ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 38649—2020

信息安全技术
智慧城市建设信息安全保障指南

Information security technology—
Guide of information security assurance framework for smartcities

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本指导性技术文件按照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。

本指导性技术文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本指导性技术文件起草单位:浙江省经济信息中心、中国电子技术标准化研究院、中国信息安全测评中心、国家信息中心、中电长城网际系统应用有限公司、中电海康集团有限公司、阿里云计算有限公司、杭州安恒信息技术有限公司、西南科技大学、浙江省发展信息安全测评技术有限公司、浙江省标准化研究院、浙江省电子产品检验所、杭州云嘉云计算有限公司、成都秦川物联网科技股份有限公司、浙江安科网络技术有限公司、深信服科技股份有限公司、浙江鑫诺检测技术有限公司、杭州世平信息科技有限公司。

本指导性技术文件主要起草人:吴前锋、上官晓丽、王惠莅、杜宇鸽、许涛、闵京华、谢海江、张向阳、黄洪、赵一农、范渊、王勃艳、张大江、张君、陈自力、祝利锋、周俊、王世晞、俞群爱、李宁、邵泽华、张亮、齐同军、刘松国、黄晓芹、史锋、麦联韬、方洪波、赵宏凯、黄晓芳、涂万彬。

引　言

智慧城市建设是一项复杂的大型系统工程，其信息安全问题显得尤为重要。智慧城市以海量信息运作与创新理念为特征，互联网、物联网、云计算、移动互联网等均为其重要支撑，因此其信息与网络乃至应用终端的安全问题均比一般互联网的信息安全问题要多，包括隐私问题、可信问题、防伪、业务拒绝(DoS)侵入与攻击问题等。系统的信息感知层、接入与传送层、应用层与终端层、智能/智慧处理及协同平台层等诸多层面存在安全风险；云平台多用户租用的包括知识产权与隐私权保护等问题，给其安全保障带来新挑战；设备无人值守、自适应管理与自断、自通连接等状态，也增加了安全系统的设计与实施难度；智能物体间进行互相识别、互通与交流，需要可靠地确保其信息安全性乃至隐私权等；而且多元异构互联、分布计算等特性导致其安全体系一体化整合难度很大，复杂的社会管理环境等也带来诸多突发性不安全因素。这些不安全因素可能会影响整个城市运行，对信息安全保障提出了更高的要求。为此，需要针对智慧城市的特征，从信息安全管理和技术保障等视角，给出智慧城市建设全过程信息安全保障规范，特制定本指导性技术文件。

本指导性技术文件可用于智慧城市建设各相关单位，有助于信息安全主管部门为智慧城市建设相关单位明确智慧城市建设全生命周期各阶段的信息安全保障要求与责任提供指导，以保障智慧城市建设主体各方的权益，增强抵御风险和自主可控的能力，同时可为智慧城市管理、工程技术及第三方服务等相关人员提供管理和技术参考。

信息安全技术
智慧城市建设信息安全保障指南

1 范围

本指导性技术文件提供了智慧城市建设全过程的信息安全保障指导，包括智慧城市建设从规划与需求分析、设计、实施施工、检测验收、运营维护、监督检查与评估到优化与持续改进的全过程信息安全保障的管理机制与技术规范。

本指导性技术文件适用于智慧城市规划、管理、建设、运营，也可为其他智慧城市建设信息安全相关标准的制定提供依据和参考。

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 22080—2016 信息技术 安全技术 信息安全管理体系 要求

GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2010 信息安全技术 术语

GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 34678—2017 智慧城市 技术参考模型

GB/T 36333—2018 智慧城市 顶层设计指南

3 术语和定义

GB/T 22080—2016、GB/T 22081—2016、GB/T 22239—2019、GB/T 25069—2010、GB/T 34678—2017 和 GB/T 36333—2018 界定的以及下列术语和定义适用于本文件。

3.1

安全域 security domain

同一系统内有相同的安全保护需求，相互信任，并具有相同的安全访问控制和边界控制策略的子网或网络，且相同的网络安全等级，共享一样的安全策略。广义可理解为具有相同业务安全要求的 IT 系统要素的集合。

3.2

安全区域边界 secure area boundary

对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。

3.3

虚拟机 virtual machine；VM

通过软件实现的主机运行环境等。

注：包括虚拟化硬件、操作系统、中间件和应用程序等。

3.4

多租户技术　multi-tenancy technology

一种软件架构技术，实现多用户的环境下共用相同的系统或程序组件，并且仍可确保各用户间数据的隔离性。

3.5

多租户隔离　multi-tenancy isolation

在多租户的应用环境下的安全防护技术，通过物理隔离、虚拟化和应用支持的多租户架构等方式实现不同租户之间数据和配置的安全隔离，以保证每个租户数据的安全与隐私。

4　缩略语

下列缩略语适用于本文件。

APT：高级持续性威胁(Advanced Persistent Threat)

DoS：拒绝服务攻击(Denial Of Service)

IPSec：IP 安全协议(Internet Protocol Security protocol)

TLS：安全传输层协议(Transport Layer Security)

VPN：虚拟专用网(Virtual Private Network)

5　概述

5.1　智慧城市建设信息安全需求

智慧城市整体框架与主要特征参见附录 A。智慧城市可分为五个层次，即物联感知层、网络通信层、计算与存储层、数据及服务融合层、智慧应用层，五个层次都可能面临着各类不同的安全威胁，需要在智慧城市建设中对每个层次进行安全保障，并根据智慧城市特征建立已知威胁纵深防御支撑、高级威胁感知监控支撑、组织管理机制流程支撑、规范运营决策应急支撑等安全体系支撑，为智慧城市建设利益相关者提供安全保障。图 1 为智慧城市建设信息安全需求示意图。

