ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL —2026

河流水质监测数据采集、传输与存储安全技术规范

Standard for Security Technology of Data Collection, Transmission and Storage in River Water Quality Monitoring

（工作组讨论稿）

（本草案完成时间：2026-01-29）

2026 - - 发布　　2026 - - 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

河流水质监测数据采集、传输与存储安全技术规范

1 引 言

随着我国生态文明建设深入推进、水污染防治行动持续攻坚，河流水质监测作为水资源管理与生态环境保护的基础性、关键性工作，其战略地位日益凸显。监测数据的真实性、完整性、机密性与可用性，是客观评价全国水环境质量状况、科学制定流域治理与保护政策、精准实施环境监管执法、保障国家水安全的核心支撑。近年来，物联网、云计算、大数据等新一代信息技术在水质监测领域的规模化应用，显著提升了监测工作的自动化、智能化与网络化水平，但同时也使监测数据在采集、传输、存储全流程面临更为复杂的安全风险，设备被篡改、通信被劫持、数据被伪造、信息被泄露等问题，直接威胁水环境管理决策的科学性与公信力，关乎国家生态安全与公共利益。为全面落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国环境保护法》等法律法规要求，规范河流水质监测数据全流程安全管理，构建覆盖采集、传输、存储各环节的安全保障体系，防范化解数据安全风险，保障监测数据安全可控，结合我国河流水质监测工作实际与国家生态文明建设战略需求，特制定本规范。本规范为河流水质监测系统的设计、建设、运行、维护提供统一的安全技术遵循，适用于各级监测机构、设备制造商、系统集成商及数据服务单位开展的河流水质监测相关活动，助力推动我国水环境监测工作高质量、安全有序发展。

2 范围

本规范规定了河流水质监测数据采集、传输与存储过程中的安全技术要求，涵盖总则、数据采集安全、数据传输安全、数据存储安全、安全管理要求及附则等核心内容。本规范适用于通过自动监测站、移动监测设备、遥感监测等各类技术手段开展的河流水质监测活动，涉及监测数据采集终端、通信网络、数据中心（含云平台）等关键环节的安全设计、实施与运维。其他类型水环境监测活动可参照本规范执行。

3 规范性引用文件

下列文件对于本规范的应用具有强制性或指导性作用。凡是注日期的引用文件，仅所注日期的版本适用于本规范；凡是不注日期的引用文件，其最新版本（包括所有修改单）均适用于本规范。

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

GB/T 37025-2018 信息安全技术物联网数据传输安全技术要求

GB/T 37973-2019 信息安全技术大数据安全管理指南

GB/T 37988-2019 信息安全技术数据安全能力成熟度模型

HJ 92-2022 地表水自动监测技术规范

HJ 477-2022 污染源在线自动监控（监测）系统数据传输标准

SL 651-2019 水文监测数据通信规约

《国家水资源监控能力建设项目标准水资源监测数据传输规约（试行）》（水利部，2014 年）

4 术语和定义

下列术语和定义适用于本规范。

4.1 河流水质监测数据

指通过自动或手动方式获取，反映河流水体物理、化学、生物等指标状况的原始数据、预处理数据及衍生数据，涵盖水温、pH 值、溶解氧、电导率、浊度、高锰酸盐指数、氨氮、总磷、总氮等核心参数监测值及对应时空信息。

4.2 数据采集终端

指部署于河流监测断面或点位，用于采集、处理和临时存储水质监测数据的现场设备及组合，主要包括水质传感器、数据采集仪、供电单元、防护箱体等组件。

4.3 监测数据中心

指承担河流水质监测数据接收、处理、存储、管理和分析职能的中心服务器集群、数据平台或云服务平台，是数据集中管控的核心载体。

4.4 安全传输

指运用密码技术和安全协议，保障监测数据在传输过程中保密性、完整性和可用性的全过程防护行为。

4.5 安全存储

指通过技术与管理双重措施，保障监测数据在存储状态下保密性、完整性和可用性的安全状态，包含静态存储安全与动态访问安全两大维度。

5 总则

本章节明确河流水质监测数据安全工作的核心遵循、等级要求与全流程管控原则，为各环节安全措施落地提供总体指引。河流水质监测数据采集、传输与存储安全工作，必须遵循“安全合规、预防为主、重点保护、全程管控、持续改进”的核心原则，全面落实总体国家安全观，严格符合国家网络安全等级保护和关键信息基础设施安全保护相关要求，确保监测数据全生命周期的真实性、完整性、机密性、可用性与可追溯性，为国家水环境治理与生态安全决策提供可靠数据支撑。应依据河流水质监测数据的重要性、敏感程度，以及监测系统遭到破坏后可能造成的生态危害、社会影响和经济损失，对照 GB/T 22239-2019 明确网络安全保护等级。其中，涉及国控、省控等重点监测断面，以及用于考核评价、环境执法、应急处置等关键用途的监测数据，其相关系统安全保护等级原则上不低于第二级；涉及国家秘密或核心敏感数据的，须严格按照法律法规要求执行更高等级安全保护标准。应建立覆盖数据采集、传输、存储、处理、交换、销毁的全生命周期安全管理体系，打破各环节安全壁垒，实现各阶段安全措施有效衔接、协同发力，构建闭环式安全防护链条，全面提升监测数据安全保障能力。

6 数据采集安全

数据采集是监测数据安全的源头环节，需强化采集终端、传感器与数据源、现场数据的全维度安全管控，从源头防范数据失真、设备被篡改等安全风险。

6.1 采集终端安全

6.1.1 物理层面：采集终端应部署于具备防盗、防破坏、防雷击、防水、防潮、防腐蚀功能的专用防护设施内，固定站房需配备门禁系统和视频监控设备，监控数据留存时间不少于 90 天；野外无人值守站点应采取隐蔽安装、结构加固等防护措施，最大限度降低物理暴露风险。

6.1.2 设备层面：应选用具备防篡改、防拆卸能力的数据采集仪，关键固件与软件需建立完整性校验机制，禁用不必要的硬件接口（如 USB）和网络服务，定期开展安全漏洞扫描与修复工作。

6.1.3 访问管控层面：终端设备本地配置接口和远程管理通道必须实施严格身份认证，严禁使用默

认口令，访问权限需按照管理人员角色实行最小化分配。

6.2 传感器与数据源安全

6.2.1 传感器选型：需符合 HJ 92-2022 等相关标准要求，具备完整出厂校准报告，同时建立常态化定期校准与维护制度，及时排查设备故障、消除恶意干扰，确保传感器测量精度与稳定性。

6.2.2 自动采样单元：需采取防样品污染、防样品混淆措施，保障采样过程的规范性与代表性，完整记录采样过程日志，实现采样环节可追溯。现场数据安全需强化临时存储防护、异常识别与日志审计。

6.2.3 临时存储方面：采集终端内置存储介质（如存储卡）需具备数据保护功能，防止非法取出读取，存储数据需实施完整性保护措施。

6.2.4 异常数据识别方面：数据采集软件应具备数据合理性检查与异常值识别功能，对显著偏离历史规律或物理极限的数据进行自动标记，并详细记录相关异常事件。

6.2.5 日志审计方面：需完整记录数据采集起止时间、采集参数、操作人员、设备状态、校准事件、异常事件等信息，日志保存时间不少于一年，建立防非法删除、防篡改机制。

7 数据传输安全

数据传输是监测数据安全的关键环节，需聚焦通信链路、传输过程、传输设备与网关三大核心要素，构建全方位、立体化的传输安全防护体系，保障数据在传输过程中不被窃取、篡改或劫持。

7.1 通信链路

安全需优化链路选型与接入管控。应结合监测点位环境条件与安全需求，科学选择专用线路、4G/5G、NB-IoT、光纤等通信方式，对于国控断面、应急监测点位等重要监测节点，应采用主备双链路传输模式，提升链路可用性与抗干扰能力。监测终端接入网络前，必须实施严格的身份认证，可采用数字证书、预共享密钥等强认证机制，坚决杜绝非法终端接入网络。

7.2 传输过程

安全需强化协议规范、数据加密与完整性保护。传输协议必须符合 HJ 477-2022、SL 651-2019 等行业规约要求，鼓励采用增强安全性的协议版本或补充安全扩展功能。监测数据在公共网络（如互联网）传输时，必须采用符合国家密码管理规定的加密算法（如 SM2、SM3、SM4）进行全程加密；在专用线路传输敏感数据时，也应根据安全需求实施加密防护。同时，采用消息认证码（MAC）或数字签名等技术保障传输数据完整性，防范数据篡改风险，并建立防重放攻击机制，抵御恶意重放攻击行为。

7.3 传输设备

与网关安全需落实安全配置与边界防护要求。通信模块、DTU、RTU、工业网关等传输设备，需进行全面安全加固，修改默认配置，关闭非必要服务和端口，定期更新安全补丁，防范设备被入侵控制。监测网络与公共网络或其他外部网络连接处，必须部署防火墙、入侵检测/防御系统等边界安全设备，制定严格的访问控制策略，精准过滤恶意流量，筑牢网络边界安全防线。

8 数据存储安全

数据存储是监测数据安全的核心保障环节，需围绕存储架构与介质、数据存储本身、数据访问与使用三大维度，构建安全可靠、可控可追溯的存储安全体系，保障监测数据长期安全留存与规范使用。

8.1 存储架构与介质安全

需强化基础防护与分级管控。监测数据中心应采用稳定可靠的存储架构，针对核心监测数据实施异地备份策略；对于海量监测数据，需依据 GB/T 37973-2019 开展分级分类存储管理，提升存储效率与安全管控精准度。存储服务器及介质需放置在符合机房安全标准的物理环境中，实施严格的物理访问控制、环境监控与消防管理措施；废弃存储介质必须进行安全擦除或物理销毁，严防数据泄露。

8.2 数据存储安全

需落实加密防护、完整性校验与备份恢复要求。对于河流水质监测原始数据、敏感管理数据等核心数据，存储时必须进行加密处理，保障静态数据保密性，同时建立加密密钥全生命周期安全管理制度，严防密钥泄露。建立常态化数据完整性校验机制，定期计算和核对数据哈希值，及时发现并处置数据篡改问题。制定完善的数据备份与恢复策略，至少每日开展一次增量备份、每周开展一次全量备份，备份数据需异地存放，定期组织恢复演练，确保备份数据有效可用；关键监测数据备份保存周期不少于 10 年，满足长期追溯与管理需求。

8.3 数据访问与使用安全

需强化权限管控、操作审计与共享防护。建立基于角色的访问控制（RBAC）模型，严格划分用户访问、查询、下载、修改、删除等操作权限，所有数据访问操作必须经过身份认证与授权验证，实现权限最小化管控。对所有用户的数据访问与操作行为进行全程记录，审计日志需包含时间、用户、操作类型、操作对象、操作结果等核心信息，日志留存时间不少于 180 天，建立防篡改、防非法访问机制。向第三方提供数据共享或对外发布数据时，需根据数据敏感级别开展脱敏处理（如模糊化非关键断面位置信息），通过安全通道传输数据，签订数据安全协议，明确各方安全责任与义务，规范数据共享使用行为。

9 安全管理要求

安全管理是监测数据安全的重要保障，需构建制度、人员、运维、应急四位一体的管理体系，压实安全责任，强化全程管控，确保各项安全技术措施落地见效。

9.1 建立健全覆盖全流程的安全管理制度体系

结合工作实际制定安全责任制度、人员管理制度、系统建设与运维安全管理制度、数据分类分级管理制度、应急响应预案等核心制度，明确各部门、各岗位安全职责，形成“责任到人、全程管控”的制度执行机制，确保各项工作有章可循、有规可依。

9.2 强化人员安全管理

严格开展系统管理员、运维人员、数据分析人员等核心岗位人员安全背景审查，定期组织保密教育与安全培训，提升人员安全意识与专业技能。实行权限分离与双人复核制度，关键操作需由两人共同完成，防范内部人员操作风险。

9.3 建立常态化安全技能考核机制

将考核结果与岗位履职挂钩，倒逼人员落实安全责任。规范安全运维管理，建立常态化安全监测机制，每季度至少开展一次安全风险评估、漏洞扫描和渗透测试，及时发现并整改安全隐患。

9.4 对安全事件实行闭环管理

建立隐患排查、整改、复查全流程工作机制，确保隐患整改到位。及时为各类软件、系统安装安全补丁，强化设备与系统日常运维管理，保障监测系统与安全设施稳定运行。

9.5 完善应急响应与处置体系

针对数据泄露、篡改、丢失、系统中断等各类安全事件，制定专项应急预案，明确报告流程、处置步骤、责任分工与恢复措施。每年至少组织一次应急演练，检验应急预案可行性与应急处置能力，根据演练结果动态优化应急预案，提升突发安全事件快速响应与处置水平，最大限度降低安全事件造成的损失与影响。

10 附则

本标准由广西电子商务企业联合会负责解释。本标准自发布之日起试行，试行期为一年。试行期满后，根据实施反馈情况进行修订和完善。各相关单位可依据本标准制定具体的实施细则。若本标准与国

家新颁布的法律法规或强制性标准有不一致之处，应以国家法律法规和强制性标准为准。本标准所引用的规范性引用文件如有更新，其最新版本适用于本标准。广西电子商务企业联合会将根据技术发展和应用需求，适时组织对本标准的复审与修订工作，以保障其持续的先进性和适用性。本标准的有效实施，有赖于各级医疗机构、主管部门、技术服务商和各相关方的共同努力，通过规范智慧医院数据互联互通共享技术，推动医疗健康数据资源有效整合与安全共享，提升医疗服务质量和效率，促进智慧医院建设规范化发展，为推进健康中国建设提供技术支撑。