

DATA AND DOCUMENT DESTRUCTION IN ACCORDANCE WITH THE SECURITY LEVELS OF STANDARD DIN 66399

The strict DIN 66399 guidelines apply to the destruction of confidential information on paper, film or digital storage devices. Their demands on machines and processes increase in line with the level of confidentiality. To meet the requirements of higher security levels, the Lindner single shaft shredder – and in particular the series Micromat and Komet – were created and certified according to this norm so that you can configure them in line with your needs.



The German standard DIN 66399, 'Office machines – Destruction of data carriers', describes in three sections how to securely destroy confidential data on documents, films, CDs, DVDs, USB sticks and other media in accordance with the state of the art. In general, the sensitivity of the data is directly proportionate to the technical effort that would be required to reconstruct the data. The three sections are divided into part 1, 'Principles and definitions'; part 2, 'Equipment requirements for the destruction of data carriers', which is particularly important for the selection of the ideal shredder configuration; and part 3, 'Process for the destruction of data carriers', which describes the procedure.

Protection classes and security levels

According to this standard, data carriers or storage devices containing sensitive information must be destroyed in such a way that it is either entirely impossible or extremely difficult to restore the information stored on them. To assess the cost-benefit ratio it is important to group the data into protection classes. Depending on the degree of confidentiality, these categories range from protection class 1 for the normal protection required for internal data, protection class 2 for the high protection required for confidential data, and class 3 for the very high protection required for confidential and top-secret data.

Classified according to DIN 66399		Protection class 1		Protection class 2			Protection class 3	
		General data	Internal data	Sensitive and confidential data	Particularly sensitive & confidential data	Secret data	Secret data for unusually high security standards	Strictly confidential / top-secret data
P	Information in original size	P-1	P-2	P-3	P-4	P-5	P-6	P-7
O	Optical data media	O-1	O-2	O-3	O-4	O-5	O-6	O-7
T	Magnetic data media	T-1	T-2	T-3	T-4	T-5	T-6	T-7
E	Electronic data media	E-1	E-2	E-3	E-4	E-5	E-6	E-7
F	Scaled-down information (film)	F-1	F-2	F-3	F-4	F-5	F-6	F-7
H	Hard drives with magnetic storage medium	P-1	P-2	P-3	P-4	P-5	P-6	P-7

These three protection classes are then subdivided into seven security levels which are explained in great detail. These refer to the possibility of restoring the data after it has been destroyed. The scale ranges from level 1 for the destruction of general data where lower protection is needed (e.g. brochures, newspapers etc.) and where reconstruction of the data presents no data protection problem, right up to level 7 for top-secret data (e.g. secret service or military documents), where the possibility of restoration can be excluded according to the present state of scientific knowledge.

In addition, the DIN 66399 also describes six media categories (see table). Combined with the individual security levels, the media can be classified as follows:

The class P-5, for example, means the destruction of information in original size such as paper or documents (data carrier group P) of security level 5 for secret data (e.g. medical documents or strategic papers). Once destroyed, this data could only be reconstructed with very dubious methods.

The standard explains in detail that, for the P-5 category, 90% of the particle size after shredding must not exceed 30 mm² (edge length < 5,5 mm).

Equipment requirements for the destruction of data carriers in line with DIN 66399-2

The ideal shredding machine is selected and configured according to the security level desired. The standard requires that the design of the machine is such that the entire storage device is acquired manually or mechanically and destroyed. In addition, a vertical chute or a capture tray must capture all elements of the destroyed devices. Also, the complete destruction of the media has to be protocolled.

For every machine used, the operator has to prove by means of a test certificate, declaration of conformity, certificate or report that it is able to keep to the specified limits. These documents can be provided by the manufacturer of the machine after the machine type has been examined by an independent expert. For this purpose, the standard also describes in detail the procedure for testing the machine's suitability. The operator is obligated to randomly check the

machine's compliance with these requirements during operation in order to identify and fix any non-compliance resulting from wear and tear.

Lindner shredding technologies – certified for operation in line with the DIN standard

Thanks to its unique combination of customised cutting system and screen design, the shredding technology of the series Micromat and Komet – which has been tried and tested by an independent institute – guarantees the secure destruction of sensitive material. The individual configurations mean the machines can be adapted to different protection classes including higher security levels (see chart).

Our extremely high-quality, tried-and-tested Lindner shredder components, the machine's easy maintenance and in particular the cutting gap that can be adjusted while the machine is running all make it possible to easily and effectively combat incorrect grain sizes resulting from wear and tear. That guarantees continuous, standards-compliant output with minimal effort.

Media Categories According DIN 66399		Level
P	Information in original size	5
O	Optical data media	4
T	Magnetic data media	5
E	Electronic data media	3
H	Hard drives with magnetic storage medium	5