ICS 91.140

**CJ**

P 40

中华人民共和国城乡建设

行业标准

CJ/T XXXXX-202X

城乡水务信息系统安全技术要求

Technical requirements for urban and rural water affairs information systems security

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

202X-XX-XX 发布 202X-XX-XX 实施

中华人民共和国住房和城乡建设部 发布

目 次

[前 言 III](#_Toc207032517)

[1 范围 1](#_Toc207032518)

[2 规范性引用文件 1](#_Toc207032519)

[3 术语和定义 1](#_Toc207032520)

[4 缩略语 2](#_Toc207032521)

[5 总体要求 2](#_Toc207032522)

[5.1安全原则 2](#_Toc207032523)

[5.2 安全技术总体架构 3](#_Toc207032530)

[5.3 水务系统生命周期管理 4](#_Toc207032531)

[5.4信创要求 4](#_Toc207032535)

[5.5等级保护要求 5](#_Toc207032538)

[6 要求 5](#_Toc207032539)

[6.1 物理安全 5](#_Toc207032540)

[6.2 网络安全 5](#_Toc207032541)

[6.3 应用安全 6](#_Toc207032542)

[6.4 基础设施安全 6](#_Toc207032543)

[6.5 数据安全 6](#_Toc207032544)

[6.6 访问控制 9](#_Toc207032552)

[6.7 云服务安全 10](#_Toc207032553)

[6.8 物联网安全 10](#_Toc207032554)

[7 管理保障体系 10](#_Toc207032555)

[7.1 信息安全组织及制度 10](#_Toc207032556)

[7.2 信息安全审计与评估 11](#_Toc207032559)

[7.3 信息安全培训 17](#_Toc207032563)

[附录A（资料性）水务行业信息系统风险等级参考表 18](#_Toc207032565)

[附录B（资料性）水务行业数据分类分级表 21](#_Toc207032583)

[附录C（资料性）安全应急预案模板 23](#_Toc207032586)

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。

本文件由住房和城乡建设部标准定额研究所提出。

本文件由住房和城乡建设部市政给水排水标准化技术委员会归口。

本文件起草单位：

本文件主要起草人：

城乡水务信息系统安全技术要求

1. 范围

本文件规定了城乡水务信息系统安全的总体要求、要求和管理保障体系。

本文件适用于城乡水务领域的信息系统建设与运维安全工作。

1. 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/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 信息系统安全等级保护定级指南

GB/T 28448 信息安全技术 网络安全等级保护测评要求

GB/T 43697 数据安全技术 数据分类分级规则

GB 50174 电子信息系统机房设计规范

1. 术语和定义

GB/T 25069、GB/T 32919界定的下列术语和定义适用于本标准

3.1

**城乡水务 urban and rural water management**

为城镇和农村地区提供水资源管理、供水、排水、污水处理、再生水等水务服务的行业。

3.2

**信息系统 information systems**

用于采集、处理、存储、传输，分发和部署信息的基础设施、组织结构、人员和组件的总和。

3.3

**信息系统安全information systems security**

通过使用合理的安全控制措施保护在存储、处理或传输等过程中的信息不被未授权用户访问并保证授权用户能够正常使用系统。

3.4

**授权authentication**

授予权限，包括允许基于访问权的访问。

3.5

**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，并保障网络数据的完整性、保密性、可用性的能力。

3.6

**风险评估 risk assessment**

针对安全性以及对可靠操作的连续性造成风险的安全问题进行评估的过程。

3.7

**信创 application innovation of information technology**

为保障国家信息安全，实现信息技术领域的自主可控而开展的信息技术应用创新过程。

4 缩略语

**下列缩略语适用于本文件。**

DDoS: 拒绝服务(Distributed Denial of Service)

ICS: 工业控制系统(Industrial Control System)

PLC: 可编程逻辑控制器(Programmable Logic Controller)

TLS：传输层安全协议（Transport Layer Security）

RBAC：基于角色的访问控制（Role-based Access Control）

SQL：结构化查询语言（Structured Query Language）

ReDOS：正则表达式拒绝服务攻击（Regular Description Denial of Service）

CSS：跨站脚本攻击（Cross-Site Scripting）

CSRF：跨站请求伪造（Cross-Site Request Forgery）

UPS：不间断电源（Uninterruptible Power Supply）

IDEA：国际数据加密算法（International Data Encryption Algorithm）

RSA：RSA加密算法（Rivest-Shamir-Adleman以三位发明者姓氏命名）

AES：高级加密标准（Advanced Encryption Standard）

NAS：网络附加存储（Network-Attached Storage）

OSS：对象存储服务（Object Storage Service）

5 总体要求

5.1安全原则

5.1.1保密性原则

确保水务相关敏感信息，如管网数据、用户用水数据、水源地位置及水质监测数据等，仅被授权人员或系统访问。采用加密技术对传输中和存储的数据进行加密处理，如在数据传输过程中使用 TLS 加密协议，防止数据被窃取或非法监听；对静态数据，如数据库中的用户信息、业务文档等，利用数据库加密功能或文件加密系统进行加密存储。同时，实施严格的访问控制策略，通过身份认证（如用户名 / 密码、生物识别技术等）、权限管理（基于角色的访问控制，不同角色分配不同的访问权限）等手段，限定人员对敏感信息的访问范围。

5.1.2可用性原则

确保授权用户、系统和业务在需要时能够持续、可靠地访问和使用水务信息及相关信息系统。通过冗余设计，如采用双机热备、多链路冗余等技术，保障信息系统的硬件、网络设备和软件系统的高可用性，避免单点故障导致系统瘫痪。建立应急响应机制，制定详细的应急预案，针对可能出现的自然灾害、网络攻击、系统故障等突发事件，明确应急处置流程和责任分工，定期进行应急演练，提高应急响应能力和恢复效率，确保在最短时间内恢复系统正常运行和信息的可用性。同时，合理规划系统资源，进行容量管理，根据业务发展和用户需求变化，及时对系统进行升级和扩展，保证系统在高负载情况下仍能正常运行。

5.1.3最小权限原则

为水务系统的用户、进程和服务分配执行其任务所需的最小权限集合。对人员权限进行精细化管理，根据员工的工作职责和业务需求，划分不同的角色并为每个角色赋予相应的最小权限，例如，水质监测人员仅具有查看和上传水质监测数据的权限，而无权修改用户账单信息；系统管理员具有管理系统配置和用户权限的必要权限，但对于敏感业务数据的访问权限受到严格限制。对于系统进程和服务，确保其仅能访问和操作完成自身功能所必需的资源，避免因权限过大导致安全风险，如限制数据库服务进程对系统文件的访问权限，防止其被恶意利用进行数据篡改或破坏。

5.1.4持续改进原则

随着信息技术的发展、水务业务的变化以及安全威胁的不断演变，水务信息安全工作应持续改进和优化。建立信息安全监测和评估机制，定期对信息系统的安全状况进行全面检测和评估，如通过漏洞扫描、安全审计、渗透测试等手段，及时发现安全漏洞和隐患；根据监测和评估结果，制定针对性的改进措施和计划，及时修复安全漏洞、优化安全策略和防护措施；同时，关注行业最新安全动态和技术发展趋势，引入先进的安全技术和管理理念，不断完善水务信息安全保障体系，提高整体安全防护能力。此外，定期组织员工进行安全培训和教育，增强员工的安全意识和技能，促进安全文化的持续提升。

5.1.5合规性原则

水务信息安全工作在数据收集、存储、使用、共享等环节遵循合规、正当、必要的原则，保护用户隐私和数据安全。积极响应国家和行业主管部门的安全监管要求，配合开展安全检查、等级保护测评等工作，对涉及关键信息基础设施的水务系统，按照相关规定落实重点保护措施，保障国家水安全和社会公共利益。同时，根据法律法规和政策标准的变化，及时调整和完善水务信息安全管理制度和措施，确保合规性的持续满足。

5.1.6先进性原则

水务行业的信息安全建设应与行业应用趋势同步发展，考虑行业技术和产品更新带来的安全影响。特别是对于发展较快的人工智能大模型、算法和应用产品，应在建设时配置相应的安全管理机制和技术防护手段，保持技术先进性。

