PAS 74:2008

PUBLICLY AVAILABLE SPECIFICATION

Internet safety – Access control systems for the protection of children online – Specification

ICS 35.040; 35.080

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

ISBN 978 0 580 49979 1

Amendments issued since publication

Amd. no.	Date	Text affected

Contents

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 33 and a back cover.

Foreword

This Publicly Available Specification (PAS) has been prepared by The British Standards Institution (BSI) in consultation with the Home Office and Ofcom and associated groups to provide a specification for access control systems for the protection of children online.

Acknowledgement is given to the following organizations that were involved in the development of this specification:

Becta

Borderware Technology

BSI Product Services

Child Exploitation and Online Protection Centre (CEOP)

Cyberpatrol from SurfControl

The Home Office

The Home Secretary's Task Force on Child Protection on the Internet

Intertek Research and Performance Testing

Microsoft

Mobile Broadband Group

NCH

Ofcom (Office of Communications)

The Children's Charities

In this Publicly Available Specification, the word ''shall'' indicates a requirement. The word ''should'' indicates a recommendation. Paragraphs marked ''NOTE'' are for guidance in understanding or clarifying the associated requirement.

This PAS has been prepared and published by BSI, which retains its ownership and copyright. BSI reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This Publicly Available Specification will be reviewed at intervals not exceeding two years and any amendments arising from the review will be published in an amended Publicly Available Specification and publicized in *Update Standards*. Feedback on this Publicly Available Specification and future work will be gratefully received. This specification is not intended to restrict new developments in design and materials.

This Publicly Available Specification is not to be regarded as a British Standard. It will be withdrawn if its content is published in, or as, a British Standard.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a Publicly Available Specification does not in itself confer immunity from legal obligations.

Introduction

The Home Secretary's Task Force for Child Protection on the Internet was created in 2001. Its aim is to make the UK the safest place in the world for children to use the Internet and to help protect children across the world from abuse fuelled by criminal misuse of new technologies. The Task Force brings together representatives from law enforcement agencies, child protection organizations, the Internet industry, Government and representatives from opposition parties.

The Task Force's work to date includes the development of models of good practice for providers of Internet chat, instant messaging, web-based services and search services, guidance on the moderation of interactive services, and is currently developing good practice guidance for providers of social networks and user-generated content services. The Task Force also contributed to the development of codes of practice for new forms of content on mobile phones and passive location services and worked on public awareness campaigns and guidance for young people, and their parents and carers, for using the Internet and related technologies safely. In addition to the above, the Task Force recommended the creation of the Child Exploitation and Online Protection Centre (CEOP).

Recognizing the role of parents and carers in developing a safe Internet environment, a subgroup of the Task Force was created in 2003 to specifically consider rating, filtering and monitoring products (access control systems) for use in the home.

At this time numerous commercial products were emerging, but there were concerns over their quality and effectiveness. Additionally, there was no permanent, independent source of evaluation for such products, meaning that parents/carers often faced difficulties in understanding the many issues, and in finding reliable products which met their requirements.

In 2004, the subgroup coordinated a short-term project to produce a guide for parents on available options for managing their children's use of the Internet. Longer-term aims included the development of a solution for keeping parents informed of the risks, and suitable products and services for managing them, which could also keep pace with technological changes. The subgroup decided to develop a third-party conformity certification scheme against which access control systems could be tested, providing impartial advice to parents on product features, capabilities, ease of use and confidence in their quality.

This Publicly Available Specification has been developed primarily for use by software developers working with access control systems. It sets out the minimum performance requirements for the access control systems to obtain a third-party conformity certification. An overview of the laboratory procedures is given in Annex A.

It must be recognized however, that no access control system can be effective 100% of the time and that, despite rigorous controls, there may still be occasions when inappropriate materials may be accessed. In such instances, providing education on the issues, and developing strategies for protecting themselves, is essential in helping children and young people become safe and discriminating users of Internet-based content and services.

This Publicly Available Specification is primarily aimed at the development of access control systems for use in the consumer market in the UK. It covers both those products installed locally (i.e. by a parent/carer on a home computer) and remotely managed products/services (i.e. those products or services offered by Internet Service Providers).

The development of this Publicly Available Specification has been jointly sponsored by the Home Office and Ofcom.

1 Scope

This Publicly Available Specification specifies requirements for products, services, tools and other systems that allow UK adult Internet users to easily control children's access to inappropriate Internet-based content and services.

It specifies requirements on:

a) ease of installation, configuration and use;

b) effectiveness;

c) minimum features;

d) ease of updating;

e) quality of instructions;

f) consumer communications and support.

By using a certified product or service, parents/carers will have confidence in the ability of the access control system to:

a) block inappropriate content (see Clause **4**);

b) block communications via Internet-based services that are inappropriate (see Clause **5**);

c) prevent unauthorized users from changing or disabling the access control settings (see Clause **6**);

d) provide an appropriate level of protection (as specified by this PAS) upon implementation/installation either through the use of default settings or configuration in accordance with user documentation (see Clause **7**);

e) configure the product or service where such a capability is offered (see Clause **8**);

f) remain up to date (within the terms of any licensing or subscription requirements) (see Clause **9**).

Furthermore, where the access control system can be installed, parents/carers will have confidence in their ability to uninstall/remove the product or service (see Clause **10**).

By using a certified product or service, parents/carers will:

a) have confidence in the ability to obtain suitable system support should they encounter problems with implementing, maintaining or installing/removing the access control system (see Clause **11**);

b) have confidence in the level and quality of information they will receive in the product description and user documentation provided with the product or service and will have confidence in the quality of the instructions to enable them to effectively install and configure the access control system to an effective level of protection (see Clause **12**);

c) have access to user education materials providing information and links to information that enable parents/carers and children to stay informed of the issues and risks of using the Internet (see Clause **13**).

2 Terms and definitions

For the purposes of this Publicly Available Specification, the following terms and definitions apply.

2.1 access control system
software product or service, including user documentation, designed to provide safeguards against inappropriate content and contact when using the Internet and/or related technologies through a process of filtering and blocking

NOTE Although this term is primarily used within this PAS to describe software used on a computer, access control systems can apply to any type of communications device providing access to Internet-based content and services, such as mobile phones, handheld devices and Internet-enabled games consoles.

2.2 blocking
prevention of access to content or services in its entirety (e.g. chat)

2.3 certification body
third-party body contracted to provide certification to a customer

2.4 chat
real time communication between two or more users over the Internet in virtual meeting places or chat rooms (see also **2.13**)

2.5 communication
any process where data (such as messages, files or administration information) is conveyed between computer systems

2.6 content
any material, such as text, images, sound, animation or video, which can be accessed or received using the Internet

2.7 email
system of sending messages (which may include text, images, sound, animation or video) over the Internet for immediate or later retrieval

2.8 end user
person who is protected by the access control system

NOTE It is anticipated that in most instances the end user will be a child, young person or vulnerable adult, but if the access control system or system software allows for multiple user accounts to be created it could be any person using the computer/device.

2.9 filtering
selective blocking of content (e.g. web pages) against specified criteria

2.10 hate material
material which promotes hatred and intolerance (see also **2.25** and **B.3**)

2.11 inappropriate content
material which, while not illegal, may not be considered suitable for a particular person

NOTE The content covered by this definition are listed in Annex B.

2.12 inexperienced user
person who has basic IT skills considered to include a basic knowledge of navigating an operating system, system desktop (user interface) and running productivity tools, but includes little to no experience of configuring system changes for both hardware and software

*NOTE It is assumed that the parent/carer is an inexperienced user (see **2.19**).*

2.13 instant message
collaborative messaging system which allows communication and sharing of files in real time over the Internet (see also chat), usually one-to-one

2.14 Internet
global interconnected network of networked computers, providing an infrastructure through which applications such as web browsing, email, chat and instant messaging operate

2.15 Internet Service Provider
provider of Internet services such as Internet connectivity and web site hosting

2.16 manufacturer
organization which develops the access control system

2.17 newsgroup
area categorized by its subject on Usenet, where users can post or read comments about that subject

2.18 overblocking
prevention of access to acceptable content as a result of the controls imposed by an access control system

2.19 parent/carer
person who authorizes the implementation and configuration of the access control system

NOTE 1 It is anticipated that in most instances the local administrator will be a parent (or other responsible adult) who wishes to provide access controls on a computer or other Internet-enabled device within the home setting.

*NOTE 2 It is assumed that the parent/carer is an inexperienced user (see **2.12**).*

2.20 post, posting
process of contributing to a forum or newsgroup or publishing comments or other material, typically on a website which is viewable by others

2.21 product description
readily accessible information stating the properties of the access control system

NOTE The product description can help potential consumers evaluate the suitability of the product before purchasing it.

2.22 product packaging
physical wrapping of a software product, or point of download for software products downloaded from the Internet

2.23 product/service type A
access control system providing default settings enabling parents/carers to provide defined levels of end user protection

2.24 product/service type B
access control system requiring full configuration of the access control settings thereby providing the parent/carer with the ability to configure access control system to provide user defined levels of end user protection

2.25 racist material
material which promotes hatred and intolerance on the basis of race (see also **2.10** and **B.3**)

2.26 software product
set of computer programs, procedures, and possibly associated documentation and data

2.27 system support provider
organization that provides technical support to consumers and parents/carers of the access control system

NOTE 1 This will not necessarily be the manufacturer of the product.

NOTE 2 System support may be provided via various means such as email, Internet-based forms, or telephone.

NOTE 3 It is not anticipated that end users seek support from system support providers.

2.28 system support
act of maintaining the access control system and its user documentation in a functional state

2.29 Usenet
collection of user-submitted notes, messages and binary files on various subjects that are posted to servers on a worldwide network

NOTE Users post to these newsgroups which are then distributed to other Usenet servers connected to the Internet.

2.30 user documentation
complete set of documents, available in print or electronic form, that provides information on the installation, configuration, use and maintenance of the access control system

2.31 user education material
material intended for use by both parents/carers and those for whom they are responsible that explains the purpose, function and limitations of access control systems

2.32 virus
program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down

2.33 web-based chat
system that allows two or more logged-in users to take part in a synchronous, text-based communication, typed in real-time, across the Internet

2.34 webcam
real time camera whose images can be accessed using Internet browser applications, instant messaging applications, video calling applications either continuously or at regular intervals dependent on application

2.35 web forum
online discussion group

NOTE Online services and bulletin board services provide a variety of forums, in which participants with common interests can exchange open messages.

3 Abbreviations

For the purposes of this PAS, the following abbreviations apply.

3.1 FAQs
Frequently Asked Questions

3.2 FTP
File Transfer Protocol

3.3 FTPS over SSL
Secure File Transfer Protocol with SSL security

3.4 HTTP
Hyper Text Transfer Protocol

3.5 IRC
Internet Relay Chat

3.6 P2P
Peer to Peer

3.7 PIN
Personal Identification Number

3.8 SSL
Secure Socket Layout

3.9 VoIP
Voice over Internet Protocol

4 Internet-based content

4.1 General

For purposes of compliance manufacturers shall apply the mandatory requirements applicable to their specific product/service type (see **4.2.1** and **4.2.2**).

*NOTE The criteria used for checking compliance for products and services offered for third-party conformity testing under Clause **4** are listed in Annex C.*

4.2 Mandatory requirements

4.2.1 Product/service type A – access control system providing default settings

For the purposes of compliance with PAS 74, **4.2.1** shall be supported by detailed user implementation/installation instructions to ensure the default settings of the access control system are implemented/installed in compliance with third-party conformity testing (see **12.2.3.2).**

4.2.1.1 As a default, the access control system shall block inappropriate content.

NOTE For the purposes of this PAS, this is deemed to be content as defined by the categories listed in Annex B.

4.2.1.2 The access control system shall not overblock access to appropriate Internet-based content.

NOTE For the purposes of this PAS, overblocking is defined by the tests outlined in Annex C.

4.2.1.3 The access control system shall provide parents/carers with the ability to access all Internet-based content.

NOTE This should not override any mandatory filtering of illegal Internet content provided by the Internet Service Provider (ISP).

4.2.1.4 The access control system shall allow parents/carers to completely block access to Internet-based content.

4.2.1.5 The access control system shall provide the parent/carer with the ability to apply the default settings of the access control system to specified user accounts.

4.2.2 Product/service type B – access control system requiring full configuration of settings

4.2.2.1 For the purposes of compliance with PAS 74, **4.2.2** shall be supported by detailed user installation/configuration instructions to ensure the access control system can be configured to an appropriate level of protection in compliance with third-party conformity testing (see **12.2.3.3**).

4.2.2.2 The access control system shall provide parents/carers with the ability to configure access control settings against specified system/device user accounts.

4.2.2.3 The access control system shall provide parents/carers with the ability to block inappropriate content.

NOTE For the purposes of this PAS, this is deemed to be content as defined by the categories listed in Annex B.

4.2.2.4 The access control system shall not overblock access to appropriate Internet-based content.

NOTE For the purposes of this PAS, overblocking is defined by the tests outlined in Annex C.

4.2.2.5 The access control system shall provide parents/carers with the ability to access all Internet-based content otherwise accessible through their Internet Service Provider.

NOTE This should not override any mandatory filtering of illegal Internet-based content provided by the Internet Service Provider (ISP).

4.2.2.6 The access control system shall provide parents/carers with the ability to completely block access to Internet-based content.

4.2.2.7 The access control system shall provide the parent/carer with the ability to configure the access control system to provide or deny access to Internet-based content following clear prompts and instructions as defined in Clause **12**.

5 Internet-based communications

5.1 General

For purposes of compliance manufacturers shall apply the mandatory requirements applicable to their specific product/service type (see **5.2.1** and **5.2.2**).

*NOTE The criteria used for checking compliance for products and services offered for third-party conformity testing under Clause **5** are listed in Annex D.*

5.2 Mandatory requirements

Where communication via Internet-based services is possible the following requirements shall be mandatory:

5.2.1 Product/service type A – access control system providing default settings

5.2.1.1 For the purposes of compliance with PAS 74, **5.2.1** shall be supported by detailed user implementation/installation instructions to ensure the default settings of the access control system are implemented/installed in compliance with third-party conformity testing (see **12.2.3.2**).

5.2.1.2 The access control system shall block inappropriate Internet-based communication services as defined in Annex E.

5.2.1.3 Where the access control system offers the ability to configure individual user accounts, parents/carers shall have the ability to apply the default settings of the access control system to specified accounts.

5.2.1.4 The update facility shall keep the access control system up to date with new programs and utilities offering the functions described in Annex E.

5.2.1.5 Where the access control system is installed and configured on a user device, e.g. a PC, the access control system shall not be required to control third-party appliances that provide access to functions as detailed in Annex E, e.g. a VoIP phone utilizing a direct wireless connection to a wireless router/modem bypassing the access control system on the user device.

5.2.2 Product/service type B – access control system requiring full configuration of settings

5.2.2.1 For the purposes of compliance with PAS 74, **5.2.2** shall be supported by detailed user installation/configuration instructions to ensure the access control system can be configured to an appropriate level in compliance with third-party conformity testing (see **12.2.3.3**).

5.2.2.2 The access control system shall provide parents/carers with the ability to configure access control settings against specified system/device user accounts.

5.2.2.3 The access control system shall provide parents/carers with the ability to block access to communications via Internet-based services that may be inappropriate.

NOTE For the purposes of this PAS, this is deemed to be the services listed in Annex E.

5.2.2.4 The access control system shall allow parents/carers to permit access to those communications via Internet-based services which they deem appropriate.

5.2.2.5 The facility within the access control system to provide automatic updates shall ensure that the access control system maintains the required levels of filtering/blocking across the categories of Internet-based communications as defined in Annex E.

5.2.2.6 The parent/carer shall be able to configure the access control system to provide or deny access to communications via Internet-based services following clear prompts and instructions as defined in Clause **12**.

5.2.2.7 Where the access control system is installed and configured on a user device, e.g. a PC, the access control system shall not be required to control third-party appliances that provide access to functions as detailed in Annex E, e.g. a VoIP phone utilizing a direct wireless connection to a wireless router/modem bypassing the access control system on the user device.

6 Security of settings

6.1 General

NOTE 1 For purposes of compliance, the mandatory requirements detailed below apply to both access control system product/service types A and B.

*NOTE 2 The criteria used for checking compliance for products and services offered for third-party conformity testing under Clause **6** are listed in Annex F.*

6.2 Mandatory requirements

6.2.1 The access control system shall be capable of preventing unauthorized users from changing or disabling the access control system, whether accidental or deliberate (e.g. by use of a password, PIN, or similar).

6.2.2 It shall not be possible to utilize functionality within the computer or device to remember or auto-enter passwords, PINs, etc. relating to the access control system.

7 Installation and implementation – including initial configuration

7.1 General

For purposes of compliance, manufacturers shall apply the mandatory requirements applicable to their specific product/service type (see **7.2.1** and **7.2.2**).

*NOTE 1 The criteria used for checking compliance for products and services offered for third-party conformity testing under Clause **7** are listed in Annex G.*

NOTE 2 A specification for the design and preparation of user documentation is given in BS ISO/IEC 18019 [1].

7.2 Mandatory requirements

7.2.1 Product/service type A – access control system providing default settings

7.2.1.1 The access control system shall, upon implementation/installation, provide the default level of protection (as specified by this PAS) through the use of default settings.

7.2.1.2 For the purposes of compliance with PAS 74, **7.2.1** shall be supported by detailed user implementation/installation instructions to ensure the default settings of the access control system are implemented/installed in compliance with third-party conformity testing (see **12.2.3.2**).

7.2.1.3 Where the access control system offers the ability to configure individual user accounts, parents/carers shall have the ability to apply the default settings of the access control system to specified accounts.

7.2.1.4 The access control system shall, upon implementation/ installation, present the user with a reminder that no access control system can be effective 100% of the time and that, despite rigorous controls, there may still be occasions when inappropriate materials may be accessed.

7.2.1.5 Any known conflicts with other software shall be notified to the parent/carer as part of the implementation/installation process.

7.2.1.6 Following implementation/installation, the access control system shall provide a mechanism for the parent/carer to test that the system is operating effectively.

7.2.1.7 Following implementation/installation, the access control system shall give a clear indication to the end user that access controls are activated on the device.

7.2.1.8 Where implementation/installation is required, parents/carers shall be able to install/configure the access control system following clear prompts and instructions as defined in Clause **12**.

7.2.2 Product/service type B – access control system requiring full configuration of settings

7.2.2.1 For the purposes of compliance with PAS 74, **7.2.2** shall be supported by detailed user installation/configuration instructions to ensure the access control system can be configured to an appropriate level in compliance with third-party conformity testing (see **12.2.3.2**).

7.2.2.2 The access control system shall provide parents/carers with the ability to configure access control settings against specified system/device user accounts as part of the installation/configuration process.

7.2.2.3 The access control system shall, upon installation/configuration, in accordance with **12.2.3.3**, provide the required level of protection through the configuration of access control settings by the parent/carer.

7.2.2.4 The access control system shall, upon installation/configuration, present the user with a reminder that no access control system can be effective 100% of the time and that, despite rigorous controls, there may still be occasions when inappropriate materials may be accessed.

7.2.2.5 Any known conflicts with other software shall be notified to the parent/carer as part of the installation process.

7.2.2.6 Following installation, the access control system shall provide a mechanism for the parent/carer to test that the system is operating effectively.

7.2.2.7 Following installation, the access control system shall give a clear indication to the end user that access controls are activated on the device.

7.2.2.8 Where installation/configuration is required, parents/carers shall be able to install/configure the access control system following clear prompts and instructions as defined in Clause **12**.

8 Configuration

8.1 General

NOTE 1 For purposes of compliance, the mandatory requirements detailed below apply to both access control system product/service types A and B.

*NOTE 2 The criteria used for checking compliance for products and services offered for third-party conformity testing under Clause **8** are listed in Annex H.*

8.2 Mandatory requirements

8.2.1 The access control system shall provide the parent/carer with the ability to complete the configuration process following clear prompts and instructions as defined in Clause **12**.

8.2.2 Amendments to the configuration shall only be actionable by the parent/carer via a secure, password-protected interface.

8.2.3 All input required to effectively configure and use the access control system shall be clearly flagged to the parent/carer.

8.2.4 The access control system shall be designed to minimize errors in user input during the configuration process. Where errors are made, the access control system shall provide clear feedback to the parent/carer.

8.2.5 The access control system shall provide a mechanism for the parent/carer to test that the system is working following configuration.

9 Maintenance

9.1 General

NOTE 1 For purposes of compliance the mandatory requirements detailed below apply to both access control system product/service types; A and B.

*NOTE 2 The criteria used for checking compliance for products and services offered for third-party conformity testing under Clause **9** are listed in Annex I.*

9.2 Mandatory requirements

9.2.1 The access control system shall be kept up to date automatically without the involvement of the parent/carer.

9.2.2 Updates to the access control system shall retain the user configuration present prior to an update taking place. In the event where this is not possible, the access control system shall present the parent/carer with a warning message describing any loss in configuration or settings.

9.2.3 The access control system shall provide a mechanism to allow the parent/carer to check that the access control system is up to date.

9.2.4 The parent/carer shall have the ability to maintain the access control system.

9.2.5 Where the parent/carer chooses to undertake maintenance of the access control system, the access control system shall provide clear prompts and instructions.

9.2.6 Parents/carers shall be notified of expiry of licence in accordance with specified notice periods contained in product description information (see **12.2.1**), at a minimum providing the user with a reminder of expiry.

9.2.7 When it is necessary for the supplier to issue software updates, patches and fixes for the access control system, in order to ensure continued security and performance in line with the requirements of this PAS, this shall be clearly explained to parents/carers, together with any consequent actions they may need to take as a result of the installation of such patches or fixes.

NOTE These patches and security fixes should not involve major changes in functionality.

9.2.8 Upgrades to the access control system involving fundamental changes to functionality shall not be made available until the access control system has undergone re-assessment in accordance with the requirements of this PAS.

10 Uninstall/removal

10.1 General

NOTE 1 For purposes of compliance, the mandatory requirements detailed below apply to both access control system product/service types A and B .

*NOTE 2 The criteria used for checking compliance for products and services offered for third-party conformity testing under Clause **10** are listed in Annex J.*

10.2 Mandatory requirements

10.2.1 The uninstall/removal process shall only be actionable by the parent/carer via authorization.

10.2.2 The uninstall/removal process shall provide the option to remove other third-party products installed as part of the access control system installation process.

10.2.3 If the uninstall/removal process requires changes to settings within the operating system, these shall be clearly explained in the installation/removal instructions.

11 System support

11.1 General

NOTE 1 For purposes of compliance, the mandatory requirements detailed below apply to both access control system product/service types A and B.

*NOTE 2 The criteria used for checking compliance for products and services offered for third-party conformity testing under Clause **11** are listed in Annex K.*

11.2 Mandatory requirements

11.2.1 Online or telephone support shall be provided as a minimum.

NOTE For example, online support may be via FAQs, on-screen enquiry forms or email.

11.2.2 System support providers shall make a first attempt to resolve a support request from a parent/carer within the specified response times of the supplier (within available support times).

11.2.3 System support providers shall provide an easy-to-use and obvious mechanism for the parent/carer to request and make amendments to the filtering and blocking rules of the access control system at a system level (e.g. reporting of inappropriate websites).

11.2.4 If requests to amend filtering and blocking rules are approved, changes to rules shall be made within the specified response times of the supplier (within available support times).

11.2.5 If requests to amend filtering and blocking rules are denied, the parent/carer shall be notified of the reason for denial.

12 Product description and user documentation

12.1 General

For the purposes of compliance with PAS 74, manufacturers shall ensure that the user documentation details the user installation/implementation/configuration process required to ensure the access control system can be effectively installed/implemented/configured to an appropriate level of protection in compliance with third-party conformity testing.

*NOTE The criteria used for checking compliance for products and services offered for third-party conformity testing under Clause **12** are listed in Annex L.*

12.2 Mandatory requirements

12.2.1 Product description

For access control systems, the following information shall be provided as a minimum in the product description:

a) information on conformity certifications awarded to the product;

b) identification information, including product name, function, date of release and version;

c) purpose and field of application;

d) operating environment, including hardware, software and communications requirements;

e) contents of the package;

f) contractual information, including licensing, conditions of use, and financial commitments (e.g. subscriptions, support costs);

g) contact details for system support, consumer communications and complaints and times of availability of support;

h) information on specifications, standards or laws that have been followed.

NOTE 1 A specification for the information that should be provided on the outside of consumer software packages is given in BS 7137 [2].

NOTE 2 Although the descriptions in this clause are based on physical product packaging, such information is still relevant for all access control systems.

12.2.2 User documentation

12.2.2.1 The user documentation shall provide as a minimum:

a) a functional description of the access control system;

b) clear instructions for the installation of the access control system (where applicable, see **12.2.3**);

c) clear instructions for the configuration of the access control system (where applicable, see **12.2.3**);

d) clear instructions for the maintenance of the access control system including anticipated costs;

e) clear instructions for testing to ensure that access controls are working correctly;

f) clear information on the methods for accessing system support services;

g) clear instructions for uninstalling/removing the access control system;

h) a table of contents and index.

NOTE 1 A specification for the design and preparation of user documentation is given in BS ISO/IEC 18019 [1].

NOTE 2 User documentation may be provided in print or electronic format.

12.2.2.2 The user documentation shall be designed to be accessible and effective for use by the parent/carer.

12.2.2.3 The user documentation shall avoid the use of jargon and custom terminology.

12.2.2.4 Any necessary technical terms used within the user documentation shall be clearly defined, and shall be used consistently throughout the documentation and within the access control system.

12.2.2.5 The user documentation shall define general terms relating to online safety issues that benefit the parent/carer in understanding the issues and applicability of features of the access control system.

12.2.2.6 All information in the user documentation shall be correct and free from ambiguities and contradictions.

12.2.2.7 If the user documentation is provided in electronic form, a print option shall be provided.

12.2.2.8 The user documentation shall be searchable (for example, an index for print user documentation or search facility for electronic user documentation), and shall guide the user to related topics.

12.2.3 Installation and configuration instructions for PAS 74 compliance

12.2.3.1 General

For purposes of compliance, manufacturers shall apply the mandatory requirements applicable to their specific product/service type (see **12.2.3.2** and **12.2.3.3**).

12.2.3.2 Product/service type A – access control system providing default settings

12.2.3.2.1 The access control system shall provide clear installation/implementation instructions to apply default settings in compliance with PAS 74 clauses **4.2.1** and **4.2.2**.

NOTE These should be provided as on-screen instructions, or in electronic document format or in printed document format.

12.2.3.2.2 The installation process documented shall be designed to be accessible and effective for use by the parent/carer.

12.2.3.2.3 The installation instructions shall avoid the use of jargon, custom terminology and acronyms.

12.2.3.2.4 Any necessary technical terms relating to the installation of the product shall be clearly defined in the installation instructions.

12.2.3.2.5 All input required to effectively install and use the access control system shall be clearly communicated to the parent/carer.

12.2.3.2.6 The access control system shall be designed to minimize errors in user input during the installation process. Where errors are made, the access control system shall provide clear feedback to the parent/carer.

NOTE 1 A specification for the design and preparation of user documentation is given in BS ISO/IEC 18019 [1].

NOTE 2 User documentation may be provided in print or electronic format.

12.2.3.3 Product/service type B – access control system requiring full configuration of settings

12.2.3.3.1 The access control system shall provide clear installation/configuration instructions to enable the parent/carer to apply system control settings in compliance with PAS 74, clauses **4.2.2** and **5.2.2**.

NOTE These should be provided as on-screen instructions, or in electronic document format or in printed document format.

12.2.3.3.2 The installation/configuration process documented shall be designed to be accessible and effective for use by the parent/carer.

12.2.3.3.3 The installation/configuration instructions shall avoid the use of jargon, custom terminology and acronyms.

12.2.3.3.4 Any necessary technical terms relating to the installation/configuration of the product shall be clearly defined in the installation/configuration instructions.

12.2.3.3.5 All input required to effectively install/configure and use the access control system shall be clearly communicated to the parent/carer.

12.2.3.3.6 The access control system shall be designed to minimize errors in user input during the installation/configuration process. Where errors are made, the access control system shall provide clear feedback to the parent/carer.

NOTE 1 A specification for the design and preparation of user documentation is given in BS ISO/IEC 18019 [1].

NOTE 2 User documentation may be provided in print or electronic format.

13 User education materials

13.1 Mandatory requirements

NOTE For purposes of compliance, the mandatory requirements detailed below apply to both access control system product/service types A and B.

All access control systems shall be provided with predefined user education materials. The user education materials may be packaged in either hard copy or electronic copy format but shall form part of the overall package.

NOTE The predefined content is available for download from the following location: www.thinkuknow.co.uk/parents/PAS74.

14 Conformity declaration

Conformity with this specification shall be indicated by the following information:

a) the number and date of this Publicly Available Specification, i.e. PAS 74:2007;[1)]

b) the name or trademark of the software provider;

c) where authorized, the mark of a third-party certification body.

[1)] Marking PAS 74:2007 on or in relation to a product or service represents the supplier's declaration of conformity, i.e. a claim by or on behalf of the supplier that the product or service meets the requirements of the standard. The accuracy of the claim is therefore solely the responsibility of the person making the claim. Such a declaration is not to be confused with third-party certification of conformity, which may also be desirable.

Annex A (normative) Overview of the test laboratory process

A.1 The laboratory

The testing laboratory will be independent and will be appointed by the Certification Body. Testing will be conducted under controlled conditions and will follow the test procedures detailed in Annexes C to L.

A.2 Test methods

Products under test will be tested on a platform (operating system and hardware) that meets or exceeds the minimum specifications displayed on the product packaging or associated material.

Where installation is required the products will be installed following the supplied instruction manual or guidelines. Any set-up wizard will be used and the default options for product/service type A or the recommended options if provided for product/service type B will be selected during the installation process, dependent upon product type under assessment (see **2.23** and **2.24**).

Connection to the Internet will be provided via an unfiltered broadband package or via the connection provided with the product.

The laboratory will ensure that test platforms are typical of what the intended user will be operating but will be free from products that could unduly hinder the performance of the product under test. The product will be tested with default applications installed on the platform where necessary. These will include browser, firewall, anti-virus, media player, office suite. If these are provided with the operating system they will be used. If they are not part of the operating system then the most appropriate/popular applications for that operating system will be used.

A.3 Reporting

The laboratory will provide a report of testing results to the Certification Body who will examine the results against the minimum requirements of this PAS.

A final report will be issued by the Certification Body detailing the results and sent to the product manufacturer. The results will not contain specific elements relating to the testing process but will contain a broad breakdown of the products conformance to the PAS requirements.

A.4 Inventory

Prior to testing, an inventory of key features will be compiled and compared to the claimed specification of the product and to the claims and descriptions given to the consumer at the point of sale or point of initial access.

Any discrepancies between the claimed specification and the product submitted for test that are noted during the inventorisation that could result in the product failing the standard will be reported back to the product manufacturer via the Certification Body before the full tests are started.

Annex B (normative) Categories of inappropriate content

B.1 Adult (sexually explicit) content

Defined as content containing sexually explicit images, video and text, the depiction of actual or realistic sexual activity including, but not limited to:

a) real or simulated sexual intercourse including explicit cartoons or animation;

b) depiction of sexual activity involving devices such as sex toys;

c) sexual activity with visible pubic areas or genitals;

d) threats of sexual violence such as rape;

e) excessive use of profanity or obscene gesticulation;

f) erotic stories and textual descriptions of sexual acts;

g) sexually exploitative or sexually violent text.

NOTE Material which genuinely seeks to inform and educate such as content relating to sexuality, safe sex, and health education may be permissible and may be defined by further categorization relating to the age range that the content would be relevant to.

B.2 Violence (including weapons and bombs)

Defined as material containing graphically violent images, video and text, including, but not limited to:

a) portrayal of graphic violence against humans, animals or institutions;

b) depictions of torture, mutilation, gore or horrific death;

c) content advocating self-endangerment, self-mutilation or suicide, including promotion of eating disorders or addictions;

d) graphic violence that in particular dwells on the infliction of pain or injury;

e) instructions for making bombs and weapons;

f) portrayal and glamorization of easily accessible weapons, e.g. knives;

g) content promoting terrorism and terrorist organizations;

h) content promoting the use and purchase of weapons, ammunition, explosives, poisons, etc.

NOTE Material which genuinely seeks to inform and educate such as content relating to current affairs, news, and historical information may be permissible and may be defined by further categorization relating to the age range that the content would be relevant to.

B.3 Racist and hate material

Defined as material which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds, including, but not limited to:

a) content that advocates or incites violence or attack based on religious, racial, ethnic, gender, age, disability, sexual orientation or cultural community grounds;

b) content that advocates social intolerance;

c) promotion of political agendas based on supremacist, exclusionary, racial, religious, ethnic, gender, age, disability or sexual orientation grounds;

d) holocaust denial, revisionist content and other sites encouraging hate;

e) militancy and extremist content.

NOTE Material which genuinely seeks to inform and educate such as content relating to current affairs, news, and historical information may be permissible and may be defined by further categorization relating to the age range that the content would be relevant to.

B.4 Illegal drug taking and the promotion of illegal drug use

Defined as material relating to the use and promotion of illegal drugs, including, but not limited to:

a) content promoting, encouraging or instructing on the use of illegal drugs, including the use of tobacco, alcohol and other substances illegal to minors;

b) information relating to disguising drug use, including alcohol and tobacco;

c) content promoting the sale and distribution of illegal drugs;

d) information relating to recipes, manufacturing and growing of illicit substances;

e) content promoting and instructing on the use of legal highs and the abuse of other legal substances;

f) content promoting and instructing on abuse of prescription drugs.

NOTE Material which genuinely seeks to inform and educate such as content relating to current affairs, news, and historical information may be permissible and may be defined by further categorization relating to the age range that the content would be relevant to.

B.5 Criminal skills/activity

Defined as material relating to the promotion of criminal and other activities, including, but not limited to, content:

a) promoting, instructing and advocating illegal activity;

b) providing advice on criminal skills such as lock picking, burglary, fraud, etc.;

c) relating to cracked or pirated software distribution;

d) relating to the unauthorized distribution of music, videos, fake IDs, etc.;

e) promoting, instructing or distributing malicious executable software, viruses, worms, etc.;

f) promoting the unauthorized use of, or attempts to circumvent or bypass the security mechanisms of, an information system or network;

g) providing information associated to workarounds of the access control system.

NOTE Material which genuinely seeks to inform and educate such as content relating to current affairs, news, and historical information may be permissible and may be defined by further categorization relating to the age range that the content would be relevant to.

B.6 Gambling

Defined as material relating to the use of online gambling websites and information relating to the promotion of gambling and gambling advice, including, but not limited to:

a) online gambling and lottery websites inviting users to risk money or valuables either virtual or real;

b) content providing information and advice relating to tips and wagers, bookmaker odds, etc.;

c) content promoting methods of gambling, including, but not limited to:

   1) participation in lotteries;

   2) sports picks;

   3) running numbers;

d) online casinos and poker rooms;

e) promoting a gambling lifestyle.

NOTE Material which genuinely seeks to inform and educate such as content relating to current affairs, news, and historical information may be permissible and may be defined by further categorization relating to the age range that the content would be relevant to.

Annex C (normative) Criteria to be used for checking compliance against Clause 4: Internet-based content

The following test criteria will be applied to ensure that the mandatory requirements detailed in Clause **4** are met. The laboratory will determine if the system is a product/service type A or type B and will configure the system as appropriate. The product under test will be configured for maximum filtering as defined in Clause **4** and Annex B.

*NOTE Type A products/services should, by default, provide the required level of content filtering. Type B products/services should provide the required level of content filtering through following clear prompts and instructions as defined in **12.2.3.2**.*

C.1 The laboratory will check the effectiveness of the access control system to prevent access to inappropriate content and services in the categories identified in Annex B.

The laboratory will use a pre-prepared list of URLs. The URLs will cover all the categories identified in Annex B. The number of URLs will be statistically significant to ensure the required accuracy of the final result. The number of sites in each category will be distributed such that 50% of the sites will correspond to category B.1 , while the remaining five categories, B.2 to B.6, will each contain 10% of the total number of sites. The list will be kept up to date by regular renewal and by pruning of ''dead'' URLs.

The list of sites will be compiled and authorized for use by the laboratory by an independently elected group of experts.

For each product tested, a laboratory benchmark product will be tested concurrently to check consistency. The benchmark will be retained by the laboratory for all tests but it will be reviewed periodically. The benchmark will be chosen as a product that performs well but will not be a near perfect or reference product.

The product under test will be required to access each entry on the URL list. A percentage successful filtering score will be calculated. This score will be compared to the current pass/fail score determined by an independent panel constituted by the Certification Body.

C.2 The laboratory will check that the access control system does not unduly overblock access to suitable Internet content.

NOTE The test will check for a satisfactory performance in relation to overblocking. It is not designed to try to ''catch out'' the access control system's performance with ambiguous sites or to test the system to extreme.

The laboratory will use a pre-prepared short-list of safe URLs that could be misinterpreted by a filter as unsafe. The sites will be checked to ensure they are safe. Ambiguous sites or contentious sites will be avoided.

The test sites will include (but not exclusively) the following common problems. These will be chosen to cover a range of common problems but will not be designed to be unduly challenging, difficult or obscure:

a) large portal or umbrella sites that could contain unsuitable materials within their many sub sites but suitable material within other areas of the domain;

b) sites with unfortunately spelled names or content where combinations of letters may spell words that could be blocked by a word list;

c) educational, government, historical and medical sites that deal with, for example, sex, drugs, violence or racial issues on a serious basis;

d) some well known children's and social networking sites.

The product under test will be required to access each entry on the URL list. A percentage successful access score will be calculated. The score will be used to establish that the product has taken reasonable steps to minimize overblocking.

C.3 The laboratory will check the ability of the access control system to allow parents/carers access to all Internet-based content.

The laboratory will install the product under test to block access to Internet content for unauthorized users.

A test will then be made to ensure that a parent/carer can override the filter, either by direct intervention or by logging on as a different user. The test will further ensure that:

a) this action is secure (e.g. password protected);

b) under default conditions it will automatically revert to filtered performance after a specified time or period of inactivity.

C.4 The laboratory will check the ability of the access control system to completely block access to Internet-based content.

The laboratory will configure the product under test for complete blocking of Internet content, in accordance with the supplied or displayed instructions. Attempts to access Internet content will then be made. This will include basic World Wide Web access and also any additional content that might be supported by the platform (e.g. special e-commerce facilities, file downloads).

The laboratory will check that this block does not adversely affect any other applications that the platform offers such as the running of installed software applications and communications services not covered by Annex E.

Annex D (normative) Criteria to be used for checking compliance against Clause 5: Internet-based communications

The following test criteria will be applied to ensure that the mandatory requirements detailed in Clause **5** are met. The product or service under test will be configured for its default settings. The laboratory will document the results.

The laboratory will determine if the product/service is a type A or a type B product and will use or configure the system as appropriate.

D.1 The laboratory will test to confirm that the Internet-based communication systems detailed in Annex E are effectively blocked. The laboratory will test this by attempting to send and receive information via each of these systems.

NOTE Any custom communication system provided by a service associated with the access control system under test, e.g. a service specifically tailored for children, can be considered exempt at the discretion of the laboratory and the Certification Body.

D.2 If the access control system under test is configurable and so allows the parent/carer to permit access to selected communication services the laboratory will conduct the following tests:

D.2.1 If the product/service is type A and allows configuration to individual accounts the laboratory will test to ensure that communication via Internet-based services is blocked by default and available by selection for selected accounts. If the product/service is a type B service the laboratory will configure the access control system to allow a selected service, in accordance with the instructions provided. The laboratory will then send and receive information via this service to confirm that it is accessible. It will then similarly test the remaining services to check that they are still blocked.

D.2.2 If the product is a type B product or service the laboratory will assess the process required for the parent/carer to carry out the configuration of the Internet communication services.

*NOTE The whole process should be designed for an ''inexperienced user'' as defined in **2.12**.*

Annex E (normative) Categories of Internet-based communication services

a) Email;

b) Instant messaging clients;

c) Usenet Newsgroups;

d) File Transfer Protocol (FTP) and Secure File Transfer Protocol (FTPs);

e) Peer to Peer (P2P) file sharing;

f) Internet Relay Chat (IRC);

g) Web-based chat and web forums;

h) Webcam programs;

i) Voice over IP (VoIP) programmes and utilities.

Some platforms may provide filtering services for some of the above, however, this PAS does not concern itself with these services and is concerned only with the requirements in Clause 5.

Annex F (normative) Criteria to be used for checking compliance against Clause 6: Security of settings

The following tests will be applied to ensure that the mandatory requirements detailed in Clause **6** are met. The laboratory will document the results.

F.1 The laboratory will carry out tests to confirm that access to the access control system's configuration settings are adequately protected and that the system cannot be disabled.

The laboratory will firstly carry out a series of basic tests to try and bypass the protection system using common techniques based around the platform's operating system and applications. The laboratory will then carry out some more advanced tests based on information that is already in the public domain – where available.

F.2 The laboratory will check that the access control system's security is not compromised by any tools provided by the platform hardware, operating system or browser, that provide auto complete, auto enter or otherwise remember functions.

F.3 The laboratory will follow through the recommended procedure for regaining control of the platform and access control system should the security system fail (e.g. parent/carer forgets password).

The laboratory will assess the security of this procedure with regard to unauthorized users trying to follow it.

Annex G (normative) Criteria to be used for checking compliance against Clause 7: Installation

The following test criteria will be applied to ensure that the mandatory requirements detailed in Clause **7** are met.

G.1 The laboratory will determine if the system is a type A or a type B product or service and will use or configure the system as appropriate.

For product/service type A systems

A test engineer with experience or formal training of assessing software usability will install the product and determine the following.

- The default settings configure the system appropriately to give the required level of protection;
- The appropriate user instructions are provided;
- Where claimed, the ability to implement and configure individual user accounts is provided;
- During the installation process, the specified reminder to the parent/carer that no access control system can be 100% effective, and also inform the parent/carer of any known software conflicts. (If there are none then this should be stated.);
- That an effective mechanism for testing that the filter is active is provided, is prominent and is easy to use;
- That there is a clear indication to the end user that a filter is present and active.

At any point where the parent/carer has to make a decision or choice or take some other action, based on the requirements of clause **7.2.1**, the test engineer will record and describe any problems encountered during the procedure. Where appropriate the laboratory will provide pictorial evidence of the problems encountered.

For product/service type B systems:

A test engineer with experience or formal training of assessing software usability will install the product and determine the following.

- The system provides the parent/carer with all the necessary tools to adequately configure the system to give the required level of protection and that these tools work effectively;
- The appropriate user instructions are provided;
- Where claimed, the ability to implement and configure individual user accounts is provided;
- During the installation process, the specified reminder to the parent/carer that no access control system can be 100% effective, and also inform the parent/carer of any known software conflicts. (If there are none then this should be stated.);
- That an effective mechanism for testing that the filter is active is provided, is prominent and is easy to use;
- That there is a clear indication to the end user that a filter is present and active.

At any point where the parent/carer has to make a decision or choice or take some other action based on the requirements of clause **7.2.2**, the test engineer will record and describe any problems encountered during the procedure. Where appropriate the laboratory will provide pictorial evidence, i.e. screen shots of the problems encountered.

For both product/service types the areas to be considered will include clarity of on-screen menus and messages, presentation and content of any (installation) instruction manual, technical understanding and terminology, intuitiveness of menus and wizards, the possibility for ambiguity in questions or options, feedback to the installer and the ability to correct errors. Additional consideration will be paid to accessibility issues as described in clause **7.2**.

Annex H (normative)

Criteria to be used for checking compliance against Clause 8: Configuration

The following test criteria will be applied to ensure that the mandatory requirements detailed in Clause **8** are met.

H.1 A test engineer with experience or formal training of assessing software usability will access the software's tools or menus that are available to the parent/carer and make amendments to the configuration. They will check that access to these tools and menus are appropriately secured.

Because the configuration options are likely to vary between different access control products and different platforms the laboratory will adopt a ''scenario'' method (rather than a fixed check list) for assessing the usability of the configuration process. The operator will record and describe any problems encountered during the procedure, based on the requirements of clauses **8.2.1** to **8.2.5**. Where appropriate the laboratory will provide pictorial evidence of the problems encountered.

The areas to be considered will include clarity of on-screen menus and messages, presentation and content of any instruction manual, technical understanding and terminology, intuitiveness of menus and wizards, the possibility for ambiguity in questions or options, feedback to the parent/carer and the ability to correct errors.

H.2 Following the default installation (type A) or system configuration (type B) as defined in **2.23** and **2.24**, the test laboratory will confirm the presence of a process for checking that the access control system is operating in accordance with the configuration and will check that it works satisfactorily. Any problems will be recorded.

Annex I (normative) Criteria to be used for checking compliance against Clause 9: Maintenance

The following test criteria will be applied to ensure that the mandatory requirements detailed in Clause **9** are met.

Tests involving software updates (patches and security fixes) may require the co-operation of the supplier/manufacturer to help the laboratory simulate the process.

I.1 The laboratory will determine the mechanism by which the access control system is kept up to date and so confirm that it is an ''automatic'' process. The laboratory will also determine if the process is working correctly.

NOTE In some situations, this may require the laboratory to contact the access control system supplier in order to initiate an update using a test site.

I.2 The laboratory will confirm that any ''user settings and configurations'' are either not changed or lost following an update or if they have been, that the product or service suitably warns the parent/carer before the access control system can be used.

I.3 The laboratory will follow the recommended procedure for the parent/carer to check that the system is up to date (e.g. the system should report the date of the last update).

NOTE In some systems where the access control is at the server side (e.g. ISP based access control) where updates occur on a continuous basis, it may not be possible to carry out this test. The laboratory will use its discretion to decide if the access control system is being kept up to date. It may be necessary for the laboratory to contact the supplier direct for this.

I.4 The laboratory will check that the product/service has adequate tools for the parent/carer to maintain the system. This should include automatic software modifications and manual updating option of filter content. The laboratory will assess that this is an intuitive process and adequate information is given to the parent/carer.

I.5 Where applicable, the laboratory will determine that adequate advanced notification of the expiry of a licence is given.

NOTE As this test may be difficult to implement in practice it may be necessary to take on trust any claims made in the user manual or online help.

I.6 The laboratory will determine that options for upgrading the access control system software are clearly explained and are suitable for the inexperienced user.

I.7 In the case of special software updates (routine patches and security fixes) the laboratory will determine that these are clearly explained to the parent/carer in terms that would be understood by an inexperienced user. If such problems were encountered the laboratory will provide pictorial evidence, i.e. screen shots of the problems encountered.

Annex J (normative) Criteria to be used for checking compliance against Clause 10: Uninstall/removal

The following test criteria will be applied to ensure that the primary objective and mandatory requirements detailed in Clause **10** are met.

J.1 The laboratory will uninstall the access control system following any supplied instructions or online instructions. If provided, the uninstall tool will be used. If no uninstall tool is supplied the system will be uninstalled using the operating system's default uninstall routine.

The laboratory will determine if the uninstall process can be carried out by an inexperienced user and requires no expert knowledge, understanding of specialist technical terms or any other obstacles. If such problems were encountered the laboratory will report this with detailed explanation and pictorial examples.

J.2 The laboratory will confirm that the access control system uninstall process was protected from unauthorized users.

J.3 The laboratory will check that after uninstalling the access control system and any associated applications have been fully removed from the platform. The laboratory will check that access control is no longer active.

J.4 The laboratory will check that any required changes to the operating system resulting from the uninstalling process are clearly explained in the installation instructions.

J.5 The laboratory will document the results**.**

Annex K (normative) Criteria to be used for checking compliance against Clause 11: System support

The following test criteria will be applied to ensure that the mandatory requirements detailed in Clause **11** are met.

K.1 The laboratory will establish what method(s) of customer support are provided and confirm that either online or telephone support are available options.

K.2.1 Phone

To confirm correct operation of the phone line help the laboratory will contact the helpline with a simple installation problem. The laboratory will record if a satisfactory response is given within the supplier's specified response time. To test the quality of the answers, the test will be repeated five times with five different questions. The laboratory will judge the quality of the responses and log any problems.

NOTE It is the intention of this PAS to test the availability and response time of the support system and not to test the technical expertise of the system or personnel.

K.2.2 Email

To confirm correct operation of the online support the laboratory will post a technical question and monitor the responses, including acknowledgment emails and progress reports.

K.3 The laboratory will discover whether the access control system offers a mechanism for users to request amendments to the access control system and if so the availability of this service and how to use it are displayed prominently.

The laboratory will test the system by requesting that some web pages be blocked. This request will be made within the suppliers specified operating times. The laboratory will record if a satisfactory acknowledgement of receipt is received within the supplier's specified response time.

The laboratory will then record:

a) if requested amendments are implemented within the supplier's specified response time in the case of accepted amendments;

b) that a notification is received within the supplier's specified response time in the case of rejected amendments.

Annex L (normative) Criteria to be used for checking compliance against Clause 12: Product description and user documentation

The following test criteria will be applied to ensure that the mandatory requirements detailed in **12.2** are met.

A test engineer with experience or formal training of assessing documentation for consumer electronic products (including computers and software) will assess the supplied documentation.

L.1 The laboratory will check that the access control system's product description, as supplied at the point of sale or at the time of signing up or subscribing, provides all eight items of information detailed in clause **12.2.2.1** of this PAS. The laboratory will report any omissions.

L.2 The laboratory will check that the access control system's user documentation meets all eight requirements detailed in clause **12.2.2.1** of this PAS. This will be assessed by a laboratory test engineer with experience or the necessary training in assessing the quality of written or online user instructions. The laboratory will report any omissions.

L.3 By reading through the user documentation the laboratory will determine that the user documentation complies with the requirements of **12.2.2**. This will be assessed by a laboratory test engineer with experience or the necessary training in assessing the quality of written or online user instructions. The laboratory will report any problems.

L.4 For user documentation supplied in electronic form the laboratory will check that it can be conveniently printed out. The laboratory will report any problems.

L.5 The laboratory will check that the user documentation is searchable either by a printed index or by electronic search. It should also guide the user to related topics. The laboratory will report any problems or omissions.

L.6 For product/service type A and type B

A test engineer with experience or formal training of assessing instructions for consumer electronic products (including computers and software) will assess and test the supplied instructions and specifically address the additional requirements of subclauses **12.2.3.2** through to **12.2.3.2.6** (type A) and subclauses **12.2.3.3.1** through to **12.2.3.3.6** (type B).

The testing will be carried out by practical application of the instructions with the product/service and the test engineer will deliberately introduce typical user errors.

Bibliography

Standards publications

[1] **BS ISO/IEC 18019:2004**, *Software and system engineering. Guidelines for the design and preparation of user documentation for application software*

[2] **BS 7137:1989**, *Specification for user documentation and cover information for consumer software packages*

Also published as **ISO 9127:1988**, *Information processing systems – User documentation and cover information for consumer software packages*

Other publications

BS 7649:1993, *Guide to the design and preparation of documentation for users of application software*

BS ISO/IEC 12119:1994, *Information technology – Software packages – Quality requirements and testing*

BS ISO/IEC 15910:1999, *Information technology – Software user documentation process*

BSI – British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this Publicly Available Specification would inform the Information Centre. Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsigroup.com.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001. Email: orders@bsigroup.com. Standards are also available from the BSI website at http://www.bsigroup.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsigroup.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002. Fax: +44 (0)20 8996 7047. Email: membership@bsigroup.com.

Information regarding online access to British Standards and Publicly Available Specifications via British Standards Online can be found at http://www.bsigroup.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsigroup.com.

Copyright

389 Chiswick High Road
London
W4 4AL