

PAS 185:2023

Connected places – Establishing and implementing a security-minded approach – Specification



National Protective
Security Authority



bsi
Documents
Document Sharing Hub

Publishing and copyright information

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

© The British Standards Institution 2023. Published by BSI Standards Limited 2023.

ISBN 978 0 539 21725 4

ICS 13.020.20

No copying without BSI permission except as permitted by copyright law.

Publication history

First published November 2017

Second edition July 2023

Contents

Foreword	ii
0 Introduction.....	iv
1 Scope.....	1
2 Normative references	2
3 Terms, definitions and abbreviations	3
4 The security-minded approach	10
5 Understanding the security context.....	12
6 Developing a security strategy	16
7 Developing a security management plan	21
8 Security breach/incident management plan (SB/IMP)	33
9 Sharing and publication of data and information	36
10 Connected place projects	42
Bibliography	43
List of figures	
Figure 1 – The integration of the security-minded approach	iv
Figure 2 – The process for developing a risk management strategy	18
Figure 3 – Generic data and information lifecycle	25
Figure 4 – Technical security considerations for the place data and information	31
Figure 5 – Data and information security triage process.....	37
Figure 6 – Personal data test	38

Foreword

This PAS was sponsored by the National Protective Security Authority (NPSA). Its development was facilitated by BSI Standards Limited, and it was published under licence from The British Standards Institution. It came into effect on 31 July 2023.

Acknowledgement is given to Alexandra Luck and Hugh Boyes, as the technical authors of the original PAS, Alexandra Luck as technical author for this revision, and to the following organizations that were involved in the development of this PAS as members of the Steering Group:

- A Luck Associates
- Aon
- Bodvoc Ltd
- City of Bradford CDC
- Department for Digital, Culture, Media & Sport (UK)
- FlyingBinary Limited
- The Institute of Asset Management
- IoT Security Foundation
- National Protective Security Authority (NPSA)
- Ove Arup & Partners Ltd

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

The British Standards Institution retains ownership and copyright of this PAS. BSI Standards Limited as the publisher of the PAS reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This PAS will be reviewed at intervals not exceeding two years.

This PAS is not to be regarded as a British Standard. It will be withdrawn in the event it is superseded by a British Standard.

The PAS process enables a standard to be rapidly developed in order to fulfil an immediate stakeholder need. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or international standard.

Supersession

This PAS supersedes PAS 185:2017, which is withdrawn.

Relationship with other publications

This PAS is issued as part of a suite of BSI publications related to connected places:

- BS ISO 37100, *Smart cities – Vocabulary* defines terms for smart cities, including smart cities concepts, across different infrastructure and systems elements and used across all service delivery channels;
- BS ISO 37106, *Sustainable cities and communities – Guidance on establishing smart city operating models for sustainable communities* gives guidance on a good practice framework for decision-makers in smart cities and communities (from the public, private and voluntary sectors) to develop, agree and deliver smart city strategies that can transition their city's ability to meet future challenges and deliver future aspirations;
- BS ISO/IEC 30182, *Smart city concept model – Guide to establishing a model for data interoperability* provides a framework that can normalize and classify information from many sources so that data sets can be discovered and combined to gain a better picture of the needs and behaviours of a city's citizens (residents and businesses);
- PAS 183, *Smart cities – Guide to establishing a decision-making framework for sharing data and information services*, gives guidance for decision-makers from the public, private and third sectors on establishing a framework which can support the sharing of city data and the creation of interoperable information services;
- PAS 184, *Smart cities – Developing project proposals for delivering smart city solutions – Guide*, which provides guidance, illustrated with case studies, on how good practice described in other BSI smart city publications can be applied when developing an individual project proposal within the broader smart city programme;

- PAS 186, *Smart cities – Supplying data products and services for smart communities – Code of practice*, helps embed good practice in the design of smart city data products and services; and
- PD 8100, *Smart cities overview – Guide* gives guidance on how to adopt and implement smart city products and services in order to facilitate the rapid development of an effective smart city.

Information about this document

This is a full revision of the document, and introduces the following principal changes:

- clarification around, and the addition of, referencing guidance that has been published since the last version of the PAS was published;
- updating definitions, as PAS 1192-5 has been superseded by BS EN ISO 19650-5;
- amendments to reflect the increasing use of the term “connected place”, replacing “smart city” with “connected place” throughout;
- reflecting the type of new initiatives that a connected place might interact with – for example, mapping of underground assets and actions to meet carbon net zero; and
- adding links to new guidance available through the National Cyber Security Centre (NCSC).

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at bsigroup.com/standards, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Presentational conventions

The provisions of this document are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the principal auxiliary verb is “shall”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of the *Shorter Oxford English Dictionary* is used (e.g. “organization” rather than “organisation”).

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient’s own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.

Particular attention is drawn to the following specific Acts and regulations:

- Data Protection Act 2018 [1]
- Environmental Information Regulations 2004 [2]
- Freedom of Information Act 2000 [3]
- Freedom of Information (Scotland) Act 2002 [4]
- UK General Data Protection Regulation (UK GDPR) [5]

0 Introduction

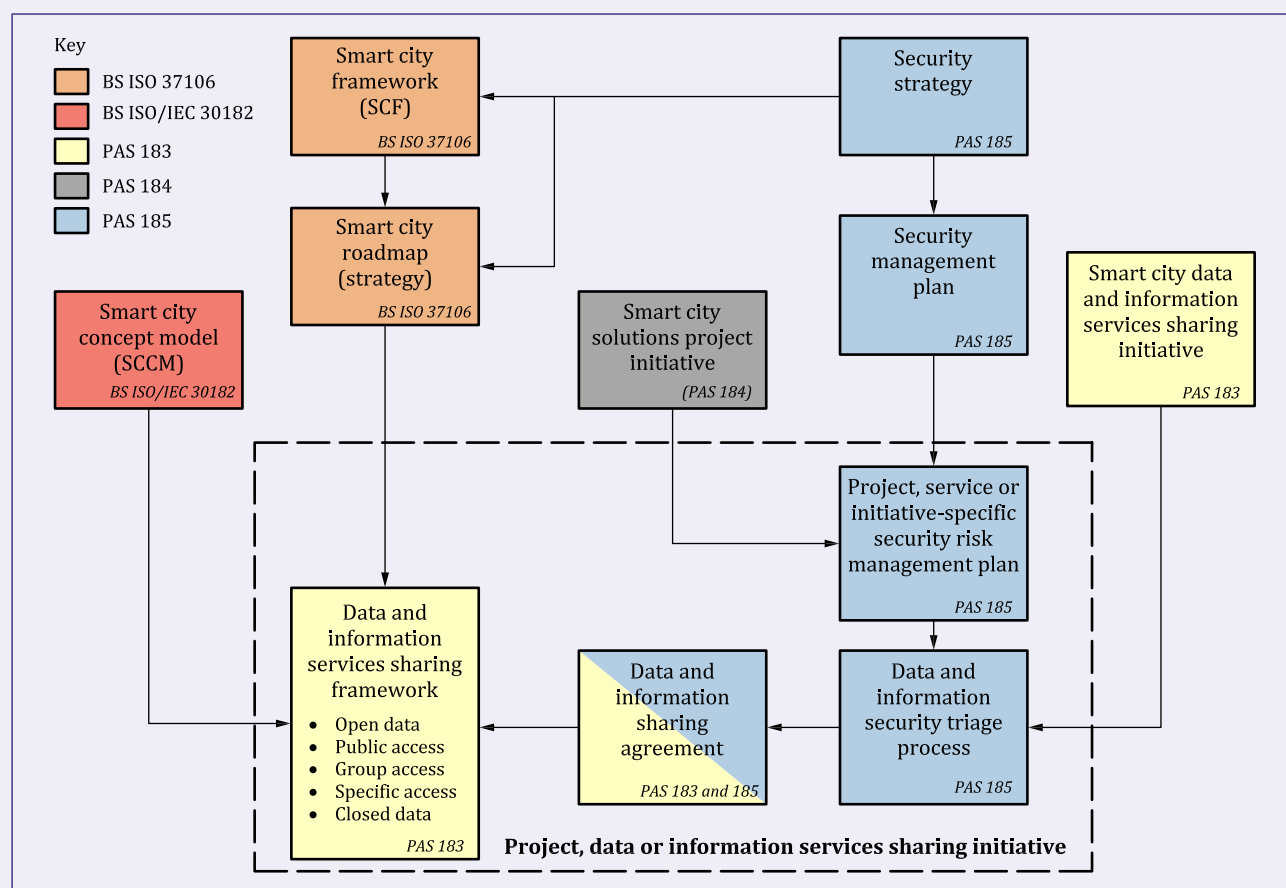
PAS 185 is a companion document to:

- BS ISO 37100, *Smart cities – Vocabulary*;
- BS ISO 37106, *Sustainable cities and communities. Guidance on establishing smart city operating models for sustainable communities*;
- BS ISO/IEC 30182, *Smart city concept model – Guidance to establishing a model for data interoperability*;
- PAS 183, *Smart cities – Guide to establishing a decision-making framework for sharing data and information services*;
- PAS 184, *Smart cities – Developing project proposals for delivering smart cities solutions – Guide*;
- PAS 186, *Smart cities – Supplying data products and services for smart communities – Code of practice*; and
- PD 8100, *Smart cities overview – Guide*.

It makes reference to the definitions and concepts contained within these publications and complements them by showing how a place-wide, strategic-level, security-minded approach can be applied alongside the development of a smart city framework, a smart city strategy and roadmap, frameworks for sharing data and information services projects, programmes and initiatives.

PAS 185 uses connected place rather than smart city, as this is the phrase now more commonly used in the UK, recognizing that it is not only urban areas that can deploy and benefit from digital technologies and cyber-physical systems. Rural communities can benefit from these in a range of uses, such as environmental monitoring, healthcare and predictive road maintenance. The relationship of PAS 185 to the key concepts set out in each of these companion documents is shown in Figure 1.

Figure 1 – The integration of the security-minded approach



A security-minded approach comprises the routine application of appropriate and proportionate security measures to deter and/or disrupt hostile, malicious, fraudulent and criminal behaviours or activities. Further, it considers security holistically, looking at people, physical, technical (including cyber) and data and information security and cross-cutting issues and solutions. In a connected place, developing and implementing a security-minded approach is supported through the security strategy, security management plan and associated documentation and processes as shown in Figure 1.

PAS 185 is also consistent with the approach set out in BS EN ISO 19650-5, which relates to security-minded information management at a stage of maturity described as “building information modelling” (BIM), as well as the security-minded management of sensitive information that is obtained, created, processed and stored as part of, or in relation to, any other initiative, project, asset, product or service. This consistency allows the appropriate sharing and disclosure of geospatial, dynamic and asset information in order to support service planning, development and delivery of assets and services in connected places.

In a connected place, digital technologies and cyber-physical systems will help to deliver new services to the built environment and enhance the quality of living for citizens. A system of sensors, networks, and applications can also be used to collect data to improve operations, including transportation, buildings, utilities, environment, infrastructure, and public services. It therefore provides a range of critical functions and services.

Joining up specific vertical sectors (e.g. utilities, transport, health) across organizational boundaries to improve the creation, delivery and use of spaces and services can enable the relevant organizations to:

- a) take better account of the needs of current and future citizens;
- b) integrate physical and digital planning;
- c) more efficiently and sustainably identify, anticipate and respond to emerging challenges, including emergency situations; and
- d) increase the capacity for service delivery and innovation which in turn has the capability to drive efficiencies and effectiveness.

However, increased use of, and dependence on digital technologies and cyber-physical systems, especially when coupled with much wider sharing and use of data and information, creates significant vulnerabilities and associated security issues. Threat actors are associated with:

- 1) organized crime;

- 2) unauthorized acquisition of personal data, intellectual property and commercially sensitive data or information;
- 3) terrorism; and
- 4) malicious acts, including sabotage and insider attack, which disrupt or corrupt information and/or systems, might seek to make use of these vulnerabilities in order to compromise the value, longevity and ongoing use of a place's built assets and services, as well as the safety, security, privacy and trust of citizens.

