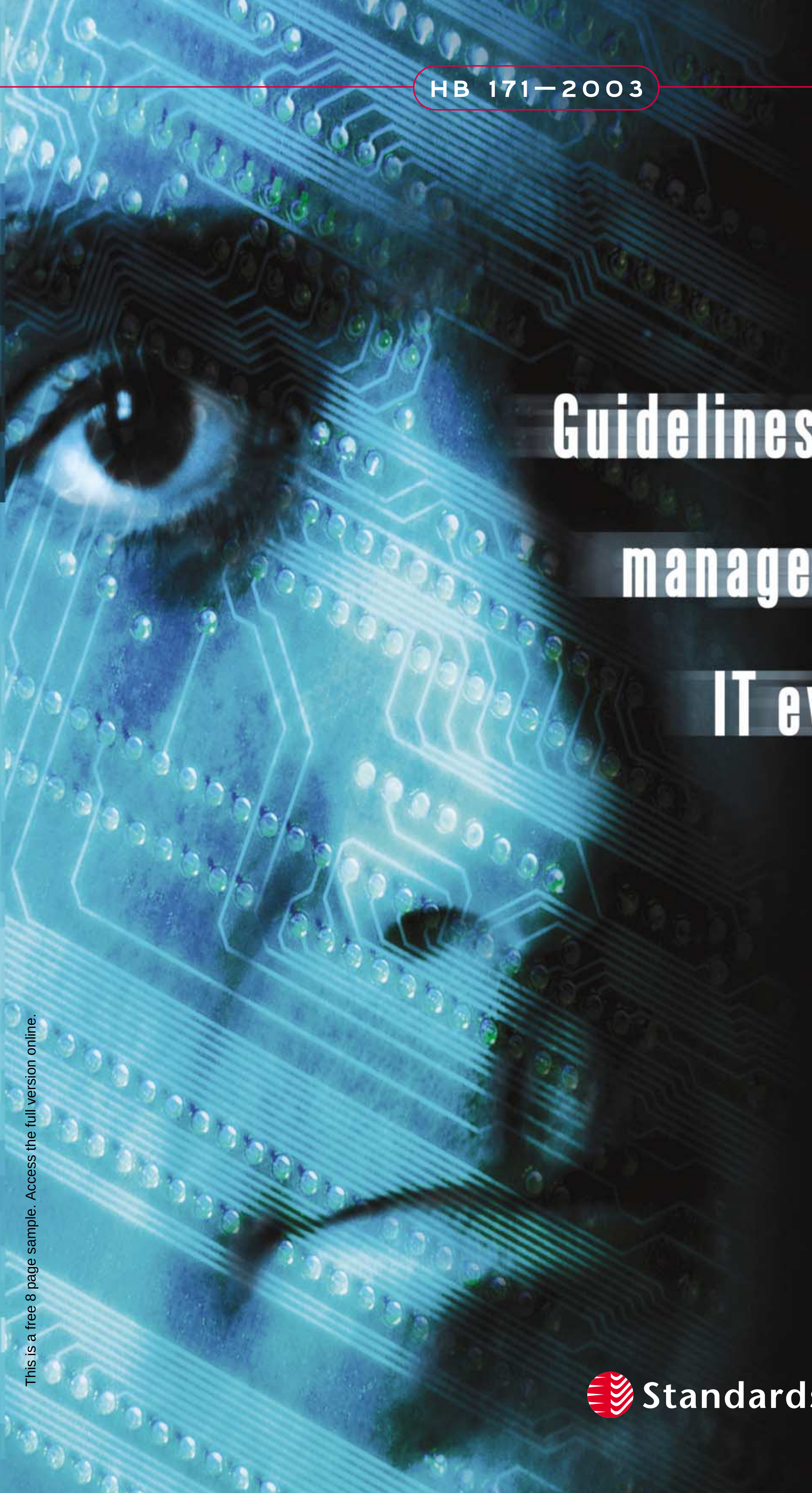
HB 171—2003



Guidelines for the management of IT evidence

Standards Australia

Handbook

Guidelines for the management of IT evidence

First published as HB 171—2003.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 2795 6

