

INTERNATIONAL
STANDARD

ISO/IEC
27038

First edition
2014-03-15

**Information technology — Security
techniques — Specification for digital
redaction**

*Technologies de l'information — Techniques de sécurité —
Spécifications pour la rédaction numérique*

Reference number
ISO/IEC 27038:2014(E)



© ISO/IEC 2014



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2014

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
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	iv
Introduction	v
1 Scope	1
2 Terms and definitions	1
3 Symbols and abbreviated terms	2
4 General principles of digital redaction	2
4.1 Introduction.....	2
4.2 Anonymization.....	2
5 Requirements	2
5.1 Overview.....	2
5.2 Redaction principles.....	3
6 Redaction processes	4
6.1 Introduction.....	4
6.2 Paper intermediaries.....	4
6.3 Digital image intermediaries.....	4
6.4 Simple digital redaction.....	4
6.5 Complex digital redaction.....	5
6.6 Contextual information.....	5
7 Keeping records of redaction work	6
8 Characteristics of software redaction tools	6
9 Requirements for redaction testing	7
Annex A (informative) Redacting of PDF documents	9

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27038 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

Some documents can contain information that must not be disclosed to some communities. Modified documents can be released to these communities after an appropriate processing of the original document. This processing can include the removal of sections, paragraphs or sentences with, where appropriate, the mention that they have been removed. This process is called the “redaction” of the document.

The digital redaction of documents is a relatively new area of document management practice, raising unique issues and potential risks. Where digital documents are redacted, removed information must not be recoverable. Hence, care needs to be taken so that redacted information is permanently removed from the digital document (e.g. it must not be simply hidden within nondisplayable portions of the document).

This International Standard specifies methods for digital redaction of digital documents.

Redaction can also involve the removal of document metadata or the removal of some information (e.g. an image) imported into the document.

It can be possible to identify redacted information in a redacted digital document by context. For example, the length of the redaction replacement text can indicate the length of the redacted information, and thus the information itself. This International Standard introduces two levels of redaction:

- BASIC redaction where context is not taken into consideration;
- ENHANCED redaction where context is taken into consideration.

Redaction techniques can be used for the anonymization of the information in a document, for example by the removal of some names within sentences. It can also involve the removal of numbers within sentences and their replacement by “XXX”.

Information technology — Security techniques — Specification for digital redaction

1 Scope

This International Standard specifies characteristics of techniques for performing digital redaction on digital documents. This International Standard also specifies requirements for software redaction tools and methods of testing that digital redaction has been securely completed.

This International Standard does not include the redaction of information from databases.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1

anonymization

process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

[SOURCE: ISO/IEC 29100:2011, definition 2.2]

2.2

document

recorded information which can be treated as a unit

Note 1 to entry: Documents can contain text, pictures, video and audio content, metadata and other associated content.

2.3

personally identifiable information

PII

any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

Note 1 to entry: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

[SOURCE: ISO/IEC 29100:2011, definition 2.9]

2.4

redaction

permanent removal of information within a document

2.5

reviewer

individual(s) who assesses a document for redaction requirements

Note 1 to entry: There could be a series of individuals who assess a particular document.