AS ISO 15801—2006
ISO/TR 15801:2004

AS ISO 15801—2006

Australian Standard®

Electronic imaging—Information stored electronically—Recommendations for trustworthiness and reliability

This Australian Standard® was prepared by Committee IT-021, Records Management Systems. It was approved on behalf of the Council of Standards Australia on 29 September 2006.
This Standard was published on 24 October 2006.

The following are represented on Committee IT-021:

- Australian Society of Archivists
- Department of Defence (Australia)
- Queensland State Archives
- Department of Foreign Affairs and Trade
- Institute for Information Management
- Monash University
- National Archives of Australia
- Public Record Office Victoria
- Records Management Association of Australasia
- State Records (New South Wales)
- The Institute of Internal Auditors - Australia

Additional Interests:

- Enterprise Knowledge
- BHP Billiton
- Recordkeeping Systems
- Sutherland Shire Council
- The University of Sydney
- NSW Department of Commerce
- Information Management Solutions
- Attorney General's Department
- AMS Imaging
- National Archives New Zealand

This Standard was issued in draft form for comment as DR 06020.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting **www.standards.org.au**

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at **mail@standards.org.au**, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Electronic imaging—Information stored electronically—Recommendations for trustworthiness and reliability

First published as AS ISO 15801—2006.

Published by Standards Australia, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 7797 X

PREFACE

This Standard was prepared by the Standards Australia Committee IT-021, Records Management Systems.

Apart from the addition of this preface, this Australian Standard is identical with and has been reproduced from ISO/TR 15801:2004, *Electronic imaging—Information stored electronically—Recommendations for trustworthiness and reliability*.

The objective of this Standard is to provide guidance on establishing processes and policies to enable the authenticity of digital records to be established.

Standards Australia wishes to thank the following organizations for their contribution enabling Australia's participation in the development of International Standards in the area of Records Management. International Standards in turn become national standards to be used in Australian industries.

Australian Society of Archivists

National Archives of Australasia

Public Record Office Victoria

Records Management Association of Australasia

Record Solutions

State Records NSW

The guidance in this Standard is applicable within the Australian recordkeeping context though some terminology may be different. To enable maximum use of this Standard for recordkeeping purposes the first paragraph in the introduction sets out the notion that 'information that has been created, captured and stored electronically is used as evidence of business activities'. This can be read as a reference to records management processes requiring explicit and managed links between the object being managed and the business context of creation, management and use. That object, in records management, is usually an aggregation of linked documents (e.g. a file, folder, in-box, out-box, or series) brought together during the conduct of business and requiring continuing management to maintain its evidential qualities.

As this Standard is reproduced from an international standard, the following applies:

(a) Its number appears on the cover and title page while the international standard number appears only on the cover.

(b) In the source text 'this Technical Report' should read 'this Australian Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian Standard*	
ISO		AS/NZS ISO	
9000 (all parts)	Quality management and quality assurance standards	9000	Quality management systems—Fundamentals and vocabulary
		9001	Quality management systems—Requirements
		9004	Quality management systems—Guidelines for performance improvements

ISO/TR 12037	Electronic imaging—Recommendations for the expungement of information recorded on write-once optical media	HB 179	Electronic imaging—Recommendations for the expungement of information recorded on write-once optical media

Only international references that have been adopted as Australian Standards have been listed.

CONTENTS

Page

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Information management policy 2
4.1 General 2
4.2 Information Management Policy Document 2
4.2.1 Contents 2
4.2.2 Information covered 3
4.2.3 Storage media 3
4.2.4 Image file formats 3
4.2.5 Standards related to information management 4
4.2.6 Retention schedule 4
4.2.7 Information management responsibilities 4
4.2.8 Compliance with policy 4

5 Duty of care 4
5.1 General 4
5.1.1 Controls 4
5.1.2 Separation of roles 5
5.2 Information security management 5
5.2.1 Information Security Policy 5
5.2.2 Risk assessment 6
5.2.3 Information security infrastructure 6
5.3 Business continuity planning 7
5.4 Consultations 7

6 Procedures and processes 8
6.1 General 8
6.2 Procedures Manual 8
6.2.1 Documentation 8
6.2.2 Content 8
6.2.3 Compliance with procedures 9
6.2.4 Updating and reviews 9
6.3 Document image capture 9
6.4 Document scanning procedures 10
6.4.1 General 10
6.4.2 Preparation of paper documents 10
6.4.3 Document batching 11
6.4.4 Photocopying 11
6.4.5 Scanning processes 12
6.4.6 Quality control 13
6.4.7 Rescanning 15
6.4.8 Image processing 15
6.5 Data capture 15
6.5.1 New data 15
6.5.2 Migration 16
6.6 Indexing 16
6.6.1 General 16
6.6.2 Manual indexing 16

Page

6.6.3 Automatic indexing 16
6.6.4 Index storage 16
6.6.5 Index amendments 17
6.6.6 Index accuracy 17
6.7 Authenticated output procedures 17
6.8 File transmission 18
6.8.1 Intra-system data file transfer 18
6.8.2 External transmission of files 18
6.9 Document retention 19
6.10 Information destruction 20
6.11 Backup and system recovery 20
6.12 System maintenance 21
6.12.1 General 21
6.12.2 Scanning systems 21
6.13 Security and protection 21
6.13.1 Security procedures 21
6.13.2 Encryption keys and digital signatures 22
6.14 Use of contracted services 22
6.14.1 General 22
6.14.2 Procedural considerations 23
6.14.3 Transportation of documents 24
6.14.4 Use of trusted remote archives 24
6.15 Workflow 24
6.16 Date and time stamps 25
6.17 Version control 25
6.17.1 Information 25
6.17.2 Documentation 25
6.17.3 Procedures and processes 26
6.18 Maintenance of documentation 26

7 Enabling technologies 26
7.1 General 26
7.2 System Description Manual 27
7.3 Storage media and sub-system considerations 27
7.4 Access levels 28
7.5 System integrity checks 28
7.5.1 General 28
7.5.2 Digital and electronic signatures (including biometric signatures) 29
7.6 Image processing 29
7.7 Compression techniques 30
7.8 Form overlays and form removal 31
7.9 Environmental considerations 31
7.10 Migration 32
7.11 Information deletion and/or expungement 32

8 Audit trails 32
8.1 General 32
8.1.1 Audit trail data 32
8.1.2 Creation 33
8.1.3 Date and time 33
8.1.4 Storage 34
8.1.5 Access 34
8.1.6 Security and protection 34
8.2 System 35
8.2.1 General 35
8.2.2 Audit trail information 35
8.2.3 Migration and conversion 35
8.3 Stored information 35
8.3.1 General 35
8.3.2 Information capture 36
8.3.3 Batch information 37

Page

8.3.4 Indexing **37**
8.3.5 Change control **38**
8.3.6 Digital signatures **38**
8.3.7 Destruction of information **38**
8.3.8 Workflow **38**

Bibliography **39**

INTRODUCTION

Increasingly, information that has been created, captured and stored electronically is used as evidence of business activities. Such evidence might be required in contract discussions, or in courts of law. This Technical Report defines recommended practices for electronic storage of business or other information in image form. As such, complying with its recommendations is of value to organizations even when the trustworthiness of the stored information is not being challenged.

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 may 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 may be demonstrated, at any time, that the contents of a specific electronic image file created or existing within a computer system have not changed since it was created within the system or imported into it. Where such a data file contains a digitized image of a physical source document, it will be possible to demonstrate that the digitized image is a true facsimile of that source document. The issue being addressed is essentially one of authentication.

Other versions of the information may legitimately develop; e.g. revision of a contract. In these cases the new versions are treated as new image files.

The same principle can be applied when a significant change is made to a document in a workflow environment.

This Technical Report describes procedures whereby an electronic copy may be demonstrated to be a true copy of the original, whether that original was itself an electronic data file or a physical source document.

The recommendations in this Technical Report are a mixture of items that are broad and general and items that are specific and detailed. 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.

Organizations that implement most of the recommendations described in this Technical Report will be in a good position to be able to demonstrate authenticity. However, there may be good economic reasons where a particular recommendation is not implemented. In such situations, the risk taken by such non-implementation decisions should be assessed.

NOTES

AUSTRALIAN STANDARD

Electronic imaging — Information stored electronically — Recommendations for trustworthiness and reliability

1 Scope

This Technical Report describes the implementation and operation of information management systems which store information electronically and where the issues of trustworthiness, reliability, authenticity and integrity are important. The whole life cycle of a stored electronic document is covered, from initial capture to eventual destruction.

This Technical Report is for use with any information management system, including traditional document imaging, workflow and COLD/ERM technologies, and using any type of electronic storage medium including WORM and rewritable technologies.

Image files may potentially contain any type of data: for example, correspondence, forms, drawings. This Technical Report covers all such image files, whether created and/or imported directly or through a network, from the time at which the system assumes control of the image file.

This Technical Report does not cover processes used to evaluate the authenticity of information prior to it being stored or imported into the system. However, it can be used to demonstrate that output from the system is a true reproduction of the original document.

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

2 Normative references

The following referenced documents are indispensable for the application 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 9000 (all parts), *Quality management and quality assurance standards*

ISO/TR 12037:1998, *Electronic imaging — Recommendations for the expungement of information recorded on write-once optical media*

ISO 12651:1999, *Electronic imaging — Vocabulary*

ISO 12653-2:2000, *Electronic imaging — Test target for the black-and-white scanning of office documents — Part 2: Method of use*