北京大学网站和信息系统

网络安全风险预警和处置规程

第一条　为保障北京大学网站和信息系统安全、稳定运行，规范网络安全风险预警和处置流程，依据《北京大学网络安全管理办法》，制定本规程。

第二条　本规程所指的网络安全风险，包括但不限于网站、信息系统及其相关组件（操作系统、数据库、中间件、第三方组件）可能存在的漏洞、后门、暗链等。

第三条　本规程适用于北京大学校本部各单位，其他校区可参考本规程制定相应管理规定。

第四条　网络安全和信息化委员会办公室（以下简称“网信办”）、计算中心为网站和信息系统网络安全风险预警和处置协调责任部门，负责统筹预警信息发布、处置协调、信息报送及监督检查。网信办、计算中心通过邮件发送《北京大学网站和信息系统网络安全风险限期整改通知书》，并采用通讯手段确认的方式与各单位进行预警信息的处置的协调。

第五条　按照“谁主管谁负责、谁使用谁负责”的原则，各单位负责本单位网站和系统网络安全风险的具体处置，各单位网信工作主管领导、安全管理员、信息系统管理员有责任根据网信办、计算中心发布的预警信息，及时进行处置，

并在预警下达确认三天内反馈处置结果。

第六条　各单位应提高网络安全风险防范意识，根据《北京大学网络安全管理办法》附属《漏洞和安全预警管理规定》，及时采取补丁升级、系统环境配置更改、安全防护策略配置等策略，降低各种风险被利用的可能性。

第七条　学校对网络安全风险处置有困难的单位提供相应的技术支持和建议。对于无合理理由拖延、拒不配合处置和整改的单位，学校将采取约谈单位主管领导、校内通报批评、停止提供网络服务等形式进行处理。对因履责不力造成网络安全事件的单位和相应责任人，学校将参照《北京大学网络安全管理办法》进行相应处置，并依据相关校规校纪进行严肃处理。

第八条　本规程由网信办、计算中心负责解释。

附件 1:《北京大学网站和信息系统网络安全风险限期整改通知书》

附件 2:《北京大学网站和信息系统限制校外访问通知书》

附件 1：

北京大学网站和信息系统网络安全风险限期整改通知书

XXXX：

学校监测到你单位网站或信息系统存在漏洞（详见附件）。根据《北京大学网络安全管理办法》的有关规定，请你单位立即对漏洞进行核实、处置，并在 3 天内反馈整改情况。在整改完成之前，你单位应采取必要的管理和技术措施，防止信息安全事件发生。

对于未按期限反馈整改情况的，学校将依据《北京大学网络安全管理办法》《北京大学网站和信息系统网络安全风险预警和处置规程》进行必要处理。

联系邮箱：security@pku.edu.cn

北京大学网络安全工作组

年　　月　　日

附件 2：

北京大学网站和信息系统

限制校外访问通知书

XXXX：

学校监测到你单位网站或信息系统存在漏洞，并于_____下达了整改通知书。由于你单位未按期完成整改并报送，学校将依据《北京大学网络安全管理办法》和《北京大学网站和信息系统网络安全风险预警和处置规程》的规定，限制该网站或信息系统的校外访问权限。

联系邮箱：security@pku.edu.cn

北京大学网络安全工作组

年　　月　　日