ICS 35.040
CCS L 80

DB37

山 东 省 地 方 标 准

DB37/T 4550—2022

智慧城市网络安全建设和评估指南

Smart city cybersecurity construction and evaluation guidelines

2022－10－21 发布　　2022－11－21 实施

山东省市场监督管理局　　发布

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由中共山东省委网络安全和信息化委员会办公室提出、归口并组织实施

智慧城市网络安全建设和评估指南

1 范围

本文件提供了智慧城市网络安全建设和评估的指导。

本文件适用于山东省内市、县（区）的智慧城市网络安全建设与评估，数字政府、数字园区、数据中心的网络安全建设运行和评估参考使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 20984—2022 信息安全技术 信息安全风险评估方法

GB/Z 20986 信息安全技术 信息安全事件分类分级指南

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 31167 信息安全技术 云计算服务安全指南

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 32400—2015 信息技术 云计算 概览与词汇（ISO/IEC 17788:2014,IDT）

GB/T 36951—2018 信息安全技术 物联网感知终端应用安全技术要求

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

GA/T 1781—2021 公共安全社会视频资源安全联网设备技术要求

3 术语和缩略语

3.1 术语和定义

GB/T 32400—2015、GB/T 36951—2018界定的及下列术语和定义适用于本文件。

3.1.1

关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的网络设施和信息系统。

3.1.2

零信任架构 zero trust architecture

基于零信任理念，围绕其组件关系、工作流规划与访问策略构建而成的一种企业网络安全架构。

3.1.3

数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

[来源：GB/T 37988—2019，3.1]

3.1.4

感知终端 sensing terminal

能对物或环境进行信息采集和/或执行操作，并能联网进行通信的装置。

[来源：GB/T 36951—2018，3.1.2]

3.1.5

云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的模式模式。

[来源：GB/T 32400—2015，3.2.5]

3.1.6

云平台 cloud platform

云服务商提供的云计算（3.1.5）基础设施及其上的服务软件的集合。

3.1.7

安全审计 security audit

对事件进行记录和分析，并针对特定事件采取相应比较的动作。

[来源：GB/T 20945—2013，3.2]

3.1.8

安全策略 security policy

用于治理组织及其系统内在安全上如何管理、保护和分发资产（包括敏感信息）的一组规则、指导和实践，特别是那些对系统安全及相关元素具有影响的资产。

3.1.9

信息技术应用创新 information technology application innovation

通过行业应用构建国产化信息技术软硬件底层架构体系和全周期生态体系。

注：简称信创。

3.2 缩略语

下列缩略语适用于本文件。

AP：访问接入点（Access Point）

API：应用程序接口（Application Program Interface）

APP：移动互联网应用程序（Application）

CA：证书颁发机构（Certificate Authority）

DDoS：分布式拒绝服务攻击（Distributed Denial of Service）

IP：网络协议（Internet Protocol）

IT：互联网技术（Internet Technology）

MAC：媒体访问控制（Media Access Control）

VPN：虚拟专用网络（Virtual Private Network）

Web：网站（Website）

4 安全管理

4.1 安全管理机构

4.1.1 岗位设置

岗位设置主要包括：

a) 智慧城市网络安全工作责任见《党委（党组）网络安全工作责任制实施办法》；
b) 宜成立指导和管理智慧城市网络安全工作的委员会或领导小组，其最高领导由地方党政主要负责人或分管领导担任；
c) 宜设立智慧城市网络安全管理工作的职能部门，负责智慧城市网络安全日常管理工作，设立安全管理、关键信息基础设施安全、重要信息系统安全、关键数据资源安全等各个方面的负责人岗位，并明确各岗位职责。

4.1.2 人员配备

人员配备主要包括：

a) 配备一定数量的智慧城市信息系统管理员、信息安全管理员和信息系统安全审计员等；
b) 信息系统管理员、信息安全管理员和信息系统安全审计员等专职安全人员不可兼任。

4.1.3 授权和审批

授权和审批主要包括：

a) 根据不同岗位的职责明确授权审批事项、审批人等；
b) 针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
c) 定期审查审批事项，及时更新需授权和审批的项目、审批人等信息；
d) 记录审批过程并保存审批文档备查。

4.1.4 审核和检查

审核和检查主要包括：

a) 制定安全审核和安全检查制度，定期按照程序进行安全审核和安全检查活动；
b) 建立并实施智慧城市网络安全考核及监督问责机制，定期进行智慧城市网络安全检查及考核，检查内容包括智慧城市现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
a) 汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

4.2 安全规划

安全规划主要包括：

a) 宜对智慧城市的安全建设进行总体规划，制定智慧城市近期和远期的安全建设工作计划；
b) 智慧城市网络安全建设与各信息系统建设同步规划、同步设计、同步实施，基于零信任架构的智慧城市网络安全防护应用场景见附录 A；
c) 宜控制智慧城市网络安全建设投资在智慧城市信息化建设投资中所占的比例在 5 %以上；
d) 智慧城市中信息系统按 GB/T 22239—2019 和 GB/T 20984—2022 定期开展等级保护测评和信息安全风险评估，按 GB/T 39786—2021 定期开展商用密码应用安全性评估；
e) 制定智慧城市基本安全措施，并依据等级保护测评、信息安全风险评估和商用密码应用安全性评估的结果补充和调整安全措施；
f) 组织相关部门和安全专家对智慧城市安全建设总体规划的合理性和正确性进行论证和评审。

4.3 安全管理制度

4.3.1 安全策略

安全策略主要包括：

a) 构建智慧城市网络安全管理制度体系，包含智慧城市网络安全方针策略、安全管理制度和工作机制等；
b) 制定智慧城市网络安全战略方针和安全策略，阐明智慧城市网络安全战略目标、范围、原则和安全框架等，重点加强智慧城市关键信息基础设施、重要信息系统和关键数据资源的安全；
c) 组建智慧城市网络安全研究队伍和智库机构或委托相关智慧城市网络安全研究机构开展智慧城市网络安全战略、策略、规划、制度体系等研究制定工作。

4.3.2 管理制度

管理制度主要包括：

a) 针对智慧城市网络安全管理活动中各类管理内容建立智慧城市网络安全管理制度；
b) 制度正式发布并进行版本控制，并定期进行专家论证、评审和修订；
c) 结合智慧城市网络安全管理实践，主导或参与智慧城市网络安全国家、行业、地方、团体标准，推动智慧城市网络安全标准的宣贯培训；
d) 建立健全网络安全评价考核制度，并推动落实。

4.3.3 工作机制

工作机制主要包括：

a) 建立智慧城市网络安全通报机制，明确通报范围、通报流程等，各通报成员单位通过智慧城市安全监测、预警、通报和信息共享的安全监测中心通报智慧城市网络安全信息，通报成员单位覆盖智慧城市关键信息基础设施保护工作部门80%以上；
b) 建立智慧城市网络安全检查机制，明确检查流程、管理责任等；
c) 每年至少开展一次智慧城市网络安全检查、网络安全等级保护测评、密码应用安全性评估，对其中发现的问题及时整改，处理相关风险；
d) 建立失泄密监管机制，及时发现泄密隐患，上报处置；
e) 建立智慧城市网络安全应急处置机制，制定应急预案，定期开展应急演练，处置网络安全事件；
f) 建立智慧城市网络安全人才培养机制，定期发布智慧城市网络安全人才培养规划，并推动落实规划，定期了解各高校、企业智慧城市网络安全人才供给与需求，推动促进智慧城市网络安全人才的交流与合作。

4.3.4 运行记录

运行记录主要包括：

a) 制定智慧城市网络安全法律法规年度宣贯计划；
b) 按照智慧城市网络安全管理制度开展智慧城市网络安全工作，重点推动国家网络安全审查、网络安全认证等的实施，并形成完整的资料文档。

4.4 人员安全管理

4.4.1 人员管理

人员管理主要包括：

a) 对智慧城市安全管理机构相关录用人员身份、安全背景、专业资格等进行审查，并对其智慧城市网络安全技术技能进行考核；

b) 与被录用人员签署保密协议；
c) 及时终止离岗人员的所有访问权限；
d) 加强外部人员对物理访问受控区域的访问管理，在履行相关申请手续后由专人陪同访问，并登记备案；
e) 加强智慧城市信息系统外包开发等外部人员对受控网络的访问管理，在履行相关申请手续后由专人开设帐户、分配权限，并登记备案；
f) 外部人员离开物理访问受控区域或不需要对受控网络访问后，及时清除外部人员的访问权限。

4.4.2 安全意识教育和培训

安全意识教育和培训主要包括：
a) 建立智慧城市关键信息基础设施的安全从业人员网络安全教育、培训和考核制度，定期开展基于岗位的网络安全教育培训和技能考核，教育培训内容包括智慧城市网络安全相关制度、网络安全保护技术、商用密码应用、网络安全风险意识、重要信息系统和关键数据资源安全保护、关键基础设施安全保护等；
b) 智慧城市关键信息基础设施的安全从业人员宜持证上岗，并定期进行考核，考核不通过者不宜从事关键信息基础设施运营管理；
c) 宜明确安全责任和惩戒措施并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；
d) 对安全教育和培训的情况和结果进行记录并归档保存。

4.5 安全建设管理

4.5.1 产品采购

产品采购主要包括：
a) 指定或授权专门的部门负责智慧城市相关网络安全产品的采购，采购过程中所需密码产品与服务、互联网网络安全产品和服务、涉及国家秘密的产品与服务宜重点考虑行业要求；
b) 涉及国家安全的网络安全产品和服务在采购前宜进行网络安全审查。

4.5.2 软件开发

软件开发主要包括：
a) 制定智慧城市信息系统相关软件开发管理制度，明确开发过程的控制方法和人员行为准则；
b) 确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制；
c) 在软件交付前检测软件包中可能存在的恶意代码；
d) 智慧城市信息系统外包开发的，与开发单位签订相应的保密协议，同时审查软件中可能存在的后门。

4.5.3 测试验收

测试验收主要包括：
a) 委托有资质的第三方测评机构对智慧城市信息系统进行等级保护测评、商用密码应用安全性评估，并出具报告，网络安全检测与评估应用场景见附录 B；
b) 验收时提交智慧城市信息系统等级保护测评报告、信息安全风险评估报告和商用密码应用安全性评估报告，当智慧城市信息系统发生重大变化及面临重大风险时重新进行等级保护测评、风险评估和商用密码应用安全性评估，并对风险及时处置；

c) 在测试验收前根据设计方案或合同等制定测试验收方案，在测试验收过程中详细记录测试验收结果，并形成测试验收报告；
d) 指定或授权专门的部门负责系统测试验收的管理，并按照管理规定完成验收工作。

4.6 数据安全管理

4.6.1 数据分类分级

数据分类分级主要包括：

a) 对智慧城市相关数据进行分类分级（参考 GB/Z 38649—2020 中附录 E），不同类别级别数据采取不同的安全措施，不同级别的数据被同时处理、应用时，按照其中最高级别来实施保护；
b) 依据数据分类分级，建立数据备份策略，依据策略进行备份，并对备份进行测试以确保备份可用；
c) 承载智慧城市数据存储、处理、分析的设备所在机房或云平台位于中国境内；
d) 宜建立数据安全全生命周期安全管理制度。

4.6.2 数据安全风险评估

数据安全风险评估主要包括：

a) 建立数据安全风险评估与应急工作机制，制定数据安全事件应急预案；
b) 定期进行风险自评估，分析由于基础信息网络、重要信息系统及关键信息基础设施与管理因素变化而新出现的安全威胁，对自身进行数据安全风险识别和评价，动态调整安全策略，适时补充和完善技术与管理措施，降低数据资产的安全风险；
c) 汇总评估数据，形成并报送风险评估报告。

4.6.3 数据关联与溯源

数据关联与溯源主要包括：

a) 不同应用之间进行数据关联性保护，防止产生数据泄露，数据防泄漏安全应用场景见附录 C；
b) 在响应同一应用或同一用户的多个数据访问请求时，做好数据关联性防护，防止不同的数据访问请求关联分析产生敏感数据；
c) 通过数据溯源追踪、管理数据之间的衍生依赖关系，对敏感数据的衍生数据进行安全保护，对敏感数据应用周期的各个环节的操作进行标记和定位，在发生数据安全问题时，利用数据溯源技术进行数据追踪，及时准确地定位到出现问题的环节和责任者。

4.6.4 数据交换与共享

数据交换与共享主要包括：

a) 制定智慧城市数据交互、融合和共享安全策略，明确交互、融合和共享的范围、要求等，跨网数据交换安全场景见附录 D；
b) 采取相应的技术措施对智慧城市数据交互、融合和共享网络安全进行监督；
c) 数据交互、融合和共享根据需要仅提取必要数据，确保隐私安全。

4.6.5 数据审查

数据审查主要包括：

a) 建立数据审查制度，对影响或者可能影响数据安全的数据处理活动进行安全审查，并形成数据审查报告；
b) 定期对数据采集、传输、共享、融合等数据处理行为进行审查和分析，审查重要数据被窃取、泄露、损毁的风险，调查可疑行为及违规操作，采取响应的措施并及时报告。

4.7 移动应用安全管理

4.7.1 APP 安全管理

APP安全管理主要包括：
a) 采取措施确保智慧城市相关 APP 应用的自身安全；
b) 加强对 APP 接入智慧城市的身份鉴别、访问控制等。

4.7.2 APP 安全认证

APP 安全认证主要包括：
a) APP 运营方宜开展 APP 安全检测和安全认证工作，规范 APP 收集、使用用户信息的相关行为；
b) 宜安装在搜索引擎、应用商店等明确标识并通过认证的 APP。

4.8 关键信息基础设施安全管理

关键信息基础设施安全管理主要包括：
a) 开展智慧城市关键信息基础设施的识别认定，并当智慧城市关键信息基础设施发生较大变化，可能影响其认定结果的，及时报告相关部门；
b) 建立健全智慧城市关键信息基础设施网络安全保护制度和责任制，保障人力、财力、物力投入，智慧城市关键信息基础设施运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题；
c) 智慧城市关键信息基础设施安全保护措施与智慧城市关键信息基础设施同步规划、同步建设、同步使用；
d) 智慧城市关键信息基础设施按 GB/T 22239—2019、GB/T 39786—2021 进行定期的安全检查、等级保护测评和商用密码应用安全性评估；
e) 每年对智慧城市关键信息基础设施开展一次网络安全检查和网络安全风险评估；
f) 智慧城市关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，及时向相关部门报告；
g) 推动智慧城市关键信息基础设施相关的关键 IT 设备（主要是操作系统、数据库、服务器、重要网络设备等）国产化，提高智慧城市关键信息基础设施相关的关键 IT 设备国产化率；
h) 加强智慧城市关键信息基础设施重要数据出境安全监测、评估和管理；
i) 智慧城市关键信息基础设施优先采购安全可信的网络产品和服务，采购网络产品和服务可能影响国家安全的，进行网络安全审查。

4.9 运维管理

4.9.1 环境管理

环境管理主要包括：

a) 建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。
b) 指定专门的部门或人员定期对智慧城市的机房供配电、空调、温湿度控制等设施进行维护管理；
c) 指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理。

4.9.2 资产管理

资产管理主要包括：
a) 编制并保存与智慧城市信息系统相关的资产清单；
b) 建立资产安全管理制度，明确智慧城市信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；
c) 根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
d) 对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

4.9.3 存储介质管理

存储介质管理主要包括：
a) 建立存储介质安全管理制度，对存储介质的采购、存放环境、使用、权属、维护和销毁等全过程作出规定；
b) 确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；
c) 对介质在物理传输过程中的人员选择、打包、交付等情况进行全要素控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点；
d) 对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质中存有敏感数据的需要有专人全程陪同；
e) 对重要介质中的敏感数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

4.9.4 设备管理

设备管理主要包括：
a) 对智慧城市信息系统相关的各种设备（包括备品备件）、线路等指定专门的部门或人员定期进行维护管理；
b) 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、许可证书、采购、发放和领用等全过程进行规范化管理；
c) 建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；
d) 对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备品备件）的启动/停止、加电/断电等操作；
e) 确保信息处理设备经过审批才能带离机房或办公地点。

4.9.5 漏洞和风险管理

4.9.5.1 漏洞管理

漏洞管理主要包括：

a) 从监测、分析、修复和验证等方面实现智慧城市各种 IT 资产漏洞的全生命周期管理；
b) 对漏洞进行监测，支持统一管理安全扫描策略，对内部网络设备、服务器、操作系统、应用软件等 IT 资产发现的安全漏洞进行持续监测；
c) 对漏洞进行分析，针对发现的漏洞结合资产信息和情报信息进行分析判断、计算风险、给出修复建议；
d) 对漏洞进行修复，根据修复建议修复漏洞；
e) 对漏洞进行验证，通过二次扫描方式对修复过的漏洞进行复测。

4.9.5.2 风险管理

风险管理主要包括：

a) 开展基础信息网络及关键信息基础设施风险识别工作，并及时处置相关风险，并依照通报机制进行智慧城市网络安全风险的通报；
b) 对数据风险进行分析，对数据风险异常行为分析和异常告警，对数据流动、数据访问的异常行为进行预警，用于发现数据泄露、数据滥用、数据篡改等数据安全风险；
c) 对数据进行溯源取证，在发生数据泄露、数据滥用等异常数据流动时，进行深入分析溯源，还原数据访问链路，定位泄露源。

4.9.6 网络安全管理

网络安全管理主要包括：

a) 建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；
b) 指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
c) 根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；
d) 实现设备的最小服务配置，并对配置文件进行定期离线备份；
e) 保证所有与外部系统的连接均得到授权和批准；
f) 不同网络之间隔离保护；
g) 依据安全策略允许或者拒绝便携式和移动式设备的网络接入。

4.9.7 系统安全管理

系统安全管理主要包括：

a) 建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定；
b) 根据业务需求和系统安全分析确定系统的访问控制策略；
c) 安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；
d) 指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险并相互制约；
e) 依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，不可进行未经授权的操作。

4.9.8 恶意代码防范管理

恶意代码防范管理主要包括：

a) 对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；
b) 指定专人对网络和主机进行恶意代码检测并保存检测记录；
c) 定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

4.9.9 密码应用管理

密码应用管理主要包括：

a) 智慧城市信息系统采用符合国家密码管理规定的密码技术进行保护，使用国家密码管理主管部门认证核准的密码技术和产品，并宜遵循密码相关国家标准和行业标准；
b) 按照密码相关国家标准和行业标准，进行密钥生命周期管理，包括密钥产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁，具体可参照 GB/T 39786—2021；
c) 在智慧城市信息系统规划和实施时，同步进行信息系统密码保障系统的规划和实施；
d) 智慧城市信息系统定期开展商用密码应用安全性评估，及时提交通过测评的商用密码应用安全性评估报告。

4.9.10 安全态势感知

安全态势感知主要包括：

a) 对智慧城市基础信息网络及关键信息基础设施涉及资产态势、数据安全态势、脆弱性态势、威胁态势、安全事件态势、违规态势、安全防护态势等进行态势评估研判；
b) 通过图示的方式实现城市网络安全实时及未来安全态势的展示。

4.9.11 安全服务管理

安全服务管理主要包括：

a) 对安全基础设施、安全大数据等安全服务的开通、应用、关闭等全过程进行管理；
b) 通过服务接口实现对通用防护、身份管理、认证管理、权限管理、密码管理、安全审计等安全基础设施安全服务的统一门户展示、统一调度监控等；
c) 通过服务接口实现对安全大数据服务的统一调度管理。

4.9.12 服务外包安全

服务外包安全主要包括：

a) 智慧城市信息技术服务外包，宜与服务外包商签订与安全相关的协议，明确约定相关责任；
b) 提供智慧城市信息技术服务外包的数据中心、云计算服务平台等设在境内。

4.9.13 运维合规管理

运维合规管理主要包括：

a) 对运维审计日志进行监控分析，发现违规操作；
b) 对用户的运维操作行为与审批记录进行对比分析和异常行为分析，及时发现运维操作安全风险，包括不限于运维特权账号的违规操作，并支持实时告警、阻止和历史溯源。

4.10 应急响应

4.10.1 应急预案

应急预案主要包括：

a) 宜在统一的应急预案框架下制定不同事件的应急预案，应急预案框架包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；
b) 宜从人力、设备、技术和财务等方面为应急预案的执行提供资源保障；
c) 对系统相关的人员进行应急预案培训，每年至少一次。

4.10.2 应急演练

应急演练主要包括：

a) 宜定期对应急预案进行演练，每年不少于一次，根据不同的应急恢复内容，确定演练的周期；
b) 明确应急预案需要定期审查和根据实际情况更新的内容，并按照执行。

4.10.3 事件处置

事件处置主要包括：

a) 制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；
b) 根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对计算机安全事件进行等级划分；
c) 制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；
d) 开展智慧城市基础信息网络及关键信息基础设施 7×24 h 网络安全事件监测工作，通过各类安全预警、威胁情报、通报信息，实现及时监测发现各类安全事件；
e) 报告所发现的安全弱点和可疑事件，但不能进行验证攻击；
f) 当安全事件发生时，评估事件的影响面和发展趋势；
g) 结合评估结果进行预警，在威胁大面积爆发前及时通报；
h) 对特定的攻击、漏洞、病毒或违规行为等发起预警通报。一次完整通报包括：通报名称、通报事件描述、通报规则、处置要求，预警通报可指定要通知的管理员或组织；
i) 对事件进行分析研判，基于安全大数据，利用数据分析、攻防经验等技术，完成安全事件的分析研判，确定安全事件的性质、影响范围；
j) 对事件进行响应处置，依据安全策略，按照不同安全事件级别进行应急响应处置，遏制安全事件进展，恢复服务并降低潜在损害风险。

4.10.4 恢复改进

恢复改进主要包括：

a) 进行调查取证，汇聚安全事件相关信息形成调查记录，通过设备环境、用户身份、操作行为、流量记录等信息进行溯源取证，还原事件过程并保全相关电子证据；
b) 对事件进行总结报告，在安全事件处置结束后，进行总结、分析和研判事件的原因和存在问题，整改安全策略，避免事件再次发生，并形成报告；
c) 对造成系统中断和造成信息泄露的安全事件采用不同的处理程序和报告程序；
d) 所有安全事件有安全审计记录。

4.11 网络安全供应商、服务商、运营商资质

网络安全供应商、服务商、运营商资质主要包括：

a) 供应商、服务商、运营商宜具备成熟的质量管理体系、信息安全管理体系和信息技术服务管理体系；
b) 软件供应商宜具备成熟的软件开发能力；
c) 涉及智慧城市敏感数据的供应商、服务商、运营商宜具备相关能力和经验。

5 安全技术

5.1 数据中心物理安全

宜符合GB 50174—2017 、GB 50462—2015 、GB/T 22239—2019、GB/T 39786—2021的规定。

5.2 物联感知与智能终端安全

5.2.1 终端安全接入

终端安全接入主要包括：
a) 智能终端宜具备有基于非对称密码算法的身份标识；
b) 智能终端和接入网关间的数据宜支持如下鉴别机制之一：
   1） 基于网络标识的鉴别；
   2） 基于 MAC 地址的鉴别；
   3） 基于通信协议的鉴别；
   4） 基于通信端口的鉴别；
   5） 基于口令的鉴别。
c) 智能终端宜具备安全的密钥存储区域和密码算法运行环境；
d) 密码算法符合相关国家标准和行业标准。

5.2.2 感知终端通信安全

感知终端通信安全主要包括：
a) 感知终端使用无线电通信时，宜符合 GA/T 1781—2021 的规定；
b) 感知终端的通信协议宜支持并启用传输完整性校验机制；
c) 感知终端宜具备处理通信延时或中断的能力；
d) 感知终端传输敏感信息时宜对传输数据进行加密；
e) 宜保证感知终端可用性，能够抵抗拒绝服务攻击。

5.2.3 感知终端数据安全

感知终端数据安全主要包括：
a) 宜采用使用加密或其他保护措施，实现重要数据的传输及存储的机密性和完整性；
b) 宜提供必要的隐私数据保护措施，防止隐私数据的泄露，为感知数据产生真实性证据；
c) 宜能够提供密码技术或其他保护措施，用来验证真实性证据和产生证据的感知设备身份是否一致；
d) 对于重要数据，宜冗余部署感知终端进行采集，保证采集数据可靠性。

5.2.4 感知终端安全防护

感知终端安全防护主要包括：
a) 感知终端宜在接入网络中具有唯一性网络身份标识；

b) 具有执行能力的感知设备宜能够对下达指令的对象进行身份鉴别和对下达指令的合法性进行验证；
c) 感知终端宜具有异常指令过滤功能，并及时告警系统安全管理员进行指令发送对象的审查；
d) 感知终端宜能够开启和关闭审计功能；
e) 感知终端与系统的连接、断开宜有提示或告警信息；
f) 感知终端宜关闭不用的通信端口。

5.3 区域边界与通信网络安全

5.3.1 区域边界接入安全

区域边界接入安全主要包括：
a) 宜对接入智慧城市网络的设备与终端进行最小权限控制，具体应用场景详见附录 E；
b) 宜对接入智慧城市网络的设备和终端进行入网注册、接入认证、入网合规检查，并进行统一管理；
c) 通过移动互联网接入的设备和终端宜开启接入认证，通过无线接入网关设备实现接入；
d) 宜采取入侵防范措施，检测非授权无线接入设备和非授权移动终端的接入行为，检测对无线接入设备的攻击行为；
e) 宜采取措施阻断非授权无线接入设备或非授权移动终端。

5.3.2 传输安全

传输安全主要包括：
a) 宜采用校验技术或密码技术保证通信过程中数据的完整性；
b) 宜对重要数据通过加密的通道进行传输，保证通信链路上数据传输机密性。

5.3.3 实体身份鉴别

实体身份鉴别主要包括：
a) 对登录网络设备的用户进行身份鉴别；
b) 对网络设备管理员的权限进行限制；
c) 网络设备用户的标识宜唯一；
d) 主要网络设备对同一用户宜选择两种或两种以上组合的鉴别技术来进行身份鉴别；
e) 网络设备的登录宜具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施，具有单点登录限制机制；
f) 当对网络设备进行远程管理时，采取必要措施防止鉴别信息在网络传输过程中被窃听、篡改和伪造。

5.3.4 访问控制

访问控制主要包括：
a) 在网络边界部署访问控制设备，启用访问控制功能；
b) 对进出网络的信息内容进行过滤，实现对应用层协议命令级的控制；
c) 按主体和客体之间的允许访问规则，决定允许或拒绝主体对客体的访问；
d) 对非授权设备私自联到内部网络的行为进行检查、阻断与追溯。

5.3.5 安全审计

安全审计主要包括：

a) 对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录，对日志记录进行保护，日志记录保护期限不少于 6 个月；
b) 采集、记录、分析网络流量，为发现网络攻击行为、网络违规行为、网络异常提供数据支撑。具体包括：
   1) 支持捕获网络流量或者导入第三方网络流量，支持协议还原和内容识别、分析和统计；
   2) 支持基于 IP 地址、时间、用户/用户组、协议、关键字等多种组合的审计策略配置，可自定义关键字；
   3) 支持将网络安全审计日志、网络流量推送到安全大数据平台。

5.3.6 入侵检测

入侵检测主要包括：
a) 在网络边界处对恶意代码进行检测和清除；
b) 在网络边界处监视端口扫描、强力攻击、APP 攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等攻击行为；
c) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击时间，在发生入侵事件时提供报警；
d) 设置防范应急安全措施，对异常攻击行为进行有效的应急处理。

5.4 云计算安全

5.4.1 云平台安全

云平台安全主要包括：
a) 云平台服务安全宜按照 GB/T 31167 执行；
b) 云平台通过国家云计算服务安全评估；
c) 云平台服务商宜符合 GB/T 31168 的规定；
d) 对云租户采取运行监督和审核采取追责措施，确保租户不会利用云平台来运行恶意的程序以及用于从事违法犯罪活动。

5.4.2 云租户安全

云租户安全主要包括：
a) 云租户应用访问控制支持应用访问控制、服务访问控制、运维访问控制和功能访问控制；
b) 云租户应用通讯加密支持应用访问传输加密、应用接口传输加密；
c) 云租户应用内容保护支持应用展示脱敏、应用数字水印、网页防篡改、应用数据反爬；
d) 云租户应用攻击防护支持 Web 攻击防护、API 攻击防护、应用层 DDos 攻击防护；
e) 云租户应用脆弱性防护支持应用漏洞扫描、应用漏洞修复、应用安全基线核查、应用代码安全审计；
f) 云租户应用特权管理支持应用运维特权防护、应用业务特权防护。

5.4.3 云资源安全

云资源安全主要包括：
a) 虚拟存储系统支持在不中断正常存储服务的前提下实现对存储容量和存储服务进行任意扩展，透明的添加和更替存储设备，并具有自动发现、安装、检测和管理不同类型存储设备的能力；
b) 在多租户的云计算环境下，实现不同租户之间数据和配置的安全隔离，保证每个租户数据的安全与隐私；

c） 虚拟存储系统支持按照数据的安全级别建立容错和容灾机制，以克服系统的误操作、单点失效、意外灾难等因素造成的数据损失。

5.4.4 物理资源安全

物力资源安全主要包括：

a） 物理设备宜进行端口访问控制，按照最小化原则，仅开启必要的服务端口；
b） 物理网络上宜根据业务安全需要划分安全域，划分结果支持虚拟化资源的按需、弹性分配，通过路由、虚拟局域网、访问控制列表等策略，对不同安全域进行隔离，确保彼此之间不同互相访问；
c） 物理网络上宜进行网络访问控制，安全域之间的访问控制策略宜能够防止非授权设备私自连接云平台内部网络，管控云平台内部设备主动外连；
d） 物理网络上宜进行网络威胁检测，宜能够及时检测、分析，并阻断物理网络中存在的安全威胁；
e） 物理主机操作系统宜采取基线核查、漏洞扫描、主机入侵检测、安全加固等措施，提高物理主机操作系统的安全防护能力。

5.5 计算和存储安全

5.5.1 身份鉴别

身份鉴别主要包括：

a） 对登录进入智慧城市计算环境的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有一定复杂度并定期更换；
b） 采用口令、密码技术、生物技术等两种或两种以上组合鉴别技术进行身份鉴别；
c） 当远程利用智慧城市计算环境时，采取必要措施防止鉴别信息在网络传输中被窃听，当远程管理云计算平台中设备时，管理终端和云计算平台之间建立双向身份验证机制。

5.5.2 访问控制

访问控制主要包括：

a） 对登录进入智慧城市计算环境的用户分配帐户和权限，授权管理用户所需的最小权限，实现管理用户的权限分离；
b） 对云租户分配帐号，能够实现对虚拟机、云数据库、云网络、云存储的访问授权；
c） 由授权主体配置访问控制策略，访问控制策略宜规定主体对客体的访问规则；
d） 访问控制的颗粒度宜达到主体为用户级或进程级，客体为文件、数据库表级；
e） 宜保证当虚拟机迁移时，访问控制策略随其迁移；
f） 宜允许智慧城市中云服务客户设置不同虚拟机之间的访问控制策略。

5.5.3 安全审计

安全审计主要包括：

a） 宜启用安全审计功能，审计应覆盖到智慧城市计算环境每个用户；
b） 宜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；
c） 宜对审计进程进行保护，防止未经授权的中断；
d） 宜对智慧城市云平台中云服务商和云租户的远程管理进行审计；
e） 宜支持云计算中租户对与本租户相关资源的审计。

5.5.4 恶意代码防范

恶意代码防范主要包括：

a) 宜采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断；
b) 宜能检测虚拟机对物理机及物理资源的异常访问；
c) 宜对云租户的行为进行监控，对云租户发起的恶意攻击进行检测和警告。

5.6 数据安全

5.6.1 大数据安全

大数据安全主要包括：

a) 宜选择安全合规的大数据平台，其所提供的大数据平台服务为其所承载的大数据应用提供相应等级的安全保护能力，数据安全治理中台应用场景见附录 F；
b) 宜以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容；
c) 当数据迁移时，宜确保在任何云环境和服务方式下，数据资源的司法管辖关系不变，资源所有权不变，安全管理责任不变，安全管理要求不变；
d) 明确约束数据交换、共享的接收方对数据的保护责任，并确保接收方有足够或相当的安全防护能力；
e) 宜以书面形式明确各种服务模式下，数据平台所有方和数据运营方对计算资源的控制范围和安全责任边的边界；
f) 宜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、数据传输、数据存储、数据处理、数据交换、数据销毁等过程；
g) 宜制定并执行数据分类分级保护策略，针对不同类别级别的数据制定不同的安全保护措施；
h) 在数据分类分级的基础上，划分重要数字资产范围，明确重要数据进行自动脱敏或去标识的使用场景和业务处理流程；
i) 在数据清洗和转换过程中宜对重要数据进行保护，以保证重要数据清洗和转换后的一致性，避免数据失真，并在产生问题时能有效还原和恢复；
j) 宜定期评审数据的类别和级别，如需要变更数据的类别或级别，依据变更审批流程执行变更。

5.6.2 重要数据保护

重要数据保护主要包括：

a) 宜采用密码技术保证重要数据在传输和存储过程中的机密性和完整性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
b) 宜提供对重要数据的密文检索能力，确保加密后的数据不能影响正常访问；
c) 宜通过文件加密、数据库加密等方式，保障重要数据存储安全；
d) 宜保证存有重要数据的存储空间被释放或重新分配前得到完全清除；
e) 宜根据数据的敏感程度，将数据进行分级管理，支持根据数据内容设定敏感级别，数据级别权限支持向下兼容，高数据级别权限可访问低级别数据。

5.6.3 个人信息保护

个人信息保护主要包括：

a) 宜按照 GB/T 35273—2020 加强智慧城市个人信息的保护，智慧城市相关信息系统和服务仅采集和保存业务所需的用户个人信息；
b) 每年宜定期开展个人信息保护监督检查工作，形成检查报告并记录完整；
c) 宜对智慧城市个人信息保护加强宣传教育。

5.7 服务与接口安全

5.7.1 服务安全

服务安全主要包括：

a) 文件服务宜具备文件访问控制、数据冗余处理、文件访问安全审计；
b) 云数据库服务宜具备访问控制及隔离、云数据库攻击防护、云数据库安全审计和敏感数据保护功能；
c) 计算服务宜提供安全访问控制能力，对重要数据支持计算过程解密存储时调用加密服务进行透明加密，对开源数据计算组件进行安全加固，为服务提供基于角色的访问控制功能；
d) 容器服务具备镜像安全机制、资源隔离、访问控制、漏洞扫描、容器防逃逸、安全加固配置功能；
e) 分布式组件服务宜通过安全认证和授权，确保分布式各组件、进程、接口和节点间的安全；
f) 密钥管理服务宜对用户密钥生命周期统一管理、支持密钥自动定期轮换、支持用户对自身密钥授权管理。

5.7.2 接口安全

接口安全主要包括：

a) 智慧城市产品选型宜满足统一安全管理和安全运维的接口；
b) 统一用户管理接口，宜通过用户管理接口实现智慧城市各信息系统的用户同步；
c) 智慧城市宜实现基于 CA 的统一认证和授权机制，通过统一的认证和授权接口，实现对用户的认证和授权操作；
d) 宜统一智慧城市安全监控接口，通过此接口获取智慧城市信息系统的安全状态，分析智慧城市整体安全态势；
e) 宜提供数据安全访问接口，可实现对高安全等级数据的访问；
f) 宜提供统一的安全策略配置接口，实现智慧城市信息系统安全策略的统一配置和管理。

5.8 智慧应用安全

5.8.1 代码安全

代码安全主要包括：

a) 宜制定代码编写安全规范，开发人员参照规范编写代码；
b) 宜保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道；
c) 宜提供具备第三方源代码安全审计服务机构出具的代码审计报告。

5.8.2 逻辑安全

逻辑安全主要包括：

a) 宜在软件开发过程中对安全性进行测试；

b) 宜制定功能、安全测试验收方案，并依据测试验收方案，实施测试验收，形成测试验收报告，测试报告由具备资质的第三方软件评测机构出具。

5.8.3 性能安全

性能安全主要包括：

a) 应用的并发用户数、相应时间、系统吞吐量指标宜达到智慧城市预设数量人员访问、使用的要求；
b) 宜制定性能测试验收方案，并依据测试验收方案，实施测试验收，形成测试验收报告，测试报告由具备资质的第三方软件评测机构出具。

5.9 安全运营

5.9.1 态势感知

态势感知主要包括：

a) 宜从国家层面、省市大地域层面，对国计民生相关的关键信息基础设施的安全态势进行整体的监测与关注；
b) 宜建立面向大数据环境，系统化、标准化、适用不同应用场景的网络安全态势感知模型，突破大数据环境下网络安全态势提取、态势评估、态势预测关键技术；
c) 采集宜包括网络的拓扑信息、脆弱性信息和状态信息等静态的配置信息，和各种防护措施的日志采集和分析技术获取的威胁信息等动态的运行信息；
d) 宜融合获取各类网络监测数据，根据网络安全特征属性的领域知识和历史数据，构建数学模型综合评估网络安全态势；
e) 宜基于对当前网络安全态势评估和已有的历史评估数据，对未来一段时间内的网络安全态势变化趋势进行预测；
f) 宜利用大数据可视化技术，从宏观呈现整体安全态势，从多维度呈现专题安全态势。具备可视化交互分析能力，从资产、用户、运行、弱点、威胁、风险等多个角度进行多方位的态势评估、预测与呈现，帮助用户全面掌控目标系统的安全态势；
g) 宜提供态势数据的多维度查询和自定义查询，形成态势分析报告；
h) 宜对智慧城市中的网络、网络设备、终端、服务器、安全产品、业务应用系统进行有效的安全管理和运行监管，掌握网络安全态势。

5.9.2 情报预警

情报预警主要包括：

a) 宜及时报送网络安全监测预警信息，为威胁预警、线索挖掘、应急处置、安全评估、攻击溯源等提供支撑；
b) 宜建立统一的威胁情报共享交换机制，实现威胁情报的及时共享，通过共享有关最新威胁和漏洞的信息，在利益相关方之间创建态势感知，并迅速实施补救措施；
c) 宜建立针对安全漏洞的早期预警机制，主动挖掘和分析系统中存在的安全漏洞缺陷，并进行预警，防止被恶意利用；
d) 宜建立针对安全威胁的中期预警，实时跟踪网络运行情况，预测潜在的网络威胁，识别高风险资产，按照规定和程序及时通报相关威胁，尽快采取应对措施，主要针对已经在其他地方出现，但尚未涉及到所防护网络的威胁源；

e) 宜建立对入侵攻击的及时预警，实时监测网络攻击行为、异常访问行为，及时报警响应，阻止大规模入侵、破坏行为的发生，防止事态扩大；
f) 宜建立对异常行为的预警，通过监测分析内部网络的用户操作和网络行为，及时发现违规操作、蓄意破坏、病毒传播等异常情况，准确追踪定位威胁源头，重点对发生在内部网络中的异常行为或攻击企图进行预警；
g) 宜建立共享交换标准，遵循结构威胁信息表达和可信自动指标信息交换相关标准，或根据实际场景需求扩展或自定义交换标准，满足结构化网络安全需求；
h) 宜建立快速、可扩展、自动化的威胁共享模式，简化和加快共享过程，以及安全信息的补救。

5.9.3 安全监测

安全监测主要包括：

a) 宜构建具备持续性、主动性、实时性的安全监测机制，实现对智慧城市安全事件的全天候动态监测；
b) 宜以网络监测为基础，全面发现网络边界和关键区域的安全威胁；深入业务应用监测，精准定位应用安全问题；聚焦数据安全监测，保证核心数据使用有迹可循；
c) 宜提供包括特征检测及异常检测等在内的监测技术手段，实现对各类安全事件的全覆盖监测；
d) 宜提供对网络攻击事件的监测能力，对网络流量中的异常网络行为和恶意通信进行实时检测和处理，识别网络攻击与异常线索信息，包括恶意文件检测、攻击向量检测、协议头异常线索提取、未知威胁提取等主要功能；
e) 宜提供对网络的脆弱性分析，对网络中的设备、系统、应用存在的脆弱性情况进行分析，发现网络中存在的安全漏洞；
f) 宜提供对恶意程序的监测，对网络中的计算机/服务器中存在的恶意程序情况进行分析，以保障处理、存储、载体与环境的安全保密性；
g) 宜提供对用户违规操作行为的监控，对终端、服务器、网络设备、应用系统进行配置性分析，识别是否存在违规操作、违规配置情况；
h) 宜能够识别用户异常行为，包括普通用户异常行为分析、管理员异常行为分析，识别用户是否存在失泄密情况；
i) 宜能够识别数据安全风险，围绕敏感数据全生命周期过程，从数据使用、存储、流转等环节进行监控分析，识别是否存在泄密情况；
j) 宜实时监控网络内设备及系统运行情况，及时发现网络可用性、连通性、健康度等相关问题；
k) 宜按照 GB/Z 20986，对安全事件进行分类分级管理；
l) 宜构建安全事件应急响应预案，当发生安全事件时自动及时通知相关的安全负责人，并启动相应的应急处置流程。

5.9.4 日志审计

日志审计主要包括：

a) 宜从网络安全、主机安全、应用安全、数据安全等角度进行安全审计；
b) 宜提供完备的日志数据采集能力，支持主动采集和被动采集的方式；
c) 宜支持广泛的采集对象及丰富的日志数据类型，能够采集不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心；

d) 宜支持对多源异构数据的标准化治理，针对不同格式的日志信息解析提取关键信息完成日志信息的过滤、日志合并和日志格式的统一化规整，使规整后的日志简单易懂便于分析，统一化处理的日志格式可通过导入解析文件的方式灵活扩展；
e) 宜提供集中可靠的日志存储，将采集的所有原始日志、事件和告警信息统一存储起来，建立集中的日志存储系统，同时，提供多种日志存储策略，能够方便地进行日志备份和恢复；
f) 宜提供快速的查询审计能力，基于大量日志索引的日志检索引擎，从数据存储方式、索引建立和查询分析方面入手，实现了对日志的快速检索能力；
g) 宜提供日志分析能力，支持常见流量协议及日志数据的解析还原，针对多源异构设备日志，可基于规则进行安全事件分析，分析出事件的类型、级别、具体内容等，并支持动态规则定义，以扩展更多的安全事件分析；
h) 宜提供报表报告，获悉全网的整体安全运行态势，实现全生命周期的日志管理。

5.9.5 策略协同

策略协同主要包括：

a) 宜对安全设备的可见性和集中管理，简化整个网络的安全策略规则管理，并减少由于安全设备配置错误而导致的安全风险；
b) 宜依据等保，实现不同品牌、不同种类的网络访问控制设备配置的采集，对策略相关数据进行提取，为上层计算模块提供标准化数据，并且可以反向将配置脚本下发至设备，最大限度地降低管理复杂性和减少错误配置的可能性；
c) 宜能够识别冗余、隐藏、重叠和冲突的规则，实现垃圾策略与风险策略的检查，通过定期对存量策略规则的清理优化，实现策略规则最小化与精细化的平衡；
d) 宜提供安全策略的审核和合规性管理，内置合规性配置文件，在违反准则时会发出警报；
e) 宜提取基于合规性的报告，并将其用于审计目的，实时识别合规性差距；
f) 宜提供策略变更的自动化管理，在实施策略变更之前，执行变更影响分析；
g) 宜提供协同处置工作流，当发现策略违规时，通过工作流来纠正违反的现有规则。

5.9.6 安全防护

安全防护主要包括：

a) 宜提供安全保护技术措施，以确保智慧城市系统中敏感数据全生命周期内的安全；
b) 宜对智慧城市运营中心的数据库系统进行安全检查，对数据库的安全状况进行持续化监控；
c) 支持系统的弱口令检查，基于各种主流数据库口令生成规则实现口令匹配扫描，提供基于字典库、基于规则、基于穷举等多重模式下的弱口令检测；
d) 宜支持数据传输加密，采用符合国家标准和行业标准的密码技术保障业务数据安全，防止数据在通过不可信或者较低安全性的网络进行传输时，发生数据被窃取、伪造和篡改等安全风险，保障数据在传输过程中的安全性；
e) 宜确保智慧城市中重要数据采取了数据泄漏防护措施，实时保护端点或网络中传输和外发数据，实时预警和阻止数据被泄漏的行为发生；
f) 宜支持访问控制，基于IP、MAC、客户端主机名、操作系统用户名、客户端工具名和数据库账号等多个维度对用户身份进行鉴别，确保设备是可信设备，应用是认证应用，账号是认证账号。

5.9.7 密钥管理

密钥管理主要包括：

a) 宜保证为智慧城市提供密钥服务的安全性；
b) 宜建立身份认证体系；
c) 可采用量子密码提供密钥管理中心多中心密钥同步，量子密钥分配协议参见附录G。

5.10 保密及密码技术安全

智慧城市涉及保密内容及密码技术、产品和服务宜遵从相关部门规定。

6 安全评价指标体系

智慧城市网络安全评价指标体系包括4个一级指标、25个二级指标、99个三级指标，如图1所示。一级指标包括网络安全责任制、网络安全保障体系、网络安全保障能力、网络安全监管，涵盖了对智慧城市网络安全进行评价的四个方面。三级指标包括指标名称、评价内容和评价方法，见附录H。

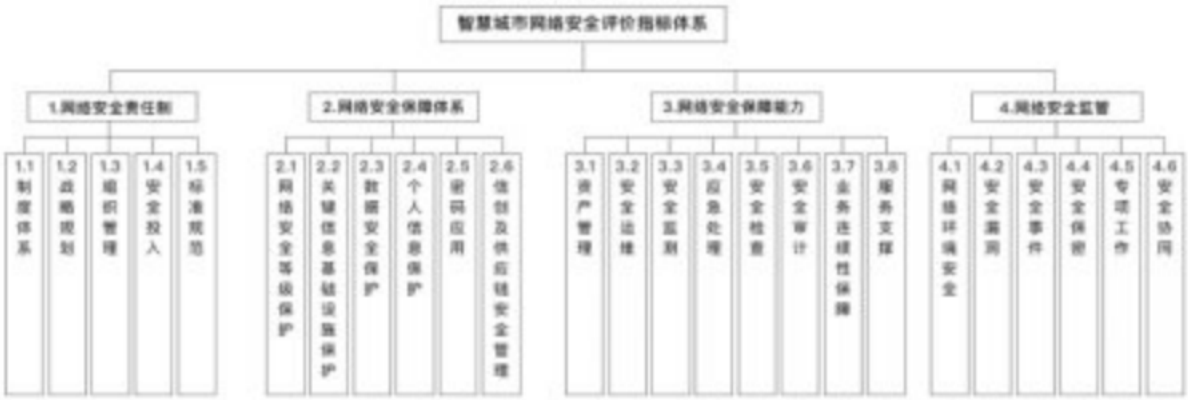

图1 智慧城市网络安全评价指标体系

附 录 A
（资料性）
基于零信任架构的智慧城市网络安全防护应用场景

A.1 场景描述

智慧城市在网络建设中，存在接入终端数据大，访问频繁，采用早起的访问控制技术已无法满足要求，需要采用一种新的网络安全防护技术来对网络进行保护。基于零信任架构的智慧城市网络安全防护可以保护智慧城市物联网应用的安全，保障智慧城市物联网所有接入设备的安全。

A.2 解决方案

基于零信任架构的智慧城市网络安全防护以构建安全便捷的城市网络为目的，以解决城市网络建设中面临的诸多安全问题为目标，在城市洞察、城市治理、产业发展、民生服务等领域提供智能化的产品和解决方案，全面应用于智慧物业、智能停车、智能红绿灯、智慧养老等系统，助力城市数字化转型升级。总体架构如A.1所示。

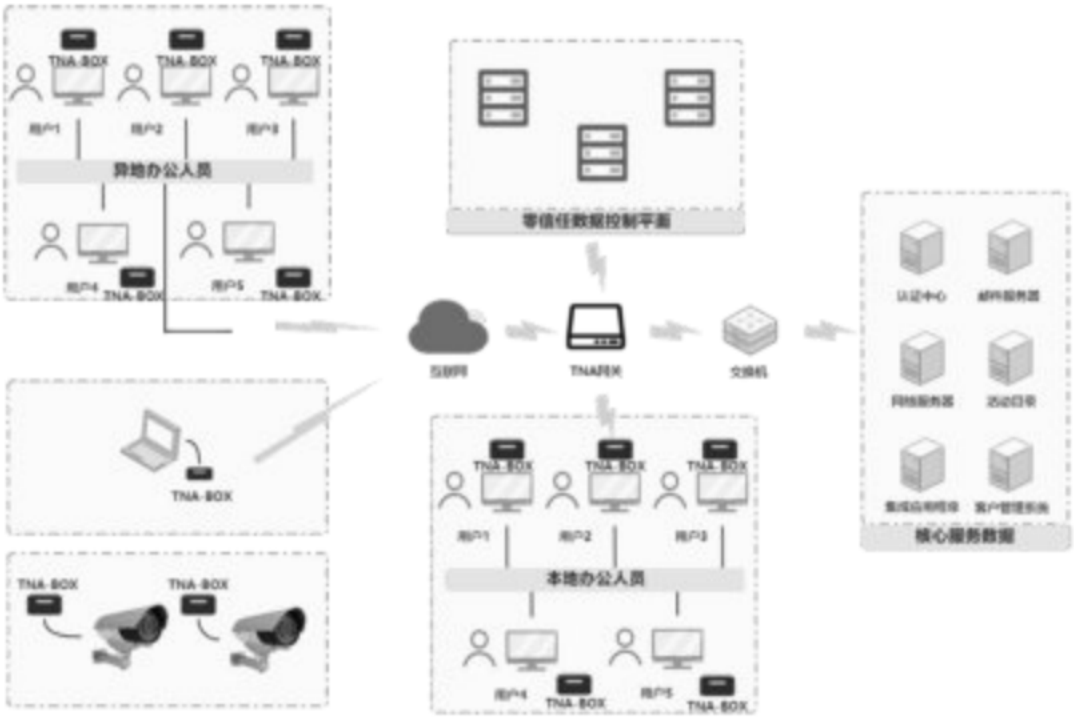

图 A.1 基于零信任架构的智慧城市网络安全防护总体架构

零信任架构的智慧城市网络安全防护在基于国密算法的全网智能终端的身份体系上构建基于零信任架构的智能终端统一接入和授权管理平台，对于接入网络的智能终端，授予最小访问权限，并对全链路访问加密和监控，确保访问合法性和可控性。对于网络应用严格控制之间的访问路径，防御东西向攻击，减小整个系统的攻击面。同时采集海量的智能终端数据信息，构建网络天眼系统，智能化的持续评估和动态感知城市安全风险，并通过和零信任安全接入网关的联动，隔离和阻断网络危险源头，确保智慧城市网络的整体可用性和健壮性。

附 录 B
（资料性）
网络安全检测与评估应用场景

B.1 场景描述

智慧城市在运行过程中应有效的识别网络中的安全风险，构建网络信任体系、容灾备份体系、监控审计体系、监测与防护体系、网络安全态势感知体系、应急指挥体系等，因此需要建立一个智慧城市网络安全检测与评估系统，协助山东省政府部门及智慧城市各相关方有效识别智慧城市网络安全风险，建立信息共享与通报预警机制、突发网络安全事件应急机制，加强智慧城市网络安全建设，保障智慧城市网络基础设施、重要信息系统和关键数据资源的安全。

B.2 解决方案

智慧城市网络安全检测与评估系统的建设要依据山东省智慧城市网络安全建设的管理和技术要求，面向物联感知安全、网络通信安全、计算环境安全、云平台安全、数据安全、应用服务安全等六大技术领域实现安全和内容的防护工作。系统要从智慧城市的基础设施层到应用服务层，实现对数据库、服务设备、网络设备、网络、数据、机房、通信、密钥管理等服务和组件的分层安全防护工作。总体框架如图B.1所示。

图 B.1 网络安全检测与评估总体架构

智慧城市网络安全检测与评估系统可以基于安全数据高速采集技术、安全行为检测分析技术、安全内容检测分析技术以及安全风险检查和安全风险评估技术，实现系统应用功能。系统通过综合安全管理门户，并依托安全防护体系的建设，实现了网络流量还原检测审计、数据泄漏风险检测、接入设备安全检查、应用与数据库安全检查、内容情报安全检查、网络风险安全评估等功能，并基于威胁情报分析与共享交换服务功能，实现更加精准的攻击与威胁的检测发现。

附 录 C
（资料性）
数据防泄漏安全应用场景

C.1 场景描述

智慧城市数据在采集、传输、存储、交换过程中，会存在因非偶然或者恶意等方式的破坏、更改、泄漏，尤其是云数据资源一旦遭受破获损失更大。因此在该场景下，需要一套数据防泄漏系统，保护智慧城市所产生的数据免遭数据丢失或泄漏。

C.2 解决方案

智慧城市数据泄漏防护系统应采用统一的管理中心，统一的防护策略，以防止数据资产违规或非授权输出为目标，以数据全生命周期管理为理念，以泄露风险为驱动，依据数据特点，灵活采用内容智能识别、深层内容分析、实时敏感数据发现、全方位审计、精准拦截等技术手段，对智慧城市内网络、终端、存储中的敏感数据进行发现、监控和保护。基于政务应用场景，提供量身定制的产品服务，通过深度内容分析和事务安全关联分析来识别、监视和保护静止、移动和使用中的数据，通过事前预警、事中保护、事后追溯的管理手段，防止存储、网络、终端、移动计算、云计算等各种具体应用场景下的数据泄露、扩散。总体框架如图C.1所示。

图 C.1 数据防泄漏总体架构

附 录 D
（资料性）
跨网数据交换安全应用场景

D.1 场景描述

为保护网络的安全性，智慧城市在网络建设过程中往往会采用多个安全网域的形式，不同网域之间会存在数据传输的需求。建立一套跨网数据安全交换系统来实现为两个不同网络业务区服务器之间的数据交换与共享，以实现两个不同网络内部的安全、数据传输的安全、数据内容的安全。系统架构如图D.1所示。

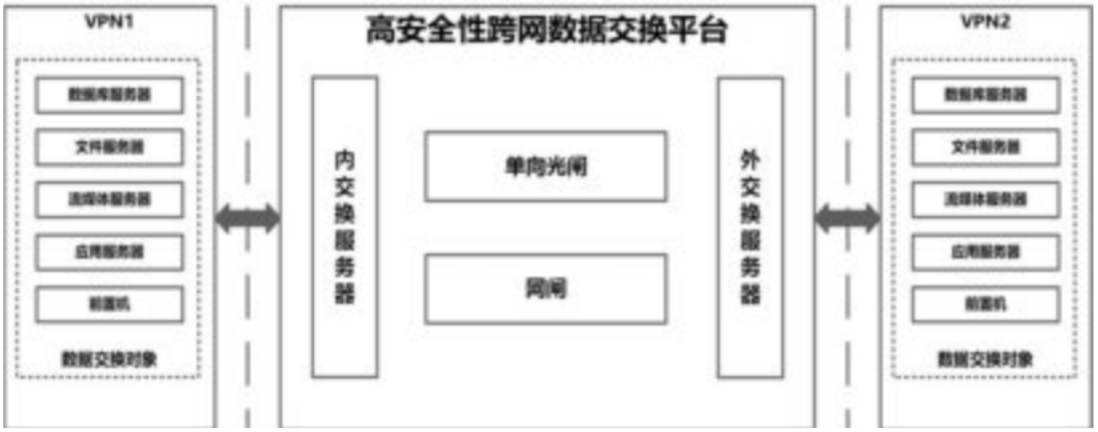

图 D.1 跨网数据安全交换架构

D.2 解决方案

D.2.1 电子政务数据交换安全解决方案

电子政务数据交换依托一体化在线政务服务平台，建设跨网数据安全交换平台，实现各个网络之间的文件交换、数据库同步、请求命令与响应数据交换、服务接口调用、数据可视化等，如图D.2所示。

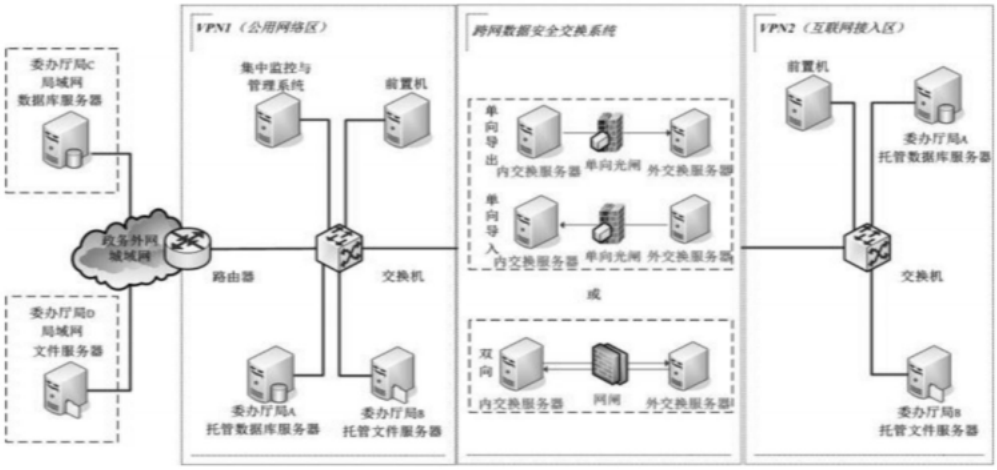

图 D.2 电子政务数据交换应用场景

D.2.2 不动产“一网通办”数据交换安全场景

不动产的“一网通办”充分考虑信息安全等级保护工作相关要求，强化网络边界安全防护，确保政务外网不动产登记审核、登簿、缮证业务数据与自然资源专网之间数据的共享，包括数据库和接口数据。同时，完善安全监控和响应处理体系，实时监控网络中的可疑事件及安全事件，并及时进行处理。不动产“一网通办”跨网数据共享的安全解决方案如图D.3所示。

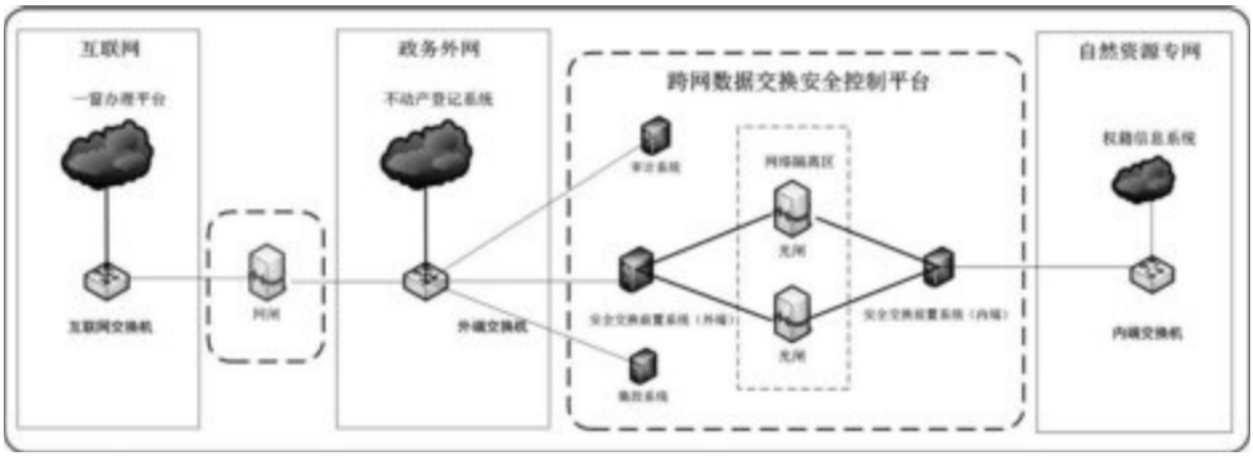

图 D.3 不动产“一网通办”跨网数据共享的安全解决方案

附 录 E
（资料性）
抗攻击安全接入应用场景

E.1 场景描述

智慧城市网络运行中，在感知设备连接控制网络、用户终端接入系统网络、运维终端接入软件系统等接入时，存在被恶意攻击。因此，需要建立一套抗攻击安全接入系统，采用在客户端设备配备安全模块，通过抗攻击网关接入系统，避免操作系统及开源组件遭受漏洞攻击，并阻止外部恶意攻击者利用上述安全威胁破坏安全边界防护设备的安全性和有效性。

E.2 解决方案

E.2.1 终端设备安全接入

抗攻击安全接入系统，对系统进行抗攻击加固防护和二次加密，防止传输内容被恶意攻击者通过非法手段截取。典型应用如图E.1所示。

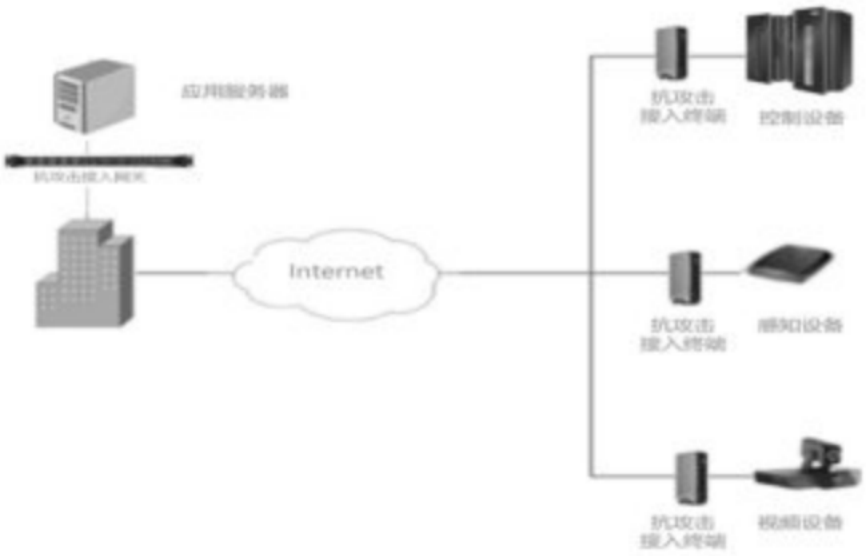

图 E.1 终端设备安全接入典型应用

E.2.2 运维安全接入

运维安全接入，在堡垒机前方部署抗攻击网关，操作员通过抗攻击接入终端访问堡垒机，可以保证访问堡垒机人员的可控性，有效避免因为堡垒机漏洞而被攻击，保障系统的安全。典型应用如图E.2所示。

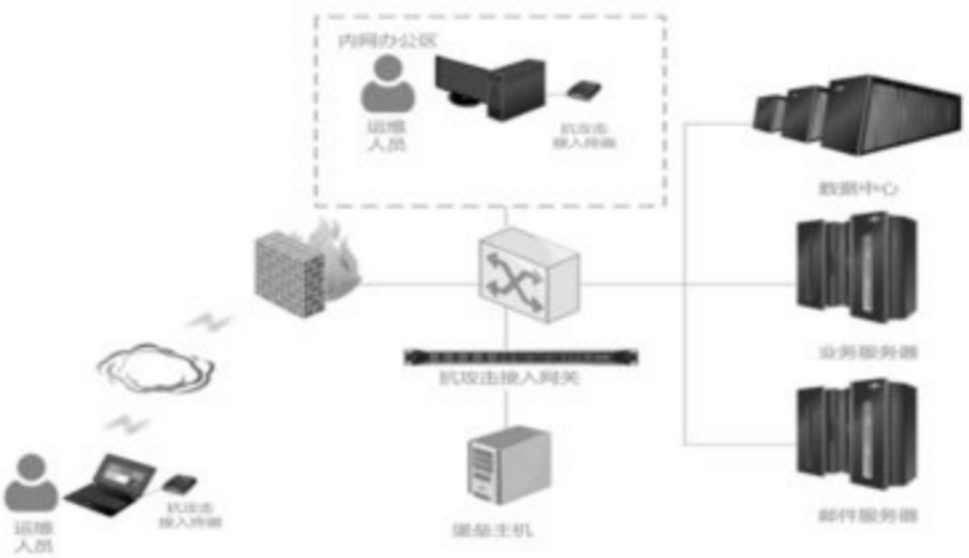

图 E.2 运维安全接入典型应用

附 录 F
（资料性）
数据安全治理中台应用场景

F.1 场景描述

智慧城市建设过程中需要考虑数据中心的安全，以及网络中存在的异常流量、攻击等，需要将数据进行统一的汇总分析，因此需要建立一套数据安全治理中台来满足该需求。该中台满足如下情况：

a) 数据安全治理中台应对智慧城市数据中心的各类数据进行采集、分析，对智慧城市数据中心资产的安全状况进行分析、刻画，全面摸清数据中心安全现状，及时发现存在的各类安全隐患，排查并督促整改重要网络安全隐患、风险和突出问题；

b) 数据安全治理中台应对智慧城市数据中心网络流量分析，感知网络中的异常威胁数据，包括非法入侵攻击数据、终端异常行为数据、病毒传播时空感知数据等；

c) 数据安全治理中台应结合云端威胁情报，感知智慧城市数据中心中各类设备的安全状态、漏洞弱点、异常威胁及非法接入等安全情况，基于自适应安全架构，针对设备安全态势的预测、防护、监控和响应，从端点安全、边界安全、数据安全和管理安全多个层面实现整体的安全能力，实现资产威胁可视化、达到资产安全可管可控。

F.2 解决方案

数据安全治理中台，以数据安全为中心，运用大数据技术汇聚智慧城市全网安全数据，从“云、数据、应用、网络、边界、端”六维构建，实现统一安全管理，构建安全、可信、合规的智慧城市大数据智能化安全立体纵深防御体系。总体框架如图F.1所示。

具体来说，数据安全治理中台，通过统一接入、统一解析，减少沟通成本和开发成本，避免数据多次重复接入；通过数据统一处理、统一组织，减少存储资源和计算资源冗余；通过数据统一治理，数据标准、业务规则统一，避免同样的业务逻辑在各个系统计算口径不一致；通过数据统一分析，挖掘数据关系，横向拉通后多维分析数据问题，打破数据孤岛；通过服务统一管理，数据出口统一管理，既降低了数据安全管理难度，又屏蔽了异构数据处理技术带来的开发成本。

数据安全治理中台的核心数据资产，是通过数据处理和组织，形成的原始库、资源库、主题库、业务库，以及人工录入、积累或者机器学习等方式产生的基础数据和知识库。

数据安全治理中台通过全面收集网络设备（路由器、交换机等）、网络安全设备（防火墙、入侵检测系统等）、应用系统（邮件、OA等）等设备系统的运行日志和安全事件日志，对日志进行分类归并、关联分析等操作把海量日志中有价值的信息提取出来，并且平台提供统计、查询及审计报表，为直观的日志查询、分析、展示提供强有力的数据支撑，便于管理员了解整个数据中心的安全态势。

数据安全治理中台提供全维度、跨设备、细粒度的关联分析，透过事件的表象真实地还原事件背后的信息，提供真正可信赖的事件追责依据和业务运行的深度安全。同时提供集中化的统一管理平台，将所有的日志信息收集到平台中，实现信息资产的统一管理、监控资产的运行状况，全面审计信息系统整体安全状况。

图 F.1 数据安全治理中台总体架构

附 录 G
（资料性）
量子密码应用场景

G.1 场景描述

量子密码是一种新兴的密码体制，其安全性基于量子物理学基本原理，具有理论上的无条件安全性。随着智慧城市网络安全重要性的提升，在智慧城市网络中采用量子密码的形式对城市安全起到重要作用。主要应用场景包括应用于密钥产生、数据加密和身份认证等。

G.2 解决方案

密钥管理中心负责对用户密钥生命周期统一管理，包括密钥产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁，同时支持用户对密钥使用授权管理。密钥管理中心支持多中心层级管理和分中心协同管理，用户的密钥可以在某一个中心上独立生成并在所管理范围内安全使用，当用户跨中心使用密钥时需要对密钥进行安全同步，为了保障密钥跨中心同步不泄露，可以通过量子密钥分配与中继技术实现密钥的在多中心间的安全同步。总体架构如G.1所示。

每个密钥中心都可以通过量子密钥源产生用户所需的密钥，将密钥分发给用户的同时中心会对密钥进行存储与备份管理，用户密钥在密钥管理中心的管理下受控使用。当用户从一个中心迁移到另一个中心使用密钥时，被使用的用户密钥通过量子密钥分配和中继技术被同步到对应的密钥管理中心，通过一次一密的密钥保护技术，实现无条件安全的密钥同步。

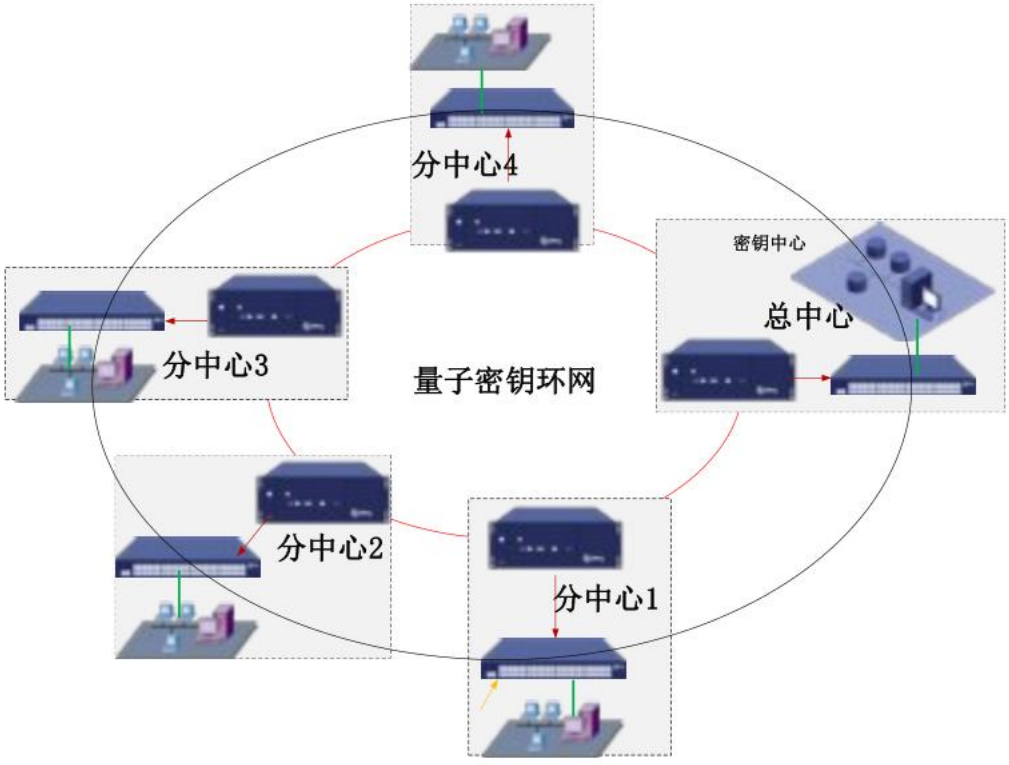

图 G.1 多密钥管理中心密钥同步总体架构

附 录 H
（资料性）
智慧城市网络安全评价指标

H.1 网络安全责任制

H.1.1 制度体系

制度体系评价指标见表H.1。

表 H.1 制度体系评价指标

指标名称	评价内容	评价方法
领导责任	明确运营单位主要负责人是第一责任人，主管网络安全的领导班子成员是直接责任人。	调研市（区）是否组织会议或正式文件明确运营单位第一责任人与直接责任人。
工作机构	a）明确负责网络安全工作的部门及其职责。 b）安全工作机构人员配备情况。	a）统计市（区）单位中通过正式制度文件明确负责网络安全工作的部门及其职责的单位比率； b）统计市（区）单位中为网络安全工作部门配备专职网络安全人员的比率。
制度建立	正式印发网络安全工作责任落实实施办法或细则等,或以相关文件明确责任落实要求。	调研市（区）单位是否正式印发网络安全工作责任落实实施办法或细则等,或以相关文件明确责任落实要求。
工作机制	网络安全工作机制落实情况。	a）调研市（区）单位领导班子主要负责人是否每年至少召集一次专题会议； b）调研网络安全直接责任人是否至少每季度召集一次网络安全联席会议，听取网络安全工作汇报，研究部署网络安全工作。

H.1.2 战略规划

战略规划评价指标见表H.2。

表 H.2 战略规划评价指标

指标名称	评价内容	评价方法
方针目标	网络安全战略方针、目标明确情况。	a）调研市（区）是否制定网络安全工作的总体方案，明确战略方针； b）调研市（区）是否明确网络安全工作的主要目标、基本要求、工作任务和保护措施。
规划制定及实施	网络安全规划制定及实施情况。	调研市（区）是否制定并发布了网络安全规划及实施方案。
创新模式	防护模式创新探索情况。	调研市（区）是否提出创新防护模式及创新运营模式。

H.1.3 组织管理

组织管理评价指标见表H.3。

表 H.3 组织管理评价指标

指标名称	评价内容	评价方法
智力支撑	a）明确智库机构建立情况。 b）专家队伍组建情况。	a）调研市（区）是否建立网络安全智库机构； b）调研市（区）是否组建网络安全专家队伍。
宣传教育	安全人员的安全意识教育、安全技能培训和宣传工作开展情况。	统计市（区）单位中组织开展安全意识教育、安全技能培训和宣传等活动的比率。
人员考核	安全人员考核与奖惩工作开展情况。	统计市（区）单位中开展技术技能考核、安全考核与奖惩工作的比率。
服务人员管理	a）保密协议签署情况； b）离岗人员管理情况。	a）调研市（区）单位与在岗安全人员签署保密协议的比率； b）调研市（区）单位中按离职流程制度办理的人员比率。

H.1.4 安全投入

安全投入评价指标见表H.4。

表 H.4 安全投入评价指标

指标名称	评价内容	评价方法
新建项目网络安全预算	新建信息化项目的网络安全预算情况。	统计市（区）新建信息化项目网络安全建设投资占比。
网络安全保障工作经费落实	安全日常运维、教育培训、安全防护加固、风险评估、升级运维、应急处置等网络安全保障工作经费落实情况。	统计市（区）采购安全日常运维服务的单位覆盖率、采购安全教育培训服务的单位覆盖率、采购安全防护加固服务的单位覆盖率、采购安全风险评估服务的单位覆盖率、采购安全升级运维服务的单位覆盖率、采购安全应急处置服务的单位覆盖率。

H.1.5 标准规范

标准规范评价指标见表H.5。

表 H.5 标准规范评价指标

指标名称	评价内容	评价方法
安全标准规范化	a）安全运行管理制度体系建设情况； b）安全标准规范、行业指引制定情况。	a）统计市（区）单位中制定网络安全管理制度的比率； b）调研市（区）是否制定并发布网络安全标准规范、行业指引。
安全标准规范执行	制定的安全标准规范执行情况。	调研市（区）单位中安全标准规范执行落实比率。

H.2 网络安全保障体系

H.2.1 网络安全等级保护

网络安全等级保护评价指标见表H.6。

表 H.6 网络安全等级保护评价指标

指标名称	评价内容	评价方法
定级备案	按照等级保护要求开展安全定级备案。	统计市（区）单位中信息系统等级保护定级备案的比率。
测评整改	按照等级保护要求开展安全等级保护测评与整改。	按照等级保护要求开展安全等级保护测评与整改。
上线前测评	系统上线前开展安全测评及整改情况。	统计市（区）单位中信息系统上线前开展安全测评的比率。
通用技术防护落实	按照等级保护标准要求，落实分层分区防御、隔离管控等安全技术要求。	统计市（区）落实分层分区防御覆盖概率、隔离管控覆盖率、互联网出口安全管控覆盖率。

H.2.2 关键信息基础设施保护

关键信息基础设施保护评价指标见表H.7。

表 H.7 关键信息基础设施保护评价指标

指标名称	评价内容	评价方法
关键信息基础设施备案	关键信息基础设施按照行业主管部门要求开展认定备案。	统计市（区）关键信息基础设施认定备案的比率。
关键信息基础设施安全防护	a）关键信息基础设施落实等级保护制度，通过网络安全等级保护测评； b）关键信息基础设施同步运行密码保障体系，通过商用密码应用安全性评估； c）关键信息基础设施及重要信息系统采用边界防护、区域隔离、身份鉴别、访问控制以及数据容灾备份等安全防护措施。	a）统计市（区）关键信息基础设施通过等级保护测评的比率； b）统计市（区）关键信息基础设施通过商用密码应用安全性评估的比率； c）统计市（区）落实关键信息基础设施落实边界防护、区域隔离、身份鉴别、访问控制以及数据容灾备份等措施比率。
关键信息基础设施安全检查	关键信息基础设施安全检查开展情况。	统计市（区）关键信息基础设施安全检查开展的比率。

H.2.3 数据安全保护

数据安全保护评价指标见表H.8。

表 H.8 数据安全保护评价指标

指标名称	评价内容	评价方法
数据分类分级	a）制定数据分类分级标准规范、重要数据目录，形成数据交互、融合和共享安全策略、范围及要求等； b）按要求开展数据资源普查，定期开展自查核查，及时完成历史数据清理与补登记工作。	a）调研市（区）是否制定了数据分类分级指引，是否建立了重要数据具体目录、是否建立了国家核心数据具体目录，是否明数据交互、融合和共享安全策略、范围及要求； b）检查市（区）单位是否已建立并能及时维护智慧城市数据资产底账，核实数据资产分责确权登记及价值评估工作的覆盖率和完成率。检查上报数据资产目录、重要数据目录、核心数据目录的准确性。
数据安全技术防护落实	a）采取相应的技术措施对重要数据安全进行保护； b）对重要数据所采取安全保护措施的有效性进行自我监管。	a）统计市（区）重要数据中采取加密、数据脱敏、数据防泄漏、数字水印、数据审计、数据访问控制等技术手段防护的比率； b）统计市（区）重要数据中采取分区管控、访问许可管理、内部流动监管、互联网泄漏监控和数据溯源分析等技术手段部署和监管活动开展比率。
数据安全管理制度建设	a）建立全流程数据安全管理制度； b）落实重要数据开发共享安全监督管理，保护数据的隐私； c）形成重要数据的出境安全管理制度。	a）统计市（区）单位中建立全流程数据安全管理制度的比率；市（区）落实数据处理人员安全责任的比率； b）统计市（区）单位中建立重要数据开发共享管理机制的比率；调研市（区）是否开展数据泄露、售卖活动的监测； c）统计市（区）单位中落实重要数据出境安全管理制度的比率。
数据安全风险评估	定期开展数据安全风险评估。	统计市（区）单位中定期开展数据安全风险评估的比率。

H.2.4 个人信息保护

个人信息保护评价指标见表H.9。

表 H.9 个人信息保护评价指标

指标名称	评价内容	评价方法
个人信息采集合规情况	按照GB/T 35273-2020要求，按照“权责一致原则、目的明确原则、选择同意原则、最少够用原则、公开透明原则、确保安全原则、主体参与”原则加强个人信息的保护，禁止非授权访问和非法使用个人信息。	统计市（区）符合“不超出履行法定职责所必需的范围和限度，严格依照法律、行政法规规定的权限、程序处理个人信息”的单位覆盖率；统计市（区）符合“履行法定职责处理个人信息时向个人告知并取得其同意”的单位覆盖率；统计市（区）符合“处理的个人信息在中华人民共和国境内存储；确需向境外提供的，先进行风险评估”的单位覆盖率；统计市（区）建立个人信息去标识化处理机制的单位覆盖率；统计市（区）建立个人信息公开披露机制的单位覆盖率。
个人信息保护责任落实	成立个人信息保护的责任部门与负责人。	统计市（区）单位中设置个人信息保护的责任部门与人员的比率。
个人信息技术防护措施	a）形成个人信息安全共享传输安全保障机制； b）形成个人信息安全存储安全保障机制。	a）统计市（区）共享传输个人信息时链路采取安全措施的比率； b）统计市（区）储存个人信息时采取安全措施的比率。
个人信息安全评估	每年定期开展个人信息安全影响评估检查工作，形成评估检查报告并记录完整。	统计市（区）单位中定期开展个人信息安全影响评估的比率。

H.2.5 密码应用

密码应用评价指标见表H.10。

表 H.10 密码应用评价指标

指标名称	评价内容	评价方法
密码技术、产品和服务合规	信息系统所采用的密码技术、产品和服务符合国家密码管理部门的相关要求。	调研市（区）信息系统是否统一建设了基于国密算法的密码基础设施。
新建信息系统密码应用	新建信息系统规划、建设和运行时，同步进行信息系统密码保障系统的规划、建设和运行。	统计市（区）单位中新建信息系统通过密码应用安全性评估的比率。
存量信息系统密码应用	存量信息系统需开展密码应用安全改造。	统计市（区）单位中存量信息系统通过密码应用安全性评估的比率。
密评定期开展情况	定期开展密码应用安全性评估，向安全主管部门提交通过测评的商用密码应用安全性评估报告。	统计市（区）单位中按要求定期开展密码应用安全性评估的信息系统的比率。

H.2.6 信创及供应链安全管理

信创及供应链安全管理评价指标见表H.11。

表 H.11 信创及供应链安全管理评价指标

指标名称	评价内容	评价方法
信息技术应用创新	优先选用国产化安全可信的产品。	统计市（区）国产化安全可信设备应用比率。
供应链风险评估	定期开展供应链风险评估。	统计市（区）单位中开展供应链风险评估的比率。
建立供应链图谱	梳理信息技术产品和服务供应链图谱。	统计市（区）单位中建立信息技术产品和服务供应链图谱的比率。
采购产品及服务安全管理	采购的产品及服务符合国家相关安全规定。	统计市（区）采购产品符合国家相关安全规定的产品占总产品的比率。

H.3 网络安全保障能力

H.3.1 资产管理

资产管理评价指标见表H.12。

表 H.12 资产管理评价指标

指标名称	评价内容	评价方法
硬件资产清单	硬件资产清单的准确性、完整性。	统计市（区）硬件资产设备类型、运行状态、物理分布内容准确、完整的单位覆盖率，明确硬件资产责任人的单位覆盖率。
信息系统清单	信息系统清单内容的准确性、完整性。	统计市（区）系统清单内容准确、完整的单位覆盖率，明确信息系统资产责任人的单位覆盖率，及时更新网络拓扑及IP清单表的单位覆盖率。
服务端口清单	信息系统服务端口清单的准确性。	统计市（区）建立信息系统服务端口及接口清单的单位覆盖率。
信息系统资源和运行集中管理	可对信息系统的资源和运行进行集中配置、控制和管理。	调研市（区）是否对信息系统的资源和运行进行集中配置、控制和管理。

H.3.2 安全运维

安全运维评价指标见表H.13。

表 H.13 安全运维评价指标

指标名称	评价内容	评价方法
系统日常运维开展	系统日常运维开展情况。	统计市（区）指定专人负责系统日常巡检工作的部门覆盖率、市（区）指定专人负责系统权限管理工作的单位覆盖率、市（区）指定专人负责系统变更管理工作的单位覆盖率、市（区）开展安全设备维保、规则库定期升级、安全策略定期更新等工作的单位覆盖率。
安全管理中心建设	a）市（区）网络安全管理中心建设情况。 b）市（区）网络安全管理中心与省平台级联对接情况。	a）调研市（区）是否使用网络安全管理中心。 b）调研市（区）网络安全管理中心是否与省平台级联对接。
日志集中管理	调研市（区）网络安全管理中心是否与省平台级联对接。	统计市（区）开展全流量威胁监测分析的单位覆盖率。

H.3.3 安全监测

安全监测评价指标见表H.14。

表 H.14 安全监测评价指标

指标名称	评价内容	评价方法
流量威胁监测	全流量威胁监测分析开展情况。	统计市（区）开展全流量威胁监测分析的单位覆盖率。
异常行为监测	异常行为监测开展情况。	统计市（区）开展异常行为监测的单位覆盖率。
失陷监测	失陷监测开展情况。	统计市（区）开展失陷监测的单位覆盖率。
威胁情报分析	威胁情报分析开展情况。	统计市（区）开展威胁情报分析的单位覆盖率。
欺骗防御	欺骗防御开展情况。	统计市（区）部署欺骗性防御技术的单位覆盖率。
网站防篡改	网站防篡改开展情况。	统计市（区）开展网站防篡改监测的单位覆盖率。
数据安全风险监测	数据安全风险监测开展情况。	统计市（区）开展数据安全风险监测的单位覆盖率。
主机入侵检测	主机入侵检测开展情况。	统计市（区）开展主机入侵检测的单位覆盖率。
办公终端安全监测	办公终端安全监测开展情况。	统计市（区）开展办公终端安全巡检的单位覆盖率。

H.3.4 应急处理

安全应急评价指标见表H.15。

表 H.15 安全应急评价指标

指标名称	评价内容	评价方法
应急机制建立	a）网络安全应急预案制定情况； b）开展网络安全应急预案培训情况； c）开展应急演练情况。	a）统计市（区）制定网络安全应急预案的单位覆盖率； b）统计市（区）定期开展应急预案培训的单位覆盖率； c）统计市（区）定期开展应急演练的单位覆盖率。
应急事件处置	a）网络安全应急事件处置情况。 b）安全事件溯源取证情况。	a）统计市（区）网络安全应急事件及时处置、报告的比率。 b）统计市（区）安全事件溯源取证的比率。

H.3.5 安全检查

安全检查评价指标见表H.16。

表 H.16 安全检查评价指标

指标名称	评价内容	评价方法
安全风险评估	全面风险评估开展情况。	统计市（区）开展网络安全全面风险评估的单位覆盖率。
安全基线核查	安全基线核查执行情况。	统计市（区）定期执行网络安全基线核查的单位覆盖率。
漏洞扫描	漏洞扫描开展情况。	统计市（区）定期开展网络安全漏洞扫描的单位覆盖率。
渗透测试	渗透测试开展情况。	统计市（区）定期开展网络安全渗透测试的单位覆盖率。
代码审计	系统代码审计开展情况。	统计市（区）按要求开展代码审计的单位覆盖率。
安全漏洞隐患整改	安全漏洞隐患整改情况。	统计市（区）及时处置网络安全风险隐患的单位覆盖率。
开源软件安全检测	开展应用系统开源组件安全检测情况。	统计市（区）开展应用系统开源组件安全检测的单位覆盖率。

H.3.6 安全审计

安全审计评价指标见表H.17。

表 H.17 安全审计评价指标

指标名称	评价内容	评价方法
安全审计制度制定及执行	安全审计制度及审计计划的制定及执行情况。	统计市（区）建立安全审计机制的单位覆盖率。
安全审计人员配备	安全审计人员配备情况。	统计市（区）配备专职安全审计人员或采购审计服务的单位覆盖率。
安全策略及制度执行审查	安全策略及安全制度执行审查开展情况。	统计市（区）定期开展安全策略和安全制度执行情况审查的单位覆盖率。
日志审计	日志审计开展情况。	统计市（区）定期对日志进行审计分析的单位覆盖率，市（区）定期对运维管理人员日常操作进行跟踪、分析和监督检查的单位覆盖率。

H.3.7 业务连续性保障

业务连续性保障评价指标见表H.18。

表 H.18 业务连续性保障评价指标

指标名称	评价内容	评价方法
数据备份及恢复	数据备份及恢复测试情况。	统计市（区）根据数据、系统重要性制定并执行备份策略的单位覆盖率，市（区）定期开展备份数据有效性测试的单位覆盖率。
业务影响分析	业务影响分析开展情况。	统计市（区）定期开展信息系统业务影响分析的单位覆盖率。
灾难恢复	a）灾难恢复培训开展情况； b）灾难恢复测试开展情况。	a）统计市（区）定期开展灾难恢复培训的单位覆盖率； b）统计市（区）定期开展灾难恢复测试的单位覆盖率。

H.3.8 服务支撑

服务支撑评价指标见表H.19。

表 H.19 服务支撑评价指标

指标名称	评价内容	评价方法
安全服务提供商/安全服务资源池的完善程度	网络安全咨询、设计、集成、运维、测试、风险评估（含等保、密评等）、应急处置、攻防演练等安全服务提供商/安全服务资源池的完善程度。	统计市（区）建立网络安全咨询服务能力的单位覆盖率、市（区）建立网络安全设计服务能力的单位覆盖率、市（区）建立网络安全集成服务能力的单位覆盖率、市（区）建立网络安全运维服务能力的单位覆盖率、市（区）建立网络安全测评服务能力的单位覆盖率、市（区）建立网络安全风险评估服务能力的单位覆盖率、市（区）建立网络安全攻防演练服务能力的单位覆盖率。
安全服务提供商资质情况	安全服务商具备国家主管部门及权威机构颁发的信息安全服务相关服务资质。如：安全开发类服务资质、应急处理服务资质、安全集成服务资质、安全运维服务资质等。	依据项目供应商资质要求，统计市（区）供应商符合资质要求的比率。
安全服务商安全评价机制建立执行	安全服务商的安全评价机制建立及执行情况。	统计市（区）建立安全服务商安全评价机制的单位覆盖率。
产业协同、合作情况	网络安全产业协同、合作情况。	统计市（区）数字政府网络安全协会组织、培训教育基地、产业基地、合作项目等形式的产学研用合作的情况。
新技术新应用安全防护	a）移动互联终端及应用加强设备安全、访问控制、接入认证、入侵防范等技术安全措施。 b）物联网设备落实设备安全、安全接入认证、入侵防范等技术安全措施。 c）云计算服务安全符合相应级别等级保护的相关要求，并通过国家云计算服务安全评估。	a）统计市（区）移动互联终端采用安全接入认证、通信加密、权限控制、安全审计等技术措施的比率。 b）统计市（区）物联网设备落实设备安全、安全接入认证、入侵防范等技术安全措施的比率。 c）统计市（区）云计算平台通过安全评估的比率。

H.4 网络安全监管

H.4.1 网络环境安全

网络环境安全评价指标见表H.20。

表 H.20 网络环境安全评价指标

指标名称	评价内容	评价方法
桌面终端安全	a）桌面终端被非法控制情况； b）桌面终端中木马、病毒情况。	a）统计市（区）桌面终端被非法控制的数量占比； b）统计市（区）桌面终端中木马、病毒的数量占比。
移动终端安全	a）移动终端被非法控制情况； b）移动终端中木马、病毒情况。	a）统计市（区）移动终端被非法控制的数量占比； b）统计市（区）移动终端中木马、病毒的数量占比。
办公场所安全	办公场所无线AP弱口令、被挟持情况。	统计市（区）办公场所无线AP弱口令、被挟持的数量占比。
虚拟专用网（VPN）安全	虚拟专用网（VPN）安全情况。	统计市（区）使用虚拟专用网（VPN）的数量占比。
信息系统互联网安全	信息系统互联网高危端口暴露情况。	统计市（区）信息系统互联网高危端口暴露比率。

H.4.2 安全漏洞

安全漏洞评价指标见表H.21。

表 H.21 安全漏洞评价指标

指标名称	评价内容	评价方法
中危安全漏洞管理	a）中危及以上安全漏洞情况。 b）中危及以上漏洞数与市（区）系统总数比例。	a）统计市（区）信息系统中危及以上漏洞数量、市（区）信息系统中危及以上漏洞及时修复率。 b）统计市（区）信息系统中危及以上漏洞数与市（区）系统总数比率。

H.4.3 安全事件

安全事件评价指标见表H.22。

表 H.22 安全事件评价指标

指标名称	评价内容	评价方法
特别重大网络安全事件	特别重大网络安全事件发生情况。	统计市（区）发生特别重大安全事件的次数与市（区）系统总数的比率。
重大网络安全事件	重大网络安全事件发生情况。	统计市（区）发生重大安全事件的次数与市（区）系统总数的比率。
较大网络安全事件	较大网络安全事件发生情况。	统计市（区）发生较大安全事件的次数与市（区）系统总数的比率。
一般网络安全事件	一般网络安全事件发生情况。	统计市（区）发生一般安全事件的次数与市（区）系统总数的比率。

H.4.4 安全保密

安全保密评价指标见表H.23。

表 H.23 安全保密评价指标

指标名称	评价内容	评价方法
网络安全泄密事件	发生网络安全泄密事件，并造成较为恶劣的社会影响。	当发生网络安全泄密事件，并造成较为恶劣的社会影响的，评价得分总分为0。

H.4.5 专项工作

专项工作评价指标见表H.24。

表 H.24 专项工作评价指标

指标名称	评价内容	评价方法
攻防演练	实战攻防演练中的情况。	统计市（区）在网络安全攻防演练中的得失分情况。
安全检查	省级安全检查中的情况。	调研市（区）重要业务系统的是否可用。
网络安全荣誉、奖励	获得国、省级网络安全竞赛、能力认证、试点示范工程等奖励、荣誉情况。	调研市（区）是否获得国、省级网络安全竞赛、能力认证、试点示范工程等奖励、荣誉。
网络安全监督检查工作成效	履行网络安全监督检查职能的工作成效。	调研市（区）是否履行网络安全监督检查职能。

H.4.6 安全协同

安全协同评价指标见表H.25。

表 H.25 安全协同评价指标

指标名称	评价内容	评价方法
单位之间沟通合作情况	与网信、公安等监管机构之间的沟通合作情况。	调研市（区）大数据管理部门与网信、公安等监管机构之间是否形成良好合作与沟通。
网络安全重大事项上报情况	按照要求及时向网信部门报告网络安全重大事项的情况。	调研市（区）大数据、智慧城市管理部门是否按照要求及时向网信部门报告网络安全重大事项。
重大活动网络安全保障情况	按照要求开展重大活动网络安全保障情况。	调研市（区）大数据、智慧城市管理部门是否按照要求开展重大活动网络安全保障。
与数据管理部门的安全工作配合情况	与上级大数据管理部门安全管理工作的配合程度。	调研市（区）大数据管理部门是否积极、主动配合省级大数据管理部门的安全管理工作。
安全事件上报情况	向上级大数据管理部门报告安全事件是否及时、全面。	调研市（区）大数据管理部门是否及时、全面向省级大数据管理部门报告安全事件。
安全监测数据上报情况	向上级大数据管理部门上报安全监测数据是否及时、准确。	调研市（区）大数据管理部门是否及时、准确向省级大数据管理部门报告安全监测数据。
安全监测平台建设情况	建立安全监测平台，支撑形成网络安全上报、通报预警机制，并纳入网络与信息安全信息通报机制。	统计市（区）安全监测平台对部门监测比率，调研市（区）是否形成信息通报预警机制。
网络安全研判情况	加强和规范本地网络安全信息汇集、分析、研判工作。	统计市（区）单位中对汇集的网络信息开展安全研判的比率。
网络安全自查评估情况	每年至少进行一次网络安全自查评估，该项工作与网信、公安、保密、密码、大数据、工信等部门的检查进行有效衔接。	统计市（区）每年开展网络安全自查评估的单位覆盖率。

参 考 文 献

[1] GB/T 20985.1—2017 信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理
[2] GB/T 25056—2018 信息安全技术 证书认证系统密码及其相关安全技术规范
[3] GB/T 25069 信息安全技术 术语
[4] 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
[5] GB/T 32915—2016 信息安全技术 二元序列随机性检测方法
[6] GB/T 34678—2017 智慧城市 技术参考模型
[7] GB/T 37043 智慧城市 术语
[8] GB/T 37092—2018 信息安全技术 密码模块安全要求
[9] GB/T 37971—2019 信息安全技术 智慧城市安全体系框架
[10] GB/Z 38649—2020 信息安全技术 智慧城市建设信息安全保障指南
[11] GM/T 0094—2020 公钥密码应用技术体系框架规范
[12] 《中华人民共和国网络安全法》
[13] 《中华人民共和国密码法》
[14] 《中华人民共和国数据安全法》
[15] 《中华人民共和国个人信息保护法》
[16] 《关键信息基础设施安全保护条例》
[17] 《网络安全等级保护条例》
[18] 《数字山东发展规划（2018-2022年）》
[19] 《山东省“十四五”数字强省建设规划》
[20] 《山东省人民政府办公厅关于加快推进新型智慧城市建设的指导意见》
[21] 《关于加强智慧城市网络安全管理工作的若干意见》
[22] 《关于促进山东省网络安全产业发展的指导意见》
[23] 《党委（党组）网络安全工作责任制实施办法》