ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Claims Testing Application Form
Form Number ADPC00020

Section 1 – Applicant Information

Company Name: Piceasoft Limited
Address: Visiokatu 1, 33720 Tampere, Finland

General Contact
Name: Jukka Tuomi
Phone:
Mobile: +358 40 511 6168
E-Mail: jukka.tuomi@piceasoft.com

Section 2 – Applicant Software Information

Manufacturer Piceasoft Limited
Version of software PiceaEraser 3 v.3.0.5809.21333

Background (Explanation of the company and software)
Piceasoft Limited brings services to the mobile retail business area. PiceaEraser, based on Varsta Software's technology, is part of complete product suite for mobile phone retail industry.

PiceaEraser is a software product that enables safe disposal, reuse or resale of mobile devices by permanently erasing all the sensitive user data. Based on smartphone manufacturer, model and operating system version, PiceaEraser applies different sorts of measures to the smartphone in order to sanitise it properly. Afterwards, the consumer who is either giving their mobile away or selling it for recycling can rest assure that no personal information will end up in anyone else's hands.

Technical / physical architecture of claims test applicant software.
Installation package contains all of the information that is required to install PiceaEraser application and run the setup user interface. The installation package is meant to run on a x64 based Windows 7 desktop PC with minimum 2 GB of free memory (4 GB installed) with latest updates installed from Windows Update. There must be at least one free USB v2 port in the PC into which the devices to be erased are connected. If you want to erase the devices simultaneously, please see the instructions from usage guides for setting up the USB HUBs correctly.

Internet connection is required for the application to be installed and ran.

License key must be provided to the application during the initial configuration setup.

Standard customer mail with installation instructions is provided with license key. Access to Piceasoft Analytics service is provided from where the erasure results are available. Reports can be saved to local folder also. Only successfully erased devices should be subjected to the recovery test.

Best practice usage guide for usage of software being tested. (Please enclose any manuals)
User guides are accessible from inside the application. Technical support via online desktop sharing services can be provided so that the application start-up and operation goes without hassles. User

guide versions:

- Android Preparation and Erasure Process Description V03
- iPhone Preparation and Erasure Process Description V04
- Windows Phone Preparation and Erasure Process Description V01
- Other user guides 1.0.

Host Information for claims test applicant software to run on. To be shipped by test claimant.
None.

Section 3 – Test Hardware Information

Type: Android smartphone
Device: LG Spirit 4G LTE (LG-H440n)
OS: Android 5.0.1
IMEI: 358819064316954

Type: Android tablet
Device: Samsung Galaxy Tab (SM-T230)
OS: Android 4.4.2
Serial: R52F90252AY

Type: Apple smartphone
Device: Apple iPhone 6 (iPhone7,2)
OS: IOS 9.1
IMEI: 352068066458952

Type: Apple tablet
Device: Apple iPad 1 (iPad1,1)
OS: IOS 5.1.1
IMEI: 012439000869483

Type: Windows Phone smartphone
Device: Microsoft Lumia 532 (RM-1034)
OS: Windows Phone 8.1
IMEI: 357129064423961

Type: Windows Phone smartphone
Device: Nokia Lumia 520 (RM-914)
OS: Windows Phone 8.1
IMEI: 358995052193488

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

Piceasoft Limited PiceaEraser 3, when used in accordance with the on-line guidance provided for version v0.3 in December 2015, will sanitise the user data on the smartphones and tablets within this test to protect from forensic attack equivalent to risk level 2 (test level 1) of the ADISA Threat Matrix.

Claim Technical Contact at applicant.

Name: Pasi Kytölä
Phone:
Mobile: +358 40 564 9722
E-Mail: pasi.kytola@piceasoft.com

Acceptance

I, Jukka Tuomi of Piceasoft Limited 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 Piceasoft Limited

SIGNED:

NAME: Jukka Tuomi

TITLE: General Manager

DATE: 8.12.2015

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: