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/IEC 2018



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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** ..... **iv**
**Introduction** ..... **v**
**1 Scope** ..... **1**
**2 Terms and definitions** ..... **1**
**3 Identifying the protection requirement and assigning the protection class** ..... **2**
**4 Security levels for data carriers** ..... **3**
**5 Assignment of protection classes and security levels** ..... **4**
5.1 Selection of security level ..... 4
5.2 Altering the security level ..... 4
5.2.1 General ..... 4
5.2.2 Responsibility ..... 5
5.2.3 Requirements ..... 5
**Bibliography** ..... **6**

© ISO/IEC 2018 – All rights reserved

# 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.


© ISO/IEC 2018 – All rights reserved

# 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.

© ISO/IEC 2018 – All rights reserved

# 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

© ISO/IEC 2018 – All rights reserved

**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.


© ISO/IEC 2018 – All rights reserved