5.2 安全技术总体架构

城乡水务信息系统安全分为安全技术要求和管理保障体系两部分，总体框架见图1。

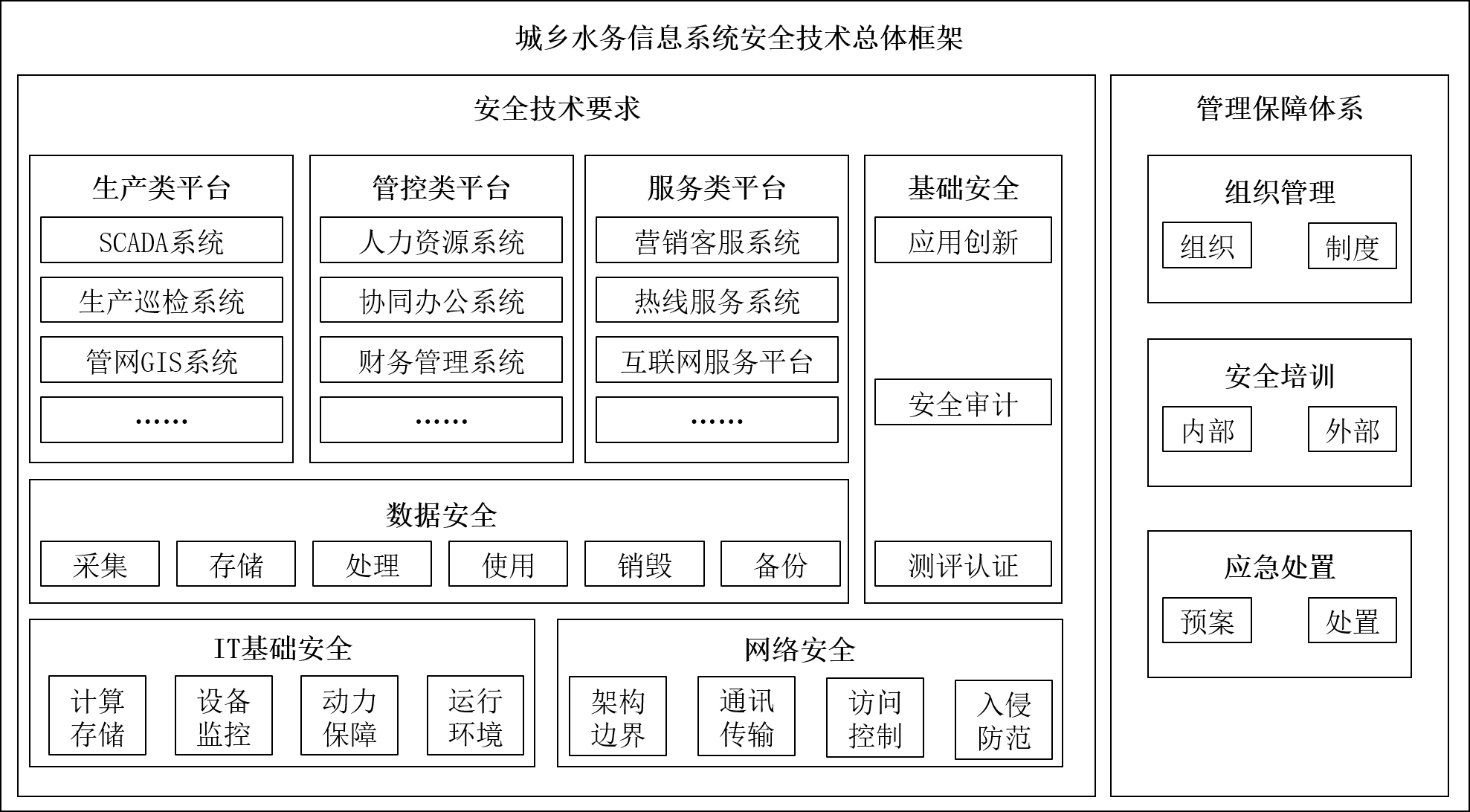


图 1城乡水务信息系统安全技术总体框架图

5.3 水务系统生命周期管理

5.3.1规划设计阶段

安全需求分析：在项目初始阶段，应识别和分析信息系统安全需求，结合水务行业特点，明确安全目标、策略、风险承受能力和应对措施。

安全方案设计：应根据需求分析结果，设计安全架构，包括但不限于物理布局、网络架构、数据分类与保护、访问控制策略、安全防护体系等。

合作伙伴安全评估：对涉及项目的各方合作伙伴（如供应商、集成商、运维服务商等）进行严格的安全资质审核和安全能力评估，确保其满足项目整体安全要求。

5.3.2建设实施阶段

安全控制集成：在系统建设过程中，应按照设计方案落实各项安全控制措施，包括软硬件设备的安全配置、网络系统的安全布设、应用程序的安全开发等。

工程监理与审计：应通过独立的工程监理和安全审计，对建设过程进行全程监控，及时发现并纠正安全隐患。

建设文档与证据保留：应建立健全完整的项目文档管理体系，每个阶段的文档记录应齐全、真实、可追溯，为后续的安全管理和审计提供依据。

5.3.3运行维护阶段

运维安全管理：在系统上线运营后，应制定并执行日常运维安全管理策略，包括系统升级维护、漏洞管理、事件响应、应急演练、备份与恢复、资产变更管理等。

安全监控与审计：应实时监控系统运行状态和安全事件，定期进行安全审计，发现并解决潜在安全问题，持续改进和优化安全措施。

多方协同与沟通：项目涉及多方合作时应建立有效的安全信息通报和协同机制，在发生安全事件时，各方能迅速响应并采取相应行动，共同保障系统的安全稳定运行。

5.4信创要求

5.4.1合规性

企业实施信创工作应接受企业主管部门指导、符合企业主管部门相关要求。

5.4.2规划先行

城乡水务企业应把信创作为企业信息化及信息系统战略的重要组成部分。企业应紧密围绕信创相关政策、标准、行业实践，结合企业自身信息化建设的需求和现状，系统科学制定信创背景下的企业信息化及信息系统战略。

5.5等级保护要求

城乡水务信息系统的安全保护等级应属于网络安全等级保护的第一级到第三级，定级参见附录A，应用系统的安全保护能力及要求应符合GB/T 22239的规定。

城乡水务信息系统安全保护等级应根据水务服务的对象和规模、水务服务连续性要求、系统破坏后对城市运行和社会生活的影响等因素确定，定级原理及流程应符合GB/T 22240的规定。

6 要求

6.1 物理安全

城乡水务信息系统物理安全措施应遵循通用原则，还应结合水务行业的特定需求，确保水处理厂、泵站、管网监控点等关键设施的物理安全，以保护水资源管理、水质监测、供水服务等核心业务的连续性和安全性。

机房的物理和环境安全建设应按GB50174的规定，结合等级保护物理安全控制项的要求进行建设，应包括环境安全（防火、防水、防雷击等）、设备和介质的防盗窃防破坏等方面，具体控制点应包括：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等十个控制点。

6.2 网络安全

平台安全应确保操作系统及数据库等平台层的可用性、完整性与保密性，具体包括网络架构、通信传输、边界防护、访问控制、入侵防范共五个方面，并应符合下列要求。

1. 网络架构方面的要求应包括：
2. 应划分不同的网络区域，并按照方便管理与控制的原则为各网络区域分配地址；
3. 宜提供通信线路、关键网络设备等冗余，以保证系统的高可用性；
4. 工业控制系统与其他系统之间应划分为两个区域，并采用技术隔离手段；
5. 涉及实时控制与数据传输的工业控制系统，应使用独立的设备组网。
6. 通信传输方面的要求应包括：
7. 应采用校验技术或密码技术保证通信过程中数据的完整性；
8. 宜采用密码技术保证通信过程中数据的保密性。
9. 边界防护方面的要求应包括：

跨越边界的访问和数据流应通过边界设备提供的受控端口进行通信。

1. 访问控制方面的要求应包括：
2. 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控端口拒绝所有通信；
3. 应对源地址、目的地址、源端口、目的端口和协议进行检查，以允许/拒绝数据包进出。
4. 入侵防范方面的要求应包括：
5. 应在关键网络节点处检测、防止或限制从外部和内部发起的网络攻击行为；
6. 宜采用技术手段对网络行为进行分析，实现对网络攻击的分析；
7. 当检测到攻击行为时，应记录源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵时提供报警。

6.3 应用安全

应用安全应保证应用系统本身的可用性、完整性和安全性，并应符合下列要求。

1. 认证与授权方面的要求包括：
2. 应支持基于RBAC机制；
3. 应采用最小权限原则（默认不授权，非显式要求无权限）；
4. 宜支持物理特征的安全认证机制。
5. 入侵防范方面的要求包括：

应采取防护SQL注入、ReDOS攻击、XSS攻击、CSRF攻击等安全威胁的措施。

1. 安全审计方面的要求包括：

应支持安全日志管理、安全审计等特性。

6.4 基础设施安全

基础设施安全包括机房及内部设备的安全、位于生产现场的工业感知与控制设备的安全。具体要求应包括下列内容。

1. 机房及内部设备的安全方面的要求应包括：
2. 机房应选择在具有防震、防风、防雨能力的建筑内；
3. 机房出入口应设置电子门禁系统，控制、鉴别与记录进出的人员；
4. 应将设备与主要部件进行固定，并设置明显的不易去除的标识；
5. 应将机柜、设施与设备等通过接地系统安全接地；
6. 宜设置防雷保安器或过压保护装置等预防雷击；
7. 应采取物理手段进行防火、防水、防潮；
8. 应在机房供电线路上配置稳压器和过电压防护设备；
9. 宜配置UPS等提供备用电力供应；
10. 宜设置冗余或并行的电力电缆线路为机房内设备供电；
11. 应隔离铺设电源线和通信线缆，避免电磁干扰。
12. 感知与控制设备应放置于采用铁板或其他防火材料的箱体或装置内紧固，且箱体或装置应透风、散热、防盗、防雨、防火等。

6.5 数据安全

6.5.1 通则

数据采集、存储、处理、交换、销毁和备份，每个环节都会遭遇不同的风险，要针对每个步骤实施相应的安全技术，保障数据生命周期安全。

水务行业数据分类分级应符合GB/T 43697的规定，附录B给出了水务行业数据分类分级参考。

6.5.2 数据采集

开展数据采集活动时，安全要求应包括但不限于下列内容：

1. 定义采集数据的目的和用途，明确数据采集源和采集数据范围。
2. 遵循合规原则，确保数据采集的合法性、正当性和必要性。
3. 遵循质量保障原则，制定数据质量保障的策略、规程和要求。
4. 遵循确保安全原则，对采集的数据进行分类分级标识，并对不同类型和级别的数据实施相应的安全管理策略和保障措施。对数据采集环境、设施和技术采取必要的安全管控措施。针对隐私和机密数据应加强数据收集人员、设备的管理，并对收集来源、时间、类型、数量、频度和流向等进行记录。
5. 对于间接途径获取隐私和机密数据的，应当与数据提供方通过签署相关协议、承诺书等方式，明确双方责任。

6.5.3 数据存储

制定数据存储架构相关的安全规则和管理规范，包括数据访问控制规则和数据存储转移安全规则等。安全要求应包括但不限于下列内容。

1. 将不同类别和级别的数据分开存储，并采取物理或逻辑隔离机制。针对隐私和机密数据，应当采用校验技术、密码技术等措施进行安全存储，并实施数据容灾备份和存储介质安全管理，定期开展数据恢复测试。
2. 遵守确保安全原则，主要考虑下列几个方面：
3. 存储架构安全；
4. 逻辑存储安全；
5. 存储访问控制；
6. 数据副本安全；
7. 数据归档安全；
8. 数据时效性管理。
9. 建立数据存储冗余策略和管理制度，及数据备份与恢复操作过程规范。

6.5.4数据处理

数据处理时，安全要求应包括但不限于下列内容。

1. 依据个人信息和重要数据保护的法律法规要求，明确数据处理的目的和范围。
2. 建立数据处理的内部责任制度，保证分析处理和使用数据不超出声明的数据使用目的和范围。
3. 遵循最小授权原则，提供数据细粒度访问控制机制。
4. 遵循确保安全原则，主要考虑下列方面：
5. 分布式处理安全；
6. 数据分析安全；
7. 数据加密处理；
8. 数据脱敏处理；
9. 数据溯源。
10. 遵循可审计原则，记录和管理数据处理活动中的操作。针对利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。
11. 对数据处理结果进行风险评估，避免处理结果中包含可恢复的敏感数据。
12. 识别人工智能数据、算法和模型相关突出风险，如数据传输安全、隐私保护和算法模型可信赖等，并采取数据加密等相应数据安全措施。

6.5.5 数据交换共享

数据交换共享时，安全要求应包括但不限于下列内容。

1. 数据交换共享应符合国家信息安全和保密相关规定，内容包括元数据、数据实体和其他相关信息。
2. 遵循责任随数据转移原则。
3. 在数据共享前，对数据进行风险评估，确保数据共享后的风险可承受，并通过合同明确数据接收方的数据保护责任。
4. 在数据共享前，对数据的敏感性进行评估，根据评估结果对需要共享的敏感信息进行脱敏操作。
5. 遵循可审计原则，记录时间、分发数据和数据接收方等相关信息。
6. 评估数据共享中的传输安全风险，确保数据传输安全。
7. 提供有效的数据安全共享机制。
8. 建立数据发布的审核制度，明确数据发布的内容和范围。对发布的数据开展定期审核。
9. 数据传输过程中，应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。针对隐私和机密数据传输，应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施。
10. 数据中台将治理后的数据推送到交换共享平台的共享库，应采用数据中台的数据传输管道功能。数据传输管道应配备敏感数据加密、解密、脱敏和还原等功能。数据交换共享阶段，应考虑下列情况：
11. 交换共享库需要明文：数据中台通过数据传输管道将数据提供给交换共享库，交换共享库需要明文。此时，数据中台应在数据传输管道将加密/脱敏数据进行解密/还原。
12. 交换共享库需要密文：数据中台通过数据传输管道将数据提供给交换共享库，交换共享库需要密文。此时，数据中台应直接将加密/脱敏数据传输给交换共享库，并将解密秘钥/还原算法一并提供给交换共享库。
13. 确保目标库数据安全。数据被推送到交换共享库（目标库，一般是前置机共享库），如果是明文，则数据安全应由数据需求方负责。如果是密文，则数据需求方应对解密秘钥/还原算法进行严格管理，保障数据安全。
14. 确保文件共享的安全性保障，可采用下列技术措施：
15. 文件所有者和文件申请者可在自己的文件存储系统进行加密，且双方加密算法可不统一。加密算法可选择：IDEA算法、RSA算法和AES算法等，可根据存储系统配置的算法功能选择加密算法。文件存储系统可采用NAS文件存储、OSS对象存储等常见的文件存储系统。为了让文件申请者能够成功解密文件，文件所有者在提供文件的时候，应附带文件解密秘钥。
16. 文件所有者将文件传输给申请者的文件存储系统，应采用加密传输通道。
17. 数据交易的前提，应先确定数据所属权、评估数据价值。确定数据所属权、评估数据价值的过程中，应符合本文件的6.5.3和6.5.4 的要求。在进行数据交易的过程中，应确保交易双方的重要信息安全，并应符合下列要求：
18. 数据交易双方的信息应保密，确保参与数据交易的组织或人员信息安全；
19. 应保证数据交易使用的数据传输通道、数据存储系统、数据交易信令的安全。在必要条件下，应采用硬件加密和软件加密双重数据安全保障机制。硬件加密秘钥和软件加密秘钥也应通过专人专责和专业设备进行保护；
20. 应保障数据价值信息的对称性，交易双方需要在封闭且安全的环境中，同时掌握数据价值详细情况。

6.5.6 数据销毁

开展数据销毁活动时，安全要求应包括但不限于下列内容：

1. 销毁超出数据留存期限的相关数据，对留存期限有明确规定的，按相关规定执行；
2. 个人和组织按照法律规定和合同约定等请求销毁的，应销毁相应数据；
3. 依照数据分类分级建立相应的数据销毁机制，明确需要进行数据销毁的数据、方式和要求，明确销毁数据范围、对象、流程、规则和技术等要求，并对销毁活动进行记录和留存；
4. 遵守可审计原则，建立数据销毁策略和管理制度，记录数据销毁的操作时间、操作人员、操作方式和数据内容等相关信息；
5. 隐私和机密数据销毁后，不得以任何理由、任何方式对已销毁数据进行恢复，引起备案内容发生变化的，应当履行备案变更手续。

6.5.7 数据备份

开展数据备份活动时，安全要求应包括但不限于下列内容：

1. 数据加密：为保护敏感数据和确保数据隐私，宜在备份过程中对数据进行加密，防止未经授权的访问和数据泄露；
2. 访问控制：应建立严格的访问控制策略，确保只有经过授权的人员才能访问和管理数据备份，防止内部和外部的恶意行为导致数据泄露或损坏；
3. 多重备份：为确保数据的安全性，宜采用多重备份策略，将数据备份到不同的存储介质或地理位置，可在一定程度上抵抗自然灾害、硬件故障或人为破坏等因素对数据的影响；
4. 数据完整性检查：确保备份数据的完整性和一致性，可定期对备份数据进行完整性检查，以发现和修复潜在的数据损坏问题；
5. 数据恢复测试：定期进行数据恢复测试，确保在实际需要恢复数据时，备份数据能够正确无误地恢复；
6. 安全监控：实时监控数据备份过程，确保备份任务正常执行，及时发现并解决问题，同时，监控系统应能记录和报告潜在的安全威胁，以便采取相应的安全措施；
7. 定期审计与更新：定期审计数据备份策略，并根据业务需求、技术发展和法规政策变化进行更新，以确保数据备份策略的有效性和合规性。
8. 定期备份检查：定期对冷热备数据进行恢复测试、日志检查、加密与访问控制、软件和设备更新、采用多重备份策略、监控存储设备健康状况及遵循合规性要求，以确保备份数据的安全性和可用性，降低数据丢失和业务中断风险。

6.6 访问控制

访问控制的安全要求应包括但不限于下列内容：

1. 应根据最小权限原则配置访问控制机制，确保软硬件设施在合理的范围和权限下使用；
2. 硬件设备和应用系统应使用密码技术防止非法访问，包括要求密码具有较强复杂度和长度，密码应定期强制更换，应考虑使用国密算法或强度较高的加密算法等；
3. 硬件设备和应用系统应具有防暴力破解机制，包括设置连接输入密码错误的最大允许次数、对暴力破解帐户或地址的自动锁定等。

6.7 云服务安全

云服务安全要求应包括但不限于下列内容：

1. 对于涉密数据及应用系统，不应使用公有云服务进行存储或运行；
2. 对于需使用云服务的敏感数据及应用系统，宜优先选用私有云实现；
3. 使用云服务时，宜定期将数据导出离线备份，或多云节点的异地备份，保障数据安全性；
4. 退出公有云服务前，应将数据作彻底删除，防止云端数据残留。

6.8 物联网安全

1. 物联网安全要求应包括但不限于下列内容：规划物联网通讯网络时，宜实现数据加密传输；
2. 宜通过配置访问白名单，实现数据定向传输，避免物联网设备的数据泄漏或非法访问；
3. 宜选用具有在线固件升级的物联网设备，便于漏洞补丁的远程下发和更新。

7 管理保障体系

7.1 信息安全组织及制度

7.1.1信息安全组织

7.1.1.1信息安全领导小组是水务公司信息安全工作的最高领导决策机构，不隶属于任何部门，直接对本单位最高领导负责，它应是一个常设机构，负责本单位信息安全工作的宏观管理。主要包括下列职责：

1. 负责制定信息系统安全的总体规划并监督规划的实施；
2. 组织制定本公司信息系统安全策略并审批上报的信息系统安全策略；
3. 负责组织细化上级规章制度，制定相应程序指南，并监督落实规章制度；
4. 负责本公司信息系统安全管理层以上的人员权限授予工作；
5. 负责审阅信息安全工作报告；
6. 负责本公司重大安全事故查处与汇报工作。

7.1.1.2信息安全领导小组应科学设计组织架构，合理调配专业技术人员，明确岗位职责，采用“多方协作、集中管理、逐级负责”的模式，确保信息安全管理到位。

7.1.2信息安全制度

信息系统安全的管理应配套制度和相关作业流程标准，可根据各单位的具体情况，选择建立如下制度：

* 1. 管理制度制定、评审、发布制度；
  2. 系统安全建设、整改、等级测评管理制度；
  3. 关键岗位人员安全管理制度；
  4. 设备安全管理制度；
  5. 信息安全运维管理制度；
  6. 信息安全事件应急响应管理制度；
  7. 信息资产管理规定；
  8. 第三方人员访问制度；
  9. 涉外活动信息安全制度。

7.2 信息安全审计与评估

7.2.1安全审计与评估管理

7.2.1.1 一般要求

城乡水务信息系统安全防护评估工作应定期进行。城乡水务信息系统的设计、开发、测试、部署、运行维护和废弃阶段均要进行安全评估，确保系统全生命周期安全性。

7.2.1.2评估工作角色与职责

城乡水务信息系统安全防护评估工作应由评估机构实施，评估人员应经培训合格。评审机构的职责包括：

1. 编制安全评估实施方案；
2. 自行组织评审评估实施方案实施安全评估；
3. 出具安全评估报告，提出整改建议；
4. 自行组织评审评估结果。

7.2.1.3保密工作

城乡水务信息系统的评估资料和评估结果的管理应按照GB/T 28448的要求做好保密工作。确保评估过程中产生或接触的所有数据及评估结果应做到保密，保密工作应符合下列要求。

1. 项目实施前，评估机构应与被评估单位签订保密协议，明确双方的保密责任。
2. 评估过程中必须接触或使用被评估单位敏感信息时，评估机构应遵循最小接触原则。仅授权且必要的人员可接触到敏感信息。
3. 应确保参与评估项目的人员均与评估机构签署保密协议。项目人员对工作过程中接触、产生的数据以及评估结果应当严格保密，未经授权不得泄露给任何第三方。项目人员不得利用项目过程中接触、产生的数据进行任何侵害被评估单位网络信息系统的行为。
4. 评估机构不应将被评估单位的任何设备带出允许的办公场地，评审结束后应立即归还。评估机构应及时归还被评估单位的有关数据与文件资料，或者设定保密期限，在保密期结束后彻底销毁。评估机构应保证不在第三方场合与第三方文档中发布或引用被评估单位的相关数据与文件资料。

7.2.1.4风险控制

城乡水务信息系统的安全审计和评估过程会引入安全风险，应加强安全评估实施过程中的风险控制。安全防护评估工作实施前，应确定评估范围，并对可能引入的风险进行分析，制定风险防范措施和风险控制措施。应当根据评估对象的不同采取相应的风险控制手段。评估实施过程的风险控制手段应包括:

1. 在实施过程中，评估操作应遵守城乡水务信息系统的相关操作章程，以防止敏感信息泄漏，确保及时处理意外事件。
2. 安全审计和评估过程应尽可能避开水务工控系统和生产调度系统生产作业敏感期。
3. 根据评估范围界定的城乡水务信息系统的实际情况,在被评估单位的配合下，在评估实施前制定应急预案，附录C给出了应急预案模板，可作为水务行业信息系统应急预案框架及主要内容的参考。
4. 对位于生产控制区域内的城乡水务信息系统在无法搭建模拟环境的情况下，不应采用评估工具进行评估，应采用人工评估的方式进行。

7.2.2安全审计与评估方法

7.2.2.1城乡水务信息系统安全审计和评估方法应符合GB/T 22229和GB/T 28448的规定。

7.2.2.2 应通过资产评估，对城乡水务信息系统的评估对象进行资产识别和分类定级，资产识别与定级应按照GB/T 28448执行。

7.2.2.3 在确定评估范围后，应对其资产价值进行分析。城乡水务信息系统的资产识别可按表1进行分类。

表 1资产识别

|  |  |
| --- | --- |
| 类别 | 解释 |
| 信息 | 以物理或电子的方式记录的数据，或者用于完成组织任务的知识产权，例如源代码、数据库数据、系统文档、计划、报告、用户手册等 |
| 软件 | 软件应用程序和服务，例如操作系统、数据库应用程序、网络软件、业务应用程序等用于处理、存储和传输信息 |
| 硬件 | 信息技术的物理设备，例如计算机硬件、路由器、交换机、硬件防火墙、程控交换机、备份存储设备、工作站、服务器等 |
| 系统 | 处理和存储信息的信息系统，代表一组信息、软件和硬件资产 |
| 其他设备 | 信息系统运行环境所涉及的必要设备，例如电源、空调、保险柜、文件柜、门禁、消防设施等 |

7.2.2.4 应根据城乡水务信息系统安全保护等级对系统重要性进行资产安全等级赋值。资产安全等级赋值可按表2进行。

表 2 资产安全等级赋值

|  |  |  |
| --- | --- | --- |
| 资产安全等级 | 级别 | 解释 |
| 5 | 很高 | 非常重要，在生产控制区域内，具有控制功能，且其安全属性破坏后可能对组织造成非常严重的损失 |
| 4 | 高 | 重要，生产控制区域内，不具有控制功能，其安全属性破坏后可能对组织造成比较严重的损失 |
| 3 | 中等 | 比较重要，生产控制区域内，其安全属性破坏后可能对组织造成中等程度的损失 |
| 2 | 低 | 不太重要，生产控制区域内，其安全属性破坏后可能对组织造成较低的损失 |
| 1 | 很低 | 不重要，其安全属性破坏后不会造成损害 |

7.2.2.5 威胁评估应包括下列内容：

1. 根据城乡水务信息系统的运行环境确定面临的威胁来源；
2. 确定威胁的严重程度和发生的频率。

7.2.2.6 威胁评估应根据资产分类结果，对城乡水务信息系统进行独立或整体的威胁评估，可按照安全分区和资产类别划分进行统一的威胁判断，并应符合下列要求：

1. 城乡水务信息系统应根据物理、网络和人员环境，对资产进行威胁判定。
2. 应根据威胁出现的频率判断得出等级，赋值越高，资产面临的威胁越大。根据威胁发生的可能性，定义年威胁等级和发生频率，见表3。

表 3威胁等级和发生频率

|  |  |  |  |
| --- | --- | --- | --- |
| 威胁等级 | 威胁赋值 | 定义 | 年发生频率(F) |
| 很高 | 5 | 威胁发生的可能性很高(或>1 次/周 )； 或在大多数情况下几乎不可避免 | F > 50 |
| 高 | 4 | 威胁发生的可能性较高(或> 1 次/月 )； 或在大多数情况下很有可能会发生 | 12 < F ≤ 50 |
| 中 | 3 | 威胁发生的可能性中等(或>1 次/半年)； 或在某种情况下可能会发生 | 2 < F ≤ 12 |
| 低 | 2 | 威胁发生的可能性较小；或一般不太可能发生；或没有被证实发生过 | 0.1 < F ≤ 2 |
| 很低 | 1 | 威胁几乎不可能发生；仅可能在非常罕见和例外的情况下发生 | F ≤ 0.1 |

1. 城乡水务信息系统面临的常见威胁表现形式见表4。

表 4 威胁表现形式

| 类型 | 描述 | 威胁子类 |
| --- | --- | --- |
| 软硬件故障 | 对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷等问题 | 设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障、开发环境故障等 |
| 物理环境影响 | 对信息系统正常运行造成影响的物理环境问题和自然灾害 | 断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等 |
| 无作为或操作失误 | 应该执行而没有执行相应的操作，或无意执行了错误的操作 | 维护错误、操作失误等 |
| 管理不到位 | 安全管理无法落实或不到位，从而破坏信息系统正常有序运行 | 管理制度和策略不完善、管理规程缺失、职责不明确、监督控管机制不健全等 |
| 恶意代码 | 故意在计算机系统上执行恶意任务的程序代码 | 病毒、特洛伊木马、蠕虫、陷门、间谍软件、窃听软件等 |
| 越权或滥用 | 通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的权限，做出破坏信息系统的行为 | 非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等 |
| 网络攻击 | 利用工具和技术通过网络对信息系统进行攻击和入侵 | 网络探测和信息采集、漏洞探测、嗅探（帐号、口令、权限等）、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏等 |
| 物理攻击 | 通过物理的接触造成对软件、硬件、数据的破坏 | 物理接触、物理破坏、盗窃等 |
| 泄密 | 信息泄露给不应了解的他人 | 内部信息泄露、外部信息泄露等 |
| 篡改 | 非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用 | 篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等 |
| 抵赖 | 不承认收到的信息和所作的操作和交易 | 原发抵赖、接收抵赖、第三方抵赖等 |

7.2.2.5脆弱性评估是发现与分析城乡水务信息系统中存在的可被威胁利用的缺陷的过程，应包括脆弱性识别和赋值两个步骤,并应符合下列要求：

1. 脆弱性识别应从技术管理脆弱性和组织管理脆弱性两个方面进行，技术管理脆弱性涉及物理层、网络层、系统层、应用层等的安全问题。组织管理方面的脆弱性主要通过访谈和调查问卷来识别。对以往安全事件的统计和分析是确定脆弱性的重要方法。
2. 脆弱性赋值应包含严重程度和对系统安全属性的影响两部分内容,即确定脆弱性对城乡水务信息系统资产的暴露程度(包括被威胁利用的可能性和难易程度)和脆弱性对安全属性的哪方面产生了破坏，脆弱性等级和赋值应符合表5的要求。

表 5 脆弱性等级和赋值

|  |  |  |
| --- | --- | --- |
| 脆弱性等级 | 脆弱性赋值 | 定义 |
| 很高 | 5 | 非常脆弱，如果被威胁利用，造成损害的可能性>95% |
| 高 | 4 | 很脆弱，如果被威胁利用，70%<造成损害的可能性≤95% |
| 中 | 3 | 脆弱，如果被威胁利用，30%<造成损害的可能性≤70% |
| 低 | 2 | 强度不好，如果被威胁利用，5%<造成损害的可能性≤30% |
| 很低 | 1 | 强度好，如果被威胁利用，造成损害的可能性≤5% |

7.2.2.6

风险分析应包括资产、威胁、脆弱性三个基本要素，应按下式进行风险计算：

风险值 = R（A，T，V） （1）

式中：

R —安全风险计算函数；

A—资产；

T—威胁；

V—脆弱性。

评估者可根据自身情况选择相应的风险计算方法计算风险值，如矩阵法或相乘法。

7.2.2.7 为实现对风险的控制与管理，可对风险评估的结果进行等级化处理。可将风险划分为五级，等级越高，风险越高，风险等级划分方法见表6，风险控制措施见表7。

表6 风险等级划分

|  |  |  |
| --- | --- | --- |
| 风险等级 | 风险等级赋值 | 描述 |
| 很高 | 5 | 一旦发生将产生非常严重的经济或社会影响，如组织信誉严重破坏、严重影响组织的正常经营，经济损失重大、社会影响恶劣 |
| 高 | 4 | 一旦发生将产生较大的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害 |
| 中等 | 3 | 一旦发生会造成一定的经济、社会或生产经营影响，但影响面和影响程度不大 |
| 低 | 2 | 一旦发生造成的影响程度较低，一般仅限于组织内部，通过一定手段很快能解决 |
| 很低 | 1 | 一旦发生造成的影响几乎不存在，通过简单的措施就能弥补 |

表 7 风险控制措施

|  |  |  |
| --- | --- | --- |
| 风险等级 | 风险值 | 风险控制措施 |
| 1 | 1-100 | 无强制要求需进行保护措施 |
| 2 | 101-200 | 无强制要求需进行保护措施，但是需要关注 |
| 3 | 201-300 | 必须进行保护措施。保护方案须在风险评定后的1月内完成，之后进行风险再次评估 |
| 4 | 301-400 | 必须进行保护措施。保护方案须在风险评定后的1周内完成，之后进行风险再次评估 |
| 5 | 401-500 | 必须立即进行保护措施，之后进行风险再次评估 |

7.2.3安全审计与评估实施

7.2.3.1 实施流程

城乡水务信息系统的信息安全审计和评估实施流程见图2。



图 2信息安全审计和评估实施流程

7.2.3.2启动准备

启动准备阶段的工作应包括：

1. 成立评估工作组；
2. 确定评估范围；
3. 评估工具准备；
4. 准备应急措施。

7.2.3.3现场实施

应针对城乡水务信息系统的运行环境、人力、IT运维、业务运维等多个方面进行现场实施。

7.2.3.4安全建议

应根据风险决策提出的风险处理计划，结合资产面临的威胁和存在的脆弱性，经过合理的统计归纳，形成安全解决方案建议报告。安全建议报告应包含安全建议阶段的所有工作内容，应包括下列内容:

1. 需求分析:需求分析根据风险分析的结论将城乡水务信息系统的防护需求进行归纳和总结，并根据评估结果进行现状分析、可行性分析和紧迫性分析；
2. 安全建议:根据需求分析的结论针对不同评估节点提出安全防护措施；评估工作组应对安全建议方案着重讨论,确保安全建议的合理性、可行性；
3. 实施计划:根据可行性分析和紧迫性分析结论提出安全建议的实施计划。

7.2.3.5安全整改

被评估单位应根据安全建议方案制定整改计划、落实整改措施，不断提高城乡水务信息系统的安全防护能力。

7.3 信息安全培训

7.3.1信息安全培训制度，应符合下列要求：

1. 应将信息安全培训覆盖企业全员，水务行业涉及相关系统的系统用户、运维人员以及各级管理人员应当参加定期的信息安全培训，并纳入新员工的入职培训中。
2. 针对性培训:根据需求分析的结论针对不同评估节点提出安全防护措施。
3. 应定期更新和重复培训。

7.3.2信息安全培训应包含下列内容：

1. 法规政策教育：培训国家相关法律法规、行业标准以及本企业相关信息安全管理制度的学习，使得相关人员明确其在信息安全管理中的法律责任和义务。
2. 基础知识普及：涵盖密码学基础、网络攻防原理、数据加密、身份认证、权限管理等信息安全基础知识。
3. 专项技能培训：包括但不限于操作系统安全设置、数据库安全、应用系统安全使用方法、移动设备和BYOD（自带设备办公）的安全管理等内容。
4. 案例分析与实践演练：通过真实案例分析，提高员工对信息安全威胁的敏感性和应对能力；定期进行模拟攻击与防御实战演练，提升应急处理能力。
5. 基础知识普及：涵盖密码学基础、网络攻防原理、数据加密、身份认证、权限管理等信息安全基础知识。

