INTERNATIONAL STANDARD

ISO 37156

First edition
2020-02

Smart community infrastructures — Guidelines on data exchange and sharing for smart community infrastructures

Infrastructures urbaines intelligentes — Cadre directeur pour l'échange et le partage de données pour les infrastructures urbaines intelligentes

Reference number
ISO 37156:2020(E)

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

Published in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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 of 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 www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 268, *Sustainable cities and communities*, Subcommittee SC 1, *Smart community infrastructures*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Community is the crystallization of human technological progress, economic development and social civilization. It is also the basic unit of human economic activities and regional production. Community function and people's daily life are highly dependent on different types of community infrastructure. As the foundation of survival and development, community infrastructure includes energy, water, transportation, waste and information and communication technology (ICT). This community infrastructure provides convenience for urban residents. Therefore, the scientific and effective management of community infrastructure is crucial. It affects the living conditions of citizens, the efficiency of the social economy and the ecological safety of the community. Poor management of community infrastructure causes problems such as environmental pollution, traffic congestion, inadequate urban resources and a weak urban lifeline system. It is incompatible with sustainable development.

Data provide the fundamental basis of effective management. It is a common problem that different organizations or departments govern the data relating to community infrastructure. The existence of information silos across different community infrastructure negatively affects effective and efficient management. Therefore, strengthening the sharing of data is an important activity for smart communities. Standardized data exchange and/or sharing will benefit business collaboration across departments, organisations and communities; it will also improve service capabilities as regards community infrastructure. Furthermore, it will base the management of communities on data and improve outcomes, making communities safer, more hospitable and more liveable.

This document is a reference for governments and other enterprises, organizations and individuals who have a responsibility or need to share data from community infrastructure. This document helps to promote a foundation of information, eliminate isolated information silos and move toward the use of data to make communities smarter. An example of the benefits of implementing this document is the promotion of efficient cooperation by establishing mechanisms for information exchange among different departments within local governments.

This document provides a set of community infrastructure data governance methods and a unified framework of community infrastructure data exchange and sharing, underpinned by privacy and security principles. The purposes of this document are:

— to provide intensive, efficient, convenient, ecological and secure infrastructure for community infrastructure users, consumers or beneficiaries;

— to provide appropriate approaches to the exchange, monitoring, sharing and maintenance of community infrastructure services.

This document relates to smart community infrastructures, and should be used alongside ISO 37101, ISO 37120, ISO 37122, ISO 37123, ISO/TR 37150 and ISO/TS 37151. ISO 37101 contains the requirements for the different types of data which are supported. ISO 37120 provides macro-guidance to cities on how to achieve the United Nations sustainable development goals. Under the macro-guidance from ISO 37101, this document, ISO/TR 37150 and ISO/TS 37151 constitute implementation guidance for smart city infrastructure. This document focuses specifically on data exchange and/or sharing for smart community infrastructures.

In addition, this document should be used with ISO 8000-110, ISO 22745-1 and ISO/IEC 30182.

Smart community infrastructures — Guidelines on data exchange and sharing for smart community infrastructures

1 Scope

This document gives guidelines on principles and the framework to use for data exchange and sharing for entities with the authority to develop and operate community infrastructure.

The guidelines in this document are applicable to communities of any size that are engaged in data exchange and sharing. The specific practices of data exchange and sharing of community infrastructures will depend on the characteristics of each community.

NOTE 1 The concept of smartness is addressed in terms of data exchange and sharing, in accordance with sustainable development and resilience of communities as defined in ISO 37100.

NOTE 2 Annex A outlines useful case studies of data exchange and sharing for community infrastructure.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

BSI PAS 183:2017, *Smart cities — Guide to establishing a decision-making framework for sharing data and information services*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1 Terms relating to smart community infrastructure

3.1.1
community
group of people with an arrangement of responsibilities, activities and relationships

Note 1 to entry: In many, but not all, contexts, a community has a defined geographical boundary.

Note 2 to entry: A city is a type of community.

[SOURCE: ISO 37100:2016, 3.2.2]

3.1.2
community infrastructure
systems of facilities, equipment and services that support the operations and activities of communities

Note 1 to entry: Such community infrastructures include, but are not limited to, energy, water, transportation, waste and information and communication technologies (ICT).

[SOURCE: ISO 37100:2016, 3.6.1]

3.1.3
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: In this document, the concept of organization refers to an entity/institution inside the community that is tasked with implementing the management system, for example the local government. The community identifies an organization that it entrusts with the implementation of this document.

[SOURCE: ISO 37100:2016, 3.2.3]

3.1.4
smart community infrastructure
community infrastructure with enhanced technological performance that is designed, operated and maintained to contribute to sustainable development and resilience of the community

[SOURCE: ISO 37100:2016, 3.6.2, modified — Notes to entry removed.]

3.1.5
smart community infrastructure data
data created, captured, collected or curated from the various sources of smart community infrastructure

3.2 Terms relating to smart community infrastructure data

3.2.1
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.2.2
authenticity
<entity> property of being genuine

3.2.3
data
reinterpretable representation of information in a formalized manner suitable for communication, interpretation or processing

Note 1 to entry: Data can be processed by humans or by automatic means.

[SOURCE: ISO/IEC 2382:2015, 2121272]

3.2.4
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.2.5
metadata
data defining and describing other data

[SOURCE: ISO/IEC 27050-1:2016, 3.19]

3.2.6
reference data
domain and community standardized data objects that define the set of permissible values to be used to populate other data objects

[SOURCE: ISO 5127:2017, 3.1.10.19]

3.2.7
reliability
property of consistent intended behaviour and results

[SOURCE: ISO/IEC 27000:2018, 3.55]

3.2.8
shared data
data that can be accessed within an existing software application as well as between different software applications, that may be executed asynchronously or concurrently

[SOURCE: ISO/IEC 2382:2015, 2122341, modified.]

