



以标准铸盾·以安全赋能

-- 水务信息安全行标解析

许冬件 2026年04月17日 深圳

目录

C O N T E N T S

01

编

制

背

景

02

标

准

内

容

03

标

准

意

义



政策背景-锚定政策导向，筑牢水务信息安全屏障

世界范围内频发的针对水务信息系统的网络攻击安全事件，为我国的水务信息化建设敲响了安全警钟。国内各级政府与部门为解决问题，积极出台了相关法律法规以及各类行动计划、规划、通知等。

2021年6月

《中华人民共和国数据安全法》

要求工业、电信、自然资源、科技等主管部门承担本行业、本领域数据安全监管职责……

2021年7月

《关键信息基础设施安全保护条例》

确认关键信息基础设施包括了水利等重要行业和领域，并对其安全保护指导工作给出具体指示。

2022年12月

中共中央 国务院《关于构建数据基础制度更好发挥数据要素作用意见》

“数据二十条”提出构建数据产权、流通交易、收益分配、安全治理等制度…初步形成数据基础制度的“四梁八柱”…

2025年1月

《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》

将安全贯穿数据供给、流通、使用全过程，落实国家数据分类分级保护制度，明晰数据流通中的安全治理规则，……

2025年10月

《中华人民共和国网络安全法》

国家对公共通信和信息服务、水利等重要行业和领域，以及其他一旦遭到破坏、失能或者数据泄露，可能严重危害国家关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

2026年2月

《供水条例》（国务院令 第 831 号）

第三十四条 供水设施信息系统的运行维护单位应当建立健全网络安全管理制度，落实网络安全防护措施等安全要求；对其中的重要网络设施、信息系统等，依法纳入关键信息基础设施范围实行重点保护。



行业背景-智慧水务国内标准建设现状

仅4项

500余项

水务行业数据标准

政务类及信息技术类数据标准

标准层级

行业标准具有权威性和针对性，但**数量偏少**，内容偏重于硬件设备设施、软件系统的技术和应用，**对于智慧水务规范化的指导不足**，行业对于智慧水务的共识有待加强。

标准标龄

现行标准中，**行业标准平均标龄最长**，由于智慧水务技术的快速发展与行业需求的升级，部分标龄较长的标准**已不能满足现在的应用需求**。

标准侧重方向

在各专业领域中，水质监测、流量监测、管网漏损监测等监测与监控类标准占比较多，涵盖了单元或业务，相对而言，**智能控制、智慧决策、新兴技术和水务业务融合方面的标准较为缺乏**。**智慧水务标准内容不均衡**，尚不能为水务行业由信息化、数字化、传统自动化向智能化运行、智慧化决策推进提供全面、有效的指导。

行业背景-新技术引入的隐藏风险

随着新型智慧城市建设和水务数字化转型加速，大数据、人工智能、物联网（IoT）、数字孪生、云计算、5G等新技术与城乡水务信息化系统深度融合，推动水务信息化系统从基础数据采集向全流程智能管控升级，在提升运营效率的同时，也引入了新的安全风险。

物联网（IoT）终端普及带来的终端安全隐患

作为水务信息化系统的“末端感知节点”，大量物联网终端直接接入主干系统，但因**终端本身防护不足、通信传输无加密、管理混乱，易被篡改、破解或入侵**，不仅威胁系统数据真实性、破坏传输链路，还会**增加信息化系统的入侵风险**，其安全隐患直接传导至整个水务信息化体系。



大数据与人工智能应用带来的数据安全与算法安全隐患

大数据与人工智能推动水务信息化系统从“数据存储”向“智能决策”升级，但**数据集中存储易因防护不足引发泄露、篡改等问题**，威胁系统核心资产；同时**算法“黑箱”特性及自身漏洞，易被攻击利用**，影响信息化系统决策的可靠性，进而引发运营风险。



5G与工业互联网融合带来的通信与协同安全隐患

5G技术支撑水务信息化系统实现远程控制、跨域协同，但**5G网络及终端存在安全漏洞，易破坏系统通信链路**；同时**水务信息化各子系统及关联部门系统安全标准不一、缺乏协同机制，易引发安全事件连锁扩散**，威胁系统稳定运行。



新技术应用带来的管理与人员安全隐患

新技术推动水务信息化系统迭代升级，但**行业普遍存在信息化管理体系滞后、相关人员安全意识和专业能力不足的问题**，进一步**放大了新技术给水务信息化系统带来的各类安全隐患**，影响系统安全防护成效。





行业背景-数据要素化背景下的数据安全挑战

在数据要素化发展背景下，水务数据已升级为行业核心生产要素和重要战略资产，而水务信息化系统作为水务数据汇聚、存储、流转、加工和应用的核心载体，其数据资产保护面临更为突出的安全挑战，具体体现在以下方面：

1

数据价值提升加剧攻击风险，威胁数据资产完整性与价值

数据要素化推动水源监测、管网运行、用户用水、水厂运营等多源水务数据向信息化系统集中整合，数据的聚合效应使**数据资产价值大幅提升**，进而**成为网络攻击的首要目标**。攻击者通过技术手段发起数据泄露、篡改、窃取等安全事件，直接损毁数据资产价值，破坏数据资产的完整性，影响水务信息化系统基于数据开展的调度、决策等核心业务。

