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 hard disk drive based on the guidelines set forth on the NIST 800-88 guidelines for media sanitization. The basic guidelines reference a full overwriting pass across all user LBAs.
STEP 1: OVERWRITE PASS – Teraware shall enumerate all logical block addresses (LBAs) with a 00h pattern.
STEP 2: MEDIA VERIFICATION – Teraware performs a full verification of all LBAs of the device to confirm the absence of any user data or unstructured data patterns using a reference pattern of 00h.

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 SAS 9211-4i HBA (processing station)
Teraware User Guide

Section 3 – Test Hardware Information

VENDER	FAMILY	MODEL	CAPACITY	INTERFACE	RISK LEVEL	TEST LEVEL	CERT LISTING NAME
Seagate	Archive HDD	ST8000AS0002	8TB	SATA-HDD	1,2,3,4	2	Seagate Archive SMR 8TB 4K SATA-HDD
HGST	Ultrastar He10	HUH721010AL4200	10TB	SAS-HDD	1,2,3,4	2	HGST Ultrastar He10 10TB SAS-HDD

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 NIST 800-88 (1-pass) sanitization method and by following instructions within Teraware User Guide v 1.0, forensically sanitise the 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: