

广西工业技师学院安全审核和检查制度

第一章 总 则

- 第一条** 为督促广西工业技师学院（以下简称“枢纽台”）落实各项信息安全管理规定和操作规程，规范各项信息安全工作，特制定本制度细则。安全检查内容可分为管理和技术两个方面，管理方面的检查侧重检查安全流程、管理要求的执行情况；技术方面的检查侧重检查枢纽台内网、SDH 网和远程监控系统符合广播电视台安全播出要求、安全配置要求以及其他技术规范的情况。
- 第二条** 检查以单位制度、部门发文和组内规定的有效执行制度、细则和流程为标准。
- 第三条** 检查内容包括但不限于：现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理体系的完备性、安全管理制度的有效性和适用性、安全管理制度的执行情况。
- 第四条** 检查对象包含但不限于：系统运行日志、变更文档、系统配置信息文档、升级文档、机房出入登记记录、机房设备上下架记录、设备维护记录、密码定期更改记录、数据备份记录、数据可恢复验证记录、故障处理报告、应急演练报告、系统风险定期排查报告等。

第二章 组织与职责

- 第五条** 发起网络与信息安全检查工作的主体包括：外部相关管理单位和枢纽台信息网络中心以及枢纽台网络与信息安全领导小组办公室。
- 第六条** 各安全职能组在网络与信息安全领导小组的领导下，组织开展枢纽台管理和技术层面安全检查工作：
- (一) 制定全面的检查标准，已指导每次的检查工作；
 - (二) 落实上级检查工作总体安排；
 - (三) 组织制定安全检查细则；

- (四) 作为枢纽台范围安全检查工作的责任主体，组织制定并实施枢纽台的检查计划。每年1月底前完成当年检查计划制定工作；
- (五) 对其他安全检查责任主体的检查工作，如制定内部检查工作计划、实施检查等，进行指导、审批、检查、备案；
- (六) 汇总、审阅检查报告，审核改进方案，督促解决检查中发现的突出问题。出现涉及枢纽台层面的重大问题或者需要对技术或者管理流程做出重大调整时，应向学院领导汇报；
- (七) 信息网络中心负责对枢纽台安全检查工作进行检查。

第七条 被检查对象应参与制定检查计划、明确检查重点，配合检查工作。

第八条 在检查过程中，检查人员应按照信息安全管理相关保密规定对接触到的敏感信息进行严格保密，尤其在安全漏洞修补之前，严禁泄露给第三方。

第三章 技术层面日常安全检查

第九条 通过监控类安全设备对远程监控系统进行安全性实时监控，通过审计类安全设备进行安全的综合性分析，多方结合以便及时发现存在的安全漏洞或恶意的攻击，从而实现动态和实时的安全控制。

第十条 机房及重要的安全设备须每天进行日常巡检，检查指示灯、服务状态等。

第十一条 所有安全设备须每月详细检查一次，记录并分析相关日志，对可疑行为及时进行处理。

第十二条 对网络层面防病毒系统的病毒库设置自动升级，对主机层面的防病毒系统每周进行病毒库升级，并查看防病毒系统事件日志，包括各客户端病毒查杀日志、升级日志等。发现病毒的情况和统一升级的情况，应记录于病毒系统安全检查表格中。

第十三条 在系统日常管理中，要定期（不少于两周一次）对系统日志文件等进行检查，并对用户登录情况进行检查，以尽早发现潜在的非法侵入。

第十四条 计算机信息系统中要有详细系统日志，记录每个用户的每次活动（访问时间、地址、数据、程序、设备等）以及系统出错和配置修改等

信息。

第十五条 信息网络中心安全管理员要定期审查系统日志并做好审查记录，审查周期不得长于一个月，同时保证系统核心日志的定期备份。

第十六条 所有的检查及审计须提供相应的记录或报告。

第四章 管理层面安全检查

第十七条 应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。

第十八条 信息网络中心安全管理员应定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

第十九条 信息网络中心安全管理员应定期或不定期检查重要安全活动是否按照相关规章制度、操作规程和标准执行。

第五章 附 则

第二十条 本办法由枢纽台信息网络中心负责解释并督促执行。

第二十一条 本办法自印发之日起执行。