

兰州理工大学文件

兰理工发〔2021〕87号

关于印发《兰州理工大学信息系统安全管理 办法》的通知

校属各单位、部门：

《兰州理工大学信息系统安全管理办法》经2021年5月14日党委常委会会议审定通过，现予以印发，请遵照执行。



兰州理工大学信息系统安全管理办法

第一章 总则

第一条 根据《中华人民共和国网络安全法》、《中华人民共和国密码法》、《网络安全等级保护条例》等法律法规，以及教育部《高等学校数字校园建设规范（试行）》要求，为提高学校信息化建设和管理水平，切实保障校内信息系统安全和稳定运行，落实网络安全主体责任，结合学校实际，制定本管理办法。

第二条 本办法所指信息系统包括校属各单位、部门建设的信息化系统、虚拟服务资源和其它任何与兰州理工大学相关的公有云租赁服务资源。

第三条 学校网络安全与信息化领导小组办公室（以下简称网信办）负责统筹协调推进网络安全和信息化工作，网络与信息中心负责网络与信息化归口管理和技术支撑工作，校内各单位、部门是本单位、部门所属信息系统管理的主体责任单位，各单位、部门主要负责人为第一责任人。为保障信息系统的安全稳定运行，各单位、部门必须指定人员对信息系统进行全生命周期管理。

第二章 信息系统建设安全管理

第四条 学校信息系统安全建设要遵循与信息系统建设“同步规划、同步建设、同步运行”的原则，确保信息系统建设安全可控。

第五条 学校信息系统建设在学校信息化总体规划框架下，按照“谁需要、谁建设，谁使用、谁管理”的原则实施。

第六条 信息系统建设需遵循学校的相关标准（数据、接口等）、规范及安全要求，确保与学校信息化基础平台有效稳定对接，并能够按照要求有效进行全量数据交换。信息系统技术架构要符合安全防护要求，并具备必要的安全防护能力。

第七条 信息系统在部署前必须由建设运行单位、部门向网络与信息中心提交安全审查申请，由网络与信息中心对该信息系统进行安全审查，审查通过后进行信息系统安全备案，实施系统部署。

第三章 信息系统资源管理

第八条 校园网及信息系统服务资源等相关基础设施由网络与信息中心统一规划、建设、管理，并提供统一资源服务，校属各单位、部门及个人不得擅自建设、更改、损毁、挪用校园网及相关基础设施，不得私接外网出口。

第九条 信息系统上线运行须申请的资源包括网络资源、服务器资源、运维资源、域名资源、数据库资源、公共数据资源、杀毒资源、备份资源等，各单位、部门根据信息系统建设内容的要求申请资源，由网络与信息中心负责审核，统一向各申请单位、部门提供资源，开放相应服务。

第十条 由学校提供的各类信息化资源实行全生命周期管理，遵循“谁申请、谁负责，谁审批、谁负责”的原则管理，要避免校内“僵尸”资源存在，实现对各类资源的申请-注销闭环管理，提高学校信息化资源利用率。

第十一条 信息系统建设单位、部门申请校内资源须在 OA 填写相关资源申请表，申请公有云服务资源实行备案制，并填写《兰州理工大学公有云租赁服务备案表》。

第十二条 各单位、部门须根据信息系统所运行业务发展需求，按照“合理申请，有限开放”的原则申请资源，避免资源浪费和安全隐患。

第四章 信息系统运行管理

第十三条 相关单位、部门在完成信息系统部署后，由系统管理人员在 OA 填写《兰州理工大学信息系统安全审查申请表》，由网络与信息中心负责组织人员进行安全核查评估，信息系统通过安全核查评估后方可上线提供服务。

第十四条 各单位、部门须指定管理人员定期对本单位、部门信息系统管理和使用情况进行检查，落实网络安全等级保护制度。每年第四季度由网络与信息中心根据相关规定对下一年度需要进行等级保护定级和测评的信息系统进行梳理并上报学校，经学校同意后由网络与信息中心负责指导各单位、部门完成信息系统等级保护及备案工作。

第十五条 为保障信息系统的安全稳定运行，网络与信息中心要定期或不定期对全校信息系统进行安全检查，对发现安全漏洞的要及时下发整改通知，相关单位、部门必须立即组织人员进行整改，对整改达不到要求的，网络与信息中心可关闭相关服务。相关单位、部门完成整改后撰写整改报告，由部门负责人审核后上报网络与信息中心，网络与信息中心进行审核测评，达到安全要求后开放相关服务。网络与信息中心应不定期的对信息系统监测中发现的安全漏洞情况进行通报。

第十六条 相关单位、部门在接到网络安全整改通知后，须在 3 个自然日内完成问题整改。对于确因技术原因 3 日内无法完成整改的，所在单位、部门提交网络安全整改承诺书，经本单位、部门主要负责人及分管校领导签字后，经由信息化分管校领导审批，方可延期整改，否则关停相应信息系统。

第十七条 各单位、部门负责人和系统管理员必须掌握本单位信息化系统资产使用和管理情况，并建立信息系统资产台账，按照“谁主管谁负责、谁使用谁负责、谁运维谁负责”的原则，做好信息系统及所承载服务的日常健康监测、软件安装管理、数据备份、杀毒、数据开放和密码管理等运维管理工作。

第十八条 为了加强信息系统密码管理，各信息系统管理人员设置的系统管理密码要具有足够强度，必须包含大写字母、小写字母、数字和特殊字符中的两种及以上，且长度不少于 8 位，并在使用过程中定期或不定期修改密码。要妥善保管密码，防止

泄露，具体管理要求按照《兰州理工大学信息系统密码管理办法》执行。

第十九条 各单位、部门系统管理人员不得擅自变更、增加所申请的服务器资源承载的业务系统，如确需变更或增加，应下线原业务系统，重新填写相关资源申请表，提交网络与信息中心审核通过后方可实施。

第二十条 各单位、部门因学校工作需要共享信息系统所承载的师生个人信息数据，必须经网络与信息中心审核同意并报备。使用师生个人信息要严格遵守国家关于个人信息保护的相关法律法规，禁止私自以任何形式对外发布或提供相关信息数据。

第二十一条 各单位、部门信息系统管理人员在日常运行管理过程中要加强对信息系统的监测，及时关注网络与信息中心相关通知。一旦发现网络安全事件，应立即向网信办和网络与信息中心报告，并采取相应的应急举措，网信办和网络与信息中心根据对安全事件的分析，采取妥善应对措施。

第二十二条 各信息系统使用单位、部门及人员须遵守国家相关法律法规和学校相关规章制度，不得利用所申请资源从事危害国家安全、违法犯罪、泄露国家和学校秘密信息的活动，不得接收、存储和发布违反国家法律法规和学校相关规定的信息，不得利用所管理、使用的信息系统从事商业相关活动。

第五章 责任追究

第二十三条 对违反本管理办法的，给予相应处理。情节较轻的，由网信办对信息系统所属单位、部门进行约谈或通报批评；情节较重或给学校名誉造成损失的，由网信办提请学校视情节对信息系统所属单位、部门及相关责任人进行追责处理。

第二十四条 对于有危害公共安全、国家安全、泄露国家秘密以及其他违反法律、法规和规章规定行为的，由公安、国家安全、保密以及其他监督管理部门依法处理；构成犯罪的，依法追究刑事责任。

第六章 附则

第二十五条 本管理办法自发布之日起执行，由网信办、网络与信息中心负责解释。

