International Standard

ISO/IEC 27040

Information technology — Security techniques — Storage security

Technologie de l'information — Techniques de sécurité — Sécurité de stockage

Second edition
2024-01

Reference number
ISO/IEC 27040:2024(en)

© ISO/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**
3.1 General 1
3.2 Terms relating to storage technology 1
3.3 Terms relating to sanitization 3
3.4 Terms relating to availability 5
3.5 Terms relating to security and cryptography 5
3.6 Terms relating to archives and repositories 6
3.7 Miscellaneous terms 8

4 Symbols and abbreviated terms **8**

5 Structure of this document **11**
5.1 General 11
5.2 Controls 11

6 Overview and concepts **11**
6.1 General 11
6.2 Storage concepts 12
6.3 Introduction to storage security 13
6.4 Storage security risks 15
6.4.1 Background 15
6.4.2 Data breaches 16
6.4.3 Data corruption or destruction 16
6.4.4 Temporary or permanent loss of access/availability 17
6.4.5 Failure to meet statutory, regulatory, or legal requirements 17

7 Organizational controls for storage **18**
7.1 General 18
7.2 Align storage and policy 18
7.3 Business continuity management 18
7.4 Compliance 19

8 People controls for storage **20**

9 Physical controls for storage **21**
9.1 General 21
9.2 Physically secure storage 21
9.3 Protect physical interfaces to storage 21
9.4 Isolation of storage systems 22

10 Technological controls for storage **22**
10.1 General 22
10.2 Design and implementation of storage security 22
10.2.1 General 22
10.2.2 Storage security design principles 23
10.2.3 Storage system quality attributes 25
10.2.4 Retention, preservation, and disposal of data 27
10.3 Storage systems security 28
10.3.1 System hardening 28
10.3.2 Security auditing, accounting, and monitoring 28
10.3.3 Storage vulnerability management 31
10.4 Storage management 31
10.4.1 Background 31
10.4.2 Authentication and authorization 32
10.4.3 Secure the management interfaces 34

© ISO/IEC 2024 – All rights reserved

10.5 Data confidentiality 35
10.5.1 General 35
10.5.2 Encryption and key management issues 36
10.5.3 Encryption of storage 37
10.5.4 Encrypting transferred data 40
10.5.5 Encrypting data at rest 41
10.6 Storage sanitization 42
10.6.1 General 42
10.6.2 Selection of sanitization methods 43
10.6.3 Media-based sanitization 44
10.6.4 Logical sanitization 44
10.6.5 Cryptographic erase 45
10.6.6 Verification of storage sanitization 46
10.6.7 Proof of sanitization 47
10.7 Direct attached storage 48
10.8 Storage networking 48
10.8.1 Background 48
10.8.2 Storage area networks 49
10.8.3 Network Attached Storage protocols 54
10.9 Block-based storage 55
10.9.1 Fibre Channel (FC) storage 55
10.9.2 IP storage 56
10.10 File-based storage 57
10.10.1 General 57
10.10.2 NFS-based NAS 57
10.10.3 SMB-based NAS 58
10.11 Cloud computing storage 59
10.11.1 Securing cloud computing storage 59
10.11.2 CDMI security 59
10.12 Object-based storage 60
10.13 Data reductions 61
10.14 Data protection and recovery 62
10.14.1 General 62
10.14.2 Storage backups 62
10.14.3 Storage replication 63
10.14.4 Storage snapshots 63
10.15 Data archives and repositories 64
10.15.1 General 64
10.15.2 Data archives 64
10.15.3 Data Repositories 68
10.16 Virtualization 68
10.16.1 Storage virtualization 68
10.16.2 Storage for virtualized systems 69
10.17 Secure multi-tenancy 70
10.18 Secure autonomous data movement 71

Annex A (informative) **Storage security controls summary** **73**

Bibliography **82**

© ISO/IEC 2024 – 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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the 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.

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. In the IEC, see 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 cover requirements;

— the clause structure has been more closely aligned with ISO/IEC 27002:2022;

— requirements have been added in Clauses 7, 9, and 10;

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

— a new controls labelling scheme has been added;

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

— 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;

— former Annex C, which provided tutorial oriented material, has been removed and references to appropriate materials have been added 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 and www.iec.ch/national-committees.

© ISO/IEC 2024 – All rights reserved

Information technology — Security techniques — Storage security

1 Scope

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 products 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

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*

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

— IEC Electropedia: available at 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)

© ISO/IEC 2024 – All rights reserved