《多功能智能杆　网络安全等级保护规范》（送审稿）编制说明

一、项目背景

1 国内外现行相关法律、法规和标准情况

多功能智能杆在网络安全方面需要遵守国内外的法律、法规和标准，以确保数据和通信的安全性。以下是一些国内外关于网络安全的主要法律、法规和标准：

国内情况：

《中华人民共和国网络安全法》： 这是中国的核心网络安全法律，于2017年实施。它规定了网络基础设施的安全要求，包括要求网络运营者采取措施保护网络安全，报告重大网络安全事件，以及维护用户数据的隐私等。

《信息安全技术 个人信息安全规范》（GB/T 35273-2020）： 这是中国国家标准，规定了个人信息的安全要求，包括个人信息的收集、存储、传输和处理。

《电信和互联网用户个人信息保护规定》： 这是中国工信部颁布的规定，针对电信和互联网服务提供商，规定了用户个人信息的保护要求。

国家密码管理法规： 中国有一系列关于密码管理的法规，包括密码使用和管理的要求。

国际情况：

ISO/IEC 27001： 这是国际上最广泛使用的信息安全管理体系标准，提供了一套用于建立、实施、监测、审查和改进信息安全管理体

系的指南。

GDPR（通用数据保护条例）： 欧洲联盟的GDPR法规涵盖了个人数据的处理和隐私保护，适用于处理欧盟居民的数据。

NIST（美国国家标准与技术研究院）： NIST发布了一系列与网络安全相关的框架和指南，例如NIST框架，用于加强关键基础设施的网络安全。

CCPA（加利福尼亚消费者隐私法）： 美国加利福尼亚州颁布了CCPA法律，规定了消费者数据隐私权的保护要求。

其他国家/地区法规： 不同国家和地区都有各自的数据隐私和网络安全法规，因此在涉及国际业务时，需要了解相关国家/地区的法规。

要确保多功能智能杆在网络安全方面合规，应根据项目的具体情况，参考适用的法律、法规和标准，并可能需要咨询网络安全专家以确保符合最新的要求。

2、 制定地方标准的必要性和意义

“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。

信息安全等级保护从与信息系统安全相关的物理层面、网络层面、系统层面、应用层面和管理层面对信息和信息系统实施分等级安全保护。管理层面贯穿于其他层面之中，是其他层面实施分等级安全保护

的保证。本文件对信息和信息系统的安全保护提出了分等级安全管理的要求，阐述了安全管理要素及其强度，并将管理要求落实到信息安全等级保护所规定的五个等级上，有利于对安全管理的实施、评估和检查。

为适应深圳市多功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特点，为多功能智能杆网络安全等级保护提供依据，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。编制地方标准《多功能智能杆　网络安全等级保护规范》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2022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　网络安全等级保护规范》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，防止黑客的入侵和恶意访问，跟踪服务器上用户行为，降低运维成本，提供控制和审计依据，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。

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。

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。为保证标准的科学性、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单位征求意见，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。在收到各单位反馈意见后，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 2 条，采纳 2 条。对原稿再次进行修改完善，形成送审稿，提交至深圳市市场监督管理局。

三、地方标准主要内容的依据以及与国内领先、国际先进标准的对标情况

1.主要内容的依据

1）《中华人民共和国网络安全法》

第 5 章 网络安全等级保护，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“网络安全等级保护对象定级、不同等级的安全保护能力、安全通用要求、安全扩展要求、密码模块安全要求和安全管理要求”

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》

本文件的 6.5、7.5、8.5 公共数据安全要求，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》，经研究对数据各个维度的基本安全，结合具体的场景应用，给出了“数据收集、存储、传输、使用、加工、共享、交易、出境、销毁与删除等维度的具体要求”

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》

本文件的7.1.3.10、8.1.3.11、9.1.3.11个人信息保护参考《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》，经研究对个人信息保护安全进行分等级管理，结合具体的场景应用，给出了不同网络安全等级的个人信息保护要求。

2.与国内领先、国际先进标准的对标情况

目前在国内外，信息安全已有相应的标准，未查到“多功能智能杆　网络安全等级保护规范”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安全的发布，但基本上都是网络安全等级保护通用技术标准，或者都是特定领域，如公安系统、广播电视、证券期货、民用航空、金融、林业的网络安全等级保护专用技术标准。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网络安全等级保护。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，比国内外的信息安全标准的内容细化和精准。

国外

1、ISO/IEC TR 13335-5-2001信息技术　IT安全管理导则　网络安全管理导则

2、ISO/IEC 18028-4-2005 信息技术　安全技术 IT网络安全第4部分：安全远程入网

3、ISO/IEC 27033-4-2014 信息技术　安全技术　IT网络安全

第 3 部分：用安全通道保证网络间通信

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 36627-2018 信息安全技术　网络安全等级保护测试评估技术指南

9、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

10、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

行业标准

1、GA/T 1349-2017 信息安全技术　网络安全等级保护专用知识库接口规范

2、GA/T 1735.1-2020 网络安全等级保护检查工具技术规范　第1部分：安全通用检查工具

3、GA/T 1389-2017 信息安全技术　网络安全等级保护定级指南

4、GA/T 1390.2-2017 信息安全技术　网络安全等级保护基本要求 第2部分：云计算安全扩展要求

5、GA/T 1390.3-2017 信息安全技术　网络安全等级保护基本要求 第3部分：移动互联安全扩展要求

6、GA/T 1390.5-2017 信息安全技术　网络安全等级保护基本要求 第5部分：工业控制系统安全扩展要求

7、GY/T 352-2021 广播电视网络安全等级保护基本要求

8、GY/T 337-2020 广播电视网络安全等级保护定级指南

9、JR/T 0060-2021 证券期货业网络安全等级保护基本要求

10、JR/T 0067-2021 证券期货业网络安全等级保护测评要求

11、JR/T 0071.1-2020 金融行业网络安全等级保护实施指引 第1部分：基础和术语

12、JR/T 0071.2-2020 金融行业网络安全等级保护实施指引　第2部分：基本要求

13、JR/T 0071.3-2020 金融行业网络安全等级保护实施指引　第3部分：岗位能力要求和评价指引

14、JR/T 0071.4-2020 金融行业网络安全等级保护实施指引　第4部分：培训指引

15、JR/T 0071.5-2020 金融行业网络安全等级保护实施指引　第5部分：审计要求

16、JR/T 0071.6-2020 金融行业网络安全等级保护实施指引　第

6 部分：审计指引

17、JR/T 0072-2020 金融行业网络安全等级保护测评指南

18、LY/T 2929-2017 林业网络安全等级保护定级指南

19、MH/T 0076-2020 民用航空网络安全等级保护基本要求

四、主要条款的说明以及主要技术指标、参数、试验验证的论述

1. 主要条款的说明

本文件主要内容包括：第 1 章范围、第 2 章规范性引用文件、第 3 章术语和定义、第 4 章缩略语、第 5 章网络安全等级保护、第 6 章第一级安全要求、第 7 章第二级安全要求、第 8 章第三级安全要求、第 9 章第四级安全要求、第 10 章第五级安全要求、附录 A（规范性）安全要求的选择和使用、附录 B（规范性）等级保护对象整体安全保护能力的要求、附录 C（规范性）等级保护安全框架和关键技术使用要求、附录 D（规范性）管理平台应用要求、附录 E（规范性）移动互联应用场景要求、附录 F（规范性）挂载设备应用场景要求、附录 G（规范性）密码模块安全技术要求、附录 H（规范性）可信验证要求、参考文献。具体说明如下：

3）术语和定义

多功能智能杆、多功能智能杆网络安全、安全保护能力、管理平台、平台服务商、平台服务客户、虚拟机监视器、宿主机 移动互联、移动终端、无线接入设备、无线接入网关、移动应用软件、等级保护对象、外部网络、公共数据、敏感数据、数据安全、挂载设备、边缘控制器、密码模块 21 个术语。

4）缩略语

列出了本文件中使用的 AP、DDoS、HTTPS、IaaS、IP、IT、PaaS、SaaS、SSID、SSH、TCB、VPN、WEP、WPS 共 14 项缩略语。

5）网络安全等级保护

5.1 明确了等级保护对象定级。

5.2 列举不同等级的安全保护能力。

5.3 提出安全通用要求。

5.4 提出安全扩展要求。

5.5 提出密码模块安全要求。

5.6 提出安全管理要求。

6）第一级安全要求

目前的等级保护对象（信息系统）的安全级别分为五个等级：1 级为最低级别，5 级为最高级别（5 级为预留级别，市面上已定级的系统最高为 4 级）。

系统级别的确定需要根据系统的重要性进行决定。如果定高了，有可能造成投资的浪费；定低了则有可能造成重要信息系统得不到应有的保护，应该谨慎定级。

一级系统简单，不需要备案，影响程度很小，自主进行保护即可，定 2 级以上就需要进行等级测评。

四级系统量级较大，比如支付宝、银行总行系统、国家电网系统。

五级系统属国家级、国防类的系统，比如核电站、军用通信系统。

6.1　安全通用要求

6.2　管理平台安全要求

6.3　移动互联安全要求

6.4　挂载设备安全要求

6.5　公共数据安全要求

一级系统简单，不需要备案，影响程度很小，自主进行保护即可，

7）第二级安全要求

7.1　安全通用要求

7.2　管理平台安全要求

7.3　移动互联安全要求

7.4　挂载设备安全要求

7.5　公共数据安全要求

章节同6.1、6.2、6.3、6.4和6.5但具体条款内容，按照等级要求不同，第二级安全要求需要进行等级测评。

8）第三级安全要求

8.1　安全通用要求

8.2　管理平台安全要求

8.3　移动互联安全要求

8.4　挂载设备安全要求

8.5　公共数据安全要求

章节同6.1、6.2、6.3、6.4和6.5但具体内容要求不同，第三级安全要求需要进行等级测评。

9）第四级安全要求

9.1　安全通用要求

9.2　管理平台安全要求

9.3　移动互联安全要求

9.4　挂载设备安全要求

9.5　公共数据安全要求

章节同6.1、6.2、6.3、6.4和6.5但具体内容要求不同。

第四级安全要求需要进行等级测评，且系统量级较大，比如支付宝、银行总行系统、国家电网系统。

10）第五级安全要求

第五级等级保护对象是非常重要的监督管理对象，对其有特殊的管理模式和安全要求，所以不在本文件中进行描述。

11）附录A（规范性）　安全要求的选择和使用

由于等级保护对象承载的业务不同，对其的安全关注点会有所不同，有的关注信息的安全性，有的关注业务的连续性。

12）附录B（规范性）　等级保护对象整体安全保护能力的要求

网络安全等级保护的核心是保证不同安全保护等级的对象具有相适应的安全保护能力。

13）附录C（规范性）　等级保护安全框架和关键技术使用要求

在开展网络安全等级保护工作中应首先明确等级保护对象，多功能智能杆网络安全等级保护对象主要包括信息系统、挂载设备和数据资源；确定了等级保护对象的安全保护等级后，应根据不同对象的安全保护等级完成安全建设或安全整改工作；应针对等级保护对象特点建立安全技术体系和安全管理体系，构建具备相应等级安全保护能力的网络安全综合防御体系。

14）附录D（规范性）　管理平台应用要求

多功能智能杆的管理平台由设施（杆体及挂载终端）、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件等组成。

15）附录E（规范性）　移动互联应用场景要求

移动互联安全扩展要求主要针对移动终端、移动应用和无线网络

部分提出特殊安全要求，与安全通用要求一起构成对采用移动互联技术的等级保护对象的完整安全要求。

16）附录F（规范性）　挂载设备应用场景要求

多功能智能杆通过挂载设备实现外部环境感知功能，挂载设备应根据其设备功能进行具体部署。

17）附录G（规范性）　密码模块安全技术要求

密码模块安全技术要求分为四级，一级密码模块是基础级，提供了最低等级的安全要求，二级密码模块在安全一级的基础上增加了拆卸证据、基于角色的鉴别等功能要求，三级密码模块在安全二级的基础上，增强了物理安全、身份鉴别、环境保护、非入侵式攻击缓解、敏感参数管理等安全机制，四级密码模块是标准中的最高安全等级。

18）附录H（规范性）　可信验证要求

可信验证是基于可信根，构建信任链，一级度量一级，一级信任一级，把信任关系扩大到整个计算节点，从而确保计算节点可信的过程。

2.主要技术指标、参数、试验验证

1）物理安全

多功能智能杆挂载设备的物理安全要求包括抗破坏性能、防水、防尘、防腐蚀等，这些要求可根据具体应用场景和环境而变化。

2）认证和身份验证

多功能智能杆挂载设备要支持各种身份验证方法，如用户名和密码、双因素认证等，以确保只有授权人员可以访问设备。

3）数据加密

要求多功能智能杆挂载设备支持数据的加密传输，以保护数据在

传输过程中的机密性。

4）漏洞管理和安全更新

要求多功能智能杆挂载设备制造商提供漏洞管理和安全更新机制，以及及时修补已知漏洞。

4）访问控制和权限管理

多功能智能杆挂载设备应该支持细粒度的访问控制和权限管理，以确保只有授权的用户可以执行特定操作。

5）日志记录和审计

多功能智能杆挂载设备应记录关键事件和活动，以便进行审计和调查。

6）网络安全协议

多功能智能杆的挂载设备要支持安全的通信协议，如 HTTPS、SSH 等，以防止数据被恶意截取或篡改。

7）漏洞和弱点扫描

要求进行定期的漏洞扫描和弱点评估，以发现和解决潜在的安全问题。

8）物理安全性测试

对多功能智能杆的物理组件，要进行一些物理安全性测试，以评估其抗破坏性能。

9）渗透测试

进行渗透测试以模拟潜在的网络攻击，并评估多功能智能杆的安全性。

10）合规性验证

根据法律、法规和国家标准，要进行合规性验证，以确保多功能

智能杆符合适用的法规和标准。

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、标准发布实施后，在相关专业媒体上宣传《多功能智能杆 网络安全等级保护规范》。

2、通过有关会议介绍《多功能智能杆　网络安全等级保护规范》。

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