ICS 35.240.01
L 70

中华人民共和国国家标准

GB/T 36621—2018

智慧城市　信息技术运营指南

Smart city—Guide for information technology operation

2018-10-10 发布　　2019-05-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位:智慧神州(北京)科技有限公司、中国电子技术标准化研究院、山西奥斯迪信息工程有限公司、华为技术有限公司、中国电子科技集团公司信息科学研究院、深圳赛西信息技术有限公司、北京航空航天大学、北京清华同衡规划设计研究院有限公司、北京天融信网络安全技术有限公司、沧州市智慧城市建设办公室、浙江大华技术股份有限公司、建设综合勘察研究设计院有限公司、北京智城信服科技有限公司、慧与(中国)有限公司、中电科新型智慧城市研究院有限公司、大唐软件技术股份有限公司、中国电子科技集团公司第二十八研究所、北京计算机技术及应用研究所、北京博锐智汇科技有限公司、浙江省杭电智慧城市研究中心。

本标准主要起草人:刘棠丽、赵菁华、吕卫锋、张红卫、相明科、崔昊、李赟、王飞飞、荣文戈、刘博胜、李方平、袁媛、秦永辉、刘延锋、李娜、张钊源、乔进朝、康子路、王树东、杨圣伟、刘晓勇、常向魁、梁勇、任爱涛、林雪梅、任燕、张凯、李毅、陈思、王新颖、王龑、李君兰、吴辉、郭春伟、孙亭、张大鹏、杨磊、董南、彭革非、陈伟权。

引　言

智慧城市是一项涉及物联网、云计算、大数据等众多技术与城市管理、公共服务、市民生活等诸多应用领域的系统工程。智慧城市运营是城市智慧化运转的核心，智慧城市信息技术运营标准化工作是其中一项重要基础性工作。为确保智慧城市运行的安全性、高效性，特制定本标准。

智慧城市　信息技术运营指南

1　范围

本标准提供了智慧城市运营的总体框架及ICT基础设施运营、数据运营、信息系统运营、安全运营等方面的相关建议。

本标准适用于智慧城市信息技术运营体系的建立和管理、运营监督和评价。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 19659.1　工业自动化系统与集成 开放系统应用集成框架 第1部分：通用的参考描述

GB/T 20720.1　企业控制系统集成　第1部分：模型和术语

GB/T 20720.2　企业控制系统集成　第2部分：对象模型属性

GB/T 20720.3　企业控制系统集成　第3部分：制造运行管理的活动模型

GB/Z 20986—2007　信息安全技术　信息安全事件分类分级指南

GB/T 20988—2007　信息安全技术　信息系统灾难恢复规范

GB/T 22239—2008　信息安全技术　网络安全等级保护基本要求

GB/T 26327—2010　企业信息化系统集成实施指南

GB/T 26335　工业企业信息化集成系统规范

GB/T 28827.1—2012　信息技术服务　运行维护　第1部分：通用要求

GB/T 28827.3—2012　信息技术服务　运行维护　第3部分：应急响应规范

GB/T 29245—2012　信息安全技术　政府部门信息安全管理基本要求

GB/T 30285—2013　信息安全技术　灾难恢复中心建设与运维管理规范

GB/T 34678—2017　智慧城市　技术参考模型

国家网络安全事件应急预案（中网办发文〔2017〕4号）

3　术语和定义

下列术语和定义适用于本文件。

3.1

智慧城市信息技术运营　smart city information technology operation

运用信息技术对城市智慧化相关的信息通信技术基础设施、数据、信息系统及其所承载服务开展的运行和管理过程。

4　缩略语

下列缩略语适用于本文件。

ICT：信息通信技术(Information and Communication Technology)

UPS：不间断电源(Uninterruptible Power System/Uninterruptible Power Supply)