2

数据流通共享引发边界混乱，加剧数据资产泄露滥用风险

数据要素流通、共享的核心需求，打破了水务数据封闭管理的传统模式，跨系统、跨部门、跨区域的数据交互日益频繁。但当前**水务行业缺乏完善的数据资产分级分类保护机制**，导致数据资产边界模糊、权责划分不清，且数据在水务信息化系统与关联系统流转过程中，**缺乏全流程安全管控措施**，进一步加剧了数据资产泄露、滥用、非法交易的风险。

3

资产保护体系滞后，难以适配数据要素化发展需求

面对数据要素化带来的新场景、新需求，现有防护措施多聚焦于传统数据存储安全，**未针对数据要素化特点构建全生命周期资产保护体系**，无法有效保障数据资产的保密性、完整性和可用性，难以应对数据要素化背景下的多元化安全挑战。

目录

C O N T E N T S

01

编

制

背

景

02

标

准

内

容

03

标

准

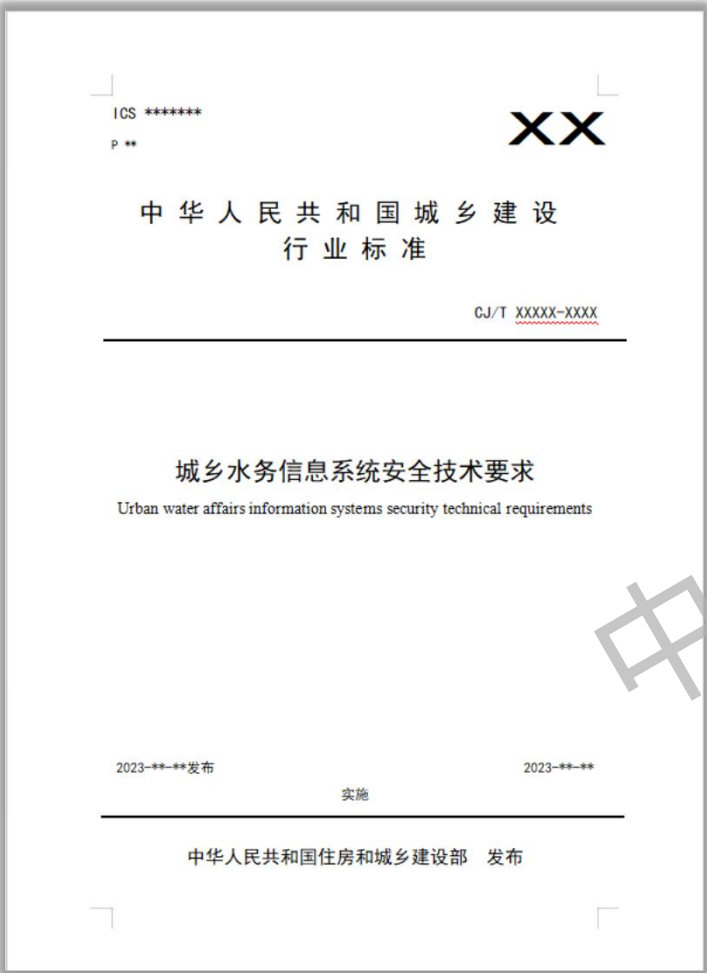
意

义



行标成果框架结构

本文件规定了城乡水务信息系统安全的总体要求、技术要求和保障体系。适用于我国城乡范围内供水、排水、污水处理、再生水、水资源管理、水环境等领域的信息系统建设与运维安全技术工作。



城乡水务信息系统 安全技术要求

第1-3章 范围、引用文件 术语与缩略语

主要介绍了标准的适用范围、规范性引用文件，以及相关术语和缩略语。

第4章 总体要求

主要阐述了安全原则、安全技术总体架构、水务系统全生命周期管理、信创实施要求以及网络安全等级保护要求。

第5章 技术要求

主要从物理安全、网络安全、应用安全、基础设施安全和数据全生命周期等方面提出了具体技术措施。

第6章 管理保障体系

主要规定了信息安全组织与制度建设、安全审计与评估以及信息安全培训的内容与要求。

附录及条文说明

提供了水务行业信息系统风险等级表、数据分类分级参考表、安全应急预案模板，并对条文执行中的注意事项进行了说明。



总体要求-安全原则

01

参照性原则

以企业网络安全需求为基础，未尽事宜及执行冲突时，优先遵循国家等级保护制度、相关法律法规及监管最新要求。

02

保密性原则

聚焦管网、用户用水、水源地等敏感信息，通过数据传输（TLS 加密）、存储加密，结合身份认证、权限管理，限制敏感信息仅被授权访问。

03

可用性原则

通过双机热备、多链路冗余等冗余设计规避单点故障，建立应急预案并定期演练，合理规划系统资源，保障授权用户、系统及业务持续可靠访问。

04

最小权限原则

为用户、进程、服务分配完成任务所需的最小权限，精细化划分角色权限，限制系统进程资源访问范围，降低权限过大带来的安全风险。

05

持续改进原则

建立安全监测与评估机制，及时发现并修复漏洞，跟踪行业安全动态与技术趋势，完善安全保障体系，加强员工安全培训，提升安全文化。

06

合规性原则

数据全环节遵循合规、正当、必要原则，配合监管检查与等级保护测评，落实关键信息基础设施重点保护，根据法规政策调整安全管理制度。

07

先进性原则

安全建设与行业应用趋势同步，针对人工智能大模型等新兴技术，配置相应安全管理机制与技术防护手段，保持技术先进性。

总体要求-信息系统生命周期管理

01

规划设计阶段

安全需求分析

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

设计涵盖物理布局、网络架构、数据分类与保护、访问控制策略、安全防护体系等安全架构。

安全方案设计

严格审核合作伙伴（如供应商、集成商、运维服务商等）的安全资质与能力。

02

建设实施阶段

安全控制集成

按方案落实软硬件配置、网络布设及应用开发的安全措施。

工程监理与审计

通过独立监理与审计全程监控，及时消除隐患。

建设文档与证据保留

确保各阶段文档齐全、真实、可追溯。

03

运行维护阶段

运维安全管理

制定并执行系统升级维护、漏洞管理、应急演练、备份与恢复、资产变更管理等日常运维安全管理策略。

安全监控与审计

实时监控运行状态，定期审计并持续优化安全措施。

多方协同与沟通

建立信息通报机制，确保安全事件发生时能快速联合响应。

04

销毁阶段

数据彻底清除

严禁逻辑删除。废弃介质须物理销毁，保留设备须按国标多次覆写，确保数据不可恢复（含主库、备份、日志）。

介质与资产处置

涉密及关键设施必须委托有资质的机构处理。

严格管控

须经业务、安全、数据多部门共同确认，并留存销毁记录归档。



总体要求-信创要求

信息技术应用创新，其核心是实现信息系统软硬件国产化、关键技术自主可控。围绕服务器、操作系统、网络安全设备及 SCADA、调度等业务系统全面适配，采用国密算法保障数据安全，确保水务生产运行稳定可靠、供应链自主安全。

基础软硬件信创替代要求

硬件自主可控，优先采用国产服务器、工控机、网络设备、安全设备、存储设备，逐步降低对国外专用硬件的依赖。

- **操作系统与基础软件：**优先使用国产操作系统、国产数据库、国产中间件，实现基础环境自主可控。
- **终端与外设信创：**逐步实现国产 CPU、国产终端、国产加密卡 / 密码机全覆盖。

网络与安全设备信创适配

- **网络设备：**交换机、路由器、防火墙、负载均衡等采用国产品牌并支持国密算法。
- **安全设备：**入侵检测、堡垒机、日志审计、终端安全管理、网闸等优先选用信创目录内安全产品。
- **边界隔离：**生产控制大区与管理信息大区隔离设备支持信创环境部署与国密协议。

国密算法与密码应用要求

- 关键数据传输、身份认证、报文签名、远程控制指令等采用 SM1/SM2/SM3/SM4 国密算法。
- 建立基于国产密码基础设施的身份认证体系，实现运维人员、设备、系统间可信认证。
- 重要配置文件、敏感业务数据采用国密算法加密存储，满足等保与密评要求。

水务业务系统信创适配

- SCADA、调度系统、营收系统、GIS管网系统、水质监测平台等核心业务系统完成信创环境适配与迁移。
- 新建系统遵循信创优先设计原则，不引入无法替代的国外技术架构。
- 支持跨平台、国产化环境稳定运行，不影响水务生产连续性。

信创环境下的安全运行保障

- 信创软硬件纳入统一安全运维、漏洞管理、版本更新体系。
- 建立信创环境兼容性测试、压力测试、故障演练机制。
- 信创设备与工控系统联动不降低实时性、可靠性与安全性。

供应链与第三方安全管控

- 关键软硬件产品来源可追溯，优先选择国内供应链稳定厂商。
- 禁止使用存在后门、漏洞风险、受限出口的国外关键技术产品。
- 第三方服务、云服务、集成服务需满足信创与数据安全双重要求。



总体要求-等级保护要求

城乡水务信息系统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，水务信息系统可按照以下原则划分风险等级：

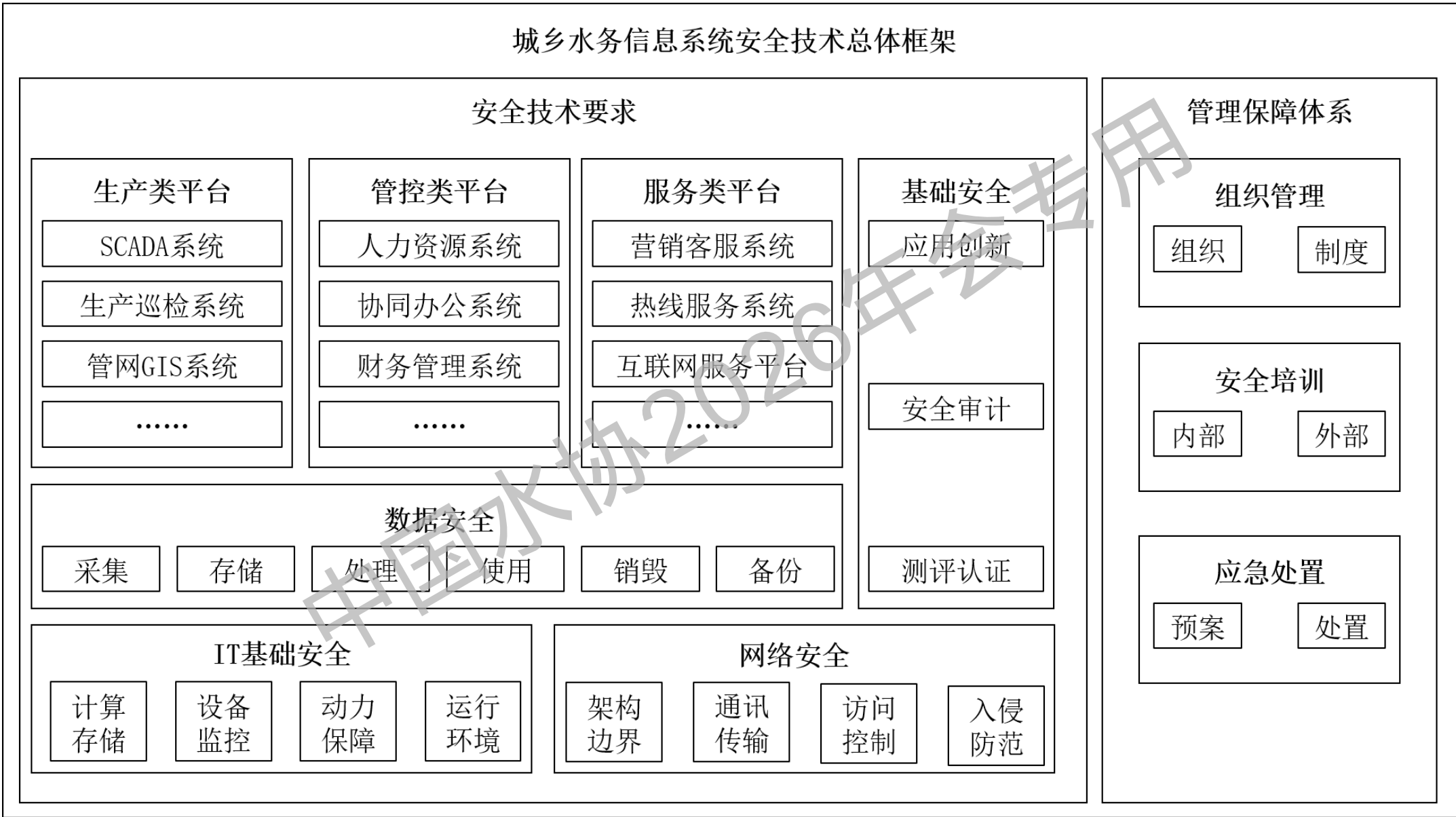
- a)系统/网站只能浏览，无信息交互，定为第一级。
- b)系统/网站不涉敏感信息（如管网坐标）或用户个人信息，定为第二级。
- c)系统/网站涉敏感信息或用户个人信息，定为第三级。

生产运营类	污水厂/污水泵站工控系统	水厂/污水厂综合管理系统	水厂/泵站工控系统	
	供排水管网地理信息系统	DMA分区计量管理系统	生产调度管理系统		
营销客服类	报装管理系统	抄表管理系统	收费管理系统	客服热线管理系统
管理管控类	办公自动化系统	安防系统	门户网站	



安全技术总体框架图

城乡水务信息系统安全技术总体框架





安全技术要求（一）

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**。

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**。

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。

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**。



安全技术要求（二）

访问控制

访问控制**须基于最小权限原则进行配置**。软硬件设备与应用系统应采用高强度或国密算法进行身份认证，设置复杂密码并定期强制更换。同时，必须具备防暴力破解机制，通过限制密码错误尝试次数以及对违规账户或IP进行自动锁定来阻断非法访问。

云服务安全

涉密数据及应用系统严禁使用公有云，敏感业务应**优先选用私有云部署**。使用云服务时，应定期将数据导出进行离线备份或多云异地备份以保障安全。在退出公有云服务前，必须彻底清除云端数据，严防信息残留。

物联网安全

物联网网络规划时应实现**数据加密传输**，并通过配置访问白名单实现数据的定向传输，防范数据泄露与非法访问。此外，宜选用支持在线固件升级（OTA）的物联网设备，以便及时远程下发补丁修复安全漏洞。



安全技术要求（三）-数据安全是重点

数据采集、传输、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。

数据采集

须**明确目的范围，确保合法合规，并对数据进行分类分级标识与安全管控**。特别是隐私和机密数据，需加强人员设备管理、全程记录流向，间接获取须签协议明确责任。

01

数据存储

须**对不同级别数据实施物理或逻辑隔离**。隐私和机密数据必须采用符合国标（GB/T 37092）的密码技术保障安全，并全面统筹架构与访问控制，建立完善的冗余与备份恢复机制。

03

数据交换共享

须**合规并落实责任转移，共享前必做风险评级与脱敏，全程可审计**。中台按需处理明密文、明晰安全责任；文件异构加密、加密通道传输；数据交易确权估值后，软硬件双重加密，封闭环境保障信息对称。

05

数据备份

须**实施加密与严格访问控制防泄露，采用异地多介质多重备份策略抵御破坏**。日常需定期开展完整性检查与恢复测试，实时监控备份状态，并定期审计更新备份策略以保障持续可用。

07

数据传输

须**采用国标加密算法保障机密性，利用数字签名或哈希算法防篡改并在接收端验证**。同时，对收发方实施双向身份鉴别与严格访问控制，高敏感数据须采用动态访问控制。

02

数据处理

明确目的范围，落实最小授权与细粒度访问控制，保障脱敏与溯源安全。操作需全程可审计，自动化决策须透明公平，重点防范处理结果中的敏感数据恢复风险及AI算法模型风险。

04

数据销毁

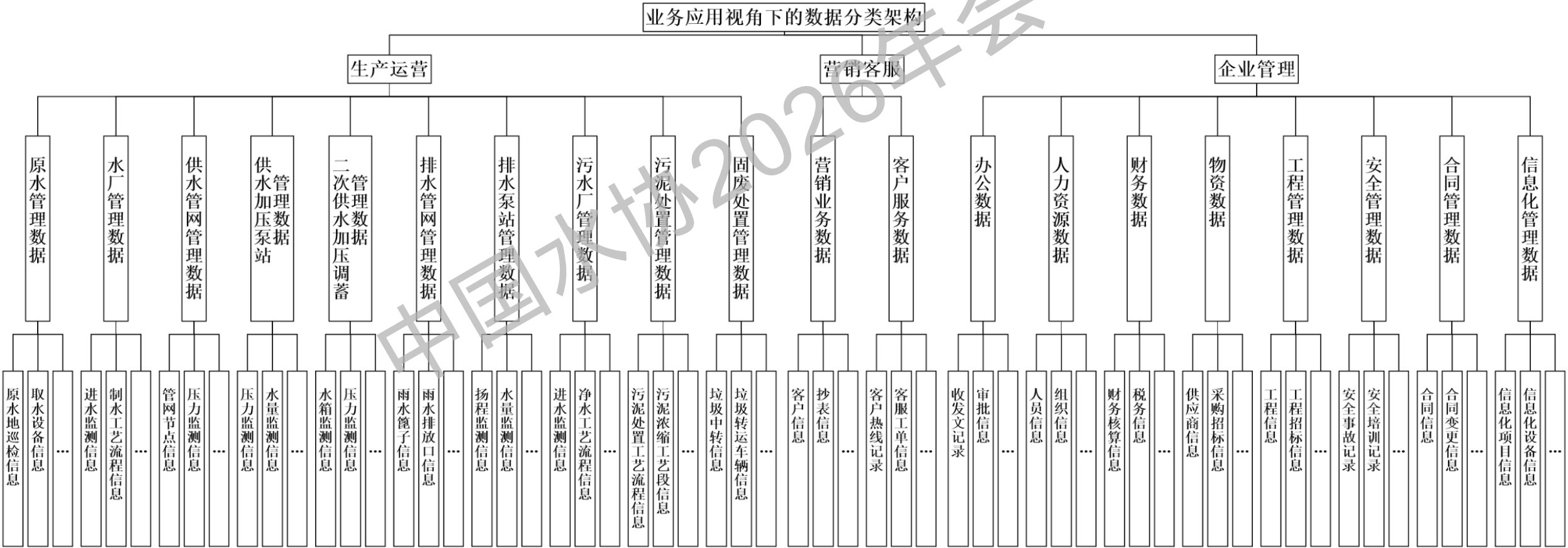
须**按分类分级建立机制，及时清理超期及依申请销毁的数据**。销毁过程须全记录留痕审计，特别是隐私和机密数据销毁后严禁以任何方式恢复，涉备案变更须及时办理。

06



安全技术要求（三）-数据安全是重点-数据分类架构（业务视角）

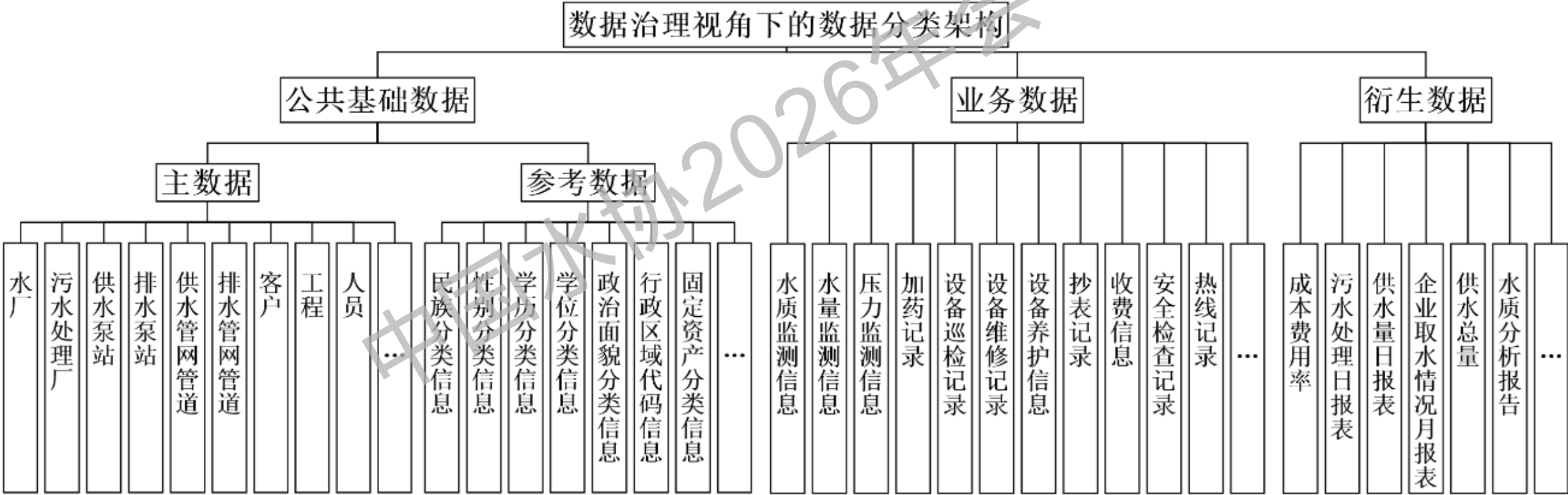
采用线分类法，结合水务的业务现状，按照数据生产来源、业务归属的维度逐次地分成三个层次类目，第一层为三大主题数据域，第二层为各条业务线主题数据，第三层为各条业务线下的业务对象及业务对象产生的记录数据，即数据实体。





安全技术要求（三）-数据安全是重点-数据分类架构（数据治理视角）

采用线分类法，按数据治理的要求，将水务数据分为三大类，即**公共基础数据**、**业务数据**和**衍生数据**。公共基础数据可按数据特性和管理要求进一步划分为主数据和参考数据。





安全技术要求（三）-数据安全是重点-数据分类架构（安全隐私视角）

采用混合分类法，按数据的敏感性、保密性以及数据遭篡改、破坏、泄露或非法利用后可能对企业生产、经济效益等带来的潜在影响，将水务数据按敏感程度分为**公开**、**内部**、**私密**、**机密**等四大类别。





安全技术要求（四）-AI大模型安全需重视（一）

➤ 模型安全评估与可信验证

投入运行前应对大模型开展安全风险评估，包括对抗性攻击风险、指令注入风险、恶意诱导风险、输出偏差风险等。确保模型在水务调度、水质研判、故障诊断、客服应答等场景中输出稳定、结果可解释、决策可复核，避免因模型幻觉、错误推理导致生产运行事故。

➤ AI 模型全生命周期安全管控

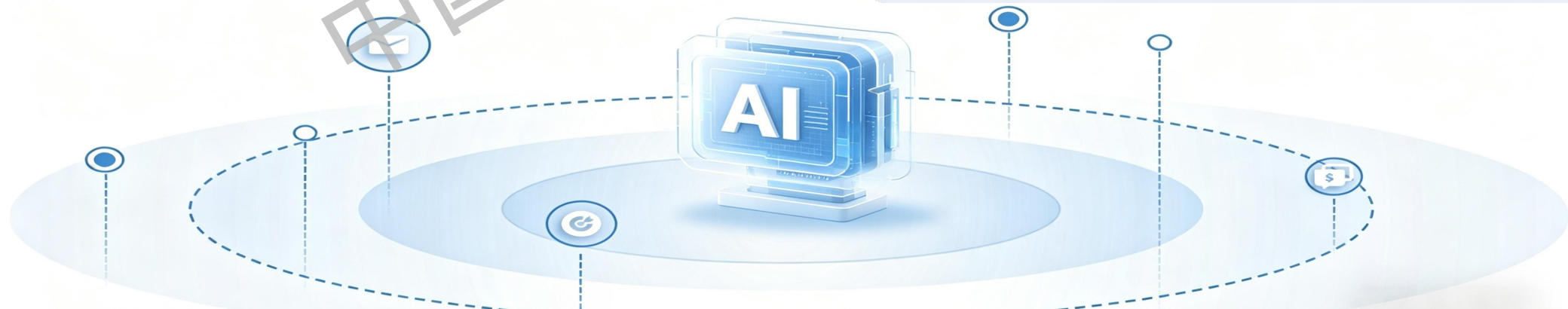
水务场景应用人工智能大模型时，应建立覆盖模型训练、数据标注、推理部署、版本迭代、下线退役的全生命周期安全管理机制。明确模型安全责任人，对模型来源、训练数据、算法逻辑、调用接口实施可追溯管理，禁止使用未经安全评估的开源或第三方大模型直接接入水务生产控制系统。

➤ 训练与推理数据安全

用于大模型训练、微调、提示词输入的水务数据，包括供排水监测数据、管网地理信息、用户用水信息、调度指令、水质数据等，应严格执行数据分类分级要求。

➤ 边界隔离与访问控制

大模型应用系统应与水务 SCADA、PLC、管网监控等生产控制区实施逻辑隔离，部署独立安全域。模型接口调用应采用身份认证、权限最小化、操作审计、流量限流等措施，禁止未授权访问、越权调用和批量数据上传，防止通过 AI 应用形成攻击跳板。





安全技术要求（四）-AI大模型安全需重视（二）

➤ 安全审计与责任可追溯

对大模型的输入提示、推理过程、输出结果、用户调用行为进行全程日志留存，满足安全审计要求。日志应不可篡改、可追溯，支撑安全事件定位、责任界定与合规检查。

➤ 应急处置与运行监控

建立 AI 模型运行异常监测机制，对模型异常响应、服务中断、非预期输出、可疑调用行为实时告警。制定模型安全应急处置预案，明确模型降级、人工接管、下线停用、溯源追责流程，确保 AI 应用失效时不影响水务核心业务连续运行。

➤ 内容安全与合规输出

大模型在水务客服、政策解读、信息发布等对外服务场景中，应建立内容审核机制，对输出结果进行安全校验与合规过滤，确保信息真实准确，不产生误导性、错误性、敏感性内容，保障水务公共服务权威性。





信息安全组织

信息安全领导小组

作为宏观领导机构，采用“多方协作、集中管理、逐级负责”模式。

主要职责包括：制定安全总体规划与策略并监督实施、细化落实上级规章制度、审批管理层以上人员权限、审阅安全工作报告，以及查处与汇报重大安全事故。

信息安全工作组

作为具体执行机构。

主要职责包括：落实安全方针与体系建设规划、建立健全并监督执行管理制度、开展安全防护建设与日常运维（含风险评估与漏洞整改）、统筹安全培训与应急演练、处置安全事件，以及组织内部合规检查与配合外部审计测评。

信息安全制度

信息系统安全管理应配套制度和相关作业流程标准，相关制度流程可根据各单位的具体情况制定，制度主要包括以下内容：

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



管理保障体系-信息安全审计与评估-安全审计与评估管理

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。



评估工作角色与职责

评估应由具备相应能力的评估机构实施，相关人员应经培训合格。
评估机构主要职责包括：编制评估实施方案、组织内部评审并实施安全评估、出具正式评估报告并提出整改建议，以及对评估结果组织评审。



保密工作

实施前需与被评估单位签订保密协议，明确双方责任；过程中对敏感信息遵循最小接触原则，仅授权必要人员知悉；所有参与人员须签署保密协议，不得擅自对外提供或不当使用相关数据与结果；不得将设备带出允许场地，评估结束后及时归还或按约定保管、销毁资料，不得在第三方场合公开引用。



风险控制

评估实施前应明确评估范围，开展风险分析并制定防范和控制措施。
实施过程中应遵守相关操作规程，防止信息泄露；评估活动应尽量避免水务工控与生产调度系统敏感作业期；必要时制定应急预案；对位于生产控制区且无法搭建模拟环境的系统，不得使用评估工具，应采用人工评估方式。



管理保障体系-信息安全审计与评估-安全审计与评估方法

资产识别

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。在确定评估范围后，应对其资产价值进行分析。资产主要包括信息、软件、硬件、人员和系统五个表现形式。

资产安全等级赋值

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，需参照GB/T 28448开展。该等级共划分为5级，等级越高代表资产重要性与受损影响越大。

威胁评估

根据城乡水务信息系统的运行环境确定威胁来源、威胁严重程度和发生频率。结合资产分类，按安全分区、资产类别对系统独立或整体开展统一判断，并满足：a) 根据物理、网络和人员环境，对资产进行威胁判定；b) 根据威胁出现频率判断得出等级，赋值越高面临威胁越大。

脆弱性评估

脆弱性评估是发现和分析城乡水务信息系统中可能被威胁利用的缺陷的过程。包括两个步骤：

脆弱性识别：

- 技术管理脆弱性主要关注物理层、网络层等方面的安全问题；
- 组织管理脆弱性则通常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也是发现脆弱性的重要方法。

风险性分析

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：

$$\text{风险值} = R(A, T, V)$$

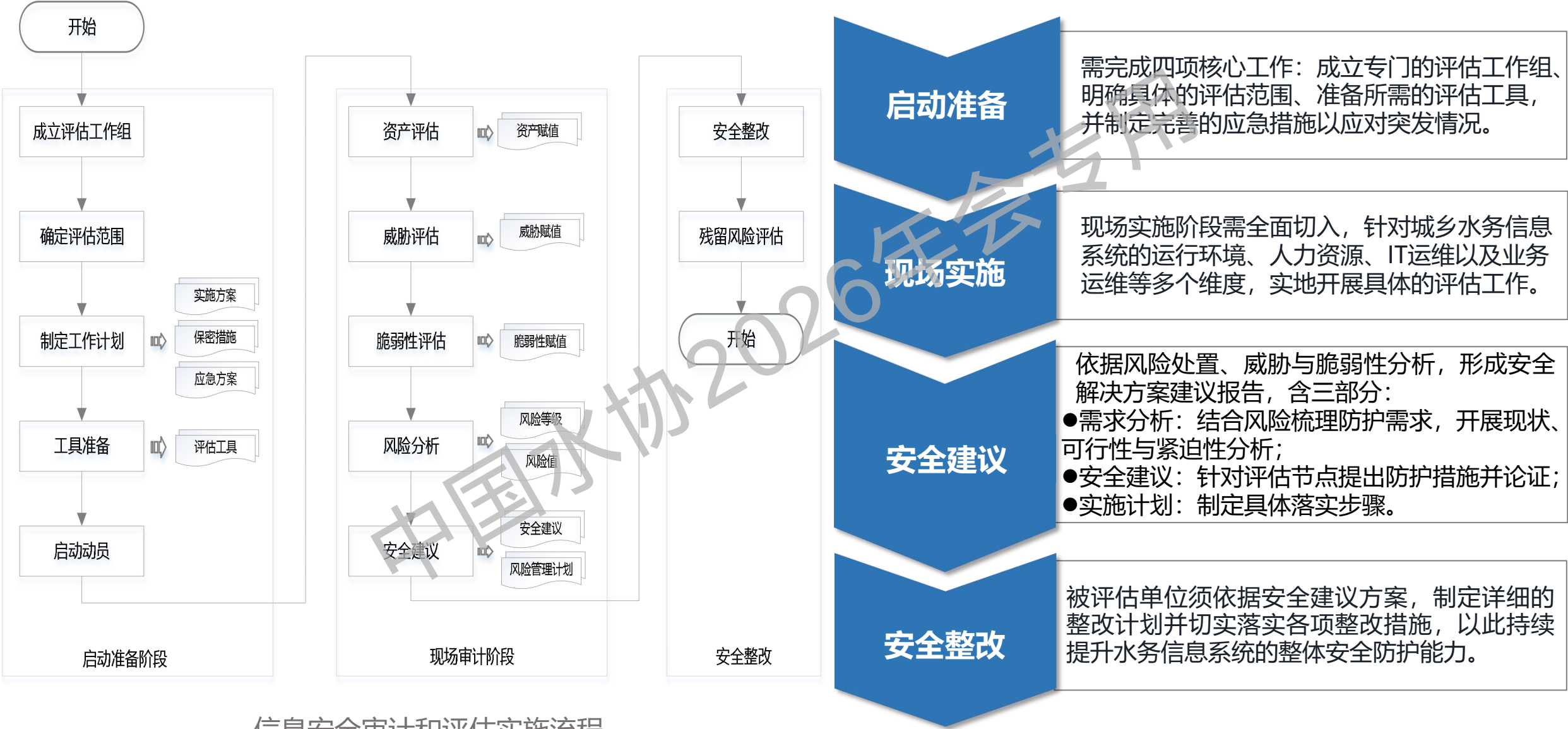
为实现对风险的控制与管理，对风险评估的结果进行等级化处理，风险共划分为五级，等级越高，风险越高。并按照风险等级采取相应风险控制措施。

脆弱性赋值：

- ◆ 脆弱性的严重程度；
 - ◆ 对系统安全属性的影响；
- 具体来说，就是要判断脆弱性让资产暴露在多大风险下，以及脆弱性破坏了哪些安全属性。



管理保障体系-信息安全审计与评估-评估实施流程





培训制度

- 需要建立覆盖城乡水务企业全员的信息安全培训制度，培训对象包括系统用户、运维人员以及各级管理人员。
- 新员工入职培训中也应纳入信息安全内容，并且培训需要定期更新和重复进行。
- 根据需求分析的结果，针对不同评估节点提出相应的安全防护措施。

培训内容

① 法规政策教育

学习国家相关法律法规、行业标准以及企业内部信息安全管理制度的相关内容，让相关人员明确自己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

包括操作系统安全设置、数据库安全、应用系统安全使用方法，以及移动设备和BYOD（自带设备办公）的安全管理等。

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；同时定期组织模拟攻击与防御实战演练，提升应急处理能力。

目录

C O N T E N T S

01

编

制

背

景

02

标

准

内

容

03

标

准

意

义

中国水协2026年会专用



标准意义-筑牢安全底线，保障关键基础设施生命线

本标准立足城乡水务信息系统全生命周期，构建物理安全、网络安全、基础设施安全、应用安全、数据安全及信息安全管理保障体系的全维度纵深防护体系。通过明确数据加密、分级防护、访问控制与应急响应等硬性要求，有效防范工控系统攻击、数据泄露与业务中断风险，将水务这一关键信息基础设施的安全韧性提升至新水平，守护城市运行与民生福祉的核心屏障。

统一技术规范，重塑行业高质量发展标尺

行业长期面临标准不一、防护水平参差不齐的痛点。本标准**填补城乡水务信息安全领域的体系化空白**，为水务业务提供**统一、可落地**的技术指引与评价依据，推动行业从“重建设、轻安全”的粗放模式转向**安全与发展并重的高质量范式，规范市场秩序**，引导资源向具备安全合规能力的主体集中，加速产业生态的协同升级。

支撑合规建设，降低全生命周期风险成本

标准**深度衔接《网络安全法》《数据安全法》及等级保护2.0要求**，为企业提供合规建设的清晰路径。**通过标准化的风险评估、策略落地与运维机制**，帮助企业系统性降低法律处罚、经济损失与声誉风险，同时减少重复建设与无效投入，**实现安全投入效益最大化**，助力企业构建可持续的安全竞争力。

赋能数据要素流通，释放数字化核心价值

标准以**数据分类分级与全生命周期安全治理**为核心，在合规前提下**打通数据流通壁垒**，支撑水务数据在跨部门共享、预测性调度、漏损控制、智慧服务等场景安全应用，推动行业从“数据可视化”向**数据驱动决策**跃迁，为数字孪生、智能运营等前沿应用奠定安全基石，释放数据要素的经济与社会价值。

引领技术创新，构建行业安全新生态

标准**引领产业链协同创新，推动一体化安全技术体系的研发与应用**。它将安全从“附加项”升级为核心竞争力，促使企业聚焦核心技术突破，形成**“标准引领、技术支撑、产业协同”**的良性生态，全面提升我国水务行业在数字化转型背景下的整体抗风险能力与国际竞争力。



打造最具价值的水务产业大脑



许冬件

Tel: 138 2566 6226

Email: xdj@shuiwujia.com

感谢聆听 欢迎交流指正