

Smart City Security Model

December, 2020



Ministry of Science and ICT

KISA KOREA INTERNET &
SECURITY AGENCY

Summary



A Background

Korea and the world living in the present era are facing various problems due to rapidly increasing urbanization. Urbanization in all fields such as politics, economy, and culture is becoming more serious over the years. However, various efforts are being made to solve this urbanization problem, and the change to a smart city is also being carried out as a way.

Smart city aims to be a sustainable city that provides various urban services by convergence or complex application of various technologies to improve the city's competitiveness and quality of life, transcending the quantitative and economic growth of existing cities.

However, smart cities are likely to be exposed to cyberattacks as information and communication technology is applied very intensively. Such cyberattacks can eventually neutralize various services of smart cities, paralyze urban functions, and in serious cases threaten the lives of citizens. Therefore, smart cities should not only strengthen security against cyberattacks, but also internalize security.

To this end, all smart cities should be able to comply with the establishment of a system that defines and checks the security requirements of the smart city integrated platform that plays a key role in smart cities, while establishing a security model that smart city services should have.

Therefore, through this document, we intend to self-check the basic security requirements that smart

cities must have and contribute to establishing and maintaining smart city services according to the security model.

B Scope and Composition

■ Scope

The scope of application of the security model presented in this document is based on an integrated platform-based smart city currently being built around local governments, and is expanded to metropolitan organizations in the future, and implemented in consideration of links between smart cities.

The integrated platform-based smart city consists of smart city infrastructure, smart city integrated platform, smart city device, smart city service, and smart city security management area, and a security model was presented based on the security requirements of each component.

■ Composition

This document consists of a total of five chapters.

Chapter 1 describes the development background and scope of the smart city security model. Chapter 2 analyzes domestic and foreign smart city standards and reference models to analyze smart city structures, identifies components, and defines their contents.

Chapter 3 presents ways to derive possible security threats in smart cities, and derives security threats and threat scenarios accordingly.

Chapter 4 implements a security model corresponding to the security threats identified in Chapter 3, and presents security requirements for each area.

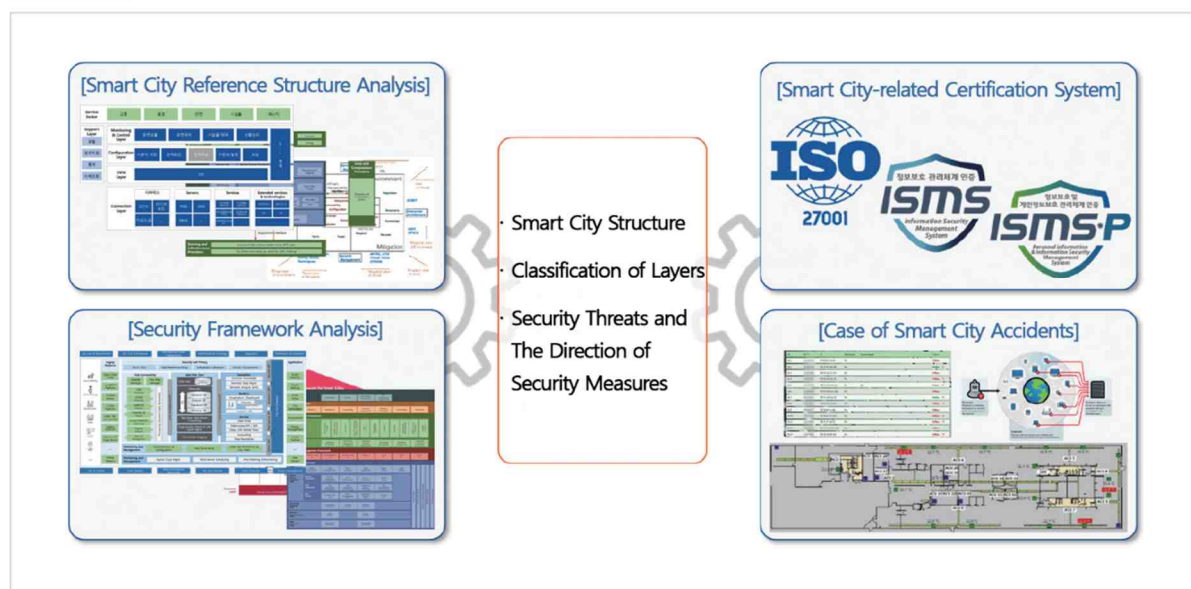
Chapter 5 presents a smart city inspection method as an example so that the smart city security model can be applied.

Smart City Composition and Components



In this chapter, smart city compositions and components were identified by analyzing domestic and foreign smart city-related standards and reference models.

Picture 1 Smart City Standard and Reference Model Analysis



Smart cities can be broadly classified into urban platforms and services. In urban platforms, public IoT platforms, data hub platforms, and digital twin platforms play a role in collecting data → storing/management → analyzing/utilizing data, and cybersecurity platforms support this.

On top of the structure of this platform, smart city infrastructure, smart city integrated platform programs,

and smart city devices are operated and managed by integrated operation centers, and various services are provided.

A

Smart City-related Standards and Reference Models

Trend of standardization of overseas smart cities



1) Smart City Infrastructure field

International standardization is in progress according to the Organization for Standardization and Development, but most of them are developing standards for performance evaluation indicators and performance evaluation guidelines for smart cities. However, the definition of performance evaluation indicators has been completed, but no specific performance evaluation guidelines have been defined.

[Table 1] International standardization status [Infrastructure]

Standardization Organization	Standard number	Development year	Related Focused Standardization Items
IEC SyC SC	IEC63205	In progress [2020]	Smart City Reference Structure Standard
JTC1WG11	ISO/IEC30146	In progress [2019]	
	ISO/IEC30145-1	In progress [2019]	
	ISO/IEC30145-2	In progress [2019]	
ETSI ISG CDP	DGR/CDP-002	2018	Standard for Smart City Performance Evaluation Indicators
ISO TC268	ISO37122	In progress [2019]	
	ISO37123	In progress [2019]	
	ISO37120	2018	
ITU-T SG20	L.1600	2016	
	L.1601	2016	
	L.1602	2016	
	L.1603	2016	



2) Smart City Platform Field

As for smart city platform technology, standardization of smart city platform technology that can be linked with conventional IoT standard technology is in progress, and the importance of smart city data as well as integrated city control platform is increasing.

Data-centric platforms, information (data) model standardization, and public data-related standards are being developed.

