

北京科技大学信息化建设与管理办公室

校信发〔2024〕4号

北京科技大学信息系统安全建设与运行管理规范

第一章 总则

第一条 为规范北京科技大学（以下简称“学校”）信息系统安全建设与运行管理工作，规范安全管理流程，明确安全管理职责，保障学校信息系统安全，根据《信息技术软件生存周期过程》（GB/T8566-2007）、《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）、《信息安全技术网络安全事件分类分级指南》（GB/T20986-2023）等要求，结合我校信息化工作实际，特制定此规范。

第二条 本规范适用非涉密信息管理，涉密信息管理按照学校信息安全保密管理体系文件进行落实。

第三条 本规范所称网络与信息安全，包括校园网络安全、信息系统安全和信息内容安全。

第四条 本规范所称信息系统，是指计算机软件应用程序，是能够满足特定单位工作或教学领域需求而设计开发的功能集合体。

第五条 本规范所称用户，分为系统管理员、安全审计员和

普通用户。系统管理员拥有信息系统用户管理最高权限，该用户可进行用户的新增、变更、注销操作，可对安全审计员、普通用户进行授权操作；安全审计员拥有信息系统日志审计等特定功能模块的业务管理功能权限；普通用户拥有信息系统普通业务功能的使用权限。

第六条 学校信息系统管理按照“谁管理谁负责、谁运维谁负责、谁使用谁负责”的原则，学校各部门和全体师生应依照本规范及相关文件履行网络安全的义务和责任。

第二章 职责和分工

第七条 信息系统安全建设与运行维护过程中,涉及的单位主要包括信息化建设与管理办公室（以下简称“信息办”）、各二级单位和服务提供商。信息办是学校网络安全归口管理部门，各二级单位是学校承办信息系统建设的承办部门，服务提供商是为信息系统提供技术、信息咨询、服务和解决方案的团队或个人。

第八条 学校网络安全归口管理部门是信息化建设与管理办公室，主要职责如下：

（一）负责学校信息化基础设施环境的安全运行与维护；

（二）对学校全量信息系统定期进行安全检测；

（三）组织学校各二级单位、服务提供商完成信息系统安全等级保护定级、备案及测评工作；

（四）配合二级单位完成资源申请、系统部署、业务开通、上线运行等工作；

（五）组织学校各二级单位、服务提供商进行故障排查

和处理。

第九条 学校各二级单位负责建设、管理、运维学校网络和信息系统。其主要职责如下：

（一）负责提出信息系统建设需求、资源需求和规划设计；

（二）负责对接和监督管理服务提供商，对信息系统进行网络和信息系统的建设以及安全测试，完成系统上线前备案登记；

（三）负责提供网络安全等级保护定级备案所需材料，配合信息办开展网络安全等级保护备案与测评工作；

（四）负责督促服务提供商及时整改安全漏洞和复测漏洞，防范网络安全风险。

（五）负责协调处理信息系统建设与运行维护过程中出现的各类问题，包括但不限于信息系统的故障申报受理、咨询和建议，并协同服务提供商、信息办进行故障处理；

（六）各二级单位应设置网络安全联络员和对应信息系统的管理员。网络安全联络员负责与信息办对接网络安全工作，信息系统的管理员负责信息系统的运行维护管理工作。

（七）在信息系统安全建设与运行维护过程中监督管理服务提供商严格遵守校内要求，履行各自职责。

第三章 上线前安全要求

第十条 规划设计。学校各二级单位应在项目建设需求初期初步确认信息系统网络安全保护等级，并依据网络安全保护等级保护要求进行需求调研与建设开发等工作，初期需开展项目立项评审会，系统需求分析、系统设计方案等作为立项材料应进行评

审，并留存信息系统安全建设方案文件。

第十一条 定级备案。学校各二级单位应根据初步确认的网络安全等级保护级别并准备等级保护备案材料，包括但不限于《网络安全等级保护定级报告》、《网络安全等级保护备案表》、《北京科技大学网络安全责任书》等（详情请见附件二、附件三和附件四），由信息办统一组织开展网络安全等级保护定级专家评审会与测评工作，加强等级保护一级系统管理将其纳入为等级保护审核范围，且一级应用系统不允许开放外网访问。

第十二条 资源申请。学校各二级单位在签订项目建设合同后，在信息系统计划部署前在网上办事大厅申请所需服务器资源（若需），提交服务器配置等具体要求，并明确申请资源用途，服务器资源申请通过后，需在网上办事大厅申请 VPN/堡垒机账号、SSL 证书、信息系统域名等其他信息系统必备网络资源。

第十三条 测试安全。测试环境安全要求应与正式环境保持一致，学校各二级单位应当在测试结束后立即清除测试环境和测试数据，同时测试环境禁止与北京科大学有任何名义的关联。学校各二级单位负责为服务提供商提供与信息系统数据格式一致的测试数据。测试数据一律不得直接使用真实数据。

第十四条 安装部署。学校各二级单位在获得所需部署资源后应根据系统部署计划、系统安装部署说明，经该系统建设部门主要负责人批准后方可开展系统部署工作。

第十五条 信息系统登记备案。学校各二级单位应在系统部署完成后通过网上办事大厅进行信息系统登记备案，并完成校内统一身份认证的对接工作，信息系统登记备案表详见附件八。

第十六条 用户策略设置。学校各二级单位在系统部署后应根据最小授权原则对用户开通账户与权限，同时设置安全审计员、系统管理员等账户角色。

第十七条 安全测试。学校各二级单位在信息系统安全建设完成初期系统上线前，应在进行功能性测试后，开展充分的安全性测试，包括不限于漏洞扫描、渗透测试、代码审计等形式。对于等保一级信息系统，由二级单位向信息办提申请，信息办开展漏洞扫描并督促二级单位整改；对于等保二级及以上的信息系统和需要互联网访问的信息系统，二级单位需要向信息办提供由第三方检测机构所提供的渗透测试报告，并确定漏洞均已修复，第三方检测机构应至少具备中国网络安全审查技术与认证中心颁发的信息安全风险评估服务资质一级认证。

第十八条 正式上线。学校各二级单位在完成安全测试后申请系统正式上线，系统正式上线前需对信息系统备案进行补充与确认，同时学校资管平台将同步备案信息进行网络安全运营管理。

第四章 上线后安全要求

第十九条 安全检测。信息系统根据网络安全等级保护等要求，按照规定定期进行安全检测，检测手段主要包括对信息系统进行渗透测试、漏洞扫描等。学校各二级单位需配合信息办开展不定期安全检测工作，并进行漏洞整改工作，其中关于信息系统漏洞管理参考《北京科技大学网络安全漏洞管理与应急处置管理细则》。

第二十条 账户角色变更。如在信息系统运行期间涉及到用户角色的变更，如信息系统负责人、网络安全联络员等人员信息

变更，应及时联系信息办进行人员基本信息的更新。

第二十一条 信息系统资产管理。信息办依托互联网信息资产探测等技术手段定期开展资产探测工作，学校各二级单位应配合信息办开展信息资产登记、确认等管理工作，并于北京科技大学安全资管平台中更新资产信息。信息办需在教育系统网络安全工作管理平台动态更新信息资产信息。

第二十二条 等级保护测评。信息系统上线后由信息办统一组织开展网络安全等级保护测评工作，学校各二级单位应配合归口管理部门开展等级保护测评工作，包括但不限于协调相应服务提供商配合上机检查、人员访谈以及安全整改等工作。

第二十三条 安全整改。信息办按照网络安全等级保护要求定期开展系统安全测试工作，学校各二级单位应对安全测试结果及时进行整改，并在规定时间内反馈整改情况，并经由信息办验证整改结果。

第二十四条 运行维护工作原则。学校各二级单位应对信息系统的维护与管理定岗、定人、定责，确保运行维护工作的持续性和有效性。

第二十五条 运行维护工作内容。学校各二级单位生产环境的运行维护工作主要包括：服务器、操作系统、中间件、数据库、文件系统及网络等的配置、管理与维护。信息系统的运行维护工作主要包括：用户、权限、数据及内容等的配置、管理与维护。

第二十六条 系统更新分类。信息系统上线运行后的系统更新按照目的分为修复性更新和功能性更新。修复性更新的主要目的是对运行过程中发现的系统问题进行修复、提升稳定性和提高

性能；功能性更新的主要目的是根据业务需求变化等对原有功能进行增加或更改。

第二十七条 功能性更新原则上需要对更新后的系统重新开展安全性测试工作，若涉及原等级保护备案变更（如级别变更、名称变更、系统合并等情况）应由学校各二级单位更新系统等级保护备案材料，编写信息系统变更情况说明，提交《系统变更信息表》，由信息办进行等保备案更新。

第五章 安全管理

第二十八条 应用系统安全运维策略应按如下原则：

1. 最小权限原则：指系统只能授予应用程序和用户必要的权限，而不能授予额外的权限；
2. 最少服务原则：指在保证系统和应用运行正常的前提下，关闭其它无关的系统服务和网络服务。

第二十九条 安全监测。学校各二级单位应指派相关人员对上线运行的信息系统安全状况进行监控。信息办定期对上线运行的信息系统进行安全测试，一旦发生安全事件应第一时间通知二级单位负责人并及时通知信息办协助共同开展安全事件应急处置与溯源。

第三十条 安全事件整改与事件处理。信息办会同学校各二级单位及服务提供商依照《信息技术安全技术信息安全事件管理》（GB/T20985-2017）与《北京科技大学网络安全事件应急预案》对发现的安全事件进行整改和处理。

第六章 撤销管理

第三十一条 当某个信息系统因业务调整、技术更新或其他

原因不再使用时，需要对其进行正式的撤销管理，为确保信息资产的安全性和合规性，撤销流程如下：由系统使用部门或负责人提交信息系统撤销申请，说明撤销原因、系统当前状态和数据存储情况；信息办对系统进行评估，包括数据安全性、系统依赖性和资源占用情况，确认无误后则同意系统撤销。

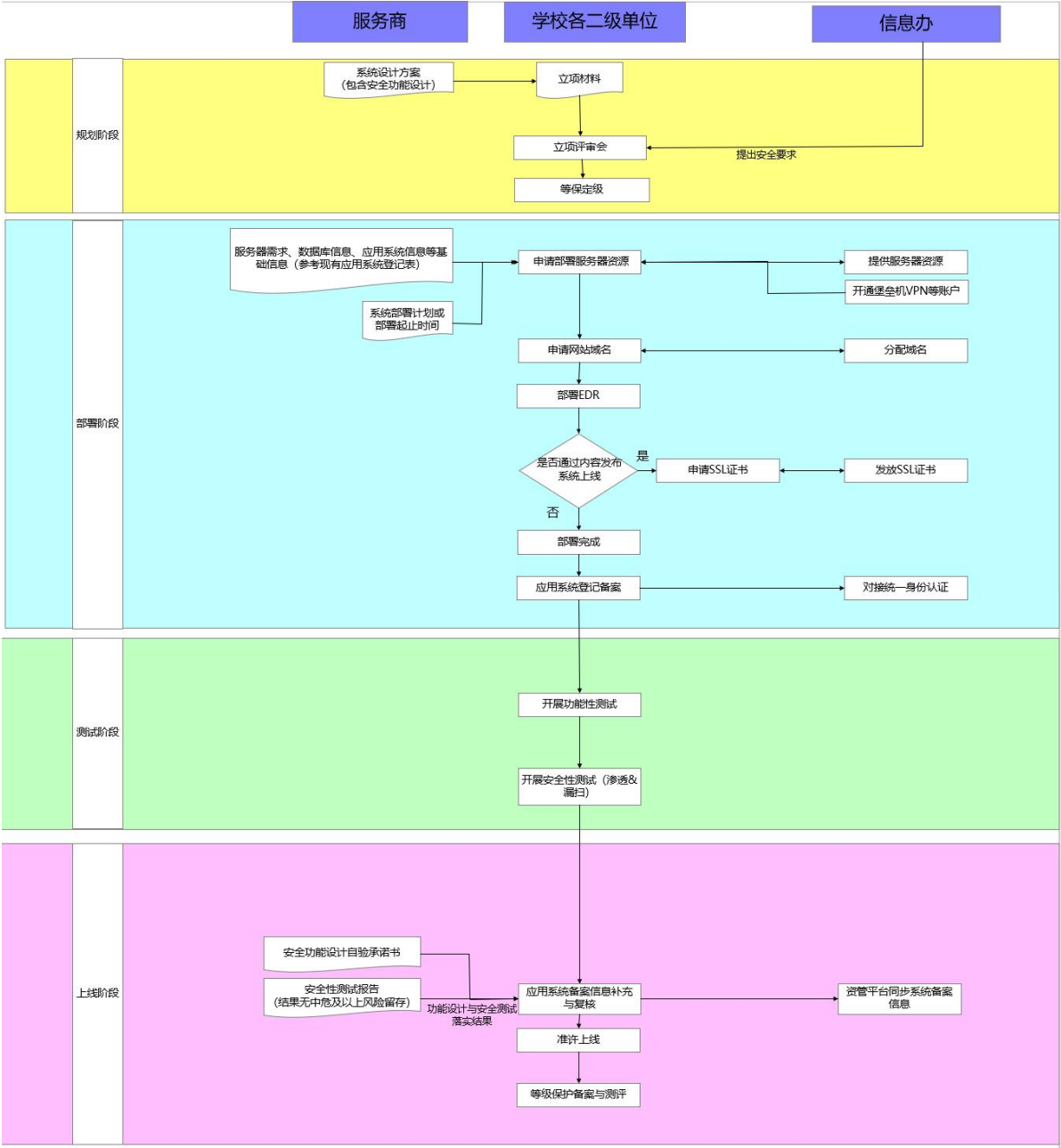
第三十二条 在系统撤销前，系统负责人必须对重要数据进行备份并迁移至其他系统或存储设备，确保数据不丢失，并由统一进行数据销毁；信息办将系统从生产环境中下线，并回收相关硬件、软件资源；信息办在资产管理系统中更新报销信息。

第七章 附则

第三十三条 本规范由信息办负责解释。

第三十四条 本规范自发布之日起施行。

附件一：系统上线前安全管理流程图



附件二：网络安全等级保护定级报告

****系统/网站**

网络安全等级保护定级报告

一、北京科技大学**门户网站系统描述

北京科技大学**门户网站主要提供***信息发布，将日常的信息、教学、招生等信息在社会、家庭、个人之间进行及时高效、全程共享的沟通和处理。北京科技大学***（二级部门名称）是该信息系统业务的主管部门及信息系统定级责任单位。

门户网站使用学校网站群管理平台。服务对象为本单位内部网站建设和维护人员，服务范围为广域互联网，主要功能是学校和各院系网站建设和维护以及访问功能，实现对于学校网站的集中式管理，提高网站管理效率和安全的统一性，实现对于学校网站的统一管理。

二、北京科技大学***门户网站安全保护等级的确定

（一）业务信息安全保护等级的确定

1. 业务信息描述

北京科技大学****网站平台包括：……等模块。

2. 业务信息受到破坏时所侵害客体的确定

该业务信息遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益。

侵害的客观方面表现为：一旦信息系统的内容遭到入侵、修

改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会对公民、法人和其他组织的合法权益造成较为严重影响和损害，可能会对学校公信力和社会形象造成危害，可以表现为：造成不良影响，引起法律纠纷等。

3. 信息受到破坏后对侵害客体的侵害程度

上述结果的程度表现为**严重损害**，即出现**严重**的法律问题，**严重范围**的不良影响等。

4. 确定业务信息安全等级

依据信息受到破坏时所侵害的客体以及侵害程度，确定业务信息安全等级为 **X** 级。

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

（二）系统服务安全保护等级的确定

1. 系统服务描述

本信息系统主要为……服务。

2. 系统服务受到破坏时所侵害客体的确定

本系统受到破坏时，会影响……有关信息的及时了解，所侵害的客体是公民、法人和其他组织的合法权益。客观方面表现的侵害结果为：可以对公民、法人和其他组织的合法权益造成侵害。

3. 信息受到破坏后对侵害客体的侵害程度。

上述结果的程度表现为：对公民、法人和其他组织的利益造

成一般损害，即会出现一般范围的不良影响。

4. 确定系统服务安全等级

查《定级指南》表 3 知，依据系统服务受到破坏时所侵害的客体以及侵害程度确定系统服务安全等级为 X 级。

系统服务被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

（三）安全保护等级的确定

信息系统的安全保护等级由业务信息安全等级和系统服务安全等级较高者决定，最终确定****门户网站系统安全保护等级为第 X 级。

信息系统名称	安全保护等级	业务信息安全等级	系统服务安全等级
北京科技大学****网站	二级	二级	一级

附件三：北京科技大学重点岗位人员网络与数据安全保密承诺书

我了解国家、学校及我部门有关网络与数据安全保密有关规定，知悉应当承担的保密义务和法律责任，本人庄重承诺：

一、严格遵守国家、学校及我部门相关管理规定，合理、规范、安全地使用计算机、网络、数据和信息资源。

二、在工作中接触到的有关重要资料、数据和信息，包括但不限于教职工、学生个人身份信息、学校教学、科研、管理、服务等重要业务信息，学校系统(网站)、服务器、数据库等各类管理员账号和密码，以及学校尚未公开的建设文件、建设规划和建设方案等资料，均视为需要保密的重要信息。

三、在未得到学校许可的前提下，不得以任何方式泄露所接触和知悉的网络与数据安全重要信息；不违规记录、存储、复制学校网络与数据安全重要信息；不私下留存网络与数据安全重要信息载体。

四、未经允许，不得进行影响系统运行的操作，包括但不限于：关闭主机（设备）、关闭关键服务、修改数据库、修改系统配置、删除系统数据等。

五、对自己使用的及管理的账号，要做到实人使用、不得外借，且必须加强密码管理，不使用弱密码。

六、离岗、离职后，对接触过的重要信息在一年之内依然承担保密责任，不得保留重要信息副本，一切关于重要信息的资料或管理账号均需返还信息责任部门，保证信息不会外泄。

七、若违反上述承诺，愿意接受学校有关处罚及追责。

单位（科室）：

承诺人签名：

年 月 日

附件四：北京科技大学二级部门网络安全责任书

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》和《信息安全等级保护管理办法》及其他国家网络安全有关法律、法规规定，为加强学校各单位的网络安全保护工作，明确和落实网络安全责任，特签订网络安全责任书，具体内容如下：

一、按照“谁主管、谁负责，谁运营、谁负责，谁使用，谁负责”的原则，各单位是本单位网络安全的责任主体，单位主要负责人是网络安全的第一责任人，要逐级落实安全责任，并为网络安全工作提供必要的人员保障。

二、各单位应加强组织领导，明确职责任务，将网络安全职责层层分解、落实到具体岗位和具体人员。

三、各单位应认真履行各项网络安全工作职责，包括并不限于以下内容：

（1）按照国家有关规定，落实网络安全等级保护管理制度和技术防护措施，积极配合学校开展定级备案、安全测评、安全整改和安全自查等工作。

（2）做好本单位系统（网站）的安全防护工作。加强各系统账号密码的安全管理，防范弱密码。敦促系统运维支持单位定期查杀病毒、后门等恶意程序；及时修补各类系统漏洞；对重要数据采取备份和加密措施；留存系统日志不少

于 6 个月。

（3）规范数据采集和使用，不采集超越职能范围的数据，保障数据安全。

（4）制定本单位网络安全应急预案，明确应急处置流程，定期开展应急演练，发生网络安全事件立即启动应急预案快速妥善处置。

（5）严格管控“双非”系统（网站）（指本单位运营使用的，但 IP 地址和域名均不属于学校管理范围的系统（网站）），采取关停并转等措施杜绝“双非”系统。

（6）对重要数据和公民个人信息，应采取措施防范数据泄露或失窃，数据接触人员、第三方运维单位须签订数据安全保密协议。

（7）积极配合学校开展网络安全知识宣传教育工作，提高本单位人员安全意识、素养，遵规守法、文明上网。

（8）积极配合学校网络安全检查工作，整改安全风险隐患。配合学校做好重要时期网络安全保障工作，加强系统（网站）安全监测和人员值守，如遇网络安全突发事件，按照应急预案处置上报。

四、对网络安全责任和工作要求不落实的单位，学校督促其及时整改。造成网络安全事件的，依法追究相关单位及责任人的法律责任。

单位负责人（签字）：

单位盖章

年 月 日

附件五：系统变更信息表

变更方联系人		联系电话	
变更方所在部门		系统变更时间	
系统变更类型	☐ 功能增加 ☐ 系统升级 ☐ 网络变更 ☐ 等级保护备案变更 ☐ 其他_____		
变更系统域名			
变更系统 IP 地址			
变更的主要内容			
变更方部门领导意见	审批人签字： 审批人时间：		

