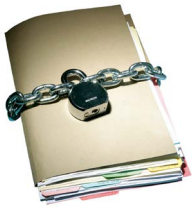
information destruction
EN15713:2009
– a complete guide



Confidential paper records, computer media, digital memory, hard disks, optical disks, smart cards, magnetic tape, product destruction etc.

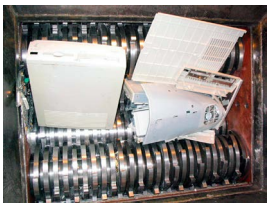
recycle

Recycling

Information Govenance

bsia
british security industry association

Approved BSIA member



Information destroyed to
BSEN15713 standards

Note: *It should be noted that EN15713:2009 incorporates the complete information destruction process, from collection, destruction and recycling and as an European Standard EN15713 takes precedence over other national standards.*

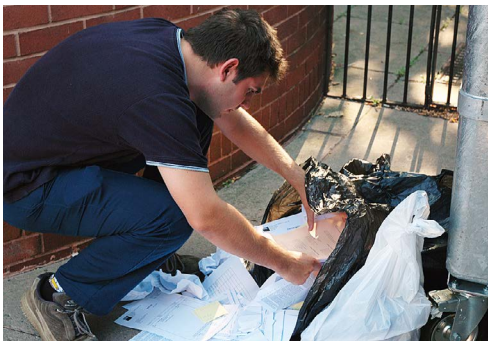
September 2014

For other information please contact:

British Security Industry Association
t: 0845 389 3889
f: 0845 389 0761
e: info@bsia.co.uk
www.bsia.co.uk

Introduction

In today's fast-paced business world, data and information is key to the success of most organisations. As such, it's essential for businesses of all sizes to protect their confidential data, including customer details, employee records and finance and accounting information. With legislation now imposing financial penalties on companies that fail to keep their data safe, there has never been a better time to put best practice in to place to ensure your confidential data is protected right through to the end of its life cycle.



As a European standard, EN15713 is the authoritative document on data destruction. It sets out the measures that organisations should take to maintain the security of confidential data and provides recommendations relating to the management and control of collection, transportation and destruction of confidential material to ensure such material is disposed of safely and securely. Developed by the European Committee for Electrotechnical Standards (CENELEC), EN15713 should be the first port of call for any organisation looking to improve its secure data destruction processes.

The standard places emphasis on guaranteeing the secure destruction service, ensuring that staff who are involved in the confidential shredding business are security vetted to BS7858, vehicles are secure, premises are alarmed and monitored and confidential material is processed and destroyed correctly. EN15713 is a complete document and deals with much more than shredding sizes as it provide the complete secure solution.

It is best practice that a client who is specifying or purchasing the services of a data destruction company should ensure the company has EN15713:2009 incorporated into an ISO9001:2008, Quality Management System. BSIA member companies incorporate EN15713:2009 into their ISO9001:2008 and are inspected annually by a UKAS accredited certification body. For details of BSIA members, visit the BSIA website at **www.bsia.co.uk/information-destruction**

The standard has the following requirements:

1. Confidential destruction premises

EN15713 states that all premises carrying out information destruction should:

- Have an administration office where necessary records and documentation is kept for conducting business.
- Be separated from other business or activities on the same site.
- Have an intruder alarm installed to EN50131- 1, monitored by an alarm receiving centre.
- Have a CCTV system with recording facilities that monitors the unloading, storage and processing areas. The images should be retained for a minimum of 31 days unless otherwise agreed with the client.

2. Contracts

The standard also requires that the following legal agreements regarding responsibility should be in place:

- A written contract covering all transactions should exist between the client and the organisation.
- Sub-contracted work should only be allocated to companies following the recommendations in EN15713:2009.
- In every case, clients should be informed if sub-contractors are used.
- The client, as data controller, should:
  - Choose a data processor providing guarantees in respect of technical and organisational security measures.
  - Take reasonable steps to ensure compliance with these measures.

Note: *Special notice should be given to the Data Protection Act (DPA) 2003, principal 7, and the requirements placed on the data controller.*

3. Personnel

EN15713 states that all personnel involved in the destruction of confidential data should:

- Be security vetted in accordance with BS7858, which includes a Criminal Records Bureau (CRB) check or Disclosure or Barring Service (DBS) check.
- Have signed a deed of confidentiality prior to commencement of employment.

4. Collection and retention of confidential material

The standard requires information destruction companies to employ the following measures when collecting confidential data:

- Confidential material to be collected should remain protected from unauthorised access from the point of collection to complete destruction.
- Collection should be made by uniformed and suitably trained staff carrying photographic identification.
- The destruction of confidential material should take place within one working day from arrival at the destruction centre, where shredding is taking place off site.