5 总体原则

5.1 总体框架

智慧城市信息技术运营的总体框架见图1。

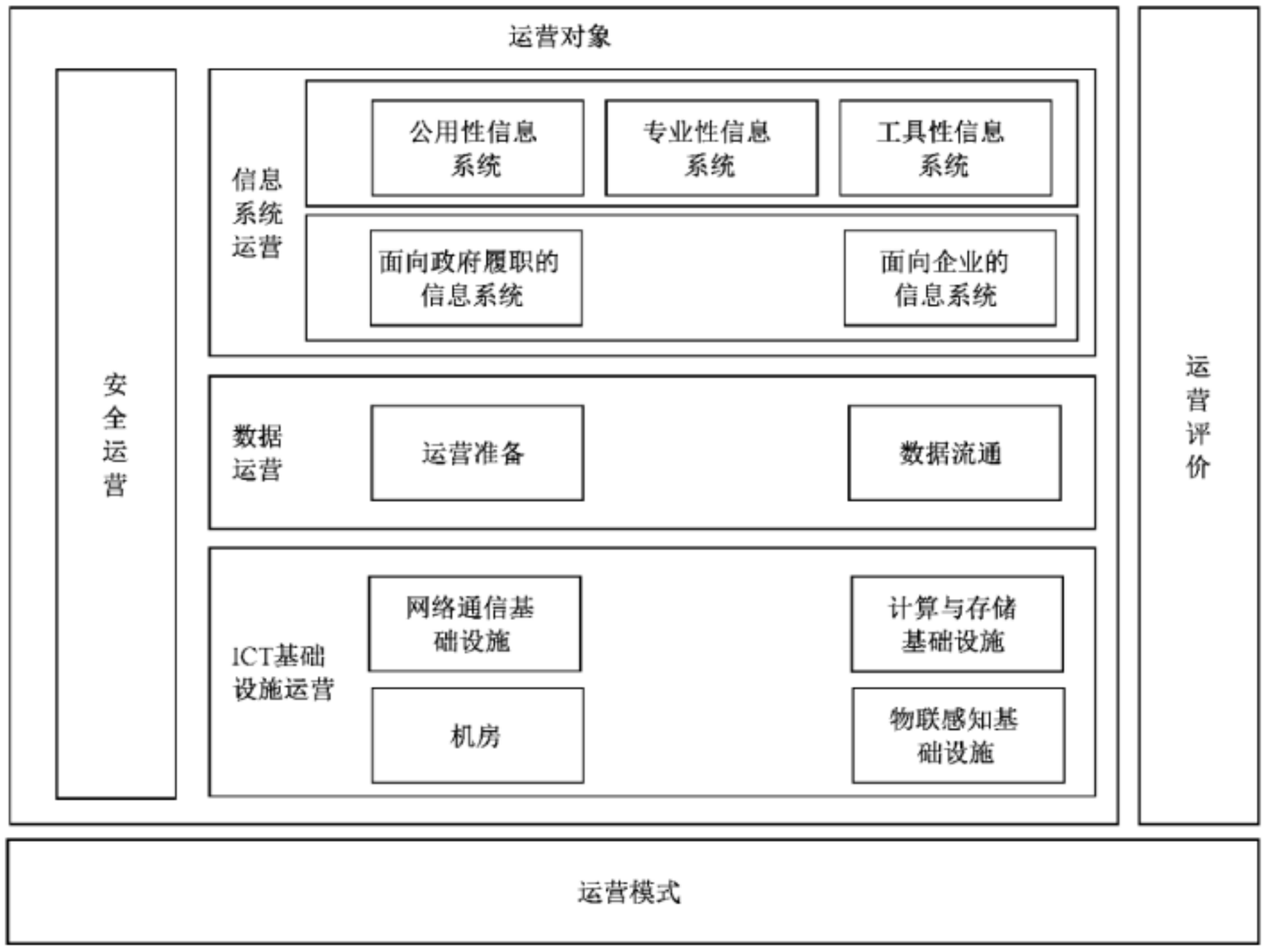

图1 智慧城市信息技术运营总体框架

5.2 需考虑的因素

5.2.1 智慧城市信息技术运营需考虑运营对象、运营评价、运营模式三方面内容。

5.2.2 智慧城市信息技术的运营对象包括信息系统运营、数据运营、ICT基础设施运营、安全运营四方面的相关对象。

5.2.3 智慧城市信息技术运营宜在确定运营对象基础上，确定运营的职责、具体内容、技术要求、工作流程等内容。

6 ICT基础设施运营

6.1 概述

6.1.1 智慧城市ICT基础设施方面的运营对象包括：机房、物联感知基础设施、网络通信基础设施和计算与存储基础设施等。

6.1.2 建议明确ICT基础设施运营方与智慧城市相关管理机构的经营责权。

6.1.3 ICT基础设施运营方面的相关建议如下：

a) 交通、通信、电力等重点领域的 ICT 基础设施运营应遵循相关标准；
b) ICT 基础设施的互联互通应符合城市 ICT 基础设施发展规划，可确保 ICT 基础设施运营安全，保障用户权益；
c) ICT 基础设施的互联互通可作为单独项目进行投资建设运营，也可纳入 ICT 基础设施建设运营项目；
d) ICT 基础设施运营方同时经营其他智慧城市业务的，应确保设施建设、数据采集、分析和查询等服务运营成本和收入真实准确；
e) ICT 基础设施运营方应按照有关规定针对提供服务的条件、获得服务的程序和剩余服务能力等信息进行公开，公平、公正地为所有用户提供设施建设、数据采集及分析查询等服务；
f) ICT 基础设施运营方不应排挤其他相关经营主体，不应拒绝为符合条件的用户提供服务或者提出不合理的要求；
