

ICS 35.040
CCS L80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/Z 38649-2020

**Information security technology - Guide of information security
assurance framework for smartcities**

信息安全技术 智慧城市建设信息安全保障指南

Issued on: April 28, 2020

Implemented on: April 28, 2020

**Issued by: State Administration for Market Regulation;
Standardization Administration of China**

Table of Contents

1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Acronyms	2
5 Overview	2
5.1 Information security requirements for smart city construction	2
5.2 Smart city construction safety guarantee process	3
5.3 Main roles of smart city construction Safety responsibility	4
6 Smart city construction safety guarantee mechanism	4
6.1 Responsible person mechanism	4
6.2 Traceability verification mechanism	5
6.3 Supervision and inspection mechanism	5
6.4 Emergency plan drill and handling mechanism	5
6.5 Service outsourcing security responsibility mechanism	5
6.6 Information security guarantee education and training mechanism	6
7 Safety assurance management of the whole process of smart city construction	6
7.1 Policy formulation, review and supervision	6
7.2 Information Security Assurance Plan	6
7.3 Analysis of information security requirements	6
7.4 Information system security assurance design	6
7.5 Information system implementation security guarantee	7
7.6 Information system operation and maintenance security guarantee	7
7.7 Information security assurance optimization and continuous improvement	8
8 Information Security Technology for Smart City Construction	8
8.1 Security Technology for Computing Environment	8
8.2 Regional border security assurance technology	9
8.3 Communication network security assurance technology	9
8.4 Application of security technology	10
8.5 Big Data Security Technology	10
8.6 Product and System Security Interface	11
19 References	23

Foreword

This guidance technical document was drafted in accordance with the rules given in GB/T 1.1-2009. Please note that some content of this document may involve patents. The issuer of this document does not assume responsibility for identifying these patents. This guidance technical document was proposed and managed by the National Information Security Standardization Technical Committee (SAC/TC260). This guidance technical document was drafted by: Zhejiang Provincial Economic Information Center, China Electronics Standardization Institute, China Information Security Survey Evaluation Center, National Information Center, CLP Great Wall Internet System Application Co., Ltd., CLP Haikang Group Co., Ltd., Alibaba Cloud Computing Co., Ltd. Division, Hangzhou Anheng Information Technology Co., Ltd., Southwest University of Science and Technology, Zhejiang Development Information Security Evaluation Technology Co., Ltd., Zhejiang Standardization Research Institute, Zhejiang Electronic Product Inspection Institute, Hangzhou Yunjiayun Computing Co., Ltd., Chengdu Qinchuan Internet of Things Technology Co., Ltd., Zhejiang An Ke Network Technology Co., Ltd., Shenzhen Convince Technology Co., Ltd., Zhejiang Xinnuo Testing Technology Co., Ltd., Hangzhou Shipping Information Technology Co., Ltd. the company. The main drafters of this guidance technical document. Wu Qianfeng, Shangguan Xiaoli, Wang Huilin, Du Yuge, Xu Tao, Min Jinghua, Xie Haijiang, Zhang Xiangyang, Huang Hong, Zhao Yinong, Fan Yuan, Wang Boyan, Zhang Dajiang, Zhang Jun, Chen Zili, Zhu Lifeng, Zhou Jun, Wang Shixi, Yu Qunai, Li Ning, Shao Zehua, Zhang Liang, Qi Tongjun, Liu Songguo, Huang Xiaoqin, Shi Feng, Mai Liantao, Fang Hongbo, Zhao Hongkai, Huang Xiaofang, Tu Wanbin.

The construction of smart city is a complicated large-scale system project, and its information security issues are particularly important. Smart city with massive information The operation and innovation concept is characterized by the Internet, the Internet of Things, cloud computing, mobile Internet, etc. are all important support, so its information and network are The security issues to the application terminal are more than the general Internet information security issues, including privacy issues, credibility issues, anti-counterfeiting, and business rejection (DoS) Intrusion and attack problems, etc. Information perception layer, access and transmission layer, application layer and terminal layer of the system, intelligent/smart processing and collaboration There are security risks at many levels such as the platform layer; the multi-user lease of cloud platforms includes issues such as intellectual property rights and privacy protection, giving them security Obstacles bring new challenges; equipment unattended, adaptive management and self-breaking, self-connecting and other states also increase the difficulty of designing and implementing safety systems Degree; for mutual recognition, communication and communication between intelligent objects, it is necessary to reliably ensure their information security and even privacy rights; and multiple and heterogeneous The characteristics of interconnection and distributed computing make it difficult to integrate the

security system, and the complex social management environment also brings many unexpected insecurity. These unsafe factors may affect the operation of the entire city, and put forward higher requirements for information security. For this, need According to the characteristics of smart cities, from the perspective of information security management and technical assurance, the information security guarantee rules for the whole process of smart city construction are given Fan, specially formulated this guiding technical document. This guidance technical document can be used by all relevant units in the construction of smart cities The relevant units clarify the information security requirements and responsibilities of each stage of the full life cycle of smart city construction and provide guidance to ensure the construction of smart city Establish the rights and interests of all parties of the main body, enhance the ability to resist risks and control independently, and can also serve smart city management, engineering technology and third parties And other relevant personnel to provide management and technical reference. Information Security Technology Guide to Information Security Guarantee for Smart City Construction

1 Scope

GB/Z 38649-2020 is the Chinese national standard on information security technology - guide of information security assurance framework for smartcities, in the field of information technology. The /Z suffix marks it as a guiding technical document: it does not prescribe requirements that can be certified against, but sets out the technique, the method or the state of the art that the standards bodies recommend following. It was issued on 28 April 2020 by the State Administration for Market Regulation; Standardization Administration of China. As a guiding technical document it carries no separate date of entry into force: it applies from publication. Classification: ICS 35.040, CCS L80. This page is published from the official record of the standard held by the Chinese standards administration: the identification, the dates, the classification and the issuing body are taken from there. The clause text, the tables and the numeric limits are in the document itself, which is delivered complete in English translation.

This guiding technical document provides information security guidance for the entire process of smart city construction, including planning and Information security for the entire process from demand analysis, design, construction, inspection and acceptance, operation and maintenance, supervision, inspection and evaluation to optimization and continuous improvement Guaranteed management mechanism and technical specifications. This guidance technical document is applicable to the planning, management, construction, and operation of smart cities, and can also be related to the construction of information security for other smart cities. The basis for standard formulation provides basis and reference.

2 Normative references

The following documents are essential for the application of this document. For dated

references, only the dated version applies to this article Pieces. For the cited documents without date, the latest version (including all amendments) applies to this document.

GB/T 22080-2016 Information Technology Security Technology Information Security Management System Requirements

GB/T 22081-2016 Information Technology Security Technology Information Security Control Practice Guide

GB/T 22239-2019 Information security technology network security level protection basic requirements

GB/T 25069-2010 Information Security Technical Terms

GB/T 25070-2019 Information Security Technology Network Security Level Protection Security Design Technical Requirements

GB/T 34678-2017 Smart City Technology Reference Model

GB/T 36333-2018 Smart City Top Level Design Guide

3 Terms and definitions

GB/T 22080-2016, GB/T 22081-2016, GB/T 22239-2019, GB/T 25069-2010, GB/T 34678-2017 and GB/T 36333-2018 and the following apply to this document.

3.1 Security domain Subnets that have the same security protection requirements, trust each other, and have the same security access control and border control policies in the same system Or network, and the same network security level, share the same security strategy. Broadly understood as IT departments with the same business security requirements Collection of traditional elements.

3.2 Secure area boundary Connect and implement security policies for the secure computing environment boundary of the grading system, and between the secure computing environment and the secure communication network Related parts.

3.3 Virtual machine; virtualmachine; VM Host operating environment realized by software, etc.

Note. Including virtualized hardware, operating system, middleware and application programs.