

内蒙古师范大学党委 贯彻落实网络安全工作责任制实施细则 (试行)

第一章 总 则

第一条 网络安全工作事关学校各项工作安全稳定运行和广大师生切身利益。为扎实推进学校网络安全工作，明确和落实各级党组织领导班子、领导干部网络安全责任，筑牢网络安全防线，提高网络安全保障水平，根据《中国共产党问责条例》、《中共中央办公厅党委（党组）网络安全工作责任制实施办法》、《内蒙古自治区各级党委（党组）网络安全工作责任制实施细则（试行）》等有关规定，学校结合实际，制定本细则。

第二条 依据《中华人民共和国网络安全法》，凡在学校管理范围内建设、运营、维护和使用网络（含网络系统中的硬件、软件及其数据），以及网络安全的监督管理，均适用本细则。

第三条 按照“属地管理，逐级负责”的原则，学校在上级主管部门指导下，负责落实校内网络安全各项任务。

第四条 加强党对学校网络安全工作的领导，发挥党委的政治核心作用，严格落实主体责任，形成党委统一领导、党政齐抓共管、有关部门各负其责的网信工作格局。

第二章 组织机构和主体责任

第五条 学校党委网络安全和信息化委员会负责统筹推进全校网络安全工作。网络安全和信息化委员会下设办公室，办公室主任由分管学校网络安全和信息化工作的校领导担任，办公室常务副主任由党委宣传部和信息中心主要领导担任。

第六条 学校党委对全校网络安全工作负主体责任，学校党委书记是第一责任人，分管网络安全工作的校领导是直接责任人，协助学校党委书记抓好统筹协调指导工作。其他校领导班子成员根据工作分工，抓好分管部门、联系单位的网络安全工作，对职责范围内的网络安全工作负领导责任，定期听取汇报，全面掌握网络安全工作情况。

第七条 按照“谁主管谁负责，谁运维谁负责，谁使用谁负责”的原则，各院级单位党委（党总支）和各部门对本单位网络安全工作负主体责任，各院级单位党委（党总支）书记和各部门主要领导是第一责任人，分管网络安全的领导班子成员是直接责任人，协助第一责任人抓好统筹协调指导工作，其他领导班子成员根据工作分工，对职责范围内的网络安全工作负领导责任。

第三章 网络安全责任制

第八条 学校党委主要承担的网络安全责任

（一）认真贯彻落实党中央关于网络安全工作的决策部署，贯彻落实网络安全法律法规，确立学校网络安全的主要目标、基

本要求、工作任务、保护措施；

（二）建立和落实网络安全责任制，健全网络安全责任制检查考核机制，并将考核结果作为对领导班子和领导干部综合考核评价的重要内容；

（三）研究网络安全重大事项，将网络安全工作纳入重要议事日程，确保人力、财力、物力的支持和保障力度，推动网络安全宣传教育常态化开展；

（四）组织领导学校网络安全保护和重大事件处置工作，研究解决重要问题；

（五）采取有效措施，为公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动等提供支持和保障。

第九条 学校党委网络安全和信息化委员会主要承担的网络安全责任

（一）负责全校网信工作的顶层设计、总体布局、综合协调、整体推进和督促落实。研究制定学校年度网信工作要点报学校党委审定，并及时汇报工作落实情况；

（二）统筹指导学校网络安全工作，建立健全学校网络安全责任制和规章制度，指导学校各单位落实各项重点工作，统筹管理学校网络安全和信息化建设项目；

（三）统筹协调学校网络安全保护和重大事件处置工作，建立跨部门事件协调和处置机制，充分发挥纵向衔接、横向协调的

组织保障作用；

（四）加强和规范网络安全信息汇集、分析和研判工作，充分发挥专家和专业机构的作用，建立网络安全专家咨询机制，分析研判网络安全态势，服务网络安全决策；

（五）向上级有关部门及时报告网络安全重大事项，出台涉及网络安全的重要政策和制度措施等。

第十条 学校党委网络安全和信息化委员会办公室主要承担的责任

（一）负责学校网络安全和信息化委员会日常事务，归口管理、协调网络安全和信息化工作，向学校党委网络安全和信息化委员会提出工作建议，督促、检查网络安全和信息化各项重点任务落实情况；

（二）落实学校网络安全联络机制，负责联系校内网络安全职能部门，落实网络安全和信息化通报机制，构建安全高效的通报渠道；

（三）及时向上级有关部门报告网络安全信息，如网络安全重大事项、网络安全风险隐患排查整改情况等；

（四）落实网络安全责任制实施情况的检查考核工作，细化考核内容、方法、程序；

（五）组织开展常态化网络安全宣传教育，指导开展重要网络安全活动，提高广大师生员工的网络安全素养。

第十一条 信息中心作为学校网信工作的技术支撑部门，主要承担的责任

（一）全面实施网络安全等级保护制度，对全校信息基础设施实行重点保护和安全监管。建立健全网络信息安全保护制度，履行网络安全保护责任。落实信息基础设施管理和运营责任，全面掌握学校信息基础设施以及所属门户网站、网络平台和信息系统的数量、规模、主要功能、安全风险等基本情况；

（二）开展网络安全监测预警和信息通报工作，建立健全学校网络安全风险评估机制，发现安全威胁及时通报相关单位，跟踪核查修复情况，尽快消除安全隐患；

（三）组织学校网络安全检查，积极配合和支持公安机关等有关部门组织开展的网络安全监测、网络安全执法检查、信息共享和通报工作，及时掌握安全状况，系统排查安全隐患，指导监督安全整改，提高安全保障水平；

（四）制定学校网络安全事件应急预案，每年至少组织一次应急预案演练；发生网络安全事件，应当第一时间组织处置并报告学校以及上级有关部门和属地网络安全职能部门；

（五）开展学校网络安全管理员知识技能培训，提升网络安全工作队伍业务能力。

第十二条 各院级单位党委（党总支）书记和部门主要领导承担的网络安全责任

（一）认真贯彻落实上级决策部署，遵守网络安全法律法规和政策文件，明确本单位网络安全的主要目标、基本要求、工作任务和保护措施；

（二）切实增强做好网络安全工作的责任感和使命感，坚持“守土有责、守土负责、守土尽责”，将网络安全工作作为教育安全稳定工作的重要组成部分，纳入重要议事日程，纳入本单位年度工作目标。建立和落实网络安全责任制，将网络安全责任落实到具体岗位和个人；

（三）配合学校网络安全检查、演练，及时向学校党委网络安全和信息化委员会办公室报告网络安全信息和网络安全事件；认真研究本单位所建网络和信息化设施涉及网络安全工作的重大问题，严格请示报告制度，确保网络安全保障措施到位。

第四章 应急处置和责任追究

第十三条 发生网络安全事件时，学校党委宣传部、信息中心会同运营单位立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，按照事件分级、预警分级进行应急响应，消除安全隐患，防止危害扩大；网络安全事件涉及相关单位应建立联动处置机制，加强设施(数据)保护，及时恢复设施运行，并同步开展调查取证、责任追究等工作。网络安全事件发生及其组织处置情况，同时报告上级有关部门和属地网络安全职能部门。

第十四条 责任主体违反或者未能充分履行本细则所列职

责，按照有关规定追究其相关责任。有下列情形之一的，学校将逐级倒查，追究当事人、网络安全负责人直至主要负责人责任。协调监管不力的，还将追究综合协调或监管部门相关人员的责任。

（一）门户网站、新闻网站、宣发平台、信息系统被攻击篡改，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）发生国家秘密泄露或学校重要数据泄露的；

（三）发生大面积个人信息泄露、造成较严重后果的；

（四）重要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；

（五）瞒报、谎报网络安全事件情况，拒不配合有关部门依法开展调查、处置工作，或者对有关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）未履行《网络安全法》等法律法规规定的义务，违法运行，并导致发生重大网络安全事件的；

（八）网络安全工作机制不健全，经费不落实，责任不明确，并造成严重后果的；

(九) 发生其他严重危害网络安全行为的。

第十五条 实施责任追究应当遵循实事求是的原则，分清集体责任和个人责任。追究集体责任时，领导班子主要负责人和分管网络安全工作的领导班子成员承担主要领导责任，参与相关工作决策的领导班子其他成员承担重要领导责任。

第十六条 学校将网络安全工作纳入院级单位党委（党总支）意识形态工作责任制考核和党建述职评议考核、安全稳定和综治工作考核、年度工作目标绩效考核以及教育信息化工作专项督导的重要内容，一并进行检查考核。

第五章 附 则

第十七条 学校网络意识形态工作责任制按照《内蒙古师范大学党委网络意识形态工作责任制实施办法》（内师党发〔2017〕33号）执行。涉密网络按照有关规定执行。

第十八条 学校网络安全技术工作按照《内蒙古师范大学网络信息安全管理办法》（内师党发〔2019〕42号）执行。

第十九条 本细则自印发之日起施行，由学校党委网络安全和信息化委员会办公室负责解释。

抄送：学校领导

内蒙古师范大学党政办公室

2022年9月18日印发