附录A

（资料性）

水务行业信息系统风险等级参考

A.1水务信息系统可按照以下原则划分风险等级：

1. 系统/网站只能浏览，无信息交互，定为第一级。
2. 系统/网站不涉敏感信息（如管网坐标）或用户个人信息，定为第二级。
3. 系统/网站涉敏感信息或用户个人信息，定为第三级。

A.2 水厂/泵站工控系统

水厂/泵站工控系统风险等级见表A.1

表 A.1 水厂/泵站工控系统风险等级表

|  |  |  |
| --- | --- | --- |
| 日供水规模 X | 有备用供水方案 | 无备用供水方案 |
| X＜5万m3/d | 第一级 | 第二级 |
| 5万m3/d≤X＜30万m3/d | 第二级 | 第三级 |
| X≥30万m3/d | 第三级 | 第三级 |

工控系统不分大小，全部要求物理隔离或利用网闸等设备进行逻辑隔离。

A.3 污水厂/污水泵站工控系统

水厂/泵站工控系统风险等级见表A.2

表 A.2 水厂/泵站工控系统风险等级表

|  |  |
| --- | --- |
| 日处理规模 X | 安全等级 |
| X＜5万m3/d | 第一级 |
| 5万m3/d≤X＜30万m3/d | 第二级 |
| X≥30万m3/d | 第三级 |

工控系统不分大小，全部要求物理隔离或利用网闸等设备进行逻辑隔离。

A.3 水厂/污水厂综合管理系统

主要包括设备管理、设备巡检、物资管理、仓库管理、生产管理等功能。风险等级一般定为第二级。

A.4 生产调度管理系统

生产调度管理系统风险等级见表A.3

表 A.3 生产调度管理系统风险等级表

|  |  |  |
| --- | --- | --- |
| 规模 X | 只能监测数据 | 能远程监控或设置运行参数 |
| X＜5万m3/d | 第一级 | 第二级 |
| 5万m3/d≤X＜30万m3/d | 第二级 | 第三级 |
| X≥30万m3/d | 第三级 | 第三级 |

A.4 供排水管网地理信息系统

系统涉及管网坐标等敏感信息，风险等级一般定为第三级。

A.5 DMA分区计量管理系统

系统涉及管网坐标等敏感信息，风险等级一般定为第三级。

A.6 报装管理系统

系统涉及用户个人信息（如：身份证号、地址、电话、照片等），一般按照用水户数量划分风险等级，见表A.4

表 A.4报装管理系统风险等级表

|  |  |
| --- | --- |
| 用水户数量 X | 风险等级 |
| X＜5000 | 第二级 |
| X≥5000 | 第三级 |

A.7 抄表管理系统

系统涉及用户个人信息（如：身份证号、地址、电话、照片等），一般按照用水户数量划分风险等级，见表A.5

表 A.5 抄表管理系统风险等级表

|  |  |
| --- | --- |
| 用水户数量 X | 风险等级 |
| X＜5000 | 第二级 |
| X≥5000 | 第三级 |

A.8 收费管理系统

系统涉及用户个人信息（如：身份证号、地址、电话、照片等），一般按照用水户数量划分风险等级，见表A.6

表 A.6 收费管理系统风险等级表

|  |  |
| --- | --- |
| 用水户数量 X | 风险等级 |
| X＜5000 | 第二级 |
| X≥5000 | 第三级 |

A.9 表务管理系统

主要包括设采购管理、库存管理、拆表管理、换表管理、表具检测、统计分析等功能。风险等级一般定为第二级。

A.10 客服热线管理系统

系统涉及用户个人信息（如：身份证号、地址、电话、照片等），一般按照用水户数量划分风险等级，见表A.7。

表 A.7 客服热线管理系统风险等级表

|  |  |
| --- | --- |
| 户数量 X | 风险等级 |
| X＜5000 | 第二级 |
| X≥5000 | 第三级 |

A.11 工单管理系统

系统涉及管网坐标等敏感信息和用户个人信息（如：身份证号、地址、电话、照片等），一般按照用水户/坐标数量划分风险等级见表A.8

表 A.8 工单管理系统风险等级表

|  |  |
| --- | --- |
| 用水户/坐标数量 X | 风险等级 |
| X＜5000 | 第二级 |
| X≥5000 | 第三级 |

A.12 安防系统

表 A.9 安防系统风险等级表

|  |  |
| --- | --- |
| 摄像头数量 X | 风险等级 |
| X＜100 | 第一级 |
| X≥100 | 第二级 |

A.13 门户网站

表 A.10 门户网站风险等级表

|  |  |
| --- | --- |
| 网站功能 | 风险等级 |
| 只能浏览 | 第一级 |
| 可以信息交互 | 第二级 |

A.14 办公自动化系统

表 A.11 办公自动化系统风险等级表

|  |  |
| --- | --- |
| 应用范围 | 风险等级 |
| 企业内网访问 | 第一级 |
| 公网访问 | 第二级 |

A.15 二次供水监控系统

表 A.12 二次供水监控系统等级表

|  |  |  |
| --- | --- | --- |
| 泵房数量 X | 只能监测数据 | 能远程监控或设置运行参数 |
| X＜100 | 第一级 | 第二级 |
| 100≤X＜500 | 第一级 | 第二级 |
| X≥500 | 第二级 | 第三级 |

附录B

（资料性）

水务行业数据分类分级表

根据国家标准 GB/T 43697-2024《数据安全技术 数据分类分级规则》，数据分为核心数据、重要数据和一般数据三个层级，水务行业数据分类分级见表B

表 B 水务行业数据分类分级表

| 数据分级级别名称 | 数据实体类别 | 数据分类说明 |
| --- | --- | --- |
| 核心数据 | 军事类等特殊行业水表运行数据；  涉密的管网基础设施数据；  …… | 核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。 |
| 重要数据 | 企业内部重要管理数据；  企业内部核心管理数据；  企业核心经营类数据；  企业核心生产数据；  企业内部管理制度及流程；  企业重要经营类数据；  企业重要生产数据；  商业机密；  核心技术资料、文档、知识库相关数据；  核心技术研发、实施、维护相关数据；  IT软硬件管理员账号密码、密钥类；  客户身份和标识信息；  自然人身份标识；  用户基本资料；  实体身份证明；  客户私密资料；  重要技术资料、文档、知识库相关数据；  重要技术研发、实施、维护相关数据；  IT软硬件非管理员账号密码、密钥类；  资产档案；  厂区、泵站、管网布局等相关数据；  非涉密的管网基础设施数据；  …… | 重要数据是指特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。仅影响组织自身或公民个体的数据一般不作为重要数据。 |
| 一般数据 | 企业公开披露信息；  已注册的专利、商标、知识产权信息；  企业内部一般管理数据；  市场一般经营类数据；  企业一般生产数据；  管网、水表运行数据；  客户关系相关数据；  客户服务记录数据；  水费等费用收缴相关数据；  一般技术资料、文档、知识库相关数据；  一般技术研发、实施、维护相关数据；  资产新增、维护、报废等资产生命周期相关数据；  …… | 一般数据是核心数据、重要数据之外的其他数据。一般数据还可细分为敏感数据和其他一般数据，其中敏感数据是指一旦被泄露或者篡改、损毁，对经济运行、社会稳定、公共利益有一定影响，或者对组织自身或者公民个体造成重要影响的数据. |
| 注：不在以上数据实体类别的数据，可根据实际在对应数据分级名称下进行类别补充或类别名称调整。 | | |

附录C

（资料性）

安全应急预案模板

C.1适用范围

本预案适用于水务行业信息系统安全应急事件的应对和处置，建立分级负责的安全应急事件处置体系，指导和规范安全应急事件的处置流程。

本预案所指安全应急事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件。

C.2安全应急事件分类分级

C.2.1安全应急事件分类

信息系统安全应急事件可分为故障、有害程序、信息数据安全三类。

1. 故障类安全应急事件：主要包括单机故障、网络故障、系统故障、不间断电源故障等，表现形式包括网络连接中断、业务连接异常、备用电源连接异常等。
2. 有害程序类安全应急事件：主要包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件等，主要表现形式为主机或服务器受病毒感染，出现异常程序干扰业务或恶意勒索等。
3. 信息数据安全应急事件：主要包括信息篡改事件、信息泄露事件、信息破坏事件等，主要表现形式为发布数据被篡改且造成不良影响、互联网出现公司内部数据，或数据无法识别、存储介质损坏等。

