ICS 35.020

CCS A 0

团 体 标 准

T/BJ I0T002—2023

物联网研发中心建设规范

Specification for construction of Internet of Things R & D Center

2023 - XX - XX 发布

2023 - XX - XX 实施

北京物联网智能技术应用协会 发 布

T/BJ I0T002—2023

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分： 标准化文件的结构和起草规则》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专利的责任。

本文件由北京物联网智能技术应用协会提出并归口。

本文件起草单位：北京惠企易点通科技有限公司、岭博科技（北京）有限公司、北京盈创力和电子 科技有限公司、新汽有限公司、帝益喜（北京）科技有限公司、北京流金岁月传媒科技股份有限公司、 北京特恩迈测控技术有限公司、领雁科技（上海）有限公司、和晟嘉信（北京） 科技有限公司、中科航 宇（北京） 自动化工程技术有限公司、北京龙德缘电力科技发展有限公司。

本文件主要起草人：

T/BJ I0T002—2023

引 言

为贯彻创新驱动发展战略，落实《中共中央 国务院关于深化科技体制改革加快国家创新体系建设 的意见》《物联网新型基础设施建设三年行动计划（2021-2023年） 》（工信部联科〔2021〕130号） ， 加快推动物联网产业创新发展， 更好发挥物联网赋能实体经济高质量发展的作用， 引导和支持企业增强 技术研发创新能力， 健全技术研发创新市场导向机制，特制订本规范。

T/BJ I0T002—2023

物联网研发中心建设规范

1 范围

本文件规定了物联网研发中心建设的基本原则、要求、信息安全、设备维护、网络运维及网络安全 管理标准。

本文件适用于物联网研发中心的建设和评价。

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。

GB 15630 消防安全标志设置要求

GB/T 20269 信息安全技术 信息系统安全管理要求

GB/T 20270 信息安全技术 网络基础安全技术要求

GB/T 20271 信息安全技术 信息系统通用安全技术要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 26189 室内工作场所的照明

GB/T 33200 社会治安综合治理 综治中心建设与管理规范

GB 50016 建筑设计防火规范(附条文说明)

GB 50068 建筑结构可靠性设计统一标准

GB 50140 建筑灭火器配置设计规范(附条文说明)

GB 55037 建筑防火通用规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

物联网研发中心 Internet of Things R & D Center

指负责物联网技术领域研发工作的研究发展中心。

3.2

网络运维 Network operation and maintenance

指对物联网研发中心各种网络设备（F5负载均衡设备、防火墙、各级交换机等）进行维护、调试， 及时处理网络运行故障， 保证网路环境的正常运行。

3.3

网络安全 Network security

指通过网络监控等手段能及早发现网络中存在的隐患并及时解决，对现有网络提出更好的安全防范 措施。能及时发现IT架构的隐患，是否存在风险。能将让目前与未来的业务系统更高效稳定运行，并把 应用和服务更快速、高效、安全地交付到客户端。

4 基本原则

4.1 安全性

T/BJ I0T002—2023

应保证物联网研发中心的设施安全、运行安全和信息安全，信息安全保护能力应符合 GB/T 22239 规定的第一级安全保护等级要求。

4.2 可靠性

应注重设备选型、专业软件研发及实现技术的协调性和可靠性，确保研发中心整体运行稳定。

4.3 先进性

在保证研发中心建设的安全性和可靠性前提下，在设备选型、软件研发方面还应注重设备、技术的 先进性，确保设备技术目前是领先的。

5 要求

5.1 申请创建

物联网研发中心申请创建材料内容应包括： 《物联网研发中心申请报告》（见附录A）、物联网研 发中心申请表及必要证明材料（见附录B）。

5.2 选址

应符合区域规划的要求， 充分利用现有资源和服务设施， 避免重复建设或过于集中。

5.3 建筑结构

按 GB 50068 的要求，物联网研发中心建筑结构的安全等级应为二级或二级以上。

5.4 环境条件

5.4.1 机房应在明显处设置区域标识。

5.4.2 机房装饰风格简洁明快， 装修严禁采用易燃材料， 地板应具有良好的防静电、防老化、耐火及 防龟裂性能。

5.4.3 机房出入口处应设置门禁系统， 根据运维人员身份设置权限， 并进行出入登记。

5.4.4 机房应设置全方位实时图像监控系统，定期保存图像记录。

5.4.5 机房应采用上走线方式， 机房应设置上走线架和光纤尾纤专用线槽， 交流电缆、直流电缆、信 号电缆严禁交叉混走，应有清晰标识。

5.4.6 机房应设置动力环境监控系统， 采用智慧运维提高机房环境的安全性和稳定性，节能运维。

5.5 设施要求

5.5.1 电力设施

<5.5.1.1> 应配备室内照明系统，并符合 GB/T 26189 的规定。

<5.5.1.2> 宜配备不间断电源系统。

5.5.2 消防设施

<5.5.2.1> 应配备消防器材，消防器材放置位置应合理、醒目，并保持完整， 消防器材的配置应符合 GB 50140 的规定。

<5.5.2.2> 应配备防火灭火系统，设置应急逃生通道和消防安全标志，防火灭火系统应符合 GB 50016、 GB 55037 的规定， 消防安全标志设置应符合 GB 15630 的规定。

5.5.3 安全设施

中心楼道、台阶、管道井、配电箱应设置防滑、防摔、防触电标识提醒，必要时安装防护装置。

5.5.4 视频监控设施

<5.5.4.1> 研发中心应配备指挥调度显示系统，含显示大屏及其相关配套设备，显示屏尺寸应不小于 150 英寸， 显示比例宜按照标准 16:9 或其整倍数设计。

<5.5.4.2> 研发中心应配备不少于 2 台视频会议设备，设备至少具备 1080P 高清传输能力。

T/BJ I0T002—2023

<5.5.4.3> 研发中心应根据环境合理配备视频监控系统，监控设施应符合 GB/T 33200 中关于公共安全 视频监控建设联网应用的要求。

<5.5.4.4> 研发中心应根据需求配备移动终端，应能通过移动端应用将现场的视频、语音接入中心，实 现互联互通。

5.5.5 布线要求

<5.5.5.1> 在机房各功能区统一设置综合布线系统。

<5.5.5.2> 综合布线系统应采用双星型拓扑结构， 该结构下的每个分支子系统都是相对独立的单元，对 每个分支单元系统改动都不影响其他子系统。

<5.5.5.3> 综合布线系统选用的电缆、光缆、各种连接电缆、跳线， 以及配线设备等所有硬件设施，均 应符合标准规定，布线整齐、规范、编号统一。

6 信息安全

6.1 网络安全等级保护应不低于 GB/T 22239 中第二级安全要求。

6.2 信息系统安全应符合 GB/T 20269 的要求。

6.3 网络基础安全应符合 GB/T 20270 的要求。

6.4 信息系统安全通用技术要求应符合 GB/T 20271 的要求。

7 设备维护

7.1 机房系统应采用物联网技术对机房环境、温度、湿度、设备运行等进行实时在线监视，所有数据 具有历史记录功能，能与整个机房智能运维系统进行融合。同时，配备机房运维人员，定期巡视机房， 对机房环境、温度、湿度、设备运行等进行登记和监视。运维人员对机房内的设施、设备及工具负有管 理责任，在巡视检查机房时，应对机房内通信设备、用户设备、认真检查，发现问题及时与相关人员联 系处理。

7.2 物联网研发中心应对各类网络设备的运行状况、系统性能进行监控。被监控的设备包括硬件防火墙 、网络核心交换机、汇聚交换机、接入交换机等各类设备，实时监测设备的性能、运行情况、系统资源等 , 统计分析设备对业务的承装能力。

7.3 物联网研发中心应对机房外部接入至网络设备的互联链路、机房各网络设备之间的互联链路、核 心交换机至本地骨干网之间的互联链路的流量监控，用以分析、统计网络带宽资源的利用率、趋势、模 型和业务流量以及发现网络的异常流量及时发现网络故障。

7.4 应设置机房智慧运维系统，包括机房环境监测、机房能耗监测、机房安全管理、机房设备管理、 机房维护管理、机房运维管理、数据分析和决策支持等内容。

8 网络运维及网络安全管理标准

8.1 职责

8.1.1 网络安全和信息化领导小组职责

<8.1.1.1> 贯彻落实中央网络安全和信息化领导小组战略部署，统筹协调物联网研发中心网络安全重大

问题。

<8.1.1.2> 研究制定物联网研发中心网络安全发展战略、宏观规划和重大政策。

<8.1.1.3> 保障网络安全所需的资金、人员、设备与设施等资源。

8.1.2 信息部部长职责

<8.1.2.1> 贯彻实施国家法律、法规、规章以及上级单位的相关标准与制度。

<8.1.2.2> 审批物联网研发中心网络运维及网络安全故障处置方案。

<8.1.2.3> 监督物联网研发中心网络运维及网络安全故障处置方案的实施。

8.1.3 信息部网络及硬件运维岗职责

T/BJ I0T002—2023

<8.1.3.1> 对网络及信息系统运行情况进行日常巡查。

<8.1.3.2> 判断、分析网络运维及网络安全问题提出解决方案。

<8.1.3.3> 组织、实施通过审批的网络运维及网络安全问题解决方案。

8.2 网络运维及网络安全管理的目的与风险

8.2.1 物联网研发中心网络运维及网络安全管理的目的是保障物联网研发中心网络及信息系统的正常 运行， 提高网络及信息系统运行的稳定性、安全性。

8.2.2 物联网研发中心网络运维及网络安全管理的原则包括：

a) 合法合规原则： 网络运维及网络安全管理标准应符合国家法律法规和相关政策的要求；

b) 快速处置原则： 网络运维及网络安全管理标准的制定应遵循快速响映， 及时处理的原则，将 对各业务部门及业务系统的影响降到最低。

8.2.3 物联网研发中心网络运维及网络安全管理的关键绩效指标包括：

a) 发现监控警告或接收业务部门报障的及时性；

b) 网络及硬件运维岗解决故障的数量及时效性；

c) 网络及信息系统运行的稳定性。

8.2.4 物联网研发中心网络运维及网络安全管理需应对的主要风险包括：

a) 发现监控警告或收到各业务部门的报障不及时；

b) 网络及硬件运维岗判断是否能够自行快速处理有误，引起网络及信息系统问题处理滞后。

8.2.5 物联网研发中心网络运维及网络安全管理风险控制矩阵见附录 C 中表 C.1。

8.3 网络运维及网络安全管理内容

8.3.1 网络及信息系统日常运行情况巡查

<8.3.1.1> 网络及硬件运维岗每日进行一次网络及信息系统运行情况的检查。

<8.3.1.2> 当网络及硬件运维岗接收业务部门报障信息或发现网络安全监控设备发出警告，登记信息类 型、发生时间等，随即进入处理过程。

<8.3.1.3> 当网络及硬件运维岗没有接收到业务部门报障且网络安全监控设备一切正常，则结束此次巡

查。

8.3.2 网络运维及网络安全故障解决方案制定

网络及硬件运维岗根据出现的故障或安全问题进行判断， 属于一般问题的及时编制整改方案，属于 特殊问题，无法自行处理时及时联系相关技术团队及分包维护单位，专业技术团队进行技术检测，查找 问题原因， 提出切实可行的方案，提交信息管理部负责人进行审批。

8.3.3 网络运维及网络安全故障处理

网络及硬件运维岗根据已经审批通过的方案，在专业技术团队的配合下，即时解决网络及信息系统 故障。解决后形成网络运维及网络安全问题处置登记表，如表 1 所示。

表1 网络运维及网络安全问题处置登记表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 报障时间 | 报障部门 | 报障人员 | 故障类型 | 解决方案 | 解除故障时间 | 备注 |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |
| 制表人： | | | | | | | |

T/BJ I0T002—2023

N

8.4 网络运维及网络安全管理权限

网络运维及网络安全管理权限指引表见表 2 。

表2 网络运维及网络安全管理权限指引表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 事项 | 责任部门 | 集团信息部 | | 相关单位 |
| 网络及硬件运维岗 | 部长 | 技术人员 |
| 1 | 对网络及信息系统日常运行情况进行巡查 | 集团信息部 | 执行 |  |  |
| 2 | 网络及硬件运维岗判断是否能够自行快速处理 | 集团信息部 | 执行 |  |  |
| 3 | 提出解决方案 | 集团信息部 | 拟定 | 审批 | 拟定 |
| 4 | 解决问题 | 集团信息部 | 组织/执行 | 监督 | 执行 |

8.5 流程

网络运维及网络安全管理流程如图 1 所示，网络运维及网络安全管理流程说明表见附录C中表C.2。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 网络运维及网络安全管理流程 | | | | | | | | | | | | | | |
| 阶段 | 集团信息部部长 | | | | | | 网络及硬件运维岗 | | | 专业技术团队及检测单位 | | | | 输出文档 |
|  | | | | | | 01  Y  3.运维人员判断是  否能够自行快速处  理  2.对网络及信息系  统日常运行情况进  行巡查  1.开始    02  Y | | |  | | | | 01  警告信息及故障信  息跟踪表  02  故障解决及业务回  复报告 |
|  | N | 03 | | | |
|  | 4.针对特殊问题 进行检测，分析 | |  |
|  |
|  |  | |
|  | 5.提出解决问题方 案 |  |
|  | | | |
| |  | | --- | | 7.信息部及相关技  术支持单位及时解  决存在问题 |   8.结束 | | |
|  | | 6. 审批 | |  |
|  |
|  | | |  | |
|  | | | | |
|  | | | | |

图1 网络运维及网络安全管理流程图

T/BJ I0T002—2023

附 录 A

（规范性）

《物联网研发中心申请报告》

A.1 物联网研发中心基本情况

包括物联网研发中心的建设与发展历程、组织结构；创新体系建设和运行机制，包括组织管理体系 建设、规章制度建立、研发项目组织管理机制、研发经费管理机制、人才激励机制、内外部合作机制等。

A.2 物联网研发中心研发开发工作开展情况

包括重大产品创新、产学研合作、与龙头企业间合作、在产业链中所处地位、国际化研发活动、特 色项目、吸引社会资本或政府基金参与研发成果转化情况等。

A.3 物联网研发中心主要创新成果

形成的核心技术及自主知识产权情况，重点介绍相关技术成果对研发中心核心产品研发、核心竞争 力提升的支撑作用，以及取得的经济社会效益。通过自主研发形成的物联网技术产品，以及相关产品的 落地转化及应用情况。

A.4 物联网研发中心未来三年建设目标

在技术创新方面拟实施的重点措施， 包括创新条件建设、创新人才集聚、重点研发项目部署等。

T/BJ I0T002—2023

附 录 B

（规范性）

物联网研发中心申请表

B.1 物联网研发中心申请表

如表 B.1 所示。

表B.1 物联网研发中心申请表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 第一部分 申请单位基本情况 | | | | | |
| 企业名称 | |  | | | |
| 登记注册时间 | |  | 登记注册类型 | |  |
| 企业性质 | |  | 是否上市公司 | |  |
| 注册地址 | |  | 法定代表人 | |  |
| 注册资本 | |  | 注册币种 | |  |
| 办公地址 | |  | 下属企业数量 | |  |
| 统一社会信用代码 | |  | | | |
| 纳统行业代码 | |  | 所属行业 | |  |
| 所属领域 | | 新一代信息技术（）集成电路（）医药健康（）智能装备()  节能环保（）新能源智能汽车（）新材料（）人工智能()  软件和信息服务（）科技服务业（）建筑业（）其他() | | | |
| 主营业务 | |  | | | |
| 第二部分 研发中心基本情况 | | | | | |
| 研发中心成立时间 | |  | 研发中心场地面积 | |  |
| 自主研发物联网技术产品数 量 | |  | 自主研发物联网技术产品是 否实现落地转化应用 | | ○是 ○否 |
| 研发中心负责人 | |  | 联系方式 | |  |
| 研发中心联系人 | |  | 联系方式 | |  |
| 固定电话 | |  | 电子邮件 | |  |
| 申请建设前1年内是否发生重大安全、重大质量事故或严重环境违法行为 | | | | | ○是 ○否 |
| 是否运营和财务状况良好， 拥有筹措研发中心建设运行资金的能力， 能够支撑保障研发 中心可持续运行 | | | | | ○是 ○否 |
| 是否已获得省级以上技术（制造业、产业）创新中心、工业设计中心、工程（技术）研 究中心、企业技术中心等创新平台认定 | | | | | ○是 ○否 |
| 序号 | 指标名称 | | | 单位 | 数据值 |
| 1 | 主营业务收入 | | | 万元 |  |
| 2 | 研发经费支出 | | | 万元 |  |
| 3 | 研发人员数 | | | 人 |  |
| 4 | 技术开发仪器设备原值 | | | 万元 |  |
| 5 | 拥有的全部有效知识产权数 | | | 项 |  |
| 6 | 近三年获得的有效知识产权数 | | | 项 |  |
| 7 | 近三年获得的有效专利数 | | | 项 |  |
| 8 | 近三年获得的有效发明专利数 | | | 项 |  |
| 9 | 近三年获得的全部有效软件著作权登记数 | | | 项 |  |
| 10 | 全部研发项目数 | | | 项 |  |
| 11 | 自主研发形成的物联网技术产品 | | | 个 |  |
| 12 | 近三年主持和参加制定的国际、国家、行业、地方、团体、 企业标准数 | | | 项 |  |
| 13 | 获国家自然科学、技术发明、科技进步奖项目数 | | | 项 |  |
| 14 | 获省部级科技进步奖项目数 | | | 项 |  |
| 15 | 是否为国家标准化试点项目承担单位 | | | 是/否 |  |
| 16 | 国家级研发平台数 | | | 个 |  |

T/BJ I0T002—2023

表B.1 （续）

|  |  |  |  |
| --- | --- | --- | --- |
| 17 | 省级研发平台数 | 个 |  |
| 18 | 开展网络安全等级保护评估 | 是/否 |  |
| 19 | 通过国家（国际组织）认证的实验室和检测机构数 | 个 |  |
| 20 | 获国家自然科学、技术发明、科技进步奖项目数 | 项 |  |
| 21 | 获省部级科技进步奖项目数 | 项 |  |
| 注： 1）纳统行业代码：对照《国民经济行业分类与代码(GB/T 4754—2017)》，填写企业主营业务对应的统计“小 类”（四位码）编号。  2）自主研发形成的物联网技术产品：报告年度内企业通过自主研发形成的物联网相关领域技术产品总件数。 | | | |

B.2 需提供的必要证明材料及其他材料

B.2.1 必要证明材料

B.2.1.1 相关财务报表、统计报表和知识产权证明材料。

B.2.1.2 相关财务报表主要包括： 资产负债表、利润表、现金流量表；如果申报主体是集团，需提供

研发中心所在企业总部和其下属分公司、子公司、控股企业（按实际控投权）等的会计合并报表。 B.2.1.3 相关统计报表主要为带统计局水印的“企业研究开发活动及相关情况表”。

B.2.1.4 相关知识产权证明材料主要包括：近三年企业获得的知识产权证明材料（专利授权证书、软 件著作权证书）。

B.2.1.5 其他材料： 表 B.2-8。

表B.2 研发经费情况表

|  |  |  |
| --- | --- | --- |
| 研发经费情况 | | 金额（万元） |
| 人员人工费用 | |  |
| 直接投入费用 | |  |
| 折旧费用与长期待摊费用 | |  |
| 无形资产摊销费用 | |  |
| 设计费用 | |  |
| 装备调试费用与试验费用 | |  |
| 委托外部研究开发费用 | 委托境内研究机构 |  |
| 委托境内高等学校 |  |
| 委托境内企业 |  |
| 委托境外机构 |  |
| 其他费用 | |  |
| 注1：如果申报主体是母公司，此表各项内容应与母公司向统计部门报送的“企业研究开发活动及相关情况表”内 容一致，单位应由千元换算成万元，“金额”一栏只填写数字即可。  注2：如果申报主体是集团， 此表应为纳入表B.2中评价数据统计范围表中的所有单位的合并报表， 表中各项内容应 为企业母公司、分公司、子公司、控股公司分别向统计部门报送的“企业研究开发活动及相关情况表”的相 关内容的合并，单位应由千元换算成万元，“金额”一栏只填写数字即可。 | | |

T/BJ I0T002—2023

表B.3 全部研发项目信息表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 项目来源 | 项目起始日 期 | 项目完成日 期 | 跨年项目当 年所处主要 进展阶段 | 项目研究开 发人员（人） | 项目经费支 出（万元） | 政府资金 |
| 1 |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |  |
| n |  |  |  |  |  |  |  |  |
| 注1：项目来源应按相应的分类填写， 具体的分类是： 1.研发中心自选项目； 2.政府部门科技项目； 3.其他企业（单 位）委托项目； 4.境外项目； 5.其他项目。  注2：跨年项目当年所处主要进展阶段应按相应的分类填写，具体的分类是：1.研究阶段；2.小试阶段；3.中试阶 段； 4.试生产阶段。 | | | | | | | | |

表B.4 拥有的全部有效知识产权信息表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 知识产权名称 | 知识产权类型 | 授权国别 | 授权号 | 是否PCT专利 | 授权公告日 | 所有人 |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |
| n |  |  |  |  |  |  |  |
| 注1：该表所填写信息应与相关知识产权证书内容一致。  注2：知识产权类型应按相应的分类填写：1.发明专利；2.实用新型；3.外观设计；4.软件著作权；5.集成电路布 图设计； 6.植物新品种； 7.临床试验许可； 8.药品注册证书；9.其他。 | | | | | | | |

表B.5 省级及以上研发平台信息表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 级别 | 主管部门 | 平台类型 | 批复文号 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| … |  |  |  |  |  |
| n |  |  |  |  |  |
| 注： 平台类型应按相应的分类填写， 具体的分类是： 1.工程实验室； 2.工程研究中心； 3.工程技术研究中心； 4.重 点实验室； 5.国家地方联合工程实验室； 6.国家地方联合工程研究中心； 7.其他（需具体说明）。 | | | | | |

表B.6 国家（国际组织）认证实验室和检测机构信息表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 类型 | 发证机关 | 证书号 | 有效期 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| … |  |  |  |  |  |
| n |  |  |  |  |  |
| 注1： “类型”指认证认可类型，应按相应的分类填写，具体的分类是： 1.CNAS；2.CMA；3.CAL；4.其他（需具体 说明）。  注2：认证机关应按相应的分类填写， 具体的分类是：1. 中国合格评定国家认可委员会（CNAS）； 2. 国家认证认 可监督管理委员会（CNCA）； 3. 其他国家（国际组织）认证认可机构（需具体说明）。 | | | | | |

T/BJ I0T002—2023

表B.7 获国家、省（市）部级奖励信息表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 奖励类型 | 奖励级别 | 证书号 | 获奖者 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| … |  |  |  |  |  |
| n |  |  |  |  |  |
| 注： “奖励类型”应按相应的分类填写， 具体的分类是： 1. 国家自然科学奖； 2.国家技术发明奖； 3. 国家科技进 步奖； 4.省部科技进步奖；5.中国专利奖； 6.工业企业知识产权运用试点企业； 7.国家标准化试点项目承担单 位； 8.全国质量标杆等。 | | | | | |

表B.8 已制定和拟制定的标准信息表

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 标准类别 | 标准类型 | 标准项 数 | 标准名称 | 标准号 | 发布日期 | 主持或参 加 | 标准制定 主导单位 | 所属产业 领域 | 标准涉及  的产品或  服务 | 标准编制  过程中存  在哪些问  题 | 需要政府  提供哪些  支持 |
| 全部已编 制 标 准 （请按照 发布日期 从晚至早 顺 序 填 写） | 国际标准 |  | 标准1名称： |  |  |  |  |  |  |  |  |
| 标准2名称： |  |  |  |  |  |  |  |  |
| 国家标准 |  | 标准1名称： |  |  |  |  |  |  |  |  |
| 标准2名称： |  |  |  |  |  |  |  |  |
| 地方标准 |  | 标准1名称： |  |  |  |  |  |  |  |  |
| 标准2名称： |  |  |  |  |  |  |  |  |
| 行业标准 |  | 标准1名称： |  |  |  |  |  |  |  |  |
| 标准2名称： |  |  |  |  |  |  |  |  |
| 团体标准 |  | 标准1名称： |  |  |  |  |  |  |  |  |
| 标准2名称： |  |  |  |  |  |  |  |  |
| 企业标准 |  | 标准1名称： |  |  |  |  |  |  |  |  |
| 标准2名称： |  |  |  |  |  |  |  |  |
| 未来三年 拟编制标 准 | 国际标准 |  | 标准1名称： |  |  |  |  |  |  |  |  |
| 标准2名称： |  |  |  |  |  |  |  |  |
| 国家标准 |  | 标准1名称： |  |  |  |  |  |  |  |  |
| 标准2名称： |  |  |  |  |  |  |  |  |
| 地方标准 |  | 标准1名称： |  |  |  |  |  |  |  |  |
| 标准2名称： |  |  |  |  |  |  |  |  |
| 行业标准 |  | 标准1名称： |  |  |  |  |  |  |  |  |
| 标准2名称： |  |  |  |  |  |  |  |  |
| 团体标准 |  | 标准1名称： |  |  |  |  |  |  |  |  |
| 标准2名称： |  |  |  |  |  |  |  |  |
| 企业标准 |  | 标准1名称： |  |  |  |  |  |  |  |  |
| 标准2名称： |  |  |  |  |  |  |  |  |
| 注1：所填标准应为现行有效标准。  注2：所属产业领域请按照十大高精尖产业（新一代信息技术、集成电路、医药健康、智能装备、节能环保、新能 源智能汽车、新材料、人工智能、软件和信息服务、科技服务）、建筑、其他来分类填写。 | | | | | | | | | | | |

T/BJ I0T002—2023

附 录 C

（规范性）

网络运维及网络安全管理

表C.1 网络运维及网络安全管理风险控制矩阵

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 风险编号 | 风险描述 | 风险类别 | 发生概率 | 影响程度 | 风险等级 | 控制编号 | 控制点 | 控制措施 | 责任部门 |
| R01 | 发现监控警告或 收到各业务部门 报障不及时 | 运营 | 3 | 4 | 高 | C01 | 巡查 | 【C01】  每日增加一次机 动巡查， 充分做到 及时了解网络及 信息系统运行情 况，增设自动化巡 检报警设备 | 集团信息 部 |
| R02 | 网络及硬件运维 岗判断是否能够 自行快速处理可 能存在差异，从 而有可能引起时 效性问题 | 运营 | 3 | 3 | 中等 | C02 | 判断 | 【C02】  通过建立应急预 案的形式加快对 问题的判断， 即时 给出解决方案 | 集团信息 部 |
| R03 | 及时按照经过审 批的解决方案处 理问题 可能在 过程中临时采用 未经审批的技术 手段 | 运营 | 2 | 3 | 中等 | C03 | 审批 | 【C03】  提出的解决问题 措施尽可能多的 涵盖各种可能使 用的技术手段 | 集团信息 部 |
| 注1：风险类别：按性质分别选填战略、财务、市场、运营、法律。  注2：发生概率按从小到大分为1～5级，影响程度按事项对本流程控制目标的影响严重程度从低到高分为1～5级。  注3：风险等级划分标准：极高风险、高风险、中风险、低风险、极低风险。风险判定标准：极低风险：风险评分  <3分； 低风险： 3分≤风险评分<6分； 中等风险：6分≤风险评分<12分；高风险：12分≤风险评分<20分； 极 高风险：风险评分≥20分（风险评分=发生概率×影响程度）。 | | | | | | | | | |

表C.2 网络运维及网络安全管理流程说明表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 流程步骤 | 步骤说明 | 时限 | 主责部门 | 重要输入 | 重要输出 |
| 1 | 开始 | 按照集团公司所属各部门业务要求对网 络及网络安全进行相应等级设置程序、 确定网络正常运行后刻启动此流程。 | 即时 | 集团信息部 |  |  |
| 2 | 对网络及信息系统日 常运行情况进行巡查 | 【C01】  网络运维管理员每日进行一次网络及信 息系统运行情况的检查。  当网络及硬件运维岗接收业务部门报障 信息或发现网络安全监控设备发出警 告，登记信息类型、发生时间，进入步 骤 3。  当网络及硬件运维岗没有接收到业务部 门报障且网络安全监控设备一切正常， 进入步骤 8，结束此流程。  每日增加一次机动巡查，充分做到及时 了解网络及信息系统运行情况，增设自 动化巡检报警设备。 | 即时 | 集团信息部 |  | 警告信息及故 障信息跟踪表 |

T/BJ I0T002—2023

表C.2 （续）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 流程步骤 | 步骤说明 | 时限 | 主责部门 | 重要输入 | 重要输出 |
| 3 | 网络及硬件运维岗判  断是否能够自行快速  处理 | 【C02】  对于出现的网络及系统运行问题进行判 断，属于常见一般问题能够自行处理的， 进入步骤 5。  属于特殊问题的即时联系相关技术团队 及分包维护部门，进入步骤 4。  控制措施：通过建立应急预案的形式加 快对问题的判断，即使给出解决方案。 | 即时 | 集团信息部 |  |  |
| 4 | 针对特殊问题进行检 测，分析 | 专业技术团队及检测机构对特殊问题进 行检测分析，查找问题原因。 | 1天 | 专业技术团队 及检测机构 |  |  |
| 5 | 提出解决方案 | 针对出现的问题， 提出切实可行的方案。 | 1天 | 集团信息部 |  |  |
| 6 | 审批 | 【C03】  若评审通过进入步骤 7，不通过返回步 骤 5。  控制措施：提出的解决问题措施尽可能 多的涵盖各种可能使用的技术手段。 | 1天 | 集团信息部 | 解决方案 |  |
| 7 | 解决问题 | 根据通过审批的解决方案由信息部及相 关技术支持单位共同解决问题。 | 1天 | 集团信息部 |  | 故障解决及业 务回复报告 |
| 8 | 结束 | 故障解决及业务回复报告存档后，此流 程结束。 |  |  |  |  |