CDL

Computer Disposals Limited

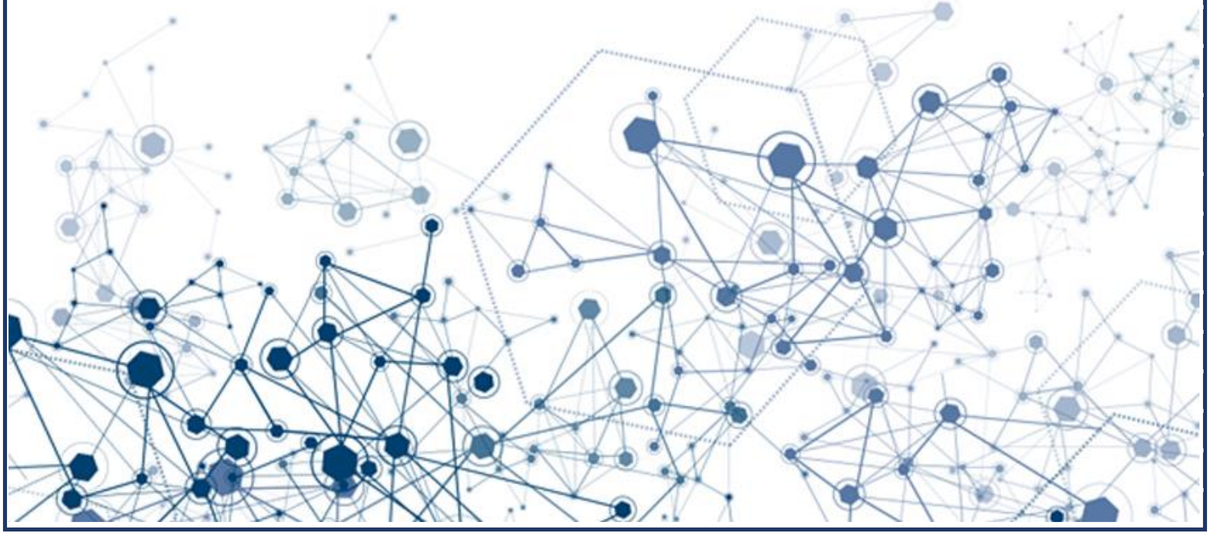
DATA CAPABILITY STATEMENT

Version 1.8 (2019)

Computing Security Awards

Data Erase Company of the Year 2019
Editors Choice 2019

Information Security Management System
27001
Certified



Computer Disposals Ltd - Introduction

The main concern faced by our customers when disposing of their redundant IT equipment is the removal and destruction of personal and/or sensitive personal data contained within them. With the new General Data Protection Regulations (GDRP) in effect it is more important than ever to ensure your data is processed correctly and lawfully.

CDL are an award winning company for providing this service, taking away the concerns of data controllers when it comes to data sanitisation. CDL hold the following accreditations, awards and insurances which will help to satisfy your GDPR 'due diligence' legal requirement...

- ADISA Accredited with Distinction
- Data Erase Company of the Year 2017, 2018 and 2019
- UK Government Cyber Essentials Plus
- ISO 27001:2013 Information Security Management Standard
- ISO 9001, 14001 and 18001
- NHS IG Toolkit compliant
- Halton Business of the year 2017 and 2018
- Cyber Security Insurance to £5,000,000
- EU GDPR Compliant
- Security Compliance Award 2018
- Security Company of the Year 2018
- Security Awards Editors Choice 2019

CDL can provide sanitisation requirements expected by data controllers in the following ways:

Non-Destructive - Data on the media type is overwritten which then allows the device to be reused.

Destructive - The media type is pysically destroyed making it un-usable.

In House and On Site sanitisation is carried out with the following compliance methods:

In House - CDL will collect your equipment using our own satellite tracked vehicles and Enhanced DBS checked drivers. All CDL vans are fitted with a two camera CCTV system, one forward facing and one in the rear of the vehicle, overlooking the equipment.

Items are then processed at CDL facility which has one of the highest rated security systems available. The site perimeter is surrounded by 2.4 meter prison mesh fencing. The site is also covered by 30 x external and internal analytic, full colour night vision CCTV cameras and a further 35 x CCTV cameras with full PIR coverage, including 7 x PTZ cameras and an ANPR camera. Both the CCTV and alarm system are externally monitored 24/7 with a PA system and regular security patrols. During working hours, a security guard is present throughout the day to make regular perimeter checks and conduct employee searches. All site gates and internal doors are access controlled with relevant permissions.

On Site - Using our dedicated data destruction vehicle we can provide all our destructive services on site. The vehicle is equipped with our high level degausser, crypto cut shredder and hard drive crush box. The vehicle can be run on generator or can be mains powered for silent running. Alternatively the destruction equipment can be removed and used in our clients premises. The vehicle is also satellite tracked and has a two camera CCTV system, one forward facing and one in the rear of the vehicle overlooking the equipment being destroyed.

IN HOUSE DATA CAPABILITY

MEDIA TYPE	Non-Destructive	Standard Level Destruction	Higher Level Destruction
Magnetic Hard Drive	Erase using Whitecanyon Wipedrive V8 (HMG IS5 Enhanced wipe method (NCSC Assured Standard)	Shred using Untha RS40 to 40mm	Shred using Untha RS40 to 20mm or 6mm
Solid State Drive	Erase using Whitecanyon Wipedrive V8 (NIST 800-88r1 wipe method (ADISA Claims Tested Standard)	Shred using Untha RS40 to 40mm	Shred using Untha RS40 to 20mm or 6mm
Back Up Tape and Floppy Disk	Not Available	Shred using Untha RS40 to 20mm	Shred using Untha RS40 to 20mm or 6mm
Mobile Device	Erase using BlackBelt Datawipe V3 (ADISA Claims Tested Standard)	Shred using Untha RS40 to 40mm	Shred using Untha RS40 to 20mm or 6mm
Flash Media / SD Card / CD-ROM	Not Available	Shred using Kobra 430 TS Shredder	Shred using Kobra 410 TS Shredder
Printer / Copier / MFD	Not Available	Remove hard drive and shred using Untha RS40 to 40mm	Remove hard drive and shred using Untha RS40 to 20mm or 6mm
Router and Switch	Reset to factory default following manufacturers instructions.	Remove boards and shred using Untha RS40 to 40mm	Remove boards and shred using Untha RS40 to 20mm or 6mm
Terminal / Thin Client	Erase using Whitecanyon Wipedrive V8 (HMG IS5 Enhanced wipe method (NCSC Assured Standard)	Shred using Untha RS40 to 40mm	Shred using Untha RS40 to 20mm or 6mm
IP Phone	Reset to factory default following manufacturers instructions.	Shred using Untha RS40 to 40mm	Shred using Untha RS40 to 20mm or 6mm

ON SITE DATA CAPABILITY

MEDIA TYPE	Non-Destructive	Standard Level Destruction
Magnetic Hard Drive	Erase using Whitecanyon Wipedrive V8 with HMG IS5 Enhanced wipe method (NCSC Assured Standard)	Destroy using eDR disk crusher
Solid State Drive	Erase using Whitecanyon Wipedrive V8 with NIST 800-88r1 wipe method (ADISA Claims Tested Standard)	Destroy using eDR disk crusher
Back Up Tape and Floppy Disk	Not Available	Degause using Verity V880 Degausser or Proton T4
Mobile Device	Erase using BlackBelt Datawipe V3 (ADISA Claims Tested Standard)	Destroy using eDR disk crusher
Flash Media / SD Card / CD-ROM	Not Available	Shred using Kobra 410 TS Shredder
Printer / Copier / MFD	Not Available	Remove hard drive and destroy using eDR disk crusher
Router and Switch	Reset to factory default following manufacturers instructions.	Remove boards and drill FPGA memory
Terminal / Thin Client	Erase using Whitecanyon Wipedrive V8 with HMG IS5 Enhanced wipe method (NCSC Assured Standard)	Remove flash drive and shred using Kobra 410 TS shredder
IP Phone	Reset to factory default following manufacturers instructions.	Not Available

Data bearing and sanisitation restricting controls

Computer Disposals Limited

The following system features have been identified by CDL as data bearing and/or impact data sanitisation attempts.

It is our standard procedure to ensure these features are cleared and/or factory reset.
If this procedure fails then the asset will be securely destroyed.

BIOS PASSWORD
A password preventing changes to the system BIOS

COMPUTRACE
A serial register held by a client which allows remote management of the machine

TPM (Trusted Platform Module)
A crypto processor on a motherboard which can store a data encryption key

AMT (Active Management Technology)
A service processor on a motherboard which can allow remote access

SPLASH SCREEN
An image displayed when booting showing the BIOS or manufacturer logo

DELL OWNERSHIP / ASSET TAG
Ownership and Asset information displayed when booting and in the BIOS

HP iLO (Integrated Lights Out)
A service processor on a motherboard or expansion card which can allow remote access

DELL DRAC (Dell Remote Access Controller)
A service processor on a motherboard or expansion card which can allow remote access

GENERIC REMOTE ACCESS CONTROLLER
A service processor on a motherboard or expansion card which can allow remote access

FMIP/ FMD LOCK
A clients Apple or Google cloud lock which makes a mobile device unusable

APPLE DEP (Device Enrolment Program)
A serial number register held by a client which allows remote management and software Installation

APPLE PRAM PASSWORD
A password preventing changes to apple PRAM

Please be aware that some features may remain active if they are held on a client register, even after data sanitisaztion. It is the clients reponsibility to ensure devices are removed prior to collection.

UNTHA RS40 Shredder

UNTHA
shredding technology

CDL's Untha RS40 shredder has a four shaft shredding system that achieves exacting output specifications and impressive throughputs. Hard-wearing cutters and integrated protection from unshreddables equate to an unrivalled data destruction method.

The Untha RS40 is a secure destruction solution for most data bearing items.

CDL shred items to the following sizes as a standard destruction method...

Hard Drives - 40mm
Switches and Hubs - 40mm
Terminal / Thin Clients - 40mm
IP Phones - 40mm
Mobile Devices - 40mm
Back up Tape and Floppy Disk - 20mm
Data Bearing SMW - 40mm

We can also offer a higher level of destruction, shredding to 20mm or 6mm on request.

WhiteCanyon Wipedrive Version 8 - Magnetic HDD

National Cyber Security Centre
a part of GCHQ

White Canyon Wipe Drive overwriting software, which is the only overwriting software that has been successfully evaluated to the EAL 4+ standard and is the only software approved by the likes of Interpol, Homeland Security, IBM, Microsoft and Cisco.

White Canyon Wipe Drive 8 is CPA (CESG) approved in the UK under the NCSC for the sanitisation of all data on magnetic hard drives.

By conforming to CPA and NIAP certification White Canyon meets many global standards to include:

GB Infosec Enhanced Standard 5
NIAP EAL 4+
US DoD 5220.22-M
NATO NAPC
NST 800-88 Rev 1 Compliant
FACTA Standards
Sarbanes-Oxley
US Army AR380-19
US Air Force System Security Instruction 5020
US Naval Staff Office Publication P-5329-26
US National Computer Security Centre TG-025
Australian Defence Signals ACSI-33 (X1-P-PD)
Canadian RCMP TSSIT OPS-II Standard Wipe
German VSITR
CSEC ITSG-06
HIPAA

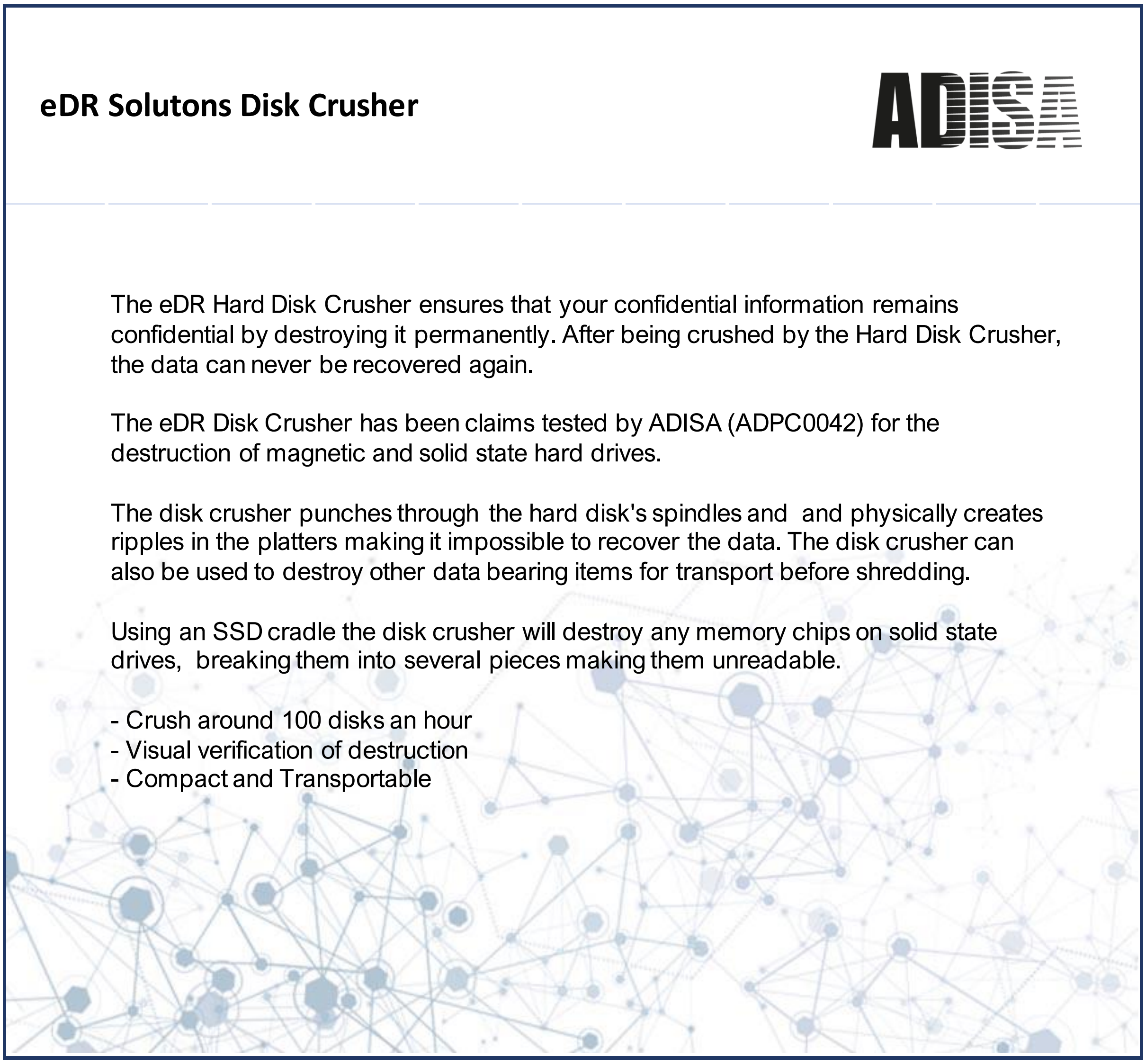
WhiteCanyon Wipedrive - Solid State Drives

While the approach for erasing magnetic hard drives is widely understood, solid state disks (SSD) require different techniques to achieve sufficient data security.

Because Solid State Disk (SSD) storage technology is inherently unique in the way data is stored, the assumption that the erasure techniques that work for traditional hard drives will also work for SSDs is problematic. This is due to wear leveling and redundant memory blocks that can't be accesed by most erasure solutions.

