西昌学院网络安全工作责任制实施细则

（试行）

第一条 为贯彻落实中共中央办公厅《党委（党组）网络安全工作责任制实施办法》，进一步加强学校网络安全工作，保障学校网络安全和信息化建设可持续发展，根据《中华人民共和国网络安全法》《西昌学院成立网络安全和信息化领导小组的通知》《西昌学院网络与信息安全管理办法（试行）》《西昌学院网络安全事件应急预案（暂行）》等有关法律和规定，制定本细则。

第二条 学校党委对全校网络安全工作负主体责任，党委书记和校长是学校网络安全工作第一责任人，分管网络安全和信息化工作的校领导是学校网络安全工作直接责任人。学校网络安全和信息化工作领导小组统筹全校网络安全工作。

各单位的联系校领导负领导责任，领导班子对本单位网络安全工作负主体责任，其中领导班子主要负责人是第一责任人，分管网络安全工作的领导班子成员是直接责任人。

第三条 学校网络安全和信息化工作领导小组是学校网络安全工作的领导机构，在网络安全方面主要承担以下职责：

（一）贯彻落实中央及省委、省政府关于网络安全和信息化工作的政策法规和决策部署，统筹协调全校网络安全和信息化重大问题。

（二）每年至少召开一次网络安全专题会议，研究重大事项。

（三）统一组织领导学校重大网络安全事件的应急处置工作，统筹协调和应急处置。

（四）完善网络安全工作责任制，健全网络安全保障体系，督促各单位按照《西昌学院网络安全工作责任制评价指标》（见附件 1）的考核工作。

第四条 学校网络安全和信息化领导小组办公室（以下简称网信办）是学校网络安全工作的综合协调和监管机构，办公室设在网络信息中心，办公室主任由网络信息中心、宣传部负责人兼任。网信办主要承担以下职责：

（一）依照国家网络安全相关法律法规和学校党委的决策部署，制定网络安全制度体系，制定年度网络安全工作计划，监督落实网络安全“同步规划、同步建设、同步实施”要求。

（二）负责网络安全和信息化领导小组的日常事务工作，协调、督促和落实各单位（部门）网络安全工作，对各单位落实网络安全工作责任制情况进行检查。建立完善学校信息系统的台账，督导各信息系统的网络安全等级保护工作。

（三）加强和规范学校网络安全信息汇集、分析和研判工作，落实学校网络安全应急预案，完善信息通报机制，每年至少组织一次预案演练。监督学校有关单位落实重要时期的各项保障工作，统筹协调开展网络安全检查，开展网络安全信息通报。

（四）负责与上级、地方网络安全管理单位的联络，配合开展网络安全检查，负责落实网络安全主管部门通报的重大网络安全风险的整改工作。

（五）网络安全事件发生后，网信办成立调查工作组，并在各级网信、网监等有关单位的指导和帮助下及时处理网络安全事件。

第五条 学校网络信息中心是学校网络安全技术保障和监督的具体执行机构，主要承担以下职责：

（一）负责健全和完善学校网络安全管理制度体系。

（二）负责学校整体网络安全防护工作，及时调整完善网络安全技术防护策略，对重要信息基础设施实行重点保护，督促和检查各单位（部门）的网络安全的建设并提供技术支持。

（三）组织落实网络安全监测、执法检查、风险漏洞排查和整改、网络安全信息共享和通报、网络安全事件应急处置等工作。

（四）组织落实学校网络安全等级保护具体工作，指导各单位（部门）完成信息系统定级、备案以及测评整改工作。

（五）全面掌握学校信息基础设施情况和网络资产台账，对新建业务系统负责上线前的网络安全风险隐患排查。

（六）负责组织开展全校性网络安全宣传教育，加强网络安全专业技术培训，提升网络用户的安全意识和从业人员的网络安全素养。

第六条 学校各单位领导班子主要承担的网络安全责任：

（一）认真贯彻落实党中央和习近平总书记关于网络安全工作的重要指示精神和决策部署，贯彻落实网络安全法律法规和政策文件，了解网络安全的主要目标、基本要求、工作任务和保护措施。

（二）确定本单位（部门）网络安全与信息化负责人及联络人，并将网络安全工作作为本单位安全稳定工作的重要组成部分。每年至少召开一次专题会议，研究重要事项，安排部署工作，保障网络安全各项工作落实到位。每半年向学校网信办提交本单位（部门）落实网络安全工作责任制情况自查报告。

（三）将网络安全教育作为国家安全教育的重要内容进行部署，积极开展常态化网络安全宣传教育，提高广大干部和师生员工的网络安全和数字化素养。

（四）切实增强做好网络安全工作的责任感使命感，把网络安全工作纳入重要议事日程，纳入本单位年度工作目标，将网络安全责任落实到具体岗位和具体人员。

（五）建立本单位（部门）网站和信息系统台账，明确负责人及管理员，落实网络安全管理规定，做好信息系统的账户管理，规范对个人信息和重要数据的采集和使用。

（六）有业务系统的主管单位，负责业务系统的安全管理和运维，做好上线前的网络安全自查、风险隐患排查的整改，完成网站和信息系统的备案，做好网络安全等级保护定级、测评和整

改工作，参加网络安全的应急演练，完成对网站、业务系统网络安全问题的整改处置和情况反馈。

第七条 各单位（部门）要认真履行网络安全职责，凡未正确履行职责或因工作疏忽而发生不安全、不稳定事件，有下列情形之一的，应逐级倒查，追究相关责任人责任。

（一）学校门户网站、其他重点网站及信息系统等遭受攻击篡改，导致反动言论或者谣言等违法有害信息大面积扩散，且没有及时报告和组织处置的；

（二）学校门户网站或者重点新闻网站存在挂码、暗链没有及时组织处置，导致不良后果的；

（三）关键信息基础设施遭受网络攻击，没有及时处置导致大面积影响学校师生工作、生活，或者造成重大经济损失，或者造成严重不良社会影响的；

（四）发生学校秘密泄露、大面积个人信息泄露或者大量教学、科研、行政等基础数据泄露的；

（五）封锁、瞒报网络安全事件情况，拒不配合相关管理部门依法开展调查、处置工作，或者对相关管理部门通报的问题和风险隐患不及时整改并造成严重后果的；

（六）阻碍公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动，或者拒不提供支持和保障的；

（七）发生其他严重危害网络安全行为的；

（八）各单位或个人因为业务系统的弱口令等低级错误，因整改不到位给学校带来严重后果受到上级部门通报批评的。

第八条 任何单位（部门）和个人对网络安全事件应及时报告，对已发生的网络安全事件不得隐瞒不报、谎报、拖延报告或阻碍、干涉事件调查。

第九条 网络意识形态工作责任制、涉密网络的网络安全工作责任制按照学校有关规定执行。

第十条 本细则以及涉及网络安全的未尽事宜由学校网信办负责解释。

第十一条 本细则自发布之日起施行。