INTERNATIONAL STANDARD

ISO/IEC 21964-3

First edition
2018-08

Information technology — Destruction of data carriers —

Part 3: Process of destruction of data carriers

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

Partie 3: Processus de destruction des supports de données

Reference number
ISO/IEC 21964-3:2018(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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Processing **1**
3.1 General 1
3.2 Process definition 2
3.3 Determination of the risk structure 2
3.4 Process execution 3
3.5 Inspection and testing 3
3.5.1 Requirements to the data controller 3
3.5.2 Process reliability 3
3.5.3 Requirements to certificates of service providers 4
4 Process criteria **4**
4.1 General 4
4.2 Criteria for all varieties of data carrier destruction 4
4.3 Criteria for variety 1 4
4.4 Criteria for variety 2 5
4.5 Criteria for variety 3 5
4.6 Criteria for the infrastructure of the service provider for variety 3 7
4.7 Take-over record 8
4.8 Destruction record 8

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 66399-3) 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

Everybody, who processes confidential, personal and/or sensitive data, for themselves or on behalf of others, is obliged to ensure an adequate and secure disposal and destruction of data carrier.

Secure destruction means in this regard, that the data carriers, on which the information in need of protection is represented, are destroyed in a way, that the reproduction of the represented information are either impossible or most widely aggravated (ISO/IEC 21964-1 and ISO/IEC 21964-2).

Not just the secure destruction itself should be noted, but also the whole process from the point of origin through to the environmentally friendly recycling/disposal in accordance with laws and regulations currently in force.

Information technology — Destruction of data carriers —

Part 3:
Process of destruction of data carriers

1 Scope

This standard defines the requirements for the process of destruction of data carriers and is applicable for the responsible authority and for all parties who are involved in the destruction process.

2 Normative references

The following quoted documents are required for the application of this document. For dated references only the referred version is valid. For undated references, the last issued version is valid (including all changes).

ISO/IEC 21964-1, *Information Technology — Destruction of data carriers — Part 1: Principles and Definitions*

ISO/IEC 21964-2, *Information Technology — Destruction of data carriers — Part 2: Requirements for equipment for destruction of data carriers*

3 Processing

3.1 General

The destruction of data carriers has to be understood as a process, in which every single process step has to be examined and designed to be secure. The responsible authority is responsible for the whole process (internal and/or external) up to the final destruction of the data carrier. The process of data carrier destruction ends as soon as the agreed security level is reached.

Usually the process involves different parties from the collection point to the environmentally friendly destruction. If service providers are involved in the process, the delimitation of responsibilities between the data controller and the service provider has to be agreed clearly. Due to legal provisions there are mainly technical and organizational measures to be taken for this process.

The depiction in Figure 1 shows the varieties of the process contained in this standard including the related process steps.

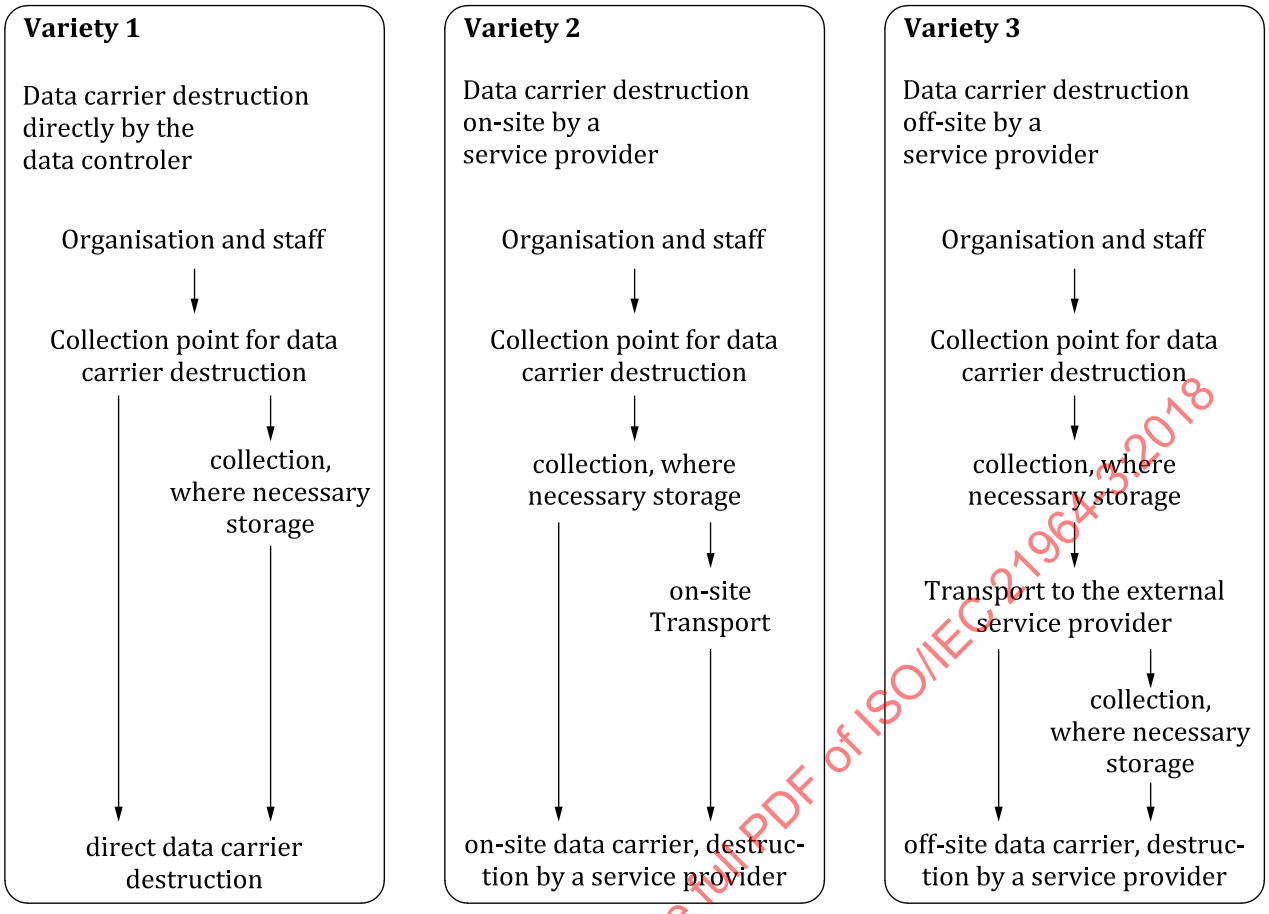

Figure 1 — Data carrier destruction

3.2 Process definition

The identified technical and organizational measures, resulting from a risk analysis, shall ensure the protection requirements by considering the state-of-the-art of restoration technologies. These protection requirements shall be adequate for the risks that may emerge by the destruction process itself, and the kind of data to protect.

To protect data from misuse, it requires a security- and control system, which ensures a reliable quality of the destruction process either on-site at the data controller or off-site at a service provider. The protective purpose is the prevention of data abuse. Taking into account economical and adequacy considerations, the data carriers intended to be destroyed, should be separated into protection classes (see ISO/IEC 21964-1, Protection classes 1 to 3).

If there are data carriers which require different security levels, it is recommended to separate them according to the different security levels at the collection point for economic and ecological reasons.

3.3 Determination of the risk structure

Data has to be categorized to its sensitivity according to ISO/IEC 21964-1.

In principle an impairment of the basic functionality of data carrier should take place in the early process steps of the destruction process.

For electronic and magnetic data carriers, it is recommended to erase or overwrite them prior to the destruction. This reduces the attraction of stealing and it originates a basic security for the subsequent process steps. Considering the protection requirement a lower security level can then be chosen. If an

impairment of the basic functionality resp. erasing/overwriting is not possible, the necessary security level of the chosen protection class shall apply.

When using one of the process varieties, it needs to be verified in advance, whether the technical and organizational requirements of the corresponding protection class and security levels are met.

The data controller defines the protection requirements and the protection class. Therefore the following questions shall be answered:

— Which information is worth being protected and categorized in which protection class	What?
— Destruction according to which security level	How?
— Destruction by the data controller directly or by an external service provider	Who?
— Destruction on-site or off-site by an external	Where
— service provider	
— Technical and organizational measures at the collection point, during transport and at the service provider	How?

The result determines the operational processing (security concept).

3.4 Process execution

A prerequisite for the proper execution of the process is a detailed organization in which the process is documented, the responsibilities defined, the legal and operational framework conditions specified and the requirements for the personnel employed in the process defined.

The process shall be designed in such a way that, after the decision of the data controller to destroy the data carrier, no unauthorized persons obtain knowledge of the data, taking into account the protection requirement. According to the local terms and conditions and the protection requirements, the conditions for the collection, storage, transportation and destruction of data carriers shall be determined.

If data carriers are transported, they have to be protected against unauthorized access. Beyond the usage of secured containers and vehicles, particular measures during transfer and storage are to be considered according to the protection requirements (see Clause 4).

3.5 Inspection and testing

3.5.1 Requirements to the data controller

The data controller shall design and verify the whole destruction process under consideration of legal and operational requirements to ensure a proper destruction.

The data controller has to convince itself of the process reliability of the service provider, before the contract is awarded, and to verify this regularly.

3.5.2 Process reliability

The processing and the process steps within the responsibility of the service provider shall be recorded in written form by the service provider.

The documentation of the processing shall be provided to the data controller.

In an audit, the processing and the process steps, shall be checked and confirmed against the requirements of this standard and if applicable against other agreements.

3.5.3 Requirements to certificates of service providers

The corresponding audits for obtaining or renewing a certificate should be conducted by an accredited certifying company, on-site at the service provider. The results shall be recorded.

Certificates of service providers are to be limited to a duration of three years.

4 Process criteria

4.1 General

In the following tables criteria will be given for the three varieties. There might be special scenarios where it can be reasonable to apply combined criteria from several varieties. Furthermore the data controller and the service provider may agree on additional criteria.

4.2 Criteria for all varieties of data carrier destruction

Table 1 specifies criteria which has to be applied for all varieties of data carrier destruction.

Table 1 — General process criteria

Scope	Criterion	Accomplishment of the criterion for compliance with the protection class		
		1	2	3
Organisation	Determination of security levels depending on the protection requirement according to ISO/IEC 21964-1.	Required	Required	Required
	The service provider / the data controller shall check the proper destruction by taking samples on a regular basis.	Possible	Required	Required
Destruction	Usage of equipment for destruction of data carriers according ISO/IEC 21964-2.	Required	Required	Required

4.3 Criteria for variety 1

The criteria which shall be kept for variety 1, data carrier destruction through the data controller directly, are specified in Table 2.

Table 2 — Criteria for variety 1

Scope	Criterion	Accomplishment of the criterion is necessary for compliance with the protection class		
		1	2	3
Organisation	Technical and organisational measures are to be defined for the destruction process (collection point, collection, storage and destruction).	Required	Required	Required
Destruction	A proof shall be provided, that appropriate equipment is used for the data carrier categories to be destroyed.	Required	Required	Required

It is recommended to make persons, involved in the process, aware of the protection requirements of the data carriers and if necessary, oblige them to data secrecy.

4.4 Criteria for variety 2

Table 3 — Criteria for variety 2

Scope	Criterion	Accomplishment of the criterion is necessary for compliance with the protection class		
		1	2	3
Staff	All employees of the service provider have been obligated to data secrecy.	Required	Required	Required
Organisation (Data controller)	There are technical and organisational measures defined for the destruction process (collection point, collection, storage, and destruction). The data controller determines which process steps and tasks shall be fulfilled by the service provider.	Required	Required	Required
Organisation (Service provider)	Technical and organizational measures are defined (in terms of the surrounding) for the destruction facility.	Required	Required	Required
	An evidence shall be provided, that appropriate machinery is used for the data carrier categories being destroyed.	Required	Required	Required
	The service provider grants the responsible authority the right to supervise he destruction of data carrier.	Possible	Possible	Required
	Redundancy and availability of the destruction facility shall be ensured by a contingency plan.	Possible	Required	Required
Collection/Storage/ Transport	For the collection, storage and transport of data carrier, closed and locked security containers, are used, which are adequate to the protective requirements.	Possible	Required	Required
Transport	For transport, vehicles with a closed and locked, fixed body are used.	Possible	Required	Required
Destruction	In principle, the operating staff shall not have access to data carriers with presentation in original size (ISO/IEC 21964-2, Category P). The machine, used for the destruction of the data carrier, is fed either by dumping the content out of the security containers directly into the machine or hopper or by a appropriately secured feed device.	Possible	Possible	Required
	Video surveillance of the discharging procedure respectively the infeed-opening or feed device.	Possible	Possible	Required
	The data controller is entitled to take or be handed a sample of his destroyed data carrier.	Possible	Possible	Required
	The vehicle with the machine for the destruction of data carriers shall have a fixed body.	Required	Required	Required

4.5 Criteria for variety 3

The criteria which shall be kept for variety 3, data carrier destruction off-site by a service provider, are specified in Table 4.

Table 4 — Criteria for variety 3

Scope	Criterion	Accomplishment of the criterion is necessary for compliance with the protection class		
		1	2	3
Staff	Everyone involved in the process and all persons with access to the security zone have been obliged to data secrecy.	Required	Required	Required
	Visitors or deliverers are escorted by an employee of the service provider, during their stay in the security zone.	Required	Required	Required
	Visitors are provided with a visitors ID.	Required	Required	Required
Organisation (Data controller)	There are technical and organizational measures defined for the destruction process (collection point, collection, storage, transport and destruction). The data controller determines which process segments and tasks shall be fulfilled by the service provider.	Required	Required	Required
Organisation (Service provider)	Technical and organizational measures are defined (in terms of the surrounding) for the destruction facility.	Required	Required	Required
	An evidence shall be provided that appropriate machinery is used for the data carrier categories being destroyed.	Required	Required	Required
	The availability of the destruction machine shall be ensured by a contingency plan.	Possible	Required	Required
	The service provider grants the data controller the right to supervise the destruction of the data carriers.	Possible	Possible	Required
Collection/Storage/ Transport	For the collection, storage and transport of data carriers, closed and locked containers, are used, which are adequate to the protective requirements.	Possible	Required	Required
	The receipt of data carriers or security containers by the service provider is recorded in a take-over protocol.	Required	Required	Required
	The handling of loose data carriers (such as reloading or emptying) is permitted only within a secured area. As a basic principle, it is not allowed for the operating staff to have access to data carriers with presentation in original size (ISO/IEC 21964-2, Category P).	Possible	Required	Required
	The service provider shall apply the highest agreed security level for the whole truckload, if the content of security containers with different security levels is tipped into a secured collection vehicle.	Possible	Required	Required
	The storage (until destruction) and emptying of the security containers takes place only in a closed and controlled area (security zone).	Possible	Required	Required
	When undestroyed data carriers are stored unattended, the operations building shall be equipped with an intruder detection system which is connected to an emergency assistance.	Possible	Required	Required