The security-minded approach developed differs from any security-minded policies and processes that might already be in place within an individual local authority or other service delivery organization as it needs to respond to new or enhanced vulnerabilities which include:

- i) the increase in volume of data and information being generated, collected, utilized and stored, including personal data, intellectual property and commercially sensitive data and information;
- ii) greater sharing and dissemination of data and information within and across organizations with various existing contractual arrangements in place;
- iii) the potential aggregation of data and information from a wider range of sources; and
- iv) potential differing organizational priorities, governance arrangements, policies and processes, security understanding and concerns, and risk appetite.

However, it is essential that the security-minded approach adopted is appropriate and proportionate to the risks and does not prevent delivery of the place's aims. It is important that, in addition, individual organizational security-minded policies and processes support and complement this wider approach, where applicable.

If the connected place is to gain, and maintain, the trust of its citizens it needs to be capable of responding to increasing citizen awareness and potential concerns about how their personal data are being used and put in place mechanisms that have the potential to prevent trust from being abused.

While this PAS is specifically written for connected place decision-makers and data officers, whether from the public, private or third sectors, it might also be of relevance to those who are interested in utilizing data and information to deliver connected place objectives effectively.

This page is deliberately left blank.

1 Scope

This PAS specifies the principles and requirements for developing and implementing a security-minded approach within a connected place to address the security risks that arise from the increased use of, and dependence on, digital technologies and cyber-physical systems, and from the wider sharing and use of data and information.

The approach outlined in this PAS enables the development of an overall security strategy and management plan for the deployment of sensors, networks, and applications as well as for the handling, management and sharing of data and information. It can be used to inform and guide the development and delivery of connected place projects and subsequent operation, delivery, evolution and disposal of assets and services.

This framework can be used to create and cultivate an appropriate, risk-based safety and security mindset and culture across the many organizations, services and individuals which use shared, disclosed and derived data, and includes the need to monitor and audit compliance.

It covers the use of trustworthiness and security controls applicable to the smart city framework (SCF) (see BS ISO 37106), smart city concept model (SCCM) (see BS ISO/IEC 30182) and data framework used for sharing data and information services (see PAS 183).

This PAS is for use by decision-makers in connected places from the public, private and third sectors and for place data officers. It might also be of relevance to those who are interested in utilizing data and information to deliver connected place objectives effectively.

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.

Standards publications

PAS 183, *Smart cities – Guide to establishing a decision-making framework for sharing data and information services*

Other publications

[N1] NATIONAL CYBER SECURITY CENTRE (NCSC). *Digital service security – Guidance*. October 2016.¹⁾

¹⁾ Available from: <https://www.ncsc.gov.uk/guidance/digital-service-security>

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this PAS, the following terms and definitions apply.

3.1.1 asset

item, thing or entity that has potential or actual value to an organization

[SOURCE: BS ISO 55000:2014, 3.2.1]

NOTE 1 An asset can be fixed, mobile or movable. It can be an individual item of plant, a system of connected equipment, a space within a structure, a piece of land, an entire piece of infrastructure, an entire building, or a portfolio of assets.

NOTE 2 An asset might also comprise data or information in digital or in printed form, as well as an organization's internal processes.

NOTE 3 The value of an asset might vary throughout its life and an asset might still have value at the end of its life. Value can be tangible, intangible, financial and non-financial.

3.1.2 asset data

data relating to the specification, design, construction or acquisition, operation and maintenance, and disposal or decommissioning of an item, thing or entity that has potential or actual value to an organization

3.1.3 asset information

information relating to the specification, design, construction or acquisition, operation and maintenance, and disposal or decommissioning of an item, thing or entity that has potential or actual value to an organization

NOTE Asset information can include design information and models, documents, images, software, spatial information and task or activity-related information.

3.1.4 built asset

building, multiple buildings (e.g. a site or campus) or built infrastructure (e.g. roads, railways, pipelines, dams, docks, etc.) that is the subject of a construction project or comprises an existing asset

NOTE 1 The built asset can include associated land or water, for example, the catchment area for a water company or the navigation channels for a dock.

NOTE 2 The built asset can comprise a portfolio or network of assets.

3.1.5 citizen

resident in, business or other organization in, or visitor or commuter to the place

3.1.6 closed data

data that has been restricted for use

[SOURCE: PAS 183:2017, 2.1, modified]

NOTE 1 Use of data might be restricted as a result of legal, regulatory or confidentiality requirements, with sharing either not permitted or only permissible under specified circumstances and/or with specified user organizations.

NOTE 2 Examples of closed data include:

- a) configuration of systems assets, for example system architectures, IP addresses, firewall rules, equipment locations, physical access controls, etc. which can be shared with systems integrators, support contractors and system accreditors; and
- b) payment details, citizens' council tax histories and details of their housing benefit claims, which can be shared with government departments and law enforcement agencies for the purposes of prevention and detection of crime (e.g. fraud).

3.1.7 closed information

information that has been restricted for use

NOTE Use of information might be restricted as a result of legal, regulatory or confidentiality requirements, with sharing either not permitted or only permissible under specified circumstances and/or with specified user organizations.

3.1.8 connected place

community that integrates digital technologies and cyber-physical systems to collect and analyse data to deliver new services to the built environment, and enhance the quality of living for citizens

NOTE When considering elements such as transport, air quality etc., the connected place could potentially cross place and regional boundaries.

3.1.9 connected place decision-makers

legal person (i.e. an individual, company, or other entity which has legal rights and is subject to obligations) in public, private or third sectors with responsibility, within the connected place, for setting the strategy, specification, development and deployment of solutions, managing the required ongoing operation of assets and services, or providing a regulatory function

NOTE Connected place decision-makers are appointed by the connected place leaders or service providers to exercise the legal rights and fulfil the obligations of their respective organization. They might include representatives from organizations outside of place, for example those responsible for regional transport and environmental issues. The connected place governance arrangements therefore need to take account of the differing legal, financial and commercial responsibilities of these different decision-makers

3.1.10 connected place organization

organization that has a role in managing the place and its services

NOTE Examples of connected place organizations include a local authority, police, fire and rescue, health service, etc.

3.1.11 context

circumstances that form the setting for data or information, and in terms of which they can be understood or interpreted

3.1.12 controlled data

data to which access has been limited to those who need to know in order to fulfil their official duties

3.1.13 controlled information

information to which access has been limited to those who need to know in order to fulfil their official duties

3.1.14 controller

competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data

[SOURCE: Data Protection Act 2018 [1], Section 32(1)]

3.1.15 cyber hygiene

conditions and practices that serve to promote or preserve cyber safety and security by individual system users

NOTE Good cyber safety and security practices are not dissimilar to good health practices related to infection and disease control, i.e. taking appropriate steps to prevent infection (e.g. malware), seeking advice in the case of a suspected infection, and when infection occurs, isolating it or taking steps to prevent further spread.

3.1.16 cyber-physical system

system that includes engineered interacting networks of physical and computational components

[SOURCE: ISO/IEC TR 15067-3-8:2020, 3.8 modified]

NOTE In a cyber-physical system, embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa.

3.1.17 data

series of marks, digital or analogue signals or encoded characters stored or transmitted electronically

NOTE 1 Marks can include writing, printed characters or graphics.

NOTE 2 There are alternative definitions of data; this specific definition builds on that contained in PAS 183 and is being used in the context of security-mindedness.

NOTE 3 Analogue data varies continuously and relates to natural phenomena such as sounds, natural light, river levels, waves and time. It can also include images such as sketches, drawings and text which have been produced by hand rather than using digital technologies.

NOTE 4 Digital data is represented as binary digits (bits) that have only two states, 0 and 1. This data can be a digital representation of analogue data, captured through a quantization process, or data that was created in digital form, for example as a result of a computer process or by entry using a human interface device (keyboard, touchscreen, stylus, etc.).

NOTE 5 The distinction between data and information is that data does not need to have any meaning attached to it; data becomes information via context.

3.1.18 data and information sharing agreement

set of rules to be adopted by the various organizations involved in a data and/or information sharing operation

3.1.19 data sharing

provision of data from one or more organizations to a third-party organization or organizations, the reciprocal exchange of data between organizations, or the sharing of data between different parts and/or systems of the same organization

[SOURCE: ICO's *Data sharing code of practice* [6], October 2021, modified]

NOTE 1 There are two main types of data sharing:

- a) *systematic, routine data sharing where the same data sets are shared between the same organizations, or parts of an organization, for an established purpose; and*
- b) *exceptional, one-off decisions to share data, for example, in unexpected or emergency situations, the provision of medical or social care data to emergency service first responders when they are responding to an incident.*

NOTE 2 Data sharing might take place implicitly as well as explicitly with outsourced services via the use of cloud services where appropriate security measures are not in place.

3.1.20 digitally excluded citizen

individual with inability to interact with the online world fully, when, where and how they need to

[SOURCE: Digital Poverty Alliance, modified]

3.1.21 disclosure

action of making sensitive, classified or closed data and/or information known

3.1.22 hostile reconnaissance

activity of acquiring information about a target with the view to planning to attack, compromise, disrupt or destroy that target

NOTE 1 The target might be an individual, organization, enterprise or built asset, in whole or in part.

NOTE 2 The planned hostile action might be physical or cyber in nature.

NOTE 3 Reputational damage might result from such hostile physical or cyber actions.

3.1.23 information

one or more data items that have a context and therefore convey a message or meaning

NOTE 1 A string of characters might be referred to generally as data; but if these characters are understood by a person or a computer program for example, as someone's name, then the characters convey information. Information always involves the presence of data in some format, on some medium, which could be, for example, a physical document, a document image on a screen, or the contents of an electronic file.

NOTE 2 There are alternative definitions of information, but from a security-mindedness perspective the context can increase sensitivity.

3.1.24 information management

policies, processes, procedures and tasks applied to inputting, processing and generation activities for the purposes of maintaining accuracy, authenticity, confidentiality, availability and integrity of information

3.1.25 information sharing

provision of information from one or more organizations to a third-party organization or organizations, the reciprocal exchange of information between organizations, or the sharing of information between different parts and/or systems of the same organization

[SOURCE: ICO's *Data sharing code of practice* [6], October 2021, modified]

NOTE 1 There are two main types of information sharing:

- a) *systematic, routine information sharing where the same information sets are shared between the same organizations, or parts of an organization, for an established purpose; and*
- b) *exceptional, one-off decisions to share information, for example, in unexpected or emergency situations, the provision of medical or social care data to emergency service first responders when they are responding to an incident.*

NOTE 2 Information sharing might take place implicitly as well as explicitly with outsourced services via the use of cloud services where appropriate security measures are not in place.

3.1.26 near-miss

incident in which a security breach is narrowly avoided, either by chance or through deliberate action

3.1.27 need to know

legitimate requirement of a prospective recipient of information to know, to access, or to possess sensitive information

[SOURCE: BS EN ISO 19650-5:2020, 3.4]

3.1.28 open data

data which anyone is free to access, use, modify and share, subject to requirements that preserve provenance and openness

NOTE 1 Open data is either:

- a) *in the public domain, i.e. the absence of copyright and similar restrictions, whether by default or waiver of all such conditions; or*
- b) *provided under an open licence.*

NOTE 2 Any additional terms accompanying the data (such as terms of use, or patents held by the licensor) should not contradict the work's public domain status or terms of the licence.

3.1.29 open information

information which anyone is free to access, use, modify and share, subject to requirements that preserve provenance and openness

NOTE 1 Open information is either:

- a) *in the public domain, i.e. the absence of copyright and similar restrictions, whether by default or waiver of all such conditions; or*
- b) *provided under an open licence.*

NOTE 2 Any additional terms accompanying the information (such as terms of use, or patents held by the licensor) should not contradict the work's public domain status or terms of the licence.

3.1.30 organization

person or group of people that has its own function with responsibilities, authorities and relationships to achieve its objectives

[SOURCE: BS ISO 55000:2014, 3.1.13]

3.1.31 outsourced service

transfer of service to an outside supplier

NOTE Within a place, services such as public transport provision are often outsourced.

3.1.32 pattern-of-life

identification of habits, routines and preferences of a citizen(s) that enable prediction of future actions and/or behaviour

3.1.33 pattern-of-use

identification of routine actions in the handling, operation and management of assets

NOTE The pattern-of-use of assets could facilitate malicious pattern-of-life analysis by increasing the number of data and information sources that can be combined.

3.1.34 people security

shaping and controlling the environment to promote vigilance and an effective security culture, and to influence and deter those seeking to cause harm

NOTE People security extends principles employed in personnel security to a wider community, including users of a connected place or its services, and to connected place stakeholders. It may employ measures such as security-minded communication to discourage hostile or malicious acts and/or to promote behaviours such as adoption of good cyber hygiene practices.

3.1.35 personal data

information relating to an identified or identifiable living individual

[SOURCE: Data Protection Act 2018 [1], Section 3(2)]

NOTE Further information regarding the protection of personal data as outlined in PAS 183:2017, 7.3.

3.1.36 personnel

individual(s) employed by an organization, including contractors or temporary staff used to fulfil roles that are undertaken by that organization

3.1.37 personnel security

system of policies and procedures that seek to mitigate the risk of personnel exploiting their legitimate access to that organization's assets for unauthorized purposes

NOTE *These measures might be applied to all personnel that have access to, or use, the asset over its lifecycle, including personnel employed within the supply chain used to design, create, operate, decommission or dispose of the asset.*

3.1.38 physical security

multi-layering of different physical measures designed to deter, detect or delay an attack

3.1.39 place data

data held by an organization related to place assets, services and citizens

NOTE *Place data can be held by public authorities (place regional and national), service providers, private and/or third sectors. It might also be subject to access controls.*

3.1.40 place information

information held by an organization related to place assets, services and citizens

NOTE *Place information can be held by public authorities (place, regional and national), service providers, private and/or third sectors. It might also be subject to access controls.*

3.1.41 processing

operation or set of operations which is performed on information, or on sets of information, such as:

- a) collection, recording, organization, structuring or storage;
- b) adaptation or alteration;
- c) retrieval, consultation or use;
- d) disclosure by transmission, dissemination or otherwise making available;
- e) alignment or combination; or
- f) restriction, erasure or destruction

[SOURCE: Data Protection Act 2018 [1], Section 3(4)]

NOTE *While the definition uses the term information, in this PAS the term should be considered to include both data and information*

3.1.42 processor

person who processes personal data on behalf of the controller, other than a person who is an employee of the controller

[SOURCE: Data Protection Act 2018 [1], Section 32 (3)]

3.1.43 referential master data

set of permissible values to be used by other data fields in shared data or information sets

NOTE *Within a connected place, examples of referential master data include the electoral register and Royal Mail Postcode Address File.*

3.1.44 resilience

ability to transform, renew and recover in a timely way in response to adverse events

3.1.45 risk

effect of uncertainty on objectives

[SOURCE: PD ISO Guide 73:2009, 1.1, modified]

NOTE 1 *An effect is a deviation from the expected. It can be positive (sometimes expressed as opportunities), negative (sometimes expressed as threats) or both.*

NOTE 2 *Objectives can have different aspects and categories (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).*

NOTE 3 *Risk is often characterized by reference to potential events and consequences, and their likelihood.*

3.1.46 risk appetite

amount or type of risk that an organization is willing to pursue or retain

[SOURCE: PD ISO Guide 73:2009, 3.7.1.2]

NOTE *In the connected place context, when determining the risk appetite, the needs and perspectives of all of the organizations involved should be taken into account.*

3.1.47 sabotage

deliberate, malicious action carried out with the aim of weakening, obstructing, disrupting, damaging or destroying an asset, activity, service, organization or other entity

NOTE *Sabotage might also be conducted with the aim of enabling the targeting of a secondary event that occurs as a result of the original action, for example, the evacuation of a building arising from the sabotage of a fire alarm.*

3.1.48 security

state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts

[SOURCE: ISO BS EN 19650-5:2020, 3.7]

3.1.49 security breach

infraction or violation of security

[SOURCE: BS ISO 14298:2021, 3.30]

3.1.50 security incident

suspicious act or circumstance threatening security

[SOURCE: BS EN ISO 19650-5:2020, 3.9]

3.1.51 security-minded

understanding and routinely applying appropriate and proportionate security measures in any business situation so as to deter and/or disrupt hostile, malicious, fraudulent and criminal behaviours or activities

[SOURCE: BS EN ISO 19650-5, 3.10]

3.1.52 sensitive data

data, the loss, misuse or modification of which, or unauthorized access to, can:

- a) adversely affect the privacy, welfare or safety of an individual or individuals;
- b) compromise intellectual property or trade secrets of an organization;
- c) cause commercial or economic harm to an organization or country; and/or
- d) jeopardize the security, internal and foreign affairs of a nation

3.1.53 sensitive information

information, the loss, misuse or modification of which, or unauthorized access to, can:

- a) adversely affect the privacy, welfare or safety of an individual or individuals;
- b) compromise intellectual property or trade secrets of an organization;
- c) cause commercial or economic harm to an organization or country; and/or
- d) jeopardize the security, internal and foreign affairs of a nation

[SOURCE: BS EN ISO 19650-5:2020, 3.11]

3.1.54 sensitive personal data

personal data the processing of which constitutes sensitive processing

3.1.55 sensitive processing

processing of:

- a) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- b) genetic data for the purpose of uniquely identifying an individual;
- c) biometric data for the purpose of uniquely identifying an individual;
- d) data concerning health;
- e) data concerning an individual's sex life or sexual orientation; or
- f) personal data as to:
 - 1) the commission or alleged commission of an offence by an individual; or
 - 2) proceedings for an offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of a court in such proceedings

[SOURCE: Data Protection Act 2018 [1], Section 86(7)]

3.1.56 service

work done to meet some administrative, general or public need

NOTE *Within a connected place, a system supplying a public need includes transport, communications and utilities.*

3.1.57 shared data

data where the data owner has the legal authority to share it with one or more organizations, subject to a data or information sharing agreement which specifies that access is granted subject to specific restrictions and, where between different legal entities, is legally enforceable

[SOURCE: PAS 183:2017, 4.3.3, modified]

3.1.58 shared information

information where the information owner has the legal authority to share it with one or more organizations, subject to a data or information sharing agreement that specifies that access is granted subject to specific restrictions and, where between different legal entities, is legally enforceable

[SOURCE: PAS 183:2017, 4.3.3, modified]

3.1.59 shared service

provision of a service by one part of an organization or group, where that service had previously been found in more than one part of the organization or group

3.1.60 smart

application of autonomous, semi-autonomous or automated technology systems, including automated decision-making, to achieve greater utilization of resources, limiting or reducing per capita resource consumption to maintain or improve quality of life

NOTE *Automated decision-making includes human decisions with system support, automated decisions that can be overridden by a human, and fully automated decisions.*

3.1.61 system

collection of interacting, interrelated or interdependent elements forming a collective functioning entity

[SOURCE: ISO/IEC 14776-121:2010, 3.1.96, modified]

3.1.62 technical security

protection of computer, digital technologies and cyber-physical systems from the theft or damage to their hardware, software, data or information, as well as from disruption or misdirection of the services they provide

3.1.63 threat

potential cause of an incident which may result in harm

[SOURCE: ISO 19650-5:2020, 3.13]

3.1.64 vulnerability

weakness that can be exploited to cause harm

[SOURCE: ISO 19650-5:2020, 3.15]

3.2 Abbreviations

CCP	certified cyber professional
CDO	chief data officer
CIO	chief information officer
CISO	chief information security officer
CPD	continuing professional development
CSIR	cyber security incident response scheme
DPA	Data Protection Act 2018
IoT	Internet of Things
OT	operational technology
OWASP	Open Web Application Security Project
SB/IMP	security breach/incident management plan
SIRO	senior information risk owner