

ISO TC 171/SC 1

Date: 2018-05

Deleted: 03

ISO 14641:2018(E)

ISO TC 171/SC 1

Secretariat: ~~BSI~~

Deleted: ANSI

Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications

Archivage électronique — La conception et à l'exploitation d'un système informatique pour la conservation intégrée de documents électroniques — Spécifications

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO 14641:2018](https://standards.iteh.ai/catalog/standards/sist/821ae94b-8838-4be9-8a5b-a57238374be0/iso-14641-2018)

<https://standards.iteh.ai/catalog/standards/sist/821ae94b-8838-4be9-8a5b-a57238374be0/iso-14641-2018>

Contents

Page

Foreword.....	7
Introduction.....	8
1 Scope	1
2 Normative references	1
3 Terms and definitions.....	2
4 General characteristics and levels of requirements	5
4.1 Characteristics.....	5
4.2 Levels of requirements.....	6
5 General specifications.....	8
5.1 General	8
5.2 Technical description manual.....	8
5.3 Archival system profiles.....	8
5.4 Operational procedures	9
5.4.1 General	9
5.4.2 Scanned documents	9
5.4.3 Digitally born documents	10
5.5 Security.....	10
5.5.1 Management and organization of security.....	10
5.5.2 Risk assessment	10
5.5.3 Physical security	11
5.5.4 Hardware security.....	11
5.5.5 Security of custom software and software products	11
5.5.6 Maintenance of the information system.....	12
5.5.7 System change-management and migration of media	12
5.5.8 Security backups.....	13
5.5.9 Continuity of access to archives	13
5.6 Date and time stamping	13
5.7 Audit trail	14
5.7.1 General	14
5.7.2 Secure preservation of the audit trail	14
5.7.3 Archive lifecycle log.....	14
5.7.4 Events log.....	15
6 Storage media considerations.....	16
6.1 Media type definition	16
6.2 Preservation of archival media	16
7 Systems using removable media.....	16
7.1 General	16
7.2 Initialization of removable storage volumes.....	17
7.3 Finalization of removable storage volumes.....	17
7.4 Labelling of physical WORM media.....	17
8 Systems using logical WORM media	17
9 Systems using rewritable media	17
9.1 General	17
9.2 Standard security level.....	18
9.3 Strong security level.....	18
9.4 Advanced security level.....	18
10 Archival capture.....	18
10.1 Electronically born documents.....	18

10.1.1	General	18
10.1.2	Procedure for archives capture (deposit)	19
10.1.3	Marked-up electronic documents	19
10.1.4	Electronic documents using a layout format	19
10.1.5	Other electronic document formats	19
10.1.6	Print streams	19
10.1.7	Verification of electronic documents	19
10.1.8	Integrity control of electronic documents transferred from source applications	20
10.1.9	Metadata capture	20
10.1.10	Indexing and document searches	20
10.2	Paper-based or microform documents	21
10.2.1	Scanning devices for documents	21
10.2.2	Image processing features	21
10.2.3	Paper document or microform capture procedure	22
10.2.4	Audit trails	22
10.3	Analogue audio/video objects on tape media	24
10.3.1	General	24
10.3.2	Preparation of original tape media	24
10.3.3	Original audio and audiovisual object digitization	24
10.3.4	Audio and audiovisual information processing	24
10.3.5	Events log	25
10.4	Image, audio and video information compression techniques	26
10.4.1	Compression types	26
10.4.2	Paper or microform documents	26
10.4.3	Audio or audiovisual recordings objects	26
10.5	Format conversion	27
11	Archival operations	28
11.1	Scope	28
11.2	Access	28
11.2.1	General	28
11.2.2	Digitized documents	28
11.2.3	Marked-up electronic documents	28
11.2.4	Electronic documents using lay-out format	28
11.3	Restitution	28
11.4	Archives disposal	29
12	Information system assessment	29
12.1	General	29
12.1.1	Audits	29
12.1.2	Objectives	29
12.1.3	Auditor responsibilities	29
12.1.4	Personnel responsible for assessment	30
12.1.5	Verification of documentation	30
12.1.6	Assessment operations documents	30
12.2	Internal assessment	30
12.3	External assessment	30
13	Trusted third-party archival	31
13.1	Activities of trusted third-party archive service provider	31
13.2	Service contract model	32
13.2.1	Service contract	32
13.2.2	Service contract duration	32
13.2.3	Preservation period	32
13.2.4	Quality of service	32
13.2.5	Security and data protection	32
13.2.6	Information and counsel	33
13.2.7	Transfer and continuity	33
13.2.8	Transferability	33
13.2.9	Restitution	34
13.2.10	Confidentiality and private data	34

ISO STANDARD PREVIEW
 (StandardSatchal)
 ISO 14641-2018
 a57238374be0/iso-14641-2018

13.2.11	Professional insurance.....	34
13.2.12	Subcontracting	34
13.2.13	Assessment	34
14	Service providers.....	34
14.1	General	34
14.2	Subcontractor agreement.....	34
14.3	Contract with subcontractor	35
14.4	Data transfer over telecommunications networks	35
Annex A (informative)	Archival policy.....	36
Annex B (informative)	Declaration of archival practices.....	37
Annex C (informative)	General service conditions.....	38
Bibliography	39

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO 14641:2018](https://standards.iteh.ai/catalog/standards/sist/821ae94b-8838-4be9-8a5b-a57238374be0/iso-14641-2018)

<https://standards.iteh.ai/catalog/standards/sist/821ae94b-8838-4be9-8a5b-a57238374be0/iso-14641-2018>

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO 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 Technical Committee ISO/TC 171, *Document management applications*, Subcommittee SC 1, *Quality, preservation and integrity of information*.

