ICS 35.240.01
I6440

团　　体　　标　　准

T/WHCSA004—2024

智慧园区网络安全防御体系建设指南

Guide to the Construction of Smart Park Network Security Defense System

2024-11-26 发布　　2025-1-1 实施

武汉市网络安全协会　发布

目　　录

前　言

本标准按照 GB/T 1.1-2009《标准化工作导则 第 1 部分：标准的结构和编写》的规则制定。

本标准由武汉市经济和信息化委员会提出并归口。

本标准起草单位：武汉市网络安全协会、智网安云（武汉）信息技术有限公司、华中师范大学、湖北大学、中国电信股份有限公司武汉分公司、中国通信建设第三工程局有限公司、武汉数智云科技有限公司、武汉虹信技术服务有限责任公司、武汉烽火创新谷管理有限公司、武汉微创光电股份有限公司。

本标准主要起草人：刘悦恒、梁忠辉、覃兵、曹高辉、黄辰、雷显开、乔奇、张玉萍、严媛、王燕青、方波、王蓉蓉、郭贤凯、朱用功、张松、张峰、邢亚平、陈佳阳。

引　言

智慧园区企业的数字化和网络环境愈加复杂化，网络恶意攻击更加专业化和产业化，入侵手法也愈发多样化与复杂化，使得传统网络安全解决方案不断受到挑战。传统边界防护设备在防御常见威胁上起到了重要作用，但不能防范所有的、新型的攻击行为，包括来自内部和外部的攻击行为，智慧园区面临网络安全威胁的风险逐步增大。

本标准通过针对共性安全防护目标提出智慧园区场景通用的安全防御体系建设指南，指导智慧园区企业对网络安全防御体系的建设。

智慧园区网络安全防御体系建设指南

1 范围

本标准为智慧园区的 IT 网络安全体系规划、建设提供指导。主要包括智慧园区的物理安全、网络安全、数据安全、应用安全和安全保障。

2 规范性引用文件

GB / T25069-2010 信息安全技术 术语

GB / T25070-2019 信息安全技术 网络安全等级保护安全设计技术要求

GB / T22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 20984-2022 信息安全技术 信息安全风险评估方法

GB/T 43697-2024 数据安全技术 数据分类分级规则

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 20986——2023 信息安全技术 网络安全事件分类分级指南

中央网信办 《国家网络安全事件应急预案》

3 术语、定义和缩略语

3.1 智慧园区

智慧园区 smart park

以信息技术为手段、信息应用为支撑，充分运用云计算、物联网、大数据、人工智能、移动互联网等新一代信息技术，推进园区技术融合、业务融合、数据融合及服务融合，实现园区基础设施信息化、运营管理精细化、功能服务便利化和产业发展高端化的软件产业园区。

3.2 网络安全

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于

稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.3 安全保护能力

安全保护能力 securityprotectionability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

3.4 信息网络系统

信息网络系统 information network system

应用计算机、通信、多媒体、信息安全等等信息技术和 IT 设备、传输线路，将功能独立的 IT 系统、各类终端系统互联，与行为科学、管理科学等共同构成信息网络平台，通过可实现各种功能的软件应用实现资源共享和信息交互。

