北京大学网络安全和信息化委员会办公室文件

网信〔2023〕2号

北京大学网络安全监测预警通报工作规程

第一条 为了切实加强网络安全保障工作，规范学校网络安全监测预警通报工作，依据《北京大学网络安全管理办法》，结合工作实际，制定本规程。

第二条 网络安全监测预警通报工作应遵循“及时发现、科学认定、有效处置”的原则，通过建立监测预警和信息通报机制，对风险进行预警，做到“早发现、早报告、早处置”。

第三条 本规程所指的网络安全风险，涵盖各种形式的信息技术安全威胁，包括但不限于：网站和信息系统的安全漏洞、未经授权的后门程序、隐藏的网站链接、恶意软件以及各种形式的数据泄露等。

第四条 网络安全和信息化委员会办公室（以下简称“网信办”）、计算中心为学校网络安全监测预警通报工作的统筹管理部门，负责监测预警通报信息发布、信息报送及监督检查。

第五条 各二级单位为网络安全监测预警通报工作的协调处置责任部门，明确专人负责预警信息通报联络，开展监测预警通报的协调处置和信息反馈工作。

第六条 各网站和信息系统管理员、移动互联网应用系统管

理员、主机用户等为网络安全风险处置的责任人，有责任根据监测预警通报信息进行风险处置。

第七条 按照上级部门工作要求，计算中心部署网络安全检测系统，对学校各级信息系统和网络环境进行主动探测和动态监测，对发现的风险问题进行评估，并根据风险程度进行通报，同时组织针对性的风险应对措施。

第八条 根据实际工作需求，计算中心不定期组织开展人工网络安全风险评估和检测，对检测到的异常和风险情况，根据严重性评定进行通报，并启动必要的风险控制措施。

第九条 各二级单位按照“谁主管谁负责，谁运维谁负责，谁使用谁负责”的原则，对本单位网站和信息系统、移动互联网应用系统、本单位用户使用的主机开展日常安全检测：

1. 实时监测信息系统和网站，及时发现并记录任何异常活动或入侵企图；
2. 实施严格的账号密码管理政策，定期检查并消除弱密码，确保关键系统的管理账户密码定期更改，并尽量推进使用多因素认证；
3. 建立并执行定期数据备份计划，对重要数据进行加密和安全存储；
4. 确保服务器定期接受系统补丁更新，进行安全配置审核，以及实施适当的安全防护措施；
5. 在服务器和主机上安装经认证的反病毒软件，并保持病

毒定义文件的最新状态，定期进行全面扫描。

第十条 各二级单位自行检测到的网络安全风险存在安全隐患或发生安全事件时，应及时向学校报告，避免事态扩大。

第十一条 网络安全预警信息来源涵盖多个方面，包括但不限于学校自主监测发现、上级部门通报、第三方安全机构的警报，以及其他可靠的安全情报渠道。

第十二条 预警信息包括发现风险来源、风险描述、风险时间、涉及 IP 或域名、处置建议等。

第十三条 学校通过北京大学网络安全综合管理平台（http://sec.pku.edu.cn）发布网络安全风险预警信息，同时发送预警电子邮件通报相关单位和负责人。

第十四条 各二级单位接到预警通报信息后，须及时动员指定的安全负责人或团队，遵循既定流程迅速采取必要措施，如切断受威胁系统的网络连接、隔离风险区域等，以降低风险影响，控制风险发展。同时，应确保整改措施的彻底执行，并对整改结果进行记录和报告。

第十五条 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。

第十六条 处置完成后，各二级单位根据处置情况撰写信息反馈报告，通过网络安全综合管理平台回复整改情况，提交报告。

第十七条 计算中心确认问题已解决后，在网络安全综合管理平台解除预警状态。

第十八条 各二级单位对预警通报情况进行事后分析，总结经验教训，完善网络安全管理措施，提高网络安全保障水平。

第十九条 各二级单位应加强师生网络安全意识和防护技能培训，提高师生对风险情况的敏感度和处理能力，提升监测预警风险整改效率。

第二十条 本规程由网信办、计算中心负责解释。