3 信息系统建设安全管理规定

第一章　　总则

第一条 根据《北京大学网络安全管理办法》（试行）要求，为规范北京大学各单位信息系统立项、建设、上线、运维等环节的安全管理，降低安全风险，提升安全防护能力，提高安全管理水平，特制定本规定。

第二条 本规定适用于北京大学如下系统：以“pku.edu.cn”为域名后缀的系统；使用北京大学 IP 地址的系统；系统名称包括“北京大学”、“北大”、“Peking University”、“PKU”、“燕园”、“未名”等与学校相关字样的系统；页面包含北京大学校徽等官方标识的系统；采用北京大学各类经费建设的系统。

第二章　　信息系统定级备案管理

第三条 依据《网络安全法》等国家和教育行业相关规定，北京大学网络安全和信息化委员会办公室（简称“网信办”）会同北京大学计算中心（简称“计算中心”）统筹开展学校信息系统定级备案工作和二级及以上系统的测评、整改工作。其中一级系统在北京大学备案，二级及以上系统在公安机关备案。

第四条 依托备案系统（https://register.pku.edu.cn）完成信息系统定级备案工作，包括新增信息系统、变更信息系统信息、撤销信息系统等功能。

第五条 学校每年定期开展信息系统在线使用情况调查，各二级单位通过备案系统确认信息系统服务情况、更新系统运行信息。

第三章 信息系统立项阶段

第六条 系统立项申请部门应填写《信息系统安全建设方案》(见附件一，以下简称《安全建设方案》)，提交给网信办和计算中心。

第七条 计算中心审核《安全建设方案》并根据国家网络安全等级保护要求提出初步定级建议，网信办对初步定级结果进行确认。

第四章 信息系统建设阶段

第八条 立项申请部门应根据初步定级结果，要求开发方（含自行开发和外包开发)，在信息系统建设阶段遵循《安全建设方案》，所开发系统应满足身份认证、访问控制、安全审计、输入验证、数据保密性等安全要求，符合《信息系统代码安全开发规范》(见附件二)。

第九条 应保证软件开发环境和测试环境分离。

第十条 外包开发，应与软件开发单位签订第三方保密协议（模板参见《北京大学网络安全管理制度人员安全管理规定》)。

第五章 信息系统上线阶段

第十一条 信息系统上线前，立项申请部门应组织对信息系统进行源代码安全审计和安全风险评估，形成《信息系统源代码安全审计报告》(模板见附件三）和《信息系统安全风险评估报告》(模板见附件四)。安全风险评估报告应参照信息系统等级保护对应级别相关要求，涵盖要求项差距分析、漏洞

扫描、渗透测试等方面，确保已实现系统安全功能、不存在高风险漏洞。

第十二条　系统立项申请部门通过“北京大学网站和信息系统备案系统”（简称“备案系统”）填写信息系统相关信息，生成《信息系统备案申请表》（见附件五），上传《信息系统源代码安全审计报告》和《信息系统安全风险评估报告》，初步定级为二级及以上系统应同步上传等保定级材料（见附件六信息系统定级备案材料）。

第十三条　系统立项申请部门应对《信息系统备案申请表》（含《信息系统安全承诺书》（见附件七））进行签字盖章，提交计算中心存档。

第十四条　计算中心按照“第六章 域名管理”和“第七章互联网开放服务管理”要求，设置域名、开放外网访问权限等。

第六章 域名管理

第十五条　域名服务是互联网重要基础服务。北京大学域名为 pku.edu.cn，由北京大学计算中心管理。

第十六条　根据《中华人民共和国网络安全法》、《互联网信息服务管理办法》、《非经营性互联网信息服务备案管理办法》、《互联网 IP 地址备案管理办法》、《中国互联网络域名管理办法》等相关法律法规，学校各二级单位、附属单位、教职工、学生不得使用校内 IP 地址注册校外（非 pku.edu.cn）未经北京大学同意在上级行业主管部门正式备案的域名。学

校不提供将北京大学域名指向校外 IP 地址的服务。

第十七条　凡属北京大学管理、带有“北京大学”、“北大”、“Peking University”、“PKU”、“燕园”、“未名”等与学校相关字样，以及北京大学校徽等官方标识、为北京大学师生提供服务或者面向社会公开提供服务的网站和信息系统，均应使用北京大学域名（*.pku.edu.cn）或其他经北京大学同意在上级行业主管部门正式备案的域名。

