TECHNICAL REPORT

ISO/TR 15801

Second edition
2009-10-15

Document management — Information stored electronically — Recommendations for trustworthiness and reliability

Images électroniques — Stockage électronique d'informations — Recommandations pour les informations de valeur et leur fiabilité

Reference number
ISO/TR 15801:2009(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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.

ISO/TR 15801 was prepared by Technical Committee ISO/TC 171, *Document management applications*, Subcommittee SC 3, *General issues*.

This second edition cancels and replaces the first edition (ISO/TR 15801:2004) which has been technically revised.

Introduction

This Technical Report 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.

Information, in the form of digital objects, originates from many sources. This Technical Report covers digital objects 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.

Users of this Technical Report should be aware that the implementation of these recommendations does not automatically ensure acceptability of the evidence encapsulated by the information. Where stored electronic information might be required in court, implementers of this Technical Report are advised to seek legal advice to ascertain the precise situation within their relevant legal environment.

This Technical Report describes means by which it can be demonstrated, at any time, that the contents of a specific electronic object created or existing within a computer system have 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 system can be reliably reproduced in a consistent manner and accurately reflects what was originally stored without any material modification.

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

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

Readers are advised to use this Technical Report in conjunction with other local sources, particularly with relevance to governmental and legal requirements in their respective jurisdictions.

Document management — Information stored electronically — Recommendations for trustworthiness and reliability

1 Scope

This Technical Report describes the implementation and operation of document management systems that can be considered to store electronic information in a trustworthy and reliable manner.

This Technical Report is for use by any organization that uses a document management system to store authentic, reliable and usable/readable electronic information over time. Such systems incorporate policies, procedures, technology and audit requirements that ensure that the integrity of the electronic information is maintained during storage.

This Technical Report does not cover processes used to evaluate whether information can be considered to be authentic prior to it being stored or imported into the system. However, it can be used to demonstrate that, once the information is stored, output from the system will be a true and accurate reproduction of the original.

Where, in this Technical Report, the term “system” is used, it should be taken as meaning the document management system that is being reviewed, unless otherwise stated.

2 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12651 and the following apply.

2.1
information type
groups of related documents

NOTE In specific applications, “groups” can be identified as “sets”, “files”, “collections” or other similar terms.

EXAMPLES Invoices, financial documents, data sheets, correspondence.

2.2
trusted system
〈document management〉 system used to store electronic information in an accurate, reliable and usable/readable manner, ensuring integrity over time

3 Document management policy

3.1 General

Information is one of the most important assets that any organization has at its disposal. Everything an organization does involves using information in some way. The quantity of information can be vast, and there are many different ways of representing and storing it. The value of information used and the manner in which it is applied and moved within and between organizations can determine the success or failure of those organizations.

Information, like any other asset, needs to be classified, structured, validated, valued, secured, monitored, measured and managed efficiently and effectively.

This clause describes documentation that states the organization's policy for the management of information. Additionally, this clause provides guidance to organizations with respect to the level of documentation required to enable an organization to clearly establish how the information contained in a trusted document management system is reliable, accurate and trustworthy. Availability of this documentation can also be used to demonstrate that document management is part of normal business procedures.

Where a system stores information that can be used as evidence in any legal or business process, one's legal advisors should be consulted (see 4.4) to ensure that one complies with relevant legal or regulatory requirements. As legal and regulatory requirements vary from country to country (and sometimes within a country), the legal advice one obtains should cover all relevant jurisdictions.

3.2 Document Management Policy Document

3.2.1 Contents

A Document Management Policy Document (the Policy Document) should be produced, documenting the organization's policy on document management and storage, as applicable to the trusted document management system.

The Policy Document should contain sections which:

- specify what information is covered (see 3.2.2);
- state policy regarding storage media (see 3.2.3);
- state policy regarding electronic object file formats and version control (see 3.2.4);
- state policy regarding relevant document management standards (see 3.2.5);
- define retention and destruction policies (see 3.2.6);
- define responsibilities for document management functions (see 3.2.7);
- define responsibilities for monitoring compliance with this policy (see 3.2.8).

The Policy Document should be approved by senior management of the organization, and should be reviewed at regular intervals.

Essential to this Technical Report is the agreement and implementation of a Retention Schedule for stored information. Where reference is made to the Policy Document in the rest of this Technical Report, the Retention Schedule is included in such a reference.

3.2.2 Information covered

In order to define the organization's document management policy, information should be grouped into types, the policy for all information within a type being consistent. For example, information types can be specified either by reference to application (e.g. financial projections, invoices, customer address list), by association with a specific business process (e.g. applications, complaints, renewals) or by reference to generic groups (e.g. accounting data, customer documents, manufacturing documents).

During the drafting of the Policy Document, specific information might need to be regrouped to ensure consistency of Policy within an information type.

The Policy Document should list all types of information that are to be stored. The Policy Document should include, as an information type, all documents produced in compliance with the Policy.

3.2.3 Storage media

Different types of media have different long-term storage characteristics. Most organizations will store information on a variety of media types: paper, microform, electronic (write-once and rewritable/erasable) or optical (write-once and rewritable/erasable). In some applications, specific pieces of information can, throughout their retention period, be stored on different media types at different times.

The organization should have policies regarding the use of specific types of media for different information storage requirements (e.g. access requirements, retention periods and security requirements). These policies should be detailed in the Policy Document.

The media type on which each information type (see 3.2.2) can be stored should be specified.

Where copies of electronic objects exist, it might be important to be able to demonstrate that no changes have occurred to any purported copy. In the case of electronic objects that exist in different versions, for the purposes of this Technical Report each version should be treated as a new source or original object.

The policy for the management of copies of electronic objects should be detailed in the Policy Document.

3.2.4 Data file formats and compression

The Policy Document should contain details of the approved data file formats that can be used for each information type.

All information stored on a computer system requires software for retrieval and display. This software is subject to change, either by the implementation of new releases, or by changes to operating systems and/or hardware. By implementing a policy of approved data file formats and compression technologies (where utilized), the necessary data migration or alternative procedures can be implemented satisfactorily to ensure long-term retrieval of the stored information.

Where compression techniques are available, policy on their use should be documented.

Where multiple versions of a document can be stored, a policy is required which ensures that all relevant versions are stored, and their relationship maintained. The Policy Document should contain details of policy on the storage of versions of documents.

For additional information on this, see 5.5.2, 5.10, 6.10 and 7.2.3.

3.2.5 Standards related to document management

Where the organization operates a quality management system (such as the ISO 9000 series), whose scope includes part or all of the trusted document management system, all relevant procedural documentation should be included in the quality system.

Where national or international regulatory requirements are mandatory, or where national or International Standards are applicable, they should be complied with.

3.2.6 Retention and disposal schedules

A retention schedule should be established for each information type.

Retention periods should be agreed by all relevant departments and personnel within the organization.

Retention periods should be agreed upon after taking relevant advice to ensure that legal or regulatory issues, or both, are resolved.

All relevant system and procedural documentation that is produced should be covered by the retention schedule.

The retention schedule should include the organization's policy for its periodic review.

The retention schedule should include the organization's policy for the controlled destruction of information.

3.2.7 Document management responsibilities

Individual or job function responsibilities for the Policy Document should be defined in the Policy Document.

Individual or job function responsibilities for each information type should be identified and included in the Policy Document.

Individual or job function responsibilities should include the need to seek relevant advice when creating or updating the contents of the Policy Document.

3.2.8 Compliance with policy

Where it is important that compliance with the Policy Document can be demonstrated, the individual or job function responsibilities for obtaining and maintaining such compliance should be identified and defined.

4 Duty of care

4.1 General

4.1.1 Trusted system

A trusted document management system is one that ensures that all electronically stored information can be considered to be a true and accurate copy of the original information, regardless of the original format. Trusted document management systems need to include the following as a minimum:

- the creation of at least one copy of the stored information on to media that protects the stored information from modification, inappropriate additions or deletion throughout its approved lifecycle; this copy needs to be stored and maintained in a safe location that is separate from the other copy of the stored information;
- the utilization of hardware and storage media that protect the stored information from modification, inappropriate additions or deletion throughout its approved lifecycle (see also 6.3);
- the ability to verify through independent audit processes of the software, hardware and/or storage media methodology(ies) that the original stored information can be rendered accurately throughout its approved lifecycle.

A trusted document management system utilizes a combination of organizational policies, operational procedures and appropriately installed and managed technologies as described in this Technical Report that will enable an organization to demonstrate trustworthiness and reliability.

4.1.2 Controls

It is essential that the organization be aware of the importance of designing and maintaining all aspects of the trusted document management system and that it execute its responsibilities under the duty of care principle.

To fulfil this objective, the organization needs to:

- establish a chain of accountability and assign responsibility for activities involving management of electronic information at all levels;
- be aware of legislative and regulatory bodies pertinent to its business;

- keep abreast of technical, procedural, regulatory and legislative developments by maintaining contact with the appropriate bodies and organizations;

- implement an Information Security Policy.

4.1.3 Segregation of roles

The segregation of roles is a fundamental aspect of duty of care. It provides a check on errors and on the deliberate falsification of records (in this respect separation of roles is particularly important in systems where there is risk of fraud or other malicious action).

There are several aspects of document management where a segregation of roles is considered:

- input reconciliation (see 5.4.3);

- quality control (see 5.4.6);

- data entry (see 5.6);

- information deletion (see 5.11);

- information security (see 4.2).

It is also important to ensure that the physical and managerial segregations that exist around a system are mirrored by the logical access controls within it.

The segregation of roles between initial operations and checking should be reviewed and implemented where appropriate.

4.2 Information security management

4.2.1 Information Security Policy

All information, irrespective of the media on which it is stored, is vulnerable to loss or change, whether accidental or malicious. To protect information stored electronically, security measures need to be developed and implemented to reduce the risk of a successful challenge to its authenticity. These security measures need to be aligned to any information classification categories that are used.

Traditionally, information security is considered a matter of confidentiality, to ensure that information is not accessible outside the requirements of the organization. However, whilst this is important (in some cases vital) to the operation of the organization, it is not the most important security issue relevant to this Technical Report.

A key objective of the Information Security Policy is to ensure the protection of the integrity of stored information. When developing security measures, it is necessary to compare the risk of integrity being compromised with the cost of implementation of such measures. Security measures need to include backup and other copies of stored information, as their integrity is of importance in circumstances where they have been used as replacements for live data.

Also of importance is availability. In some cases, it might be necessary to be able to demonstrate that all information on a specific topic is available for review at any time. In this category, topics such as indexing accuracy and business continuity planning are key.

Security is not singularly a concern of computer systems. Security and availability of the operating environment (including buildings, temperature controls, network links, etc.) and the auditable implementation of procedures by all staff are both key elements.