17 信息系统开发安全管理规定

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，为规范北京大学信息系统开发、验收等环节的安全管理，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。

第三条　信息系统开发安全是指对信息系统开发、实施、验收和交付全流程进行安全管理。

第二章 自行开发

第四条　学校自行开发的项目，信息系统主管单位应结合实际要求提供系统要求，向开发实施单位提供项目的功能需求和安全需求文档，制定实施计划和安全建设方案。开发实施单位结合技术的可行性对功能需求、安全需求和安全建设方案进行确认并执行。重要信息系统的自行开发计划应经过专家审核，提交网信办和计算中心备案。

第五条　开发人员应遵守以下开发管理规定和行为准则：

(一) 开发人员应保证信息系统中不存在无用的资源（如代码、图片文件等）；

(二) 开发人员应遵循相关系统开发安全命名规范：

(三) 不允许包含后门代码、一句话木马及木马代码等；不得把代码提供给第三方；

(四) 代码的编写工作应该在独立的模拟环境完成，与实际运行环境物理分开；

(五) 对程序代码及相应的技术文档进行集中存放，并指定专人进行管理；

(六) 对程序代码及相应的技术文档进行版本控制及变更管理；

(七) 应定期做好程序代码及相应的技术文档的备份工作，以防意外引起代码和技术文档的丢失。

第六条 信息系统开发人员在设计与代码编写应遵循以下安全性要求：

(一) 应该具备独立、完整且集中的输入验证，对全部的数据输入框和 URL 进行校验，校验内容包括长度、类型、字符等；

(二) 用户界面必须要支持主流浏览器，避免因某类浏览器的安全问题或者在非 IE 浏览器下用户界面不能正常显示；

(三) 应设置默认的错误页面，对所有的异常构造统一的错误页面，包括 HTTP 错误和未经处理的异常；

(四) 使用较强的会话标识符，如使用包含至少 128 位安全随机数密码的会话标示符；

(五) 应具有日志审计模块对每个重要的行为都记录日志。如认证尝试、重要传输、重要数据更改、管理行为等。

第三章 外包开发

第七条 信息系统开发在实施外包前，信息系统主管单位应结合实际要求提供系统要求，向开发实施单位提供项目的功能需求和安全需求文档，制定实施计划和安全建设方案。实施计划应包括项目负责人、外包开发单位情况（包括实施系统建设的资质证明和能力保证）和项目开发方案、安全实施方案等内容。重要信息系统的外包实施计划和安全建设方案应该经过专家审核，提交网信办和计算中心备案。

第八条 在外包开发工作的实施过程中，信息系统主管单位指定的项目负责人应具备业务和技术能力承担相关工作，对信息系统外包开发实施过程的管理和指导。重要信息系统的外包开发应配备信息系统监理工程师。

第九条 外包开发商应遵守在遵循第四条和第五条开发管理规范的基础上，按照以下要求开展系统开发：

(一) 在开发实施前，应该提供详细的开发实施方案，以便于控制开发实施过程；

(二) 在开发过程中阶段性提交开发成果，保证项目负责人对信息系统质量和工作进度进行监督控制；

(三) 信息系统开发完成后需配合完成信息系统质量检测，保证信息系统功能、性能和安全符合要求；

第四章 实施

第十条　信息系统主管单位应对开发实施进行监督，进行进度和质量控制，形成的阶段性工程报告等文档。

第十一条 开发实施过程的安全管理主要由实施单位负责，信息系统主管单位可以督促检查，对于存在网络安全风险的现象须协助及时处理。

第十二条 项目负责人应进行阶段性工程质量安全检查，以便发现问题及时解决。质量检查内容应参照以下标准：

(一)　国家颁布的信息系统开发实施规范、技术操作规程、技术标准、质量检验评定标准；

(二)　信息系统需求说明、设计变更通知单、技术核定单、会审纪要、会议决定等；

(三)　合同中的细节要求。

第五章 验收

第十三条 在验收前，信息系统开发方应对系统进行安全性测试，形成详细安全报告，包括恶意代码检测结果、系统后门检测结果及安全漏洞检测结果等；重要信息系统建设中还要对源代码进行审核。

第十四条 在验收前，信息系统开发方应对信息系统使用操作人员进行培训，以保证使用人员能独立操作和使用。

第十五条 信息系统主管单位应对验收过程中的文档记录进行整理，编写验收报告，明确验收结论。验收报告中须包括系统的安全性测试，明确是否达到合同要求的安全性设计要求，明确所达到的国家网络安全等级保护标准的级别。重要的信息系统，应有第三

方测试机构对信息系统进行独立的安全性测试。未达到合同要求的安全性设计要求，不能通过验收。

第十六条 对未通过验收的项目必须按要求限期改正，符合验收条件后，可再次提出验收申请，直至重新验收合格后方可投入运行。对造成重大经济损失和责任事故的有关人员将依照国家有关法律法规追究责任。

第六章 交付

第十七条 验收通过后，负责人负责系统交接工作，系统交付前应完成的文档包括：

(一) 系统交付清单：根据合同完成，包括需要交接的设备、文档、软件等；

(二) 系统培训文档：包括培训手册、培训记录等；

(三) 系统建设文档：包括信息系统建设的详细步骤、注意事项和配置参数，以及建设过程中出现问题的解决方法；

(四) 系统运维手册，含安全运维方案。

第十八条 验收负责人根据系统交付清单对所交接的物品进行清点并签收。

第七章 附则

第十九条 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）。

第二十条 其他校区参考本规定制定相应管理规定

第二十一条　本规定由北京大学网络安全和信息化委员会办公室及北京大学计算中心负责解释。

第二十二条　本规定自发布之日起施行。