ICS 33.040.50
CCS L 78

# 团　　体　　标　　准

T/BYIDA 001—2025

# 白云区城中村网络通信管线整治与社区数字基础设施管理规范

Standardization of network communication pipeline rectification and community digital infrastructure management for urban villages in Baiyun District

（发布稿）

2025 -09 - 29 发布　　2025 - 10 - 01 实施

广州市白云区数智化发展协会　　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这些专利的责任。

本文件由中通服中睿科技有限公司、广东南方电信规划咨询设计院有限公司、国科华盾（广州）信息科技有限公司、北京电信规划设计院有限公司、广州市西迈信息科技有限公司提出。

本文件由广州市白云区数智化发展协会归口。

本文件起草单位：中通服中睿科技有限公司、广东南方电信规划咨询设计院有限公司、国科华盾（广州）信息科技有限公司、北京电信规划设计院有限公司、广州市西迈信息科技有限公司、公诚管理咨询有限公司、广州市汇源通信建设监理有限公司、广州元沣智能科技有限公司、山东正中信息技术股份有限公司广东分公司、海格怡创(广州)信息科技服务有限公司、广州仁信网络科技有限公司、广州天域通信设备有限公司、广州广玉电子科技有限公司、广州嘉通通讯科技有限公司、广州市凯兆通信设备工程有限公司、广州仁信网络科技有限公司、广州市景天通信技术有限公司、广州昊迅通信科技有限公司、广东国咨招标有限公司、广州市嘉红通信技术有限公司、广州市松鑫电子产品有限公司、广州金敏云科技有限公司、中城（广州）工程科技有限公司、广州云果信息科技有限公司、广东晟标建设咨询有限公司、广州全民通信科技有限公司、广州恒煜科技有限公司、中国铁塔股份有限公司广州市分公司、广州星速网络科技有限公司、广州云继科技有限公司、佛山市中汇达建设工程咨询有限公司、广州激战软件开发有限公司、广州高洋软件开发有限责任公司、广州航睿网络通讯技术有限公司、广州鑫昇网络通讯技术有限公司。

本文件主要起草人：郑礼峰,李尊,刘伟,朱玉春,杨三,张远航,胡智霖,杨炽培,周阳,叶楚滨,杨戈,宋攀,肖宇尘,何甜甜,石欣欣,杜呈旭,赵婷,陈伟杰,李烙荣,陈小东,黄环辉,廖兵森,符阳海,丁佳琪,唐艺龙,丘钰霞,邓伟旋,黎国灿,陈玉彬,苏应巨,梁永志,刘志伟,邓广煊,肖树耀,宋远金,范殿锋,钟惠娟,魏辉,蔡振宇,赵桂锋,董必民,骆掌民,罗伊莉,梁永同,张斌,陈世平,何晋生,袁国华,杨健,王佑彰。

本文件是首次发布。

# 引　言

为充分解决白云区城中村通信管线的问题，规范白云区城中村“三线”整治及及社区数字基础设施建设，提升公共安全与数字化治理水平，目的是为“三线”整治工作有序发展提供参考和指引，特制定本文件。电力线的整治由南方电网另行规范，本文件仅对通信及广播电视管线提出技术要求。

# 白云区城中村网络通信管线整治与社区数字基础设施管理规范

## 1 范围

本文件规定了白云区城中村通信管线整治与智慧化管理的技术要求、数字化设计、通信网络整治、数据中心与云计算、系统集成、智慧化应用、运维管理及安全与隐私保护的要求。

本文件适用于白云区及广州市其他区域的城中村通信管线整治及社区数字基础设施建设、运行和管理。

## 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。

YD/T 5211—2014 通信工程设计文件编制规定

YD/T 5178—2017 通信管道人孔和手孔图集

GB 50374—2018 通信管道工程施工及验收规范

DB4401/T 11—2018 广州市缆线管廊工程技术指引

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

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 50325—2020 民用建筑工程室内环境污染控制规范

GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

GB 50847—2021 住宅区和住宅建筑内光纤到户通信设施工程设计规范

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

YD 5102—2022 通信线路工程设计规范

GB/T 35273—2023 信息安全技术 个人信息安全规范

YD/T 5138—2019 本地通信线路工程设计规范

YD/T 5139—2019 本地通信线路工程验收规范

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

GB/T 40692 政务信息系统定义和范围

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**城中村** urban villages

位于城市建成区内，仍保留农村集体土地所有制性质、管理体制和部分原有建筑形态的聚居区域。

3.2

**网络通信管线** network communication pipeline

用于承载通信光缆、同轴电缆及相关设备的物理通道，包括架空管线（沿建筑物或杆路架设）、地下管线（埋设或管廊敷设）和室内布线（建筑内部线路）。

3.3

**三线整治** communication network reconstruction

对城中村内电力线、通信线、广播电视线（“三线”）的交叉缠绕、违规架设等问题进行规范梳理、归、下地或入盒的技术改造。

3.4

**城中村管理规范** management specification for urban-village

对城中村既有通信、广播电视线等进行全面排查、建档立册，并按用途、权属分类归整；具备条件的区域统一下地、入盒或钢绞线敷设，消除空中“蜘蛛网”，同步预留扩容与维护空间，确保线路安全、有序且不干扰居民生活的全过程技术与管理要求。

3.5

**智慧化管理平台** intelligent management platform

集成GIS地图、管线数据、设备状态监控、故障报警等功能的数字化系统，支持对通信管线资源的全生命周期管理数字化系统。

3.6

**网络秩序哨点** network-order sentry point

指部署在城中村通信网络关键节点，具备实时流量监测、异常行为识别、安全预警与联动处置功能的硬件-软件一体化设施；用于发现非法组网、违规流量、DDoS 攻击、黑宽带等网络乱象，形成“发现-告警-处置”闭环，维护社区网络秩序与安全。

## 4 总体原则

a)应统筹规划管线布局，避免重复建设，并确保强弱电分离。
b)应消除私拉乱接、消防隐患，保障线路运行安全。
c)应消除私架设网络交换机设备，进行流量分发、网络共享等组网体系。
d)应预留冗余资源，支持未来5G/6G、物联网等技术扩展。
e)应建立运营中心，保持统一运维和常态化巡查。

## 5 通信网络整治

### 5.1 整体要求

按照“进村入管道”“上墙入套盒”“强弱电分离”“走向横平竖直”和“楼房之间不随意横跨”的原则，采用“下地入管道”“上墙入套盒”标准，通过分类捆扎、分类穿管、分层架设等方式实施实施信号平移、旧线清理等整治工作，实现光纤到户覆盖率100%。其中各类通信电力架空管线具备入地条件的应入地，暂不具备入地条件的要采取“捆绑、贴墙”等方式进行规范整治。

### 5.2 技术要求

a)架空线路应用钢绞线或桥架敷设，高度统一为2.5m～4.5m，与电力线垂直间距≥1.5m，墙壁光（电）缆离地面高度≥3m。

b)地下管线应埋深≥0.8m，管道路径符合DB4401/T 11-2018的规定。

c)标签规范应用“红底黑字（电信）”“白底黑字（移动）”“黄底黑字（联通）”“浅紫底黑字（长城宽带）”“浅绿底黑字（监控线路）”标识。

### 5.3 走线要求

#### 5.3.1 楼宇外墙走线

线缆应沿墙体水平或垂直敷设，弯曲半径不小于线缆外径的10倍。固定间距为2 m±0.2 m，跨越楼宇的布线通过桥架或地下管道实现。严禁跨楼宇空中飞线。

#### 5.3.2 宽带箱盘线

宽带箱盘线及箱体数量，一楼栋箱体 1～2 个，箱体外多余线缆应盘好，并采用扎带固定好。箱体采用三网合一分纤箱，可共用。

### 5.4 标签标注

线缆标签应包含账号、安装位置等信息，标签需使用标签机打印，内容完整清晰，粘贴位置准确、美观。

### 5.5 光缆整治

光缆采用管道或直埋敷设时，管道或直埋光缆要做好聚乙烯塑料管以及硅芯管保护；墙壁敷设时，墙壁光缆建议要做好金属槽道保护；进行架空敷设时，架空光缆要做好每个杆子的防水弯及预留长度保护，与强电交越时要做好防护处理。

### 5.6 光交箱整治

#### 5.6.1 箱体状态

箱门锁具完好，外观整洁无污损，箱内无垃圾杂物。

#### 5.6.2 跳线布放

光纤跳线走线统一、整齐，严禁交叉、牵拉、挤压或扭绞；跳纤需盘绕固定，绑扎规范，避免受力。

#### 5.6.3 跳纤长度

跳纤长度宜为1m，最长不超过1.5m，禁止冗余堆积。

#### 5.6.4 走线规则

严格按路由横平竖直布放，全部纳入走线环；多余跳纤需绕至合适长度，松紧适度，确保整齐美观。

### 5.7 用户线整治

楼内用户线走线应横平竖直，并用塑料槽板进行固定和保护，做到线缆即美观又安全。

## 6 数字化设计

### 6.1 设计要求

a)对城中村内信息化终端（需要网络的物联设备:包括门禁、视频监控、停车管理、环境监测等）进行标准化接口设计，支持TCP/IP、HTTP/HTTPS、MQTT等通用协议，实现数据互联互通。

b)应建立全息感知体系，涵盖环境参数（温湿度、空气质量）、人流密度、设备状态等实时数据采集，数据上传频率不低于1次/min。

c)应用边缘计算技术，对高时效性数据进行本地预处理，关键数据需同步至云端平台存储。

d)应建立数据中心，实现多源异构数据的清洗、融合与标准化存储，支持API接口对外提供数据服务。

### 6.2 网络架构设计

#### 6.2.1 实名制管理

a)接入网络的用户及设备应通过实名认证，且安装至标准地址对应的真实套间内，采用“身份证+人脸识别”双因子验证，并绑定至统一身份管理平台。

b)网络设备（如路由器、交换机）需注册至智慧化平台，MAC地址与物理位置信息关联，实现精准溯源。

#### 6.2.2 网络秩序哨点建设

a)在关键节点部署流量监测设备，实时分析网络行为，识别异常流量（如DDoS攻击、非法爬虫），并自动触发告警。

b)建立分级管控机制，对高风险区域实施动态访问控制，支持黑白名单策略与IP封禁功能。

#### 6.2.3 架构分层设计

a)采用“接入层-汇聚层-核心层”三层架构，接入层支持千兆光纤到户，汇聚层部署冗余链路，核心层具备负载均衡与灾备切换能力。

b)无线网络覆盖应确保信号强度≥-65dBm，丢包率≤0.1%。

## 7 数据中心和云计算

### 7.1 总体要求

数据中心和云计算基础设施应具备弹性可扩展性，保障系统运行的稳定性和响应速度，防止平台受到外部攻击，保障系统的安全性和可靠性。

### 7.2 平台服务器

#### 7.2.1 系统服务器

a)计算性能要求：配置双处理器，主频≥2.2GHz，单颗 CPU 物理核数≥32 核，缓存≥64MB，支持超线程技术，确保每个处理器内核可并发运行多个线程，以最大限度提高多线程应用和并行处理能力。

b)内存配置要求：支持≥32 根 3200MT/s DDR4 ECC 规格内存，为系统提供更大内存带宽和容量，保障内存密集型应用高效运行。

c)存储要求：支持全 SSD 配置，需配置 480GB 6G SSD 硬盘≥2 块，1.92TB NVMe SSD 硬盘≥2 块，8TB SATA 硬盘≥10 块；支持掉电数据保护功能，缓存≥2GB。

d)网络功能要求：支持 VXLan 特性，降低网络负荷、简化配置部署，针对云计算应用场景下的安全需求提供优秀解决方案；支持 SR-IOV 特性，通过虚拟化技术，为业务提供独享网络设备，简化管理、保障业务安全并增强体验感。

#### 7.2.2 运算服务器

企业级高性能双路 GPU 服务器。

a)计算性能要求：支持双处理器，物理核心总数不少于 64 个，主频≥2.5GHz，提供强大的并行计算能力，满足复杂运算任务需求。

b)内存配置要求：具备高内存带宽设计，内存插槽数≥32 个，支持 DDR4 RDIMM 内存，内存运行频率≥3200MHz，内存容量≥1TB，保障内存密集型应用高效运行。

c)存储要求：支持 RAID 配置，具备高级内存容错功能，支持在线恢复 RAID 阵列，保障硬盘故障时数据安全。存储容量≥10TB，读写速度≥1000MB/s。

d)网络性能要求：适配 10G、25G、100G 等多种网络环境，最大支持 8 个单宽半高半长 GPU 应用，满足高速数据传输与多 GPU 协同运算需求。

e)冷却与散热要求：采用高效散热设计，确保在高负载运行时，关键部件温度≤60℃，保障服务器稳定运行。

f)远程管理与维护要求：支持远程操作、维护功能，配备故障指示系统，可实时监测并预警故障，提升维护效率，平均修复时间（MTTR）≤1h。

g)扩展性：具备强大的 I/O 扩展能力，可纳入云平台，调入大模型，以适应数据中心不同应用工作负载。

h)性能优化要求：针对运算密集型任务进行优化，确保在大数据处理、科学计算、人工智能训练等场景下，运算效率提升≥30%。

i)总拥有成本（TCO）优化：通过节能设计、高效散热及优化的硬件配置，在保证性能的前提下，

降低能耗及运维成本，使 TCO 在同级别服务器中降低≥20%。

### 7.3 主机安全

#### 7.3.1 总体要求

主机安全防护软件需纳入现网集群，实现集群管理的无缝对接。

#### 7.3.2 功能要求

a)云主机安全防护要求：支持无代理模式，满足云主机在病毒防护、访问控制、入侵检测、入侵防护、虚拟补丁等方面的安全需求。

b)运维管理要求：满足用户对云主机运维的需求，包括完整性监控、日志审计、资产管理、漏洞风险管理、检测与响应、基线检查、主机资源监控等功能。

c)虚拟化环境防护要求：支持虚拟主机和虚拟系统的全面防护，助力用户满足信息系统等保合规性的审计要求，构建虚拟化平台基础架构的多层次防护体系。

d)操作系统兼容性要求：支持主流操作系统虚拟机的无代理底层防病毒能力，包括但不限于 CentOS、SUSE、Ubuntu、统信、银河麒麟等。

e)网络数据包检测要求：支持无代理底层网络数据包检测，能够同时保护虚拟机操作系统及服务应用（如数据库、Web、DHCP 等），提供虚拟补丁功能，在已知漏洞修复前防范漏洞攻击，屏蔽漏洞以防止入侵。

f)宿主机安全防护要求：提供宿主机安全防护功能，支持宿主机和虚拟机通过同一网络和同一平台进行安全防护，确保业务网和管理网隔离，及时识别并有效阻断对宿主机和虚拟机发起的入侵攻击和病毒破坏行为。

## 8 系统集成

### 8.1 总体框架

智慧社区平台基础设施是通过整合图纸数据、社区物联设备、社区数据、云资源、网络资源等，保障平台稳定运行与数据安全。实行统一云管，提供全方位的云资源供给、统一门户，统一运维和运营管理能力，具备一体化管控、自动化运维、智能化分析及个性化扩展等功能。

### 8.2 核心功能

以“智慧大脑”应用层为核心，依托平台基础设施，综合数据层的工程数据和外部数据接口数据构建数仓。通过模型引擎与机器学习能力，深入分析数据，连接社区管理、电力消防、社区服务、网络安全、民生、环境等多个领域。利用公共应用服务和产业应用服务为社区管理提供智能支持，并通过可视化手段为管理团队提供直观展示。

### 8.3 覆盖范围

a)电力消防：具备管线布设再现、电力消耗分析、管线并行发热分析、消防隐患预警功能，为社区

消防安全提供数据支持与可视化展示。

b)社区管理：涵盖社区规划与建设、公共安全监控，提升管理效率和安全性，同时关注社会保障、就业与人才服务、智慧医疗健康，提高居民生活质量。

c)综合环境：通过环境监测、生态资源管理，保护和改善城市环境。

### 8.4 技术路线

依托数据中台进行数据采集、加工和分析，构建主体画像模型和供需匹配模型，实现资源优化配置。平台需具备实时数据处理、时空数据服务、数字孪生展示、AI 能力开发等功能，以支持智能化决策。系统框架图见图 1。


图 1 系统框架图

### 8.5 数仓建设

应实现数据整合、标准化处理与安全管理，为高效分析决策奠定基础。

#### 8.5.1 数据源管理

a)注册登记：支持录入不同系统或服务的数据接口信息。

b)授权管理：确保数据源按需分配给有权访问的用户或服务，实现数据接入的标准化与安全性控制。

#### 8.5.2 数仓模型设计

##### 8.5.2.1 物理模型设计

应明确业务需求及关键业务实体关系，将概念模型转化为逻辑模型，并创建物理模型，定义表结构及主外键。需检查物理模型的一致性，优化表结构、索引及分区策略，并在评审通过后创建数据库表结构。同时，要持续监控物理模型并进行优化。

#### 8.5.2.2 模型一致性校验

要求对逻辑模型与物理模型进行映射，并自动比对两者的结构，同时检测物理模型的字段属性定义，检查表间的关联性及外键约束。需智能识别不一致之处并生成详细报告，依据报告修正物理模型设计，优化其结构，最后再次校验，确保模型符合设计规范与业务需求。

#### 8.5.2.3 库表异常感知

应先配置监控范围及指标，实时监测库表结构变化，并对比物理库表结构信息。发现不一致时发送预警，通过一键同步功能快速调整物理模型，经审核后用变更并记录日志，同时持续监控以维持模型一致性。

### 8.5.3 数据字典

a)数据传输：支持大容量数据传输、断点续传、多线程传输。
b)数据标准化管理：定义和管理基础数据元素，确保数据一致性。

## 8.6 人工智能中台

a)数仓建设应融合人工智能中台其核心组件包括：高性能模型引擎：支持 AI 模型的快速训练与高效运行。
b)AI 能力开放平台：促进算法与业务场景的深度融合，简化定制化智能服务的开发过程。
c)时空数据服务体系：专注于处理时空维度信息，强化对动态及地理相关数据的智能分析与应用。

### 8.6.1 大模型训练

收集社区各类数据并预处理，选择合适模型进行训练和评估优化，以提高模型准确性和泛化能力。

### 8.6.2 数字孪生配置

进行实体建模，集成数据并融合，模拟测试场景，确保模型准确性。

### 8.6.3 预测预警模型

提取特征搭建预测模型，设计预警机制，根据反馈持续优化迭代，提升模型适应性和准确性。

### 8.6.4 智慧社区应用平台

应包括社区基础设施管理、电力设施管理、网络设施管理、消防设施管理、安防设施管理、社区组织与人员管理、居民防疫管理、社区医疗管理、智慧社交平台和社区数据全景驾驶舱等功能模块，以实现社区的智能化管理和服务。

# 9 智慧化应用管理要求

### 9.1 总体要求

应符合国家 B 类机房要求。包含中心机房、UPS 和精密空调机房、消防间、操作间等。

### 9.2 功能要求

应满足实时监控管线状态及监测设备运行数据，支持 GIS 地图标注故障点，自动派单维修。实现公安、政务视频资源互联互通，实现多部门协同。

### 9.3 安全要求

应符合网络安全等级保护三级标准（GB/T 22239—2019），保证数据加密传输，关键信息基础设施冗余设计。

### 9.4 中心机房功能要求

#### 9.4.1 供电系统要求

a)电压变动范围 220V—5%～220V+5%
b) 频率变化范围 50HZ±0.2
c) 波形失真率≤±5%

#### 9.4.2 环境系统要求

a)温度 22℃±2℃，温度变化率：＜5℃/H 不结露；
b) 湿度 45%～65%，含尘量≤10000 粒/$dm^3$；噪音：≤65dB（A）；
c) 照度≥500LX；应急照明≥50LX。

#### 9.4.3 消防系统要求

应采用七氟丙烷气体灭火，联动门禁及视频监控。

#### 9.4.4 监控系统要求

应满足涵盖供配电系统、UPS 系统、环境系统、消防系统、报警系统等中心机房相关的监控、数据采集及视频监控功能。基础的监控系统结构如图 2。


图 2 系统结构图

### 9.4.5 综合布线系统要求

#### 9.4.5.1 铜缆插座

电缆连接应符合 TIA/EIA568B 标准，电口数据信息点采用六类 RJ45 模块，信息插座输出口为模块式结构。

#### 9.4.5.2 跳线

电口数据应采用相应的非屏蔽六类 RJ45 系列厂家原装跳线，光口模块采用相应的单多模厂家原装跳线。

#### 9.4.5.2 线路延伸

应采用单多模光纤及 6 类非屏蔽双绞线进行线路延伸，双绞线最大传输距离为 100m，配线架至最

远端工作区端口的距离不超过 90m。

### 9.5 FTTH 系统要求

#### 9.5.1 光纤敷设要求

a)光纤连接线的型号、规格应符合设计要求，超出长度不应超过 1m。
b)布局要整齐，机架内和机架间的走线要分开走线。
c)静态曲率半径不应小于 30mm。

#### 9.5.2 ODF 框防雷接地要求

a)ODF 架外壳的设备保护地应采用 16mm$^2$ 以上的多股铜线连接至机房设备专用地排。
b)光缆的加强芯和金属屏蔽层的地线先接在 ODF 架内的专用防雷地排，再用 16mm$^2$ 以上的铜线多股线接在机房内的 ODF 专用地排。
c)ODF 专用地排和机房设备专用地排应分开，两者均应分别计入机房通用地网引出点。

## 10 运维管理

### 10.1 管理体系

运维服务管理体系的实体包括运维服务管理对象、运维活动角色及运维管理组织结构、运维服务管理流程、运维服务支撑系统和运维服务五个要素，见图 3。

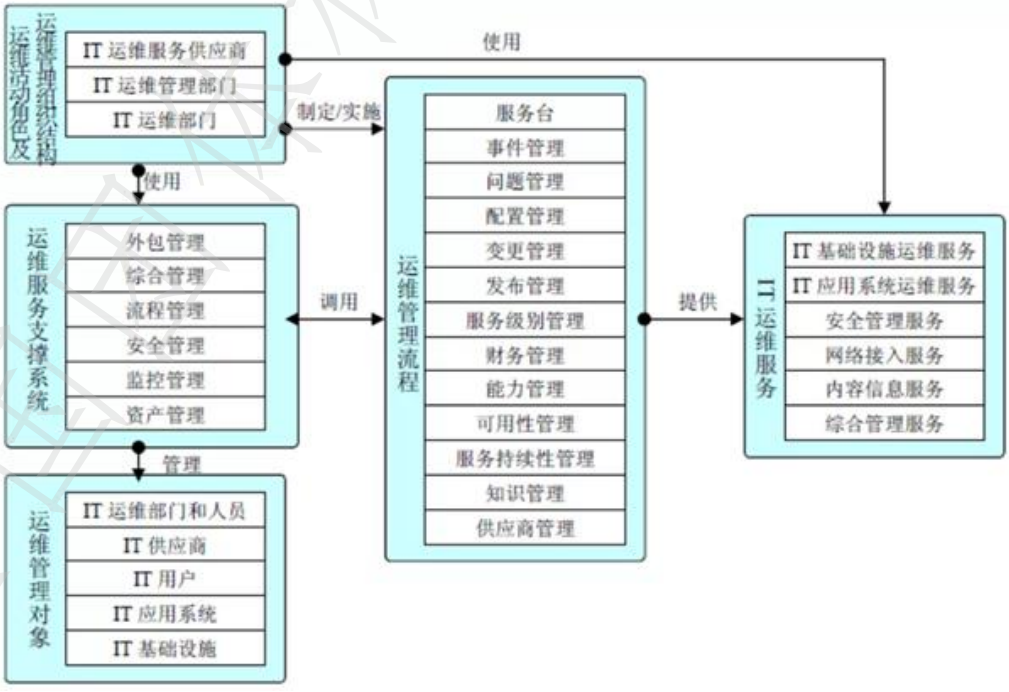


图 3 运维服务管理体系

### 10.2 服务标准

故障响应时间≤2h，修复时间≤24h。

### 10.3 巡查机制

每月定期巡查，重点区域每周一次，记录存档备查。

## 11 安全和隐私保护

### 11.1 网络安全设计

#### 11.1.1 系统可靠性设计

a)关键系统（如数据中心、核心交换机）需采用双机热备或集群部署，单点故障恢复时间≤5min。

b)网络设备及服务器冗余电源配置率需达到100%，UPS后备供电时长≥4h。

c)数据传输链路需支持自动切换，主备链路切换延迟≤30s。

#### 11.1.2 安全防护设计

a)防火墙策略应基于“最小权限原则”，仅开放必要端口，并定期进行漏洞扫描与策略审计。

b)网络边界部署入侵检测系统（IDS）与入侵防御系统（IPS），应符合GB/T 22239—2019 网络安全等级保护基本要求中第5章二级以上安全要求。

### 11.2 网络安全设施

#### 11.2.1 防火墙

a)高性能与吞吐量：防火墙应支持至少 10Gbps 以上的吞吐量，确保在高并发访问和大数据传输时网络性能不受影响。

b)深度包检测：具备深度包检测能力，能够有效识别并阻止网络协议中的恶意流量。

c)应用控制：支持基于应用层的精细控制策略，涵盖 HTTP、HTTPS、FTP、SMTP 等协议，确保仅授权应用服务可通过。

d)多 WAN 口负载均衡与故障切换：支持多线路接入，实现流量负载均衡及线路故障自动切换，保障网络连续性。

e)日志审计与报告：提供详尽的日志记录与报表功能，便于追踪分析网络行为及安全事件。

f)其他要求：支持远程操作与管理，符合相关行业标准和法规要求。

#### 11.2.2 防毒墙

a)实时威胁防护：集成最新病毒库，实现对病毒、木马等恶意软件的实时扫描与隔离，有效阻止其传播。

b)邮件安全：针对 SMTP、IMAP、POP3 协议进行邮件内容过滤，阻断携带病毒的邮件进入内网。

c)Web 内容过滤：对 HTTP、HTTPS 流量进行深度内容分析，防止用户访问恶意网站或下载危险文件。

d)文件沙箱技术：在未知文件执行前，先将其隔离运行，评估安全性后再决定是否放行，以应对新型未知威胁。

e)集成管理：支持集中管理功能，便于统一配置策略、同步更新病毒库以及实时监控全网安全状态。

#### 11.2.3 行为检测

a)全面行为监控：系统应能够监控并记录网络用户或系统的所有行为，监控范围包括但不限于网页访问、文件传输、即时通讯以及社交媒体活动等，确保所有网络活动均处于可审计状态。

b)异常行为识别：系统需具备异常行为识别功能，通过机器学习算法对用户或系统的行为模式进行分析。一旦识别出异常行为，系统应立即发出预警，以便及时采取措施。这些异常行为可能暗示存在潜在的安全威胁。

c)敏感内容过滤：系统应支持敏感内容过滤功能，允许设定关键词或模式匹配规则。对于包含敏感信息的邮件、聊天记录等通信内容，系统应能够进行拦截或发出警告，以有效防止敏感数据的泄露。

d)系统集成与管理：系统应具备良好的集成性，能够无缝对接现有的网络安全架构。同时，提供直观的管理界面，便于统一配置策略、更新规则及实时监控全网安全状态，降低管理复杂度，提升运维效率。

e)性能与可靠性：系统应具备高性能处理能力，确保在高并发网络环境下稳定运行，不影响正常业务开展。具备高可用性设计，支持冗余配置，保障系统无单点故障，确保 7×24h 不间断监控与防护。

#### 11.2.4 入侵检测

a)实时监测与响应：系统应具备实时监测网络流量、系统日志等数据的能力。一旦发现潜在入侵行为或安全威胁，能够立即触发预定义的响应措施，如阻断攻击源、通知管理员等，以确保快速反应并降低安全风险。

b)签名库更新：集成并持续更新最新的攻击签名库，确保能够及时发现并应对新的入侵行为或安全威胁，保持系统的安全性和有效性。

c)可视化监控与报警：提供直观的可视化界面，展示网络流量、攻击趋势等关键信息，并支持自定义报警规则，使管理员能够及时发现并处理潜在的安全威胁，提高安全管理效率。

d)与其他安全设备的联动：支持与防火墙、防毒墙等安全设备的联动，实现信息共享和协同工作，以构建更加全面、智能的网络安全防护体系，增强整体安全防护能力。

### 11.3 信息安全

#### 11.3.1 防护体系建设

a)基础设施层安全：通信基础设施应支持多种网络接入，实现 5G 信号覆盖，提高数据传输效率和安全性。

b)系统层安全：IoT 物联接入层应包含设备管理等功能，确保接入设备的安全性和可控性。数据服务与数据库符合相关要求，采取加密存储和传输技术，防止数据泄露。应用支撑层具备相应的安全规范，确保上层应用流程的安全性。

c)应用层安全：应包含社区人员、车辆、事物管理等功能的应用层，实施严格的访问控制和身份认证机制，对服务器、数据库等关键资源实施重点保护，限制访问权限。

d)安全技术应用：应使用防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等网络安全软件防

御黑客攻击，定期进行系统和网络的安全审计，检查潜在的安全漏洞和风险。

#### 11.3.2 社区网络流量和异常行为监测

a)定义正常流量模式：应记录网络中正常流量的行为模式，包括流量大小、访问时间、访问频率等。

b)部署网络监控工具：应使用 Wireshark、SolarWinds、Nagios 等工具实时监控网络流量，设置流量阈值，超出阈值时发出警报。

c)异常行为检测：应部署 IDS 和 IPS 检测分析网络中的异常行为，应使用安全信息和事件管理（SIEM）系统集中管理和分析安全数据。

#### 11.3.3 网络安全预警

a)威胁情报收集与分析：应获取最新网络安全威胁情报，评估其对智慧社区系统的潜在影响，制定防范策略。

b)实时监测与预警：应实时监测社区网络，触发预警机制并向安全团队发送警报。

c)应急响应计划：预警触发后，应迅速启动计划，遏制威胁扩散，恢复系统正常运行。

d)定期演练与评估：定期组织网络安全应急演练，提高应急响应能力；评估预警机制有效性并优化完善。

#### 11.3.4 系统安全扫描日志

a)日志收集与存储：应集中存储于高可用、可扩展、具数据保护能力的日志数据库。

b)日志分析与监控：实时分析日志数据，识别异常模式、检测潜在安全事件，整合外部威胁情报源信息，应以图形、图表和报告形式呈现分析结果。

c)警报与响应：检测到潜在安全事件时应触发警报，通过多种渠道发送给安全团队。配置自动化响应操作，记录详细事件信息以便后续分析和审计。

d)合规性与审计：应提供审计日志和报告证明系统安全扫描活动的合规性和有效性。

#### 11.3.5 隐私保护

应通过多因子认证、授权方式保护敏感数据，防止未经授权的第三方访问、使用。应用身份认证 USBKey 进行本地认证，登录系统或服务时向身份认证服务器发送请求，认证成功后生成认证令牌返回给用户，后续请求携带令牌访问授权资源数据。

### 11.4 数据安全

#### 11.4.1 数据分类与加密

敏感数据（如用户身份信息、设备运行日志）需采用AES-256或SM4算法加密存储，传输过程须启用TLS 1.3协议保障端到端安全性12。

#### 11.4.2访问控制

建立基于角色的权限管理体系（RBAC），实施最小权限原则，系统管理员操作需通过动态令牌二次验证25。

#### 11.4.3日志审计

关键系统操作日志应保留6个月以上，日志记录需包含操作者身份、时间戳、操作内容及IP地址，审计周期不超过7天。

### 11.5 隐私保护

#### 11.5.1个人信息处理

人脸识别数据存储周期不得超过30天，且需进行匿名化处理（如差分隐私技术），禁止用于非授权场景。

#### 11.5.2数据共享规范

跨系统数据交换需通过数据脱敏网关，确保姓名、身份证号等字段实现掩码处理。

#### 11.5.3用户知情权

在公共区域部署视频监控设备时，需设置显著标识牌（尺寸≥30cm×40cm），标注监控范围、数据用途及投诉渠道。

### 11.6 安全审计与应急响应

#### 11.6.1 风险评估

每半年开展一次渗透测试，针对OWASP Top 10漏洞进行专项整改，整改完成率需达100%。

#### 11.6.2 灾备机制

核心数据库实施同城双活+异地灾备架构，业务系统RTO≤15min，RPO≤5min。

#### 11.6.3 应急预案

编制网络安全事件分级响应手册，对大规模数据泄露事件需在2h内启动应急响应，24h内向主管部门报备。

# 附录 A 整治工作流程示意图

（资料性）

Informative