

Australian Standard[®]

Closed circuit television (CCTV)

Part 1: Management and operation



This Australian Standard® was prepared by Committee EL-051, Non-Broadcast Television. It was approved on behalf of the Council of Standards Australia on 19 May 2006. This Standard was published on 29 June 2006.

The following are represented on Committee EL-051:

- Australasian Railway Association
 - Australian Communications and Media Authority
 - Australian Federal Police
 - Australian Security Industry Association
 - Engineers Australia
 - National Security Association of Australia
 - Society of Motion Picture and Television Engineers
-

This Standard was issued in draft form for comment as DR 05405.

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Standards may also be withdrawn.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.

STANDARDS AUSTRALIA

RECONFIRMATION

OF

AS 4806.1—2006

Closed circuit television (CCTV)

Part 1: Management and operation

RECONFIRMATION NOTICE

Technical Committee EL-051 has reviewed the content of this publication and in accordance with Standards Australia procedures for reconfirmation, it has been determined that the publication is still valid and does not require change.

Reconfirmed documents cannot be amended, but may be formally revised and a new edition published.

Certain documents referenced in the publication may have been amended since the original date of publication. Users are advised to ensure that they are using the latest versions of such documents as appropriate, unless advised otherwise in this Reconfirmation Notice.

Approved for reconfirmation in accordance with Standards Australia procedures for reconfirmation on 12 May 2015.

Reconfirmed documents cannot be amended, but may be formally revised and a new edition published.

The following are represented on Technical Committee EL-051:

Attorney General's Department (Australian Government)
Australian Federal Police
Transport for NSW

NOTES

Australian Standard[®]

Closed circuit television (CCTV)

Part 1: Management and operation

First published as AS 4806.1—2006.

COPYRIGHT

© Standards Australia

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

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

ISBN 0 7337 7565 9

PREFACE

This Standard was prepared by the Standards Australia Committee EL-031, Intruder Alarm Equipment and Installations.

The objective of this Standard is to present a set of principles for the management and operation of closed circuit television (CCTV) systems for reference by users, manufacturers, tenants of premises with CCTV systems installed and regulators.

The term ‘informative’ has been used in this Standard to define the application of the appendix to which it applies. An ‘informative’ appendix is only for information and guidance.

CONTENTS

	<i>Page</i>
FOREWORD.....	4
1 SCOPE AND GENERAL	5
2 PRINCIPLES AND MANAGEMENT OF THE CCTV SYSTEM.....	7
3 PROCEDURES.....	9
4 PERSONNEL	15
5 CCTV CONTROL ROOM.....	16
6 EFFECTIVE RESPONSE	16
7 PRIVACY AND DISCLOSURE ISSUES.....	18
8 RECORDED MATERIAL MANAGEMENT	21
9 DOCUMENTATION	24
10 LICENCES	25
11 SIGNAGE.....	25
APPENDICES	
A SUMMARY OF LEGISLATION	26
B STAFF RECRUITMENT AND SELECTION.....	28

FOREWORD

All closed circuit television (CCTV) systems that receive, hold or process data about a known person are obliged to conform to certain legislation, such as Federal, State and Territory Privacy and Surveillance Legislation. This Standard is designed to supplement that legislation in a model that ensures fairness, purpose and accountability within the Australian CCTV industry.

Irrespective of the ownership, this Standard covers CCTV systems used in areas where the public would have a ‘right to visit’. These include, but are not limited to—

- (a) a place that is in private ownership, but where the public perceives no boundary;
- (b) a place where a public service is offered;
- (c) public footpaths, roads, etc.;
- (d) educational establishments, hospitals; and
- (e) sportsgrounds, supermarkets, housing areas.

CCTV applications within government may require extra consideration in regard to the security of the system installed, the operation of such and the data they contain and transmit. The methods by which data is stored, destroyed and disposed of and the re-use of media are other issues that may need to be addressed in certain instances.

Any CCTV application within a government department or an organization contracting to it should be designed, implemented and operated in full consultation with the relevant government agency security adviser.