This first edition cancels and replaces ISO 14641-1:2012, which has been technically revised.

Introduction

Electronic documents are an essential part of everyday business, whether the sources are incoming communications or output from organizations. It is important that electronic documents be stored appropriately, either fully or in part, in secure information systems designed for operations and archiving, in order to meet business, legal or regulatory requirements.

The objectives of secure information systems are to resolve organizational issues such as:

- a) optimization of long-term electronic document preservation, archiving and integrity;
- b) provision of information search facilities;
- c) ensuring ease of access and use of electronic documents.

This document is intended to provide a reference framework for organizations. It describes the methods and techniques to be used for the implementation of an electronic information system for managing documents within an archive. In conjunction with related archival policies of organizations, it describes criteria for system design and specifications for operational processes.

These specifications are intended to ensure that all documents to be managed by the information system are captured, stored, retrieved and accessed in a way that guarantees that the archived document is an authentic rendition of the original document for the duration of preservation. An authentic rendition means that the rendered document corresponds to the source document as it was at the time of input in the information system in respect of criteria of fidelity and integrity, and that this state is maintained for the duration of preservation.

This document takes into account the use of three possible archiving media: physical WORM, logical WORM and rewritable media. Archival integrity is ensured on physical and logical WORM media by the inherent properties of WORM solutions. On rewritable media, integrity is ensured using encryption-like techniques, in particular with checksum calculation or hash function, date and time stamp or digital signature. In all cases, it is necessary to comply with related procedures.

Depending on the types of documents to be archived, other specialized standards can be relevant and used to complement the recommendations in this document.

This document provides a specific and complementary definition of issues addressed in other standards or specifications concerning the management of electronic information. Its content is intended to address execution issues raised in several other documents. These include ISO/TR 15801, ISO 15489-1 and MoReq2^[15], which detail specifications for organizing and controlling the lifecycle of archived information for purposes of evidence and operational history, and ISO 14721, which describes the characteristics of an open system for the preservation of digital data.

Annexes A, B and C are complementary.

Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications

1 Scope

This document specifies a set of technical specifications and organizational policies to be implemented for the capture, storage and access of electronic documents. This ensures legibility, integrity and traceability of the documents for the duration of their preservation.

This document is applicable to electronic documents resulting from:

- the scanning of original paper or microform documents;
- the conversion of analogue audio or video content;
- the “native” creation by an information system application;
- other sources that create digital content such as two- or three- dimensional maps, drawings or designs, digital audio/video and digital medical images.

This document is not applicable to information systems in which users have the ability to substitute or alter documents after capture.

This document is intended for the following users. [ISO 14641:2018](#)

- a) Organizations implementing information systems in which:
 - 1) electronic documents created from scan captures are kept in an environment that ensures fidelity with regard to the original and long-term preservation;
 - 2) digitally born documents are kept in an environment that ensures the content integrity of the information and document legibility;
 - 3) traceability is ensured for all operations relating to the electronic documents.
- b) Organizations providing information technology services and software publishers seeking to develop information systems that ensure the fidelity and integrity of electronic documents.
- c) Organizations providing third-party document archiving services.

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 2859 (all parts), *Sampling procedures for inspection by attributes*

ISO 8601, *Data elements and interchange formats — Information interchange — Representation of dates and times*

ISO/TR 12033, *Document management — Electronic imaging — Guidance for the selection of document image compression methods*

ISO 12653-1, *Electronic imaging — Test target for the black-and-white scanning of office documents — Part 1: Characteristics*

ISO 12653-2, *Electronic imaging — Test target for the black-and-white scanning of office documents — Part 2: Method of use*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12653-1, ISO 12653-2 and the following apply.

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

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

3.1

access

processes of retrieving and displaying (playing) electronic documents for operational, evidential or historical purposes

3.2

archive

set of documents produced or received, whatever their date, format or storage media, by any individual, organization, public or private service, in the course of their activity

3.3

archival policy

legal, functional, operational, technical and security requirements of an internal or external information system

Note 1 to entry: Annexes A and B give principles of an archival policy and of a declaration of archival practices.

3.4

archive lifecycle log

log which records *audit trail* (3.9) data related to the document lifecycle archiving process

3.5

archive restitution

return and transfer of archived documents to their originator, or to a duly appointed person or organization

3.6

archival system profile

set of properties that applies to a class of *archives* (3.2) that share common characteristics in terms of confidentiality, retention and disposal schedules, and *access* (3.1) rights (e.g. create, read, modify, delete)

3.7

ACU

attestation creation unit

hardware and/or software devices for the delivery of *electronic attestations* (3.23)

Note 1 to entry: Attestations include a unit identifier and the related archival service identifier.