[Table 2] International standardization status [Platform]

Standardization Organization	Standard name	Individual year	Standardized items
ITU-T SG20	Y.SC-Open Data, Framework of Open Data in Smart Cities	In progress (2019)	Smart City Data Platform Standard
	Y.API4IOT, API for IoT Open Data in Smart Cities	In progress (2019)	
	Y.ODI, Open Data Indicator in smart cities	In progress (2019)	
	Y.4201, High-level requirements and reference framework of smart city platform	2018	Smart City Control Platform Standard
JTC1 WG11	ISO/IEC30145-3, Smart City ICT Reference Framework– Part3: Smart City Engineering Framework	In progress (2020)	Smart City Control Platform Standard
ETSI ISG CDP	DGS/CIM-005, Data Publication Platform	In progress (2019)	Smart City Data Platform Standard
	DGS/CIM-006, Information Model	In progress (2019)	Smart City Information Model Standard
	DGR/CIM-008, NGSI-LD Primer	In progress (2019)	Smart City Data Platform Standard
	DGS/CIM-009, NGSI-LD API	In progress (2019)	Smart City Data Platform Standard
	DGS/CIM-004, API Preliminary	2018	
oneM2M	TR-0036, Smart City	2018	Smart City Data Platform Standard



3) Smart City Service Field

Standardization of smart city service perspectives is starting to standardize various smart city services, centering on official international standardization organizations such as ITU-T, ISO, and IEC, and various standardization organizations are developing and distributing service standards suitable for the characteristics of each organization.

[Table 3] International standardization status [Service]

Standardization Organization	Standard name	Individual year	Standardized items
ITU-T SG20	Y.SSL, Requirements and Reference Framework for SmartStreetLight	In progress (2019)	Smart Street Light Service Reference Structure Standard
	Y.smartport, Requirements of smart management of supply services in smart port	In progress (2018)	Standard for Smart Port Service Requirements
	Y.SPL, Requirements and Functional Architecture for Smart Parking Lots in Smart City	2018	Standard for Smart Parking Lot Service Reference Structure

■ Korea Smart City Standardization Trend



1) Korea Smart City Standardization Promotion System

As a result of research and development projects led by the Ministry of Land, Infrastructure and Transport, more than 20 forum standards have been developed, and the standardization of smart city integration platforms has recently been promoted. Accordingly, the National Institute of Technology and Standards is developing national standards based on the smart city reference structure established by the U-City Forum, and the Smart City Standardization Forum is promoting standardization of smart city integrated platforms to develop the smart city software industry.

[Table 4] Smart city standardization tasks by Korea ministries

Department	Work	Plan
Ministry of Science and ICT (National Radio Research Agency)	Smart city communication infrastructure ICT technology standardization	-National/international standardization of major ICT such as infrastructure -ICT-based infrastructure/data/service organization standardization (TTA) (5G, IoT, blockchain, big data, realistic broadcasting, etc.) - International standardization of common technologies for smart cities (guidelines for establishing smart cities, performance indicators, etc.)
Ministry of Land, Infrastructure and Transport	Control Tower of Smart City Construction Project	-General responsibility for standard application when building a smart city. -Smart City Platform Organization Standardization (Smart City Association) -Finding a standard based on demonstration
Ministry of Trade, Industry and Energy (National Institute of Technology and Standards)	Control Tower for national/international standardization of smart city industrial application	- National/International Standardization of Industrial application technology. -Corporate Standard Application Support -International standardization of common technologies for smart cities.



2) Standardization Status by Smart City Field

(A) Smart City Infrastructure Field

Although standardization related to infrastructure technologies such as smart city performance evaluation indicators is insufficient, standard development is expected to begin in earnest in connection with national strategic projects. In particular, the Smart City Standardization Forum (SSF) established test standards to test platform software functions and interworking functions for integrated smart city management and operation.

[Table 5] Kora Standardization Status [Infrastructure]

Development Organization	Standard name	Individual year	Related focus standardization items
Smart City Standardization Forum	SSF-ST-2020, Smart City Reference Structure	2016	Smart City Reference Structure Standard

(B) Smart City Platform Field

Platform technology standardization is mainly focused on international standardization, and domestic standardization has been completed through the forum to establish platform technology standards required for the domestic environment.

[Table 6] Kora Standardization Status [Platform]

Development Organization	Standard name	Individual year	Related focus standardization items
Smart City Standardization Forum	SSF-ST-2021, Platform software requirements for integrated management and operation of smart city information.	2017	Smart City Control Platform Standard
	SSF-ST-2022, Platform linkage standard for integrated management and operation of 119 emergency dispatch support service system and smart city information.		

	SSF-ST-2023, Platform linkage standards for integrated management and operation of emergency disaster situation support service systems and smart city information.		
	SSF-ST-2023, Platform linkage standards for integrated management and operation of smart city information with the socially disadvantaged support service system.		
	SSF-ST-2023, Platform linkage standard for integrated management and operation of 112 emergency dispatch support service system and smart city information.		
	SSF-ST-2023, Platform Linkage Standards for Integrated Management and 112 Operation of Emergency Video Support Service System and Smart City Information in the General Situation Room		
	SSF-ST-2023, Platform software function and interworking test standard for integrated smart city management and operation (1.0)		



3) Smart City Service Field

The smart city service sector is in the process of standardizing platform technologies, interfaces, and profile specifications to secure data compatibility for each industry.

[Table 8] Kora Standardization Status [Service]

Development Organization	Standard name	Individual year	Related focus standardization items
TTA SPG11	TTAK.KO-10.0965-Part1, Urban underground facility monitoring system – Part 1: Requirements	2016	Digital Twin Technology Standard for Urban Administration
	TTAK.KO-10.0965-Part2, Urban underground facility monitoring system – Part 2: Reference Structure		
	TTAK.KO-10.0965-Part3, Urban underground facility monitoring system - Part 3: Interfaces between the water leakage detection device and the collection device of the water pipeline		

■ Standardization status by smart city technology

The current status of domestic and foreign technology standardization related to smart cities is as follows.

[Table 9] Domestic and international standardization status in the smart city common technology field

