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

*Archivage électronique — Conception et exploitation d'un
système informatique pour la conservation intégrée de documents
électroniques — Spécifications*

(<https://standards.iteh.ai>)
Document Preview

ISO 14641:2018

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



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 14641:2018

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



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

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
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	vi
Introduction	vii
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	9
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	15
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	19
10.1 Electronically born documents	19
10.1.1 General	19
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	20
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	21
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	23
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	25
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	27
10.4.3	Audio or audiovisual recordings objects	27
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	29
11.2.3	Marked-up electronic documents	29
11.2.4	Electronic documents using lay-out format	29
11.3	Restitution	29
11.4	Archives disposal	29
12	Information system assessment	30
12.1	General	30
12.1.1	Audits	30
12.1.2	Objectives	30
12.1.3	Auditor responsibilities	30
12.1.4	Personnel responsible for assessment	30
12.1.5	Verification of documentation	31
12.1.6	Assessment operations documents	31
12.2	Internal assessment	31
12.3	External assessment	31
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	33
13.2.3	Preservation period	33
13.2.4	Quality of service	33
13.2.5	Security and data protection	33
13.2.6	Information and counsel	33
13.2.7	Transfer and continuity	34
13.2.8	Transferability	34
13.2.9	Restitution	34
13.2.10	Confidentiality and private data	34
13.2.11	Professional insurance	35

13.2.12	Subcontracting.....	35
13.2.13	Assessment.....	35
14	Service providers.....	35
14.1	General.....	35
14.2	Subcontractor agreement.....	35
14.3	Contract with subcontractor.....	35
14.4	Data transfer over telecommunications networks	36
Annex A	(informative) Archival policy.....	37
Annex B	(informative) Declaration of archival practices.....	38
Annex C	(informative) General service conditions.....	39
Bibliography		40

iTeh Standards (<https://standards.iteh.ai>) Document Preview

ISO 14641:2018

<https://standards.iteh.ai/catalog/standards/iso/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.

ISO 14641:2018

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

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.