C.2.2安全应急事件分级

安全应急事件分为四级：特别重大安全应急事件（I级）、重大安全应急事件（Ⅱ级）、较大安全应急事件（Ⅲ级）、一般安全应急事件（Ⅳ级）。

1. 符合下列情形之一的，为特别重大安全应急事件（I级）：
2. 网络和重要信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。
3. 内部重要敏感信息和关键数据被窃取并在互联网上发布，对企业造成严重经济损失或产生严重不良社会影响。
4. 对外发布渠道被入侵、信息被篡改为政治敏感信息，对企业造成严重经济损失或产生严重不良社会影响。
5. 其他对企业造成严重经济损失或产生严重不良社会影响的安全应急事件。
6. 符合下列情形之一且未达到特别重大安全应急事件的，为重大安全应急事件（Ⅱ级）：
7. 网络和重要信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。
8. 重要信息系统数据被篡改或损坏且无法恢复，对企业造成经济损失或产生不良社会影响。
9. 对外发布信息被篡改，对企业造成经济损失或产生不良社会影响。
10. 其他对企业造成经济损失或产生不良社会影响的安全应急事件。
11. （3）符合下列情形之一且未达到重大安全应急事件的，为较大安全应急事件（Ⅲ级）：
12. 网络和重要信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。
13. 重要信息系统数据被篡改或损坏且只能部分恢复，对企业造成一定经济损失或产生一定不良社会影响。
14. 生产调度中心或呼叫热线中心由于电力故障等突发因素无法正常运转，对企业造成一定经济损失或产生一定不良社会影响。
15. 其他对企业造成一定经济损失或产生一定不良社会影响的安全应急事件。
16. 除上述情形外，网络和重要信息系统由于突发事件造成小范围中断、故障，对部分使用人员造成一定影响，影响部分业务开展的，为一般安全应急事件（Ⅳ级）。
17. 重要信息系统包括：生产运营类支撑系统（如供排水管网GIS系统、调度系统、模型系统、巡检工单系统等）、营销服务类支撑系统（如营业收费系统、呼叫热线系统、网上营业厅、微信公众号）等、管理管控类支撑系统（如OA、财务管理系统、工程管理系统等）。

C.3组织机构与职责

水务企业应建立安全应急事件领导小组（以下简称：应急领导小组），作为安全应急事件的管理决策机构，在信息系统应急工作中的主要职责包括：

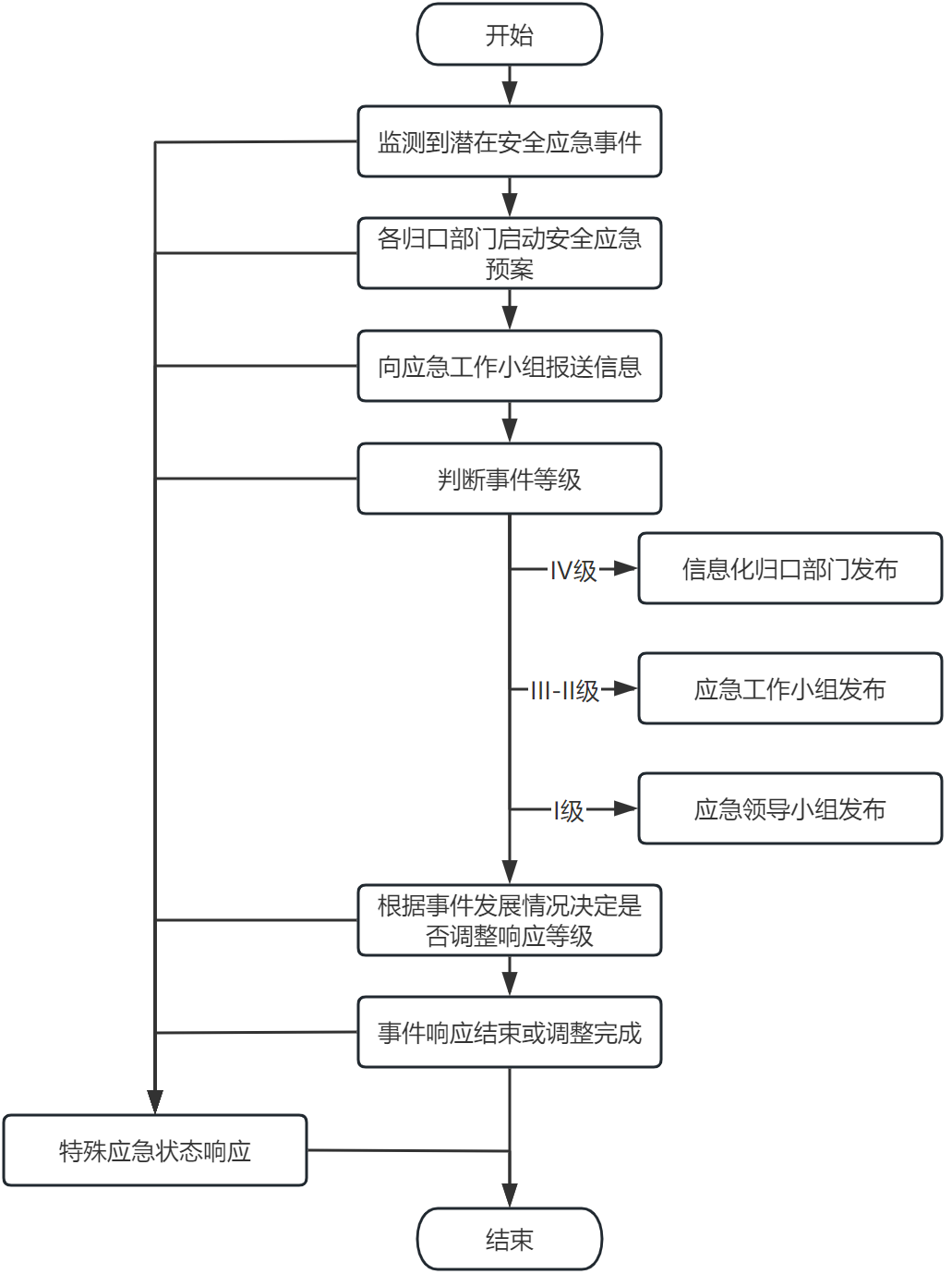
1. 贯彻落实与宣贯国家、省、市、行业有关网络信息系统突发事件应急处置的法规、规定；
2. 研究和部署信息系统重大安全应急决策；
3. 宣布进入和解除应急状态，决定实施和终止信息系统安全应急预案；
4. 统一领导、指挥协调企业安全应急工作。

应急领导小组宜下设安全应急事件工作小组（以下简称：应急工作小组），作为安全应急事件的具体执行机构，在信息系统应急工作中的主要职责包括：

1. 监督执行应急指挥部下达的应急指令、重大应急决策和部署，协调各方应急资源，组织应急处置；
2. 组织制定网络信息系统应急工作相关制度、标准、规范和预案，定期组织评估、修订和复核，并监督、检查贯彻执行情况；
3. 及时了解和掌握网络信息系统突发事件与应急处置工作情况，向应急指挥部报告应急处置过程中发现的重大问题，并按照“谁主管、谁负责，谁运营、谁负责”的要推进应急处置工作；
4. 组织参与网络信息系统事件调查、总结应急处理经验和教训等后期处置工作。

C.4应急响应流程

C.4.1响应流程图



图C.1 流程图

监测到潜在安全应急事件发生后，各归口部门应尽快启动安全应急预案，及时向应急工作小组报送信息。应急工作小组根据监测信息进行分析研判，IV级安全应急事件宜由信息化归口部门负责发布，III-II级安全应急事件宜由应急工作小组负责发布，I级安全应急事件宜由应急领导小组负责发布。处置过程中，视事件发展情况、危害程度、事件分级条件等综合因素研究决定是否调整事件响应。

业务自检或可靠人员反映已发布错误应急信息时，宜由应急领导小组负责启动特殊应急状态响应，全体在岗员工应按照流程有序组织错误应急信息下线工作，并消除影响。

C.4.2各级别响应行动

C.4.2.1 IV级应急行动

1. 业务归口部门在应急响应启动后的2小时内向应急工作小组汇报工作内容和计划。
2. 技术保障部门及时处理事件问题，分析事件原因，并在24小内排查完毕，排除故障。
3. 业务归口部门同步发布应急响应信息，并做好信息报送工作及修复期间的业务配合工作。
4. 业务归口部门及技术保障部门做好复盘，并更新《应急问题QA表》。
5. 技术保障部门加强系统维护力度,加大系统设备巡检和监控力度,及时排除设备和安全隐患,保障业务网络安全运行。

C.4.2.2 III级应急行动

1. 应急工作小组全天排班，相关人员取消休假，随时待命，手机24小时保持联络畅通。
2. 应急工作小组随时收集、整理、发布应急响应活动的信息并每日向应急领导小组报告，直至应急事件结束。
3. 相关责任部门、人员及时处理紧急情况，加强值守，排除隐患。
4. 各业务部门在应急响应结束后24小时内向应急工作小组提交应急工作总结。
5. 应急工作小组向应急领导小组提交应急事件报告。

