大连科技学院文件

大科校发〔2025〕52 号

关于印发《大连科技学院校园网络安全保护制度（修订）》的通知

校内各单位：

《大连科技学院校园网络安全保护制度（修订）》经学校研究通过，现印发给你们，请遵照执行。

附件：大连科技学院校园网络安全保护制度（修订）

大连科技学院

2025 年 4 月 24 日

抄送：学校党政领导。

大连科技学院　　2025 年 4 月 24 日印发

附件

大连科技学院校园网络安全保护制度
（修订）

第一章 概　述

第一条 为了建立、实施、运行、监视、评审、保持和改进网络安全管理体系，确定网络安全方针和目标，对网络安全风险进行有效管理，确保全体人员理解并遵照执行网络安全管理体系文件、持续改进网络安全管理体系的有效性，特制定本制度。

第二章 管理体系组织与职责

第二条 网络安全组织架构

成立网络安全和信息化领导小组，人员组织如下：

一、人员组成

组　长：校长

副组长：副校长

成　员：各部门负责人

领导小组下设网络安全办公室，设在数据服务中心，办公室主任由数据服务中心主任担任。

二、领导小组职责

贯彻落实教育部、省教育厅的网络安全和信息化的部署和要求，统筹协调我校网络安全和信息化建设重大问题，研究制定我校网络安全和信息化发展规划、重大政策和重点工作。

三、网络安全办公室职责

1.组织落实领导小组网络安全和信息化建设的决策与部署以及各项工作任务。

2.推进和落实我校网络安全和信息化基础设施建设、网络安全管理制度建设、智慧教学建设、教育信息化运维服务体系建设、标准体系建设等工作。

3.组织开展我校网络安全和信息化建设宣传普及、人员培训等工作。

4.领导交办的其他教育系统网络安全和信息化相关工作。

第三章 安全管理策略

第三条 人力资源安全策略

1.应对所有应聘人员进行恰当筛选和背景调查，明确网络安全职责和各项权限。

2.应在人员任用条款中落实网络安全职责，建立必要的培训和奖罚制度，所有人员都必须接受网络安全培训和教育，增强网络安全意识。

3.应对任用终止与任用变化建立规范的安全控制程序，确保及时冻结或取消人员所拥有的与其目前职责不相符的信息的使用权。

第四条 信息资产管理策略

1.应确定信息资产和信息处理设施相关资产的资产清单，应制定和维护资产清单。

2.应当对所有信息资产进行识别，建立资产清单和使用规则，明确定义信息资产责任人及其职责，建立信息资产管理和使用问责制。

3.应确保各项信息资产都能得到妥善保护，确保信息的机密性，维持信息的完整性和可用性，防止信息非授权访问。

4.在就业合同或协议终止后，所有人员和外部方用户应退还所有他们使用的资产。

5.应根据信息的分类，制定和实施信息处理程序，使信息资产可以得到适当的保护。

6.对存有信息的可移动介质加强管理，防盗防丢失，原则上不使用可移动介质拷贝重要信息。

7.设备废弃或闲置前，应对存储介质进行安全处置（例如格式化等），确保信息不泄密。

第五条 访问控制策略

1.应根据业务要求建立用户对信息的访问控制规则，分配相应权限前必须经过审批。

2.只允许用户访问被授权使用的网络和网络服务。

3.必须按照用户注册和注销的手续对用户的账户和口令进行分配和注销，严禁私下操作。

4.所有用户应妥善保管自己的账户和口令，不得想其他人泄露。

5.管理员应定期对系统的用户账户、权限等进行审查，发现

问题的及时进行纠正。

第六条 工作环境安全策略

1.入校人员必须取得授权方可入校。正式教职工、本校学生可通过刷脸进出校园，临时人员应通过OA系统进行申请，经过被访部门及后勤保障及安全保卫处的审批后方可入校。

2.人员进出应随手关门，下班时应锁门，关闭窗户。

3.办公室内禁止私接电源，违规使用大功率电器，以免引起火灾。

4.应妥善保护无人值守的设备，例如如打印机、传真机、复印机等。

5.离开座位时应锁屏，重要文件及可移动存储应放入柜子中，下班时应关闭电脑。

第七条 运行安全策略

1.所有电脑应安装防病毒软件,实施更新,并定期进行扫描。发现病毒应采取必要手段进行杀毒，必要时断开网络，寻求技术人员帮助。

2.对核心设备进行操作时,必须按照既定的工作程序进行操作，留下工作记录。涉及更改重大配置或重大变更时，应进行风险评估，获得相关领导的批准后方可进行。

3.核心设备应实时监控，监测容量的使用情况，以及故障等现象，发现问题及时进行处理。

4.应分离开发、测试和运营环境，以降低未授权访问或对操

作环境变更的风险。

5.对重要信息进行备份，备份后的信息，每年进行一次复查，确保确保信息的可用性。

6.对重要系统进行监测，记录信息系统的日志，定期分析日志，识别出信息系统存在的或潜在的问题。

7.设置时钟服务器，确保所有相关信息处理系统的时钟保持同步。

8.终端电脑上应安装正版、开源的软件，不得安装违规软件。核心设备上不随意安装软件，如因工作需要，应按照变更管理流程进行安装。

第八条 通信安全策略

1.严禁使用学校网络访问违规网络服务，包括宗教、暴力、色情等等。严禁发布不实信息，传播不良内容，违者将按照相关规定予以严惩。

2.学校内部网络，根据应用需求，划分不同网段，并建立访问控制规则。用户应按照访问控制规则访问相应内部网络服务。

3.应在网络中隔离信息服务、用户和信息系统。

第九条 信息系统安全策略

1.所有信息系统，无论是采购，或是自行研发的，在开始阶段，调研需求时，必须确认安全性需求，并且应将其作为总体需求的一个组成部分，在设计阶段、开发阶段和测试阶段等予以实现。

2.在应用运维阶段应进行安全管理培训、安全监控、安全运行管理、安全风险评估、制定安全计划。

3.信息系统应采用加密技术进行保护，确保信息的保密性、完整性，选用的密码系统和密码技术应当符合国家的有关规定。

4.对信息系统的系统文件、源代码、技术资料等，采取必要的访问控制措施，防止未授权的访问。

5.信息系统开发过程中，应按照安全开发要求进行开发，包括但不仅限于工程原则、开发测试环境分离、软件包安全等等。

6.信息系统上线前，应对信息系统开展必要的安全性测试，包括但不仅限于压力测试、漏洞扫描、防病毒检测等。采购的信息系统，可要求开发商提供第三方安全检测报告。

第十条 供应商安全管理

1.对于可接触到学校内部资源的供应商，均应签订相关的保密协议。

2.如有必要，应对供应商人员进行网络安全要求的讲解，使其按照学校的安全要求开展工作。

3.对于提供有关网络安全的重要供应商（例如网络服务提供商）应与其达成协议，确保信息传输的安全。

4.供应商在提供服务的过程中，应对服务过程进行监控，确保满足合同或协议中的安全条款得以满足。对于服务的变更，应按照正式的变更流程对服务的变更进行控制。

第十一条 应急管理策略

1.成立专门的应急小组，负责重大故障发生时，实施应急方案，迅速解决故障，回复业务的正常运行。

2.应急小组，应针对重要业务应用系统，应当建立必要的应急预案，当发生重要业务应用系统中断时，能及时启动应急预案，快速恢复业务应用系统的正常运行。

3.当发生重大灾难时，应针对关键业务实施业务连续性计划，保证学校关键业务流程不受重大灾难的影响。

4.应做好应急预案和业务连续性计划的演练和持续更新，应急预案和业务连续性计划的演练至少每年执行一次，在每次总结过程中应当对业务连续性计划的有效性进行检查，并及时改进。

5.信息处理设施应实施足够的冗余，以满足可用性要求。

第十二条 其他安全要求

1.所有人员发现网络安全事件时，应及时上报网络安全及信息化领导小组，网络安全办公室应第一时间进行调查取证，并采取必要措施解决事件。

2.事件解决后，应针对事件发生的原因、解决过程进行总结，找出事件的根本原因，并制定相应的策略，消除根本原因，避免同类事件再次发生。

3.所有人员应妥善保护个人隐私数据，未经授权不得传播、滥用他人个人数据。

4.所有的安全策略必须符合相关的法律法规的要求，凡是违法的行为均视为违反学校的安全策略，将根据相关规定予以惩

罚。

第四章 附　则

第十三条 本规定由数据服务中心制定、维护，并负责解释。

第十四条 本规定自发布之日起生效，同时废止《大连科技学院校园网络安全保护制度》（大科院发〔2016〕106 号）。