This page is intentionally left blank

Preface

This handbook has been prepared by Committee IT/012, Information Systems, Security and Identification Technology. It is intended for use as a reference document by a variety of audiences, including—

a) executives and Boards responsible for ensuring the existence of records that can be used in protecting the interests of their organization by initiating or defending legal proceedings or in their fulfilling a social responsibility as a witness;

b) personnel who are responsible for designing/acquiring information technology systems that produce and/or store records and the staff responsible for their use and operation;

c) personnel conducting an investigation or enquiry involving electronic records; and

d) adjudicators who base their decision, at least partially on IT evidence (e.g. judiciary, tribunal members, administrative management).

The authors recognize the cross-disciplinary nature of the management of IT evidence, involving as it does business, legal and information technology professionals. As far as possible, the handbook has been written in "plain English" minimizing both legal and technical jargon.

Qualification

This handbook does not purport to provide legal advice. Compliance with this handbook does not guarantee the legal admissibility of electronic records—it is a statement of best practice.

Organizations are encouraged to seek both legal and other expert advice when implementing information technology systems that create, store, process or transmit documents of significant evidentiary value.

Acknowledgements

Standards Australia would like to acknowledge Ajoy Ghosh's efforts in drafting this handbook, authorship of which was sponsored jointly by the Commonwealth Attorney-General's Department and the Australian Federal Police.

The following organizations have contributed to the writing of this handbook:

AusCERT

Australian Federal Police

Australasian Centre for Policing Research

Australian Prudential Regulation Authority

Australian Securities and Investment Commission

Australian Taxation Office

Action Group on E-Commerce

Commonwealth Attorney-General's Department

Deacons

Defence Signals Directorate

Standards Australia sub-committee IT/012/04 (Security Techniques)

Contents

APPENDICES

1 Introduction

1.1 General

Organizations are increasingly reliant on information communications technology (ICT) as a crucial component of operations. However, commentators have noted the apparent ease at which the complexities of the Internet and electronic records can be grossly oversimplified in judicial, commercial and academic contexts[1]. As a result, information is often, partially or otherwise, in electronic form.

ICT brings potentially increased (or at least different) risks in terms of civil or criminal wrongdoing and organizations need to be able to protect themselves against those risks. Failure to do so raises governance and accountability issues for which the management of the organization could be held responsible.

Many business decisions/actions are open to litigation or could involve official investigation e.g. contract disputes, employment issues, fraud, computer intrusion and copyright breaches.

Records maintained on information systems increasingly govern our everyday business decisions/actions – decisions/actions that are open to litigation or could involve official investigation e.g. contract disputes, employment issues, fraud, computer intrusion and copyright breaches. Organizations must be able to vouch for the reliability of the records upon which such decisions are made, or actions taken. This is particularly so for safety critical records e.g. health records upon which medical practitioners rely to know which leg to amputate (the patient is anaesthetized and can't say) or which medication to prescribe. Organizations need to be able to initiate or defend litigation or be in a position to refer matters to the authorities where appropriate. Alternatively, organizations may be required to give evidence in proceedings in which they are not parties. To do so, relevant information held by an organization must be in a form that can be used as evidence if required.

1.2 Purpose

This handbook aims to provide guidance on the management of electronic records that may be used as evidence in judicial or administrative proceedings, whether as a plaintiff, defendant, or witness. It will also be useful where suspect criminal activity is to be referred to appropriate authorities for investigation.

By complying with this benchmark, organizations can make investment decisions and implement them with confidence that records created, stored, processed or transmitted electronically will be of evidentiary value.

[1] Lim, Y *Cyberspace Law: Commentary and materials*, Oxford University Press, Melbourne, (2002) pg 51.