

网络信息安全基本方针

第一章 总则

第一条 信息安全基本方针为学校的网络信息安全指明了目标和方向，并确保网络信息安全管理体系被充分理解和贯彻实施。为明确其基本方针，特制定本文件。

第二条 本文件适用于学校网络信息安全管理体系涉及的所有人员和全部重要信息资产及管理过程。

第二章 方针

第三条 坚持“业务为主、安全为重，预防为先、综合防范，统筹兼顾、科学管理”的总体方针，实现网络信息系统安全的可控、能控、在控。

第四条 依照信息安全的总体防护策略，落实信息系统安全等级保护等各项安全制度。通过对网络信息系统的全面梳理、全面诊断和全面加固，掌握现状、找准问题、制订措施、有效改进。

第三章 目标

第五条 使已识别的信息资产满足信息安全的各项要求，包括法律法规、用户与相关方和组织业务要求。具体目标包括：

- (一) 信息泄漏事件为零；
- (二) 引起学校主要业务中断时间累计不能超过 2 h/年；
- (三) 引起学校主要业务中断事件发生次数小于 1 次/年；
- (四) 严重影响网络与信息系统可用性的事件小于 1 次/年；

(五)信息安全事件发生时，以损失最小化、恢复时间最短化、避免再次发生为工作目标；

(六)保护信息免受各种威胁的损害，确保信息系统持续、稳定、可靠运行；

(七)对整个网络信息安全管理体制体系及信息安全工作本身做出持续性改进。

第四章 信息安全管理体制

第六条 物理安全管理体制：机房要选择合适的物理位置，对进出人员执行必要的访问控制。机房内部必须划分区域管理，并部署基础防护系统和设备等。

第七条 网络安全管理体制：要求网络中主要设备必须进行双机热备，且除接入交换机链接工作终端的线路外，其他线路必须进行双线冗余；在保证整体网络带宽充足的基础上，需划分地址段进行网络管理，并突出优先级；网络边界处必须部署防火墙、IPS 等安全设备；网络设备必须开启相应的日志审计功能等。

第八条 主机安全管理体制：要求系统登陆必须进行身份标识和鉴别，系统管理用户身份标识应确保其唯一性，避免共享账户的存在；口令应有复杂度要求并定期更换，且必须及时删除多余的、过期的账户；系统必须启用登录失败处理功能；对服务器进行远程管理时，必须采取必要的防窃听措施；必须开启日志审计功能，并安装统一管理的防恶意代码产品等。

第九条 应用安全管理体制：要求登录应用系统必须进行两种或两种以上的复合身份验证，并保证应用系统用户的唯一

性；应用系统必须开启身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数，且必须开启日志审计功能；应用系统存储用户信息的设备在销毁、修理或转其他用途时，必须清除内部存储的信息是否牵涉泄密等。

第十条 数据安全管理体系：要求业务应用数据和设备配置文档都必须进行备份，并保证数据及传输过程的完整性。必须使用专业备份设备和工具，进行加密数据的传输和存储。进行异地备份时，必需利用通信网络将关键数据定时批量传送至备用场地。

第五章 重要原则、标准和符合性要求

第十一条 学校在建立和管理信息安全管理体系时，必须符合相关法律法规和合同的要求。

第六章 附则

第十二条 本文件由网络安全与信息化领导小组办公室负责解释与修订。

第十七条 本文件自发布之日起执行。

山东中医药高等专科学校

二〇二四年五月十四日