

IEEE Standard for Sanitizing Storage

IEEE Computer Society

Developed by the
Cybersecurity and Privacy Standards Committee

IEEE Std 2883™-2022

STANDARDS

IEEE Standard for Sanitizing Storage

Developed by the

Cybersecurity and Privacy Standards Committee
of the
IEEE Computer Society

Approved 16 June 2022

IEEE SA Standards Board

Abstract: Methods for sanitizing logical storage and physical storage, as well as for providing technology-specific requirements and guidance for the elimination of recorded data, are specified in this standard.

Keywords: clear, crypto erase, cryptographic erase, crypto scramble, data destruct, data removal, destroy, IEEE 2883™, media sanitization, purge, sanitization, sanitize, security

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2022 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 17 August 2022. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

CF+ and CompactFlash are registered trademarks in the U.S. Patent & Trademark Office, owned by CompactFlash Association.

FireWire is a registered trademark in the U.S. Patent & Trademark Office, owned by Apple, Inc.

LTO and Linear Tape-Open are registered trademarks in the U.S. Patent & Trademark Office, owned by Quantum Corporation.

NVM Express and NVMe are registered trademarks in the U.S. Patent & Trademark Office, owned by NVM Express, Inc.

PCIe and PCI Express are registered trademarks in the U.S. Patent & Trademark Office, owned by PCI-SIG.

SMBus is a registered trademark in the U.S. Patent & Trademark Office, owned by Intel, Inc.

TCG and Trusted Computing Group are registered trademarks in the U.S. Patent & Trademark Office, owned by Trusted Computing Group.

PDF: ISBN 978-1-5044-8856-3 STD25526
Print: ISBN 978-1-5044-8857-0 STDPD25526

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the [IEEE SA myProject system](#).¹ An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.²

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

¹ Available at: <https://development.standards.ieee.org/myproject-web/public/view.html#landing>.

² Available at: <https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html>.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#).³ For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#).⁴ Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

³ Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴ Available at: <https://standards.ieee.org/standard/index.html>.

Patents

IEEE Standards are developed in compliance with the [IEEE SA Patent Policy](#).⁵

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

⁵ Available at: <https://standards.ieee.org/about/sasb/patcom/materials.html>.

Participants

At the time this IEEE standard was completed, the Security in Storage Working Group had the following membership:

Jim Hatfield, *Chair*
Eric Hibbard, *Vice Chair*

Richard Austin
Moshin Awan
Sridhar Balasubramanian
David Black
Joseph Chen
Tim Chevalier
Tim Courtney
Anthony Duran
Monty Forehand

John Geldman
JonMichael Hands
Michael Harstrick
Chris Hillier
Walt Hubis
Glen Jaquette
B.J. Lang
Chandra Nelogal

Jamie Pocas
Anna Polubaryeva
Thomas Rivera
Yoni Shternhell
Curtis Stevens
Paul Suhler
Gary Sutphin
Danny Ybarra
Jemmee Yung

The following members of the individual Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Robert Aiello
Johann Amsenga
Philippe Astier
Richard Austin
Ted Bardusch
David Black
Koti Reddy Butukuri
Peter Capelli
Juan Carreon
Joseph Chen
Roger Cummings
Ronald Dean
Andrew Fieldsend

Thomas Friend
John Geldman
Jim Hatfield
Mariana Hentea
Jonathan Herrera
Shui Heung
Eric Hibbard
Chris Hillier
Werner Hoelzl
Richard Jessop
Piotr Karocki
N. Kishor Narang

Henry Newman
Jamie Pocas
R. K. Rannow
Lakshman Raut
Thomas Rivera
Scott Robertson
Bartien Sayogo
Walter Struppler
Paul Suhler
Dmitri Varsanofiev
John Vergis
Forrest Wright
Oren Yuen

When the IEEE SA Standards Board approved this standard on 16 June 2022, it had the following membership:

David J. Law, *Chair*
Ted Burse, *Vice Chair*
Gary Hoffman, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy
Ramy Ahmed Fathy
J. Travis Griffith
Guido R. Hiertz
Yousef Kimiagar
Joseph L. Koepfinger*
Thomas Koshy
John D. Kulick

Johnny Daozhuang Lin
Kevin Lu
Daleep C. Mohla
Andrew Myles
Damir Novosel
Annette D. Reilly
Robby Robson
Jon Walter Rosdahl

Mark Siira
Dorothy V. Stanley
Lei Wang
F. Keith Waters
Karl Weber
Sha Wei
Philip B. Winston
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 2883-2022, IEEE Standard for Sanitizing Storage.

