



BSI Standards Publication

Information technology — Data centre facilities and infrastructures

Part 6: Security systems

National foreword

This Published Document is the UK implementation of ISO/IEC TS 22237-6:2018.

The UK participation in its preparation was entrusted to Technical Committee TCT/7/3, Telecommunications; Installation requirements: Facilities and infrastructures.

A list of organizations represented on this committee can be obtained on request to its secretary.

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

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 99303 9

ICS 35.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2018.

Amendments/corrigenda issued since publication

| Date | Text affected |
|------|---------------|
|------|---------------|

**Information technology — Data centre
facilities and infrastructures —**

**Part 6:
Security systems**

*Technologie de l'information — Installation et infrastructures de
centres de traitement de données —*

Partie 6: Systèmes de sécurité



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

| | |
|--|-----------|
| Foreword | v |
| Introduction | vi |
| 1 Scope | 1 |
| 2 Normative references | 1 |
| 3 Terms, definitions and abbreviated terms | 2 |
| 3.1 Terms and definitions..... | 2 |
| 3.2 Abbreviated terms..... | 3 |
| 4 Conformance | 3 |
| 5 Physical security | 3 |
| 5.1 General..... | 3 |
| 5.2 Risk assessment..... | 4 |
| 5.3 Designation of data centre spaces — Protection Classes..... | 5 |
| 6 Protection Class against unauthorized access | 5 |
| 6.1 General..... | 5 |
| 6.2 Implementation..... | 8 |
| 6.2.1 General..... | 8 |
| 6.2.2 Access to the data centre premises..... | 10 |
| 6.2.3 Protection Class 1..... | 12 |
| 6.2.4 Protection Class 2..... | 13 |
| 6.2.5 Protection Class 3..... | 14 |
| 6.2.6 Protection Class 4..... | 16 |
| 6.2.7 Cabinets and arrangement of cabinets..... | 17 |
| 7 Protection Class against fire events igniting within data centre spaces | 17 |
| 7.1 General..... | 17 |
| 7.1.1 Protection Classes..... | 17 |
| 7.1.2 Fire compartments and barriers..... | 18 |
| 7.1.3 Fire detection and fire alarm systems..... | 19 |
| 7.1.4 Fixed fire fighting systems..... | 19 |
| 7.1.5 Portable fire fighting equipment..... | 20 |
| 7.1.6 Structural considerations..... | 21 |
| 7.2 Implementation of Protection Class requirements..... | 21 |
| 7.2.1 Protection Class 1..... | 21 |
| 7.2.2 Protection Class 2..... | 21 |
| 7.2.3 Protection Classes 3 and 4..... | 21 |
| 8 Protection Class against environmental events (other than fire) within data centre spaces | 22 |
| 8.1 Protection Classes..... | 22 |
| 8.2 Implementation..... | 22 |
| 8.2.1 General..... | 22 |
| 8.2.2 Protection Class 1..... | 23 |
| 8.2.3 Protection Class 2..... | 23 |
| 8.2.4 Protection Class 3..... | 23 |
| 8.2.5 Protection Class 4..... | 24 |
| 9 Protection Class against environmental events outside the data centre spaces | 24 |
| 9.1 Protection Classes..... | 24 |
| 9.2 Implementation..... | 24 |
| 9.2.1 General..... | 24 |
| 9.2.2 Protection Class 1..... | 25 |
| 9.2.3 Protection Class 2..... | 25 |
| 9.2.4 Protection Class 3..... | 25 |
| 9.2.5 Protection Class 4..... | 25 |

| | | |
|-----------|--|-----------|
| 10 | Systems to prevent unauthorized access | 25 |
| 10.1 | General..... | 25 |
| 10.2 | Technology..... | 26 |
| 10.2.1 | Security lighting..... | 26 |
| 10.2.2 | Video surveillance systems..... | 26 |
| 10.2.3 | Intruder and holdup alarm systems | 27 |
| 10.2.4 | Access control..... | 27 |
| 10.2.5 | Alarm monitoring..... | 27 |
| | Annex A (informative) Pressure relief: Additional information | 28 |
| | Bibliography | 30 |

Foreword

ISO (the International Organization for Standardization) and IEC (the 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 through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 39, *Sustainability for and by Information Technology*.

A list of all parts in the ISO/IEC TS 22237 series can be found on the ISO website.

Introduction

The unrestricted access to internet-based information demanded by the information society has led to an exponential growth of both internet traffic and the volume of stored/retrieved data. Data centres are housing and supporting the information technology and network telecommunications equipment for data processing, data storage and data transport. They are required both by network operators (delivering those services to customer premises) and by enterprises within those customer premises.

Data centres need to provide modular, scalable and flexible facilities and infrastructures to easily accommodate the rapidly changing requirements of the market. In addition, energy consumption of data centres has become critical both from an environmental point of view (reduction of carbon footprint) and with respect to economical considerations (cost of energy) for the data centre operator.

The implementation of data centres varies in terms of:

- a) purpose (enterprise, co-location, co-hosting, or network operator);
- b) security level;
- c) physical size;
- d) accommodation (mobile, temporary and permanent constructions).

The needs of data centres also vary in terms of availability of service, the provision of security and the objectives for energy efficiency. These needs and objectives influence the design of data centres in terms of building construction, power distribution, environmental control and physical security. Effective management and operational information is required to monitor achievement of the defined needs and objectives.

The ISO/IEC TS 22237 series specifies requirements and recommendations to support the various parties involved in the design, planning, procurement, integration, installation, operation and maintenance of facilities and infrastructures within data centres. These parties include:

- 1) owners, facility managers, ICT managers, project managers, main contractors;
- 2) architects, consultants, building designers and builders, system and installation designers;
- 3) facility and infrastructure integrators, suppliers of equipment;
- 4) installers, maintainers.

At the time of publication of this document, the ISO/IEC TS 22237 series will comprise the following documents:

ISO/IEC TS 22237-1, *Information technology — Data centre facilities and infrastructures — Part 1: General concepts*;

ISO/IEC TS 22237-2, *Information technology — Data centre facilities and infrastructures — Part 2: Building construction*;

ISO/IEC TS 22237-3, *Information technology — Data centre facilities and infrastructures — Part 3: Power distribution*;

ISO/IEC TS 22237-4, *Information technology — Data centre facilities and infrastructures — Part 4: Environmental control*;

ISO/IEC TS 22237-5, *Information technology — Data centre facilities and infrastructures — Part 5: Telecommunications cabling infrastructure*;

ISO/IEC TS 22237-6, *Information technology — Data centre facilities and infrastructures — Part 6: Security systems*;

ISO/IEC TS 22237-7, *Information technology — Data centre facilities and infrastructures — Part 7: Management and operational information*;

The inter-relationship of the specifications within the ISO/IEC TS 22237 series is shown in [Figure 1](#).

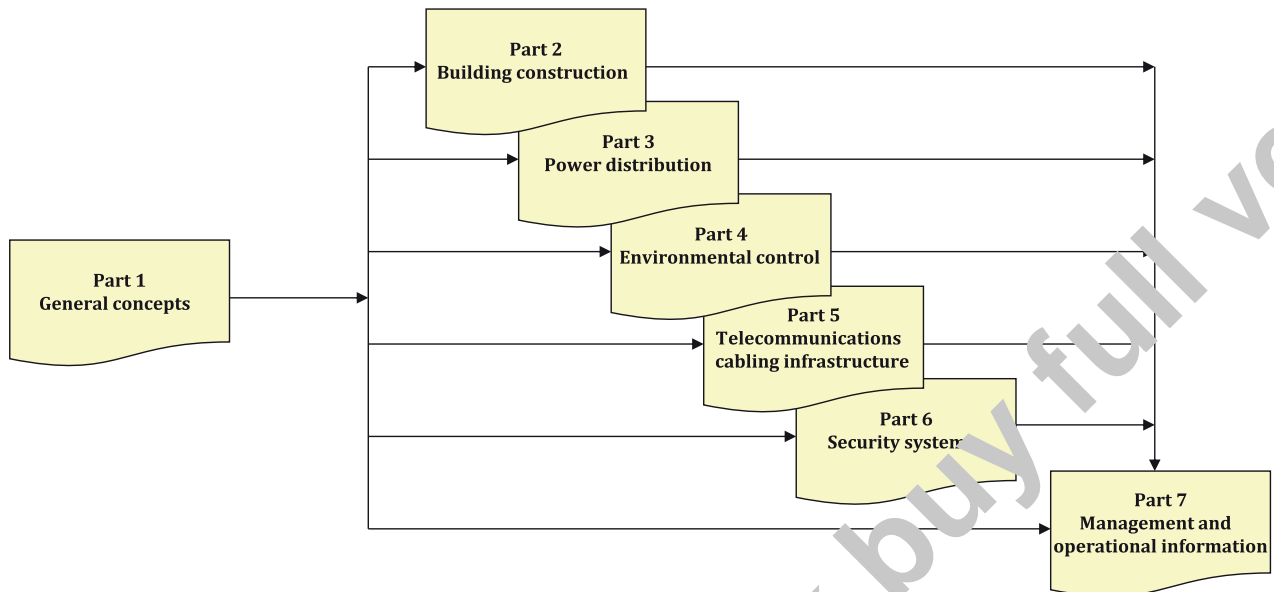


Figure 1 — Schematic relationship between the ISO/IEC TS 22237 series of documents

ISO/IEC TS 22237-2 to ISO/IEC TS 22237-6 specify requirements and recommendations for particular facilities and infrastructures to support the relevant classification for “availability”, “physical security” and “energy efficiency enablement” selected from EN 50600-1.

This document, addresses the physical security of facilities and infrastructure within data centres together with the interfaces for monitoring the performance of those facilities and infrastructures in line with ISO/IEC TS 22237-7 (in accordance with the requirements of ISO/IEC TS 22237-1).

ISO/IEC TS 22237-7 addresses the operational and management information (in accordance with the requirements of ISO/IEC TS 22237-1).

This document is intended for use by and collaboration between architects, building designers and builders, system and installation designers and security managers among others.

The ISO/IEC TS 22237 series does not address the selection of information technology and network telecommunications equipment, software and associated configuration issues.

Information technology — Data centre facilities and infrastructures —

Part 6: Security systems

1 Scope

This document addresses the physical security of data centres based upon the criteria and classifications for “availability”, “security” and “energy efficiency enablement” within ISO/IEC TS 22237-1.

This document provides designations for the data centre spaces defined in ISO/IEC TS 22237-1.

This document specifies requirements and recommendations for those data centre spaces, and the systems employed within those spaces, in relation to protection against:

- a) unauthorized access addressing constructional, organizational and technological solutions;
- b) fire events igniting within data centre spaces;
- c) other events within or outside the data centre spaces, which would affect the defined level of protection.

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

2 Normative references

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

ISO/IEC TS 22237-1, *Information technology — Data centre facilities and infrastructures — Part 1: General concepts*

ISO/IEC TS 22237-2:2018, *Information technology — Data centre facilities and infrastructures — Part 2: Building construction*

ISO/IEC TS 22237-3, *Information technology — Data centre facilities and infrastructures — Part 3: Power distribution*

ISO/IEC TS 22237-4, *Information technology — Data centre facilities and infrastructures — Part 4: Environmental control*

ISO/IEC TS 22237-5, *Information technology — Data centre facilities and infrastructures — Part 5: Telecommunications cabling infrastructure*

IEC 60839-11-1, *Alarm and electronic security systems — Part 11-1: Electronic access control systems — System and components requirements*

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

EN 3 (all parts), *Portable fire extinguishers*