《多功能智能杆　信息系统安全管理规范》解读

一、制定背景

标准是构成国家核心竞争力的基本技术要素，是规范经济和社会发展的重要技术制度。习近平总书记提出：“标准决定质量，有什么样的标准就有什么样的质量，只有高标准才有高质量”。

当前，智慧城市的建设与发展迅速，作为近年来新兴的城市公共设施，多功能智能杆整合城市各类基础设施与新型设施，融合多种城市功能，并通过运用信息和通信技术手段感测、分析、整合城市运行系统的各项关键信息，实现城市服务与城市管理的智慧化，是智慧城市的重要载体。

2021 年 2 月 10 日，为了规范多功能智能杆基础设施的管理，有效利用资源，提高城市管理效能和公共服务水平，提升城市品质，维护智慧城市感知网络安全，根据有关法律法规、规章等规定，深圳市人民政府下发《深圳市人民政府关于印发深圳市多功能智能杆基础设施管理办法的通知》(深府规〔2021〕3 号)，要求充分发挥深圳信息产业发展特别是 5G 率先独立组网全覆盖的先发优势，坚持高标准规划建设、高水平运营管理，推进多功能智能杆建设，进一步提升城市管理水平，加快实现万物感知、万物互联、万物智能，努力为打造一流智慧城市提供有力支撑。

近年来，随着 5G 技术的迅速发展与新基建进程的加速，多功能智能杆建设正在全国各地蓬勃开展，各地纷纷出台相关建设标准，但是现阶段，多功能智能杆在信息系统安全管理方面尚无相关标准。本

文件将为多功能智能杆信息系统安全提供依据，防范对多功能智能杆网络的攻击、侵入、干扰、破坏和非法使用以及意外事故提出防范应对措施，提升多功能智能杆系统网络数据的完整性、保密性、可用性的能力，助力多功能智能杆产业高质量发展。本文件的编制将对完善我国智慧城市标准体系，助力智慧城市建设具有重要现实意义。

二、目的和意义

“让城市更聪明一些、更智慧一些，是推进城市治理体系和治理能力现代化的必由之路，前景广阔”。习近平总书记的讲话为未来城市的发展指明了道路和方向。

智慧城市是在物联网、云计算、大数据等新一代信息技术快速发展背景下产生的城市发展新模式，通过“更加透彻的感知、更加深入的计算和更加广泛的连接”，改变着物与物之间、人与物之间的联系方式，改变着我们的生存环境，也深刻改变着人类的思维方式和生活模式。

多功能智能杆作为新基建的重要组成和智慧城市建设的入口，也是未来承载 5G 基站布点的载体，它通过深度整合城市各类资源，实现资源的共享、集约和统筹，降低城市建设成本，提升城市运维效率，将为城市治理的快速发展带来多重效益。

2018 年 6 月，深圳出台《深圳市多功能智能杆建设发展行动计划（2018—2020 年）》，成为国内首个政府出台的顶层行动计划。

2019 年 9 月，《深圳市人民政府关于印发率先实现 5G 基础设施全覆盖及促进 5G 产业高质量发展若干措施的通知》印发，要求加快推进多功能智能杆建设。

2020 年 4 月，中华人民共和国国家发展和改革委员会明确“新基建”范围主要包括：包含以 5G、物联网为代表的信息基础设施，以大数据、人工智能等技术深度应用的融合基础设施和以支撑科学研究、技术开发等的创新基础设施。随着我国物联网新型基础设施建设的全面推进，多功能智能杆的产业发展步入快车道。

2021 年我国多功能智能杆建设的最大特点是从北上广深延伸到了全国各地，2021 年度共有 28 个省（自治区、直辖市）新增了多功能智能杆建设项目，新增项目总量达到 350 个，新增多功能智能杆拟建数量达到 12.8 万根。

多功能智能杆包括杆体及其搭载的感知终端（各类设备和传感器），它是集智慧照明、视频监控、交通管理、环境监测、无线通信、应急求助等多功能于一体的信息基础设施。梳理和分析多功能智能杆系统之间的数据流通路径，将系统中不同设备、软件、数据、资源分不同重要等级进行分等级保护显得尤为重要。

近年来，数据安全形势不容乐观，世界各国均高度重视数据安全及隐私保护，例如美国发布了《网络安全信息共享法》，欧盟发布了《一般数据保护法案》、德国发布了《联邦数据保护法》、英国发布了《数据保护法》等；十九届四中全会，我国首次增列“数据”作为生产要素，数据安全与国家安全息息相关。我国国家数据安全相关法律法规有《中华人民共和国网络安全法》《中华人民共和国数据安全法》及《中华人民共和国个人信息保护法》等；国内数据安全标准有 GB/T 35273—2020《信息安全技术　个人信息安全规范》、GB/T 37988—2019《信息安全技术　数据安全能力成熟度模型》等。

习近平总书记高度重视信息网络安全工作，多次提出：没有网络安全就没有国家安全，没有信息化就没有现代化；网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进。

多功能智能杆信息系统是指由计算机及其相关和配套的挂载设备、设施构成的，按照一定的应用目标和规则对信息进行存储、传输、处理的系统或者网络；信息是指在信息系统中存储、传输、处理的数字化信息。

多功能智能杆系统信息安全是指在政府主导和社会参与下，综合运用技术、法律、管理、教育等手段，在信息空间积极应对敌对势力攻击、网络犯罪和意外事故等多种威胁，有效保护信息基础设施、信息系统、信息应用服务和信息内容的安全，为经济发展、社会稳定、国家安全提供安全保障的活动。

三、主要内容

本文件包括7个章，分别为范围，规范性引用文件，术语和定义，信息系统安全管理的原则、策略、内容和制度，机构建设和人员管理、风险管理和控制、运维和服务管理。

1　范围

本文件规定了多功能智能杆信息系统安全管理的原则、策略、内容和制度、机构建设和人员管理、风险管理和控制、运维和服务管理。

本文件适用于指导多功能智能杆信息系统安全管理工作。

2　规范性引用文件

本文件在制定过程中规范性引用了下列国家标准：

GB/T 20271—2006　信息安全技术　信息系统通用安全技术要求

GB/T 25069—2022　信息安全技术　术语

GB 50016—2014　建筑设计防火规范

3　术语和定义

3.1　完整性

数据、系统或信息在存储、传输和处理过程中保持无误、不受损坏、不受篡改的状态。

3.2　可用性

表征数据或系统根据授权实体的请求可被访问与使用程度的属性。

3.3　访问控制

按确定的规则防止对资源的未授权使用，对实体之间的访问活动进行控制的安全机制。

3.4　安全审计

按确定规则的要求，对与安全相关的事件进行审计，以日志方式记录必要信息，并作出相应处理的安全机制。

3.5　鉴别信息

确认系统中身份真实性过程的信息。

3.6　风险评估

对信息系统所面临的威胁、存在的弱点、造成的影响以及对信息系统处理、传输和存储信息的保密性、完整性（3.1）和可用性（3.2）等进行科学识别和评价，确定信息系统面临风险可能性的过程。

3.7　安全策略

为信息系统安全管理制定的行动方针、路线、工作方式、指导原则或程序。

4　信息系统安全管理的原则、策略、内容和制度

4.1　信息系统安全管理原则

本条规定了信息系统安全管理的9个原则。

4.2　信息系统安全管理策略

本条规定了信息系统安全管理的5个安全管理策略。

4.3　信息系统安全管理内容

本条规定了落实安全管理机构及安全管理人员、开发安全策略、实施风险管理、制定业务持续性计划和灾难恢复计划、选择与实施安全措施、确保配置、变更的正确与安全、进行安全审计、确保维护支持、进行监控、检查，处理安全事件、安全意识与安全教育、人员安全管理等信息系统安全管理内容。

4.4　信息系统安全管理制度

本条规定了基本的安全管理制度要求、完整的安全管理制度要求、体系化的安全管理制度要求、强制保护的安全管理制度要求、专控保护的安全管理制度要求。

5　机构建设和人员管理

5.1　建立安全管理机构

本条规定了配备安全管理人员要求、建立信息系统安全职能部门要求、成立安全领导小组要求、主要负责人担任领导要求、建立信息安全保密管理部门要求。

5.2　信息系统安全领导小组

本条规定了安全管理的领导职能要求、保密监督的管理职能要求。

5.3　信息系统安全职能部门

本条规定了基本的安全管理职能要求、集中的安全管理职能要求。

5.4　安全管理人员配备

本条规定了配备兼职安全管理人员要求、配备专职安全管理人员要求、关键部位的安全管理人员要求。

5.5　关键岗位人员管理

本条规定了关键岗位人员的基本要求、兼职和轮岗要求、权限分散要求、多人共管要求、全面控制要求。

5.6　人员录用管理

本条规定了人员录用的基本要求、人员的审查与考核要求、人员的内部选拔要求、人员的可靠性。

5.7　人员离岗管理

本条规定了人员离岗的基本要求、调离后的保密要求、离岗的审计要求、关键部位人员的离岗要求。

5.8　人员考核与审查

本条规定了定期的人员考核要求、定期的人员审查要求、管理有效性的审查要求、全面严格的审查要求。

5.9　人员教育和培训

本条规定了“应知应会”培训要求、有计划培训要求、针对不同岗位培训要求、按人员资质要求培训要求、安全意识自觉性培训要求。

6　风险管理和控制

6.1　风险管理要求

本条规定了基本风险管理要求、定期风险评估要求、规范风险评估要求、独立审计的风险管理要求、全面风险管理要求。

6.2　风险管理策略

本条规定了基本的风险管理策略要求、风险管理的监督机制要求、风险评估的重新启动要求。

6.3　风险分析

本条规定了资产识别和分析要求、威胁识别和分析要求、脆弱性识别和分析要求。

6.4　风险评估

本条规定了经验的风险评估要求、全面的风险评估要求、建立和维护风险信息库要求。

6.5　风险控制

本条规定了基于安全等级标准选择控制措施要求、基于风险评估选择控制措施要求、基于风险评估形成防护控制系统要求。

6.6　安全确认

本条规定了残余风险接受要求、残余风险监视要求、安全风险再评估要求。

7　运维和服务管理

7.1　运维环境管理

本条规定了运维环境管理的一般要求、运维环境安全管理要求、机房安全要求、办公环境安全要求。

7.2　服务资源管理

本条规定了资产清单要求、资产的分类与标识要求、存储介质要求、挂载设备要求。

7.3　用户管理

本条规定了用户管理要求、运行操作管理要求。

7.4 运行操作管理

本条规定了系统计算机操作要求、终端计算机操作要求、网络及安全设备操作要求、业务应用操作要求、变更控制和重用要求和信息交换要求。

7.5 运行维护管理

本条规定了日常运行要求、运行监控要求、软件硬件维护要求、外部服务访问要求。

7.6 外包服务管理

本条规定了外包服务合同要求、外包服务商要求、外包服务的运行管理要求。

7.7 机制管理和安全管理

本条规定了身份鉴别机制要求、访问控制机制要求、管理平台安全要求、网络安全要求、挂载设备安全要求、病毒防护要求、密码管理要求。

7.7 业务连续性管理

本条规定了数据备份和恢复要求、备份与冗余要求、安全事件处置和管理要求、安全事件报告和响应要求、应急处理要求。