3.2.9
thematic data
patterns of data within the data framework that are deemed important to support the provision of city services and the four levels of insight in the city

[SOURCE: BSI PAS 183:2017]

3.2.10
data spectrum
differentiation of data assets on the basis of whether they are considered closed, shareable or open

[SOURCE: BSI PAS 183:2017]

3.3 Terms relating to data exchange and sharing for smart community infrastructure

3.3.1
data access
right, opportunity, means of finding, using or retrieving data

[SOURCE: ISO 15489-1:2016, 3.1, modified — original term was 'access'.]

3.3.2
data creator
organization that creates, captures, collects or transforms data for a city or services, for example

[SOURCE: BSI PAS 183:2017]

3.3.3
data owner
designated curator for the community infrastructure data related to a city service

[SOURCE: BSI PAS 183:2017]

3.3.4
data publisher
organization that performs the publication role for community infrastructure data

[SOURCE: BSI PAS 183:2017]

3.3.5
data exchange
accessing, transferring and archiving of data

[SOURCE: ISO/TS 13399-5:2014, 3.7, modified.]

3.3.6
data sharing
providing shared, exchangeable and extensible data to enable community infrastructure

3.3.7
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected – positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential events (ISO Guide 73:2009, 3.5.1.3) and consequences (ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (ISO Guide 73:2009, 3.6.1.1) of occurrence.

[SOURCE: ISO 37100:2016, 3.4.12, modified.]

4 Principles for data exchange and sharing

4.1 General

This document shows the various possibilities for the use of data exchange and sharing for smart community infrastructures. The expectations of communities related to the outputs from and the use of data are often very high. However, it should be noted that there are many different constraints related on the range and validity of the outputs of data exchange and sharing. Examples are data reliability, availability, quality, complex relationships and temporal interpretation of data. Reasonable expectations should be set by smart communities related to the impact achieved as a result of the data exchange and sharing of community infrastructure data.

4.2 Principles

The following principles should be considered:

a) The community infrastructure data should be available to be exchanged and shared.

b) To be effective, the data should be of sufficient quality in order to be useful across smart community infrastructure services, or by more than one organization.

c) The data owner has the accountability and responsibility to ensure the exchange and sharing of the community infrastructure data is enabled.

d) The data creator should maintain the integrity of the community infrastructure data to be exchanged or shared.

e) The security and privacy of the community infrastructure data should be continuously preserved.

f) The data should use spatial methods to achieve the positioning and control of urban infrastructure objects.

g) The data should have temporal information to maintain changes to the community infrastructure for any reason, such as societal, environmental, cultural, strategic and policy changes. Temporal data allows timely interventions when required and supports the tracking of community infrastructure changes to enable smart management and efficiency improvements.

h) A systematic approach to the exchange and sharing of data should be taken, with every data attribute identifiable by a set of mechanisms to facilitate the interoperability of community infrastructures.

i) The city, in its role as the curator of the exchange and sharing of infrastructure data, should ensure that this activity is carried out in an equitable and ethical manner in order to ensure that all parties are treated equally.

5 Type and model for data exchange and sharing

5.1 General

Smart community infrastructure includes energy, water, transport, ICT and waste services. The data addressed in this document are those related to the infrastructures and the built environment which support the community infrastructure.

The development and complexity of the smart community infrastructure and the planning, construction, operation, management and evaluation of the smart community infrastructure information services should be based on the construction, development and utilization of data resources. The data resources used should reflect the physical and operational conditions and interactions which are defined in ISO 37155-1.

Data exchange and sharing takes place between different application services and systems for smart community infrastructure. Different types of data exchange and sharing use different data types and functions.

The data framework for a smart city and community infrastructure is used to classify data as either metadata, reference data or thematic data. The data framework details how current city data assets are transitioned from the existing siloed service provision to the interoperable use of data across the entire data lifecycle.

The collective data assets relate to the data concepts specified in ISO/IEC 30182, and utilizes the classifications of open, shared and closed data within the data spectrum used by the community.

5.2 Types of data

5.2.1 Metadata

Metadata are data which define basic information about data used to verify the provenance and validity of the data to be exchanged and shared. An example of metadata in a smart community data framework is the data relating to the voluntary services organizations who deliver city services on behalf of the city to citizens.

5.2.2 Reference data

Reference data are any data which define the set of permissible values for the data which are to be exchanged or shared. For example, an atmospheric temperature reading at a certain location or video footage for a specific street which can be used for multiple purposes[41].

5.2.3 Thematic data

To deliver services to citizens, thematic data in a community should initially be the data sets and legacy data that are created, processed and managed by community. Examples of thematic data include bus traffic congestion along a specific street or electric power frequency fluctuations and pressure distribution along a specific underground water pipe line. The characteristics of smart community infrastructure, as an integration of sub-systems, should be considered in the thematic data, for example, interaction between infrastructures services, if applicable according to ISO 37155-1.

Data exchange and sharing is primarily conducted between metadata, reference data and thematic data. The data types for data exchange and sharing of smart community infrastructure are described in 5.3.

5.3 Concept model for infrastructure data

Data should be made available and be collectable from community infrastructure services for exchanging and sharing. The collection of data are expected to be automated via technical interfaces, such as smart meters supported by APIs.

Tables 1 to 3 identify the elements of the smart city concept model (SCCM) defined in ISO/IEC 30182 which relate specifically to community infrastructure. Collectable community infrastructure data can be categorized into characteristics of something, consumption of something, movement of something, presence of something, production of something, status of something, supply of something and use of something. These are shown in Table 1. These descriptions are not exhaustive or mutually exclusive.

Table 1 — Example of collectable data from community infrastructure using concepts from SCCM

Collectable data	Infrastructures	Data interfaces	Example observation	Prime concept (SCCM[a])
Characteristics of something	Buildings	Survey	Building use	State
	Transportation network	API for the transportation network data	Structure and design information of the road, bridge or tunnel	Infrastructure
Consumption of something	Street lighting	Smart meters	Energy used per hour (kWh)	Case
Movement of something	Transport network	Vehicle GPS	Journey destinations	Place
Presence of something	Waste management	Waste bin sensors	Empty/full	State
Production of something	Renewable power plant	Smart grid	Energy load per hour (MWh)	Case
Status of something	Public realm	Environmental sensor	Outdoor temperature	State
	Metro/subway	API for the subway data	Operation status of the subway; normal operation, suspension or plan/developing Inspection data of the car and railways	State/event
Supply of something	Water mains	Flow sensors	Leaks	Case
Use of something	Communication networks	System logs	Megabytes of data used	Event

NOTE Infrastructure is a concept of fundamental facilities and systems serving a country, city or other area. Infrastructure is not defined in SCCM. However, it is a fundamental concept in expressing data exchange and sharing for smart community infrastructure.

[a] SCCM defined in ISO/IEC 30182.

The collected data results in information that provides insights, the types of which are also defined in the SCCM as operational, critical, analytical and strategic. The insights can help identify opportunity and rationale for sharing such data among infrastructures (see Table 2).

Table 2 — Examples of the level of insights (operational, critical, analytical and strategic) for collectable community infrastructure data from SCCM

Collectable data	Resulting data (examples)	Insights (SCCM)
Characteristics of something	Building data: dimensions; occupancy; equipment; indoor temperature; indoor air quality; gas supply pressure; water flow rates; heat delivery temperature Demographic data: user registration details and profile Structure or design data: position, dimensions and materials; load-bearing capacity; functions included in the object; route to exit	Operational Strategic
Consumption of something	Energy data: domestic use of electric, thermal, gas; district consumption; tariffs and costs	Critical
Movement of something	Transport data: modal mix; vehicle type; vehicle ID; vehicle occupancy; journey start/end times and locations; traffic speed and density; pedestrian movements; energy consumption per km; emissions/pollutants per km	Analytical
Presence of something	Image data: congestion; integrity of the public realm, such as road maintenance; incidents; unrest and community safety	Strategic
Production of something	Energy data: local renewable production	Critical
Status of something	Environmental data: outdoor air quality; water quality; flood levels; noise levels; temperature; weather conditions; carbon emissions; luminescence Operation status data: status of planning, construction, operation, suspension, stopped; period of time for the status Inspection data: method/person in charge of inspection; data inspected; judgement result	Analytical
Supply of something	Energy data: network power loads	Critical
Use of something	Network utilization: number of bus journeys taken	Strategic

The observations are also related to concepts defined in the SCCM, including active agents or items, metrics and places. The SCCM notes that by adding the concepts of time and role to the collectable data, it would be possible to further understand relationships in the sharing of data (see Table 3).

Table 3 — Examples of observations which can be used to further understand relationships to be shared or exchanged

Collectable data	Agent/item (SCCM)	Metric (SCCM)	Place (SCCM)	Time	Stakeholder roles[a]
Characteristics of something Consumption of something Movement of something Presence of something Production of something Status of something Supply of something Use of something	Person or household Building, infrastructure or community Government or municipality	Cost Frequency Quantity Scale Specification State Velocity Life expectancy	Location points Departure points Arrival points Transit routes Neighbourhoods Districts Cities	Date/time stamp	Infrastructure owners, suppliers and operators Investors Planners Citizens

[a] Stakeholders are defined in ISO 37153.

5.4 Data dictionary and catalogue

Data dictionaries and the use of a catalogue for data exchange and sharing can be considered as an efficient approach to assist the exchange and sharing of different attributes, for example by industry, structure, format and classification. These tools are optional and not limited to the approaches listed below.

a) Data dictionary is the definition and description of the data items, data structures, data streams, data storage, processing logic and external entities that constitute the data resources of a domain.

b) Data catalogue is the presentation of data resource organization and relevance, including catalogue, dictionary identification scheme and development of guidelines related to recognition system. The form is based on open technical dictionary (OTD) databases as the core.

The expected architecture if these tools are used is based on the OTD of ISO 8000 and the ISO 22745 series, for creation and maintenance of the data.

5.5 Data spectrum

5.5.1 General

To better understand how a community can maximize the value of its data, it is important that the data framework classifies data for use. Data should be differentiated to classify the type of data held and whether they are considered closed, shareable or open. The extent to which restrictions have been implemented can vary depending on the security, access and control requirements. The use of data within the data spectrum is restricted to the use, reuse and the purpose for which data can be shared. ISO 31000 outlines good practice on the management, assessment and analysis of risk and can be used by the community when implementing the data framework.

An appropriate risk-management regime for the sharing, publishing and reuse of data should be established and implemented.

5.5.2 Closed data

Closed data are data which are restricted for use. These data should be designated as information that is not permitted to be shared. In a community, these data are mainly related to privacy and security concerns, for example payment details for citizens for a specific infrastructure service, such as their council tax.

5.5.3 Shared data

Shared data are data which exist and cannot be considered as either open or closed. This varies between cities and is assumed to represent the majority of the data in a community.

This document specifies in detail on:

- the suitability of sharing data for new purposes (see Clause 8); and
- access rights to data (see Clause 9).

It is important as part of the data spectrum to understand that there are three top-level access restrictions which apply to shared data:

a) specific access is when the data owner makes data accessible to either named individual(s) or named organization(s);

b) group access is when data are made available to specific groups of people or organization(s) based on predetermined criteria;

c) public access is when data are made available publicly but only under certain terms and conditions that cannot be considered open.

Publishers of community data have a duty of care when restricted data are considered for sharing to ensure that potential harm to individuals or assets is considered prior to publication. An example of shared data such as this is control of major accidents and hazards (COMAH) data.

5.5.4 Open data

This document uses the definition of 'open' that is maintained by the Open Project.

'Open data' means data which anyone can freely access, use, modify and share for any purpose (subject at most to guidelines that preserve provenance and openness). This definition is also used to determine whether data can be classified as open data.

