PAS 185:2023

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

National Protective Security Authority

bsi.

Publishing and copyright information

ISBN 978 0 539 21725 4

ICS 13.020.20

Publication history

First published November 2017
Second edition July 2023

Contents

List of figures

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.

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This PAS supersedes PAS 185:2017, which is withdrawn.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

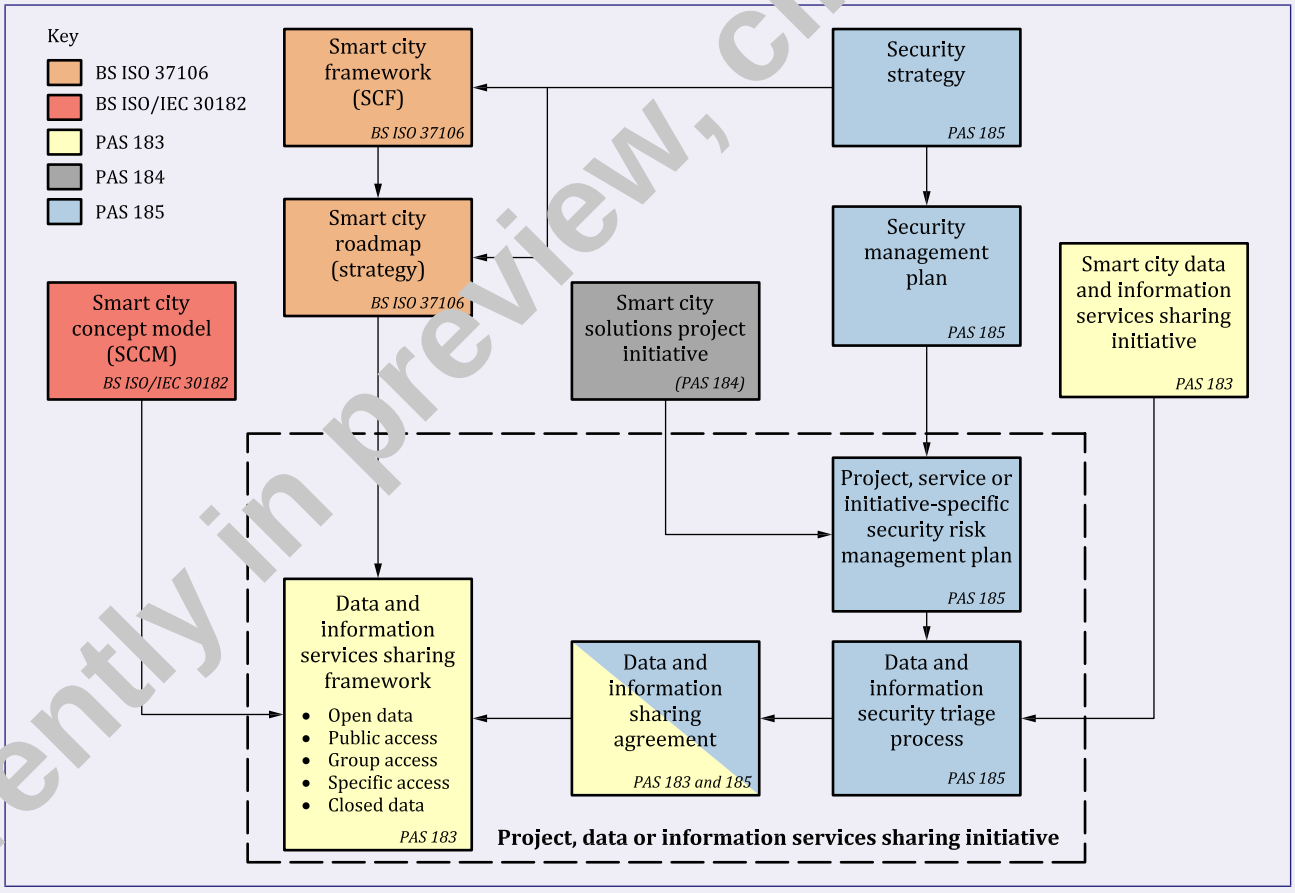
PAS 185 is a companion document to:

- 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 required 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.