g) ICT 基础设施运营方应遵守价格主管部门有关 ICT 基础设施建设、数据采集、分析查询等 ICT 基础设施服务价格的规定，并与用户签订 ICT 基础设施服务合同；
h) 通过 ICT 基础设施提供的数据和服务应符合相关质量标准，并符合 ICT 基础设施运营方和委托方的相关安全和技术要求；
i) ICT 基础设施需要永久性停止运营的，运营方应提前告知原审批、核准或者备案部门及相关主管部门，并通知服务用户，不得擅自停止运营；
j) ICT 基础设施停止运营、封存、报废的，运营方应按照国家有关规定处理，组织拆除或者采取必要的安全防护措施；
k) ICT 基础设施运营方应按照有关规定提交真实准确的统计信息，并对涉及商业秘密的信息采取保密措施。

6.2 机房

机房运营方面的相关建议如下：

a) 宜通过提供监控室和监控终端，对资源的运行状况进行 7×24 h 监测、记录和趋势分析。其中，机房监控的内容包括但不限于：空调温湿度、漏水告警、电流电压、UPS 负载、消防气体钢瓶压力等。
b) 宜配置 7×24 h 值班人员，负责数据中心基础设施的日常巡检，并检查、记录基础设施运行情况，及时处理发现的问题。
c) 宜实现资源的统一管理和优化，可采用的措施包括：机柜空间释放、机房的温湿度调整、机房高低压配电调整、机房 UPS 设备负载调整、消防气体钢瓶增压等。
d) 宜制定机房环境安全、线缆通信安全、设备安全等运行安全管理制度。
e) 宜实现机房运行的监控管理，包括机房整体集中展现、机柜运行状态展现、应急集中关机等。
f) 宜保障机房相关配套基础设施的日常运行管理、维护和巡检，配套基础设施包括供配电系统、机房空调系统、新风系统、消防系统、漏水检测系统、监控系统、门禁系统等。
g) 宜安排专人负责机房、现场支持值班室及其周边环境的清洁卫生。

