SHRED STATION

SHREDDING STANDARDS

DIN, EN 15713 & NPSA explained.

ONE GOAL: DESTRUCTION.

Regardless of what materials you want to destroy, what sort of organisation you work for, and what sort of data you collect, you choose to shred documents for the fundamental reason that you do not want your paperwork or confidential materials to be recovered. You want to ensure the fragments of your paper – even if shredding a single sheet – cannot be put back together.

The development of shredding standards such as DIN 66399, EN 15713 and NPSA ensure that, when standards are met, reassembly is not possible – not even for a single sheet.

But what does this all mean?

When considering the destruction of confidential materials, it's important to know what the different shredding standards mean. This will enable you to ensure the shred standard you require is met.

If you've ever used a home or office shredder, you may be familiar with DIN 66399 standards as these are mostly focused on shred size. If you're using a shredding service provider, you're probably looking for EN 15713 as the standard encompasses more than shred size; it covers staff vetting, depot security, storage of confidential materials and more. NPSA (National Protective Security Authority), formerly the CPNI (Centre for the Protection of National Infrastructure), requirements are something different altogether. This is because the standard is defined around the requirements needed to safely destroy Top Secret government materials.

This guide will break down the specifics of each standard without technical lexis or jargon. By the end, you will be confident in what these standards mean, and will know what standards you need to look for.

DIN 66399 STANDARDS

DIN (Deutsches Institut für Normung, translated to the German Institute for Standardisation) has thousands of standards that cover many fields. The DIN 66399 standard is the German national standard for shredding. DIN 66399 focuses mainly on shred size rather than overall security.

Why do so many organisations and products refer to DIN standards?

The reason DIN standards might sound familiar is that most household shredders specify the DIN 66399 standard shred sizes in their product descriptions. For example, your household paper shredder may shred to DIN Level 1 security (known as P-1).

What does this mean?

Under DIN 66399 standards, there are two main areas of focus.
- **The first** is the classification of data.
- **The second** is shred particle sizes, defined by levels of security.

How is data classified?

Data is classified by DIN into protection classes. These classes are determined by how much protection that data needs.

- **Class 1** is data there is a normal need for. While this data could contain personal information and should be protected, there is only a slight to moderate risk that any individual or business would be adversely affected by the unlawful access of this data. An example of Class 1 data could be a business telephone list or address details.

- **Class 2** is data where there is a high demand for confidentiality. Unauthorised access to Class 2 information could risk an individual or a company experiencing significant adverse impairments. This could be financial or personal. An example of Class 2 data could be items such as company balance sheets or a HR department's personnel files.

- **Class 3** data is data with a requirement for a very high level of confidentiality. With Class 3 data, there must be a guarantee of protection of personal data. It also includes any data where the disclosure could pose a significant risk to health or even life. Some examples of Class 3 data could be Top Secret government documents or information that could identify individuals in witness protection.

DIN 66399 STANDARDS

What are the levels of security?

DIN has determined seven levels of security that shred sizes represent. Level 1 is the lowest level of security and the largest particle size. Level 7 is the highest level of security and the smallest particle size.

In general, Security Levels 1, 2 and 3 are generally recommended for Class 1 data. Class 2 data is usually recommended to be shredded to Level 3, 4 or 5. Class 3 data is recommended to be shredded to Security Level 4, 5, 6 or 7.

Using a household shredder as an example again, a DIN Level 1 (P-1) household shredder will slice paper into strips of approximately 12mm in width. For an A4 piece of paper, this works out to be around 17 or 18 strips.

One thing to remember with DIN is that the level parameters change across materials. For example, for paper materials to meet DIN Level 3 (P-3), the paper should be shredded to be smaller than or equal to 320mm^2. For electronic data media to fit under the scope Level 3 (E-3), the particle size must be a maximum of 160mm^2.

A full guide to DIN 66399 shred sizes can be found in Appendix 1.

DIN 66399 PAPER LEVEL EXAMPLES*

*Please note, these sizes are to scale when viewed or printed at A4 sizing. Sizes are less than or equal to DIN standards maximum particle size.

Shred size is important to consider, but wider security measures, such as those set out by EN 15713, are a better indicator of how secure a shredding service is.

EN 15713 STANDARDS

EN 15713 standards are a list of standards and recommendations for the management and control of confidential material destruction. They cover the whole process, from collection to destruction, plus onward recycling and vetting of personnel and site security.

A summary of these security measures, as outlined in the BS EN 15713 Code of Practice, are below.

- **Company Facilities**

The company should have an office or operational centre for keeping business documents, records, files etc., and this space should be separate from other business or activities on the same site.

- **Security**

The company premises should have approved intruder alarm systems which cover processing, storage and office areas. There should also be closed-circuit CCTV recording the unloading, storage and processing areas. The company must keep all CCTV for a minimum of 31 days unless an alternative agreement is in place with the company's client. Authorised visitors can visit operational areas if supervised by appropriately screened personnel. Unauthorised visitors should not have access to operational areas.

- **Contracts and Audit Trail**

Between all clients and the company, there should be a contract covering all transactions. This contract should be in writing.

- **Sub-contracting**

If a company sub-contracts work where the sub-contractor destroys confidential material, the sub-contractor must also conform to EN 15713 standards. In every instance where a company uses a sub-contractor, they must inform the client.

- **Security Screening of Personnel**

Businesses should screen all staff in the business to BS7858 standards and each member of staff must sign a deed of confidentiality. BS7858 screening involves DBS checks, credit checks, five years of written employment verification and any gap verification. It also involves character references and right-to-work checks.

- **Retention of Confidential Material**

Confidential materials that are collected for destruction must be destroyed within one working day from the time of arrival at the destruction centre.

EN 15713 STANDARDS

- Collection of Confidential Material

All collections of confidential material should be made by properly trained staff. They must wear identifiable clothing and carry photo ID. All materials collected should be protected from unauthorised access at every step, from collection until destruction is complete. Where possible, confidential materials collected should also be stored in secure locked containers or containers secured by an individually numbered security seal.

- Off-Site Collection Vehicles

Off-site shredding vehicles should be box-bodied or have a secure demountable container. They should also be fitted with lockable or sealable doors, as well as electro-mechanical immobilisers or alarm systems. They should be immobilised or alarmed when left unattended, and be locked and locked/sealed during transit. The vehicle operatives must have a clear line of communication available for contact with the company at all times.

- On-Site Shredding Vehicles

On-site shredding vehicles should be box-bodied and fitted with lockable or sealable doors. Vehicles should never be left unattended when unprocessed confidential materials are on board. Nor should any unprocessed confidential material be removed from the client's site. As with the off-site collection vehicles, the operatives in on-site vehicles must have a clear line of communication with the company, either by phone or radio.

- End Product Disposal

Businesses should recycle all recyclable materials where practicable. Where recycling isn't possible, companies should consider the environmental impacts, costs, and convenience of using other waste disposal methods. At Shred Station, we recycle 100% of the paper we shred and all other materials where we can. Non-recyclable materials are used to generate Energy from Waste. Nothing we shred goes to landfill.

BS EN 15713 standards also consider material types and shred sizes. These shred sizes should be suitable for rendering the material unreadable, illegible and not possible to reassemble.

We outline these sizes and materials in Appendix 2.

NPSA STANDARDS

The National Protective Security Authority (NPSA), formerly known as the CPNI, is the UK government's national authority for physical and personnel protective security. It works to protect national security and reduce vulnerability to espionage, sabotage, and terrorism. It does this by working with partners responsible for infrastructure sectors such as the government, organisations within the critical national infrastructure, and security specialists such as the police.

The NPSA standard for shredding provides organisations with the procedures, processes and performance monitoring necessary to securely destroy sensitive materials that are classified as Secret or Top Secret.

Some elements of the standard are detailed below, and the full standard can be found here.

- **Secure Destruction Policy**

The owner must maintain a secure and effectively managed destruction policy.

- **Destruction Equipment**

The outcome of destruction must be that items are no longer sensitive. It must be possible for an authorised person to visually confirm the destruction of their sensitive items.

Destruction equipment must be operated by authorised, trained personnel who are regularly assessed.

Destruction equipment must be serviced and maintained in line with the manufacturer's instructions and performance of the equipment should be monitored and documented. Equipment usage instructions must also be available at the point of use of the destruction equipment.

Equipment should be installed within a secure area only accessible by authorised personnel. When the equipment is installed, modified or decommissioned, the person/s performing the work must produce a report including a technical description of work or modifications. There must also be regular integrity inspections of equipment.

- **Personnel**

Personnel with access to sensitive items must sign non-disclosure agreements.

Those with unaccompanied access to sensitive items must have documented authorisation by the owner. The owner may at their discretion grant access to sensitive items to people who are not authorised. When this happens, they should be accompanied and observed, with at least one authorised person for every two without authorisation. Records of this must be kept.

NPSA STANDARDS

- **Storage of Sensitive Items**

When materials are stored in holding areas, these areas must be at least as secure as the areas where documents were originally stored or used.

Sensitive items pending destruction must be physically separate from non-sensitive items. This must be a separate room or holding container.

- **Tracking of Sensitive Items**

Sensitive items must be tracked throughout the destruction process and there must be proof of tracking. Tamper-evident seals should also be used and checked throughout the process. Full details of tracking requirements can be found in the complete NPSA standard.

- **Verification of Custodians and Their Vehicles**

The owner and custodian must have a documented procedure to identify and verify custodians and their vehicles. There should be a denial of access to sensitive items until all personnel and vehicles are verified.

- **Transport of Sensitive Items**

The NPSA standard for transport of sensitive items covers many areas including vehicle security features, transport procedures, how sensitive items and non-sensitive items are segregated, and the presence of authorised personnel. Full details are available in the complete NPSA standard.

- **Business Continuity Procedures**

Maximum legal driving hours should be taken into account to minimise unplanned stops. A replacement crew must be available to complete the journey if the vehicle crew is unable to complete the transportation of sensitive items due to exceeding maximum driving hours or any other unforeseen circumstances. If a vehicle is no longer able to deliver sensitive items, for instance, in the event of a breakdown, a replacement vehicle must be available. Loading into the replacement vehicle must occur within a secure perimeter, and an inventory must be taken.

- **External Destruction Facilities**

When destroying sensitive items at a destruction facility, the procedure must be observed and attended by at least one authorised person.

The facility must have a secure perimeter and sensitive items must be destroyed within 24 hours of arriving at the facility.

Sensitive items from different owners must be separated within the destruction area, and any

personnel in this area must be accompanied by one or more authorised people.

If an event would prevent the timely destruction of sensitive items, there must be an agreed and documented procedure in place between the owner and the destruction facility to ensure the emergency storage or alternative destruction of sensitive items.

- **Mobile Destruction Facilities**

Sensitive items processed by a mobile destruction facility must be observed and attended by an authorised person at all times. Facilities should have secure perimeters, and vehicles must be fitted with security features including an audible anti-theft alarm and immobiliser.

- **Tamper-evident Seals**

When used, tamper-evident seals must be used properly and personnel should be trained to document and verify the serial numbers of these seals and to spot signs of tampering.

- **Compromise Procedures**

There must be documented procedures for custodians to identify and record suspected, potential, attempted or confirmed compromises of sensitive items.

- **Use of Service Providers**

Each service provider and any sub-contractors must have a written contract with the owner. They must also hold professional indemnity insurance, and the service provider must have the prior written approval of the owner before sub-contracting.

In addition to the above, there are also specified destruction outcomes (particle sizes) required for different materials destroyed through shredding.

The destruction outcomes for shredding can be seen in Appendix 3.

Appendix 1 - DIN Sizes

PAPER DOCUMENTS

SECURITY LEVEL	PARTICLE SIZE	STRIP WIDTH
P-1	≤ 2000 mm²	≤ 12 mm
P-2	≤ 800 mm²	≤ 6 mm
P-3	≤ 320 mm²	≤ 2 mm
P-4	≤ 160 mm²	6 mm
P-5	≤ 30 mm²	2 mm
P-6	≤ 10 mm²	≤ 1 mm
P-7	≤ 5 mm²	≤ 1 mm

ELECTRONIC DATA MEDIA

SECURITY LEVEL	PARTICLE SIZE
E-1	mechanically inoperable
E-2	split
E-3	max 160 mm²
E-4	max 30 mm²
E-5	max 10 mm²
E-6	max 1 mm²
E-7	max 0.5 mm²

OPTICAL DATA MEDIA

SECURITY LEVEL	PARTICLE SIZE
O-1	max 2000 mm²
O-2	max 800 mm²
O-3	max 160 mm²
O-4	max 30 mm²
O-5	max 10 mm²
O-6	max 5 mm²
O-7	max 0.2 mm²

HARD DRIVES MAGNETIC DATA MEDIA

SECURITY LEVEL	PARTICLE SIZE
H-1	mechanically inoperable
H-2	damaged
H-3	deformed
H-4	max 2000 mm²
H-5	max 320 mm²
H-6	max 10 mm²
H-7	max 5 mm²

MAGNETIC TAPE MEDIA

SECURITY LEVEL	PARTICLE SIZE
T-1	mechanically inoperable
T-2	max 2000 mm²
T-3	max 320 mm²
T-4	max 160 mm²
T-5	max 30 mm²
T-6	max 10 mm²
T-7	max 2.5 mm²

INFORMATION IN REDUCED FORMS

SECURITY LEVEL	PARTICLE SIZE
F-1	max 160 mm²
F-2	max 30 mm²
F-3	max 10 mm²
F-4	max 2.5 mm²
F-5	max 1 mm²
F-6	max 0.5 mm²
F-7	max 0.2 mm²

The information cited in the table above is taken from the DIN 66399 Code of Practice, cited by the German Society for Data Protection and Data Security and PRODevice EU. It is correct at the time of publication, July 20th 2022.

Appendix 2 - EN 15713 Sizes

MATERIAL-SPECIFIC SHRED AND DISINTEGRATION

SHRED NO.	AVERAGE SURFACE AREA OF MATERIAL	MAX CUTTING WIDTH	METHOD OF DESTRUCTION	MATERIAL CATEGORIES √ Acceptable x Unsuitable for material							
	mm^2	mm		A	B	C	D[a]	E	F[b]	G[b]	H
1	5000	25	Shred	√	X	√	√	X			√
2	3600	60	Shred	√	X	√	√	X			√
3	2800	16	Shred	√	X	√	√	X			√
4	2000	12	Shred	√	X	√	√	X			√
5	800	6	Shred or disintegrate	√	X	n/a	√	√			n/a
6	320	4	Shred or disintegrate	√	X	n/a	√	√			n/a
7	30	2	Disintegrate	n/a	√	n/a	√	√			n/a
8	10	0.8	Disintegrate	n/a	√	n/a	√	√			n/a

[a] Materials in category D should be destroyed so that information is unreadable and subject to secure disposal.
[b] Client and specific material.

TABLE TO SHOW CATEGORIES OF CONFIDENTIAL MATERIAL

CATEGORY	DESCRIPTION
A	Paper, plans, documents and drawings
B	SIM cards and negatives
C	Video/Audio tapes, diskettes, casettes and film
D	Computers including hard drives, embedded software, chip card readers, components and other hardware.
E	ID cards, CDs and DVDs
F	Counterfeit goods, printing plates, microfiche, credit and store cards and other products
G	Corporate or branded clothing and uniforms
H	Medical X-Rays and overhead projector slides
NOTE	Hazardous waste is not included in this table. Users are advised of the existence of legislation applicable to the destruction and/or disposal of hazardous waste.

The information cited in the tables above is taken from the BSIA Information Destruction BS EN 15713:2009 - A Complete Guide.
It is correct at the time of publication, July 20th 2022.

Appendix 3 - NPSA Sizes

DESTRUCTION OUTCOMES FOR MATERIALS PROCESSED THROUGH SHREDDING

SENSITIVE ITEM	REQUIRED OUTCOME
DIGITAL MEMORY	6mm (any direction) particle
FLOPPY DISK	6mm (any direction) particle
HARD DISK	6mm (any direction) particle
MAGNETIC TAPE	6mm (any direction) particle
MICROFORM	2mm (any direction) particle
OPTICAL DISK	2mm (any direction) particle
PAPER*	60mm^2
SIM OR SMART CARD	2mm (any direction) particle
VISUAL DISPLAY UNIT	6mm (any direction) particle

* For shredding paper printed with 12pt Times New Roman font, the width along the line of the text should be no more than 4mm, such that no more than two adjacent characters are visible on a single particle. A narrower cut width may be necessary where smaller font sizes are present.

The information cited in the table above is taken from the NPSA/CPNI Secure Destruction of Sensitive Items Standard.
It is correct at the time of publication, July 20th 2022.