**关于加强校园网信息安全管理和检查的通知**

**校内各单位、现代学院：**

网络安全是国家安全的重要组成部分。随着网络安全法规、制度的实施，学校及各单位工作机制基本建立，防护能力不断加强，校园网用户的网络信息安全意识显著提高。但是，校园网内信息系统较多、情况复杂，网络安全仍存在许多问题。主要有：岗位变动导致安全责任不明确、信息安全管理不规范、安全隐患检查不彻底、安全漏洞修复不到位、监测预警和应急响应能力不足，致使网络安全事件有时发生。这些问题不仅给学校声誉造成不良影响，同时危害到师生用户切身利益。为全面贯彻上级管理部门关于网络安全的文件精神，落实《网络安全法》，迎接党的十九大胜利召开，各单位要进一步加强本单位的网络与信息安全管理和检查，具体要求如下：

**1、落实网络与信息安全责任，理顺管理机制。**

根据《西北大学校园网络信息安全管理规定》，校内各单位党政一把手是本单位网络信息安全主要责任人，全面负责本单位所属网站、服务器和应用系统的信息安全工作。同时各单位要设置网络信息安全管理岗位，配备信息安全管理人员，履行相关职责。

各单位要制定网络信息安全应急预案，落实发现预警、封堵清除、系统恢复等关键行动的处置岗位、人员和措施，提升网络信息安全水平，增强系统防护能力，有效防范和抵御安全风险，切实保障信息系统和网站稳定运行和数据安全。

**2、开展网络信息安全检查，积极消除安全隐患。**

根据校内外的监控与通报，我校已经收到涉及网页暗链、页面篡改、弱密码、SQL注入和目录遍历漏洞、病毒攻击、外网嗅探攻击等多种信息安全问题的警告，表明我校校园网络信息安全形势依然严峻。各单位要积极联系开发、部署本单位网站、应用系统和服务器的企业，对本单位所属网站、服务器和应用系统进行梳理，重点排查僵尸网站、应用系统安全漏洞、操作系统安全补丁，以及邮件、公告板等账号弱密码等问题，发现问题要立即予以处理。

学校近期将委托专业网络安全厂商在近期对校内的网站和信息系统进行漏洞扫描，发现的问题会及时通报各单位，届时请各单位高度重视，积极配合整改。

**3、积极开展《网络安全法》宣传与教育。**

各单位要积极向师生员工开展《网络安全法》的普法宣传教育，提高网络信息安全意识，保护隐私数据，防范网络诈骗、钓鱼网站等违法犯罪；高度重视网络实名制对个人权利保护的重要意义，倡导各类账号专人专用，增强账号密码强度，保护自身权益；个人用户应及时安装系统漏洞补丁和安全保护软件，避免点击各种来历不明或者存在安全隐患的网络联接，主动远离各种黑客工具和行为。

**4、重视信息系统的安全建设，主动开展重要信息系统等级保护定级及测评、整改工作。**

各单位在新建或升级信息系统时，要高度重视信息安全问题，在项目需求分析、立项、建设实施、验收移交和后期维护各个环节均要充分考虑信息安全问题，督促合同乙方有效解决并进行安全测试。各单位信息系统服务器原则上部署在学校数据中心机房，由学校提供统一的供电、防火、防盗等物理安全防护，各单位二级网站原则上统一部署在学校站群系统上，请需要技术协助的单位积极与现代教育技术中心联系。

要重点落实国家法定的重要信息系统等级保护制度，完成信息安全管理部门的检查任务，以此促进各单位完善和优化网络信息安全工作。所有涉及学校重要数据、涉及全校师生切身利益的信息系统都必须依据等级保护的相关要求开展等保工作，已定级的系统主管部门要积极开展等级评测，并根据评测结果进行整改。

请校内各单位根据上述要求开展网络信息安全自查工作，并于6月23日前将检查简报及信息安全责任人及手机联系方式、信息员及手机、QQ等联系方式保送信息化建设领导小组办公室（现代教育技术中心）。

信息化建设领导小组办公室

现代教育技术中心

2017年5月27日