

CLAIMS TESTING APPLICATION FORM

FORM NUMBER: ADPC100



SECTION 1 – APPLICANT INFORMATION

Company Name: FutureDial Incorporated

Address: 392 Potrero Avenue, Sunnyvale, CA 94085

General Contact

Name: Clarice Liao

Phone: 001 (408)-2458880 x 205

Mobile: 001 (408) 8281110

E-Mail: cliao@furedial.com

SECTION 2 – APPLICANT SOFTWARE INFORMATION

Manufacturer: FutureDial Incorporated

Version of software: Data Storage Eraser 3

Version of user manual: 3.0

Algorithm to be used: DOD (3) for HDD and Security Erase for SSD

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

FutureDial's Data Storage Eraser™ (DSE) erases HDD/ SSD drives through externally-connected USB drive. When the work station is booted from FutureDial's DSE USB drive, FutureDial DSE starts to erase the local HDD/SSD. The internet connection is required during the operation for reporting, tracking and validation purpose.

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

1. FutureDial USB boot drive with DSE 3 installed.

CLAIMS TESTING APPLICATION FORM



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

The target of this claims test will be:

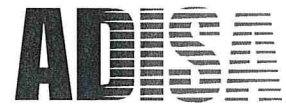
Disk Maker Disk Model Disk Capacity Disk Interface

1 x Westgate WD5000LPLX-66ZNTT1 500Gb SATA-HDD
 1x Kingston SKC400S37256G 256Gb SATA-SSD

ADISA Threat Matrix

RISK LEVEL	THREAT ACTOR AND COMPROMISE METHODS	TEST LEVEL
1 (Low)	<p>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.</p> <p>Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.</p>	1
2 (Medium)	<p>Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising COTS products.</p> <p>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.</p>	2
3 (High)	<p>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.</p>	3

CLAIMS TESTING APPLICATION FORM



SECTION 4 – THE CLAIM

FutureDial's Data Storage Eraser™ (DSE), when used in accordance with User Manual version 3.0 and using algorithm as specified in section 2, will sanitize the solid state and magnetic hard drives listed in Section 3 of this claims test application, such that the all user data is unrecoverable using techniques aligned to ADISA Test Levels 1 and 2 as outlined in Section 3. Upon successful sanitization, it produces a Certification of Sanitization to validate this.

I, Clarice Liao of Future Dial, Inc 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 Future Dial, Inc

SIGNED: 

NAME: Clarice Liao

TITLE: Executive Director, Operations

DATE: 2/8/2021

ACCEPTANCE

Claim Accepted by:

ADISA Research Centre

SIGNED: 

NAME: Dr Andrew Blyth

TITLE: Director of Research and Technology

DATE: 05.02.2021