C.4.2.3 II级应急行动

1. 应急领导小组安排领导带班，其他成员随时待命，手机24h保持联络畅通。
2. 应急工作小组全天排班，相关人员取消休假，手机24h保持联络畅通。
3. 应急工作小组随时收集、整理、发布应急响应活动的信息并每日上午10点和下午4点向应急领导小组报告，直至应急事件结束。
4. 相关责任部门、人员及时处理紧急情况，加强值守，排除隐患。
5. 各业务部门在应急响应结束后24h内向应急工作小组提交应急工作总结。
6. 应急工作小组向应急领导小组提交应急事件报告。

C.4.2.4 I级应急行动

1. 应急领导小组全体在岗待命，企业进入应急状态，值班领导30min内到达应急指挥中心，手机24h保持联络畅通，随时关注事态进展。
2. 应急工作小组在响应启动的1h内向应急领导小组上报未来3d的应急值班表。
3. 应急领导小组2h内发布应急响应活动信息并随时向上级主管部门报告，直至应急事件结束。
4. 各业务部门做好应急处置的协调、监督、处置工作，后勤部门做好生活保障工作，加强值守班的安全管理。
5. 各业务部门在应急响应结束后24h内向应急工作小组提交应急工作总结。
6. 应急工作小组向应急领导小组提交应急事件报告。

C.4.2.5 特殊应急状态响应活动

1. 企业遇到以下情况时：
2. 业务自检时发现由于业务事故导致应急领导小组发布了错误应急事件信息。
3. 可靠人员反映有错误应急事件信息发布。
4. 相关人员在5min内上报应急领导小组，由应急领导小组安排核实工作，并在核实发布错误信息后的10min内，应急工作小组联系发布应急信息的渠道进行下线工作，直至所有错误信息下线。
5. 应急工作小组复盘事件原因，并提交应急事件报告。

C.4.3 具体处置措施

C.4.3.1 故障类安全应急事件

故障类安全应急事件主要包括单机故障、网络故障、系统故障、不间断电源故障等，可按照单机故障-网络故障-系统故障-电源故障的顺序进行排查。

1. 单机故障

单机故障为仅本机出现异常，其他设备均无异常情况。经判断为单机故障的问题，影响范围较小，可直接由计算机维护员或网络维护员处理。

1. 网络故障

网络故障通常表现为网络中断，通常处于Ⅱ-Ⅳ级之间，即网络大面积或局部中断。一般可尝试由计算机维护员或网络维护员切换备用线路、接口替换、更换网线、交换机配置调整、交换机替换等操作进行网络修复。如果无法恢复，可向相关支撑单位寻求技术支持。

1. 系统故障

系统故障通常表现为业务响应异常等现象，通常处于Ⅱ-Ⅳ级之间，即重要信息系统大面积或局部不可用，一般可由系统负责人员根据系统提供的运维手册进行故障确认与修复。如果无法恢复，可向开发单位寻求技术支持。

1. 市电电源故障且不间断电源无法使用

市电电源故障且不间断电源无法使用表现为需要临时供电设备无法使用，可由物业部门确认现场市电情况，确认市电恢复时间；由机房管理员确认现场不间断电源情况，设备是否正常开机，电力开关是否跳闸。如不间断电源未开机或电力开关跳闸，应在第一时间进行恢复；如不间断电源与电力开关均正常且不间断电源无负载显示，由机房管理员进一步确认现场电力线路是否进行过改动，现场用电设备是否自身故障。各不间断电源使用部门宜至少每半年度进行一次不间断电源放电切换，用于验证不间断电源可靠性与电池持久性。

C.4.3.2 有害程序类安全应急事件

有害程序类突发事件大多表现为电脑或服务器感染恶意软件，导致电脑或服务器运行缓慢或直接失去响应。有害程序类安全应急事件通常需要计算机维护员、网络维护员、机房管理员等人员共同处置，将包括但不限于受感染服务器和相应连接主机进行大范围断网隔离后进行杀毒处理，并对全网进行扫描恶意软件扫描。如有条件可协调更换设备确保业务继续进行。如过无法恢复，可向相关支撑单位寻求技术支持。

C.4.3.3 信息数据类安全应急事件

信息数据类安全突发事件主要表现为外发布信息内容被第三方篡改和内部数据泄露、信息数据破坏。

1. 外发布信息内容被第三方篡改

外发布信息内容被第三方篡改往往表现为对外发布内与原内容产生偏差，有相关外来举报；或被恶意篡改为政治敏感信息，造成恶劣的社会影响，干扰正常公司对外服务，损害公司对外形象。因由及时恢复对外信息原本内容，切断对外网络，排查信息篡改途径，修复漏洞，必要时可联系支撑单位获取技术支持。宜由应急工作小组协助外宣及服务部门进行舆情监控，配合进行宣传与解释的信息发布。请求网络安全部门。若为I级安全应急事件，宜上报至行业安全主管部门并申请介入调查，配合相关证据收集整理工作。

1. 内部数据泄露

内部数据泄露表现为内部重要敏感信息和关键数据被窃取并在互联网上发布，对企业造成严重经济损失或产生严重不良社会影响。应由应急领导小组发布I级安全应急事件，第一时间与发布泄露数据的平台取得联系，请求立刻将公布的内容删除，并上报至行业安全主管部门并申请介入调查，配合相关证据收集整理工作。由应急工作小组对内部接触数据的人员进行审查，调查数据泄露途径，并对所有操作记录进行提取并备案，用于配合行业安全主管部门调查。协助外宣及服务部门进行舆情监控，配合进行宣传与解释的信息发布。

1. 信息数据破坏

信息数据损坏表现为数据无法识别、存储截止损坏，导致业务无法正常进行。根据数据的重要程度和数据可恢复性，通常划分为Ⅱ-Ⅲ级。发生信息数据破坏事件时，应由重要信息系统负责人及机房管理员第一时间提取备份数据，确定损坏数据范围并对缺失的数据进行修复，并组织业务部门对数据进行核对确认、对损坏数据进行补录，同步排查数据损坏原因。针对无法修复的数据应联系支撑单位提供技术支持，确保业务继续进行。

C.5培训与演练

C.5.1培训

C.5.1.1 企业每年应当制定培训计划，组织培训人员、培训内容和培训活动，提升和加强员工的技能和应急事件的应对能力。

C.5.1.2培训内容

1. 有关信息系统安全的法律、法规、政策、规章和标准；
2. 有关企业内部的管理体系、制度、组织架构、应急响应流程；
3. 水务应急系统相关的基本知识、运维技术、应急预案和预防措施。

C.5.2 演练

C.5.2.1企业每年应当制定培演练计划，明确演练目标、参与人员、演练场景、应急事件等级，确保演练的有效性和实用性。

C.5.2.2 定期开展演练，设计真实的场景和情境，演练期间相关人员表现纳入考核。

C.5.2.3 演练结束进行评估，收集反馈意见和演练效果，发现问题并提交改进报告。

C.6预案后评估

C.6.1 预案回顾

C.6.1.1 回顾已执行应急预案的流程和具体应对措施，执行过程中的效率、沟通和风险情况。

C.6.1.2 回顾发现的问题、响应时间、资源分配、人员参与度和协作情况。

C.6.2 总结与改进

C.6.2.1 总结预案执行过程中的经验教训，包括成功经验和失败教训。

C.6.2.2 提出改进建议、行动计划和改进时间表，更新应急问题QA表。

C.6.2.3 组织培训应急领导小组、应急工作小组和相关业务部门，培训分享相关改进内容。

C.7 安全责任人联系清单

C.7.1 重要信息系统责任人清单

重要信息系统责任人见表C1。

表 C1 重要信息系统责任人表

|  |  |  |  |
| --- | --- | --- | --- |
| 系统名称 | 系统责任人  联系电话  （A角） | 系统责任人  联系电话  （B角） | 责任领导  联系电话 |
|  |  |  |  |
|  |  |  |
|  |  |  |

C.7.2 重要干系人清单

重要干系人见表C2。

表 C2 重要干系人表

|  |  |  |
| --- | --- | --- |
| 角色 | 责任人  联系电话  （A角） | 责任人  联系电话  （B角） |
| 网络维护员 |  |  |
| 计算机维护员 |  |  |
| 机房维护员 |  | ... |

C.7.3 应急问题QA表

应急问题QA表C3。

表 C3 应急问题QA表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 问题描述Q | 解决方案A | 最后更新日期 | 负责人 | 状态 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |