ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

ADISA Certified Members Statement

PRM Green Technologies LTD

Unit 16A Watling Street Business Park,Cannock ,Staffordshire ,WS11 9XG

The Asset Disposal and Information Security Alliance (ADISA) was launched in 2010 as a certification scheme for companies who participate in IT asset recovery offering data sanitisation services. These companies are Data Processors and must operate in a specific way in order to help their customers, the Data Controller, comply with previous and new data protection regulations.

The scheme is open to those wish to operate their business to the very highest of standards and are willing to undertake regular scrutiny by an experienced auditing team.

The ADISA standard comprises of six main modules with a total of 112 Essential Criteria that MUST be passed to gain certification with over 80 further criteria which are classed as Highly Desirable. These extra marks are added to the overall score with members being certified as a Pass, Pass with Merit, Pass with Distinction or with a Pass with Distinction with Honours which is the highest award ADISA can give and with only five members achieving this.

ADISA members agree to being subjected to regular (Full) audits at least once every three years but also undergo completely unannounced (Spot-check) audits at least once a year. At these, our auditor turns up with no prior warning and not only checks that the operational side of the business is running in accordance with the ADISA Standard but also selects ten or more data bearing assets and forensically checks them to ensure data has been removed. Only when these checks are passed does the member retain their certification. Unlike some other schemes, ADISA members are only remain on if they maintain their compliance with the Standard and organisations have been removed and / or suspended until such a point that their business returns to a compliant position. ADISA's view is that where data security is concerned, we cannot afford to permit organisations to work towards compliance whilst holding the title of "ADISA Certified". As a result, the ADISA membership works very hard to meet this robust approach in order to maintain their certificated status.

The forensic checks follow the following guidelines:

Testing of Hard and Solid-State Drives

This is a forensic level attack using COTS products to replicate a professional level of threat.

Each drive selected is connected to a computer via a forensic write-blocker. The role and function of the write-blocker is to ensure that:

a) No data was written back to the hard-drive when the hard-drive was powered up and connected to the ATA command bus,

b) The drive at all times when connected to the ATA command bus, remains in a stable state.

Once the hard-drive had been powered up, a forensic analysis of the hard-drive is performed using FTK. This analysis allows us to identify if data is present on the hard-drive.

Testing of Smart Phones Procedure

This is a keyboard level attack to replicate a user level of threat. The auditor follows this process:

- Identify the IMEI either by physically checking on battery cover (if appropriate) or powering the device up.
- Power up phone and see if any previous data is present by the following:
    - Check Phone Directory.
    - Check browsing history.
    - Check Text.
    - Check for third party apps.

Testing of Networking Equipment Procedure

This is a proficient user level attack to replicate a professional level of threat.

- Switch on device and connect to it via a terminal connection.
- Log onto the networking equipment using manufacturers' standard network user name and password.
  (This is to be found via internet search).
- Examination of config files to confirm factory reset.

The ADISA Standard has been formally recognised by DIPCOG, a UK MoD and NCSC Committee, and is listed on the National Cyber Security Centre's own guidelines as an accreditation to be considered by companies when disposing of their assets.

In addition to certifying the ITAD service ADISA also offers approval of software and hardware data sanitisation tools. ADISA is the only entity worldwide that is approving software overwriting tools for use on Solid State Drives and broader flash media. This is undertaken with the test laboratory at University of South Wales overseen by one of the world's leading IT forensics experts – Professor Andrew Blyth.

Later in 2018, ADISA will be launching a GDPR compliance certificate for members who will be able to show how they comply with the requirements for their customers (Data Controllers) and themselves as Data Processor for key criteria listed within Chapter 4 of the GDPR.

Finally, ADISA also offers its member's customers Monitoring Service where the audit results are sent directly to the members customers giving them peace of mind that their chosen ITAD is still operating to the very highest of standards.

Steve Mellings

FOUNDER, ADISA

ADISA Member PRM Green Technologies LTD

Certified Location: Unit 16A Watling Street Business Park,Cannock ,Staffordshire ,WS11 9XG

ADISA members since December 2019 PRM are certified with Distinction and have undergone the following audit schedule since joining.

Audit Date	Audit Type	Result
Thursday 18th February 2020	Full Audit to Transition over to the new ADISA Standard 7.0	Pass with Distinction
Tuesday December 10th 2019	Gateway Audit	Pass with Distinction