

# ISO/IEC 27040:2024-01 (E)

## Information technology - Security techniques - Storage security

---

### 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        |
| 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        |
|         | <b>Annex A (informative) Storage security controls summary.....</b> | <b>73</b> |
|         | <b>Bibliography.....</b>                                            | <b>82</b> |