Various data types are recorded on a range of data storage technologies. When these systems or their storage media are repurposed or retired from use, access to the recorded data often needs to be eliminated (sanitized) to avoid unauthorized access to the data. Depending on the storage technology, specific methods can be employed to help ensure that the data are either eliminated or the logical storage and physical storage associated with the data devices/storage media are disposed of properly.

The stakeholders for this standard include all consumers of data storage technologies, especially those that store sensitive or high-value data, and the vendors that manufacture, maintain, and support these technologies. Additionally, regulators and other standards development organizations can leverage the contents of this standard.

Contents

1. Overview	12
1.1 Scope	12
1.2 Using this standard	12
1.3 Word usage	13
2. Normative references	13
3. Definitions, acronyms, and abbreviations	13
3.1 Definitions	13
3.2 Acronyms and abbreviations	15
4. Conventions	16
4.1 Precedence	16
4.2 Lists	17
4.3 Numbering	18
4.4 Bit conventions	19
4.5 Number range convention	19
4.6 Small caps	19
5. Storage sanitization	19
5.1 General	19
5.2 Elements of sanitization	20
5.3 Conformance	21
5.4 Accessibility	21
5.5 Sustainability and media sanitization	22
6. Sanitization methods and techniques	22
6.1 General	22
6.2 Clear	23
6.3 Purge	24
6.4 Destruct	24
6.5 Clear and purge techniques	25
7. Verification of sanitization outcomes	27
7.1 General	27
7.2 Full verification	28
7.3 Representative sampling	28
7.4 Verification for media based cryptographic erase	28
7.5 Verification by physical inspection	29
8. Media type-specific sanitization	29
8.1 General	29
8.2 Hard copy	30
8.3 Optical media	31
8.4 HDD, SSHD, and SSD (ATA, SCSI, and NVMe) storage	31
8.5 Other magnetic media	49
8.6 USB removable media	51
8.7 Memory cards	52
8.8 Embedded flash on boards and storage devices	52
8.9 RAM and ROM-based storage devices	53

Annex A (normative) Storage devices with embedded storage.....	55
A.1 Networking device.....	55
A.2 Equipment.....	56
A.3 Devices with built-in storage	57
Annex B (informative) Cryptographic erase	59
Annex C (informative) Developing storage technologies	63
Annex D (informative) Bibliography	64

List of Figures

Figure 1—Sanitization process.....	23
------------------------------------	----

List of Tables

Table 1—Numbering conventions.....	18
Table 2—General sanitization method comparison.....	22
Table 3—Storage media types in this standard	30
Table 4—Paper and microforms.....	30
Table 5—CD, DVD, Blu-ray sanitization	31
Table 6—Transports for ATA, SCSI, and NVMe command set families	32
Table 7—Relevant standards and specifications for ATA, SCSI, NVMe, and TCG	32
Table 8—Choosing sanitization method for ATA, SCSI, and NVMe.....	33
Table 9—Sanitize cryptographic erase commands.....	47
Table 10—Sanitize block erase commands.....	48
Table 11—Sanitize overwrite commands.....	49
Table 12—Floppy disk sanitization.....	50
Table 13—Removable flexible or rigid magnetic disk sanitization	50
Table 14—Reel and cassette format magnetic tape sanitization.....	51
Table 15—Memory cards sanitization.....	52
Table 16—Embedded flash on boards and storage devices sanitization	52
Table 17—DRAM sanitization.....	53
Table 18—EAPROM sanitization	54
Table 19—EEPROM sanitization	54
Table A.1—Router and switch sanitization.....	56
Table A.2—Office equipment sanitization.....	57
Table A.3—Devices with built-in storage	58
Table B.1—Cryptographic erase considerations	60

IEEE Standard for Sanitizing Storage

1. Overview

1.1 Scope

This standard specifies methods for sanitizing logical storage and physical storage, as well as for providing technology-specific requirements and guidance for the elimination of recorded data.

1.2 Using this standard

The reader can use this standard to do the following:

- become familiar with the principles of storage *sanitization* in Clause 5;
- find the details of the relevant *sanitization* techniques in Clause 6;
- review options and issues for verification of *sanitization* outcomes in Clause 7; and
- find a description of *sanitizing* the specific *storage device* type of interest in Clause 8.

Readers can find conformance details in 5.3, 5.4, and Clause 8.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).^{1,2}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

2. Normative references

The following referenced documents are indispensable for the application of this standard (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

No normative references are cited in this standard.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this standard, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.³

addressable: A characteristic of data, locations, or physical *storage media* in a storage device indicating an ability to be read or written through a *host interface*.

clear: Sanitize using logical techniques on *user data* on all *addressable* storage locations for protection against simple noninvasive data recovery techniques using the same *host interface* available to the user.

cryptographic erase: Method of sanitization in which the encryption key for the encrypted *target data* is *sanitized*, making recovery of the decrypted *target data* infeasible using state-of-the-art laboratory techniques.

degauss: Render magnetically stored data unreadable by applying a strong magnetic field to *storage media* with an organizationally approved field strength.

¹ The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

² The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

³ *IEEE Standards Dictionary Online* is available at: <http://dictionary.ieee.org>. An IEEE account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

destruct: *Sanitize* using physical techniques that make recovery of *target data* infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the *storage media* for *storage*.

NOTE 1—*Disintegrate, incinerate, and melt* are *destruct* forms of *media sanitization*.⁴

NOTE 2—If the *storage media* cannot be removed, then the *storage device* can be subjected to the *destruct sanitization* method; a *storage device* can contain multiple instances of *storage media*.

device: Mechanical, electrical, or electronic contrivance with a specific purpose.

deprecated: A *sanitization* method still permitted although its use is discouraged, and it is not guaranteed to be a part of future specification versions.

disintegrate: *Destruct* by separating a *storage device* into its component parts.

host: Computing system that accesses a *storage device* through a *host interface*.

host interface: A component in a *storage device* through which a *host* transfers commands, data, and status.

incinerate: *Destruct* by burning a *storage device* completely.

logical storage: An abstraction of *physical storage* presented at a *host interface*.

logical storage sanitization: *Sanitization* of logical storage.

NOTE 1—*Clear* and *purge* are actions that can be taken to *sanitize logical storage*.

NOTE 2—*Logical storage sanitization* is a subset of *storage sanitization*.

media based cryptographic erase: Method of *cryptographic erase* in which the encryption key is only resident on the *storage device*.

media sanitization: *Sanitization* of *storage media*.

NOTE 1—*Clear, purge, and destruct* are actions that can be taken to *sanitize storage media*.

NOTE 2—*Media sanitization* is a subset of *storage sanitization*.

melt: *Destruct* by changing *storage media* from a solid to a liquid state, generally by the application of heat.

nonaddressable: A characteristic of data, locations, or physical *storage media* in a *storage device* indicating an inability to be read or written through a *host interface*.

nonvolatile storage: *Storage media* that retains its contents even after power is removed.

physical storage: Physical *storage media*.

pulverize: An obsolete form of *destruct* that grinds a *storage device* to a powder or appropriately small particles.

⁴ Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

purge: *Sanitize* using logical techniques or physical techniques that make recovery of *target data* infeasible using state-of-the-art laboratory techniques, but that preserves the *storage media* and the *storage device* in a potentially reusable state.

NOTE—Judicious selection of the *purge* technique increases the likelihood of preserving the *storage device* in a usable state.

sanitization: Process or method to *sanitize*.

sanitize: Render access to *target data* on *storage media* infeasible for a given level of effort.

shred: An obsolete form of *destruct* that cuts or tears a *storage device* or *storage media* into small particles.

storage: *Device*, function, or service supporting data entry and retrieval.

storage device: Any component or aggregation of components made up of one or more *devices* containing *storage media*, designed, and built for the purpose of accessing *nonvolatile storage*.

storage media: Material on which data are or can be recorded or retrieved.

storage sanitization: *Sanitization* of *logical storage* or *storage media*.

store: Record data on *volatile storage* or *nonvolatile storage*.

target data: Information subject to *sanitization*, generally including most or all data on a piece of *storage media*.

user data: *Target data* written and read by users.

volatile storage: *Storage media* that fails to retain its contents after power is removed.