3.8

audiovisual

communication techniques combining sound and image

3.9

audit trail

aggregate of the information necessary to provide a historical record of all significant events associated with stored information and the information system

3.10

data

digital form of information which can be accessed, read and/or processed

3.11

date and time stamp

sequence of characters denoting the date and/or time at which a certain event occurred

3.12

deposit

set of documents sharing the same *archival system profile* (3.6)

3.13

digital archival

set of actions aiming to identify, capture, classify, preserve, retrieve, display and provide *access* (3.1) to documents for informational or historical purposes, or for the duration required to meet legal obligations

3.14

digital document

digital representation of content that is stored and managed electronically

Note 1 to entry: Association of content, logical structure and display attributes, retrievable by a device capable of rendering a human-readable (or machine-readable) object. A document can be digitally born (creation) at source or converted from an analogue document.

3.15

digital fingerprint

bit sequence generated from a *digital document* (3.14) using an algorithm that uniquely identifies the original document

Note 1 to entry: Any digital document modification will produce a different fingerprint.

3.16

digital seal

method for ensuring the *integrity* (3.27) of a document including *hash functions* (3.26), *digital signatures* (3.17) and, optionally, a *date and time stamp* (3.11)

3.17

digital signature

data which, when appended to a *digital document* (3.14), enable the user of the document to authenticate its origin and *integrity* (3.27)

3.18

digitization

conversion of an analogue document (paper, microform, film, analogue audio or *audiovisual* (3.8) tapes) to digital format for the purpose of preservation or processing

3.19

digitized document

result of *digitization* (3.18) of information initially stored on physical media (paper, microform, and film, analogue audio or *audiovisual* (3.8) tapes)

3.20
document fidelity

property of an archived document which renders all the information contained in the original source document

Note 1 to entry: This notion is applicable to any change of form, including *digitization* (3.18) or *format conversion* (3.25).

3.21
durability

attribute of a document which remains readable during its entire lifecycle

3.22
electronic information system

system designed to receive, preserve, *access* (3.1) and transfer *archives* (3.2) in an electronic form

3.23
electronic attestation

information produced to provide evidence that an action or an electronic transaction has occurred

3.24
events log

log which records *audit trail* (3.9) *data* (3.10) related to the system operations

3.25
format conversion

operation converting a *digital document* (3.14) to a different electronic format

Note 1 to entry: This operation preserves the fidelity of the document.

3.26
hash function

mathematical algorithm used for turning some kinds of *data* (3.10) into a relatively small integer

3.27
integrity

attribute of a document whose content is complete and unaltered

Deleted: completed

3.28
legibility

attribute of an archived document which allows *access* (3.1) to all the information it contains

Note 1 to entry: This could be facilitated by certain *metadata* (3.31) associated with the document.

3.29
lossy compression

compression algorithm which loses some of the original information during compression

Note 1 to entry: The resulting decompressed object is only an approximation of the original.

3.30
media migration

act of transferring a document from one medium to another, particularly with regard to managing media obsolescence

3.31
metadata

data (3.10) describing the context, content and structure of a document and their management over time

**3.32
replication**

process which consists of copying information between redundant resources, notably software or hardware components, to improve reliability, fault-tolerance or accessibility

**3.33
time source**

internal or external component of an information system providing a reliable and objective time reference suited to requirements

**3.34
time-stamp token**

data (3.10) object that binds a representation of data to a particular time (expressed in UTC), thereby providing evidence that the data existed at that time

**3.35
transferability**

ability to recover an authentic *digital archive* (3.13) (information, *data* (3.10), objects and all related *metadata* (3.31) from one information system) in order to transfer it to another information system by means of a procedure specified in advance

Note 1 to entry: This issue is of particular importance when information is stored by a third-party archive service provider.

**3.36
trusted third-party archive service provider**

third-party individual or organization in charge of *archives* (3.2) preservation

4 General characteristics and levels of requirements

4.1 Characteristics

In order that an organization might apply a recognized specifications framework for the storage, use, archiving, retrieval and display of electronic documents, both technical and organizational measures need to be taken to ensure document integrity and long-term preservation.

In this context, an electronic information system shall implement a pre-defined archival policy; a description of the general principles of such a policy is described in Annex A.

It is important to recognize that information systems will capture electronic documents that are being submitted for long-term storage and use. The term "capture" in this sense reflects the receipt and processing of information to be managed by the information system. Where hardcopy documents need to be stored and managed in electronic form, these documents shall be scanned and indexed prior to their capture in the information system.

This document is applicable only to unalterable captured documents. Related document reference data in the file system or database shall not be erasable, changeable or able to be replaced by new data.

Procedures and security requirements shall be implemented in order to:

- a) control the process of archiving;
- b) prevent and/or detect modifications made to documents or to the data necessary for their retrieval and display;