6 Opportunities for data exchange and sharing

6.1 General

The availability of open data enables smart communities to explore the value of data to improve city services. However, the majority of data within a smart community is not suitable for opening due to privacy and security considerations. With the appropriate access restrictions, the three types of shared data can be unlocked for the benefit of the city and its citizens. The value of shared data includes, but is not limited to, optimizing infrastructure services, promoting business, facilitating urban planning, enabling proactive maintenance, promoting environmental protection and improving safety and security. A diverse range of options can be articulated for all smart cities when community infrastructure data are shared.

6.2 Optimizing infrastructure services

Data exchange and sharing can provide citizens with better services, including water, gas, electricity, housing, transportation, waste disposal and information services. For example, citizens can have access to one-stop, comprehensive and efficient government information services through data exchange and sharing.

Through data exchange and sharing, city managers and related providers of public services cannot only optimize the construction of community infrastructure, but also improve efficiency in daily management of community infrastructure, as well as operation and monitoring. For example, street lampposts are shared by many users and can be used as charging points to provide energy for electric vehicles. They can also be equipped with billboards. By installing various sensors or cameras on street lampposts, traffic, noise levels and weather conditions can be monitored. Therefore, it is very important that this information can be shared.

6.3 Promoting business

Data exchange and sharing improves the efficiency of resource allocation and promotes business development. For example, a developer can utilize the shared data from community infrastructure such as telecommunications capacity, water-supply capacity from infrastructure companies and the number of passengers from one station to another to explore the best location for building a new hotel, in order to minimize development costs.

Data exchange and sharing provides opportunities for innovation to create new business models in a community. For example, the traffic data of existing transportation and the general movement of citizens, when combined, could be used to create a driverless taxi operation.

6.4 Facilitating urban planning

Data exchange and sharing can help city planners draw up comprehensive infrastructure planning, which can enhance the development and utilization of urban spaces, achieve a balance between urban and rural infrastructure and make a city more harmonious and liveable.

Through data exchange and sharing, control and avoidance guidelines between adjacent infrastructures can be met, planning errors can be effectively avoided, problems caused by insufficient infrastructure capacity can be reduced, and the efficiency of government and approval processes can be improved. For example, by sharing data, a certain distance both vertically and horizontally between power and gas supply pipelines can be maintained to ensure safety is considered.

Data exchange and sharing can help city managers make collaborative infrastructure implementation plans. Through collaborative construction of various infrastructures, the refinement of urban planning and management can be promoted, and unsighted excavation, duplicate construction and resource waste can be avoided.

6.5 Enabling proactive maintenance

Data exchange and sharing can be used for more efficient and preventive maintenance of smart community infrastructure. It can provide timely relevant information to infrastructure owners, decision-makers, operators or other relevant stakeholders regarding the operational condition of the infrastructure and detect the first signs of defects or malfunctioning, enabling efficient and cost-saving operation and maintenance activity.

Additional analysis of the collected data enables predictive maintenance aimed at effective budgeting, planning and cost savings for maintenance activities. Proactive maintenance is enabled by data collected. Shared data should additionally increase operational safety and the effective operation of smart community infrastructures. For example, combining road traffic data and people flows, street light switching times can be adjusted to save energy and improve the efficiency of operation and maintenance schedules.

6.6 Promoting environmental protection

Data exchange and sharing can promote environmental protection. Through data exchange and sharing, community infrastructure services can be designed to limit the extent of pollution and more efficiently use resources such as materials and energy, and reduce waste. It can limit the impacts on existing green spaces (e.g. parks, wetlands, watercourse buffers, existing trails) and the control of surface run-off and drainage.

Data exchange and sharing also contributes to the improvement of public health. For example, the sharing of air quality data, heating information and traffic data can help city managers adopt appropriate heating and traffic control measures to avoid deterioration of air quality.

6.7 Improving safety and security

Community infrastructure data can be utilized to improve the safety and security of services across a community. For example, utilizing data related to the geographical location of gas piping, communication and electrical lines can help community managers with disaster management. This could be used in the event of earthquakes, fires, floods and other natural disasters. Sharing of data can support a government to deal with emergency situations more effectively.

7 Security of data exchange and sharing

7.1 General

The underlying premise of smart communities is that greater utilization of data available from community infrastructures should be exchanged and shared to maximize the availability, reliability and resilience of city service provision for the benefit of citizens.

The use of technology is a significant enabler of improved services based on data exchange and sharing. However, this creates an increased dependence on such technologies, particularly when this enables new service delivery models. It also creates significant vulnerabilities and associated security issues.

Interfaces are particularly sensitive points for data exchange and sharing. It is important that interfaces are specifically considered and that the necessary security data and access permissions are applied. Administration of data access permissions should be limited to an authorized and vetted group of individuals.

The multiple agencies and organizations participation model of a smart city is made up of several agencies and organizations that can provide different city infrastructure. In this model, all agencies and organizations which are involved in providing infrastructure are responsible for maintaining the safety and security of data exchange and sharing.

The approach needed to ensure the security of data for a smart city differs from the security policies and processes which might already be in place for community infrastructure at an individual services provision level. The data security for smart city infrastructure needs to respond to the new or increased threats which exist as a result of the sharing and exchanging of available data.

7.2 Data security approach

Security of the community infrastructure data which is exchanged and shared needs to take a holistic city-wide approach, should be appropriate and proportionate, and should aid the delivery of the city's vision and objectives. To ensure a holistic data security approach, the security measures used need to take into account physical, cyber, personnel and cyber physical aspects of community infrastructure services. This means security of data exchange and sharing should be treated as a whole; separate security planning should be avoided.

A key aspect of secure community infrastructure data provision is to consider data from city services which cross the boundaries of individual service providers (e.g. transportation, water or waste) and provide effective and secure data use for the delivery of city-wide services.

A holistic data security approach with appropriate and proportionate security measures should be introduced to deter and disrupt hostile, malicious, fraudulent and criminal behaviour or activities which threaten community infrastructure. The security approach should seek to preserve confidentiality, integrity and availability of data, ensuring, where possible, that data are free from danger or threat of unintended access and use.

The vulnerabilities of community infrastructure data exchange and sharing arise because of:

- differing organizational priorities of individual infrastructure service providers;
- incompatible governance arrangements, policies and processes of infrastructure providers;
- the aggregation of community infrastructure data with a wider range of data sourced for inside and outside of the city;
- different levels of security understanding and concerns across community infrastructure providers;
- a difference in the range of risk appetites to manage data security across the city and community infrastructure providers.

The volume and accelerating pace of data generated, collected, utilized and stored adds to the security vulnerabilities of community infrastructure data. Security measures need to consider the specialist data exchange and sharing requirements (e.g. the aims and subsequent usage after the user obtains the exchanged and shared data) of personal data, intellectual property and commercially sensitive data which facilitate the provision of city-wide services.

Storage of data needs specific consideration, for example a decentralized method of data storage may be deemed more secure than centralized data storage. Duplication of data storage should be avoided.

It is important to consider the threat from actors who seek to undermine any vulnerability in the data security measures for community infrastructure. These actors may be associated with organized crime, seeking to acquire unauthorized personal or sensitive data, intellectual property or commercially sensitive data. It is important to consider potential acts of terrorism whose perpetrators are seeking to sabotage the exchange and/or sharing of community data to disrupt city services or compromise the city's infrastructure or the safety and security of citizens.

7.3 Security strategy and policy

7.3.1 General

For a smart city to obtain and retain the public trust, it needs to be able to respond to increasing public awareness and any potential concerns regarding the exchange and sharing of community infrastructure data. A city should be prepared to put in place appropriate mechanisms to maintain the trust of its citizens. A city needs to be capable of responding to increasing public awareness and potential concerns about how city data are being used, and put in place mechanisms to prevent the erosion of public trust.

When determining appropriate security governance for community infrastructure data, it is important that security measures consider citizens who are residents, visitors and those who enable the efficient provision of city services.

7.3.2 Security strategy

Cities should operate different service delivery options. Ownership of the community infrastructure provision could be complex and will affect the data security measures which can be deployed. Cities need to consider the autonomy which is allowed for service providers when devising the appropriate data security measures to be implemented.

The data security strategy which the city develops needs to consider the secure delivery of community infrastructure and all aspects of the services deployed, in particular:

- the safety of data exchange and sharing;
- the authenticity of the data exchanged and shared;
- the availability, provenance and reliability of community infrastructure data;
- confidentiality and commercial sensitivities of service data;
- appropriate measures to ensure the integrity of data exchanged and shared;
- resilience requirements of data exchanged and shared;
- the fact that interfaces are sensitive points for data exchange and sharing, and that data access permissions need to be put in place.

A city needs to develop a security strategy which articulates the overall security policy for community infrastructure, detailing which data are to be shared and exchanged and how they should be collected, managed and processed. This security strategy should also take into account legislation or regulation appropriate to the jurisdiction of the city. The security policy can also be used as the basis to develop and deliver additional community infrastructure services for the benefit of citizens.

7.3.3 Security policy

The data security measures which need to be considered for community infrastructure data exchange and sharing should include the following key areas:

- governance;
- service personnel;
- citizens;
- service delivery organizations;

- appropriate and proportional city-wide security processes;
- physical security required for the city services.

It is important to ensure that data security measures are set in the context of the complexity of the community infrastructure and the scale of the city where the infrastructure operates. The data access permissions should be limited to a small and trustworthy group of people.

7.3.4 Accountability and responsibility

The approach to data security should enable an appropriate, multi-agency model for the provision of community infrastructure in a city. Moreover, this security approach can also support the development of the data framework and enable the city to determine the accountability and responsibility of each community infrastructure service provider.

As the maturity of the secured data exchange and sharing of the data framework evolves, city decision-makers should be appointed to reflect this changing data landscape. The changes to the data framework may arise for a number of reasons, including:

- the introduction of new community infrastructure;
- changes to contractual arrangements for exiting services.

The benefit of this approach to data security is that the city will curate the data which is routinely shared and exchanged, and will therefore be able to understand the normal operating procedures. This can help city leaders to ensure that city service providers are both accountable and responsible for the secure sharing, processing and exchange of community infrastructure data.

7.4 Assessment of security risks

7.4.1 Threat landscape

Smart community leaders need to understand the threat landscape which needs to be mitigated for their community. There needs to be an understanding of the range of threats the community faces and potential vulnerabilities, which could include:

- disruption or corruption of data from community infrastructure services;
- loss of personal data, intellectual property or commercially sensitive data related to community infrastructure services;
- the compromising of the use, operation or value of city infrastructure services;
- the targeting of city-wide vulnerabilities by one or more organizations related to the exchange and/or sharing of community infrastructure data; for example, the targeting of integrated transport and traffic management services;
- sabotage via either internal or external attacks; for example, damage caused by malware, hackers or disaffected personnel;
- the compromising of cyber physical systems, resulting in damage to the physical community infrastructure;
- theft, blackmail, unauthorised use of community infrastructure services, impairment or disruption of the service;
- operational risks, such as an attack on an electronic driverless vehicle (EDV), unknown program bugs which affect the handling of the EDV, threats which arise as a result of the complexity of supporting EDV infrastructure, or some other unexpected dysfunction of EDVs or the infrastructure related to the vehicles;

— financial risks.

An assessment of the threat landscape should consider that an attack could result in loss of confidentiality, availability, safety, resilience, possession, authenticity, utility and/or integrity of data which is exchanged and shared by community infrastructure service providers.

City leaders should ensure that any potential for insecure or poorly maintained services to leak, expose or permit unauthorized access to data which is exchanged and shared is considered. An attack on these infrastructure services could result in a city-wide vulnerability.

Contractual arrangements should be in place for the providers of city infrastructure services to enable interoperable data exchange and sharing. It is important to consider whether these contractual arrangements give additional access to other organizations' intellectual property and/or commercially sensitive data or give extended access to other service providers' infrastructure data, which would not normally be the case under existing contractual arrangements.

7.4.2 Management of security risks

7.4.2.1 General

There needs to be effective management of security risks for all community infrastructure services. City leaders should ensure all relationships related to the accessing of data for community infrastructure service provision are specifically managed to mitigate the security risks which have been identified.

7.4.2.2 Personal data

To provide interoperable community infrastructure services, the community is likely to exchange and share personal data across more organizations than is currently the case. A personal data security incident could endanger citizens, infrastructure agencies and organizations, and could prejudice citizens' trust in agencies and organizations, adversely impacting the whole community.

7.4.2.3 Metadata

Metadata provides information about the data which the city exchanges and shares, for example the usage and access rules which apply to data in the data framework. This community infrastructure metadata represents an additional security risk. A security breach involving metadata would reveal key details of how the community infrastructure data are managed. Specific security measures should be introduced to ensure the effective management of metadata.

7.4.2.4 Reference data

Reference data do not need regular updates and are not updated regularly in terms of content. For example, the tolerances of sensors or the location of key buildings. However, the potential impact of an attack on these data has city-wide implications and could significantly impact community infrastructure services. Specific security measures should be introduced to ensure the effective management of reference data.

7.4.2.5 Aggregated data

To provide, monitor and maintain community infrastructure services, data which is exchanged and shared should be aggregated. This aggregation may lead to increased risks and sensitivities for individuals, groups of individuals and organizations. Particular combinations or absences of data might allow directly or by inference the identification of citizens, putting those citizens at risk. Specific security measures should be introduced to ensure the effective management of aggregated data.

It is important that any study of the risks of aggregating data which is exchanged and shared also considers the security measures which are required to mitigate the threat of aggregated data being used in malicious pattern-of-life analysis.

8 Data privacy

8.1 General

Considerations of data privacy are of equal importance to those guidelines related to the security of data related to all smart community infrastructures. Data privacy applies to all personal data or data which can be used to construct personal data about a citizen.

The multi-agency model of a smart city consists of many different organizations, each of which have the responsibility of delivering city services and share responsibility for the preservation of the privacy of citizens' data.

The data privacy guidelines specified in this document are limited to the exchange and sharing of data which is used by smart city infrastructures.

8.2 Privacy guidelines and activities

8.2.1 General

The data privacy protection detailed in this document is to be used by smart communities to determine the privacy and confidentiality protection required for data relating to individuals and organizations involved in the provision of community infrastructure services. Specifically, these privacy protection guidelines relate to those organizations participating in data exchange and sharing of smart community infrastructures in smart communities.

8.2.2 Privacy principles

The following eight privacy principles should be applied for the exchange and sharing of smart community infrastructure data where personal data are included or can be inferred:

- fairly processed within the jurisdiction to which they apply;
- obtained only for specified purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate and up-to-date;
- not kept for longer than is necessary;
- processed in line with the rights afforded to individuals, including the right of subject access;
- kept secure;
- not transferred to countries or regions outside the jurisdiction to which it applies without adequate protection.

If any exemptions from the eight privacy principles have been determined by the smart community, these exemptions should be documented and acknowledged for each smart community infrastructure service to which they apply.

Each organization participating in data exchange and sharing of smart community infrastructure data should ensure that these privacy principles are carried out consistently within the requirements and guidelines of the smart community infrastructure service to which they apply.

8.2.3 Consideration of city stakeholders

The eight privacy principles should apply to the exchange and sharing of data for all smart community infrastructure services during the design, building and implementation of each city community infrastructure service. Consideration should be given to all stakeholders, for example the public, patients, students, clients, suppliers, business partners and city service organizations.

At all stages of the implementation of the city community infrastructure service, the data owner, data publisher and service user roles should be identified and considered alongside the privacy preservation principles. Organizations should be identified and the data responsibilities they hold should be determined. Additionally, the appropriate mechanisms should be implemented to facilitate confidential exchange and sharing of smart community infrastructure data.

Smart cities should ensure the explicit identification and documentation of the high-risk categories of personal data processed by the city service organizations because of the operation of smart community infrastructure services.

High-risk categories of personal data can include:

- sensitive personal data as determined by legislation or regulatory regimes;
- personal bank account and other financial information;
- national identifiers, such as national insurance numbers;
- personal data relating to vulnerable adults and children;
- detailed profiles of individuals;
- sensitive negotiations which could adversely affect individuals.

It is important that the smart community takes account of community infrastructure services where high volumes of personal data are processed and appropriately manages the increased level of risk in these circumstances.

8.2.4 Specific thematic data

Each smart community infrastructure organization participating in city data exchange and sharing should have their own guidelines to protect data related to the service, for example intellectual property rights or commercially sensitive data. These organizations should be considered when developing the appropriate data exchange and sharing mechanisms for each smart community infrastructure service. It is important to recognize when specific data guidelines should be considered in order to maintain not only privacy but also security. If such data were inadvertently or deliberately made available it could have implications, not just for individuals or the city service, but for the whole community.

8.2.5 Operational guidelines

Once smart community infrastructure systems are implemented, they form important and sometimes essential city services. A smart community expects to apply urban management, personalization and customization of some or all of these services. During the operation of these services, it may change the privacy mechanisms, rules and policies which govern the exchange and sharing of data. Identified roles and responsibilities should be managed in order that any changes needed are appropriately reflected. These changes should support the updating of all aspects of the management strategy, such as:

- updating of internal service rules;
- interaction rules between organizations;
- operational process changes;
- protective measures, such as defining new roles;
- changes to data access management rules;
- maintenance responsibilities.

In each of these cases where operational changes are required, a city should ensure that this also involves the examination of guidelines for authentication, authorization, access and audit.

8.3 Privacy strategy and governance

8.3.1 Senior management team

The smart community should ensure that a senior management team is tasked with issuing and maintaining a privacy policy that sets a clear framework and demonstrates support for, and commitment to, the exchange and sharing of smart community infrastructure data. This should include managing compliance with data protection legislation and regulation, and the application of appropriate good-practice policies.

8.3.2 Privacy policy

The privacy policy should state that it covers either:

- the entire city and the organizations who deliver services; or
- identified organizations involved in the design, building, implementation or delivery of smart community infrastructure services.

The privacy policy should be communicated to all personnel responsible for delivering smart community infrastructure services in the city.

8.3.3 Accountability and responsibility

The city should designate a member of the senior management team to be accountable for the privacy guidelines of city services. The designated team member should be accountable for the management of privacy, exchange and sharing of data for the city. This team member should also be responsible for compliance with data protection legislation and regulation, and endeavour to demonstrate and promote a good privacy practice regime.

The complexity of a smart community and its services may require a number of officers to be responsible for the establishment of appropriate data exchange and sharing policies and compliance activities. The privacy procedures should ensure that the city service organizations process personal data:

- fairly;
- only where this is justified;
- only where this is necessary for the city service organizations' purposes, taking into consideration any legislation or regulation which applies within the appropriate jurisdiction.

Any individual or organization supplying personal data to the city should be provided with access to the exchange and data-sharing rules which apply. The city should produce a privacy notification which clearly communicates the following information:

- the identity of the city service organization;
- the purposes for which data are to be exchanged, shared or processed;
- information about the disclosure of exchanged or shared data to third parties;
- information about an individual’s right of access to personal data when data are exchanged, shared or processed;
- whether personal data are transferred outside the legislative or regulated jurisdiction without adequate protection;

- details of how to contact the city with queries related to the processing of data which is exchanged or shared;
- details of any technologies, for example cookies, used on a website to collect personal data about individuals;
- any other information that would make the processing fair.

8.3.4 Privacy processes

A smart community should incorporate privacy processes which ensure that any city organization shares personal data with another city organization for the provision of city services. The responsibilities of both parties with regard to the data exchanged or shared are in line with the smart community privacy policy. These privacy processes should be formally documented in a written data agreement or contract as appropriate.

Privacy processes should incorporate procedures which ensure that, when each organization is using the data for the provision of community infrastructure services,

- the written agreement or contract describes both the purposes for which the data may be used and any limitations or restriction on the use of the data;
- each organization provides an undertaking or evidence of its commitment to processing the data in a manner which does not contravene the smart city privacy policy.

The privacy policy should incorporate procedures which ensure that, wherever possible, any new processing which involves the exchange or sharing of data with third parties is compatible with the privacy notification policy of the city, and the terms of privacy notifications provided to the individual.

Where this is not possible, the community infrastructure organization should ensure that it has, if required, the individual’s consent to the data exchange and sharing.

Where data exchange and sharing with third parties is permitted without the consent of the individual, the privacy process should incorporate procedures which ensure that an auditable record of the protocols and controls for this data exchange and sharing is documented.

Where data exchange and sharing with third parties are required, for example by legislation, the privacy process should incorporate procedures which ensure that the protocols and controls for data exchange and sharing are documented.

8.3.5 Privacy rights of individuals

Irrespective of who was the creator of the personal data, it is important to recognize that individuals have rights over their own data. The privacy process should include procedures which ensure that individuals’ rights in relation to their data are respected, and that requests to exercise such rights are dealt with within any statutory time limits. Privacy rights include access to information, objection to processing and review of automated processing.

8.3.6 Complaints and appeals

The privacy process should incorporate a complaints procedure which ensures that complaints about the exchange, sharing or processing of personal data are handled correctly. This should include procedures for considering appeals by individuals about the way their complaints have been handled.

9 Data roles and responsibilities

9.1 General

The data related to smart cities may contain citizens' behaviour, location, trajectory and communication records, which are regularly and automatically collected by all kinds of fixed and mobile terminals, sensors, cameras and applications.

While the value of continuously collected data increases, security threats to data are also increasing. Data roles and responsibilities should clearly include the obligation to facilitate privacy and security measures.

9.2 Data roles

Although individual cities have their own data value chain, there are five key roles to be fulfilled to maximize the impact of the data framework in a city.

The roles that exist across the data value chain include:

a) Data creator

The data creator role defines those organizations who collect and/or transform data for the city or its services. This role can be passive, where the organization is responsible for the creation of data for a city as part of the provision of a city service, for example the creation of the city data relating to the location of lampposts in the city. Additionally, this role can be a reactive role where operational insight data are collected and transformed to provide the city with critical insight, for example a transport operator in a city who supplies data collected from cameras in the event of a critical incident. For derived or aggregated data, the data creator is the provider of the process which transforms the data created by others.

b) Data owner

The data owner is the designated curator for the data related to a city service on behalf of the city. The responsibilities of this role include the authority to change the data where appropriate and maintain the transparency for the provenance of the data within the data framework on behalf of the city.

c) Data custodian

The data custodian role differs from the data owner role as this organization does not own the data, it is merely the custodian of the data for a specific purpose or task related to the provision of a service within the city

d) Primary publisher

The primary publisher role relates to the organization that performs the publication role for all data across the data spectrum. All sources of data can be viewed by the organization which performs this publisher role; however, all data might not be published. Publication of the data depends on which part of the data spectrum the data belongs to and the access restrictions which apply.

e) Secondary publisher

In a smart community, an additional publication role exists. The publication of some of the data on the data spectrum is facilitated by the primary publisher. As a result, for some of the published data an organization creates additional value from the city data which has been published. This secondary organization should be encouraged to publish the new value data which has been created, performing the role of secondary publisher. The secondary publisher should monitor the quality of the data in the data framework, feeding back to the city on any variance detected as part of the data publication process. Any access restrictions to the data to be published as part of this secondary publication role are determined by the primary publisher. A feedback loop should be incorporated which supports the primary publisher delegating authority to the secondary publisher to oversee the publication of the data itself.

f) User

There are various organizations which can have differing roles in the data value chain but are also considered to be the users of city data. Although this varies between cities, the key user groups common to all cities are:

- city organizations which support the operation of city services, for example emergency services, community health services and contractors;
- third-sector organizations providing or supporting city services;
- business users, for example corporations and SMEs (small to medium-sized enterprises);
- citizens;
- academic organizations;
- other cities.

9.3 Provenance of data

The metadata and reference data within the data framework should be specific to a city and it is crucial to understanding the provenance to have effective data exchange and sharing of city infrastructure data. The value of the city data can be unlocked by ensuring that the smart community infrastructure data are findable, accessible and interoperable, as follows:

- findable: mechanisms which ensure the data are discoverable and identifiable.
- accessible: licenses and/or license restrictions that are applicable to the use of the data and how the data are made accessible for use by third parties.
- interoperable: the extent to which the data are made available to all organizations for use or reuse.

  The data framework provides a useful tool, acting as an inventory of the smart community infrastructure data, facilitating city leaders to identify the potential impacts and benefits of sharing and exchanging smart community infrastructure data.
- data quality: degree to which a set of inherent characteristics of data fulfils requirements.

NOTE The requirement means a need or expectation that is stated, generally implied or obligatory.

9.4 Accountability

Data owners are accountable for ensuring that data collection, exchange and sharing processes are implemented in a consistent manner across all city infrastructures, particularly in terms of the underlying definition of metadata and reference data, data quality, protocols and formats.

City stakeholders encounter a number of general problems that are the result of inherited siloed data estates, for example:

- fragmented data sets;
- different temporal frameworks;
- different spatial footprints;
- different granularity;
- different and proprietorial formats;

- different definitions of the same data sets;
- low motivation to share.

Consequently, issues of ownership and associated intellectual property rights can act as barriers to the exchange and sharing of city infrastructure data and create obstacles to the realization of the value in the data framework.

Nonetheless, it is in the wider interests of city data owners to accommodate the exchange and sharing of data between city infrastructure services to promote investment in city infrastructure that maximizes city performance, reduces costs, harmonises the needs of citizens, supports city leadership, protects the environment and promotes sustainable development and city resilience.

9.5 New business models

There are many new business and commercial models which could support the creation of the data framework and overcome the siloed data legacy.

One example is a city data cooperative, as an accountable trusted partner. This business model is a mechanism to provide the collaborative framework to develop and support a range of quality and accountability agreements for smart community infrastructure data. A city data cooperative could be formed to reduce the burden of the exchanging and sharing of data between infrastructures. These organizations create quality protocols and provide useable data formats to maximize the benefits of exchanging and sharing smart community infrastructure data.

As infrastructure owners, suppliers and operators make use of data generated by city activities and interactions, cities should continue to develop use cases around which standards are agreed, leading to practical templates and processes that support good data governance.

9.6 Standards framework for cooperative models

A standards framework for cooperative data exchange and sharing should include the interfaces, processing, integration, measures and assessment of impacts on a scale for each city area and organization. This can be achieved by understanding the organization and utilizing the concepts which are affected using the SCCM defined in ISO/IEC 30182. Technical standards for other interfaces, such as devices and meters, are already well established.

Integration standards include the technical aggregation and management of data with the assignment of interdependent roles among data controllers, processors, integrators and suppliers which support the legislative and regulatory jurisdiction for the city.

Regarding the measurement of impact, smart community indicators, such as those recommended in ISO 37120, help interpret impacts for the four levels of insight – operational, analytical, strategic and critical – as defined in ISO/IEC 30182 via the SCCM.

To understand impact, standards which prepare impact assessments should closely align with ISO 37153.

This is a complex and well-served standards arena. BSI PAS 183:2017 shall be used for guidance on the exchange and sharing of smart community infrastructure data.

Annex A
(informative)

Case studies

A.1 Data exchange and sharing for community infrastructure based on “Map World — Nanjing”

Project title	Data exchange and sharing for community infrastructure based on “Map World — Nanjing” service platform
Project profile	With the continuous development of Smart Community, the demand by government departments for spatial and other information applications are also increasing. The need for data sharing is very strong. Based on “Map World — Nanjing”, the Nanjing government builds up community infrastructure public service platform and establishes an integrated map of all kinds of community infrastructure data. The platform provides portal, standard online service, API, front server, mobile APP and other application patterns. It carries out community infrastructure data exchange and sharing. It also plays an important role in smart community, mainly including portal, data management system, service publication system, catalogue and data exchange system, operation management system and collaborative management system. This case study constructs a smart community infrastructure data system, and could provide services for data integration, synthesis and management. A framework for data exchange and sharing is established. Based on data security within the life cycle, smart community infrastructure data exchange and sharing could be completed. Regarding the data type, the platform constructs community infrastructure data systems for “energy, water, transport, waste, ICT”, and feature refined. Besides the property of geo-information, smart community infrastructure also contains abundant thematic information and reference information. The data management system can realize the effective organization and management of multi-type and multi-format data. The data fusion, catalogue and data exchange system is based on the CSW directory service specification, and provides service registration, discovery and binding to achieve interoperability between national, provincial and municipal community infrastructure service. Based on “Map world — Nanjing”, the platform could carry out data integration, synthesis and management in the fields of, for example, rail traffic, sewage and rainfall and establishes one map of community infrastructure data. Regarding the data exchange and sharing framework, the service publishing system provides online information services and supports service-based application construction with regular programming languages. The platform provides a variety of shared patterns such as portal, standard service, API development, server front and mobile APP. Regarding the data security, the operation management system realizes platform users and authority management, service management and service application operation status monitoring.