATA-SSD |
| Intel | X25-M | SSDSA2M160G2GC | 160GB | SATA-SSD | 1,2 | 1 | Intel X25-M 160GB SATA-SSD |
| Kingston | SMS450S3 Series | SMS450S380G | 80GB | SATA-SSD | 1,2 | 1 | Kingston SMS450S3 Series 80GB SATA-SSD |
| Samsung | PM800 Series | MMCRE28G5MXP-0VB | 128GB | SATA-SSD | 1,2 | 1 | Samsung PM800 Series 128GB SATA-SSD |
| Samsung | PM810 Series | MZ7PA128HMCD-01 | 128GB | SATA-SSD | 1,2 | 1 | Samsung PM810 Series 128GB SATA-SSD |
| Samsung | SS410 Series | MCBQE32G5MPP-0V | 32GB | SATA-SSD | 1,2 | 1 | Samsung SS410 Series 32GB SATA-SSD |
| Toshiba | THNSNCxxxGMMJ Series | THNSNC128GCSJ | 128GB | SATA-SSD | 1,2 | 1 | Toshiba THNSNCxxxGMMJ Series 128GB SATA-SSD |

ADISA Threat Matrix

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

The Teraware Digital Asset Disposition Platform can forensically sanitise the solid state devices supplied within this claim with reference to the ADISA Risk Levels identified within section 3; and generates a Certificate of Sanitisation upon successful sanitisation.

Claim Technical Contact at applicant.

Name: _____

Phone: _____

Mobile: _____

E-mail: _____

## Acceptance

**I, Matt Mickelson of ITRenew 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 ITRenew

SIGNED:

NAME: Matt Mickelson

TITLE: Director, Product Management

DATE:

Claim Accepted by:

Signed on behalf of University of South Wales

SIGNED:

NAME: Andrew Blyth

TITLE: Professor

DATE: 19.05.2014

Signed on behalf of ADISA

SIGNED:

NAME: Steve Mellings

TITLE: Director

DATE: 19.05.2014