3.2 Acronyms and abbreviations

ATA	AT attachment
BD	Blu-ray disc
CF	CompactFlash
CFast	CompactFlash on serial ATA
CMB	controller memory buffer
DRAM	dynamic random access memory
EAPROM	electrically alterable programmable read-only memory
EEPROM	electrically erasable programmable read-only memory
EEDP	end-to-end data protection
EHM	enable host memory
HDD	hard disk drive
HMB	host memory buffer
ICT	information and communication technology

I/O	input/output
KEK	key encryption key
LBA	logical block address
LTO	linear tape-open
MAM	medium auxiliary memory, a type of nonvolatile data area
MEK	media encryption key
NAND	type of nonvolatile flash memory
NVMe	NVM Express
NVMe-MI	NVMe Management Interface
PATA	Parallel ATA
PI	protection information
PMR	persistent memory region
RAM	random access memory
ROM	read only memory
RPMB	replay protected memory buffer
SATA	Serial ATA
SCSI	small computer storage interface
SED	self-encrypting device or self-encrypting drive
SSC	security subsystem class ⁵
SMBus	system management bus
SSD	solid-state drive
SSHD	solid-state hard drive (e.g., hybrid drive)
TCG	Trusted Computing Group
WORM	write once read many

4. Conventions

4.1 Precedence

When a conflict between text, figures, and tables occurs, the precedence shall be (in decreasing order) as follows:

- a) text;
- b) tables; and
- c) figures.

⁵ See Annex D.

4.2 Lists

4.2.1 Lists overview

Lists are associated with an introductory paragraph or phrase and are numbered relative to that paragraph or phrase [i.e., all lists begin with an “a)” or an “—” entry].

Each item in a list is preceded by an identification with the style of the identification being determined by whether the list is intended to be an ordered list or an unordered list.

Each item in a list ends with a semicolon, except the last item, which ends in a period. The next-to-the-last entry in the list ends with a semicolon followed by an “and” or an “or” (i.e., “...; and” or “...; or”). The “and” is used if all the items in the list are required. The “or” is used if only one or more items in the list are required.

4.2.2 Unordered lists

An unordered list is one in which the order of the listed items is unimportant (i.e., it does not matter where in the list an item occurs as all items have equal importance).

Each list item shall start with an em dash (“—”). If it is necessary to subdivide a list item further with an additional unordered list (i.e., have a nested unordered list), then the nested unordered list shall be indented and each item in the nested unordered list shall start with an em dash.

The following example shows an unordered list with a nested unordered list:

EXAMPLE—The following items are used for the assembly:

- a box that contains the following:
 - a bolt;
 - a nut; and
 - a washer;
- a screwdriver; and
- a wrench.

4.2.3 Ordered lists

An ordered list is one in which the order of the listed items is important (i.e., item n is required before item $n+1$).

Each listed item starts with a lowercase Western-Arabian letter followed by a closed parenthesis.

If it is necessary to subdivide a list item further with an additional ordered list (i.e., have a nested ordered list), then the nested ordered list shall be indented and each item in the nested ordered list shall start with a decimal number followed by a closed parenthesis.

If it is necessary to subdivide a list item further with an additional unordered list (i.e., have a nested unordered list), then the nested unordered list shall be formatted as specified in 4.2.2.

The following example is of an ordered list with a nested unordered list and a nested ordered list.

EXAMPLE—The instructions for the assembly are as follows:

- a) remove the contents from the box;
 - unwrap each item; and
 - check the inventory;
- b) assemble the item;
 - use a screwdriver to tighten the screws; and
 - use a wrench to tighten the bolts;and
- c) take a break.

4.3 Numbering

A binary number is represented in this standard by any sequence of digits consisting of only the Western-Arabic numerals 0 and 1 immediately followed by a lowercase b (e.g., 0101b). Underscores or spaces may be included between characters in binary number representations to increase readability or delineate field boundaries (e.g., 00101 1010b or 0_0101_1010b).

A hexadecimal number is represented in this standard by any sequence of digits consisting of only the Western-Arabic numerals 0 through 9 and/or the uppercase English letters A through F immediately followed by a lowercase h (e.g., FA23h). Underscores or spaces may be included between characters in hexadecimal number representations to increase readability or delineate field boundaries (e.g., B FD8C FA23h or B_FD8C_FA23h).

A decimal number is represented in this standard by any sequence of digits consisting of only the Arabic numerals 0 through 9 not immediately followed by a lowercase b or lowercase h (e.g., 25). This standard uses the following conventions for representing decimal numbers:

- the decimal separator (i.e., separating the integer and fractional portions of the number) is a period;
- the thousands separator (i.e., separating groups of three digits in a portion of the number) is a space; and
- the thousands separator is used in both the integer portion and the fraction portion of a number.

Table 1 shows numbering conventions for this standard with comparisons to other national conventions.

Table 1—Numbering conventions

French	English	This standard
0,6	0.6	0.6
3,141 582 65	3.14158265	3.141 582 65
1 000	1,000	1 000
1 323 462,95	1,323,462.95	1 323 462.95

A decimal number represented in this standard with an overline under one or more digits following the decimal point is a number where the overlined digits are infinitely repeating (e.g., $666.\overline{6}$ means 666.666 666... or $666\frac{2}{3}$, and $12.\overline{142857}$ means 12.142 857 142 857... or $12\frac{1}{7}$).