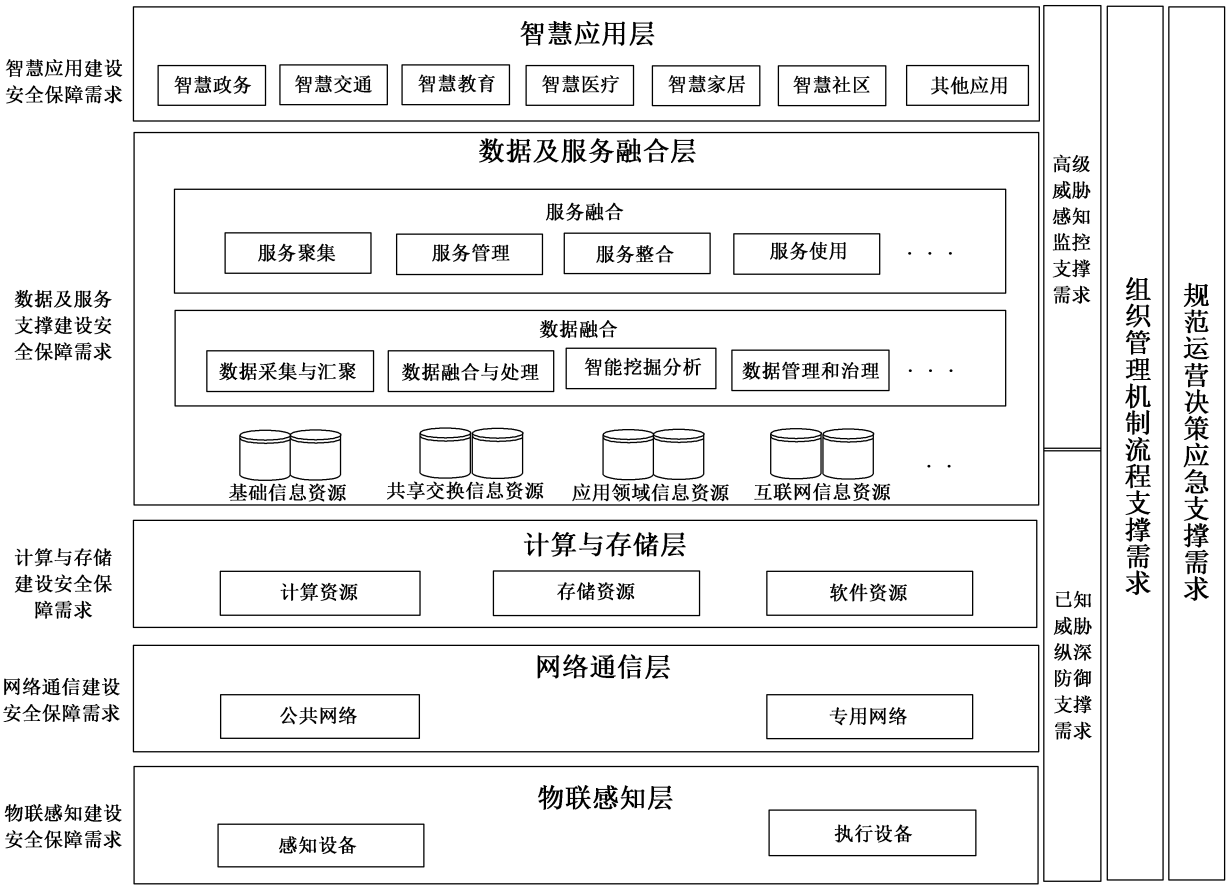

图 1　智慧城市建设信息安全需求示意图

5.2　智慧城市建设安全保障过程

智慧城市建设安全保障过程如图 2 所示，包括智慧城市建设信息安全政策制定与审查监督、智慧城市信息安全保障规划、需求分析与设计、智慧城市实施安全保障、智慧城市运维安全保障与持续优化等方面。

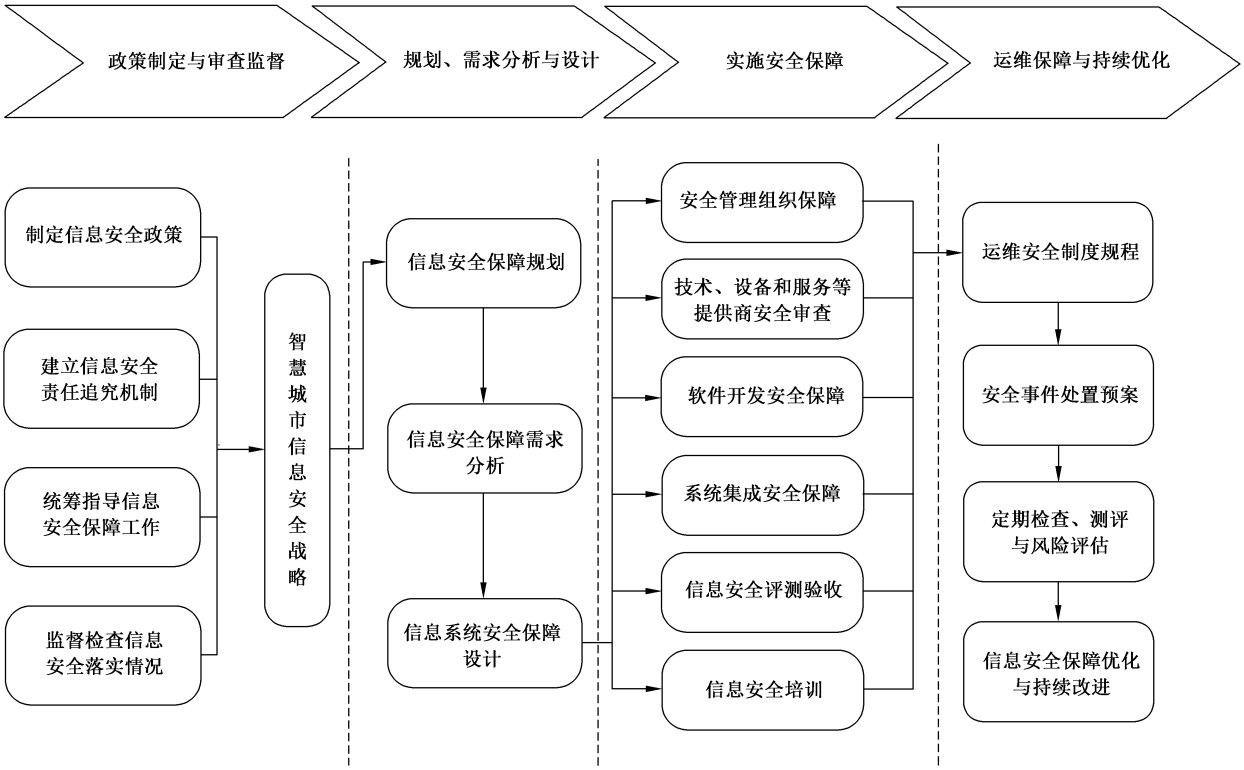

图 2　智慧城市建设安全保障过程示意图

5.3　智慧城市建设主要角色安全责任

本项需考虑的因素包括：

a）　智慧城市建设主管部门。作为智慧城市决策者和管理协调者，负责智慧城市建设和发展的规划和监管，协调、指导智慧城市建设信息安全保障工作。

b）　智慧城市规划设计咨询机构。智慧城市安全体系中承担智慧城市前期规划设计与跟踪咨询服务。

c）　智慧城市建设者。在主管部门的授权指导下，负责智慧城市建设，保证智慧城市建设过程符合安全保障要求。

d）　智慧城市服务提供者。通过利用各种技术提供智慧城市产品和服务，保证智慧城市产品和服务符合安全保障要求。

e）　智慧城市运营者。在主管部门的指导监管下，负责智慧城市运营，保障智慧城市安全，由信息安全专业人员承担智慧城市运营安全保障岗位。

f）　第三方安全评估机构。对智慧城市建设安全开展独立的评估，智慧城市风险评估方法和流程可参照附录 B。

g）　智慧城市服务使用者。依据国家法律法规、政策文件及标准规范，合理使用或应用智慧城市产品和服务并自觉接受安全培训，以及向智慧城市运营者反馈合理的需求诉求。

6　智慧城市建设安全保障机制

6.1　责任人机制

本项需考虑的因素包括：

a) 智慧城市项目建设单位指定项目信息安全保障第一责任人。
b) 智慧城市建设项目及时向主管部门备案。
c) 智慧城市建设项目贯彻执行相关法规和技术标准，落实主管部门的要求，编制信息安全保障等相关内容并履行。

6.2 追溯查证机制

本项需考虑的因素包括：

a) 建立智慧城市安全取证机制，建立全流程有效的责任追溯查证体系，明确各环节的主体责任，制定信息系统安全保障岗位责任制度，并监督落实。
b) 智慧城市各系统详细记录用户的活动信息，包括时间、地点、操作和操作结果，以建立取证的数据基础。
c) 建立智慧城市调查与取证体系，实现符合法律的取证过程，以对存在的违法入侵进行快速而有效的调查和取证。
d) 保证证据数据在调查和取证过程数据不被改变和删除，具体措施可以参考 ISO/IEC 27037：2012 和 ISO/IEC 27042。

6.3 监督检查机制

本项需考虑的因素包括：

a) 智慧城市建设的信息安全保障监督管理由信息安全监管部门通过备案、检查、督促整改等方式，对建设项目的信息安全保护工作进行指导监督。
b) 主管部门会同信息安全管理部门，定期对建设项目进行全面的安全检查，排查安全隐患，堵塞安全漏洞，通报发现问题并敦促整改。
c) 智慧城市建设者和运营者对抽查、抽检发现的问题，认真落实整改意见，并在规定期限向主管部门报告整改情况。

6.4 应急预案演练与处理机制

本项需考虑的因素包括：

a) 参照 GB/Z 20986—2007，根据智慧城市网络空间安全事件分类及信息系统损失划分，确定智慧城市网络空间安全事件应急响应分级，参见附录 C。
b) 结合智慧城市网络空间与物理空间联动配合情况，开展监测与预警、应急处置、调查与评估以及预防工作。监测与预警包括预警监测、预警研判和发布、预警响应、预警解除；应急处置包括事件报告、应急响应、应急结束；预防工作包括日常管理、制定应急预案、定期组织演练、检验和完善预案、宣传培训以及重要活动期间的预防措施。
c) 随着信息系统的变更定期对原有的应急预案重新评估，修订完善。
d) 安全故障发生时，按应急处理程序处置，及时向主管部门报告项目信息系统发生的重大系统事故或突发事件，并按有关预案快速响应。

6.5 服务外包安全责任机制

本项需考虑的因素包括：

a) 智慧城市服务者的选择符合国家的有关规定；与选定的服务者签订与安全相关的协议，明确约定相关责任。
b) 严格管理信息技术服务外包的安全，确保提供服务的数据中心、云计算服务平台等设在境内。

6.6 信息安全保障教育培训机制

本项需考虑的因素包括：

a) 制定安全教育和培训计划，对各类人员进行信息安全意识教育和相关信息安全技术培训。

b) 建立信息系统安全保障的专业队伍，适应信息智慧技术的发展。

7 智慧城市建设全过程安全保障管理

7.1 政策制定与审查监督

本项需考虑的因素包括：

a) 智慧城市建设主管部门提出信息安全保障的基本管理政策和工作要求；信息安全保障以GB/T 22081—2016为基础，根据智慧城市特征加强对关键信息基础设施、重点行业、公共安全、公用事业等重要信息系统安全防护，施行重要系统与网络安全设施同步设计、同步建设、同步管理的信息安全政策要求。

b) 明确智慧城市建设相关单位负责人、要害信息系统运营单位负责人的网络信息安全责任，建立信息安全责任追究机制；建立自主审查和主管部门审查结合的审查机制，在立项、验收等重要环节进行信息安全专项审查。

c) 智慧城市建设主管部门负责统筹协调、指导智慧城市建设信息安全保障工作；并对各智慧城市建设者、运营者、服务提供者和使用者所开展的信息安全保障实施情况进行监督检查。

7.2 信息安全保障规划

本项需考虑的因素包括：

a) 进行智慧城市建设信息安全保障整体规划，遵循国家和行业现有的适合于智慧城市信息安全保障的法律、法规、政策、标准规范，针对智慧城市建设存在的信息安全威胁与隐患，明确信息安全保障的目标和重点关注领域，建立与智慧城市建设战略目标相一致的信息安全保障总体方针。

b) 规划智慧城市容灾备份体系，推行联合灾备和异地灾备。

c) 规划智慧城市建设信息安全保障风险评估、过程反馈、优化改进的闭环管理体系；规划建立重要信息使用管理和安全评价机制，落实企业商业信息和个人信息保护。

7.3 信息安全保障需求分析

本项需考虑的因素包括：

a) 根据智慧城市建设信息安全保障目标，分析系统运行环境、潜在威胁、资产重要性、脆弱性等，提出安全保障需求，以实现防御攻击、重要信息授权获取、敏感信息加密、系统信息防篡改、行为审计以及系统高可用性等安全保障目标。

b) 通过安全影响范围和受损害影响程度分析，拟定所建智慧城市信息系统安全保护等级，经过主管部门组织论证，并报相关行政主管部门审核、备案。

c) 根据信息系统的安全保护等级，分析智慧城市信息系统现有的安全保护水平与等级保护基本要求之间的差距，提出系统的信息安全保障需求。

7.4 信息系统安全保障设计

本项需考虑的因素包括：

a) 在智慧城市建设信息系统设计阶段，加强安全风险论证，根据安全保护等级同步设计安全保障

防护方案，提高网络管理、态势预警、应急处理和可信服务等能力。

b) 根据信息系统安全保障设计方案的安全总体架构、保障策略、措施要求，落实信息安全产品、系统具体技术规范，为信息安全产品、系统采购和安全保障开发阶段提供明确依据。

c) 根据智慧城市建设安全保障管理目标，设计信息安全保障管理体系，保证安全技术与管理同步建设。

d) 汇总技术措施落实方案、管理措施落实方案等，形成指导安全实施的指导性文件。信息安全建设内容编制可参考附录D。

7.5 信息系统实施安全保障

7.5.1 建立配套的安全管理职能部门，通过管理机构的岗位设置、分工以及资源配备，为智慧城市建设信息安全管理提供组织上的保障。

7.5.2 以制度和规范形式，加强对技术、设备和服务提供商的安全审查，同步建设安全防护手段：

a) 指定或授权专门的部门负责产品的采购；对安全相关产品实行分级管理，确保其安全功能符合相应安全等级的要求；密码产品采购和使用符合国家密码主管部门的要求。

b) 对已有技术信息安全产品，应依据相关标准规范要求，进行安全符合性查验。

c) 对新技术相关产品进行安全测评，使其符合系统基本要求保障需求。

7.5.3 软件开发需考虑的因素：

a) 制定软件开发管理制度，明确开发过程的控制方法和人员行为准则。

b) 提供软件开发的相关文档和使用指南，并由专人负责保管。

c) 自行软件开发环境与实际运行环境物理分开；外包软件开发单位需提供软件源代码，并在软件安装之前代码性检测、性能压力测等。

7.5.4 系统集成安全保障需考虑的因素：

a) 信息系统试运行前，对信息系统开发过程中所提交的有关文档资料进行评估，审阅信息系统的安全控制、权限设置，确保其正确性、完整性、可审计性等内容，指出其中存在的风险，了解是否具有相应的控制措施，并提出评价和建议的过程。

b) 明确系统上线前进行测试，从而确定系统是否满足项目建设、实施规范的要求。

c) 信息系统试运行过程中随时关注信息系统运行效果，记录发现的问题，并形成文档文件。

7.5.5 信息系统安全评测验收需考虑的因素：

a) 验收前委托具备资质的第三方测试单位对系统进行代码安全性检测，渗透测试和风险评估，并出具安全测评报告。

b) 组织相关部门和相关人员对系统安全测评报告进行审定，并签字确认。

c) 制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。

d) 对系统控制方法和人员行为准则进行书面规定。

e) 对系统实现的风险控制措施进行评估判断，针对存在的不可接受风险项，需要制定风险处理计划并采取新的安全措施降低、控制风险。

7.5.6 对人员的职责、素质、技能等方面进行培训，保证人员具有与其岗位职责相适应的技术能力和管理能力，以减少人为因素给系统带来的安全风险。

7.6 信息系统运行维护安全保障

7.6.1 建立信息系统运行维护保障行为规范和操作规程，需考虑的因素包括：

a) 机房安全管理制度，对有关机房物理访问、物品带进或带出机房和环境安全等方面的管理要求。

b) 资产安全管理制度，规定信息系统资产管理的责任人员或部门，并规范资产管理和使用行为。

c) 介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面的管理要求。
d) 建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。
e) 网络安全管理制度，对网络安全配置、日志审计、安全策略、升级与补丁、日常管理等方面的管理要求。
f) 系统安全管理制度，对系统安全策略、安全配置、日志审计和日常操作流程等方面的管理要求。
g) 个人桌面终端安全管理制度，对个人桌面终端操作系统、周边硬件、通信设备、应用系统等的安全使用管理要求。

7.6.2 定期检查安全管理制度的落实情况，确保安全管理制度落实，并不断优化管理制度。

7.6.3 制定安全事件处置预案，结合信息系统的实际情况，分析安全事件对信息系统的破坏程度，所造成后果的严重程度，将安全事件依次进行分级，按照分级情况进行处置。

7.6.4 定期开展检查、等级评测和风险评估，排查安全风险隐患，增强日常监测和应急响应处置恢复能力；定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，向相关主管部门备案，并采取必要的应对措施。

7.6.5 建立重要信息使用管理和安全评价机制，落实个人信息保护。

7.7 信息安全保障优化与持续改进

本项需考虑的因素包括：

a) 定期对系统进行安全测评，对发现的安全问题进行及时分类处置。
b) 系统变更后评估变更后的部分对系统造成的安全影响。
c) 在信息系统正常运行一段时间后进行评估，旨在评估对信息系统各项风险的控制是否恰当，能否实现预定的设计目标。

8 智慧城市建设信息安全保障技术

8.1 计算环境安全保障技术

本项需考虑的因素包括：

a) 智慧城市安全计算环境遵循 GB/T 25070—2019 中的安全计算环境设计技术要求，对智慧城市建设涉及的通用安全、云安全、移动互联安全、物联网系统安全等实现保障。
b) 支持用户标识和用户鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度并定期更换；采用口令、密码技术、生物技术等两种或两种以上的组合机制进行用户身份鉴别；支持建立云租户账号体系，实现主体对虚拟机、云数据库、云网络、云存储等客体的访问授权；采用密码技术支持的鉴别机制实现感知层网关和感知设备之间的双向身份鉴别；对感知设备和感知层网关进行统一入网标识管理和维护，并确保在整个生存周期设备标识的唯一性。
c) 由授权主体配置访问控制策略，规定主体对客体的访问规则；访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和(或)记录或字段级；对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问；根据安全策略，控制移动终端接入访问外设，并记录日志；通过制定安全策略，实现对感知设备的访问控制；感知设备和其他设备通信时，根据安全策略对其他设备进行权限检查。
d) 启用安全审计功能，审计覆盖到每个用户；审计记录包括安全事件的主体、客体、时间、类型和结果等内容；对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；对审计进程进行保护，防止未经授权的中断；支持对云服务商和云租户远程管理时执行的特权命令进行审计；支持租户对与本租户相关资源的审计。

e) 可基于可信根对计算设备(包括移动终端)的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证,并在应用程序的关键执行环节进行动态可信验证,在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心。

f) 采用密码等技术支持的完整性校验机制,检验存储和处理的用户数据的完整性,在其受到破坏时能对重要数据进行恢复。

g) 采用密码等技术支持的保密性保护机制,对在安全计算环境中存储和处理的用户数据进行保密性保护;提供云计算环境加密服务,加密密钥由租户自行管理,保证虚拟机在迁移过程中重要数据的保密性。

h) 通过主动免疫可信计算检验机制及时识别入侵和病毒行为,并将其有效阻断;能检测到虚拟机对宿主主机物理资源的异常访问;支持对云租户进行行为监控,对云租户发起的恶意攻击或恶意对外连接进行检测和警告。

i) 提供重要数据的本地数据备份与恢复功能;根据安全保护等级提供异地备份功能以及重要数据处理系统的热冗余高可用性;云计算环境采取冗余架构或分布式架构设计,支持数据多副本存储方式;支持通用接口确保云租户业务系统及数据可移植性。

8.2 区域边界安全保障技术

本项需考虑的因素包括:

a) 遵循 GB/T 25070—2019 中的安全区域边界技术要求,对智慧城市建设涉及的通用安全、云安全、移动互联安全、物联网系统安全等实现保障。

b) 保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信;实现不同租户间虚拟网络资源之间的隔离,并避免网络资源过量占用;提供开发接口或开放性安全服务,允许云租户接入第三方安全产品或在云平台选择第三方安全服务。

c) 在安全区域边界设置自主和强制访问控制机制,对进出安全区域边界的数据信息进行控制,阻止非授权访问;建立租户私有网络实现不同租户之间的安全隔离;允许云租户设置不同虚拟机之间的访问控制策略;保证当虚拟机迁移时,访问控制策略随其迁移;对接入系统的移动终端,采取基于 SIM 卡、证书等信息的强认证措施;能根据数据的时间戳为数据流提供明确的允许/拒绝访问的能力;能根据通信协议特性,控制不规范数据包的出入。

d) 在安全区域边界设置审计机制;根据云服务商和云租户的职责划分,实现各自控制部分的审计;为安全审计数据的汇集提供接口,并可供第三方审计。

e) 在区域边界设置探测器,探测非法外联和入侵行为,并及时报告安全管理中心;移动终端区域边界检测设备监控范围完整覆盖移动终端办公区,并具备无线路由器设备位置检测功能,对于非法无线路由器设备接入进行报警和阻断。

f) 在安全区域边界设置准入控制机制,能够对设备进行认证,保证合法设备接入,拒绝恶意设备接入;能够对接入的感知设备进行健康性检查。

8.3 通信网络安全保障技术

本项需考虑的因素包括:

a) 遵循 GB/T 25070—2019 中的安全通信网络技术要求,对智慧城市建设涉及的通用安全、云安全、移动互联安全、物联网系统安全等实现保障。

b) 在安全通信网络设置审计机制,由安全管理中心集中管理;保证云服务商对云租户通信网络的访问操作可被租户审计。

c) 采用由密码技术支持的保密性保护机制,以实现通信网络数据传输保密性保护;支持云租户远程通信数据保密性保护。

d) 通信节点采用具有网络可信连接保护功能的系统软件或可信根支撑的信息技术产品，在设备连接网络时，对源和目标平台身份、执行程序及其关键执行环节的执行资源进行可信验证；实现基于密码算法的可信网络连接机制，确保接入通信网络的设备真实可信，防止设备的非法接入。

e) 采用接入认证等技术建立异构网络的接入认证系统，保障控制信息的安全传输；根据各接入网的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并采取相应的防护措施。

