山西省水利厅办公室文件

晋水办科外〔2024〕20号

山西省水利厅办公室关于进一步加强全省水利信息系统、网络和数据安全管理工作的通知

各市水利(水务)局、厅管厅直各单位:

为进一步做好全省水利信息系统、网络和数据安全工作，加强防范各类安全风险，确保全省水利系统信息基础设施平稳运行。经研究，现就加强信息系统、网络和数据管理提出如下具体要求:

一、落实信息系统、网络和数据管理“十三严禁”

1.严禁未通过等保备案、日志留存不足六个月以及存在高危漏洞的信息系统上网运行。

2.严禁将水利政务、业务系统和数据私自部署在“山西省政务云”以外的任何其他公有或私有云上（市县两级可根据当地网信管理部门要求确定部署环境）。

3.严禁信息化设备、信息系统存在弱口令现象。

4.严禁未采用必要防护措施，将水利专网与互联网接通。

5.严禁将信息化设备同时跨接内外网，未经本单位网络管理部门安全审核的各类终端不得接入水利专网。

6.严禁未安装杀毒软件的信息化设备接入网络，已安装杀毒软件的须及时升级为最新版本。

7.严禁个人终端设备未经授权存储各类口令信息、网络拓扑资料和系统开发源代码等敏感文件。

8.严禁将信息系统源码、口令、数据库表结构、网络拓扑及任何可能带来网络安全风险的信息上传至互联网或在微信等公共社交媒体软件中传播。

9.严禁点击来源不明邮件中的链接或可疑附件。

10.严禁私自开启远程协助类工具，包括但不限于Windows远程桌面程序、向日葵、TeamViewer、VNC等软件，确有必要的需提前向本单位网信管理部门报备。

11.严禁访问来源不明和未经确认安全的网站。

12.严禁以任何形式将工控网与互联网接通。

13.严禁互联网、工控网、涉密网中计算机设备共用或混用带有存储功能的电子设备（如U盘、移动硬盘等）。

二、信息系统、网络及数据安全管理要求

结合当前网络安全和数据安全等各项法规管理制度和要求，提出如下管理要求：

（一）信息系统安全管理要求

1. 建立健全信息系统安全管理制度和流程，明确责任分工和权限控制。

2. 定期进行信息系统安全风险评估，识别潜在的安全威胁和漏洞。

3. 加强信息系统硬件和软件的安全防护，确保系统的稳定性和可靠性。

4. 严格控制对信息系统的访问权限，合理分配权限。

5. 部署有效的入侵检测和防御系统，及时发现和应对安全事件。

6. 建立持续的安全监控体系，定期进行系统安全检查、漏洞扫描、日志审计，及时发现并处置安全风险。

7. 对核心业务数据和关键用户数据进行实时备份，确保在数据丢失或损坏时能迅速恢复。执行严格的隐私保护策略，确保个人信息、涉密文件等敏感数据得到妥善保护。

8. 设立应急响应机制，制定应急预案并定期演练。

9. 建立信息系统安全审计机制，对系统操作进行记录和监控。定期开展内部安全审计，并接受外部独立机构的安全审查，以确保应用系统满足法律法规及相关安全标准的要求。

10.根据安全审计结果、新的安全威胁态势和技术发展情况，不断优化和完善应用系统安全管理制度和技术措施，形成动态调整、持续改进的安全管理体系。

11.对信息系统使用的移动存储介质管理，应登记造册，加强使用管理，避免损坏和丢失。

12.厅管、厅直单位应认真全面梳理在用信息系统，汇总尚未迁移的系统，按照“应迁尽迁”的原则，迁移至“省政务云”部署。

13.在应用系统的规划设计阶段，应充分考虑系统的安全性需求，采用安全架构设计，包括但不限于权限管理、访问控制、加密技术、审计追踪等功能模块，并对可能的安全风险进行全面评估。

14.在应用系统开发、集成、测试过程中，参与的工作人员应进行合理的角色权限划分，实施严格的代码审查，确保软件无漏洞、后门等问题。同时，正确配置各类安全设备和服务，如防火墙、入侵检测系统等。

15.关注源代码的安全性，采用安全编码标准和工具，防范注入攻击、跨站脚本攻击等常见安全威胁。加强对第三方组件、服务提供商的安全审核，确保供应链安全。

（二）网络安全管理

1.建立健全网络安全管理制度和策略，规范网络使用和访问行为。

2. 采用分层、分区的网络架构设计原则，明确内外网边界，实行严格的访问控制策略，防止非法入侵和数据泄露。

3. 所有网络相关软件系统及硬件设备驱动程序应及时升级、打补丁，定期进行安全检查和漏洞扫描，确保设备本身不存在安全隐患。设备配置信息应加密存储并定期备份。

4. 设置防火墙等边界防护设备，实现对外部攻击的有效阻断。同时，部署入侵检测系统、反病毒软件等，实时监控和预警各类网络安全事件。

5. 合理分配网络资源访问权限，严格控制用户对网络资源的访问行为。严禁未经授权的访问或越权操作。

6. 加强对网络设备和通信线路的物理安全保护，防止非法访问和破坏。

7. 采用多因素身份认证机制，包括但不限于口令、数字证书、生物特征等方式，提高身份验证的安全性和可靠性。

8. 对敏感信息和重要数据在传输过程中实施加密处理，采用SSL/TLS 等安全协议保障数据传输过程中的完整性、保密性和抗抵赖性。

9. 定期对网络进行安全漏洞评估和渗透测试，确保网络的安全性。

10. 加强对无线网络安全的管理，采取加密和认证措施保护无线传输数据的安全。

11. 加强工控网的管理，严格落实工控网与互联网物理隔离

要求。

12.对工控网使用的所有移动存储设备管理应登记造册，加强使用管理，避免损坏和丢失。坚决杜绝工控网使用移动存储介质与互联网使用移动存储介质混用情况的发生。

13.建立健全各类终端接入网络的安全检查和准入机制。

14.加强涉密网络管理，严格落实相关管理和规定。

15.建立健全的网络安全应急预案，设立应急指挥机构，定期组织演练，确保在发生网络安全事件时能快速启动响应程序，最大限度降低损失。

16.定期对网络安全策略进行审查和更新，以应对新的安全威胁和挑战。

17.建立网络安全审计机制，对网络操作进行记录和监控。要求所有网络设备及系统必须开启日志功能，对网络活动进行全面记录，并定期进行日志审查和分析，以发现潜在的安全问题。

18.及时更新完善本单位，本部门网络拓扑图。

19.针对关键网络服务和业务系统，制定详细的灾难恢复方案，确保在网络故障或受到攻击后能够迅速恢复正常运营。

20.接受上级监管部门和独立第三方的定期审计，主动配合完成相关安全测评，确保网络安全管理符合国家法律法规和行业标准的要求。

（三）数据安全管理

1.建立健全数据安全管理制度和流程，明确数据分类和访问

权限，可参考水利部办公厅印发的《水利部办公厅关于印发〈水利数据分类分级指南（试行）〉的通知》（办信息〔2022〕256号）。

2. 加强对敏感数据的保护，采取加密和脱敏措施防止敏感数据泄露。按照数据敏感性和重要性进行分类分级，针对不同级别的数据采取相应级别的安全防护措施，如敏感数据加密存储、传输，限制不必要数据的流动。

3. 在合法合规的前提下进行数据采集，公开透明地告知用户数据采集目的、范围及方式，并取得用户的明示同意。对于涉及敏感信息或重要数据的收集，应采取严格的脱敏或匿名化处理。

4. 根据数据的重要性、敏感度等因素对数据进行分类分级存储，并采用物理隔离、逻辑隔离等多种措施保护不同级别的数据资源。所有存储设备必须具备必要的安全防护能力，如防火墙、入侵检测系统等，并定期更新安全补丁和密码策略。

5. 对敏感数据的处理和传输进行加密，确保数据在处理过程中不被非法篡改、泄露。同时，设定清晰的数据流转路径，限制不必要的数据复制、转移行为，对数据的跨境传输严格遵守相关法律法规要求。

6. 依据“按需知悉”原则分配数据访问权限，禁止未经授权的访问、使用或披露数据。在数据共享、开放和交易过程中，须签订保密协议并明确各方的安全责任。

7. 当数据达到保存期限或不再需要时，应按照规定程序进行

安全销毁，确保销毁过程不可恢复，并记录销毁过程以备审计。

8.部署数据防泄漏（DLP）系统、数据库审计系统等，实时监控数据操作行为，及时发现和处置违规操作等潜在风险。

9.严格控制对数据的访问和操作权限，合理划分权限。

10.定期进行数据安全风险评估和漏洞扫描，及时发现和修复数据安全隐患。

11.建立完善的数据备份与恢复机制，确保在发生数据丢失或损坏时能够快速恢复。

12.各有关单位应设立专门的数据安全管理机构，负责制定、执行和监督数据安全政策。

13.对存储重要数据数据的移动介质应登记造册，加强使用管理，避免损坏和丢失。

14.建立数据泄露应急响应机制，及时应对数据泄露事件。

15.定期进行数据安全演练，提升应急响应能力。

16.定期对数据安全管理制度、技术措施、人员操作等方面进行全面的内部审计，必要时引入第三方专业机构进行独立评估，确保数据安全管理符合国家法律法规和行业标准要求。

17.结合审计结果、业务发展和技术进步，持续优化和完善数据安全管理体系，针对新的安全威胁和漏洞及时调整防护策略，形成闭环管理，不断提升数据安全保障能力。

（四）人才培养及宣传教育

1.加强对信息系统管理人员、网络和数据安全管理人员、供

应链相关人员的培训和监督，定期开展信息系统安全、网络安全、数据安全知识培训，提高职工的安全意识和技能水平，明确各自岗位职责，培养一批具备专业知识和技能的水利信息系统、网络和数据安全管理人才。

2.定期组织信息系统、网络和数据安全科普专题宣传。通过线上线下宣传结合，提升全体干部职工安全意识，营造良好的信息系统、网络和数据安全环境。

三、其他相关要求

各单位要高度重视此项工作，根据通知要求落实自查责任，制定自查工作方案，逐条逐项认真开展自查，对自查发现的问题认真评估，逐一落实整改措施。各单位的自查总结报告(报告模板参见附件)于3月29日前以书面形式(加盖公章)反馈厅科外处，电子扫描版发送至sxs1tkwc@163.com。

联 系 人：冯 毅

联系电话：0351-4666280

附件：自查总结报告模板

山西省水利厅办公室

2024年3月12日

附件

自查总结报告模板

一、自查工作概述

二、自查结果及问题分析

1.信息系统安全管理自查

此处根据实际情况，对不符合要求的部分进行具体描述和分析，如存在弱口令现象、未及时更新杀毒软件等。

2.网络安全管理自查

此处根据实际情况，对不符合要求的部分进行具体描述和分析，如未建立健全网络安全应急预案、网络使用和访问行为不规范等。

3.数据安全管理自查

此处根据实际情况，对不符合要求的部分进行具体描述和分析，如对敏感数据保护不足、数据采集流程不规范等。

三、整改情况及下一步工作计划

针对自查中发现的问题，将采取哪些改进措施。

山西省水利厅办公室　　2024年3月12日印发