6.3 物联感知基础设施

6.3.1 智慧城市运营阶段宜保证前端物联感知基础设施的安全，为智慧城市信息技术运营提供准确、安全、完整的基础数据支撑。

6.3.2 物联感知基础设施运营方面的建议如下：

a) 应保证前端物联感知设备工作环境的安全稳定性，工业控制领域的物联感知设备方面应遵循工控信息安全相关标准的安全要求；
b) 建立统一的标识管理和身份认证机制，保证物联感知设备合法、有序接入；
c) 建立传输、配电、加热/通风等物联感知基础设施配套支撑设备的安全管理机制；
d) 建立物联感知设备软硬双层安全防护；
e) 对于敏感物联感知设备，应防止未授权访问、窃取、损坏和干扰，确保采集数据和执行指令的真实性、准确性和可用性；
f) 严格管理敏感物联感知设备访问控制权限，保证敏感数据不被泄露，物联感知设备被访问应授权并被记录；
g) 应保证物联感知设备接入控制安全、访问控制、资源控制、配置更新、数据安全、恶意入侵和代码防范、管理运维安全。

6.4 网络通信基础设施

6.4.1 根据 GB/T 34678—2017 中 8.2 规定，网络通信分为公共网络和专用网络。

6.4.2 网络通信基础设施运营的相关建议如下：

a) 计算与存储基础设施公共网络运营应满足运营商相关运营管理要求；
b) 专用网络运营模式应包括但不限于：分散运营、集中运营；
c) 分散运营可由资产拥有者自身运营，也可采用服务外包方式运营；
d) 集中运营应采用服务外包方式运营。

6.5 计算与存储基础设施

计算与存储基础设施运营方面的相关建议如下：

a) 支持高可用性部署，支持智慧城市关键计算基础设施业务转离受自然灾害等不可控因素影响的区域。
b) 智慧城市关键业务数据的处理与存储基础设施应位于中国境内。
c) 硬件系统运营维护应支持包括基本安装、按服务条款维护以及按次计的故障维修，维护地点可以是用户所在地或厂商的维护中心。电话热线解决问题和收费的升级维护应包括在硬件维护服务范围内。
d) 软件系统运营维护应支持包括故障排除服务、预防性维护服务、软件管理服务等，维护地点可以是用户所在地。
e) 采用高安全性的数据备份保护机制。
f) 制定计算与存储基础设施的数据访问策略，规定数据可被存放的地理区域及相关安全要求，明确数据可被访问的人员角色和操作权限。
g) 提供计算与存储基础设施资产管理，覆盖采购、入库、库存、分派、部署、监控、更新、保修、维保，直至报废处置的整个周期，管理和控制资产的开销与服务。

7 数据运营

7.1 概述

智慧城市数据运营包括运营准备和数据流通两个阶段。

7.2 运营准备

7.2.1 资源梳理

7.2.1.1 资源梳理包括数据目录梳理、数据脱敏脱密、目录活化、资源图谱、资源画像等内容。

7.2.1.2 资源梳理方面的相关建议如下：

a) 数据目录梳理：应包括元数据管理、指标管理、分类管理、标签管理、数据编码等内容。

b) 数据脱敏脱密：即保密信息通过脱敏脱密规则进行数据的变形，实现敏感隐私与保密数据的可靠保护。数据脱敏脱密应分别从数据层脱敏脱密和应用层脱敏脱密。

c) 目录活化：即在数据目录上加载数据编址、数据组装等功能。目录活化应实现数据服务请求和数据源的打通，并通过访问监测及时获取到数据源的变更情况，以及对数据目录的同步维护。

d) 资源图谱：可将已有目录进行数据关联和分类归集，通过算法模型、语义分析等人工智能处理，构建起多种维度的可视化图谱。

7.2.2 确权授权

7.2.2.1 数据确权包括数据所有权、数据使用权、数据管理权、数据处理权、数据知晓权、数据隐私权确立等内容。

7.2.2.2 数据所有权包括政府数据所有权和企业数据所有权。数据权方面的建议包括：

a) 在数据目录梳理的过程中进行登记确权，数据所有权应归属采集部门；

b) 应由企业申报并经协议确认后进行企业数据的登记确权。其中，企业数据指企业自己在生产经营过程中产生的数据。

7.2.2.3 数据使用权方面的建议如下：

a) 建议将数据向社会进行适度开放；

b) 企业数据应由所有权归属企业授权提供给第三方进行处理或使用，并获得第三方提供的数据服务或经济收益；

c) 个人数据应由本人授权提供给第三方进行处理或使用，并获得第三方提供的数据服务。

7.2.2.4 数据管理权方面，通过对数据进行存储、备份等，保持数据的完整性。

7.2.2.5 数据处理权方面，应对数据进行进一步加工，形成新的数据和服务。

7.2.2.6 数据知晓权方面，应允许相关机构通过知晓数据来获取外部信息。

7.2.2.7 数据隐私权方面，数据管理方在提供数据给第三方使用时，在涉及个人或企业的非公开信息时，应经过数据所属者的授权才可以提供数据服务。

7.3 数据流通

7.3.1 数据共享

7.3.1.1 数据共享平台可提供城市信息资源点到点、点到中心、中心到中心的各种业务场景下的数据交换、数据共享服务。

7.3.1.2 数据共享平台一般由政府/企业投资建设，或政府企业共同投资建设，数据共享平台的运营可由政府运营，或者政府授权企业运营。

7.3.1.3 数据共享运营建议采用以下模式：

a) 平台运营：市、区、县或委办局根据业务需求租用数据共享平台，费用主要指平台服务费；

b) 接入点运营：市、区、县或委办局根据业务需求按点接入数据共享平台，费用主要包括接入费

用、服务费；

c) “平台＋接入点”运营：市、区、县或委办局根据业务需求租用数据共享平台，费用主要包括平台服务费、每增加一个接入点的接入费。

7.3.2 数据开放

7.3.2.1 数据开放是指数据对社会的开放，应包括无条件开放和契约式开放两种形式。

7.3.2.2 在涉及个人及企业的隐私与保密信息时，宜通过授权、鉴权的方式形成开放契约，确保数据是经过数据所有方和提供方的授权，保障数据的合规、安全使用。

7.3.3 数据交易

为实现数据使用价值，宜通过数据生产、数据流通、数据应用等环节开展数据交易。

8 信息系统运营

8.1 概述

8.1.1 根据功能的不同，信息系统可分为三大类：公用性信息系统、专业性信息系统和工具性信息系统。

8.1.2 根据建设主体的不同，信息系统可分为两大类：面向政府履职的信息系统和面向企业的信息系统。

8.2 按信息系统功能划分的运营

8.2.1 公用性信息系统

8.2.1.1 项目建成后由运营方负责在运营期间持续为使用者提供技术支持和专业信息服务。

8.2.1.2 公用性信息系统运营方面的相关建议如下：

a) 根据项目的业务定位与能力，梳理各单位服务需求，策划运营服务的具体内容与要求，并细化整理形成服务目录。运营中心的服务目录包括但不限于基础服务如场地服务、城市运行体征监测等，增值服务如针对各领域、行业、部门的运行状况监测预警等。公共信息与服务支撑平台服务目录包括但不限于资源授权、确权、开发环境与运行环境等。

b) 根据项目业务定位与发展需要，制定相应的项目运营模式，运营模式可以是购买服务模式、场地租赁模式、扩展服务模式、管理输出模式等。

c) 根据业务发展需要，建立相应的沟通协调管理机制支持服务目录的实施或实现。应建立相应的协调组织机构推动相关的工作，确保项目日常运行过程中数据接入、各部门资源的协调、跨部门跨领域的协同与联动；对涉及的部门职能、人员、资源、任务进行梳理和优化，组织机构按照相关的法律、法规政策开展相关工作，统筹推进各项工作并负责评价与考核等。

d) 建立项目的日常运行机制，明确本项目的业务范围与职能，与国家级、城市其他平台或中心的相互关系与职责边界，明确相互协作的业务流程与合作运行机制。

e) 研究并制定数据接入来源渠道，数据接入来源包括但不限于政府已有云计算/数据中心、电信运营商、网络服务提供商等。

f) 在相关的合同、章程中明确政府方对政府数据的所有权及掌控权，并签署相关保密协议确保政府数据的保密和安全需求。

8.2.2 专业性信息系统

8.2.2.1 宜建立跨部门协调机制和组织，支持跨部门的信息整合、综合展现、业务协同。

8.2.2.2 建议各业务系统信息模型和元数据进行统一管理，支持多应用系统的数据整合，为智慧城市运营管理系统的信息综合展现和业务协同提供支撑。

8.2.3 工具性信息系统

8.2.3.1 工具性信息系统的运营管理包括日常运行、事件管理、故障告警、日志管理、计量管理五个方面。

8.2.3.2 工具性信息系统运营方面的相关建议如下：

a) 提供监控室或监控终端，对资源的运行状况进行监测、记录和趋势分析；
b) 配置监控工具，通过声音、短信、电话和邮件等告警方式进行报警提醒；
c) 建立运行服务资源监测制度，规范服务监测的人员操作和监测指标等；
d) 对监控记录数据进行保存，保存期至少半年；
e) 建立运行事件管理机制，管理内容包括但不限于：建立事件响应组织、制定事件响应制度、制定事件响应预案等；
f) 制定演练计划，确保事件预案的有效性，演练内容包括但不限于：演练准备、实施演练、演练总结分析、事件预案优化等；
g) 在监控指标超出阈值范围提出告警；
h) 支持按多种条件对告警信息进行查询；
i) 提供告警分级分域上报，各级域用户应见本级域内告警信息；
j) 提供统一的日志采集功能，为运维监控、安全监管等提供统一日志采集服务；
k) 支持业务数据统计、服务流程统计、性能监测统计、配置数据统计；
l) 支持日志的分类、日志导入导出、日志转存；
m) 支持按照多种模式对用户对于资源的使用情况进行计量；
n) 针对每一类资源服务分别规范其服务度量计价要素和计价模式；
o) 将各类资源服务计价要素分解到可度量计价的粒度，包括服务类别、度量指标项(基准单位、等级划分参数、数值)、数量、时长、价格(单价、总价)。

8.3 按信息系统建设主体划分的运营

8.3.1 面向政府履职的信息系统

面向政府履职的信息系统运营方面的相关建议如下：

a) 按照 GB/T 28827.1—2012 第 6 章～第 9 章的相关要求，规定运营方在人员、资源、技术和过程方面应具备的条件和能力；
b) 涉及政府部门信息安全防护应按照 GB/T 29245—2012 第 5 章的要求；
c) 保证智慧城市信息系统运营所需的资源，例如，资金、场地、人力等；
d) 组建专业的智慧城市信息系统运营以及第三方安全支撑服务团队，制定第三方安全支撑服务机制和人员从业管理制度，对关键人员要求签署保密协议，明确相关方的目的、义务与责任；
e) 制定智慧城市安全工程实施、供应链及合规性管理的策略和制度，明确运营管理的责任部门、责任人和工作职责；
f) 保证国家关键信息基础设施安全运行，规范操作规程，采用通过国家相关部门安全资质认证的

产品和服务，并建立相关产品和服务备案机制；

g） 对网络设备的报警检查、服务器的日志检查、服务器安全策略配置、安全漏洞扫描、物理机房安全检查等进行网络安全监测，发现问题应按照 GB/T 28827.3—2012 第 6 章、第 7 章，启用应急响应机制。

8.3.2 面向企业的信息系统

8.3.2.1 面向企业的信息系统建设运营宜遵循国家信息化规划要求。

8.3.2.2 面向企业的信息系统运营相关建议如下：

a） 按照 GB/T 26327—2010 第 5 章，根据企业所处的集成阶段设计不同的集成方案，采用信息资源共享和知识管理等技术；

b） 企业数据集成包括纵向集成和横向集成，应按照 GB/T 26335、GB/T 20720.1、GB/T 20720.2、GB/T 20720.3、GB/T 19659.1 的要求执行；

c） 企业信息系统应确保用户个人敏感信息的安全；

d） 企业信息系统应确保信息的可追溯性、可靠性与安全性；

e） 特殊行业企业信息系统应遵循该行业的相关标准。

9 安全运营

9.1 概述

智慧城市安全运营特指智慧城市相关基础设施、数据、信息系统的网络安全运营，其内容包括：监测预警、应急处置以及灾难恢复。

9.2 安全运营职责

智慧城市安全运营职责一般包括：

a） 负责智慧城市网络安全运行与维护管理；

b） 监测智慧城市网络安全风险，分析安全态势；

c） 发现智慧城市网络安全事件和脆弱性，防范、阻断网络攻击；

d） 共享智慧城市网络安全威胁信息，及时通报智慧城市网络安全事件；

e） 制定、评估并修订智慧城市网络安全事件应急预案；

f） 定期开展智慧城市网络安全应急演练活动；

g） 应急处置智慧城市网络安全风险与网络安全事件；

h） 及时向上级管理部门上报网络安全威胁信息与网络安全事件；

i） 保证灾后城市信息系统快速恢复正常运转状态；

j） 有效控制智慧城市网络安全事件造成的负面影响。

9.3 安全运营内容

9.3.1 监测预警

9.3.1.1 智慧城市网络安全运营者宜依据网络安全标准，建立智慧城市网络安全监测预警体系，监测智慧城市信息系统运行状态，发现智慧城市信息系统的脆弱性和安全风险，收集分析智慧城市网络安全事件信息，对安全风险及时上报和通报，按需发布智慧城市网络安全监测预警信息。

9.3.1.2 监测预警方面的相关建议如下：

a) 按照《国家网络安全事件应急预案》规定的第3章进行预警分级、监测预警、预警研判及预警响应发布与解除；

b) 按照GB/T 22239—2008中第8章，采用安全保护能力中第三级或以上安全要求，对智慧城市中的基础信息网络、信息系统、云计算平台、大数据平台、物联网系统、工业控制系统等的运行状态、脆弱性以及恶意攻击风险进行监测、监控；

c) 建立智慧城市网络安全威胁信息交换系统，制定城市威胁信息共享机制，监测、监控数据行为风险；

d) 监控智慧城市信息系统的整体运行状态，对关键信息基础设施系统的网络和系统、设备、环境、资产，以及介质等进行安全控制和权限管理，对日志、监测数据和报警数据，及时发现网络安全风险，感知城市网络安全态势，保证智慧城市信息系统日常的安全运行和业务连续性；

e) 建立有效的安全漏洞和恶意代码识别机制，采取必要措施修补和防范；

f) 建立智慧城市网络安全事件上报与通报机制，建立通报预警系统。

9.3.2 应急处置

9.3.2.1 智慧城市网络安全运营者按照法律法规、政策文件和网络安全标准的要求，制定智慧城市网络安全事件应急预案，对不同级别的事件，明确启动条件、处理流程、恢复流程。

9.3.2.2 应部署安全保护措施，预防智慧城市网络安全事件的发生。

9.3.2.3 在发生网络安全事件时，及时采取应急处置措施，向主管部门上报智慧城市重大网络安全事件。

9.3.2.4 应急处置方面的相关建议如下：

a) 应按照《国家网络安全事件应急预案》规定制定智慧城市网络安全事件应急预案；

b) 制定智慧城市网络安全事件应急处置机制，提高城市应对网络安全事件的能力，降低网络安全事件的风险和影响；

c) 按照《国家网络安全事件应急预案》规定的第1.4章节及GB/Z 20986—2007中第5章的要求，对网络安全事件进行分级；

d) 根据网络安全事件的不同的分类分级，制定应急处理流程、系统恢复流程等；

e) 定期开展智慧城市应急演练活动，验证可操作性，并向上级主管部门上报演练情况；

f) 定期对应急预案的有效性进行评估，定期对应急预案和处置流程优化完善；

g) 根据报告和通报机制，对智慧城市网络安全事件及安全弱点及时上报、调查和评估；

h) 定期开展智慧城市网络安全相关教育、培训，提供人员、资源和相关保障；

i) 当网络安全事件发生时，应及时进行处置，必要时启动跨部门、跨行业、跨系统的应急处置预案；

j) 建立智慧城市网络安全事件应急指挥体系，统筹协调各部门，制定有效的跨部门联动应急处置机制，保障应对网络安全事件时的响应、处理和恢复有序进行，定期进行应急演练以提高各部门协同配合能力；

k) 按照GB/T 22239网络安全等级保护基本要求，满足应急预案管理和网络安全事件处置相关的等级保护要求。

9.3.3 灾难恢复

9.3.3.1 在智慧城市网络安全事件发生后，智慧城市网络安全运营者根据网络安全事件的影响程度和业务的优先级，采取适当的恢复措施，确保智慧城市信息系统业务流程按照规划目标恢复。

9.3.3.2 灾难恢复方面的相关建议如下：

a) 根据智慧城市业务的重要性，对业务信息、重要系统和数据资源进行容灾备份；

b) 按照 GB/T 20988—2007 中第 7 章和 GB/T 30285—2013 中第 8 章，制定智慧城市网络安全灾难恢复策略和流程，建立智慧城市网络安全事件处理及恢复中心，制定容灾机制，实现快速协同处理，降低或控制城市信息安全事件的影响，及时恢复智慧城市信息系统正常的运转状态；

c) 按照 GB/T 22239 网络安全等级保护基本要求标准，满足备份与恢复管理相关的等级保护要求。

10 运营模式

10.1 常见的智慧城市运营模式包括：政府投资建设政府运营、政府投资建设企业运营、企业投资建设企业运营、合伙投资建设企业运营。

10.2 宜通过对城市的投融资渠道与主体、市场能力、产业链、项目资金来源、财政承受能力、使用需求、市场化程度、回报机制、风险管理等多个维度进行定性定量分析，确定智慧城市运营模式，明确不同角色的职责分工、投融资方式及运营方式。

10.3 各地宜建立个性化的智慧城市运营模式。

10.4 智慧城市运营模式宜兼顾各相关方利益。

11 运营评价

11.1 概述

11.1.1 应针对智慧城市信息技术运营过程中提供服务的效率、效益、效果、能满足运营要求而持续提供服务的能力等方面进行综合考量。

11.1.2 评价对象应涉及智慧城市的各类运营事项。

11.1.3 评价主体可为城市管理者、服务对象、第三方评价机构等。

11.1.4 评价客体应为服务提供者。

11.1.5 评价目的包括：发现服务偏差，修正运营控制项，促进运营目标实现；对购买服务（资本支出或资源置换）提供支付依据或置换效果评判；对产业运营管理提供产业政策调整参考；对投融资的方式、方法、措施的调整提供参考；对运营发展提供决策依据。

11.1.6 评价范围可由运营的服务边界确定。

11.2 总体要求

智慧城市运营评价方面的相关建议如下：

a) 评价依据可包括为支持运营而签订的服务合同及本交易中其他相关文件；

b) 评价指标、数据权值、量化分类、采集节点由评价主体、客体协商确定；

c) 应针对不同的运营服务类别，确定具体的评价周期；

d) 数据采集可利用网上采集和线下调查问卷、访谈等方式；

e) 结果识别可包括多渠道采集数据，多方式分析评价，相互印证，综合甄别等；

f) 信息技术服务类评价报告宜按月或季以文本方式报告，产业、投融资、其他运营的评价报告周期可根据运营类别确定；

g) 若运营过程发现重大问题或预测有严重风险时应及时报告。

11.3 评价模型构建

11.3.1 可从评价输入、评价方法、评价结果等方面来建立智慧城市运营评价模型。

11.3.2 运营评价模型构建方面的建议如下：

a) 输入反映服务质量、服务数量、服务效果、服务持续能力的数据及矫正评价目标的要素权值；

b) 依照评价目标，通过设定评价指标和评价模型，运用特定的评价标准，按照严格的评价流程，在定量与定性相结合的基础上进行对比分析，对运营服务的效率、效益、效果等方面，做出客观、公正的判断；

c) 应建立评价结果，形成服务运营评价报告。

中 华 人 民 共 和 国
国 家 标 准
智慧城市 信息技术运营指南
GB/T 36621—2018
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2018年9月第一版
*
书号:155066·1-61198

GB/T 36621-2018