This Standard aims to provide good practice to assist owners in obtaining reliable information that may be used as evidence. Compliance with this Standard is strongly recommended, particularly where CCTV systems include an element of observation of the public.

This Standard also aims to provide pointers and references to assist owners and installers in verifying whether the installation and service has been carried out to an acceptable standard.

Because there is separate Federal, State and Territory Privacy and Surveillance Legislation in Australia it is the owners’ and their advisers’ responsibility to make themselves fully aware of the Privacy and Surveillance Legislation that applies to their State or Territory in relation to CCTV systems.

STANDARDS AUSTRALIA

Australian Standard

Closed circuit television (CCTV)

Part 1: Management and operation

1 SCOPE AND GENERAL

1.1 Scope

This Standard provides recommendations for the operation and management of closed circuit television (CCTV) within a controlled environment, where data that may be offered as evidence is received, stored, reviewed or analysed.

This Standard is applicable to CCTV systems used in public places (i.e., areas where the public is encouraged to enter or have a right to visit, such as town centres, shopping malls, public transport, health, etc.) systems that overlook a public place (such as traffic monitoring systems) and systems where a camera view adjoins a public place. The Standard also provides good practice guidelines for all other CCTV systems.

Clauses on management of data, etc., are applicable to the storage of recorded images/data from CCTV systems.

NOTES:

- 1 Throughout this Standard the statement Federal, State and Territory Privacy and Surveillance Legislation means all Privacy and Surveillance Legislation applicable to the particular State or of the Territory of the installation. See Appendix A for a summary of some current Australian Privacy and Surveillance Legislation.
- 2 Some Australian States and Territories have Government Guidelines for CCTV systems in public places, which may also be a requirement for the implementation of a CCTV system in public places in some States and Territories.

1.2 Referenced documents

The following documents are referred to in this Standard:

AS

- 2342 Development, testing and implementation of information and safety symbols and symbolic signs

AS/NZS

- 4806 Closed circuit television (CCTV)
4806.2 Part 2: Application guidelines

ISO

- 11064 Ergonomic design of control centres
11064-1 Part 1: Principles for the design of control centres
11064-2 Part 2: Principles for the arrangement of control suites
11064-3 Part 3: Control room layout

Federal and State Government Privacy and Surveillance Legislation

OH&S Acts and Regulations (States and Territories and Commonwealth for its own employees)

1.3 Definitions

For the purposes of this Standard the definitions given in AS/ZS 4806.2, and those below apply.

1.3.1 *CCTV control room*

Area in a building where CCTV data is monitored, retrieved and analysed.

1.3.2 *CCTV system*

- 1 Totality of arrangements for CCTV systems including, but not limited to, the technological system, staff and operational procedures.
- 2 Surveillance items comprising cameras and associated equipment for monitoring, transmission and controlling purposes, for use in a defined security zone.

NOTE: A whole system is not limited to equipment sited at one locality. It may include systems that use dial-in dial-out, remote transmission or decentralized control.

1.3.3 *Observation mode*

Mode of operation of a CCTV system whereby monitoring is carried out live, the sole purpose of which is to observe an operation in real time.

1.3.4 *Storage system*

CCTV system with the capability, in any medium, to effectively capture and store data that can later be retrieved, viewed or processed.

1.3.5 *Distributed system*

Subsystem, any part of which may be linked temporarily or permanently for remote monitoring within the CCTV system.

1.3.6 *Data*

All information, including that about a person.

NOTE: In CCTV systems, this includes pictures, sound and any other associated, linked or processed information.

1.3.7 *Incident*

Activity that raises cause for concern that an offence has been, is being, or is about to be, committed or that an occurrence has taken place warranting specific action.

1.3.8 *Owner*

Legal person or entity, agency or individual designated as having overall responsibility for the formulation and implementation of the policies, purposes and control of a CCTV system.

NOTE: The role of owner also includes all statutory responsibilities of the data controller, such as Federal, State and Territory Privacy and Surveillance Legislation. The owner may be a partnership, provided it has a formal constitution.

1.3.9 *Manager*

Person or persons designated, and trained to have, direct responsibility for the implementation of the policies, purposes and methods of control of a CCTV system, as defined by the owner of the system.

NOTE: This may include the role and responsibilities of 'data controller'.

1.3.10 *Supervisor*

Person trained and specifically designated and authorized by the owner of a system to ensure that the system is at all times operated in accordance with this Standard and any procedural instruction issued by the owner or manager.

NOTE: This may include the role and responsibilities of 'data controller' (see Note to Clause 1.3.9).

1.3.11 *Operator*

Person specifically designated and authorized by the owner of a CCTV system to carry out the physical operation of controlling that system.

NOTE: This may include the role and responsibilities of 'data controller' (see Note to Clause 1.3.9).

1.3.12 *Storage medium*

Any medium that has the capacity to store data on a more permanent basis, able to keep such data even when power is switched off and from which data can later be recalled.

1.3.13 *Recorded information*

Any data recorded on any recording medium (e.g., electronic, magnetic or optical) that contains information of events and camera views that have happened in the past.

1.3.14 *Hard copy (print)*

Paper copy of an image or images that already exist on the recorded material.

1.3.15 *Image authentication*

A means of providing proof that images presented as evidence have not been tampered with.

1.3.16 *Image verification*

A method of verifying images and associated data so that the origin, date and time can be used to support its credibility and acceptability in a legal process.

1.3.17 *Evidence quality*

Evidence is required to provide all the necessary elements that can legally stand up in court.

NOTE: Some of the elements that would be required are: acceptable and clear content, creation date, data and time stamp, proof of non-tamper and verification methodology.

1.3.18 *Clarity of image*

The technical 'quality' of the image represented in terms of resolution, noise, grey scale depth and colour.

1.3.19 *Image archive*

Images that are stored for long periods of time on long-term permanent, or partially permanent storage.

NOTE: For example CDs, DVDs or digital tape are considered to be 'archived'.

2 PRINCIPLES AND MANAGEMENT OF THE CCTV SYSTEM

2.1 Objectives

The objectives of the operation of a CCTV system should be documented in writing, clearly indicating intended uses.

Every reasonable effort should be made to ensure data is accurate and sufficient for the objectives and that it is not held for longer than necessary. Data that is to be destroyed should be destroyed under controlled conditions.

2.2 Policy

2.2.1 General

The operation of a CCTV system should have a written policy statement. This should identify the owners and details of how they may be contacted.

2.2.2 Purposes

The purposes and extent of any system, along with any changes or revisions to the policy, should be defined.

The following are some examples:

- (a) Availability of car parking relayed to local radio or the internet.
- (b) Traffic congestion reports, local radio, phone-in or answering service.
- (c) Public awareness, crime watch (vulnerable areas monitored more actively to allay public concern about safety and enable a swift response to incidents).
- (d) Improved staff safety.
- (e) Reduction in theft and shrinkage.

The purposes of the system should be appropriate; that is, the information should be relevant and the owner should have reasonable cause to hold the data.

NOTES:

- 1 The Federal, State and Territory Privacy and Surveillance Legislation may require that clearly visible signs be placed to identify areas where a CCTV system is operating.
- 2 Many CCTV systems have developed ancillary public information outputs that do not relate directly to an individual. The extended use of such systems is aimed at improving public information and confidence and does not compromise non-disclosure.
- 3 Recording sound in a public place may be covered by Federal, State and Territory Privacy and Surveillance Legislation.

2.2.3 Information availability

Members of the public or contracted customers should be able to obtain on request certain details of any system, including—

- (a) the name and official address of the owner of the system;
- (b) a contact point;
- (c) the objectives and policy of the system;
- (d) how to make a complaint; and
- (e) how to obtain a recorded footage copy of an incident or event that involved them.

2.2.4 Additional policies

The following policies should also be included:

- (a) A complaints policy.
- (b) A policy relating to the release of information to the public (see Clause 7.2).

NOTES:

- 1 See Clause 7.2 for disclosure of data.
- 2 This policy should provide safeguards relating to the security and integrity of the system while allowing the disclosure of recorded information to third parties who can show legitimate requirements for this information.