WhiteCanyon WipeDrive 8 has been claims tested by ADISA (ADPC0036) for sanitisation of data on solid state drives unsing the NIST 800-88r1 algorithm.

CDL has worked closely with WhiteCanyon and ADISA to achieve this claims test which is something many other data processor's cannot offer.



eDR Solutons Disk Crusher

The eDR Hard Disk Crusher ensures that your confidential information remains confidential by destroying it permanently. After being crushed by the Hard Disk Crusher, the data can never be recovered again.

The eDR Disk Crusher has been claims tested by ADISA (ADPC0042) for the destruction of magnetic and solid state hard drives.

The disk crusher punches through the hard disk's spindles and and physically creates ripples in the platters making it impossible to recover the data. The disk crusher can also be used to destroy other data bearing items for transport before shredding.

Using an SSD cradle the disk crusher will destroy any memory chips on solid state drives, breaking them into several pieces making them unreadable.

- Crush around 100 disks an hour
- Visual verification of destruction
- Compact and Transportable

BlackBelt - Smartphone and Tablet DataWipe

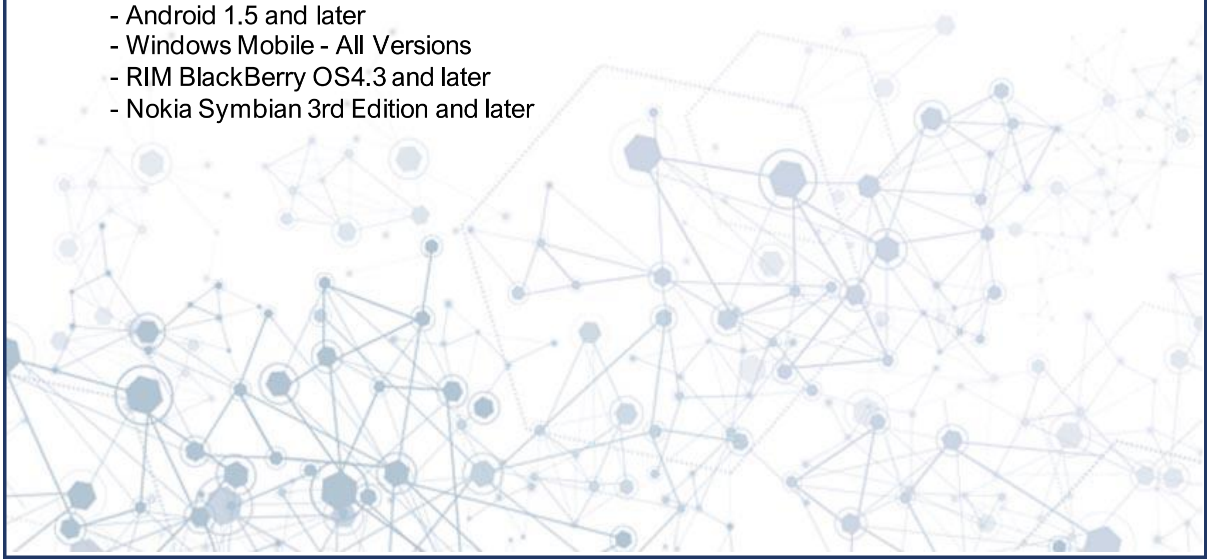
Blackbelt data erasing solution ensures that any handsets or tablets with confidential information attached, is wiped clear as effectively as possible. It means that all data is permanently removed from that device with three overwrites and a verification pass.

Erasing mobile device data is an excellent way to protect customer data and avoid any unnecessary destruction or re-procurement costs. Not only that, but erasing mobile device data also allows recycler companies to redistribute used handsets quickly and effectively, safe in the knowledge that all previous data has been destroyed.

BlackBelt Datawipe 3.8 has been claims tested by ADISA (ADPC0038) for use on iOS and Android mobile devices.

