

信息化系统日常维护操作规程（试行）

第一章 总则

第一条 为加强学院网络安全管理，保障学院电子班牌、网上办事大厅、广播系统、监控系统、电子显示屏等网络相关系统的安全、稳定运行，依据国家《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国保守国家秘密法》《网络数据安全条例》，结合学院实际情况，特制定本操作规程。本规程适用于学院网络安全日常维护管理的全过程，包括系统运行监控、数据备份与恢复、安全漏洞管理、应急响应等方面。

第二章 设备巡检与维护

第二条 日常巡检安排：各信息化设备管理部门需对接技术支持方对电子班牌、网上办事大厅服务器、广播系统设备、监控系统主机、电子显示屏及相关网络设备定期进行巡检。巡检内容包括设备外观完整性检查：查看是否有物理损坏、线路连接是否松动；设备运行状态检查：观察指示灯是否正常显示、设备是否有异常发热或噪声；网络连接状况检查：通过 Ping 命令等工具测试各设备与网络的连通性。

第三条 定期深度维护：每季度进行一次深度维护，包括设备内部清洁，使用专业工具清理服务器、交换机等设备内部灰尘，防止因积尘导致散热不良或电路短路；硬件性能检测，运用专业检测软件对设备硬件进行全面检测：检测硬

盘健康状况、内存性能等，并记录检测数据以便对比分析设备性能变化趋势；系统日志分析：查看各系统日志，排查是否存在潜在故障隐患或异常访问记录，对发现的问题及时进行处理或上报。

第四条 设备故障处理流程：按照故障优先级进行处理，影响教学、管理等核心业务的紧急故障优先处理，一般性故障在不影响正常工作的前提下有序安排修复。对于紧急故障，设备管理员立即赶赴现场，迅速判断故障原因，如网络中断故障，排查网线连接、交换机端口、路由器配置等环节，采取临时修复措施恢复网络连接，后续再深入排查根本原因并彻底解决。对于一般性故障，如系统报错、部分功能异常等，在故障日志、知识库中查找类似案例，借鉴已有解决方案，若无法解决，及时联系软件供应商技术支持团队协助处理。

第三章 系统软件更新与升级

第五条 系统升级流程：在进行系统升级前，应制定详细的升级方案，明确升级目标、步骤、风险评估及回退措施。升级方案需经学院网络综合治理、网络安全和信息化领导小组办公室审核批准后实施。升级过程中，应安排技术人员密切监控升级进度和系统状态，如发现异常应立即暂停升级并按照回退措施恢复系统至升级前状态。升级完成后，应对系统进行全面测试，包括功能测试、性能测试、安全测试等，确保系统升级后稳定运行，并及时发布升级成功通知。

第四章 数据备份与恢复管理

第六条 数据备份策略：针对电子班牌、网上办事大厅、广播系统、监控系统、电子显示屏系统中的重要数据，制定差异化的数据备份策略。网上办事大厅用户数据等核心数据实行每日全量备份，备份数据存储在本地专用存储设备；电子班牌课程安排数据等每日进行增量备份，备份数据保留 7 天；监控系统视频数据根据存储容量和法规要求，采用循环覆盖式备份，重要视频片段及时进行单独备份并标记。

第七条 备份数据验证与恢复演练：每季度对备份数据进行完整性和可用性验证，随机抽取部分备份数据进行恢复测试，确保在数据丢失或损坏时能够快速、准确地恢复。

第五章 网络安全防护与监控

第八条 防火墙与入侵检测系统维护：每日检查防火墙规则设置是否合理有效，监控入侵检测系统的报警信息，及时处理可疑的网络入侵行为。每周对防火墙和入侵检测系统进行一次规则库更新，确保能够有效抵御最新的网络攻击手段。每月对防火墙和入侵检测系统的性能进行评估，根据学院网络流量变化和安全需求，适时调整设备配置参数。

第九条 网络流量监测与分析：利用专业网络流量监测工具，实时监测学院网络流量，分析流量分布、来源及去向。对异常流量，如流量突然大幅增加、来自特定 IP 地址的大量连接请求等，及时进行阻断并深入调查原因。每日生成网

络流量监测报告，记录流量概况、异常事件及处理情况，为网络优化和安全决策提供数据支持。

第十条 安全漏洞扫描与修复：每两周进行一次全面的网络安全漏洞扫描，涵盖网络设备、服务器、应用程序等各个层面。对扫描发现的安全漏洞进行分类分级评估，制定详细的修复计划，明确修复责任人与时间节点。对于高危漏洞，应立即采取临时防护措施，并在 24 小时内完成修复；中低危漏洞在一周内修复完成。修复后再次进行扫描验证，确保漏洞已成功修复。

第六章 人员培训与技术支持

第十一条 维护人员技能培训计划：定期组织网络安全维护人员参加专业技能培训，包括网络设备维护技术、系统软件管理、数据安全防护、网络安全最新技术动态等方面的培训课程和研讨会。每月安排一次内部技术交流分享会，鼓励维护人员分享工作中的经验与问题解决方案，促进团队整体技术水平提升。

第十二条 外部技术支持合作：与专业的网络安全技术服务厂商建立长期合作关系，获取外部技术支持。在遇到重大网络安全问题或复杂技术难题时，及时邀请外部专家进行技术指导和协助解决。积极参与相关行业技术交流活动，拓展技术支持渠道，提升学院网络安全维护工作的技术保障能力。

第七章 附则

第十三条 本管理制度自发布之日起正式实施。由网络综合治理、网络安全和信息化领导小组办公室负责解释与修订工作。在实际执行过程中，将依据国家法律法规调整、学院网络架构变化及网络安全技术发展等情况，及时对本制度进行完善优化，确保其始终契合学院网络安全维护管理的实际需求，为学院教育教学工作的顺利开展提供坚实可靠的网络安全保障。