《多功能智能杆　信息系统安全管理要求》

（送审稿）编制说明

一、项目背景

“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，要求加快推进多功智能杆建设。

2020 年 4 月国家发改委明确“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《国家安全和个人数据保护法 (草案)》、《网络安全信息共享法》等，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》、《数据安全管理办法》征求意见稿等；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。

2017 年 6 月 1 日正式实行的《中华人民共和国网络安全法》中第二十一条明确规定：国家实行网络安全等级保护制度。网络运营者应

当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

信息安全保障能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分，是全世界各国奋力攀登的制高点。网络信息安全问题如果解决不好，将全方位地危及我国的政治、军事、经济、文化、社会生活的各个方面，使国家处于信息战和高度经济金融风险的威胁之中。

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、公众权益和军事斗争提供安全保障的活动。

为适应深圳市多功能智能杆发展的新形势，满足新形势下多功智能杆对标准化发展的新需求，规范多功能智能杆建设与管理全过程中的网络安全、通讯安全、数据安全，根据《中华人民共和国网络安全法》的基本原则，结合深圳经济特区地域实际，编制地方标准《多功

能智能杆 信息系统安全管理要求》十分必要。

二、工作简况

1、任务来源

根据“深圳市市场监督管理局关于下达 2021 年第一批深圳市地方标准计划项目任务的通知”，《多功能智能杆　网络安全等级保护基本要求》地方标准批准立项。

2、主要工作过程

（一）预研阶段

项目下达后，充分吸收来自深圳多功能智能杆多个不同领域内有能力、经验和研究工作基础的专家、学者、企业代表组成标准编制组，编制组充分考虑深圳多功能智能杆信息安全潜在的风险因子，为提高系统运维管理水平，满足相关法规的要求，从信息内容的被泄露、被假冒、被伪造；信息系统被攻击、被入侵、被染毒；信息网络被堵塞、被中断、被致瘫；信息基础设施被损伤、被破坏、被损毁等维度，确定本文件的主要内容，完成标准编制大纲。

（二）编制阶段

1）成立起草组

充分吸收来自多功能智能杆建设与管理各个不同领域内有能力、经验和研究工作基础的专家、学者、企业代表等，于标准立项批准后立即成立标准编制组。

2022 年 8 月 15 日，深圳市《多功能智能杆 网络安全等级保护规范》和《多功能智能杆 信息系统安全管理规范》地方标准编制工作启动会在深圳市前海深港合作区南山街道桂湾五路 123 号前海大厦 T2

栋 5 楼会议室隆重举行，会议由深圳市脉山龙信息技术股份有限公司总裁主持，市工信局信息基础设施处、深圳市信息基础设施投资发展有限公司以及脉山龙、深信投、洲明科技、昂楷科技等二十五家单位代表出席了会议。本次会议的召开，统一了两项标准的编制思路和原则，确定了标准编制的下一步计划，为标准编制工作的顺利推进奠定了基础。

2）形成标准草案

2022 年 9 月 23 日，深圳市《多功能智能杆 网络安全等级保护规范》和《多功能智能杆 信息系统安全管理规范》地方标准编制第二次工作会议在深圳市新一代产业园深信投公司 1 号会议室召开。参会专家对两项地标的标准草案做了深入研讨，拟定了两项地标修该完善的任务分工。

1. 鼎铉商用密码测评技术（深圳）有限公司完善密码模块及加密方式等内容。
2. 深圳市万集科技股份有限公司完善密码运算功能接口及软硬件模块内容。
3. 深圳市博通智能技术有限公司完善安全物理环境、安全管理制度、安全管理机构等内容。
4. 深圳市可信计算有限公司完善可信验证的流程图内容。
5. 华为技术有限公司完善接入控制及接口协议等内容。

深圳昂楷科技有限公司完善数据分类及分级保护内容。

3）形成征求意见稿

2022 年 12 月 13 日下午，两项地标编制第三次工作会议在深圳市新一代产业园深信投公司 1 号会议室召开。会议对多功能智能杆网络安全、信息系统安全两项地标的标准草稿进行了研讨。参会专家对照标准草稿从网络安全的等级适应范围、密码模块、网络架构、接入控制、可信计算、数据安全及系统安全的管理要求等方便展开充分研讨。本着保证标准的科学性、先进性、规范性和可操作性，完成讨论稿的第三次修改。

2023 年 3 月 6 日，深圳市工业和信息化局将会后修改标准稿发给相关局征求意见，深圳市交通运输局、深圳市通信管理局、深圳市水务局、深圳市气象局、深圳大学都有书面反馈意见。

在收到各个局的反馈意见后，对原稿再次进行修改完善，形成现在的征求意见稿。

4）形成送审稿

2023 年 5 月 28 日- 2023 年 6 月 30 日，深圳市工业和信息化局挂网公开征求意见，收到意见 8 条，采纳 7 条，其中 1 条不采纳。对原稿再次进行修改完善，形成现在的送审稿。

三、编制原则、技术依据、国际先进标准的对标情况

1、编制原则

遵循“科学、实用、适度”的原则，既考虑标准的前瞻性又顾及深圳市多功能智能杆网络安全等级保护发展的实际情况，充分调研深圳市多功能智能杆信息系统安全管理的实际情况，信息安全的重要性

主要体现在信息内容安全、信息系统安全、信息网络安全、信息基础设施安全等等方面。信息内容的被泄露、被假冒、被伪造等，信息系统被攻击、被入侵、被染毒，信息网络被堵塞、被中断、被致瘫等，信息基础设施被损伤、被破坏、被损毁等等，这些都是重要的信息安全事件，都应该也必须引起高度重视和迅速解决。本文件以安全管理要素作为描述安全管理要求的基本组件。

2、技术依据

1）《中华人民共和国网络安全法》

第 4 章 信息系统安全管理，参考《中华人民共和国网络安全法》，经研究对体系化的安全管理制度，结合具体的场景应用，给出了“应制定系统互联评估、网络使用授权、网络检测、网络设施（设备和协议）变更控制和相关的操作规程等方面的网络安全管理规定。”

2）《中华人民共和国数据安全法》

GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》

第 4 章 信息系统安全管理，参考《中华人民共和国数据安全法》和 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》，经研究对基本的安全管理制度，结合具体的场景应用，给出了“应制定系统互联评估、网络使用授权、网络检测、网络设施（设备和协议）变更控制和相关的操作规程等方面的网络安全管理规定。”

3、《中华人民共和国个人信息保护法》

GB/T 35273-2020《信息安全技术 个人信息安全规范》

第 7 章 运维和服务管理，参考《中华人民共和国个人信息保护法》和 GB/T 35273-2020《信息安全技术 个人信息安全规范》，经研究对信息资产进行分类管理，结合具体的场景应用，给出了“个人隐

私信息、个人专有信息、公民个人可公开共享的信息”的分类管理。

3、与国内领先、国际先进标准的对标情况

目前在国内外，信息系统安全管理已有相应的标准，未查到“多功能智能杆　信息系统安全管理要求”的相关标准。我们国家则在国家、行业、地方、团体标准等各个层面皆有信息系统安全管理的发布，但基本上都是信息系统安全管理通用技术标准，本文件与上述标准侧重点不同：主要是针对智慧城市信息基础设施中多功能智能杆的信息系统安全管理。深圳在多功能智能杆的实践探索，无论从深度和广度上都已经远超出国内外标准所述的范围。本地方标准将在实践探索中的经验融入到条款中，比国内外的信息系统安全管理标准的内容细化和精准。

国际标准

1、ISO/IEC 17799-2005 信息技术.信息安全管理用实施规程

国家标准

1、GB/T 20269-2006 信息安全技术 信息系统安全管理要求

2、GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

3、GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

4、GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南

5、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

6、GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

7、GB/T 28449-2018 信息安全技术 网络安全等级保护测评过程指南

8、GB/T 28453-2012 信息安全技术 信息系统安全管理评估要求

9、GB/T 34990-2017 信息安全技术 信息系统安全管理平台技术要求

和测试评价方法

10、GB/T 36627-2018 信息安全技术 网络安全等级保护测试评估技术指南

11、GB/T 36958-2018 信息安全技术 网络安全等级保护安全管理中心技术要求

12、GB/T 36959-2018 信息安全技术 网络安全等级保护测评机构能力要求和评估规范

13、GB/T 37094-2018 信息安全技术 办公信息系统安全管理要求

行业标准

1、GA/T 713-2007 信息安全技术 信息系统安全管理测评

2、MH/T 0031-2009 民用航空运输机场信息系统安全管理规范

3、SY/T 5231-2010 石油工业计算机信息系统安全管理规范

四、各章节主要条款的说明

本文件包括 7 个章节分别为范围，规范性引用文件，术语和定义，信息系统安全管理内容、原则、策略和制度，信息系统安全管理机构建设和人员管理，信息系统安全管理风险控制，信息系统安全管理通用要求。

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，包括数据完整性和系统完整性。

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

用以确认系统中身份真实性的过程。

3.6 风险评估

通过对信息系统的资产价值/重要性、信息系统所受到的威胁以及信息系统的脆弱性进行综合分析，对信息系统及其处理、传输和存储的信息的保密性、完整性和可用性等进行科学识别和评价，确定信息 系统安全风险的过程。

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

4.1　信息系统安全管理内容

是对管理平台、移动互联、挂载设备和公共数据的生存周期全过程实施符合安全等级责任要求的管理全管理内容

4.2　信息系统安全管理原则

提出 11 个原则

4.3　信息系统安全管理策略

提出 5 个安全管理策略

4.4　信息系统安全管理制度

从五个维度提出安全管理制度

5 机构建设和人员管理

5.1　建立安全管理机构

本条规定了从“配备安全管理人员、建立安全职能部门、成立安全领导小组、主要负责人出任领导、建立信息安全保密管理部门”5个维度建立安全管理机构

5.2　信息安全领导小组

本条信息系统安全领导小组负责领导本组织机构的信息系统安全工作，规定了至少行使“安全管理的领导职能”或者“保密监督的管理职能”之一。

5.3　信息安全职能部门

本条信息安全职能部门在信息系统安全领导小组领导下，负责本组织机构信息系统安全的具体工作，规定了至少行使“基本的安全管理职能”或者“集中的安全管理职能”之一。

5.4　安全管理人员配备

本条不同安全等级的安全管理人员配备，规定了从“专职安全管理人员”、“专职安全管理人员”、“关键部位的安全管理人员”中选择。

5.5　关键岗位人员管理

本条不同安全等级的关键岗位人员管理，规定了从“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”中进行选择。

5.6　人员录用管理

本条不同安全等级的人员录用管理，规定了从“录用的基本要求”、“人员的审查与考核”、“人员的内部选拔”、“人员的可靠性”中进行选择。

5.7 人员离岗管理

本条不同安全等级的人员离岗管理，规定了从“离岗的基本要求”、“调离后的保密要求”、“离岗的审计要求”中进行选择。

5.8 人员考核与审查

本条不同安全等级的人员考核与审查管理，规定了从“定期的人员考核”、“定期的人员审查”、“管理有效性的审查”、“全面严格的审查”中进行选择。

5.9 人员教育和培训

本条不同安全等级的人员教育和培训，规定了从“应知应会要求培训”、“有计划培训”、“不同岗位培训”、“人员资质要求培训”、“安全意识自觉性培训”中进行选择。

6 风险管理和控制

6.1 风险管理要求

风险管理作为等级保护的手段，在保证信息等级系统的最低保护能力的基础上，根据风险增加某些管理要求。

6.2 风险管理策略

不同安全等级的风险管理策略不同。

6.3 风险分析

从资产识别、威胁识别和脆弱性识别提出风险分析。

6.4 风险评估

应由用户和部分专家通过经验来判断风险，并对风险进行评估，

形成风险评估报告，其中必须包括风险级别、风险点等内容，并确定信息系统的安全风险状况。

6.5　风险控制

以信息系统及产品的安全等级标准对不同等级的技术和管理要求，选择相应等级的安全技术和管理措施，决定需要实施的信息系统安全控制措施。

6.6　安全确认

采用系统化的方法对信息系统安全风险实施再次评估，通过再次评估，验证防护措施的有效性。

7　运维和服务管理

7.1　物理环境管理

本条规定了从“物理位置选择、防盗窃和防破坏、防雷击、防水和防潮、防静电、温湿度控制、电力供应、电磁防护”等方面提出物理环境管理。

7.2　资源安全管理

本条规定了从“资产清单管理、资产的分类与标识要求、介质管理、挂载设备管理要求”提出资源安全管理。

7.3　用户操作管理

本条规定了从“用户管理要求、运行操作管理要求”提出用户操作管理。

7.4　运行维护管理

本条规定了从“日常运行安全管理、运行状况监控要求、软件硬件维护管理要求、外部服务方访问管理要求”提出运行维护管理

7.5　外包服务管理

本条规定了从“外包服务合同、外包服务商、外包服务的运行管理”提出外包服务管理

7.6　安全机制管理

本条规定了从“身份鉴别机制管理要求、访问控制机制管理要求、管理平台安全管理要求、网络安全管理要求、挂载设备安全管理要求、病毒防护管理要求、密码管理要求”提出安全机制管理。

7.7　业务连续性管理

本条规定了从“数据备份与恢复管理要求、设备和系统的备份与冗余、安全事件划分管理、安全事件报告和响应管理、应急处理要求”提出业务连续性管理。

五、是否涉及专利等知识产权问题

无。

六、重大意见分歧的处理依据和结果

本文件制定过程中无重大分歧意见。

七、实施标准的措施建议

1、在相关专业媒体上宣传《多功能智能杆 网络安全等级保护基本要求》。

2、通过有关会议介绍《多功能智能杆 网络安全等级保护基本要求》。

3、在运行单位的管理系统中，严格执行《多功能智能杆 网络安全等级保护基本要求》。

八、其他需要说明的事项

无。