National Protective Security Authority

PAS 185:2017

SMART CITIES

SPECIFICATION FOR ESTABLISHING AND IMPLEMENTING A SECURITY-MINDED APPROACH

INTRODUCTION

PAS 185:2017 is a specification for establishing and implementing a citywide, strategic-level, security-minded approach as part of both its development and operation. It details the approach for applying holistic measures that are appropriate and proportionate to the risks and that do not prevent the delivery of a city's aims.

The underlying premise of smart cities is that greater availability of data and information, integration of services and systems, and outcome-based contracting can:

- increase the capacity, efficiency, reliability and resilience, and thereby availability, of existing assets to enable enhanced service provision for its citizens; and
- improve efficiency in design and delivery of new built assets through a better understanding of the whole-life performance of those already in place.

A key purpose of a smart city is to join up specific vertical sectors (e.g. utilities, transport, health, etc.) across organisational boundaries into a whole-city approach for the creation, delivery and use of city spaces and services.

PAS 185 specifies the types of policies and processes that need to be in place across city service delivery organisations in order for the city to respond to the new or enhanced vulnerabilities created by these changes to existing ways of working that could:

1. compromise the value, longevity and ongoing use of a city's built assets and services;

2. compromise a city's citizens;

3. cause harm, damage or distress to individuals or vulnerable groups, including injury, death or social unrest;

4. disrupt or corrupt data, information and/or systems;

5. cause reputational damage; and/or

6. enable acquisition of personal data, intellectual property or commercially sensitive data or information.

PAS 185:2017 was commissioned by the Centre for the Protection of National Infrastructure (NPSA), who provided the technical authors for its development. The British Standards Institution (BSI) facilitated its production with input from a panel of industry experts.

PURPOSE OF THIS BOOKLET

This booklet provides a high-level overview of the key components of PAS 185. The full version of the PAS is available to download at http://shop.bsigroup.com/pas185

WHO IS IT FOR?

PAS 185 is applicable where a service applies to multiple assets and/or data and information is shared or processed by more than one city organisation. While specifically written for smart city decision-makers and smart city data officers, whether from the public, private or third sectors, it is also of relevance to those who are interested in utilising data and information to deliver smart city objectives effectively.

SUMMARY OF THE PAS 185 PROCESS

Create governance structure and appoint smart city decision-makers

Understand new or enhanced smart city-specific security risks

Security risks arise through:

- greater availability of data and information;
- integration of services and systems;
- increased dependency on IT-based systems.

Conduct a city-specific security risk assessment

Decide on appropriate and proportionate mitigation measures commensurate with the city's collective risk appetite

Formally record the risk management process as part of a Smart City Security Strategy

Develop a Smart City Security Management Plan that will allow the mitigation measures to be implemented consistently on a city-wide scale

It should contain policies and processes covering the following aspects of security:

- people
- physical
- data and information
- technological

It should also contain:

- the arrangements for governance of, and accountability and responsibility for, delivery of the security-minded approach;
- the approach to managing the deployment and use of Internet of Things and other distributed technologies; and
- the arrangements for monitoring and auditing the plan's implementation.

Develop a Security Breach/Incident Management Plan

Conduct reviews on a regular basis, as well as in response to significant internal or external changes

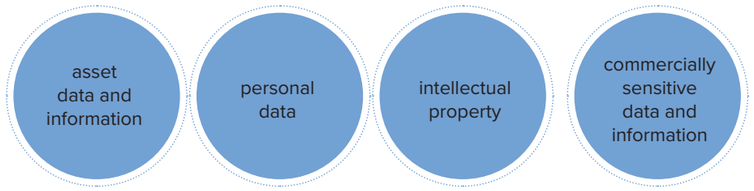
DEVELOPING A SMART CITY SECURITY STRATEGY

The security-minded approach developed within a smart city needs to respond to the vulnerabilities created by changes to more traditional ways of working, and the range of threats that may seek to expolit them, without preventing delivery of the smart city's aims.

WHAT ARE THE NEW VULNERABILITIES THAT ARE CREATED?

In June 2012, the UK Government published its Open Data White Paper **'Unleashing the Potential'** which was aimed at:

- an increase in the volume of data and information being generated and processed, including:



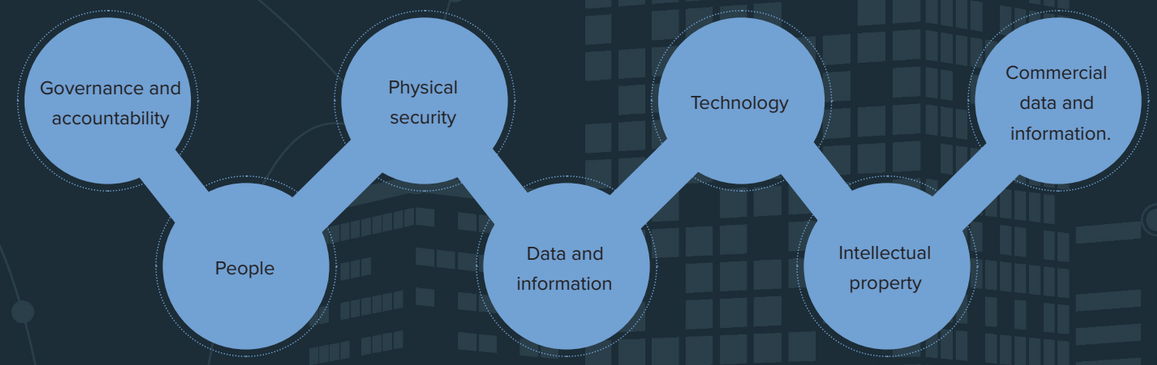
- greater sharing and dissemination of data and information within and across organisations with various existing contractual arrangements in place; the potential aggregation of data and information from a wide range of sources;
- potential differing organisational priorities; governance arrangements; policies and processes; security understanding and concerns; and risk appetite; and
- the use of interfaces to share data between applications which can increase the exposed data, information and systems to attack.

SECURITY RISK MANAGEMENT STRATEGY

ASSESSMENT OF RISK

Where a security-minded approach is adopted, a key component of the process set out in PAS 185 relates to the management of risk. The smart city decision-makers need to assess potential vulnerabilites and threats, in combination with an assessment of the nature of harm that could be caused.

The assessment needs to identify high level security risks associated with:



Available at https://theodi.org/about-the-odi/the-data-spectrum/

CONTENTS OF A SMART CITY SECURITY STRATEGY

The Smart City Security Strategy should comprise a record of:

- The smart city security risk management strategy;
- A list of those to be informed of residual risks;
- The mechanisms for reviewing and updating the strategy.

RISK MITIGATION

For each identified risk it will be necessary to assess possible mitigation measures. The process should consider and record:

- The cost of the measure and its implementation;
- The organisation(s) responsible for implementing the measure;
- The achievable risk reduction;
- The predicted cost saving;
- Other impacts that the measure might have on the city;
- The potential for the measure to create further vulnerabilities;
- Delivery of any other benefits to the city.

RESIDUAL RISKS

It is important for any residual risks to be reassessed and put through the risk mitigation process until they fit within the city's risk appetite.

REVIEW

Periodic reviews should be undertaken to identify and assess any security risks that have changed for political, economic, social, technological, legal or environmental reasons.

SMART CITY SECURITY MANAGEMENT PLAN

The Smart City Security Management Plan sets out the policies and processes that allow the mitigation measures identified in the Smart City Security Strategy to be implemented and managed consistently across the city.

IT SHOULD:

- Be implementable on a city-wide scale;
- Be implementable within the organisational complexity and the extent of autonomy that exists within a smart city;
- Not prevent efficient and effective response to incidents, security breaches, events or any fast-occurring change in risk level.

IT SHOULD INCLUDE:

- arrangements for governance of, and accountability and responsibility for, delivery of the security-minded approach;
- the process for embedding the security-minded approach into new or revised contracts;
- the management of the deployment and use of IoT and other distributed technologies;
- arrangements for monitoring and auditing implementation;
- policies and processes relating to the aspects of people, physical, data and information and technological security;
- mechanisms for review and updating; and
- the security-minded approach to individual smart city projects or initiatives.

COVERAGE OF THE POLICIES AND PROCESSES

PEOPLE:

- security competence of staff fulfilling specific roles;
- security screening and vetting;
- induction requirements;
- general security training and awareness;
- role-specific security training; • demobilisation

of personnel and organisations.

PHYSICAL:

- physical security measures at locations processing sensitive data or information;
- protective measures for equipment handling city data and/or information; and
- protective measures for infrastructure supporting data and information sharing and access by citizens.

DATA AND INFORMATION:

- security features required for the city's data and information architecture;
- managing the accuracy, authenticity and long-term utility of city data and information;
- managing the security of data and information that could be used to cause harm to assets, services and/or the city's citizens; and
- data and information sharing and publication.

TECHNOLOGY:

- cyber security of systems and the interconnections and interactions between them;
- interoperability of systems;
- configuration management and change control for systems processing city data and/or information;
- level of software trustworthiness;
- secure retention, deletion, destruction and/or removal of access to city data and information.

EMBEDDING SECURITY

In order to be effective, the security-minded approach must be integrated with other strategic policies, plans, and requirements for the delivery, maintenance and operation of the smart city.

PAS 185 provides a comprehensive framework to help smart cities adopt a security-minded approach to the use of information and data in the built environment.

Acknowledgement

PAS 185 was commissioned by the National Protective Security Authority (NPSA). Acknowledgement for its development is given to the external technical authors Alexandra Luck and Hugh Boyes. Production was facilitated by the British Standards Institution (BSI). In addition, we would like to thank the following contributing organisations:

- Arup
- BIM Task Group
- City of Bradford, Metropolitan District Council
- Bristol City Council
- Cities Standards Institute
- National Protective Security Authority (NPSA)
- Co-opted members
- Department for Transport
- Digital Catapult
- FlyingBinary
- Future Cities Catapult
- Institute of Asset Management
- IoT Security Foundation
- National Cyber Security Centre (NCSC)
- Peterborough City Council
- Trustworthy Software Foundation
- Turner & Townsend
- University of Cambridge, Centre for Smart Infrastructure and Construction
- Co-opted members

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

How to order a copy

Copies of PAS 185 may be downloaded from: http://shop.bsigroup.com/pas185

National Protective Security Authority

Department for Business Innovation & Skills

bsi.

PAS 185:2017
SMART CITIES
SPECIFICATION FOR ESTABLISHING AND IMPLEMENTING A SECURITY-MINDED APPROACH