Balckbelt DataWipe can santise the following platforms..

- Apple iOS - All Versions
- Android 1.5 and later
- Windows Mobile - All Versions
- RIM BlackBerry OS4.3 and later
- Nokia Symbian 3rd Edition and later



Proton T-4 Higher Level Deguasser

The Proton T-4 deguasser is NSA approved which is recognised by the NCSC for meeting higher level degaussing standards as defined in HMG IS5. This is the highest level of data santisiation offered in the UK. This approval applies to all magnetic media such as..

- Hard Dirves
- DLT/LTO Tapes
- Other Magnetic Tapes
- Floppy Disks
- Audio Tapes

The Proton T-4 produces a bi-directional field which provides a 20,000 Gauss positive field and a 20,000 Gauss Negative field. The T-4 achieves this by using a unique, patented "Reverse Polarity". Other degaussers may have either a positive or negative pulse, but only one. The T-4 has both and it is fully automatic. This ensures complete and permanent erasure of your data.

- Approved to erase all magnetic media available today and guaranteed on 8 TB hard drives

- Listed on the National Security Agency's Evaluated Products List (NSA EPL-Degausser) and complies with DoD requirements for destroying classified information on magnetic media

- Internal software requires all parameters (capacitor voltage, switch, etc.) are present before degaussing. This software guarantees that each degauss cycle delivers sufficient strength and consistent performance

Kobra 410TS HS - High Security Crypto Cut Shredder

CPNI
Centre for the Protection of National Infrastructure

The Kobra 410TS is CPNI approved for high security shredding to meet standards as defined in HMG IS5.

The 410 TS is a High Security 0.8x9.5mm Crypto Cut shredder, suitable for shredding Top Secret and Crypto Paper documents as well as Optical Media including CD's/DVD's & Blu-Ray Discs, 80mm mini disks and credit cards.

The 410 TS has a security Level of P-6 and has been approved by the UK Government to meet the most stringent High Security requirements required and are recommended for all Military Bodies, Government Agencies or Security Commercial Organisations.

The 410 TS can shred up to 3000 pieces of Optical Media per hour and will turn a single sheet of paper into 10-15,000 individual pieces. The special 2.5x1.5mm OM cutting system has the highest security level available today and exceeds the Optical Media Destruction Devices guidelines and the ASIO T-4 standards for TOP SECRET level destruction of Optical Media.

- 0.8x9.5mm Crypto Cut
- Din Security Level P-6
- 410mm Entry Throat (A4, A3 and Printouts)
- CPNI Approved for Paper, Credit Cards, CD ROMS and Floppy Disks

Kobra 430TS - High Performance Cross Cut Shredder

The Kobra 430 TS Industrial Shredder is a very high performance, electric conveyor belt fed machine that is designed for large shredding requirements and continuous shredding operations, processing up to 300kg of waste per hour.

The 430 TS is supplied with new design of carbon hardened cutting knives which allow for up to 40% more efficiency in shredding capacity. Shredding up to 130 sheets of 70gsm paper documents with ease to tiny 5.8 x 50mm cross-cut pieces.

The Kobra 430 TS will shred the following items to DIN security level P-3...

- Paper
- Cardboard
- USB Media
- CD / DVD / BluRay
- Credit Cards
- Floppy Disks

Verity Systems V880 High Energy Degaussser

VS Security Products

The Verity V880 Automatic Metal Tape Degausser offers highly efficient erasure of high energy cassettes and cartridges in a compact conveyor degausser.

The cassettes are placed onto the moving conveyor belt and carried over two degaussing coils that are orientated at 90 degrees to one another in a "V" formation. The belt speed is fixed at 4 inches per second. This permits the machine to completely degauss media with "one pass" degaussing.

Security level - Standard Commercial Security
Technology - Dual V conifgured Degaussing Coils

Media Type - VHS/S-VHS, LTO, DLT, DAT as well as Computer cartridges,
DC, TK 50/70/85, 3480/3490/3490e & 4/8mm