ISO/IEC ~~DIS~~ FDIS 27040:2023(E)

2023-~~01-30~~08-25

ISO/IEC JTC~~-~~ 1/SC 27/WG 4

Secretariat: ~~ILNAS~~DIN

Information technology — Security techniques — Storage security

~~Edited DIS - MUST BE USED FOR FINAL DRAFT~~

Style Definition: Heading 1: Indent: Left: 0 pt, First line: 0 pt, Tab stops: Not at 21.6 pt

Style Definition: Heading 2: Font: Bold, Tab stops: Not at 18 pt

Style Definition: Heading 3: Font: Bold

Style Definition: Heading 4;h4: Font: Bold

Style Definition: Heading 5: Font: Bold

Style Definition: Heading 6: Font: Bold

Style Definition: ANNEX

Style Definition: AMEND Terms Heading: Font: Bold

Style Definition: AMEND Heading 1 Unnumbered: Font: Bold

Style Definition: IneraTableMultiPar: Font: 12 pt, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 19.85 pt + 39.7 pt + 59.55 pt + 79.4 pt + 99.25 pt + 119.05 pt + 138.9 pt + 158.75 pt + 178.6 pt + 198.45 pt

Formatted: German (Germany)

Formatted: German (Germany)

Formatted: German (Germany)

Formatted: German (Germany)

Formatted: German (Germany)

ISO ~~copyright office~~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~~

Email: copyright@iso.org

Website: ~~www.iso.org~~www.iso.org

Published in Switzerland.

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: No page break before, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Contents

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

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.

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. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see ~~www.iso.org/directives~~www.iso.org/directives or ~~www.iec.ch/members_experts/refdocs~~www.iec.ch/members_experts/refdocs).

~~Attention is drawn~~ISO and IEC draw attention to the possibility that ~~some of~~ the ~~elements~~implementation of this document may ~~be~~involve the ~~subject~~use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights~~.~~ in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. 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) or the IEC list of patent declarations received (see https://patents.iec.ch).~~

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

For an explanation of 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 ~~www.iso.org/iso/foreword.html~~www.iso.org/iso/foreword.html. In the IEC, see ~~www.iec.ch/understanding-standards~~www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC~~-~~ 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27040:2015), which has been technically revised.

The main changes are as follows:

- the scope has been expanded to ~~include~~cover requirements;
- the clause structure ~~of the clauses~~ has been more closely aligned with ISO/IEC 27002:2022;
- requirements have been added in Clauses 7, 9, and ~~9.4~~10;

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Default Paragraph Font

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

- adjustments have been made regarding the storage technologies which are covered;

- a new controls labelling scheme has been added;

- ~~the original~~former Annex A, which provided guidance on sanitizing specific types of media, has been removed and text has been added in ~~9.4~~Clause 10, recommending IEEE ~~Std~~ 2883 for this purpose;

- ~~the original~~former Annex B, which included table to help prioritize the adoption of recommendation, has been replaced with Annex A that summarizes the requirements and guidance contained in this document;

- ~~the original~~former Annex C, which provided tutorial oriented material, has been removed and references to appropriate materials have been added ~~to the document~~in Clause 10.

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~~www.iso.org/members.html and ~~www.iec.ch/national-committees~~www.iec.ch/national-committees.

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

~~Introduction~~

~~This document provides implementation requirements and guidance for storage security, which builds upon requirements specified in ISO/IEC 27001. This document recommends the information security risk management approach as defined in ISO/IEC 27005. It is the responsibility of the organization to define their approach to risk management, depending on, for example, the scope of the ISMS, the context of risk management and industry sector. A number of existing methodologies can be used under the framework described in this document to implement the requirements of an ISMS.~~

~~This document is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.~~

~~The objectives for this document are the following:~~

- ~~to highlight the risks arising out of potential threats and attack surfaces;~~
- ~~to assist organizations in better securing their data;~~
- ~~to provide a basis for designing, auditing, and reviewing storage security controls.~~

~~In addition, ISO/IEC 27002 identifies this document for details on methods for sanitizing storage media as well as retention and archive considerations. ISO/IEC 27002 details associated with backups, information deletion, media handling, and ICT readiness for business continuity can also benefit from the requirements and guidance provided in this document.~~

Formatted: Foreword Text

~~Edited DIS - MUST BE USED FOR FINAL DRAFT~~

FINAL DRAFT INTERNATIONAL STANDARD **ISO/IEC ~~DIS~~ FDIS 27040:2023(E)**

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Information technology — Security techniques — Storage security

1 Scope

Formatted: Tab stops: Not at 21.6 pt

This document provides detailed technical requirements and guidance on how organizations can achieve an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security applies to the protection of data both while stored in information and communications technology (ICT) systems and while in transit across the communication links associated with storage. Storage security includes the security of devices and media, management activities related to the devices and media, applications and services, and controlling or monitoring user activities during the lifetime of devices and media, and after end of use or end of life.

Storage security is relevant to anyone involved in owning, operating, or using data storage devices, media, and networks. This includes senior managers, acquirers of storage product and services, and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information or storage security, storage operation, or who are responsible for an organization's overall security programme and security policy development. It is also relevant to anyone involved in the planning, design, and implementation of the architectural aspects of storage network security.

This document provides an overview of storage security concepts and related definitions. It includes requirements and guidance on the threats, design, and control aspects associated with typical storage scenarios and storage technology areas. In addition, it provides references to other international standards and technical reports that address existing practices and techniques that can be applied to storage security.

2 Normative references

Formatted: Tab stops: Not at 21.6 pt

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

~~ISO/IEC 27001:2022, *Information technology — Security techniques — Information security management systems — Requirements*~~

~~ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*~~

~~ISO/IEC 20648, *Information technology — TLS specification for storage systems*~~

~~IEEE 2883, *IEEE Standard for Storage Sanitization*~~

3 Terms and definitions

3.1 General

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at ~~https://www.iso.org/obp~~https://www.iso.org/obp
- IEC Electropedia: available at ~~https://www.electropedia.org/~~https://www.electropedia.org/

3.2 Terms relating to storage technology

3.2.1
block
unit in which data is *stored* (3.2.17) and retrieved on *storage devices* (3.2.14) and *storage media* (3.2.16)

3.2.2
compression
reduction in the number of bits used to represent an item of data

Note 1 to entry: For *storage* (3.2.12), lossless compression (i.e. compression using a technique that preserves the entire content of the original data, and from which the original data can be reconstructed exactly) is used.

3.2.3
data at rest
data recorded on stable, *non-volatile storage* (3.2.11)

3.2.4
data in motion
data being transferred from one location to another

Note 1 to entry: These transfers typically involve interfaces that are accessible and do not include internal transfers (i.e. never exposed outside of an interface, chip, or device).

3.2.5
deduplication
method of reducing *storage* (3.2.12) needs by eliminating redundant data, which is replaced with a pointer to the unique data copy

Note 1 to entry: Deduplication is sometimes considered a form of data reduction.

3.2.6
device
mechanical, electrical, or electronic contrivance with a specific purpose

[SOURCE: ISO/IEC 14776-372:2011, 3.1.10~~.]~~]

3.2.7
Fibre Channel

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Tab stops: Not at 21.6 pt

Formatted: English (United States)

Formatted: Font: Cambria, English (United States)

Formatted: English (United States)

Formatted: English (United States)

Formatted: Font: Cambria

Formatted: Tab stops: Not at 21.6 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

serial input/output interconnect capable of supporting multiple protocols, including access to open system *storage* (3.2.12), access to mainframe storage, and networking

Note 1 to entry: Fibre Channel supports point to point, arbitrated loop, and switched topologies with a variety of copper and optical links running at speeds from 1 gigabit per second to over 128 gigabits per second.

3.2.8
Fibre Channel Protocol
Serial Small Computer System Interface (SCSI) transport protocol used on *Fibre Channel* (3.2.7) interconnects

3.2.9
over provision
technique used by *storage devices* (3.2.14) in which a subset of the available *storage medium* (3.2.16) is exposed through the interface

Note 1 to entry: Storage medium is used internally and independently by the storage device to improve performance, endurance, or reliability.

3.2.10
network attached storage
storage device (3.2.14) or system that connects to a network and provides file access services to computer systems

3.2.11
non-volatile storage
storage (3.2.12) that retains its contents after power is removed

3.2.12
storage
device (3.2.6), function, or service supporting data entry or retrieval

3.2.13
storage area network
network whose primary purpose is the transfer of data between computer systems and *storage devices* (3.2.14) and among storage devices

Note 1 to entry: A storage area network consists of a communication infrastructure, which provides physical connections, and a management layer, which organizes the connections, storage devices, and computer systems so that data transfer is secure and robust.

3.2.14
storage device
component or aggregation of components made up of one or more *devices* (3.2.6) containing *storage media* (3.2.16), designed and built primarily for the purpose for accessing *non-volatile storage* (3.2.11)

3.2.15
storage ecosystem
system of interdependent components that work together to enable *storage* (3.2.12) services and capabilities

Note 1 to entry: The components often include *storage devices* (3.2.14), storage networks, storage management, and other information and communications technology (ICT) infrastructure.

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

3.2.16
storage medium
material on which digital data are, or can be, recorded or retrieved

3.2.17
store
record data on *volatile storage* (3.2.20) or *non-volatile storage* (3.2.11)

3.2.18
target data
information subject to a given process, typically including most or all information on *storage* (3.2.12)

3.2.19
virtualized storage
logical storage
abstraction of physical *storage devices* (3.2.14) or *storage media* (3.2.16) that masks the characteristics and boundaries of the physical *storage* (3.2.12)

Note 1 to entry: Virtualized storage can employ multiple levels of virtualization prior to presenting the virtualized storage to a system or an application.

3.2.20
volatile storage
storage (3.2.12) that fails to retain its contents after power is removed

3.3 Terms relating to sanitization

Formatted: Tab stops: Not at 21.6 pt

3.3.1
clear
sanitize (3.3.12) using logical techniques on user data on all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same host interface available to the user

3.3.2
degauss
render magnetically stored data unreadable by applying a strong magnetic field to the *storage medium* (3.2.16) with an organizationally approved field strength

3.3.3
destruct
sanitize (3.3.12) using physical techniques that make recovery of *target data* (3.2.18) infeasible using state of the art laboratory techniques and results in the subsequent inability to use the *storage medium* (3.2.16) for *storage* (3.2.12)

Note 1 to entry: *Disintegrate* (3.3.5), *incinerate* (3.3.6), *melt* (3.3.7), *pulverize* (3.3.9), and *shred* (3.3.13) are destruct forms of *media sanitization* (3.3.16).

Formatted: Font: Italic

Note 2 to entry: If the storage medium cannot be removed, then the *storage device* (3.2.14) can be subjected to the destruct technique; a storage device can contain multiple storage media.

3.3.4

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

Formatted: Font: 11.5 pt

destruction

result of *destruct* (3.3.3) actions taken to ensure that the *storage medium* (3.2.16) cannot be reused as originally intended and that user data is virtually impossible or prohibitively expensive to recover

3.3.5

disintegrate

destruct (3.3.3) by separating *storage medium* (3.2.16) into its component parts

3.3.6

incinerate

destruct (3.3.3) by burning *storage medium* (3.2.16) completely

3.3.7

melt

destruct (3.3.3) by changing *storage medium* (3.2.16) from a solid to a liquid state generally by the application of heat

3.3.8

cryptographic erase

method of sanitization in which the encryption key for the encrypted *target data* (3.2.18) is *sanitized* (3.3.12), making recovery of the decrypted target data infeasible

3.3.9

pulverize

destruct (3.3.3) by grinding *storage medium* (3.2.16) to a powder or appropriately small particles

3.3.10

purge

sanitize (3.3.12) using physical or logical techniques that make recovery of *target data* (3.2.18) infeasible using state of the art laboratory techniques, but which preserves the *storage media* (3.2.16) and *storage device* (3.2.14) in a potentially reusable state

3.3.11

sanitization

process or method to *sanitize* (3.3.12)

3.3.12

sanitize

render access to *target data* (3.2.18) on *storage* (3.2.12) infeasible for a given level of effort

3.3.13

shred

destruct (3.3.3) by cutting or tearing *storage medium* (3.2.16) into small particles

3.3.14

storage sanitization

logical storage sanitization (3.3.15) or *media sanitization* (3.3.16)

3.3.15

logical storage sanitization