河北传媒学院文件

院信〔2021〕2号

河北传媒学院
网络与信息安全管理规定

第一章 总 则

第一条 为保护学校网络与信息系统的安全，有效防范各类安全事故或人为有意的破坏事件，确保网络设施和信息系统的安全稳定运行，防范重大网络与信息安全事件的发生，根据《中华人民共和国网络安全法》等法律法规的相关精神，特制定本规定。

第二条 本规定主要内容包括：组织管理、物理环境与设备安全、网络安全、主机安全、应用安全、数据安全、运行安全、应急管理等九个方面。

第二章 组织管理

第三条 学校成立“网络安全和信息化领导小组”，负责全校

网络和信息安全工作的领导、决策和重大工作部署，信息管理中心负责全校网络安全和信息化的具体工作。

第四条 建立完善的网络与信息安全管理制度，并对安全管理制度的合理性和适用性进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。

第三章 物理环境与设备安全

第五条 设备与物理环境安全的目标是保护信息化设施，包括计算机设备、网络与安全设备、业务系统及其他相关设施的物理环境免遭自然灾害和其他形式的破坏，保证信息系统的实体安全。

1. 信息化设施的选址及建设应遵照国家计算机场地安全标准和有关主管部门的场地环境设施标准，配备防火、防雷、防水、防静电、防鼠等机房安全设施，维持系统不间断的运行能力，确保信息系统运行的安全可靠。

2. 主机房设备与物理环境安全由信息管理中心进行管理。信息管理中心应负责机房内所有信息化设施的物理安全，包括制定物理环境安全、设备安全、设备交付、人员及设备进出、区域访问控制、巡检值守等方面相应的规范和管理细则，配备相关管理人员，落实防护措施。

3. 对机房及弱电间的设备及物理环境安全，管理人员应落实:

(1) 必须遵守《机房管理规定》中的管理人员守则。

(2) 机房及弱电间应安装电子门禁或上锁并处于常闭状态。

(3)机房及弱电间内应设置视频监控、防盗系统。

(4)进入机房、弱电间人员应经过申请和审批流程，并限制和监控其活动范围。

(5)设施上应设置明显且不易去除的标识。

(6)建立设备清单并定期核查，严格确定信息设备的合法使用人，建立详细的设备使用运行日志及故障维修记录，实施定期的设备维护、保养操作。

(7)设备相关的输入、输出、控制部件、空闲端口等应加锁保护或安全封闭，防止被非法切断、占用、搭线。

(8)机房应安排专人值守，机房及弱电间应定期巡检，发现问题及时上报并做好应急处理。

4.对办公区域和公共区域的信息化设施，应防止被偷盗和破坏，定期巡检并记录，对重要信息化设施应专人值守，发现设施存在故障或丢失应及时上报并做好应急处理。

5.对重要安全设备产品的选择，必须符合国家有关技术规范或经过专业测评机构检测不低于本行业计算机安全管理技术规范中的最低安全要求，并核实是否具备安全部门的设备准用证或国家有关部门的安全产品许可证书。

6.应对突发事故建立应急计划，配备应急电源，实施系统主机及重要设备的备份、冗余技术保护措施；对数据应做到异地备份或做到异地存放。

第四章 网络安全

第六条 网络安全的目标是有效防范网络体系的安全风险，为网络信息系统提供安全、可靠、稳定的网络管理和技术平台。

第七条 互联网出口应实施防火墙、入侵检测、网络防病毒等安全技术措施，防范资源被非法访问、篡改和破坏。

第八条 通信网络架构设计应采用冗余技术，提高安全可靠性。

第九条 网络应按功能及业务特点划分 VLAN，制定合理的 ACL 访问控制策略，在一定程度上防止 ARP 攻击和病毒及恶意代码的大肆传播。

第十条 网络设备应根据系统的不同等级进行相应的安全配置设置。

第十一条 网络管理员应确保各信息系统的数据安全，保障连接的服务的有效性，避免非法访问。

第五章 主机安全

第十二条 主机是由服务器、存储等硬件设备、与设备内运行的操作系统、数据库系统及其他系统软件共同构成。主机安全要求通过操作系统、数据库管理系统以及其他安全软件（包括防病毒、防入侵、木马检测等软件）实现的安全功能来满足。

第十三条 主机操作系统和数据库操作系统应按照系统的安全等级进行安全加固，进行服务最小化配置。

第十四条 操作系统和数据库系统需建立认证访问控制，规范用户对文件、数据库表等的访问。认证采用的密码必须遵循复

杂密码的要求。服务器、信息设备等重要信息资产密码需定期更新，密码的变更需登记并安全保存，未经同意不得随意将密码信息泄露给第三方人员。

第十五条 定期对主机的安全进行评估，检测主机的安全配置和存在的安全漏洞，及时进行修补，增强主机系统的健壮性。

第十六条 提高主机恶意代码防护能力，安装恶意代码防护软件，并对主机的防病毒进行统一管理，病毒库进行统一更新。

第十七条 操作系统和数据库系统应及时安装补丁，补丁安装前需做模拟测试，以保障补丁安装不会影响当前系统的稳定运行。

第六章 应用安全

第十八条 应用软件安全的目标是防止由于软件质量缺陷或安全漏洞使信息系统被非法控制，或使之性能下降、拒绝服务、停机。

1. 无论是通用的应用软件，还是量身定做的应用软件，都存在安全风险。对前者可通过加强与软件提供商的沟通，及时发现、堵塞安全漏洞。对后者可考虑优选富有行业软件开发和市场推广经验的软件公司，加强软件开发质量控制，加强容错设计，安排较长时间的试运行等策略，以规避风险，提高安全防范水平。

2. 安全建设必须与应用系统建设同步进行，质量管理和安全监控必须实施于应用系统从计划到运行全周期的各阶段。

3. 应用系统的总体需求计划阶段，应全面评估系统的安全风

险，分析系统的潜在威胁及保护等级策略，确立系统的访问控制、身份认证、信息加密、审计跟踪、稽核检查等安全需求。

4. 在应用系统的总体架构设计的过程中，应实施安全需求设计，根据安全需求设计实施安全技术，防止技术开发人员故意保留“后门”，保证系统最终产品的安全性质量。并确立安全服务机制、项目开发人员安全技术要求和操作规程。

5. 在应用系统建设的各阶段，必须保证应用软件的完整性，即确保软件的变更是经过授权及合法性的验证；必须形成各阶段相应的系统功能设计及技术实施的规范性文档，以及重要的系统安全策略，安全规划、应急计划、风险分析、安全服务机制等安全性文档，并随着系统实现的进程应保持文档变更的同步及准确。

6. 应用系统投产运行之前，必须充分进行局部功能、整体功能、压力测试，以及与安全需求目标一致的系统安全性能、操作流程、应急方案等重要安全性测试，只有正式经过管理、操作、技术控制等安全鉴定获准的应用项目，可以投入生产运行。

7. 对应用系统重要安全事件进行审计，提供覆盖到每个用户的安全审计功能，审计记录的内容至少包括事件的日期、时间、发起者信息、类型、描述和结果。

第七章 数据安全

第十九条 数据安全的目标是防止数据被偶然的或故意的非法泄露、变更、破坏，或是被非法识别和控制，以确保数据完整、保密、可用。数据安全包括数据的存储安全和传输安全两个方面。

1. 采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输和存储保密性。

2. 配备数据库安全审计系统，对数据库安全事件进行审计。

3. 应定期进行数据备份，经常检测备份以保证其可用性，重要的系统和数据必须做到异地备份。

4. 主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性，条件允许情况下建立异地容灾。

5. 数据清除及销毁应进行严格的审批，并由专人进行处理，保证数据不可恢复。

第八章 运行安全

第二十条 运行安全的目标是保证网络信息系统日常运行的安全稳定，对运行环境、技术支持、操作使用、病毒防范、备份措施、文档建立等方面实施安全性管理。

1. 进行完善的资产登记，包括信息资产、软件资产和物理资产。

2. 系统维护应由信息管理中心授权的机构和人员进行，现场的实施应由信息管理中心工作人员陪同和监督。

3. 信息系统维护和操作应有相应的文档，以确保支持的连续性和一致性，防止对安全的忽视、减少操作的失误。

4. 系统的开发、测试和运行系统应进行有效分离，不允许在运行系统上直接进行开发、测试和修改工作。

5. 系统应定期进行安全日志的审计，至少每个月要进行一次

安全日志的分析和审计工作。

6. 对各种信息媒介应实施物理环境保护及其他各种控制措施，确保重要媒介不失密、不被破坏、不被篡改和不失效，维护其完整性和可用性，并授权专人负责介质的登记、存放、检验等维护工作。

7. 根据业务数据保存的要求及时进行数据备份，备份介质应保存在单独的安全场所。

8. 当数据信息、硬件设备、软件程序结束运行使用时，视需求分别进行存档、废弃和销毁处理。存档的信息应充分考虑将来查找和检索的需要；电子信息的存档要考虑到数据生成技术的未来可用性；为满足加密信息的查询需要，应对加密密钥采取有效的存放保管措施。重要信息的销毁应在相关人员的监督下完成。

第九章 应急管理

第二十一条 应急管理的目标是防止业务活动中断，保证重要业务流程不受重大故障和灾难的影响。

1. 应实施应急管理程序，将预防和恢复控制措施相结合，将灾难和安全故障造成的影响降低到可以接受的水平。

2. 应分析灾难、安全故障和服务损失的后果。制定和实施应急计划，确保能够在要求的时间内恢复业务的流程。

第二十二条 应该在整个系统内部制定和维护应急的管理流程。包括以下主要内容：

1. 考虑突发事件的可能性和影响，包括确定重要业务流程及

其优先级别。

2. 了解中断信息系统服务可能对业务造成的影响，并确定信息处理设施的业务目标。

3. 适当考虑风险处理措施，可以将其作为应急程序的一部分。

4. 定期对应急管理的计划和流程进行检查和更新。

5. 确保在组织的程序和结构中纳入应急管理。应急管理流程的协调责任应该在信息系统管理部门进行适当分配。

第二十三条 应该根据风险评估结果制定相应的战略计划，确定应急总体方案。

第二十四条 应该制定计划维护业务运作，或在重要业务流程中断或发生故障后在规定时间内恢复业务运作。

第二十五条 应急计划应该考虑以下内容：计划执行条件、应急程序、恢复程序、说明计划检查方式和维护安排、宣传培训活动、个人责任。

第二十六条 应该对计划进行定期检查，保证其可实施性和有效性。

第二十七条 应急计划的检查计划应该说明各部分计划的检查方式和时间。

第二十八条 应该通过定期审议和更新对应急计划进行维护，确保其始终有效。应该在组织的变更管理计划中采用适当程序，确保应急问题得到适当处理。

第十章 附 则

第二十九条 为了保证本文件的时效性、可行性，必须根据相关审核规定进行评审和修订，修订后重新发布。

第三十条 本规定自发布之日起试行。

二〇二一年十二月十二日

河北传媒学院院长办公室 2021年12月12日印发