



Shred Standard ISO/IEC 21964 or DIN 66399 Explained

by Frank Lauterslager

Contents

1.0 Introduction.....	1
2.0 Protection class and security level	2
3.0 Types of data carriers.....	2
4.0 Particle size	2
5.0 Equipment requirements	3
6.0 Physical destruction process.....	3
7.0 Other related information which you can find on our site .	4

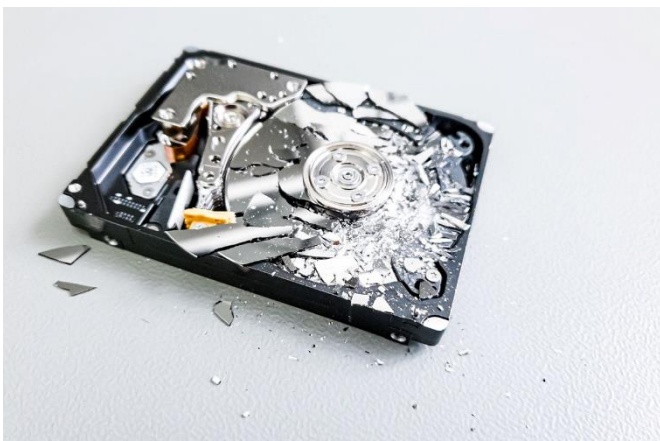
1.0 Introduction

Since 2018, the ISO/IEC 21964 or DIN 6399 standards are referenced by international organizations when referring to the physical destruction requirements of data carriers.

The standard consists of 3 parts:

- ✓ In the first, terms and principles for the destruction of data carriers are defined.
- ✓ The second part specifies the requirements for equipment to ensure the safe destruction of data carriers.
- ✓ The third part defines requirements for the process of destruction of data carriers, applicable for all parties involved in the destruction process.

The main focus of this standard is on shredding or granulating data carriers. Other methods of physical destruction like degaussing, incineration, and dissolving are rarely discussed. The standard also includes data on paper shredding, what is out of scope for us as we focus only on digital media.



2.0 Protection class and security level

The starting point is the sensitivity of the stored data. Based on a risk analysis, the data contained in data carriers must be assigned to a protection class. The security level which is chosen for the destruction of the data carrier is determined by the protection level of the data. The standard defines 3 protection classes of data subdivided into 7 security levels:

Protection class 1: Normal protection required for data where disclosure can have a negative economic impact and on the reputation of the organization.

Protection class 2: Higher protection level for confidential data where disclosure can have a considerably negative effect or could breach legal obligations of an organization or can generate a risk to individuals that could damage their social standing or economic circumstances.

Protection class 3: Very high protection level for strictly confidential and top-secret data, which if disclosed without authorization can have serious to existence-threatening effects on the organization and/or very serious breach of legal obligations or can generate a risk to the safety, health, or personal freedom of individuals.

3 protections classes are be assigned to the security levels								
Protection class	Security level							
	1	2	3	4	5	6	7	
1	x	x	x					
2			x	x	x			
3					x	x	x	

In case data carriers with different security levels are mixed, their destruction shall be according to the higher security level.

3.0 Types of data carriers

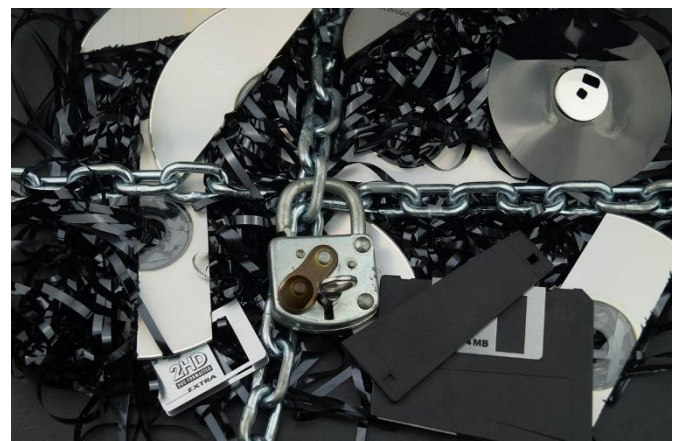
Digital data carriers are classified in different material categories:

Type	Description of the media carrier
Electronic (E)	Electronic data carriers including SSDs, mobile phones, memory sticks, cards with magnetic chip
Magnetic (H)	Magnetic data carriers including HDDs (SATA, IDE, SCSI, SAS)
Optical (O)	Optical data carriers including CDs, DVDs
Media (T)	Magnetic data carriers including ID-cards, magnetic tapes, floppy discs
Film (F)	Data carriers with miniaturized information, including microfilm, microfiche

4.0 Particle size

The standard for machines to destroy data carriers defines the degrees of destruction results. These results are grouped by the type of data carrier and by the 7 security levels. An example is in the table hereunder. The complete tables in the standard give more details like strip width and alternatives like dissolving or shredded ash. It also indicates a tolerance: a percentage and a limit of size to the particles that may not exceed the maximum size and shape.

At a certain volume, the security level can be increased by mixing and compacting the destroyed data carriers. On-site destruction is preferred above other methods.



Max cross-section particle size in mm ² for data carriers					
Security level	Electronic (E)	Magnetic (H)	Optical (O)	Media (T)	Film (F)
1	Inoperable	Inoperable	2000	Inoperable	160
2	Split	Damaged	800	Split	30
3	160	Deformed	160	2000	10
4	30	2000	30	320	2,5
5	10	320	10	160	1
6	1	160	5	10	0,5
7	0,5	10	0,2	2,5	0,2

5.0 Equipment requirements

The degree of destruction per data carrier type is a helpful tool for evaluating if a machine will comply to the security level needs of an organization. A manufacturer or service provider can provide information like: "E3, H6, O3, T5, F1".

The standard also defines the exact conditions and reporting methods to test a machine for assessment or certification. It recommends that users check particle size regularly due to wear or damage of the machine.



- 1) The organization responsible for the data carriers organizes the destruction by members/employees of the organization on-site.
- 2) The data carriers are destroyed on site by a service provider.
- 3) The data carriers are destroyed at an external site by a service provider.

In the standard you will find security criteria regarding elements such as:

Organization of the process: the need to define technical and organizational measures for the destruction process from point of origin, collection, storage and to destruction.

Destruction equipment: the ability to prove that equipment is used which destroys different data carriers according to their category as described in part 1 and 2. Redundancy of equipment avoids unexpected delays.

Staff: identification of personnel and their obligation to confidentiality,

Service provider: definition and criteria of parts of the destruction process for which the service provider is responsible.

Storage, destruction facility, and safety zones: closed spaces, access, surveillance, quality of the building.

Transport: temporary storage of data carriers is in closed containers, vehicle types, loading and unloading.

Surveillance and Control: Surveillance and regulatory control of the execution of the process and sample verification of the results.

6.0 Physical destruction process

The standard defines important requirements for the steps to the destruction of data carriers.

Three different scenarios are distinguished:

These elements are to be included in the acceptance protocol and destruction protocol.

7.0 Other related information which you can find on our site:

- * [Data classification and organization](#)
- * [Destructing data carriers not so simple](#)
- * [ISO/IEC has become the international shred standard](#)
- * [How to organize the destruction of data carriers](#) (PDF)
- * [Is ISO/IEC good enough?](#) (PDF)

This article has highlighted some of the most important elements of this standard. It is meant for a general understanding. It is not intended to replace or reproduce the complete official standard and its publication in any way. The complete standard should be purchased directly from one of the official organizations, or through their commercial representation.

Contact us

info@it-responsible.com

For more reports, go to:
it-responsible.com

© Copyright 2021 DERROF.
All Rights Reserved.