INTERNATIONAL STANDARD

ISO/IEC 21964-1

First edition
2018-08

Information technology — Destruction of data carriers —

Part 1: Principles and definitions

Technologies de l'information — Destruction de véhicules de données —

Partie 1: Principes et concepts

Reference number
ISO/IEC 21964-1:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by DIN, German Institute for Standardization (as national standard DIN 66399-1) and drafted in accordance with its editorial rules. It was assigned to Joint Technical Committee ISO/IEC JTC 1, *Information technology*, and adopted under the "fast-track procedure".

A list of all parts in the ISO/IEC 21964 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Anyone who processes confidential, personal and/or sensitive data for themselves or on behalf of others must ensure that data carriers containing such information are safely destroyed in a way that ensures privacy.

In this context, safely destroyed means that data carriers containing sensitive data must be destroyed in such a way that reproduction of the information on them is either impossible or is only possible with considerable expenditure (in terms of personnel, resources and time).

NOTE This standard takes into account that data carriers have different physical characteristics and contain information with various levels of sensitivity.

Information technology — Destruction of data carriers —

Part 1:
Principles and definitions

1 Scope

This standard defines terms and principles for the destruction of data carriers.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

2.1
collection point
place where data carriers are kept before they are destroyed

2.2
data
representation of facts, concepts, or instructions in a formalized manner, suitable for communication, interpretation, or processing by humans or by automatic means

[SOURCE: EN 14968:2006-11]

2.3
data carrier
object or item that contains data

Note 1 to entry: Typical data carriers include paper or electronic, magnetic and optical storage media.

2.4
data controller
<destruction of data carriers> any person or body which collects, processes or uses data for itself or assigns others to do so

2.5
destruction
<destruction of data carriers> process in which the form or condition of data carriers is changed, usually by shredding, dissolving, melting, heating or burning

2.6
destruction of data carriers
process by which the form or condition of data carriers is changed, usually by shredding, dissolving, melting, heating or burning, making it difficult or impossible to recover the information

2.7
dissolving
transforming the data carrier to a suspension

2.8
equipment
collection of spatially and functionally linked machinery for the purpose of destroying data carriers

2.9
information
meaningful data

[SOURCE: ISO 9000:2005-12]

2.10
intruder alarm system
alarm system to detect and indicate the presence, entry or attempted entry of an intruder into supervised premises

[SOURCE: EN 50131:2010-02]

2.11
outsourced data processing
collection, processing and use of data by assigned third parties

Note 1 to entry: The destruction of data carriers is also a form of outsourced data processing.

2.12
personal data
details of the personal or material circumstances of an identified or identifiable natural person

2.13
protection class
classification of the protection requirement of data

2.14
protection requirement
property of data and information which describes the need to protect it from violation of the basic principles of confidentiality, integrity and availability, taking into account the harm which would arise from such a violation

Note 1 to entry: The protection requirement is classified as normal, high or very high.

Note 2 to entry: For the destruction of data carriers, the higher the protection requirement of the data they contain, the higher the protection class.

2.15
regular particles
particles which, as a result of the cutting process used, have a generally unalterable, mostly rectangular shape, as well as a specified length and width

2.16
security level
<destruction of data carriers> classification of the effort needed to recover information

2.17
security zone
area protected according to the protection class

3 Identifying the protection requirement and assigning the protection class

In order for the destruction of data carriers to comply with the principles of economy and proportionality, the data contained on them shall be assigned a protection class. The security level which is chosen for the destruction of the data carriers is determined by the protection level of the data.

Protection class 1

Normal protection level for internal data:

— The most common classification of information, intended for large groups of people.

— Unauthorized disclosure or transfer would have limited negative effects on the organization.

— Protection of personal data shall be ensured. Otherwise there is a risk that persons affected may suffer damage to their reputation and economic circumstances.

Protection class 2

Higher protection level for confidential data:

— The information is restricted to a small group of people.

— Unauthorized disclosure would have serious effects on the organization and may lead to violation of laws or contractual obligations.

— The protection of personal data shall meet stringent requirements. Otherwise there is a risk that persons affected may suffer serious damage to their social standing or economic circumstances.

Protection class 3

Very high protection level for strictly confidential and secret data:

— The information is restricted to a very small group of persons, known by name, who are authorized to access it.

— Unauthorized disclosure would have serious (existence-threatening) effects on the organization and/or would lead to violation of professional secrets, contracts and laws.

— The protection of personal data shall be strictly ensured. Otherwise, the life and safety of persons affected may be at risk, or their personal freedom may be jeopardized.

4 Security levels for data carriers

Table 1 shows the various security levels for data carriers.

Table 1 — Security levels for data carriers

Security level	Explanation
1	**Destruction of data carriers** in such a way the data on them can be reproduced without special tools or skills, but not without a certain expenditure of time *Recommended, for example, for data carriers containing general data to be rendered unreadable.*
2	**Destruction of data carriers** in such a way that the data on them can only be reproduced with tools and a certain amount of effort. *Recommended, for example, for data carriers containing internal data to be rendered unreadable.*
3	**Destruction of data carriers** in such a way that the data on them can only be reproduced with considerable expenditure (in terms of personnel, resources and time) *Recommended, for example, for data carriers with sensitive and confidential data.*
4	**Destruction of data carriers** in such a way that the data can only be reproduced with extraordinary expenditure (in terms of personnel, resources and time) *Recommended, for example, for data carriers with particularly sensitive and confidential data.*

Table 1 *(continued)*

Security level	Explanation
5	**Destruction of data carriers** in such a way that the data on them can only be reproduced with non-standard or specially designed equipment, or using forensic methods *Recommended, for example, for data carriers with secret data.*
6	**Destruction of data carriers** in such a way that the data on them cannot be reproduced with current technology *Recommended, for example, for data carriers with secret data where unusually high security measures shall be maintained.*
7	**Destruction of data carriers** in such a way that the data on them cannot be reproduced with current technology or scientific knowledge *Recommended, for example, for data carriers with top secret data where the highest security measures shall be maintained.*

5 Assignment of protection classes and security levels

5.1 Selection of security level

The three protection classes can be assigned to the security levels using Table 2, but a risk analysis should be carried out in each case.

If there are data carriers with different security levels at the collection point, they should be sorted there by security level for economical and environmental reasons. If this is not possible, all the data carriers shall always be destroyed according to the higher security level. This is to minimize the risk of incorrect assignment leading to inadequate destruction of data carriers containing sensitive data.

When selecting the appropriate security level, the density and/or size of the represented information on the data carrier shall be taken into consideration. If the colour or other characteristics of the data carrier make it easier to reconstruct, a higher security level may have to be selected.

Table 2 — Assignment of security levels and protection classes

Protection class	Security levels						
	1	2	3	4	5	6	7
1	x[a]	x[a]	x				
2			x	x	x		
3				x	x	x	x

[a] This combination can not be used for personal data.

5.2 Altering the security level

5.2.1 General

Mixing and compacting the destroyed data carriers impedes reproduction. This does not affect the possible information content of individual particles of material.

The security level of the machine and how this is assured shall be openly and clearly indicated.

If it is possible for data controllers to destroy data carriers directly on site at any time, this increases security and is preferable to other methods, provided the selected security level is used.

5.2.2 Responsibility

The method of increasing the security level shall be determined by the data controller, insofar as the protection level and the applicable regulations allow it.

5.2.3 Requirements

For data carriers with information shown in the original size or miniaturized, which are destroyed according to security level one, two or three, mixing and compacting increases security to the next higher level once only, up to a maximum of security level four. This procedure requires a minimum of 100 kg of data carriers, which shall be destroyed in a single, uninterrupted cycle of the machine or equipment.