5. Vehicles (off site)

Vehicles collecting confidential data for destruction off site should:

- Be either box bodied or have a demountable container.
- Where a curtain side vehicle is used, material should be transported within a suitable sealed secure container.
- Be able to communicate with home base by radio or telephone.
- Be fitted with electro-mechanical immobiliser or alarm system.
- Be closed and locked/or sealed during transit.
- Be immobilised or alarmed when left unattended.

6. Vehicles (on site)

Vehicles destroying confidential data on site should:

- Be box bodied.
- Be fitted with lockable and/or sealable doors.
- Be able to communicate with the home base by radio or telephone.
- Not be left unattended when unprocessed material is onboard.

Note: *Although not specified in EN15713, it is the Association's view that vehicles:*

- Should have a trading standards approved weighing system if charging by weight.
- Should have a satellite tracking system.

7. Environmental issues

EN15713 requires the following environmental measures to be taken when destroying confidential waste:

- Where practicable, end products should be recycled.
- If recycling is not practicable, the cost and convenience of other methods should be taken into account.
- Landfill should only be used where no other method of disposal is practical.
- Waste Transfer Notes should be issued for each consignment, or annually for regular scheduled collections.

8. Customer due diligence

In addition to the requirement of the EN15713:2009 standards, it is also recommended that customers carry out due diligence directly with their existing or prospective destruction company. Although not a requirement, clients should also ensure suppliers of confidential destruction services carry out the following checks, together with yearly review of relevant certificates & licenses.

- **Physical check of destruction process, equipment, and vehicles.**

- **Duty of Care audit to ensure environmental regulatory compliance:** Destruction companies must be registered with the Environment Agency and have a Waste Carriers Licence, and if processing off site an Environmental Waste Permit or registered exemption. Copies of certificates should be provided. **www.environment-agency.gov.uk/research/library/publicregisters/default.aspx**

- **Vehicle Operating Licence:** destruction companies collecting confidential material must have an approved Driver and Vehicle Standards Agency licence if operating a fleet of commercial vehicles. **www.gov.uk/government/organisations/driver-and-vehicle-standards-agency**

- **Information destruction EN15713 compliant:** Customers should ask for an up to date copy of the ISO 9001 (UKAS approved) certificate of compliance as BSIA members have this written into their quality management systems and this is evidence that the standards are monitored and maintained. Please check **www.bsia.co.uk/information-destruction** for up to date certificates for each approved & vetted member.

- Insurance minimum cover of £5,000,000 public & products liability and £10,000,000 employers liability and Professional Indemnity up to a minimum of £1,000,000.

- Health & safety policy, risk assessments and safe operating procedures should be provided to customers to ensure safe operating standards and welfare.

9. Useful websites

British Security Industry Association
www.bsia.co.uk/information-destruction

Information Commissioner's Office (ICO)
www.ico.org.uk

Environment Agency
www.environment-agency.gov.uk

Driver and Vehicle Standards Agency
www.gov.uk/government/organisations/driver-and-vehicle-standards-agency

British Standards Institute (BSI)
www.bsigroup.co.uk

National Archives
www.nationalarchives.gov.uk

Centre for the Protection of National Infrastructure (CPNI)
www.cpni.gov.uk

Cabinet Office Government Security Classifications Policy – high security
www.gov.uk/government/publications/government-security-classifications

Centre of Excellence in Cyber Security (CESG) - CESG Assured Service CAS Service Requirement Destruction
www.cesg.gov.uk

Information Destruction Matrix

Material specific shred and disintegration sizes

Paper based material categories acceptable/unsuitable

BSEN 15713 Shred No.	Average surface area of material (mm^2)	Maximum cutting width (mm)	Method of destruction	Paper based information
1	5000	25	Shred	Y
2	3600	60	Shred	Y
3	2800	16	Shred	Y
4	2000	12	Shred	Y
5	800	6	Shred or Disintegrate	Y
6	320	4	Shred or Disintegrate	Y
7	30	2	Shred or Disintegrate	n/a
8	10	0.8	Shred or Disintegrate	n/a

Material specific shred and disintegration sizes

Material categories acceptable/unsuitable for other materials

BSEN 15713 Shred No.	SIM cards, negatives	Medical x-rays. Video/ audio tapes, diskettes, cassettes & film	Computer including hard drives, embedded software, chipcard readers, components & other hardware	ID cards, CDs & DVDs	Corporate or branded clothing and uniform. Counterfeit goods, printing plates, microfiche, credit & store cards & other products
1	N	Y	Y	N	Y
2	N	Y	Y	N	Y
3	N	Y	Y	N	Y
4	N	Y	Y	N	Y
5	N	n/a	Y	Y	Y
6	N	n/a	Y	Y	Y
7	Y	n/a	Y	Y	Y
8	Y	n/a	Y	Y	Y

Note: *EN15713:2009 incorporates the complete destruction process and should not be viewed as only providing shred sizes. As an European Standard EN15713 takes precedence over other national standards such as DIN (Deutsches Institut für Normung).*

It should also be noted that, as a general rule, the smaller the shred size required (output), the slower the throughput (tonnage per hour) achieved and therefore the higher the cost to achieve that particular output. Consequently, self classification by the end user / creator of the material or data, along with guidance from other informed bodies or associated third parties is the most logical approach to specifying desired shred sizes. For example, a book publisher creates a large surplus of a publication that they want destroyed. In this case a 25mm cutting width is more than adequate to render the product useless and to specify a smaller output would not be sensible commercially. The same principle applies to other products such as uniforms. The BSIA supports this 'risk management' versus desired outputs approach to classifying products & data for destruction. In general, the ID sector as a whole (manufacturers, outsourcing service providers & customers) is aligning behind a maximum 16mm cross cut shred size as being appropriate for 'confidential shredding'.

10. Glossary

Confidential Material – this can be information stored or printed on paper records, computer media, digital memory, hard discs, optical discs, smart cards, magnetic tape. This also means commercial and intellectual products and property etc. The term 'confidential' does not refer to UK Government security classifications, but is a generic industry standard term.

Information Destruction – the destruction (shredding or disintegration) of confidential material to a state that is unrecognisable and compliant with the Data Protection Act 1998.

Information Governance – the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organisation's immediate and future regulatory, legal, risk, environmental and operational requirements.

Data Protection Act 1998 – if you handle personal information about individuals, you have a number of legal obligations to protect that information. Principle 7 of the Act states that appropriate technical and organisational measures shall be taken against unauthorized processing of personal data.

BSEN15713 – Approved European standards for Information Destruction, that supersedes any other national standards. Providing secure information governance from collection, destruction and recycling. These standards must be incorporated within a robust quality management system and audited through an approved UKAS approved auditor to ensure compliance.

ISO 9001 & 14001 – UKAS approved Quality management and Environmental systems ensures a service provider belonging to the BSIA operates to the highest standards incorporating the BSEN15713 and is audited yearly to ensure quality procedures are maintained.

DIN (Deutsches Institut für Normung) – the German national organisation for standardisation and is that country's ISO member body. DIN is a Registered German Association for standards.

Centre for the Protection of National Infrastructure (CPNI) – High security – The Centre for the Protection of National Infrastructure (CPNI) protects national security by providing protective security advice to the UK's national infrastructure as defined by the Government as: "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends".

Centre of Excellence in Cyber Security (CESG) – protects the vital interests of the UK by providing policy and assistance on the security of communications and electronic data, working in partnership with industry and academia. CESG is the UK Government's National Technical Authority for Information Assurance (IA). Core customers are the UK's central government departments and agencies, and the Armed Forces. It also works with the wider public sector, including the Health Service, law enforcement and local government, as well as all essential services that form the UK's Critical National Infrastructure, including power and water.

Cabinet Office Government Security Classifications Policy – High security - The Cabinet Office issued the Government Security Classifications Policy, which took effect in April 2014 replacing the old Government Protective Marking Scheme.

TOP SECRET. The Government's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

SECRET. Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

OFFICIAL. The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. A limited subset of OFFICIAL information that would have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media is classified 'OFFICIAL-SENSITIVE'.

Most public authorities will fall into the OFFICIAL Category (subject to individual risk assessments), **with best practice information destruction standards BSEN15713 incorporated within a robust ISO9001 quality control system, demonstrating good compliance.** If further guidance is required within the public authorities this should be obtained from their internal security controller, and for further guidance refer to the Cabinet Office website.

information destruction
EN15713:2009
– a complete guide

Please watch the information destruction governance video to ensure customer compliance: www.bsia.co.uk/information-destruction

Note: *It should be noted that EN15713:2009 incorporates the complete information destruction process, from collection, destruction and recycling and as an European Standard EN15713 takes precedence over other national standards. This guide is only an aide-memoire and does not replace any of the requirements of the standard.*

For other information please contact:

British Security Industry Association
t: 0845 389 3889
f: 0845 389 0761
e: info@bsia.co.uk
www.bsia.co.uk/information-destruction

@thebsia