第十八条　域名的命名一般由 26 个英文字母（不区分大小写）、数字组成，域名的命名应以单位缩写或简称或对应英文名为优先，建议 4-8 个字符长度，最长不超过 25 个字符。计算中心对申请的域名进行审核。

第十九条　北京大学域名用于学校日常的教学、科研、管理和服务活动，严禁用于商业和其他用途。

第二十条　域名注册申请人必须是提供信息服务的二级单位，包括北京大学各教学单位、管理部门、挂靠单位、群团组织、直属附属单位。域名申请需经二级单位安全管理员确认。

第二十一条信息系统上线发布前、通过备案系统提交基本信息时，填写初定域名名称。

第二十二条完成备案并确定域名后，计算中心为信息系统开通域名服务。

第二十三条对因重要活动、会议等临时开通的域名，应在活动结束后，由各二级单位及时知会计算中心予以注销。

第二十四条域名变更或注销，应重新填报“备案申请表”。

第二十五条信息系统域名纳入北京大学网站和信息系统年审制度统一管理。

第七章 互联网开放服务管理

第二十六条北京大学网站和信息系统根据其业务服务需要分为互联网访问（校外访问）和校园网访问（校内访问）两种。

第二十七条系统备案单位应在填写信息系统基本信息时明确是否需开通校外访问，以及需要开放的端口。

第二十八条根据最小权限原则，仅对必要服务的必要端口开通校外访问。

第八章 附则

第二十九条本规定是《北京大学网络安全管理办法》(试行)配套系列制度之一,从属于《北京大学网络安全管理办法》（试行)。

第三十条　其他校区参考本规定制定相应管理规定。

第三十一条本规定由北京大学网络安全和信息化委员会办公室和北京大学计算中心负责解释。

第三十二条本规定自发布之日起施行。

附件一 《信息系统安全建设方案书》

信息系统安全建设方案书

<table>
<tr><td colspan="6">项目立项申请单位</td></tr>
<tr><td>项目名称</td><td colspan="3"></td><td>项目编号</td><td></td></tr>
<tr><td>立项申请单位</td><td colspan="2"></td><td>执行单位</td><td colspan="2"></td></tr>
<tr><td rowspan="3">项目负责人
（处级）</td><td>姓名</td><td colspan="2"></td><td>职　务</td><td></td></tr>
<tr><td>所在单位</td><td colspan="4"></td></tr>
<tr><td>移动电话</td><td colspan="2"></td><td>电子邮箱</td><td></td></tr>
<tr><td rowspan="3">项目联系人</td><td>姓　名</td><td colspan="2"></td><td>职　务</td><td></td></tr>
<tr><td>所在单位</td><td colspan="4"></td></tr>
<tr><td>移动电话</td><td colspan="2"></td><td>电子邮箱</td><td></td></tr>
<tr><td rowspan="5">信息系统情况描述</td><td>业务类型</td><td colspan="4">□1 网站类 □2 内部办公类系统 □3 学生管理类系统
□4 公众服务类系统</td></tr>
<tr><td>服务对象</td><td colspan="4">□1 单位内部人员 □2 社会公众人员</td></tr>
<tr><td>业务描述</td><td colspan="4"></td></tr>
<tr><td>开放服务范围</td><td colspan="4">□校园网 □互联网</td></tr>
<tr><td>存储数据描述</td><td colspan="4">1. 学生基本信息：□1 姓名 □2 身份证号 □3 学籍号 □4 手机号 □5 家庭地址 □6 成绩信息 □7 学历信息 □8 其他信息 _____
2. 教职工基本信息：□1 姓名 □2 身份证号 □3 教职工号 □4 手机号 □5 家庭地址 □6 其他信息 _____
3. 其他个人信息数据 _____
4. 其他业务数据 _____</td></tr>
</table>

		5. 涉及个人信息人数 约_____人/年
系统安全功能方案	信息系统安全功能方案可参考如下要求明确其系统安全功能设计： *1、 系统账户的鉴别信息需对密码复杂度做限制，要求至少8位以上，包括三类字符（数字、字符、大小写字母等）；* *2、 应用系统账户需对密码有效期做限制，要求最长使用期限不超过1年，强制密码历史记录为至少1次；* *3、 应强制用户首次登录时修改初始口令；* *4、 用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全。* *5、 通信双方建立连接前， 应用系统应具备利用密码技术对会话的初始化进行验证，即通过身份认证后方可执行业务操作* *6、 系统中用户身份必须唯一；* *7、 需要有账户登录失败处理；（如限制非法登录次数超5次后，账户锁定15分钟或者程序自动退出等处理方式）* *8、 系统正式应用时，应禁用默认账户或测试账户，删除多余账户。* *9、 系统需提供安全审计功能；（即对用户的操作行为进行日志记录，审计要素包括日期、时间、发起者信息、类型、描述、结果。审计内容覆盖登录、注销、添加删除用户、重要变更、重要业务操作等）* *10、 审计日志不能被手动删除，并配置日志定期备份；* *11、 审计日志应至少保留180天；* *12、 应用系统用户端与服务器端之间进行通信时，应具有校验数据完整性的功能（如CRC校验码或采用密码技术的校验算法，例如国产的SM3算法、国际的SHA256\SHA512、MD5+SALT方*	

	式等算法） *13、 应用系统用户端与服务器端之间进行通信时，应对会话过程（例如用户登录信息或其他敏感字段）进行加密传输（例如 SSL 加密或其他类似加密算法的传输方式）;* *14、 应用系统的鉴别信息（如密码）和重要业务数据在数据库中应加密存储，且使用健壮的加密算法。（可采用国际的 AES、DES、RSA、SHA-512 结合添加 SALT 随机字符串的方式，以及国产 SM4 算法；应避免直接采用 MD5 算法。）* *15、 通信双方中的一方若在至多 30 分钟内未做任何响应，另一方应能够自动结束会话，即实现用户登出处理操作;* *16、 应用系统管理员权限应分离，如业务操作员、系统管理员、安全审计员权限分离;* *17、 应用系统的输入处应进行严格的格式、长度校验，如 URL、登录输入、文本输入、文件上传等处应有数据格式、数据长度、数据类型等方面的限制;* *18、 应用系统根据业务需要设置最大并发连接数;* *应用系统与数据库连接时，应支持使用非数据库默认账户（如：sa、sys 等）*

计算中心审核	
技术内容审核意见	
系统初步定级意见	□一级　□二级　□三级
安全方案审核意见	
网信办审批	
审批意见	

附件二 《信息系统代码安全开发规范》

应用系统安全开发规范（参考）.doc

附件三 《信息系统源代码审计报告》（模板）

附件四 《信息系统安全风险评估报告》（模板）

上线前安全评估报告.docx

附件五 《信息系统备案申请表》（模板）

网站和信息系统备案申请表（空）.pd

附件六 《信息系统定级备案材料》（模板）

信息系统安全等级保护备案表.doc

XX系统安全等级保护定级报告.doc

附件七 《信息系统安全承诺书》

信息系统安全承诺书

为切实加强北京大学网络安全管理，落实信息系统安全责任制，提升信息系统安全防护能力，作为_____（网站/系统）管理员，承诺履行如下岗位安全责任：

(一) 遵守北京大学信息系统安全相关各项规章制度和操作流程；

(二) 遵照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，根据《北京大学网络安全管理办法》（试行）和《北京大学信息系统安全管理规定》承担本信息系统的安全管理责任；

(三) 落实安全技术防护策略，采用防火墙等专用安全设备，对操作系统、数据库、中间件、web 访问进行安全配置与加固；

(四) 留存系统运行日志，包括不限于操作系统日志、数据库日志、中间件访问日志、应用系统日志等。至少留存 6 个月。

(五) 落实安全监测预警，对来自网信办、计算中心等渠道的安全通报预警，及时处置；协调开发单位开展漏洞整改；定期更新漏洞补丁；

(六) 负责本系统安全事件应急处置工作：具体包括应急预案编制、安全事件应急处置实施、安全事件处置报告编制、安全整改报告编制等。

本承诺书在系统校内备案时，连同《信息系统备案申请表》一并提交计算中心。

单位名称（加盖单位公章）：

单位网信工作负责人（签字）：

网站负责人（签字）：

网站管理员（签字）：