长沙职业技术学院
校园网与信息系统安全管理办法

第一章 总则

第一条为了保障学校校园网与信息系统安全稳定，促进学校教育信息化健康发展，根据国家相关法律法规，结合我校实际情况，制定本办法。

第二条校园网与信息系统安全是指校园网基础设施、信息系统及数据内容等受到保护，保证网络、信息及内容的安全性、完整性、可用性、可控性。

第三条校园网与信息系统安全管理的总体方针是以《教育部关于加强教育行业网络与信息安全工作的指导意见》（教技〔2014〕4号）、《网络安全法》、《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）为指导，预防为主、综合防范。

第四条校园网与信息系统安全管理的基本原则是“谁主管谁负责、谁运维谁负责、谁使用谁负责”，分级管理、逐级负责，自主防护、明确责任，突出重点、保障安全。

第五条校园网与信息系统安全管理的目标是建立健全网络与信息安全保障体系，提高安全防护能力，确保学校网络与信息安全工作规范、有序开展，保障学校教育信息化可持续发展。

第二章 组织架构

第六条网络安全与信息化领导小组负责制定学校网络与信息安全相关政策，研究处理重大网络与信息安全事件，定期召开网络与信息安全工作会议，统筹指导学校网络与信息安全建设。

第七条网络安全与信息化领导小组下设办公室，挂靠信息管理中心，负责学校网络与信息安全的日常工作。

第八条学校各部门负责本部门信息系统（网站）的建设、管理及安全运维等工作。各部门负责人是本部门网络与信息安全工作的第一责任人。各部门须设置信息管理员，负责本部门网络与信息安全等具体工作，具体职责见《部门（院部）信息管理员工作职责》（附件 1）。各部门年度网络与信息安全考核工作由信息管理中心统筹。

第三章 安全建设

第九条各部门在编制本部门年度经费预算时，须包含网络与信息安全的专项经费，用于本部门信息系统（网站）的安全建设与运维。

第十条各部门须明确信息系统（网站）是否需要对校外开放，对校外开放的信息系统（网站），须满足国家标准《信息安全技术网络安全等级保护基本要求》规定的二级（或以上）安全等级要求，明确其网络及信息安全需求，提供安全访问策略，由信息管理中心进行防火墙设置。

第十一条各部门信息系统（网站）在上线前，须填写《信息系统（网站）登记表》（附件 2），须签署《网络安全承诺书》（附件 3）和《信息系统（网站）安全协议书》（附件 4），由本部门负责人签字确认后，提交信息管理中心备案。非我校 IP

地址和域名的“双非” 信息系统（网站）在上线前，除履行上述程序外，还须分管校领导同意，并请校外挂靠平台会签承诺书，提供网站及信息系统安全检测报告。

第十二条各部门信息系统（网站）上线运行前，信息管理中心采用专业技术手段对其进行安全检测。检测未通过的，须进行安全整改，直至通过检测，方可上线运行。

第四章 运行管理

第十三条各部门须定期对本部门的信息系统（网站）开展安全巡检，并做好巡检记录，填写《信息系统（网站）巡检记录表》（附件 5）。对校外开放的信息系统（网站），要求每周巡检一次；对校内开放的信息系统（网站），要求每月巡检一次。

第十四条各部门须定期对信息系统（网站）进行漏洞修补，包括主机系统漏洞、WEB 应用漏洞、中间件漏洞、数据库漏洞等。

第十五条学校将定期对全校的网络与信息系统开展安全检查，检查不合格的信息系统（网站），视其安全漏洞级别暂停其外网访问，同时通知责任部门限期整改，并将《信息系统（网站）巡检整改报告》（附件 6）提交信息管理中心。经信息管理中心安全复查合格后，方可恢复其正常访问。

第十六条特殊时期，各部门须加强网络与信息系统的安全监管工作，安排专人值守，加强安全巡检，做好安全整改。

第五章 网络与信息安全事件应急响应

第十七条网络与信息安全事件分为紧急事件和非紧急事件。

第十八条紧急事件

（一）可由校外访问的页面发生篡改或被替换成非法信息的事件，尤其是发生在主页、新闻网站、招生信息网等访问量高的系统或网站的事件。

（二）影响学校系统正常运转的攻击事件，如与服务门户、教务系统、一卡通系统、财务系统、OA 系统等相关的攻击事件。

（三）可能造成师生隐私信息被窃取、丢失、损坏的事件。

（四）其它可能对社会公共安全或学校造成危害或不良影响的事件。

第十九条非紧急事件

（一）对校内开放系统或网站的页面发生无害篡改或有隐藏漏洞的事件。

（二）影响不大的攻击事件或可能造成中低隐患漏洞的事件。

（三）其他不构成公共危害或社会不良影响的安全事件。

第二十条 网络与信息安全事件应急响应流程如下：

（一）信息管理中心接到上级安全事件通报或发现安全事件，立即切断引起安全事件设备的网络连接；保持设备原有运行状态，以备获取安全事件的相关证据。

（二）通知责任部门网络与信息安全事件情况。

（三）若事件为紧急事件：信息管理中心第一时间向分管信息化工作校领导汇报，若涉及到意识形态领域的非法信息，还需要向党委宣传部通报。

（四）信息管理中心指导分析事件原因，并提供整改建议。

（五）责任部门对发生安全事件的信息系统（网站）进行安全修复，并向信息管理中心提交整改报告。

（六）信息管理中心对修复后的信息系统（网站）进行安全复查，复查通过后恢复其访问权限。

第二十一条信息管理中心负责编制学校的网络与信息安全应急预案；组织开展网络与信息安全应急预案的宣传、教育和培训。

第六章 附则

第二十二条涉密网络与信息系统的运行安全保护工作不适用本管理办法。

第二十三条本管理办法自学校批准之日起施行。

附件 1

部门（院部）信息管理员工作职责

为规范学校各部门信息系统管理，夯实校园网网络安全基础，切实提升广大师生员工网络安全意识和安全防护技能，真正做到“网络安全为人民，网络安全靠人民”，依据学校有关规定，特制定本工作职责：

第一条 部门兼职信息管理员为学校各部门网络与信息系统安全直接责任人，由各部门岗位设置时统筹安排。

第二条 负责本部门网络与信息系统安全管理、运行维护等日常工作，定期接受信息管理中心培训和指导。

第三条 负责参与制定本部门年度信息化项目建设计划、撰写总结，并及时向信息管理中心报送。

第四条 负责本部门网络与信息系统安全知识的宣传和教育工作，并及时向信息管理中心提交有关工作开展的图文资料。

第五条 负责本部门网络与信息系统安全保密工作，切实加强信息系统（网站）后台管理，严禁私自转借登录口令。

第六条 负责本部门校园网接入用户行为管理，坚守网络意识形态主阵地，预防并制止本部门师生员工利用校园网从事不良活动的行为，发现问题及时上报。

第七条 负责本部门信息技术推广应用工作，及时处理本部门日常工作中遇到的各类信息故障。

第八条 负责收集并整理本部门师生员工信息化诉求，在能力范围内能解决的，应及时解决；不能解决的，应报送信息管理中心。

第九条 负责管理学校安装、布放在本部门的信息化基础设施的物理安全，未经许可，一律不得对外提供。

第十条 信息管理中心负责对部门兼职信息管理员工作进行考核，并计入各部门年度绩效考核中。