4.4 Bit conventions

$n:m$, where n is greater than m , denotes a set of bits [e.g., Feature (7:0)]. $n:m$ where n is greater than m , denotes a bit range.

4.5 Number range convention

$p..q$, where p is less than q , represents a range of numbers (e.g., bytes 100..103 represents 100, 101, 102, and 103).

4.6 Small caps

A word is written in SMALL CAPITALS if it occurs in SMALL CAPITALS in a referenced standard or specification.

5. Storage sanitization

5.1 General

ICT systems capture, process, and *store* data using a wide variety of storage. These data are not only located on the intended *storage media* but also on *storage devices* used to *store*, process, or transmit this information. These *storage media* can require special disposition to mitigate the risk of unauthorized disclosure of data (e.g., to help ensure the confidentiality of that data). Efficient and effective management of data created, processed, and stored by an ICT system throughout its life, from its inception through disposition, is a primary concern of an ICT system owner and the custodian of the data.

When *storage devices* are transferred, become obsolete, are no longer usable, or required by an ICT system, it is important that residual magnetic, optical, electrical, or other representation of data are not recoverable. For sensitive or regulated data, controlled elimination of data recorded on *storage media* is a necessity. *Storage sanitization*, henceforth *sanitization*, refers to the general process of denying access to data from *storage media*, such that reasonable assurance exists that the data cannot be retrieved or reconstructed. The focus on access is important because sometimes the data on the *storage media* cannot be eliminated, so other steps (e.g., destruction of the *storage media*) can become necessary.

If the *sanitization* of data is intended to remove all instances of specific data, then all media on which that data has been stored (e.g., as a result of caching, replication, mirroring or other redundancy, backup or point in time copies, swapping, and paging) also requires *sanitization*.

An example of this is NVMe HMB data stored in persistent memory (e.g., NVDIMM) or swapped to backing storage.

The concept of *sanitization* of data recorded on *storage media* is easy to understand; however, putting the concept into practice can be challenging. An additional complication is the inconsistent use of vague terminology to describe this elimination of data. Vague terms with poorly defined meanings include the following:

- deletion, which can refer to the file system operation that removes a few file system pointers (e.g., no data are removed);
- secure data deletion, which potentially only removes currently accessible copies of data as opposed to all copies of data on the *storage media*; and
- data shredding, which can refer to a physical *shredder* or scrambling of returned data by the deletion of the encryption key.

Annex C describes some emerging technologies out of scope for this standard.

5.2 Elements of sanitization

Sanitization is often an important part of an organization's data governance program, which generally includes policies and processes that focus on handling sensitive data (e.g., personal data, personally identifiable information, electronic healthcare records, trade secrets, intellectual property, customer records, financial records, or mission-critical data). Such a governance program covers the full data lifecycle (creation/generation/collection, processing, transferring, storing, archiving, and destruction of data) and the ICT infrastructure associated with these data. An important aspect of this governance addresses the need to eliminate data due to changes in business needs or compliance obligations, which can include producing appropriate documentation to serve as evidence of the actions taken.

Eliminating data, or rendering data permanently inaccessible, can be handled by one or more of the following:

- *data sanitization*: Focused on all instances of stored data, wherever the data resides. Such elimination can be quite challenging because all copies need to be identified, and adequate data maps potentially do not exist. These data copies can exist within applications, cloud services, virtual environments, primary compute and storage resources, secondary and off-line storage, archives, and data protection systems (e.g., backups and replications). For each of these data locations, specific technology-oriented actions (to achieve *storage sanitization*) are then necessary to eliminate the data;
- *storage sanitization*: Focused on data stored on ICT infrastructure that uses *nonvolatile storage* (e.g., fixed-block *storage* arrays, network attached storage systems, object storage, cloud storage, and backup systems) that can take the form of *logical storage* or physical storage that contains *storage media*; and
- *media sanitization*: Focused on data stored on *storage devices* or *storage media*.

Sanitization can involve some or all of the following:

- identifying the type of storage involved: *logical storage* or *media* aligned (*media sanitization*);
- selecting the *sanitization* method (i.e., *clear*, *purge*, or *destruct*) appropriate for the type of *storage device* and the data sensitivity;
- executing one or more of the selected *storage sanitization* techniques;