8.4 应用安全保障技术

本项需考虑的因素包括：

a) 应用安全覆盖身份鉴别、访问控制、安全控制、通信完整性、通信保密性、抗抵赖、软件容错、资源控制等部分的内容。

b) 制定安全开发管理规范，以保证应用系统开发过程得到相应的控制，从而保障系统从开发到生产运行的全过程的安全管控，需要注意代码安全开发，防范不安全的代码给系统带来的安全风险；加强内存管理，防止驻留在内存中的剩余信息被他人非授权获取。

c) 应用系统建立统一的账号、认证、授权和审计系统，实施严格的身份管理、安全认证与访问权限控制，提供用户访问记录，访问可溯。

d) 应用程序进行可信执行保护，构建从操作系统到上层应用的信任链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复。

e) 应用系统上线前，对其进行全面的安全评估，并进行安全加固；遵循安全最小化原则，关闭未使用的服务组件和端口；采用专业安全工具对应用系统进行定期评估；在补丁更新前，对补丁与现有系统的兼容性进行测试。

f) 应用系统访问控制支持结合安全管理策略，对账号口令、登录策略进行控制，支持设置用户登录方式及对系统文件的访问权限；对远程访问控制进行限制，限制匿名用户的访问权限，支持设置单一用户并发连接次数、连接超时限制等，采用最小授权原则，分别授予不同用户各自所需的最小权限。

8.5 大数据安全保障技术

本项需考虑的因素包括：

a) 保证承载智慧城市大数据存储、处理和分析的设备机房位于中国境内。

b) 保证智慧城市大数据平台不承载高于其安全保护等级的大数据应用；提供信息分类分级安全管理功能，供大数据应用针对不同类别级别的数据采取不同的安全保护措施；信息分类分级参见附录 E。

c) 大数据平台对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别；并能对不同客户的大数据应用实施标识和鉴别。

d) 大数据平台为大数据应用提供管控其计算和存储资源使用状况的能力；能屏蔽计算、内存、存储资源故障，保障业务正常运行。

e) 大数据平台提供静态脱敏和去标识化的工具或服务组件技术；对其提供辅助工具或服务组件实施有效管理。

f) 对外提供的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理。

g) 对数据二次应用严格安全管理，对数据转移导出进行严格控制；针对外部系统有固定的数据需

求时，建立具有严格安全审批控制互动接口；大数据对外服务时，要将整个服务过程中涉及的数据生产、加工、消费链路部署在提供方可监控的环境中，并对外部合作方的数据使用进行监控审计；根据具体的保护策略对合作方所访问数据的行为进行数字水印保护，以便对信息泄露的行为进行追踪；对外服务过程中，针对外部合作方制定严格的安全控制、安全管理和安全审计的管理制度。

h) 建立数字资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、存储、处理、应用、流动、销毁等过程；具备一种可用技术，能保证全面和有效地定位云计算数据、擦除/销毁数据，并保证数据已被完全消除或使其无法恢复。

8.6 产品与系统安全接口

本项需考虑的因素包括：

a) 智慧城市产品选型满足统一安全管理和安全运维的接口要求。

b) 满足统一用户管理接口要求，为每个用户分配唯一标识符，并统一管理，通过用户管理接口实现各产品/系统的用户同步。

c) 满足统一认证和授权接口要求，智慧城市全系统实现基于 CA 的统一认证和授权机制，各系统通过统一认证和授权接口实现对用户的认证和操作授权。

d) 满足统一安全监控接口要求，智慧城市安全运维系统通过安全监控接口获取各系统的安全状态，进而分析智慧城市整体安全态势。

e) 对高安全等级数据提供安全访问接口，如果产品涉及高安全等级的数据的访问，各产品需提供加密访问接口。

f) 满足统一安全策略配置接口要求，智慧城市需要实现全系统统一安全策略管理，各产品需提供安全策略配置接口，以实现对各产品安全策略的统一配置和管理。

8.7 安全管理中心技术要求

本项需考虑的因素包括：

a) 可通过系统管理员对系统资源和运行进行配置、控制和可信及密码管理；对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

b) 云计算平台安全管理提供查询云租户数据及备份存储位置的方式；物联网系统通过系统管理员对感知设备、感知网关等进行统一身份标识管理。

c) 通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置可信验证策略，维护策略库和度量值库；对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并进行审计。

d) 云计算安全管理具有对攻击行为回溯分析以及对网络安全事件进行预测和预警的能力；具有对网络安全态势进行感知、预测和预判的能力；物联网系统通过安全管理员对系统中所使用的密钥进行统一管理。

e) 通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等；对审计记录进行分析，并根据分析结果进行处理；对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。

f) 云计算平台对云服务器、云数据库、云存储等云服务的创建、删除等操作行为进行审计；通过运维审计系统对管理员的运维行为进行安全审计；通过租户隔离机制，确保审计数据隔离的有效性。

附 录 A
（资料性附录）
智慧城市整体框架与主要特征

A.1 智慧城市整体架构

智慧城市技术参考模型如图 A.1 所示。

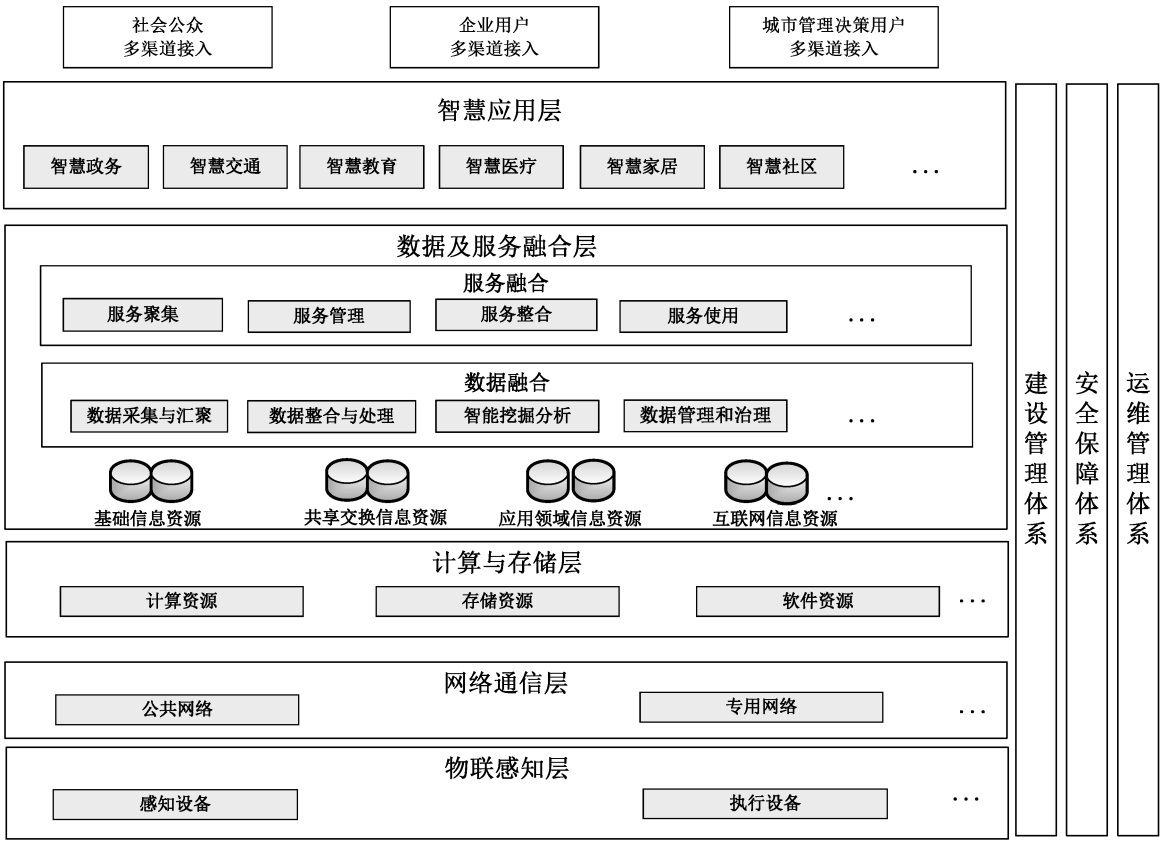

图 A.1 智慧城市技术参考模型

智慧城市技术参考模型包括五个横向层面和三个纵向体系：

a) 物联感知层：提供对环境的智能感知能力和执行能力，通过感知设备、执行设备及传输网络实现对城市范围内基础设施、环境、设备和人员等要素的识别、信息采集、监测和控制；

b) 网络通信层：为智慧城市提供大容量、高带宽、高可靠的光网络和全城覆盖的无线宽带接入网络所组成的网络通信基础设施，包括以互联网、电信网、广播电视网等为主体的核心传输网，提供无线接入服务的蜂窝无线网络，以及集群专网等一些专用的网络等；

c) 计算与存储层：包括软件资源、计算资源和存储资源，为智慧城市提供数据存储和计算以及相关软件环境的资源，保障上层对于数据的相关需求；

d) 数据及服务融合层：通过数据和服务的融合支撑，承载智慧应用层中的相关应用，提供应用所

需的各种服务，为构建上层各类智慧应用提供支撑，本层处于智慧城市总体参考模型的中上层，具有重要的承上启下的作用；

e) 智慧应用层：在物联感知层、网络通信层、计算与存储层、数据及服务融合层之上建立的各种基于行业或领域的智慧应用及应用整合，如智慧政务、智慧交通、智慧公共服务、智慧医疗、智慧园区、智慧社区、智慧旅游等，为社会公众、企业用户、城市管理决策用户等提供整体的信息化应用和服务；

f) 安全保障体系：为智慧城市构建统一的安全平台，实现统一入口、统一认证、统一授权、日志记录，涉及各横向层次；

g) 运维管理体系：为智慧城市提供整体的运维管理机制，涉及各横向层次，确保智慧城市整体的建设管理和长效运行；

h) 建设管理体系：为智慧城市建设提供整体的建设管理要求，加强智慧城市建设管理机制，指导智慧城市相关建设，确保智慧城市建设的科学性和合理性。

A.2 智慧城市的主要特征

智慧城市是运用信息通信技术，有效整合各类城市管理系统，实现城市各系统间信息资源共享和业务协同，推动城市管理和服务智慧化，提升城市运行管理和公共服务水平，提高城市居民幸福感和满意度，实现可持续发展的一种创新型城市。

注：参见 GB/T 37043—2018。

智慧城市的基础是推进实体基础设施和信息基础设施相融合、构建城市智能基础设施；主线是推进物联网、云计算、大数据、移动互联网、空间地理信息集成等新一代信息技术应用与城市经济社会发展的深度融合；其核心是最大限度地开发、整合、融合、共享和利用各类城市信息资源，构建城市规划、建设、管理和服务的智慧化体系；主要手段包括为居民、企业和社会提供及时、高效、智能的信息服务等；其宗旨是实现城市规划管理信息化、基础设施智能化、公共服务便捷化、产业发展现代化、社会治理精细化。

智慧城市具有以下主要特征：

a) 系统工程。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。

注：参见 GB/T 36621—2018。

b) 资源集中与大数据融合。云计算 IT 资源的集中化促进资源共用、提高资源伸缩性。按照城市经济社会发展需求，实现相关部门、行业、群体、系统之间的数据融合、信息共享，形成海量数据。社会信息高度集中也将带来巨大的潜在风险。

c) 泛在接入与全面感知。智慧城市通过感知技术，对人、物的相关信息进行全面的感知与互联，形成城市智慧的泛在信息源。机构和个人通过标准接入机制，利用手持设备、传感器、移动电话、平板、机顶盒等各种终端、物联网互联感知设备通过网络随时随地使用智慧城市服务。

d) 协同运作与多安全域。城市中的各个主体之间利用智慧技术实现互连互通，彼此之间实现实时感知，及时传递信息，迅速做出反应。除少数涉及秘密信息的领域之外，大多数信息系统都将是一种开放的协同系统。智慧城市要解决跨部门、跨区域、跨系统的问题，构建跨越不同安全域之间的智能化管理与服务系统。因此，解决不同安全域之间的互联是重点。

e) 移动化和开放性。随着泛在网络和手持终端的普及应用，移动化成为智慧城市的重要特征。智慧城市中广泛应用无线技术，如物联网感知层的电子标签，由于受成本等的限制，未采用很强的密码机制，电子标签内部数据容易被破解。同时，众多机构通过 VPN 等方式将机构网络建构在公共网络之上。开放性导致安全风险增加。

f) 高渗透与个人隐私。物联网、无线宽带网等网络规模大大增加，人们使用网络的时间和位置限制被突破；新的智慧应用让普通民众主动地参与信息创造和发布以及网络运转的其他环节，因此，智慧城市对人类社会的渗透水平大大提升。同时，智慧城市建设以人为本，涉及隐私数据，包括个人基本信息、个人偏好、个人位置及个人行为数据等。高渗透造成个人隐私保护风险剧增。

附 录 B
（资料性附录）
智慧城市风险评估方法和流程

B.1 实施计划

信息化主管部门制定检查评估年度实施计划。

B.2 评估机构

信息化主管部门委托符合条件的风险评估服务机构，对重要信息系统实施检查评估。

B.3 系统规划风险评估

对总体规划、设计方案等相关配套文件的合理性和正确性以及安全控制措施的有效性进行评估；评估结果体现于信息系统整体规划或项目建议书。

B.4 总体风险评估

对本机构所有信息系统共有的公共部分进行评估，实施总体风险控制；根据信息系统的总体风险状况确定评估频率。

B.5 系统风险评估

对研发、运行及废弃的全过程进行风险评估，分别包括试运行与运行后的风险评估。

B.6 试运行系统评估

对信息项目开发过程中所提交的有关文档资料进行评估，指出其中存在的风险，了解是否具有相应的控制措施，并提出评价和建议的过程。信息系统运行前的系统审阅需关注信息系统的安全控制、权限设置、正确性、连贯性、完整性、可审计性和及时性等内容。

B.7 运行后系统评估

在信息系统正常运行一段时间后进行的评估，旨在评估对信息系统各项风险的控制是否恰当，能否实现预定的设计目标。运行后的系统评估一般在信息系统正常运行半年后进行，评估报告对被评估的信息系统提出改进或增加风险控制、能否继续运行等内容的评估建议。

B.8 专项风险评估

对被评估系统发生信息安全事故进行的调查、分析和评估，或原有信息系统进行重大结构调整的评估，或信息化主管部门认为需要对信息系统某项专题进行评估。

附 录 C
（资料性附录）
智慧城市网络空间安全事件分类分级

C.1 智慧城市网络空间安全事件分类

智慧城市网络空间安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。具体分类如下：

a) 有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

b) 网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

c) 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

d) 信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

e) 设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

f) 灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

g) 其他事件是指不能归为以上分类的网络安全事件。

C.2 智慧城市网络空间安全事件应急响应分级

智慧城市网络空间安全事件应急响应分为四级，分别对应特别重大、重大、较大和一般网络安全事件。Ⅰ级为最高响应级别。具体包括：

a) Ⅰ级响应

属特别重大网络安全事件的，及时启动Ⅰ级响应，成立指挥部，履行应急处置工作的统一领导、指挥、协调职责。

城市应急指挥机构进入应急状态，在指挥部的统一领导、指挥、协调下，负责城市应急处置工作或支援保障工作，24 小时值班，并派员参加应急办工作。

跟踪事态发展，检查影响范围，及时将事态发展变化情况、处置进展情况报应急办。指挥部对应对工作进行决策部署，有关部门负责组织实施。

b) Ⅱ级响应

网络安全事件的Ⅱ级响应，由城市管理部门根据事件的性质和情况确定。具体分为：

1) 事件发生城市应急指挥机构进入应急状态，按照相关应急预案做好应急处置工作。

2) 事件发生部门及时将事态发展变化情况报应急办。应急办将有关重大事项及时通报上级部门。

3) 处置中需要其他有关地区、部门和国家网络安全应急技术支撑队伍配合和支持的，商应急办予以协调。

4) 有关部门根据应急办的通报，结合各自实际有针对性地加强防范，防止造成更大范围影响和损失。

c) Ⅲ级响应、Ⅳ级响应

事件发生地区和部门按相关预案进行应急响应。

C.3 智慧城市网络信息系统损失程度划分说明

智慧城市网络信息系统损失是指由于智慧城市网络空间安全事件对系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事发组织所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失，说明如下：

a) 特别严重的系统损失：造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的；

b) 严重的系统损失：造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的；

c) 较大的系统损失：造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的；

d) 较小的系统损失：造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

附 录 D
（资料性附录）
信息安全建设内容编制指南

D.1 项目建议书编制指南

在“必要性”“需求分析”“建设方案”等篇章专设一节描述“信息安全”相关内容。具体内容如下：

a） 项目建设的必要性

增加“信息安全保障现状与差距”：阐述目前信息安全软硬件装备和应用情况，梳理信息安全有关规定和要求，分析存在的主要问题和差距。

b） 需求分析

增加“信息安全风险与需求分析”：识别影响网络与信息安全的主要因素，分析可能面临的信息安全主要风险。

c） 本期项目建设方案

专设“网络与信息安全保障体系建设”一节：描述保障本项目基础网络安全、重要系统安全和信息内容安全的软硬件配置方案、标准规范建设框架以及信息安全检测与审查措施。

D.2 项目可行性研究报告/建设方案编制指南

在“必要性”“需求分析”“建设方案”等篇章专设一节描述“信息安全”相关内容。具体内容如下：

a） 项目建设的必要性

增加“信息安全保障现状与差距”：阐述目前信息安全软硬件装备和应用情况，梳理信息安全有关规定和要求，分析存在的主要问题和差距。

b） 需求分析

增加“信息安全风险与需求分析”：识别影响网络与信息安全的因素，分析可能面临的信息安全风险及危害程度。

从业务需求出发，进行信息安全风险评估。对信息资产的重要性、威胁发生的频率、系统自身脆弱性进行识别和关联分析，判断信息系统面临的风险及应采取什么强度的安全措施将风险可能造成的影响控制在可接受的范围内，分析信息及信息系统对国家安全、经济建设和社会生活的重要程度及遭到破坏后对其的危害程度。

c） 本期项目建设方案

专设“网络与信息安全保障体系建设”一节，按照信息安全等级保护要求，确定等级，阐述保障本项目基础网络安全、重要系统安全和信息内容安全的软硬件配置方案、标准规范建设内容、信息安全检测计划、项目建设与运行维护过程的信息安全审查与控制措施。

附 录 E
（资料性附录）
信息分类分级管理

E.1 政府信息分类

E.1.1 概述

本指导性技术文件中的政府信息是指政府机关，包括受政府委托代行政府机关职能的机构，在履行职责过程中，以及政府合同单位在完成政府委托任务过程中产生、获取的，通过计算机等电子装置处理、保存、传输的数据，以及相关的程序、文档等。

涉密信息的处理、保存、传输、利用按国家保密法规执行。

本指导性技术文件将非涉密信息分为敏感信息、公开信息两种类型。

E.1.2 敏感信息

E.1.2.1 敏感信息的概念

敏感信息指不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及企业和公众利益密切相关的信息，这些信息一旦未经授权披露、丢失、滥用、篡改或销毁可能造成以下后果：

a） 损害国防、国际关系；
b） 损害国家财产和公共利益，以及个人财产或人身安全；
c） 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；
d） 影响行政机关依法调查处理违法、渎职行为，或涉嫌违法、渎职行为；
e） 干扰政府部门依法公正地开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；
f） 危害国家关键基础设施、政府信息系统安全；
g） 影响市场秩序，造成不公平竞争，破坏市场规律；
h） 可推论出国家秘密事项；
i） 侵犯个人隐私、企业商业秘密和知识产权；
j） 损害国家、企业、个人的其他利益和声誉。

注：参考 GB/T 31167—2014。

E.1.2.2 敏感信息的范围

敏感信息包括但不限于：

a） 公开但正式发布前不宜泄露的信息，如规划、统计、预算、招投标等的过程信息；
b） 执法过程中生成的不宜公开的记录文档；
c） 一定精度和范围的国家地理、资源等基础数据；
d） 个人信息，或通过分析、统计等方法可以获得个人隐私的相关信息；
e） 企业的商业秘密和知识产权中不宜公开的信息；
f） 关键基础设施、政府信息系统安全防护计划、策略、实施等相关信息；
g） 行政机构内部的人事规章和工作制度；
h） 政府部门内部的人员晋升、奖励、处分、能力评价等人事管理信息；
i） 根据国际条约、协议不宜公开的信息；

j） 法律法规确定的不宜公开信息；
k） 单位根据国家要求或本单位要求认定的敏感信息。

E.1.3 公开信息

公开信息指不涉及国家秘密且不是敏感信息的智慧城市相关信息，包括但不限于：
a） 行政法规、规章和规范性文件，发展规划及相关政策；
b） 统计信息，财政预算决算报告，行政事业性收费的项目、依据、标准；
c） 政府集中采购项目的目录、标准及实施情况；
d） 行政许可的事项、依据、条件、数量、程序、期限以及申请行政许可需要提交的全部材料目录及办理流程；
e） 重大建设项目的批准和实施情况；
f） 扶贫、教育、医疗、社会保障、促进就业等方面的政策、措施及其实施情况；
g） 突发公共事件的应急预案、预警信息及应对情况；
h） 环境保护、公共卫生、安全生产、食品药品、产品质量的监督检查情况等；
i） 其他根据相关法律法规应该公开的信息。

E.2 政府业务分类

E.2.1 业务分类原则

确定了信息类型后，还需要对承载相关信息的业务进行分类。根据业务不能正常开展时可能造成的影响范围和程度，本指导性技术文件将政府业务划分为一般业务、重要业务、关键业务三种类型。

E.2.2 一般业务

一般业务出现短期服务中断或无响应不会影响政府部门的核心任务，对公众的日常工作与生活造成的影响范围、程度有限。

通常政府部门、社会公众对一般业务中断的容忍度以天为单位衡量。

E.2.3 重要业务

重要业务一旦受到干扰或停顿，会对政府决策和运转、对公众服务产生较大影响，在一定范围内影响公众的工作生活，造成财产损失，引发少数人对政府的不满情绪。此类业务出现问题，造成的影响范围、程度较大。

满足以下条件之一的业务可被认为是重要业务：
——政府部门对业务中断的容忍程度小于 24 h；
——业务系统的服务对象超过 10 万用户；
——信息发布网站的访问量超过每天 500 万人次；
——出现安全事件造成 100 万元以上经济损失；
——出现问题后可能造成其他较大危害。

E.2.4 关键业务

关键业务一旦受到干扰或停顿，将对政府决策和运转、对公服务产生严重影响，威胁国家安全和人民生命财产安全，严重影响政府声誉，在一定程度上动摇公众对政府的信心。

满足以下条件之一的业务可被认为是关键业务：
——政府部门对业务中断的容忍程度小于 1 h；

——业务系统的服务对象超过 100 万用户；
——出现安全事件造成 5 000 万元以上经济损失，或危害人身安全；
——出现问题后可能造成其他严重危害。

E.3 优先级确定

在分类信息和业务的基础上，综合平衡采用智慧城市建设运营后的效益和风险，确定优先部署到智慧城市云计算平台的数据和业务，如图 E.1 所示。

承载公开信息的一般业务可优先采用包括公有云在内的云平台，尤其是那些利用率较低、维护和升级成本较高、与其他系统关联度低的业务应优先考虑采用社会化的公有云平台。

承载敏感信息的一般业务和重要业务，以及承载公开信息的重要业务也可采用云平台，但宜采用安全特性较好的私有云或社区云。

关键业务系统暂不宜采用社会化的公有云平台，但可采用场内私有云（自有私有云）。

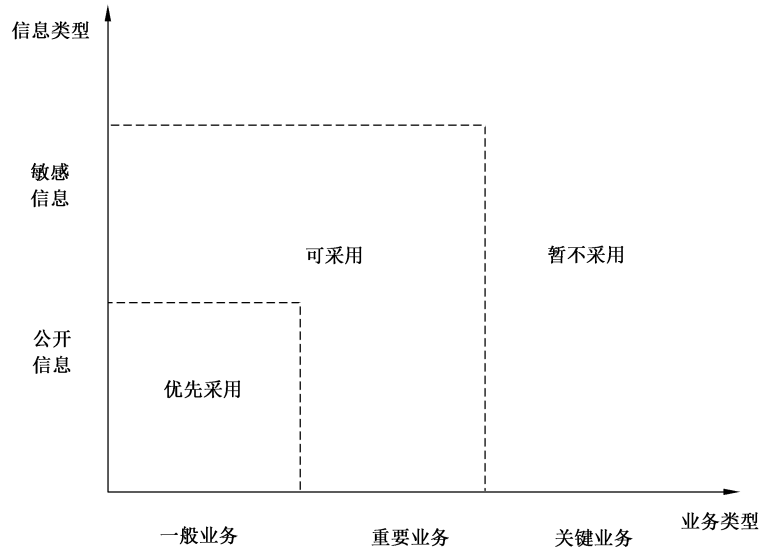

图 E.1 采用智慧城市建设的优先级

E.4 安全保护

客户信息需得到适当的保护。对于公开信息主要是防篡改、防丢失，对于敏感信息还要防止未经授权披露、丢失、滥用、篡改和销毁。

客户业务需得到适当保护，保证业务的安全性和持续性。

云服务商对不同类型的信息和业务需根据客户需求提供相应强度的安全保护，如图 E.2 所示。

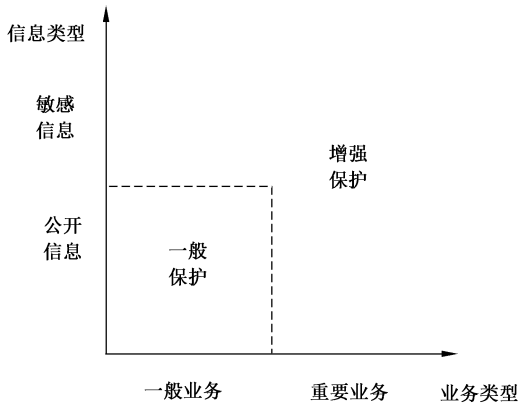

图 E.2　安全保护分类需求

对智慧城市建设的安全能力需求如下：

——承载公开信息的一般业务需要一般安全保护；

——承载敏感信息的一般业务和重要业务，以及承载公开信息的重要业务需要增强安全保护；

——关于一般安全保护和增强安全保护的具体指标要求，见相应的国家标准。

参 考 文 献

[1] GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南
[2] GB/T 28450—2012 信息安全技术 信息安全管理体系审核指南
[3] GB/T 29828—2013 信息安全技术 可信计算规范 可信连接架构
[4] GB/Z 29830(所有部分) 信息技术 安全技术 信息技术安全保障框架
[5] GB/T 30271—2013 信息安全技术 信息安全服务能力评估准则
[6] GB/T 31167—2014 信息安全技术 云计算服务安全指南
[7] GB/T 31495(所有部分) 信息安全技术 信息安全保障指标体系及评价方法
[8] GB/T 31496—2015 信息技术 安全技术 信息安全管理体系实施指南
[9] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南
[10] GB/T 31722—2015 信息技术 安全技术 信息安全风险管理
[11] GB/T 36621—2018 智慧城市 信息技术运营指南
[12] GB/T 37043—2018 智慧城市 术语
[13] ISO/IEC 27037 信息技术 安全技术 数字证据识别、收集、获取和保存指南(Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence)