附件 31

内蒙古农业大学网络与信息安全管理办法

（修订）

第一章 总　则

第一条 为加强学校网络与信息安全管理，规范网络与信息安全工作，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《关键信息基础设施安全保护条例》、《网络安全等级保护条例》及其他有关法律、行政法规的规定，结合学校实际，制定本办法。

第二条 网络与信息安全工作的目标是为了提高学校师生网络与信息安全意识，建立健全网络与信息安全工作的组织体系、管理制度；有效防范、控制和抵御安全风险，确保校园网络、网站及信息系统正常、安全运行；提高网络与信息安全防护水平，增强安全预警、应急处置和灾难恢复能力；形成与学校信息化发展相适应的、完备的网络与信息安全保障体系，促进信息化建设的健康发展。

第三条 本管理办法所称的校园网络及信息系统，是指由学校投资或引入社会资金建设的，支持学校教学、科研、管理和服务工作的软硬件集成系统，包括校园网络设备、网络线缆设施、服务器、网站、管理信息系统、业务系统等。

第四条 本管理办法适用于接入内蒙古农业大学校园网

的所有网络设施、设备、信息系统以及使用校园网的机构、团体和个人的安全管理。

第二章 管理架构

第五条 网络与信息安全工作实行校、院（部、处）两级管理。

（一）学校“网络与信息安全工作领导小组”（以下简称领导小组）统一领导全校的校园网络与信息安全工作。领导小组下设办公室，办公室设在党委宣传部，信息与网络中心负责网络与信息安全的日常工作。

（二）各职能处室、教辅单位、学院等二级单位是本部门网络与信息安全的责任主体，应成立“网络与信息安全工作组”（以下简称工作组），负责本部门及挂靠、归口管理部门的网络与信息安全工作。组长由各职能处室、教辅单位主要负责人、院部党委（总支）书记兼任，并设立网络信息安全员。与学校签订《网络与信息安全管理责任书》。

（三）设立网络与信息安全专家组及技术保障组，为领导小组提供技术咨询和支撑。形成以信息与网络中心技术人员为核心，重点处室网络信息安全员为骨干的全校性网络与信息安全专业队伍。

第三章 管理职责

第六条 网络与信息安全工作总体原则是统一领导、分级管理、主办（主管）负责、责任追究。各部门按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则切实落实

网络与信息安全主体责任。

第七条 领导小组主管学校网络与信息安全工作，领导小组办公室，负责网络与信息安全管理、监督和协调等工作。具体职责如下:

（一）统筹协调全校的网络与信息安全工作，研究制定网络与信息安全政策，讨论解决安全管理中的重大问题；提出网络与信息安全工作要求，制定工作计划，指导宣传教育。

（二）检查、督促各部门建立网络与信息安全管理组织，明确第一责任人和网络信息安全员。

（三）拟定网络与信息安全规章制度，组织审核校内各部门所制定的网络安全管理措施。

（四）监督、检查各部门网络与信息安全管理责任的落实情况，督促整改安全隐患。

（五）组织有关部门实施网络与信息安全的风险评估，审定网络安全保护等级，确定要害计算机信息系统。

（六）制定网络与信息安全的应急处置预案；处理违反网络与信息安全管理的事件，配合公安机关查处危害信息系统安全的违法犯罪案件；通报网络与信息安全的信息；协调安全管理工作中的有关问题。

（七）履行法律、法规、规章制度规定的其他职责。

第八条 党委宣传部负责学校网站信息的发布与监管，负责网络舆情信息的监控和管理，联合学生工作处、团委等部门开展网上舆情疏导和正面宣传工作。

第九条 保卫处负责对校园内发生的网络与信息违法行为和犯罪案件进行调查、取证，根据相关证据及事态影响或破坏程度，对违规者按照有关规定进行处理。

第十条 信息与网络中心负责，负责网络与信息安全管理的日常工作，包括网络与信息安全技术防护体系的设计、建设、运行和维护，网络与信息安全事件监控及协助处理，提供网络与信息安全技术保障和服务支持等。

第十一条 保卫处和信息与网络中心负责网络与信息安全监查工作，使用校园网的各部门、用户必须接受相应的监督检查，并对所采取的必要措施给予配合。

第十二条 网络与信息系统的主办（主管）部门承担安全监管责任，包括内容安全监管、技术安全保障和监督检查等；网络与信息系统的使用部门和个人对系统操作与信息内容的安全监管承担直接责任。网络与信息系统通过外包服务方式进行维护的，主办（主管）部门负责监督外包服务单位做好安全运维工作，安全监管责任主体为主办（主管）部门。

第十三条 各部门工作组履行下列职责：

（一）负责本部门的网络与信息安全管理工作，制定实施细则，建立健全网络与信息安全的各项措施，并检查各项措施的落实情况。

（二）对本部门的员工进行安全和保密教育。

（三）负责本部门网络设备的物理、系统及数据安全，做好安全管理工作，防止信息泄露和非法攻击，及时报告安全隐患和有害信息。

（四）制定或修订本部门的网络与信息安全应急预案。

（五）协助查处利用校园网进行各种违法犯罪活动的案件。

（六）对委托发布信息的部门和个人进行登记，并对所提供的信息内容进行审核。

（七）发现危害网络与信息安全的有害信息，应当保留有关原始记录，并向信息与网络中心报告，配合切断有害信息传播渠道或者关闭服务器。

第十四条 专家组及技术保障组履行下列职责:

（一）为领导小组提供技术及软硬件设备咨询，提供有关网络与信息安全的技术方案、可行性论证、事故分析等技术支持。

（二）研究、分析网络与信息安全事件。

（三）负责实施校园网用户、部门的网络与信息安全培训工作。

第十五条 各级网络与信息安全管理人员，在调任其他岗位时，应移交有关网络与信息安全的管理材料，并对材料内容负有保密责任。

第四章 安全保护

第十六条 任何部门或个人不得利用校园网危害国家安

全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

第十七条 校园网用户的通信自由和通信秘密受法律保护。任何部门或个人不得违反法律规定，不得利用校园网侵犯其他网络用户的通信自由和通信秘密。

第十八条 信息与网络中心要加强校园网账号的管理，建立账号使用登记制度，建立备案档案，进行备案统计。

第十九条 按照“同步规划、同步建设、同步运行”的原则，全面实施网络安全等级保护制度。

第二十条 涉及国家事务、经济建设、国防建设、尖端科学技术等重要领域的单位和个人办理备案手续时，应当出具其行政主管部门的审批证明。本条所涉单位和个人接入校园网时，应当采取相应的安全保护措施。

第二十一条 在特定紧急情况下，领导小组可以采取特别措施以维护校园网络与信息安全。

第五章　安全教育培训

第二十二条 学校及各部门须制定网络与信息安全教育培训规划，组织开展形式多样、针对性强的全员安全教育，不定期举办面向全员的普及性安全培训，提高全校师生员工的网络与信息安全防范意识。

第二十三条 为提升管理和技术人员的安全管理水平和安全防范能力，学校及各部门每年应不定期举办网络与信息安全管理人员和技术人员专业培训。

第六章 应急管理

第二十四条 制订《网络与信息安全事件应急管理规定》、《网络与信息安全事件应急处置预案》；明确定义重大、突发事件及其处置流程、处置机构、人员、处置目的等关键性内容。

第二十五条 健全网络安全检测、预警、信息通报与快速反应机制。根据《网络与信息安全事件应急处置预案》，成立相应的预案处置小组，配备相应的技术及操作人员。处置小组参照应急处置预案，负责处置重大、突发网络与信息安全事件。

第二十六条 任何单位及个人出现或发现网络与信息安全事件时，应按照《网络与信息安全应急处置预案》所规定的流程和《重大网络与信息安全事件报告制度》，第一时间报告网络与信息安全领导小组办公室，根据安全事件的级别进行相应处置。

第二十七条 各部门要做好预案的实战演练，切实提高校园网突发事件的预防、反应和处理能力。

第七章 安全监督与处罚

第二十八条 党委宣传部、保卫处和信息与网络中心定期组织安全检查，对所发现的问题提出改进意见，做出详细记录，存档备查。

第二十九条 各部门工作组要经常检查本部门网络与信息安全的防护管理及其技术措施的落实情况，参加领导小组

办公室组织实施的安全检查。

第三十条 本办法所涉及部门和个人，应严格履行职责。因工作疏忽，管理不善，落实不到位的，学校将追究相关人员的责任；对造成严重影响的事件，根据学校有关规定给予处分；情节特别严重，构成违法犯罪的移交司法机关处理。

第八章 附　则

第三十一条 本办法由信息与网络中心负责解释。

第三十二条 本办法自 2022 年 1 月 1 日起施行。