3.5 网络空间

网络空间 cyberspace

基于网络形成的虚拟的数字社会。

4 建设指导框架图

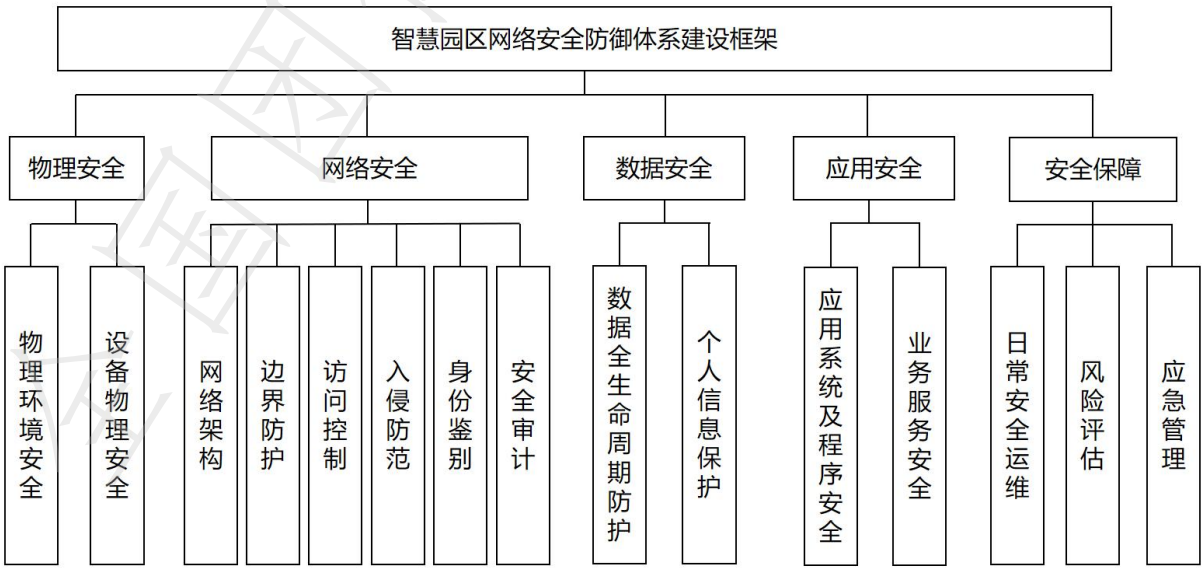

图 1 智慧园区网络安全防御体系框架

5 物理安全

物理安全主要规范智慧园区物理安全措施，包含信息系统所处物理环境安全、设备自身物理安全等方面。

5.1 物理环境安全

5.1.1 物理环境安全主要定义信息系统所处物理环境的安全保障，包含温湿度、防火、防雷、防潮、电力保障等方面。

5.1.2 信息系统所处的物理环境应设置访问控制措施，配置电子门禁系统，控制、鉴别和记录进出的人员。

5.2 设备物理安全

5.2.1 设备物理安全主要定义设备(网络设备、传感设备等)自身的物理保护，包含物理访问接入、设备输入输出管控等方面；

5.2.2 保证设备电力供应，应在供电线路上配置稳压器和过电压防护设备；应提供短期的备用电力供应，至少满足设备在突发断电情况下的正常运行要求；

5.2.3 应具备电磁防护措施。

6 网络安全

网络安全是指对园区网络环境及运行的业务系统采取的安全防护措施，具体包括网络架构、边界防护、访问控制、入侵防范、身份鉴别和安全审计。

6.1 网络架构

6.1.1 应保证园区信息系统使用的链路带宽满足业务高峰需求；网络链路各设备的业务处理能力满足园区业务高峰需求；

6.1.2 应根据园区业务重要性划分网络安全区域，分区重点防护。

6.2 边界防护

6.2.1 应能够对非授权设备私自接入园区内部网络的行为进行检查或限制；

6.2.2 应能够对园区内部用户非授权连接外部网络的行为进行检查或限制；

6.2.3 应限制园区无线网络的使用，保证无线网络通过受控的边界设备接入园区内部网络；应明确禁止使用无线网络的区域，如园区数据中心、核心生产区域等；

6.2.4 应对园区网络接入边界的网络流量和访问行为进行实时检测，阻断异常网络行为并告警。

6.3 访问控制

6.3.1 应根据网络安全区域设置安全策略，设置匹配园区业务访问需求的控制规则；

6.3.2 应删除多余或无效的访问控制规则，持续优化访问控制规则列表；

6.3.3 应对进出园区网络的数据和流量进行基于应用协议和应用内容的访问控制；

6.3.4 访问控制的粒度应达到主体为用户级，客体为业务系统、端口级。

6.4 入侵防范

6.4.1 应在园区网络边界、核心节点处检测、防止或限制从外部发起和从内部发起的网络攻击行为；

6.4.2 应采取相关技术措施对网络行为进行分析；

6.4.3 应在园区网络核心节点处、主机环境中对恶意代码进行检测和清除，并维护恶意代码防护技术的升级和更新；

6.4.4 应记录网络攻击信息的攻击源、类型、目标、时间；

6.4.5 应对园区重要网络节点的入侵和攻击行为进行实时告警。

6.5 身份鉴别

6.5.1 应对接入园区网络的用户进行身份表示和鉴别，且身份标识具有唯一性；

6.5.2 身份鉴别信息具有复杂度要求并定期更换；应对登录失败行为配置限制会话、结束会话等措施；

6.5.3 应采取加密措施，防止身份鉴别信息在网络传输过程中被窃听；

6.5.4 应采用双因子认证鉴别技术对用户进行身份鉴别。

6.6 安全审计

6.6.1 应在园区网络边界、核心网络节点处进行安全审计，审计范围覆盖到每个入网用户；

6.6.2 安全审计内容包含日期、时间、用户、事件类型、是否成功及其他审计信息；

6.6.3 安全审计记录应采取保护措施，定期备份，避免发生删除、修改或覆盖等；

6.6.4 应对采用远程访问的用户行为进行单独审计和分析；

6.6.5 应对审计进程进行保护，防止未经授权的中断。

7 数据安全

数据安全主要规范园区业务系统中的数据安全及存储的个人信息安全，包含数据全生命周期防护和个人信息保护。

7.1 数据全生命周期防护

7.1.1 应根据园区业务类型和重要级别进行分类，分类维度应包含数据来源、数据组织、数据字段和其他等；

7.1.2 应根据园区业务系统数据内容的敏感度进行分级，按照实际业务需求制定多层级别。

7.1.3 应采用身份认证、准入控制、链路加密、应用层加密等方式防止假冒数据源接入，确保采集数据的真实性和完整性；

7.1.4 在数据（流式数据、数据库、文件、服务接口等类型的数据）传输过程中，应采取加密措施保障数据的完整性、机密性；

7.1.5 应对数据使用者身份进行鉴别，防止假冒合法人员使用数据；对使用者进行权限控制，防止数据使用者越权访问数据；

7.1.6 应对园区存在的敏感数据进行脱敏处理，对所有访问敏感数据的行为进行监控和审计；

7.1.7 应根据数据类别、级别采用不同的安全存储机制，对于重要程度低的数据，可以明文存储；对于重要程度很高的数据，使用加密存储，保证关键数据的保密性；

7.1.8 应对不再具有价值或需要保护隐私时的数据，对其进行销毁。

7.2 个人信息保护

7.2.1 应按照《中华人民共和国个人信息保护法》的相关要求，处理园区业务系统中存储的个人信息。

8 应用安全

应用安全主要规范智慧园区网络中的应用系统及程序安全、业务服务安全。

8.1 应用系统及程序安全

8.1.1 园区应用系统及程序主要包含智慧园区运营管理平台、园区及企业服务平台、无线管理系统、视频监控系统、门禁管理系统、停车管理系统、接警应急指挥系统、数字广播系统、LED 大屏显示系统、信息发布系统等，以及园区 APP、微信小程序等其他应用程序；

8.1.2 应对园区 WEB 应用系统采取技术措施，防止恶意攻击、非法访问、防篡改等攻击行为；

8.1.3 应对承载园区 WEB 应用运行的主机采取技术措施，防止主机入侵、病毒木马感染、后门上传等攻击行为；

8.1.4 园区 APP、微信小程序等其他应用程序应开展风险评估、安全加固、实时监测等技术防护工作。

8.2 业务服务安全

8.2.1 应对接入园区无线管理系统、门禁管理系统、数字广播系统、LED 大屏显示系统等系统的客体进行准入控制，严格限制未经授权的客体接入；设置控制策略，限制接入客体的最小权限；

8.2.2 应对智慧园区运营管理平台、园区及企业服务平台、视频监控系统、门禁管理系统、停车管理系统等包含园区敏感数据的系统进行数据保护措施，防止敏感数据泄漏及未经授权的数据使用；

8.2.3 应对接警应急指挥系统、数字广播系统、LED 大屏显示系统、信息发布系统等系统进行传播数据的安全监控和审计，防止非法信息的传播。

9 安全保障

安全保障主要规范智慧园区网络安全管理与支撑相关的标准与措施，包含日常安全运维、风险评估、应急管理。

9.1 日常安全运维

9.1.1 应制定园区网络安全管理制度，并根据制度完成对应的技术工作；管理制度应定期修订完善；

9.1.2 应对园区业务系统及程序进行安全监测，制定监测指标，包含可用性、安全性等；安全监测手段具备风险实时告警能力；

9.1.3 应定期进行安全巡检，对安全设备进行配置及策略检查，输出安全巡检报告，报告内容包含运行状态、优化建议等内容；

9.1.4 完成日常安全运维工作后，输出工作报告，工作报告形式有周报、月报、季报、年报表。

9.2 风险评估

9.2.1 应进行园区网络资产、业务资产梳理，形成园区资产台账，并定期更新完善；根据资产梳理台账，确定网络安全风险评估目标；

9.2.2 应制定网络安全风险评估流程及周期，定期开展评估工作，输出风险评估报告；

9.2.3 应采用专业风险评估工具，结合人工验证，确定风险是否可利用及风险值；

9.2.4 对已确认的风险制定修复和加固方案，并完成加固；

9.2.5 应定期更新和迭代风险评估技术及流程，确保评估技术的可用性。

9.3 应急管理

9.3.1 应编制园区网络安全应急管理制度，并定期修改完善，加强制度的宣贯和下发；

9.3.2 应制定安全事件应急响应流程，组建网络安全应急响应团队；

9.3.3 应定期组织网络安全应急演练，模拟安全攻击，检测园区网络安全防护策略的有效性；

9.3.4 应建设安全事件溯源技术措施，对正在发生及已发生的安全事件进行溯源定位。

10 附录：智慧园区相关知识库

附录 A：数据分类分级示例

数据类别	数据子类分类参考	数据分级参考
研发域数据	开发及测试代码	核心开发及测试代码数据
		重要开发及测试代码数据
		一般开发及测试代码数据
	应用设计原型	核心应用设计原型数据
		重要应用设计原型数据
		一般应用设计原型数据
	园区设计规划图纸	核心园区设计规划图纸数据
		重要园区设计规划图纸数据
		一般园区设计规划图纸数据
监控域数据	生产监控数据	核心生产监控数据
		重要生产监控数据
		一般生产监控数据
	园区环境监控数据	重要园区环境监控数据
		一般园区环境监控数据
	园区车辆监控数据	重要园区车辆监控数据
		一般园区车辆监控数据
	园区人员流动监控数据	重要园区人员流动监控数据
		一般园区人员流动监控数据
管理域数据	园区安全管理制度	重要园区安全管理制度数据

		一般园区安全管理制度数据
	固定资产信息	重要固定资产信息
		一般固定资产信息
	经营与财务数据	核心经营与财务数据
		重要经营与财务数据
		一般经营与财务数据
	人力与客户数据	重要人力与客户数据
		一般人力与客户数据
	资源管理数据	重要资源管理数据
		一般资源管理数据
运维域数据	供应链数据	核心供应链数据
		重要供应链数据
		一般供应链数据
	日常运维数据	重要日常运维数据
		一般日常运维数据

参考文献

GB / T25069-2010 信息安全技术 术语

GB / T25070-2019 信息安全技术 网络安全等级保护安全设计技术要求

GB / T22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 20984-2022 信息安全技术 信息安全风险评估方法

GB/T 43697-2024 数据安全技术 数据分类分级规则

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 20986——2023 信息安全技术 网络安全事件分类分级指南

中央网信办 《国家网络安全事件应急预案》