

---

---

**Document management —  
Electronically stored information —  
Recommendations for trustworthiness  
and reliability**

*Gestion de document — Information stockée électroniquement —  
Recommandations pour contribuer à l'intégrité et à la fiabilité des  
informations stockées*



This document is a preview generated by EBS



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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  
Ch. de Blandonnet 8 • CP 401  
CH-1214 Vernier, Geneva, Switzerland  
Tel. +41 22 749 01 11  
Fax +41 22 749 09 47  
copyright@iso.org  
www.iso.org

# Contents

	Page
<b>Foreword</b> .....	<b>vi</b>
<b>Introduction</b> .....	<b>vii</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Information management policy</b> .....	<b>2</b>
4.1 General.....	2
4.2 Information management policy document.....	2
4.2.1 Contents.....	2
4.2.2 ESI covered.....	3
4.2.3 ESI roles and responsibilities.....	3
4.2.4 ESI security classification.....	3
4.2.5 Storage media.....	4
4.2.6 Data file formats and compression.....	4
4.2.7 Outsourcing.....	4
4.2.8 Standards related to information management.....	4
4.2.9 Retention and disposal schedules.....	5
4.2.10 Information management responsibilities.....	5
4.2.11 Compliance with policy.....	5
<b>5 Duty of care</b> .....	<b>5</b>
5.1 General.....	5
5.1.1 Trusted system.....	5
5.1.2 Controls.....	5
5.1.3 Segregation of roles.....	6
5.2 Information security management.....	6
5.2.1 Information security policy.....	6
5.2.2 Risk assessment.....	7
5.2.3 Information security framework.....	8
5.3 Business continuity planning.....	8
5.4 Consultations.....	8
<b>6 Procedures and processes</b> .....	<b>9</b>
6.1 General.....	9
6.2 Procedures manual.....	9
6.2.1 Documentation.....	9
6.2.2 Content.....	9
6.2.3 Compliance with procedures.....	10
6.2.4 Updating and reviews.....	10
6.3 ESI capture.....	10
6.3.1 General.....	10
6.3.2 Creation and importing.....	11
6.3.3 Information loss.....	11
6.3.4 Metadata.....	12
6.4 Document image capture.....	12
6.4.1 General.....	12
6.4.2 Preparation of paper documents.....	12
6.4.3 Document batching.....	13
6.4.4 Photocopying.....	13
6.4.5 Scanning processes.....	14
6.4.6 Quality control.....	15
6.4.7 Rescanning.....	17
6.4.8 Image processing.....	17
6.5 Data capture.....	17

6.5.1	Data creation .....	17
6.5.2	Conversion and migration .....	18
6.6	Database considerations .....	18
6.6.1	General .....	18
6.6.2	Database systems .....	18
6.6.3	Database schemas .....	20
6.6.4	Master data management .....	20
6.6.5	Transactional vs. updating .....	21
6.7	Indexing .....	21
6.7.1	General .....	21
6.7.2	Manual indexing .....	21
6.7.3	Automatic indexing .....	21
6.7.4	Index storage .....	21
6.7.5	Index amendments .....	22
6.7.6	Index accuracy .....	22
6.8	Authenticated output procedures .....	22
6.9	ESI transmission .....	23
6.9.1	Intra-system ESI transfer .....	23
6.9.2	External transmission of files .....	23
6.10	Information retention .....	24
6.11	Information preservation .....	25
6.12	Information destruction .....	25
6.13	Backup and system recovery .....	25
6.14	System maintenance .....	26
6.14.1	General .....	26
6.14.2	Scanning systems .....	26
6.15	Security and protection .....	27
6.15.1	Security procedures .....	27
6.15.2	Encryption keys .....	27
6.16	Use of contracted services .....	28
6.16.1	General .....	28
6.16.2	Procedural considerations .....	28
6.16.3	Transportation of paper documents .....	29
6.16.4	Use of trusted third party .....	29
6.17	Workflow .....	29
6.18	Date and time stamps .....	30
6.19	Version control .....	30
6.19.1	Information .....	30
6.19.2	Documentation .....	30
6.19.3	Procedures and processes .....	31
6.20	Maintenance of documentation .....	31
<b>7</b>	<b>Enabling technologies .....</b>	<b>31</b>
7.1	General .....	31
7.2	System description manual .....	32
7.3	Storage media and sub-system considerations .....	32
7.4	Access levels .....	33
7.5	System integrity checks .....	33
7.5.1	General .....	33
7.5.2	Digital and electronic signatures (including biometric signatures) .....	34
7.6	Image processing .....	34
7.7	Compression techniques .....	35
7.8	Form overlays and form removal .....	36
7.9	Environmental considerations .....	36
7.10	Migration .....	36
7.11	Information deletion and/or expungement .....	37
<b>8</b>	<b>Audit trails .....</b>	<b>37</b>
8.1	General .....	37

8.1.1	Audit trail data.....	37
8.1.2	Creation .....	38
8.1.3	Date and time.....	38
8.1.4	Storage.....	38
8.1.5	Access.....	39
8.1.6	Security and protection.....	39
8.2	System.....	39
8.2.1	General.....	39
8.2.2	Audit trail information.....	40
8.2.3	Migration and conversion.....	40
8.3	ESI.....	40
8.3.1	General.....	40
8.3.2	ESI capture.....	40
8.3.3	Batch information.....	41
8.3.4	Indexing.....	42
8.3.5	Change control.....	42
8.3.6	Digital signatures.....	42
8.3.7	Destruction of information.....	43
8.3.8	Workflow.....	43
<b>Bibliography.....</b>		<b>44</b>

## 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](http://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](http://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](http://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 third edition cancels and replaces the second edition (ISO/TR 15801:2009), which has been technically revised.

## Introduction

This document defines recommended practices for electronic storage of business or other information in an electronic form. As such, complying with its recommendations is of value to organizations even when the trustworthiness of the stored information is not being challenged, especially in jurisdictions with e-discovery legislation.

Information originates from many sources. This document covers information in any form, from the traditional scanned images, word processed documents and spreadsheets to the more “modern” forms which include e-mail, web content, instant messages, CAD drawing files, blogs, wikis, etc. Also included is information stored in databases and other data storage systems. Recommendations in this document can be useful in systems that use local and/or cloud storage.

Users of this document should be aware that the implementation of these recommendations does not automatically ensure acceptability of the evidence contained within the information. Where electronically stored information (ESI) might be required in court or other adversarial situation, implementers of this document are advised to seek legal advice to ascertain the precise situation within their relevant legal environment.

This document describes means by which it can be demonstrated, at any time, that the information created or existing within an information management system has not changed since it was created within the system or imported into it.

Regardless of the original format, it will be possible to demonstrate that information stored in a trustworthy information management system can be reliably reproduced in a consistent manner and accurately reflects what was originally stored without any material modification.

Alternative versions of the information in a document might legitimately develop, e.g. revision of a contract. In these cases, the new versions are treated as new documents. The same principle can be applied when a significant change is made to a document in a workflow environment.

Information technology based systems can store, in an electronic form, both documents and records. This document describes means for storing all types of ESI in a trustworthy and reliable manner, as part of an information governance strategy. Where records (as defined in ISO 15489-1) are stored, the requirements of this document can be used in conjunction with those specified in ISO 15489-1 to ensure that the policies and procedures described in this document work in conjunction with those specified in ISO 15489-1.

When information preservation is considered, the requirements of ISO 14641 can be used in conjunction with this document. Readers are advised to use this document in conjunction with other local sources, particularly with relevance to governmental and legal requirements in their respective jurisdictions.





# Document management — Electronically stored information — Recommendations for trustworthiness and reliability

## 1 Scope

This document describes the implementation and operation of information management systems that store and make available for use electronically stored information (ESI) in a trustworthy and reliable manner. Such ESI can be of any type, including “page based” information, information in databases and audio/video information.

This document is for use by any organization that uses systems to store trustworthy ESI over time. Such systems incorporate policies, procedures, technology and audit requirements that ensure that trustworthiness of the ESI is maintained.

This document does not cover processes used to evaluate whether ESI can be considered to be trustworthy prior to it being stored or imported into the system. However, it can be used to demonstrate that, once the electronic information is stored, output from the system will be a true and accurate reproduction of the ESI created and/or imported.

## 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 12651 (all parts), *Electronic document management — Vocabulary*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12651 (all parts) 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 <http://www.iso.org/obp>

### 3.1 electronically stored information ESI

data or information of any kind and from any source, whose temporal existence is evidenced by being stored in or on any electronic medium

Note 1 to entry: ESI includes traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations and other electronic formats commonly found on a computer. ESI also includes system, application and file-associated metadata such as timestamps, revision history, file type, etc.

Note 2 to entry: Electronic medium can take the form of, but is not limited to, storage devices and storage elements.

[SOURCE: ISO/IEC 27040:2015, 3.16]