青岛农业大学文件

青农大校字〔2023〕2号

关于印发《青岛农业大学网络与信息安全管理办法（试行）》的通知

校属各单位：

《青岛农业大学网络与信息安全管理办法（试行）》已经2022年第28次校长办公会研究通过，现印发给你们，请认真遵照执行。

青岛农业大学

2023年1月9日

青岛农业大学
网络与信息安全管理办法（试行）

第一章　总　则

第一条　为加强学校网络与信息安全管理，提高网络与信息安全防护能力和水平，保障学校教育事业健康有序发展，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》《中华人民共和国密码法》《计算机信息网络国际联网安全保护管理办法》《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》等法律法规和文件精神，结合学校实际，制定本办法。

第二条　本办法所称网络与信息安全工作，是指由学校建设或管理，服务于学校教学、科研、管理和生活的校园网络、信息系统、互联网站、数据中心和计算机及相关配套的设备与系统，为防止发生系统故障、网络攻击、数据破坏和窃取、有害程序植入等发生而开展的预防、管理和整治工作。

第二章　管理体制与责任

第三条　学校网络安全和信息化领导小组（以下简称“领导小组”）统一领导学校网络与信息安全工作。

第四条　网络信息管理处具体负责学校网络与信息安全管理工作。主要职责是：

（一）拟定网络与信息安全管理规章制度，并组织实施；

（二）负责学校网络与信息安全防护体系的建设、运行维护、技术指导和服务支持;

（三）组织开展网络安全等级保护工作;

（四）负责网络与信息安全应急管理，并做好与上级部门的沟通对接，及时应对和处理网络安全突发事件;

（五）组织网络与信息安全技术教育和实施工作;

（六）负责网络与信息安全监督检查等相关工作。

第五条 按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，各二级单位是本单位网络与信息安全工作的责任主体，主要负责人是第一责任人。

各二级单位应明确指定专人负责网络与信息安全工作，责任人名单报备网络信息管理处，人员变动时应及时调整。

第三章 校园网络安全管理

第六条 校园网络是指校园范围内连接各种信息系统及信息终端的计算机网络，包括校园有线网络、无线网络、物联网和各种业务虚拟专网。

第七条 网络信息管理处负责校园网络与信息基础设施的建设、运行、维护和管理，包括光缆布线、网络机房、网络设备、网管系统、域名管理、IP 地址管理、安全防护、认证计费、网络接入与运维等。

第八条 网络信息管理处负责校园网络出口的统一管理和

防护。未经批准，各单位不得擅自通过其他渠道接入互联网及其他公共信息网络。禁止以任何方式破坏校园网线路及设备，妨碍校园网稳定运行。非涉密信息系统接入校园网，实行审批和备案登记制度；校园财务、图书等专用网络与互联网及其他公共信息网络实行逻辑隔离；涉密信息系统实行专网专接专用，不得接入校园网。

第九条 校园网接入实行“实名注册、认证上网”制度，禁止盗用他人的合法账号。遵守网络安全使用规定，接入校园网的计算机终端（如各类 PC 终端、机房服务器或云主机等）应安装杀毒软件且定期更新，定期升级系统漏洞补丁，保证入网计算机安全。

第十条 严禁任何单位和个人利用校园网络开展经营性活动。

第四章 信息系统安全管理

第十一条 各二级单位要按照国家网络安全等级保护制度的相关法律法规落实信息系统安全管理工作，按要求进行信息系统安全等级保护测评备案。

第十二条 各二级单位是其建设的信息系统（含移动客户端软件）的责任部门，应制定相应的系统运维和安全管理方案，指定专人负责信息系统安全管理工作，规范信息系统使用者和维护者的操作行为。

第十三条 各二级单位应定期对其建设的信息系统及操作系统、中间件、数据库进行安全检查，安装杀毒软件，定期更新和升级漏洞补丁，处置相关安全问题。

系统管理员和使用者要妥善保管账号和密码，增强密码强度，避免系统存在弱密码，定期更新密码、防止密码泄露。

第十四条 系统管理员负责信息系统日志保存工作，保留期限不少于6个月。

第十五条 对于无人管理、无力维护、存在高危风险漏洞、长期不更新的“僵尸”网站或系统，责任单位应关闭并进行整改处置，降低安全风险。对拒不关闭或整改处理的，网络信息管理处有权对其关闭。

第五章 内容安全管理

第十六条 学校域名（qau.edu.cn）及子域名由网络信息管理处负责管理。单位或个人注册申请和使用域名及子域名，应向网络信息管理处申请。若使用非学校域名并开展学校相关业务，须到网络信息管理处登记备案，自行承担一切责任。

第十七条 各二级单位开办互联网站应优先选择学校网站群平台，并遵守《青岛农业大学二级网站管理办法》相关规定。

第十八条 校园网所有用户必须遵守国家有关法律法规和学校的有关管理规定，严格执行信息安全保密制度，涉密信息不得通过互联网发布，发布者对所提供和发布的信息承担相应责任。

各单位要加强信息发布审核管理，涉及师生个人隐私敏感信息的，必须做脱敏处理，不得发布未经审核通过的信息。

第十九条 校园网用户必须自觉配合国家和学校有关部门依法进行的监督、检查，发现违法有害信息，应向学校有关部门报告。

第六章 数据安全管理

第二十条 按照“谁产生数据，谁负责管理”的原则，各二级单位负责本单位业务系统数据的产生、维护、存储、归档和备份的全周期管理。

网络信息管理处负责学校公共基础平台的数据的存储、备份、容灾和恢复等管理工作，保障数据的完整性和安全性。

第二十一条 任何单位和个人有义务保护信息系统数据安全。

第七章 监测预警与应急处置

第二十二条 网络信息管理处联合相关单位对全校各单位网络与信息安全工作落实情况进行监督检查。主要工作包括信息系统、网站的安全状况，安全保护制度及措施落实情况，以及配合上级有关部门开展的安全检查、内容检查、保密检查等。

第二十三条 宣传部加强对各二级单位网站内容发布、审核、规范和更新监督管理，对信息内容更新不及时，发布不规范的，应及时关闭处理；涉及网络舆情的遵照《青岛农业大学网络舆情

处理办法》处理。

第二十四条 网络信息管理处负责组建学校网络与信息安全应急技术队伍，提高网络与信息安全事件的应对能力，加强网络防护，做好监测预警，定期组织全校范围内的网络与信息安全事件应急演练；各二级单位组织开展网络与信息安全应急预案的宣传、教育、培训和演练，掌握应急处置方案。

第二十五条 按照学校网络安全事件应急报告与处置流程，各二级单位要做好应急事件处置工作，建立本单位安全值守制度，制定安全事件应急预案和处置方案，组织应急演练，做到安全事件早发现、早报告、早控制、早解决。

第八章 保障措施

第二十六条 学校保障网络与信息安全所需的人员和经费投入，建设高水平网络与信息安全技术支撑队伍。

第二十七条 宣传部开展面向全校的培训和宣传教育，提高师生员工的网络安全防范意识；网络信息管理处负责组织网络与信息安全技术培训。

第九章 责任追究

第二十八条 学校与各二级单位签订《青岛农业大学网络与信息系统安全责任书》。各单位要切实落实本单位网络与信息安全主体责任。

第二十九条 各二级单位要按照网络与信息安全事件报告

与处置流程及时、如实地报告和处置网络与信息安全事件。对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者在应急管理工作中有其他失职、渎职行为的，依照相关规定对有关部门及责任人进行处理；构成犯罪的，移交司法机关。

第三十条 个人违反网络与信息安全相关管理规定造成不良后果的，视情节轻重，学校按相关规定进行处理；构成犯罪的，移交司法机关。

第十章 附 则

第三十一条 本办法由网络信息管理处负责解释。

第三十二条 本办法自印发之日起施行。原相关规定与本办法不一致的，按本办法执行。

青岛农业大学党政办公室 2023年1月9日印发