ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Claims Testing Application Form

Form Number ADPC0028

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.mickelson@itrenew.com

Section 2 – Applicant Software Information

Manufacturer **ITRenew Inc.**
Version of software **Teraware v3.00**

Technical / physical architecture of claims test applicant software.

The Teraware platform discovers the target device and capabilities to formulate a multi-step, forensic-level, sanitization protocol for a solid state device.
STEP 1: CRYPTOGRAPHIC ERASE – Teraware designates the first step in the process to address the devices that support the means to delete the cryptographic key between the flash controller and the NAND flash. This step uses one of several possible commands best suited to address the cryptographic key erasure.
STEP 2: PRNG OVERWRITE – Teraware applies a pseudorandom pre-deterministic data pattern to the device that covers all user block address.
STEP 3: BLOCK ERASE – Teraware will issue a firmware based command that will trigger a back-end block erase command to the NAND flash that will eliminate all data from the user provisioned data areas and also the reserved blocks of the NAND. This step uses one of several possible commands best suited to address the block erase command.
STEP 4: OVERWRITE ERASE – Teraware performs another overwrite step that is designed to prepare the device for re-use by remapping the poor performing NAND blocks and re-write the bad block table. To execute this process, Teraware may issue a firmware based technique that will perform a full medium overwrite of the drive. If the device does not offer a means of self-overwrite, Teraware shall issue a host overwrite method.
STEP 5: MEDIA VERIFICATION – Teraware performs a full verification of all user provisioned blocks of the device to confirm the absence of any user data or unstructured data patterns.

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

Teraware_User_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 and deployment system)
1x Dell CS24-TY server w/LSI 4Gb FC HBA (processing station)
1x EMC DAE Disk Enclosure
Teraware User Guide

Section 3 – Test Hardware Information

VENDER	FAMILY	MODEL	CAPACITY	INTERFACE	RISK LEVEL	TEST LEVEL	CERT LISTING NAME
Intel	DC P3600 Series	SSDPEDME400G401	400GB	NVMe-SSD	1,2	1	Intel DC P3600 Series 400GB NVMe Adapter
Intel	540s Series	SSDSC2KW480H6X1	480GB	SATA-SSD	1,2	1	Intel 540s Series TLC 480GB SATA-SSD
EMC/STEC	EMC Enterprise Flash Drives	Z16IFE3B-200	200GB	FC-SSD	1,2,3,4	2	EMC Clariion EFD 200GB FC-SSD

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

The Teraware Digital Asset Disposition Platform version 3.0 can, using Teraware SAS/SATA SSD sanitization method and by following instructions within Teraware User Guide v 1.0, forensically sanitise the solid state devices supplied within this claim removing all user data such that it is unrecoverable using techniques aligned to ADISA Test Levels 1 or 2 as outlined in section 3. Upon successful sanitisation, it produces a Certificate of Sanitisation to validate this.

Claim Technical Contact at applicant.
Name: Matt Mickelson
Phone: 408-799-4118
Mobile: 408-799-4118
E-mail: matt.mickelson@itrenew.com

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: 12/09/2016

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: