



DPC: 19 / 30405196 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 05 November 2019

Origin: International

Latest date for receipt of comments: 12 December 2020

Project No. 2019/03351

Responsible committee: TCT/7 Telecommunications - Installation requirements

Interested committees:

Title: Draft BS ISO/IEC 24383 Information technology - Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 12 December 2020**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Mr Christopher Brown (BSI)**Direct tel: **02089967441**E-mail: **christopher.brown@bsigroup.com**

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



JTC1-SC25/2914/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER:

ISO/IEC 24383 ED1

DATE OF CIRCULATION:

2019-10-18

CLOSING DATE FOR COMMENTS:

2020-01-10

SUPERSEDES DOCUMENTS:

JTC1-SC25/2859/NP, JTC1-SC25/2883/RVN

IEC ISO/IEC JTC 1/SC 25 : INTERCONNECTION OF INFORMATION TECHNOLOGY EQUIPMENT

SECRETARIAT:

Germany

SECRETARY:

Mr Marco Peter

OF INTEREST TO THE FOLLOWING COMMITTEES:

PROPOSED HORIZONTAL STANDARD:



Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.

FUNCTIONS CONCERNED:

☐ EMC

☐ ENVIRONMENT

☐ QUALITY ASSURANCE

☐ SAFETY

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

Information technology - Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment

NOTE FROM TC/SC OFFICERS:

As decided at the Nagasaki meeting, the attached 1st CD is circulated to National Committees for comment.

1 CONTENTS

2	FOREWORD.....	5
3	INTRODUCTION.....	6
4	1 Scope.....	7
5	2 References.....	7
6	3 Definitions and abbreviations.....	7
7	3.1 Definitions.....	7
8	3.2 Abbreviations.....	12
9	4 CONFORMANCE.....	12
10	5 RISK ASSESSMENT AND SECURITY CONCEPTS.....	12
11	5.1 Risk assessment.....	12
12	5.2 Security Grades.....	13
13	6 DESIGN.....	14
14	6.1 General.....	14
15	6.2 SG2.....	15
16	6.2.1 Spaces and structures of SG2.....	15
17	6.2.2 Pathways of SG2.....	16
18	6.2.3 Infrastructure components of SG2.....	17
19	6.3 SG3.....	17
20	6.3.1 Spaces and structures of SG3.....	17
21	6.3.2 Pathways of SG3.....	18
22	6.3.3 Infrastructure components of SG3.....	19
23	7 PLANNING.....	19
24	7.1 General.....	19
25	7.2 SG2.....	19
26	7.2.1 Spaces and structures of SG2.....	19
27	7.2.2 Pathways of SG2.....	19
28	7.2.3 Infrastructure components of SG2.....	21
29	7.3 SG3.....	21
30	7.3.1 Spaces and structures of SG3.....	21
31	7.3.2 Pathways of SG3.....	21
32	7.3.3 Infrastructure components of SG3.....	22
33	8 INSTALLATION.....	22
34	8.1 General.....	22
35	8.2 SG2.....	22
36	8.2.1 Spaces and structures of SG2.....	22
37	8.2.2 Pathways of SG2.....	22
38	8.2.3 Infrastructure components of SG2.....	23
39	8.3 SG3.....	24
40	8.3.1 Spaces and structures of SG3.....	24
41	8.3.2 Pathways of SG3.....	24
42	8.3.3 Infrastructure components of SG3.....	24
43	8.4 Commissioning.....	25
44	9 OPERATION.....	25
45	9.1 SG2.....	25

46	9.1.1	Spaces and structures of SG2	25
47	9.1.2	Pathways of SG2	26
48	9.1.3	Infrastructure components of SG2	26
49	9.2	SG3.....	26
50	9.2.1	Spaces and structures of SG3	26
51	9.2.2	Pathways of SG3.....	27
52	9.3	Automated infrastructure management (AIM) systems for security	27
53	9.3.1	General	27
54	9.3.2	Detect changes to patch cord connectivity	28
55	9.3.3	Port status information.....	28
56	9.3.4	Critical network circuits.....	28
57	9.3.5	Device alarms.....	28
58	9.3.6	Security camera integration	28
59	9.3.7	Communication with other systems.....	28
60	9.3.8	Emergency call origination location.....	28
61	10	EVOLUTION OF SECURITY SYSTEMS.....	28
62	Annex A	(normative) Free standing barriers	29
63	Annex B	(normative) Video surveillance	30
64	B.1	Requirements	30
65	B.1.1	Cabling, pathways and spaces	30
66	B.1.2	Cameras.....	30
67	B.1.3	Monitoring	30
68	B.2	Recommendations.....	30
69	B.2.1	Pathways.....	30
70	B.2.2	Cameras.....	30
71	B.2.3	Monitoring	31
72	Annex C	(normative) Intrusion detection	32
73	C.1	Requirements	32
74	C.1.1	Cabling, pathways and spaces	32
75	C.1.2	Deployment	32
76	C.1.3	Monitoring	33
77	C.1.4	Documentation	33
78	C.1.5	Operation	33
79	C.2	Recommendations.....	33
80	C.2.1	Security lighting.....	33
81	Annex D	(normative) Access control	35
82	D.1	Requirements	35
83	D.1.1	Cabling, pathways and spaces	35
84	D.1.2	Deployment	35
85	D.2	Recommendations.....	36
86	D.2.1	Planning	36
87	D.2.2	Pathways.....	36
88	Annex E	(normative) Management of personnel	38
89	E.1	Requirements	38
90	E.1.1	Employees and other authorized personnel	38
91	E.1.2	Manned guarding.....	38
92	E.1.3	Visitors	39
93	E.1.4	D.1.4 Deliveries	39

94	E.2 Recommendations.....	39
95	E.2.1 Visitors	39
96	E.2.2 Deliveries	40
97	Bibliography.....	41
98		
99	List of figures	
100	Figure 1 – Risk assessment concepts	13
101	Figure A.1 – Examples of free-standing barriers and minimum effective heights	29
102		
103	List of tables	
104	Table 1 – Overview of Security Grades	13
105	Table 2 – Requirements for door hardware and their corresponding conformance	
106	standards for Europe and the USA.....	15
107		
108		

INFORMATION TECHNOLOGY –

Generic cabling – Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment

FOREWORD

ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards. Their preparation is entrusted to technical committees; any ISO and IEC member body interested in the subject dealt with may participate in this preparatory work. International governmental and non-governmental organizations liaising with ISO and IEC also participate in this preparation.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO member bodies.

IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

In order to promote international uniformity, IEC and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

ISO and IEC provide no marking procedure to indicate their approval and cannot be rendered responsible for any equipment declared to be in conformity with an ISO/IEC publication.

All users should ensure that they have the latest edition of this publication.

No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

International Standard ISO/IEC 24383 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

INTRODUCTION

ISO/IEC 14763-2 specifies requirements and recommendations for the installation specification, quality assurance and installation practices for customer premises cabling in accordance with the ISO/IEC 11801 series.

Those requirements provides basic level of physical network security for the cabling and associated infrastructure.

This Standard builds upon the requirements of ISO/IEC 14763-2 by facilitating the timely and effective protection of the customer premises cabling infrastructure to avoid loss/damage to the physical information transport network.

This document provides comprehensive planning and installation requirements for physical network security as well as methods that protect the telecommunications infrastructure from theft, vandalism, intrusions, and unauthorized modifications.

The requirements and recommendations may be applied to existing buildings and also during building construction, or renovation, when actions significantly less expensive and less disruptive than after the building is occupied.

The standard incorporates the use of automated infrastructure management (AIM) systems, including those in accordance with ISO/IEC 18598, to further enhance the security of cabling infrastructure and integrate the physical network security with other security systems in the premises.

This document is intended to be used by

- architects, building owners, building designers and builders,
- consultants,
- facility managers and network managers,
- designers, suppliers, installers, inspectors (auditors), maintainers and owners of information technology cabling.

INFORMATION TECHNOLOGY - Generic cabling – Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment

1 Scope

This document specifies requirements and recommendations providing security to the physical network comprising customer premises cabling in accordance with ISO/IEC 11801 series, associated infrastructure and accommodation of information technology equipment.

The document covers the security of the telecommunications cables, pathways, spaces, and other infrastructure components of the telecommunications physical infrastructure to protect the telecommunications infrastructure from theft, vandalism, intrusions, and unauthorized modifications.

The document addresses

- risk assessment,
- design (including construction), planning and installation practices based on a required Security Grade (SG),
- intrusion detection,
- administration including Automated Infrastructure Management (AIM).

The document applies to existing buildings and structures together with those being planned for construction.

The following are outside the scope of this International Standard

- data protection methods such as encryption,
- practices that address protection from non-contact cable tapping, audio, visual or RF snooping and other forms of unauthorized monitoring.

Safety and electromagnetic compatibility (EMC) requirements are outside the scope of this international standard and are covered by other standards and regulations. However, information given in this international standard can be of assistance in meeting these standards and regulations.

2 References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 14763-2:20xx, *Information technology - Implementation and operation of customer premises cabling - Part 2: Planning and installation*

IEC 62676-1-1:2014, *Video surveillance systems for use in security applications. System requirements - General*

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this document the following definitions and those of ISO/IEC 14763-2 apply.

Editors NOTE: The "greyed-out" definitions are from ISO/IEC 14763-2 and are for clarity in early drafts of this document. They will be removed in the later stages of development.

- 219 **3.1.1**
 220 **access control system**
 221 system that provides selective restriction of access to a space or cabling component
- 222 **3.1.2**
 223 **administration**
 224 methodology defining the documentation requirements of a cabling system and its containment, the
 225 labelling of functional elements and the process by which moves, additions and changes are recorded
 226 [SOURCE 11801-1:2017, 3.1.1]
- 227 **3.1.3**
 228 **AIM system**
 229 integrated hardware and software system that automatically detects the insertion or removal of cords,
 230 documents the cabling infrastructure including connected equipment enabling management of the
 231 infrastructure and data exchange with other systems
 232 [SOURCE 18598:2016, 3.1.3]
- 233 **3.1.4**
 234 **alarmed carrier**
 235 system for detecting intrusion into a pathway using optical fibre as a vibration sensor
- 236 **3.1.5**
 237 **alarm-enabled**
 238 capable of triggering an alarm with the intrusion alarm system
- 239 **3.1.6**
 240 **authorized personnel**
 241 persons able to access a space or pathway of a defined Security Grade
- 242 **3.1.7**
 243 **cabinet**
 244 enclosed construction intended for housing closures and other telecommunications components and
 245 equipment
 246 [SOURCE 14763-2:20xx, 3.x.x1]
- 247 **3.1.8**
 248 **cable management system**
 249 system used for the support and/or containment, retention, protection of all types of cables,
 250 information and communication lines, electrical power distribution conductors and their associated
 251 accessories
 252 Note 1 to entry Includes ducts and tubes housing, or intended to house, blown telecommunications cables and/or cable
 253 elements.
 254 [SOURCE 14763-2:20xx, 3.x.x]
- 255 **3.1.9**
 256 **cabling**
 257 system of telecommunications cables, cords and connecting hardware that supports the connection of
 258 information technology equipment
 259 [SOURCE 11801-1:2017, 3.1.21]
- 260 **3.1.10**
 261 **cabling component**
 262 any product associated with the cabling installation including cables, connecting hardware, closures,
 263 cabinets, frames, racks and pathway systems together with components used to provide bonds to
 264 earthing systems
 265 [SOURCE 14763-2:20xx, 3.x.x]

- 266 **3.1.11**
267 **closed pathway system**
268 cable management system which does not allow installation of cables by laying without tensile load
269 [SOURCE 14763-2:20xx, 3.x.x]
- 270 **3.1.12**
271 **common distribution space**
272 primary or secondary building distribution space
- 273 **3.1.13**
274 **countermeasure**
275 step taken to prevent a threat triggering an event
- 276 **3.1.14**
277 **dialler unit**
278 device that communicates with external monitoring or response entities to report exceptions to pre-programmed
279 conditions via a specific telephone number, set of telephone numbers or a network connection.
- 280 **3.1.15**
281 **door hardware**
282 metallic fixtures that enable opening, closing, and locking a door
- 283 **3.1.16**
284 **entrance room**
285 space within, or at the boundary of, a building housing the demarcation point where facilities owned by
286 external access and/or service providers interface with the premises cabling
287 [SOURCE 14763-2:20xx, 3.x.x, modified by deletion of NOTE 1 to entry]
- 288 **3.1.17**
289 **electronic locking mechanism**
290 device that allows access following receipt of digital or analog information indicating an appropriate
291 authorisation status of the person entering the information
- 292 **3.1.18**
293 **effective height of a free-standing barrier**
294 shortest distance between any point on the top of the permanent part of the free-standing barrier
295 (excluding any toppings) and the surface of the supporting ground when measured in the plane of the
296 barrier
- 297 **3.1.19**
298 **event**
299 vulnerability that has been exploited by a threat
- 300 **3.1.20**
301 **external boundary**
302 physical barrier(s) demarcating a space or structure of a given Security Grade (SG)
303 Note 1 to entry: access floors and suspended ceilings through which unauthorised access to a space may be gained are not
304 considered to be external boundaries. In such cases, the fixed building fabric upon which these structures are built is the
305 external boundary.
- 306 **3.1.21**
307 **external telecommunications cabinet**
308 outdoor enclosure accommodating telecommunications equipment and associated cabling
- 309 **3.1.22**
310 **free-standing barrier**
311 wall, fence, gate, turnstile or other similar self-supporting barrier, and its associated foundations,
312 designed to prevent entry to a space of a given Security Grade

- 313 **3.1.23**
 314 **frame (rack)**
 315 open construction intended for housing closures and other telecommunications equipment
 316 [SOURCE 14763-2:20xx, 3.x.x]
- 317 **3.1.24**
 318 **hand hole**
 319 point of access to a pathway that is too small for a person to enter to perform work but that allows the
 320 routing of cables during the cable installation process such that bending and pulling requirements are
 321 met (an example of a hand-hole within a building is called a draw-box)
 322 [SOURCE 14763-2:20xx, 3.x.x]
- 323 **3.1.25**
 324 **intelligent building system**
 325 equipment and telecommunication infrastructure that supports monitoring, control, operation and
 326 management of building services
- 327 **3.1.26**
 328 **keypad**
 329 manual input devices, typically requiring telecommunications connectivity, that allow individuals to
 330 enter specific codes to arm, disarm or diagnose intrusion systems
- 331 **3.1.27**
 332 **joint closures**
 333 sealed housing protecting the joining or splicing of the conductors and optical fibres of
 334 telecommunications cables
- 335 **3.1.28**
 336 **junction box**
 337 junction box space that enables cables to be routed between pathway systems
- 338 **3.1.29**
 339 **maintenance hole (telecommunications)**
 340 vault/chamber located in the ground or earth as part of an underground conduit system and used to
 341 facilitate placing, connectorization, and maintenance of cables as well as the placing of associated
 342 equipment, in which it is expected that a person will enter to perform work
 343 [SOURCE 14763-2:20xx, 3.x.x]
- 344 **3.1.30**
 345 **mechanical locking mechanism**
 346 device that allows access by means of physically coded key or tool
- 347 **3.1.31**
 348 **open pathway system**
 349 pathway system which allows installation of cables by laying without tensile load
 350 [SOURCE 14763-2:20xx, 3.x.x]
- 351 **3.1.32**
 352 **openable pathway system**
 353 cable management system which restricts access to installed cables but which can be opened to allow
 354 installation of cables by laying without tensile load
 355 [SOURCE 14763-2:20xx, 3.x.x]
- 356 **3.1.33**
 357 **pathway (cable route, cable way)**
 358 defined route for cables between termination points
 359 [SOURCE 14763-2:20xx, 3.x.x]

- 360 **3.1.34**
361 **pathway system**
362 cable management system or other area or volume defined by markings or fittings used to protect
363 and/or support the cabling in order that its desired performance is maintained
364 [SOURCE 14763-2:20xx, 3.x.x]
- 365 **3.1.35**
366 **primary building distribution space**
367 space accommodating primary point of distribution of any common cabling infrastructure within multi-
368 tenant buildings
369 [SOURCE 14763-2:20xx, 3.x.x]
- 370 **3.1.36**
371 **rack**
372 see frame
373 [SOURCE 14763-2:20xx, 3.x.x]
- 374 **3.1.37**
375 **secondary building distribution space**
376 space accommodating optional points of distribution, additional to the main point of distribution, of any
377 common cabling infrastructure within multi-tenant buildings
378 [SOURCE 14763-2:20xx, 3.x.x]
- 379 **3.1.38**
380 **space**
381 specified volume (e.g. room, maintenance hole or part thereof) housing closures and/or other
382 telecommunications equipment
383 [SOURCE 14763-2:20xx, 3.x.x]
- 384 **3.1.39**
385 **surveillance system**
386 devices and mechanisms used to monitor and detect behaviour or activity to protect the physical
387 network
- 388 **3.1.40**
389 **tamper evident**
390 designed or enabled to show access or attempts to access
- 391 **3.1.41**
392 **terminal equipment**
393 equipment at an outlet used to access information provided by transmission equipment
394 [SOURCE: ISO/IEC 11801-1:2017, 3.1.81]
- 395 **3.1.42**
396 **terminal equipment outlet**
397 fixed connecting device which provides an interface to the terminal equipment
398 [SOURCE: ISO/IEC 11801-1:2017, 3.1.80, modified by deletion of Note 1 to entry]
- 399 **3.1.43**
400 **threat**
401 method by which a vulnerability can be exploited to create an event
- 402 **3.1.44**
403 **topping**
404 construction, added to the top of a free-standing barrier, and designed to be an effective intruder
405 deterrent or for a decorative display of security