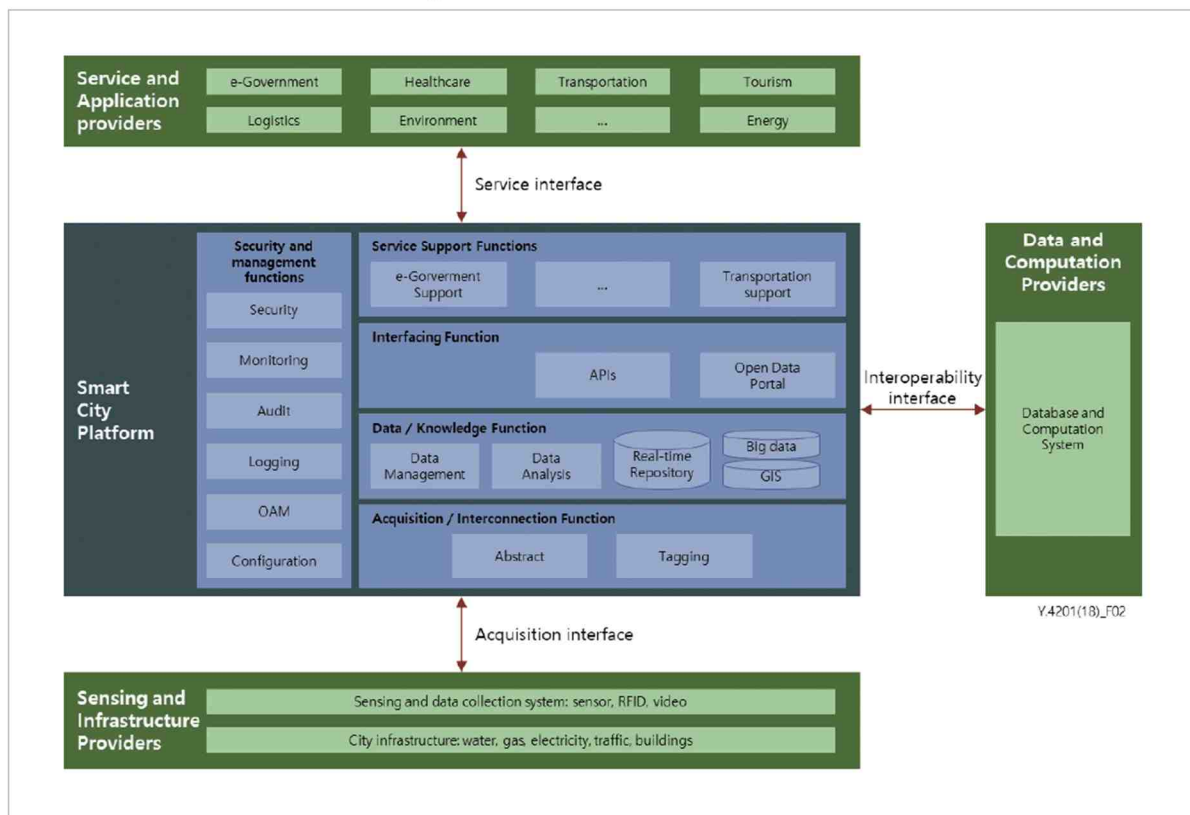
Standardized items		Main contents
Guidelines	Smart city reference structure	Define functional components of a smart city and define interfaces between each functional element at a higher level.
	Standard for Smart City Maturity Model	Define a maturity model to measure the technological performance, process and interoperability, and improvement of a smart city.
Evaluation indicators	Smart City Performance Evaluation Index	Definition of indicators to evaluate the performance of smart cities
	Ontology for Smart City Performance Evaluation Indicators	Define ontology to describe performance evaluation indicators of smart cities.
Platform	Smart City Control Platform	Define the structure, function, and interface of the platform for integrated control of the city.
	Smart City Data Platform	As a middleware platform that can store/manage smart city data collected from IoT and non-IoT systems in an integrated manner, define platform structure, function, API and protocol interworking adapter, test specification, utilization model, etc.
	Smart City Public Data Management System	Definition of Management System for efficient utilization and sharing of public data(Data or information created or managed by public institutions) in Smart City.
Infrastructure	5G	Vehicle-terminal, enhanced V2X between vehicle-infrastructure, 5G network technology for smart city infrastructure, etc.
	IoT	Object intelligence interface, etc that recognizes and responds to adaptive situation by objects between element technologies of smart city.
	WLAN/WPAN	Ultra-low power wireless LAN technology for wireless LAN-based smart city services.
	Intelligent network	Wired and wireless optical access networks and smart grid communication for smart city infrastructure.
Data	Artificial intelligence	Intelligent services that help users interact and act using core element technologies such as language, vision, and voice intelligence, etc.
	Blockchain	Standard for responding to security threats to

Standardized items		Main contents
		distributed ledger-based financial services and convergence of smart city information linkage
	Next generation security	Interfaces for information protection between information collection, processing, and utilization technologies for smart city services, etc.
	Big data	Improvement of analysis/prediction precision, big data frameworks for each sector such as finance, communication, public, bio, etc., service architecture, etc.
Service	Self-driving car	Standard for ensuring interoperability between infrastructure and the component technologies constituting autonomous self-driving cars and for industries to enter the global market.
	Smart Health	Smart health standards that provide disease prevention, management, treatment, and personalized health care services anytime, anywhere.
	Realistic show/media	UHDTV, immersive media broadcasting, and cloud media standards for convergence and intelligent delivery of various contents to users without time and space and device restrictions
	Unmanned Aerial Vehicle ICT	Standards such as complete autonomous and remote flight using ICT, big data, and AI technologies.
	Public safety/ Disaster Prevention ICT	Communication infrastructure and convergence services required in terms of public safety and disaster prevention.
	Intelligent robot	Standards such as robot intelligence, safety and compatibility that recognize the external environment and operate autonomously through sensory sensors such as sight and hearing.

■ ITU-T

ITU-T presents the reference structure for the smart city platform as follows.

Picture 5 ITU-T Y.4201 Smart City Platform Reference Structure



The smart city platform has an interface with service/application providers, sensor/infrastructure providers, data and computing providers.

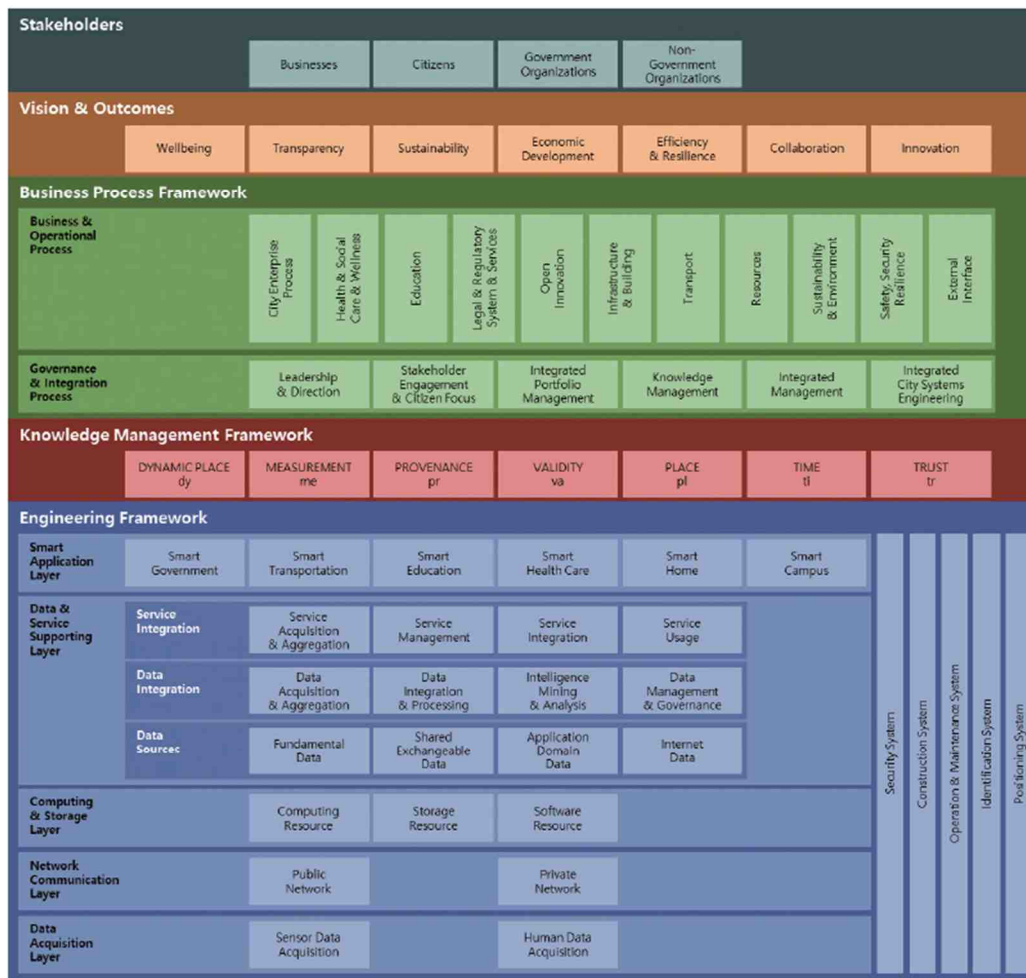
It consists of security/management functions, service support functions, connection functions, data/knowledge functions, and acquisition/interconnection functions inside the platform.

Among them, the structure related to information security is included in the "security and management functions" and presents Security / Monitoring / Audit / Logging / OAM / Configuration.

ISO/IEC 30145

ISO/IEC 30145 configures the reference structure of the smart city as follows.

Picture 6 Smart City Reference Structure of ISO/IEC 30145



It presents stakeholders and goals of smart cities and consists of a business process/knowledge management/engineering framework accordingly. Among them, information security-related functions are representative of information protection systems among engineering frameworks.

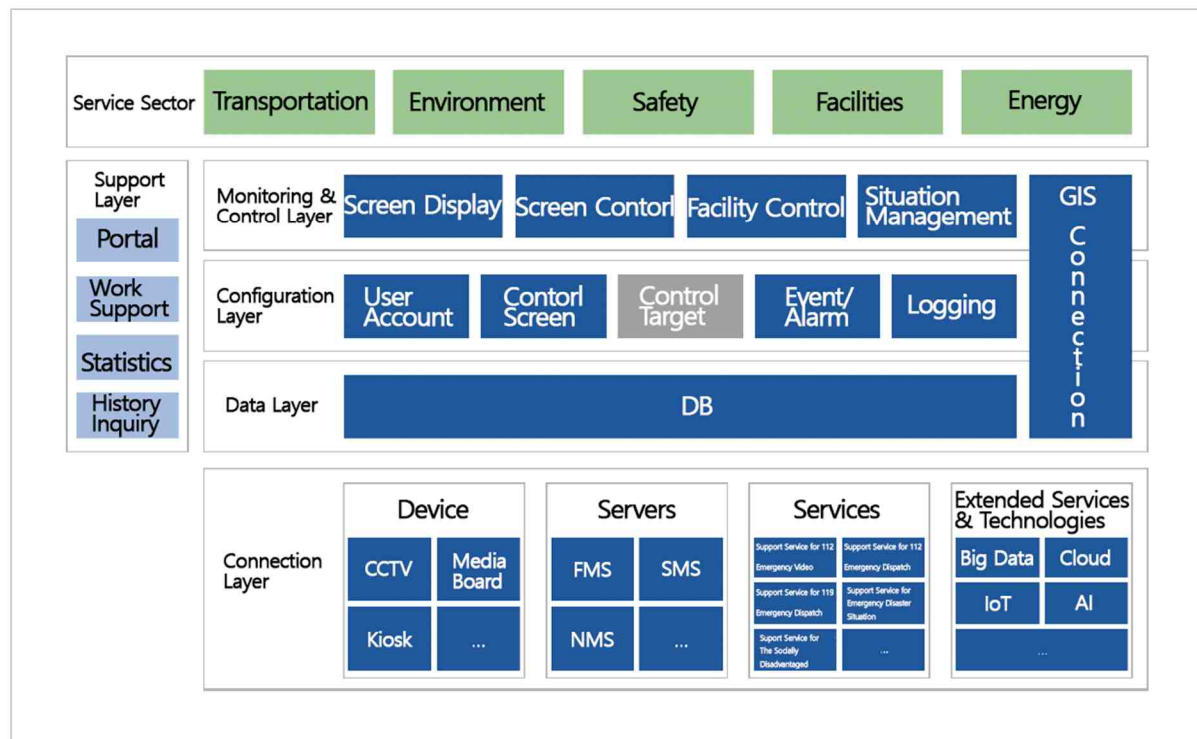
■ Smart City Standardization Forum (SSF-ST-T-001R1)



1) Smart City Reference Model

The Smart City Standardization Forum presents various standards related to smart cities. Among them, the Platform Software Requirements (SSF-ST-T-001R1) for Integrated Management and Operation of Smart City Information was established and the reference model is presented as follows.

Picture 7 Software Reference Model of Smart City Platform



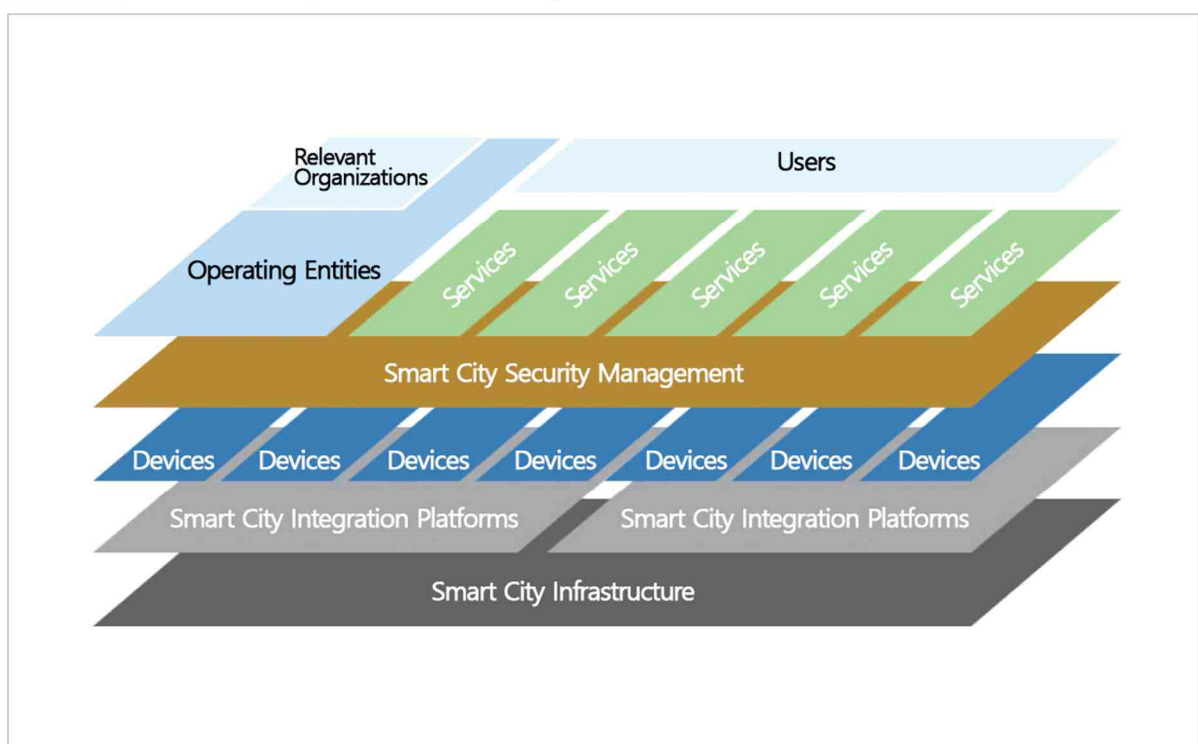
In the above reference model, the smart city platform is presented by dividing it into a support layer, a monitoring and control layer, a setting layer, a data layer, and a linked layer. However, what is regrettable is that there are no requirements related to information security.



2) Smart City Structure and Components

Smart city services aim to improve the quality of life of citizens regardless of form and direction of service. Therefore, only technical security factors cannot be considered, and security models must be established from various angles. These various angles may start from the following detailed configuration constituting the smart city service.

Picture 8 Detailed Configuration of Smart City Service



The smart city service can summarize the above picture by installing a software called "Smart City Integrated Platform" on infrastructure such as servers and DBs to utilize data collected from various "smart city devices" and provide various services to citizens by security management.

■ The Entity of Smart City Operation and Use

The entities constituting the smart city can be broadly divided into operating entities and users.



1) The User Entity

The users are citizens of smart cities that use the service, citizens of other cities that visit smart cities, and foreigners. Since they simply use smart city services, they can provide security functions according to the use of the service by the user, but cannot present security requirements.



2) The Operating Entity

The operating entity is the entity that conceives smart city services and provides services for citizens and visitors to use. They are responsible for operating safer smart city services and must meet various security requirements accordingly.

(A) Local Governments

Local governments are key operating entities that plan, build, and operate smart cities. Local governments establish an integrated operation center to operate smart city services and use related information systems to make the services available to citizens and visitors.

Therefore, they should identify information protection requirements and develop services from the planning stage of smart city services to operate services using information systems or devices to which information protection is applied. In addition, the integrated operation center is a place where all smart city data is concentrated and processed, so it must be able to meet the requirements in terms of special security.

(B) Service provider

The service provider is a local government or a smart city service operator (SPC) selected by the local government, and has the same status as the local government in establishing and operating smart city services. Therefore, it should be possible to meet the requirements in terms of security, such as local governments.



3) Related Organizations

Other related organizations can be divided into data providers that provide city-related data and linked organizations that provide linked services. Data providers support urban virtualization (digital twin, etc.) by providing GIS and BIM, and related organizations refer to institutions that provide services at police/fire/hospitals in response to citizens' emergencies. These related organizations may provide direct security requirements depending on the service, but most of them are not covered in this document because they must meet the requirements of each organization's own management system.

■ Smart City Components



1) Smart City Infrastructure

Smart city infrastructure is the most basic and classic area that makes up smart city services. It plays a role in collecting, storing, and moving data necessary to operate services such as servers, databases, network equipment, security equipment, and management PCs. Accordingly, security requirements in the smart city infrastructure area can be combined with other security requirements continuously covered in the security field, and smart cities can be classified as infrastructure, so it can be replaced by "Major information and communication infrastructure vulnerability analysis criteria".



2) Smart City Integrated Platform

The smart city integrated platform belongs to the basic area of smart city services along with the smart city infrastructure. It includes service webs, mobile apps, and operating software, and is responsible for processing collected data or providing information after processing data to provide results of services requested by users. Like smart city infrastructure, the "Major information and communication infrastructure vulnerability analysis criteria" can be replaced by security requirements.



3) Smart City Devices

Devices such as IoT equipment, CCTVs, and various sensors play a role in collecting data in smart city services. Only when accurate data is collected can the smart city integrated platform process and provide accurate services. In addition, smart city devices are located closest to citizens, so it is common for users to use them normally, but they can be easily exposed to attackers with mistakes or malicious intentions. According to these equipment characteristics, security settings are needed to minimize the impact on smart city services even in situations of theft or loss. Since these security settings must clearly reflect the characteristics of smart city devices, security cannot be secured with the "Major information and communication infrastructure vulnerability analysis evaluation criteria" that check the security settings of general information systems. Therefore, smart city devices can substitute "IoT security certification application standards for IoT products" as security requirements.



4) Smart City Security Management

Smart city security management is an area that manages all components that operate smart city services. For smart city security management, it is necessary to have an operating organization, physical space, business procedures, business processing information systems, and business systems, and to provide smart city services using them. There are various risks that can arise from these tasks, and in the end, security requirements must be derived from the perspective of the management system.

The most similar form to smart city security management is the operation of computer centers such as IDC. However, computer centers are similar and cannot apply mutatis mutandis to information security standards, so separate security requirements are required.



5) Smart City Service

Smart city services are wider than platform operations. Smart city services include matters to be considered in advance according to the characteristics of various services provided.

In particular, security is required in five linked services (smart city safety net services) included in the establishment of a smart city integrated platform, related institutions with high possibility of future linkage, and unique services selected by local governments according to the characteristics of each smart city. Therefore, separate security requirements are required because general ISO/IEC 27001 or ISMS & ISMS-P authentication standards cannot be replaced by security requirements.

Smart City Security Model



Smart City Security Management

Field		category		Details	Guidelines for implementation
1	Policy, Organization, Asset management	1.1	Smart City Security Policy	Smart city security policies and enforcement documents should be reviewed periodically according to laws and regulations, linkage with higher-level organizations and related institutional policies, and changes in the internal and external environment of the organization, enacted and revised if necessary, and the details should be managed.	• Establish and implement regular feasibility review procedures for smart city security policies. • Smart city security policies will be enacted and revised according to changes in the internal and external environment related to smart city services. • When enacting or revising smart city security policies, it conducts review and history management by stakeholders.
		1.2	Management of manpower and organization	The person in charge and person in charge of the security of the smart city service should be designated, and important personnel should be identified, and appropriate training should be implemented after the security pledge following smart city service operation. city services,	• Clearly assign the roles and responsibilities of security officers and personnel related to smart city services. • Personnel who handle and manage smart city service infrastructure, integrated platform, and devices are identified as important personnel and managed as a list. • A separate security pledge is received for key personnel who handle and

Field		category		Details	Guidelines for implementation
					manage smart city service infrastructure, integrated platforms, and devices. • Establish and implement education plans for key personnel of smart city service.
		1.3	outsider management	For outsiders related to smart city services, documents such as contracts and agreements including maintenance and security management must be followed.	• When contracting external companies and manpower related to smart city services, the contents of the smart city security policy are reflected in the contract and agreement. • The maintenance contents, including the integrated platform, are reflected in contracts with external smart city service companies.
		1.4	Smart City Asset Management	Assets related to smart city services should be managed as a list and the current status should be identified periodically.	• Identify the current status of all assets related to smart city services and manage them as a list. • Identify and manage changes in all assets related to smart city services periodically.
	2 Integrated Operation Center Security	2.1	Protected area	Smart city services should be able to protect against physical and environmental threats.	• In order to protect against physical and environmental threats, the classification and designation standards of protected areas are established/implemented. • Protection measures are established according to the grade and designation standards of the protected area, and are implemented according to the protection measures.
		2.2	Physical access control	The protected area should be periodically reviewed for access and access history so that only authorized persons can enter and exit and accountability can be secured.	• Access to the protected area is controlled so that only authorized persons can access it.. • Even if only authorized persons enter the protected area, records of access to the protected area are maintained and reviewed periodically. • Control the release date within the protected area

Field		category		Details	Guidelines for implementation
					and periodically check the history.
		2.3	Operation of support facilities	The infrastructure and integrated platform managed by the integrated operation center must operate support facilities capable of maintaining power, temperature, etc.	• It operates support facilities such as UPS and thermo-hygrostat in the integrated operation center.
3	Access control	3.1	Access control policy	Access control policies for smart city services should be established and updated periodically.	• Establish and implement procedures for registration, termination, change, and deletion of accounts. • Access control policies are reviewed periodically or according to environmental changes and are currently being implemented.
		3.2	Account and permission management	All users must be given an account and authority, and must periodically review whether it is an appropriate authority.	• One account is granted per person according to the access control policy, and the authority according to the account is different. • All passwords are managed according to safe password management procedures. • The authority according to the account shall be reviewed periodically in accordance with the access control policy.
		3.3	Access control implementation	Infrastructure, integrated platforms, and devices used in smart city services must be accessible only on specific networks.	• Smart city infrastructure, integrated platforms, and devices are controlled to be accessible only from specific networks. • The administrator-only application controls access only to a limited network within the smart city service.
4	Network security	4.1	Network separation	The network in which the smart city service is operated must be logically/physically separated and disclosed, and the server and web must be operated in the DMZ.	• Infrastructure, integrated platform, and devices for smart city service operation are physically or logically separated and operated according to importance or legal requirements. • Separated networks allow access only to necessary services by using intrusion

Field		category		Details	Guidelines for implementation
					prevention systems and ACLs for each section.. • The web server used by citizens forms a DMZ for external services and blocks direct connections from the outside to the internal system.. • All equipment in the DMZ applies enhanced protection measures such as vulnerability inspection, access control, authentication, and operation of information collection, storage, and disclosure procedures.
		4.2	Transmission section	Section encryption technology should be applied to all data transmitted and received on the smart city service network.	• All sections transmitted using a communication network within the smart city service are protected using section encryption technology. • After sending a control command to the device or receiving status information, the session is immediately terminated.
5	Privacy management	5.1	Protection of personal information	Personal information such as personal identification information, personal image information, and personal location information used in smart city services must be protected in accordance with legal requirements.	• Before citizens use smart city services, various consents are obtained in accordance with laws related to personal information protection. • Encryption is applied according to the collection, transmission, and storage of personal information within the smart city service. • When providing video information according to smart city services to external institutions, the faces of individuals unrelated to the purpose of the service are masked and delivered. • In smart city services, personal location information is not processed without permission. • In the case of analyzing and utilizing personal

Field		category		Details	Guidelines for implementation
					information, which is citizen data, de-identification measures are applied.
		5.2	Prevent invasion of privacy.	Care should be taken not to infringe on privacy that may occur due to smart city services.	- Periodically check whether the privacy of ordinary citizens is violated by smart city services. - Identify and improve matters that may infringe on privacy.
6	Record and review	6.1	Log management	Important events occurring in all infrastructure, integrated platforms, and devices in smart city services must be recorded and stored safely.	- Important events that occur in all infrastructures, integrated platforms, and devices within the smart city service are kept as records. - Important events that occur in all infrastructures, integrated platforms, and devices within the smart city service include access records and post-access activity records. - All records are stored securely in a dedicated storage so that no one can tamper with them.
		6.2	Log-based review	Smart city services should be reviewed periodically according to records.	- Periodically check whether smart city services are operating according to smart city policies. - Periodically review the collected records to identify signs of an accident.
7	Service introduction and development security	7.1	Define security requirements	When introducing, developing, or changing, security requirements such as legal requirements related to information protection and personal information protection, the latest security vulnerabilities, and safe coding methods should be defined and applied.	- When developing all software including integrated platform and device software used in smart city services, define security requirements before development and reflect them in development. - Before development and introduction, we review the laws related to smart city services and include the matters that must be complied with in the security requirements.
		7.2	Review and test security requirements	Establish and implement review standards and procedures such as compliance with legal requirements, latest	If security requirements are derived before development, check whether all relevant requirements have been

Field		category		Details	Guidelines for implementation
				security vulnerability check, safe coding implementation, and personal information impact assessment to review whether information systems have been introduced or implemented according to predefined security requirements. And Corrective measures should be carried out for the problems found.	effectively taken. • When introducing smart city infrastructure, integrated platform, and devices, select products with proven security. • When introducing smart city infrastructure, integrated platform, and device, if security is not verified, it is checked whether the latest vulnerabilities are taken and whether or not the security acceptance criteria are met. • During development, we comply with security standards that must be observed during development, such as secure coding.
		7.3	Separation of test and operating environment	Development and testing systems should, in principle, be separated in order to reduce the risk of unauthorized access and modifications to the operating system.	• The test environment and development environment for the introduction of smart city infrastructure, integrated platform, and devices are operated separately from the operating environment. • If it is difficult to separate development and operating environment for unavoidable reasons, mutual review, supervisory monitoring, change approval, and accountability are secured.
		7.4	Test security data	In order to prevent leakage of operating data during the system test process, procedures for generation, use, management, destruction, and technical protection measures of test data must be established and implemented.	• When developing smart city-related integrated platforms and device software, we control the use of operational data in the testing process. • When operational data must be used in the course of testing, controls such as pre-approval, data de-identification, and post-test data deletion are applied.
		7.5	Managing the source program	In principle, source programs should be managed so that only authorized users can access them and not stored in an operating environment.	• All source programs are safely stored by applying access control. • All source programs manage the history of change.

Field		category		Details	Guidelines for implementation
		7.6	Transferring the operating environment	When transferring a newly introduced, developed, or changed system to an operating environment, a controlled procedure must be followed, and the execution code must be executed according to the test and user acquisition procedures.	• Establish and implement procedures for safely transferring smart city infrastructure, integrated platform, and devices that have been introduced and developed to the operating environment. • If there is a problem with the service when transferring it to the operating environment, we are operating a procedure for immediate recovery.
8	Prevent and respond to accidents	8.1	Accident prevention	Infringement accidents that may occur in smart city services should be defined in advance, and response plans should be established and operated accordingly.	• It establishes and operates detailed plans for detection, analysis, and response assuming that an intrusion has occurred in the smart city service. • All infrastructures, integrated platforms, and devices in the smart city service periodically analyze and take action for vulnerabilities. • Periodically check the safety of smart city services from the perspective of information security. • Receive periodic confirmation of the security status of smart city services from a third party.
		8.2	Response to accidents	In the event of an infringement accident, etc. in the smart city service, a system that can respond immediately should be maintained.	• Training on detection, analysis, and response assuming that an infringement accident has occurred in the smart city service is regularly conducted. • After the training for smart city service infringement accidents is completed, implications are derived and reflected in the detailed plan.

■ Smart City Service

Field		Category		Details	Guidelines for implementation
1	Smart city service	1.1	Service authority management	The authority of all external institutions using smart city services should be limited and controlled to prevent any activities exceeding the authority from occurring.	• External organizations that use smart city services control activities other than the granted authority. • Controlling the use of the functions of the smart city service for purposes other than the situation in which it should be provided. • The function of controlling CCTV in the smart city service is not provided to external organizations.
		1.2	Video information security management	Video information according to the smart city service should be used for the purpose of connection, relay, and export.	• Controls so that video information is not transmitted to unspecified external organizations after approval in advance. • We control video information provided to external organizations so that they are not copied without permission. • Equipment for linking, relaying, and exporting video information guarantees availability through redundancy. • Records are maintained when video information is linked, relayed, or exported.
2	Data flow management	2.1	Data validity management	Data used for smart city services should be up-to-date and managed so as not to be tampered with.	• The city data provided shall be periodically checked and kept up to date. • Ensure that all data transmitted and received within the smart city service is not tampered. • Apply the function to verify message integrity when connecting using API.

■ Smart City Devices

Field		Category		Details	Guidelines for implementation
1	Authentication management	1.1	Authentication and authorization	In the case of accessing smart city services,	• According to the smart city service access control policy, access to all devices through

Field		Category		Details	Guidelines for implementation
2				access should be controlled only to the privileges granted according to the authentication and authorization procedures.	authentication. • When accessing smart city devices, limited privileges for each account are granted based on individual accounts. • When accessing data in smart city devices, it is operated so that access is possible according to the differentially granted authority.
		1.2	Safe use of authentication information	Authentication information used for authentication and authorization must be safely managed.	• Operate procedures to safely manage authentication information(ID/PW, authentication key, token, etc.) used for authentication.
	Monitoring	2.1	Audit monitoring	Monitoring should be performed based on the record of actions of users and administrators performed within the smart city service.	• Users and administrators accessing smart city devices monitor abnormal behavior. • In the case of abnormal behavior according to monitoring, the legitimacy is checked through the clarification procedure.
		2.2	Threat monitoring	Vulnerabilities and malicious codes should be continuously monitored and reflected in consideration of the threats of smart city services.	• Information on vulnerabilities related to smart city devices is continuously checked using external specialized agencies. • If vulnerability information is checked, it is applied after considering whether internal application is necessary and considering the service impact. • A vaccine program is installed and operated to prevent the inflow and propagation of malicious codes to smart city devices. • Vaccine program is operated as a real-time monitoring system.
		2.3	Monitoring the condition	Smart city infrastructure, integrated platforms, and devices should be able to know in real time whether they operate normally.	• Smart city infrastructure continuously checks the performance and capacity of each equipment. • Set thresholds for performance and capacity of infrastructure and apply improvement plans in preparation for exceeding the thresholds. • An alarm function is set and operated so that the abnormal status of the smart city integrated

Field		Category		Details	Guidelines for implementation
					platform can be checked immediately. • Smart city devices check daily whether they are operating normally. • The smart city device periodically checks the status value as well as the normal operation.
3	Continuity management	3.1	Change management	Smart city infrastructure, integrated platforms, and devices should be recorded and reviewed for changes in policies, settings, and detailed status.	• Smart city infrastructure, integrated platform, and devices record all changes such as policies, set values, and current status. • All changes periodically review the appropriateness of the changes.
		3.2	Security patches and updates	Security patches to be applied to smart city infrastructure, integrated platforms, and devices should be continuously checked and applied without delay in consideration of the impact of application.	• It continuously monitors patches and updates that should be applied to smart city devices. • When security patches and updates are checked, they are applied without delay in consideration of the impact of smart city services.
		3.3	Backup and recovery	In order to secure the availability of smart city services, backup such as data and set values and recovery plans using backup copies must be established and operated.	• To ensure the availability and data integrity of smart city devices, backup and recovery plans are established for all data and settings. • Backup is performed according to the backup plan for all data and settings to ensure the availability and data integrity of smart city devices. • Periodically check whether backed up data and settings are recoverable. • Improve your backup and recovery plan by regularly training whether it is possible to recover from your backup data and settings.
4	Device security management	4.1	Device asset management	Devices scattered in smart city urban space must be	• Smart city devices manage assets including spatial location (GIS).

Field		Category		Details	Guidelines for implementation
				managed in detail separately from general assets, and additional physical protection controls must be applied.	• Sensitivity of sensors in smart city devices is checked periodically. • Smart city devices are installed in a physically safe space or in such a way that physical access is impossible. • Smart city devices operate a separate power supply for smooth power supply.
		4.2	Physical interface protection	Access should be allowed by limiting the physical interface of the smart city device to management purposes.	• The external interface within the smart city device is deactivated and access is controlled only after approval when necessary. • Physically remove and use the interface used for debugging on the device. • The device's wireless communication function is activated after approval only when necessary for smart city service configuration.. • Protects the device from physical access.
		4.3	Device software protection	The software installed on the device should be safely developed and controlled to prevent reverse engineering.	• Device software applies secure coding during development. • The device software periodically checks and takes action for security vulnerabilities. • Device software is obfuscated to prevent source code from being analyzed. • It has the function to identify and prevent whether the device software last installed by the administrator has been tampered with during operation.
5	Data flow management	5.1	Security when collecting data	Data collected by smart city services should be collected within the purpose of the service.	• The data collected by the device is not collected other than data according to the purpose of the service. • Periodically check whether the data collected by the device is out of service purpose.

■ Smart City Integrated Platform

Field		Category		Details	Guidelines for implementation
1	Authentication management	1.1	Authentication and Authorization	When accessing smart city services, access should be controlled only to the authority granted according to the authentication and authorization procedures.	• In accordance with the smart city service access control policy, access to the integrated platform is accessed through authentication. • When accessing the smart city integrated platform, individual accounts are the principle, and limited privileges are granted for each account. • When accessing data in the smart city integrated platform screen, it is operated so that access is possible according to the differentially granted authority.
		1.2	Safe use of authentication information	Authentication information used for authentication and authorization must be safely managed.	Operates procedures to safely manage authentication information (ID/PW, authentication key, token, etc.) used for authentication.
2	Monitoring	2.1	Audit monitoring	Monitoring should be performed based on the behavior records of users and managers performed within the smart city service.	• Users and administrators accessing the smart city integration platform monitor cases where they are not normal behavior. • In the case of abnormal behavior according to monitoring, the justification is confirmed through an explanation

Field		Category		Details	Guidelines for implementation
					procedure.
		2.2	Threat monitoring	Vulnerabilities and malicious codes should be continuously monitored and reflected in consideration of the threats of smart city services.	• Information on vulnerabilities related to the smart city integrated platform is continuously checked using external specialized agencies, etc. • If vulnerability information is checked, it is applied after considering whether internal application is necessary and considering the service impact. • Install and operate a vaccine program to prevent the inflow and spread of malicious code on the smart city integrated platform. • Vaccine program is operated as a real-time monitoring system.
		2.3	Status Monitoring	Smart city infrastructure, integrated platforms, and devices should be able to know in real time whether they operate normally.	• Smart city infrastructure continuously checks the performance and capacity of each equipment. • Set thresholds for performance and capacity of infrastructure and apply improvement plans in preparation for exceeding the thresholds. • An alarm function is set and operated so that the abnormal status of the smart city integrated platform can be checked immediately. • Check daily whether the smart

Field		Category		Details	Guidelines for implementation
					city device is operating normally. • The smart city device periodically checks the status value as well as the normal operation.
3	Continuity management	3.1	Change management	Smart city infrastructure, integrated platforms, and devices should be recorded and reviewed for changes in policies, settings, and detailed status.	• The smart city integrated platform records all changes such as policies, set values, and current status. • All changes periodically review the appropriateness of the changes.
		3.2	Security patches and updates	Security patches to be applied to smart city infrastructure, integrated platforms, and devices should be continuously checked and applied without delay in consideration of the impact of application.	• Continuously monitor patches and updates to be applied to the smart city integration platform. • If security patches and updates are checked, they are applied without delay in consideration of the smart city service impact.
		3.3	Backup and recovery	In order to secure the availability of smart city services, backup of data and set values, and	• To ensure the availability and data integrity of the smart city integrated platform, backup and recovery plans for all data and settings are established.

Field		Category		Details	Guidelines for implementation
				recovery plans using backup copies should be established and operated.	• In order to secure the availability and data integrity of the smart city integrated platform, backup is performed according to the backup plan for all data and installation values. • The backed up data and settings are periodically checked for recoverability. • Improve your backup and recovery plan by regularly training on whether recovery is possible with your backup data and settings.
4	Data flow management	4.1	Security when using data	When using data in smart city services, the scope of data provided and users should be identified and controlled so that only the minimum amount of data is utilized.	• Information provided to external organizations is controlled so that they are not used without permission by the organization and the personnel included in the organization. • Synchronize with standard time for accuracy and reliability of information provided to external organizations, and check whether time synchronization is normally performed. • Establish and apply measures (redundancy, etc.) to secure the availability and service continuity of smart city services. • When the infrastructure and devices used in the smart city are not used, all data is completely deleted before processing.

Field		Category		Details	Guidelines for implementation
					City data used in smart cities identifies and discloses the scope of disclosure.

■ Smart City Infrastructure

Field		Category		Details	Guidelines for implementation
1	Authentication management	1.1	Authentication and Authorization	When accessing smart city services, access should be controlled only to the authority granted according to the authentication and authorization procedures.	- In accordance with the smart city service access control policy, access to the integrated platform is accessed through authentication. - When accessing the smart city integrated platform, individual accounts are the principle, and limited privileges are granted for each account. - When accessing data in the smart city integrated platform screen, it is operated so that access is possible according to the differentially granted authority.
		1.2	Safe use of authentication information	Authentication information used for authentication and authorization must be safely managed.	Operates a procedure for safely managing authentication information (ID/PW, authentication key, token, etc.) used for authentication.
2	Monitoring	2.1	Audit monitoring	Monitoring should be performed based on the behavior records of users and managers performed within the smart city service.	- Users and managers accessing the smart city infrastructure monitor cases that are not normal behavior. - In the case of abnormal behavior according to monitoring, the justification is confirmed through an explanation procedure.
		2.2	Threat monitoring	Vulnerabilities and malicious codes should be continuously monitored and reflected in consideration of the threats of smart city services.	- Continuously check information on vulnerabilities related to smart city infrastructure using external specialized agencies. - If the vulnerability information is checked, it is applied by considering the service impact after reviewing whether internal application is necessary.

Field		Category		Details	Guidelines for implementation
3					• Install and operate a vaccine program to prevent the inflow and spread of malicious code to the smart city infrastructure. • Vaccine program is operated as a real-time monitoring system.
		2.3	Status Monitoring	Smart city infrastructure, integrated platforms, and devices should be able to know in real time whether they operate normally.	• Smart city infrastructure continuously checks the performance and capacity of each equipment. • Set thresholds for performance and capacity of infrastructure and apply improvement plans in preparation for exceeding the thresholds. • An alarm function is set and operated so that the abnormal status of the smart city integrated platform can be checked immediately. • Smart city devices check daily whether they are operating normally. • Smart city devices periodically check their status values as well as their normal operation.
	Continuity management	3.1	Change management	Smart city infrastructure, integrated platforms, and devices should be recorded and reviewed for changes in policies, settings, and detailed status.	• The smart city infrastructure records all changes such as policies, settings, and status. • All changes periodically review the appropriateness of the changes.
		3.2	Security patches and updates	Security patches to be applied to smart city infrastructure, integrated platforms, and devices should be continuously checked and applied without delay in consideration of the impact of application.	• If security patches and updates are checked, they are applied without delay in consideration of the smart city service impact.

Field		Category		Details	Guidelines for implementation
		3.3	Backup and recovery	In order to secure the availability of smart city services, backup of data and set values, and recovery plans using backup copies should be established and operated.	• To ensure the availability and data integrity of the smart city infrastructure, backup and recovery plans for all data and settings are established. • Backup is performed according to the backup plan for all data and installation values to ensure the availability and data integrity of the smart city infrastructure. • Periodically check whether backed up data and settings are recoverable. • Improve your backup and recovery plan by regularly training whether it is possible to recover from your backup data and settings.
4	Data flow management	4.1	Security when saving data	Among the data stored in the smart city service, data requiring encryption must be encrypted with a secure encryption algorithm.	• If some of the data collected by the device is stored in the device's own memory, it is encrypted and stored. • Identifies the target of encryption among the data stored in the smart city infrastructure and stores it after encryption. • City data and citizen data received from external organizations will be destroyed after the purpose of use ends.

Smart City Security Model (Summary)

KISA released this Smart City Security Model (Summary) in English, which is a separate compilation of some items of the original entire report. For more details, please refer to the original report, only available in Korean.