西北农林科技大学文件

校信息化发〔2026〕53 号

关于印发《西北农林科技大学网络安全事件应急预案》的通知

各单位：

《西北农林科技大学网络安全事件应急预案》已经 2026 年 3 月 17 日校长办公会议审议通过，现予以印发，请遵照执行。

西北农林科技大学

2026 年 3 月 24 日

西北农林科技大学网络安全事件应急预案

第一章 总　则

第一条 为健全完善学校网络安全事件应急工作机制，规范网络安全事件工作流程，提高学校网络安全应急处置能力，预防和减少网络安全事件造成的损失和危害，维护学校安全稳定，特制定本预案。

第二条 本预案根据《中华人民共和国网络安全法》《教育系统网络安全事件应急预案》《信息技术安全事件报告与处置流程》《信息安全技术 网络安全事件分类分级指南》等法律法规及相关文件，结合学校实际情况制定。

第二章 网络安全事件的分类分级

第三条 本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对学校网络、信息系统（网站）或其中的数据造成危害，对学校或社会造成负面影响的事件，可分为恶意程序事件、网络攻击事件、数据安全事件、设备设施故障事件、违规操作事件、异常行为事件、不可抗力事件和其他事件。信息内容安全事件的应对，参照有关规定和办法。

第四条 根据可能造成的危害，学校网络安全事件可分为三级：重大网络安全事件（Ⅰ级）、较大网络安全事件（Ⅱ级）、一般网络安全事件（Ⅲ级）。

1.符合下列情形之一的，为重大网络安全事件（Ⅰ级）：

（1）全校范围大量用户无法正常上网。

（2）重要信息系统（网站）遭受严重损失，丧失业务处理能力。

（3）重要信息系统（网站）的敏感个人信息或重要数据丢失或被窃取、篡改。

（4）学校官网、公共电子屏、广播台内容遭恶意篡改，造成严重影响。

（5）网络病毒在校园网广泛传播，造成严重影响。

2.符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件（Ⅱ级）：

（1）学校部分区域大量用户无法正常上网。

（2）重要信息系统（网站）遭受较大损失，业务处理能力大幅下降。

（3）重要信息系统（网站）的数据丢失或被窃取、篡改。

（4）学校官网、公共电子屏、广播台内容遭篡改，造成较大影响。

（5）网络病毒在校园网多个子网内传播，造成较大影响。

3.一般网络安全事件（Ⅲ级）：

除上述情形外，对学校安全稳定和正常秩序构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

第三章 组织机构与职责

第五条 学校网络安全和信息化领导小组（以下简称网信领

导小组）统筹协调网络安全整体工作，网信领导小组办公室指导、监督、统筹具体工作，指挥网络安全事件的应急处置。

第六条 根据“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，各单位主要负责人是本单位网络安全工作第一责任人，各单位网信工作分管负责人是本单位网络安全工作直接责任人。各相关单位积极配合，共同做好网络安全事件的预防和处置工作。

第七条 信息化管理处负责网络安全事件的初步处置，研判事件类型和等级，提供事件应急响应的技术支持，负责预案的演练及修订。事发单位协助完成初步处置，负责网络安全事件的整改处置、编写报告等工作。党委宣传部负责网络安全事件的舆情监测工作。

第四章 应急处置

第八条 初步处置

网络安全事件发生后，事发单位应立即报信息化管理处。涉及公共电子屏、广播台的，管理员应第一时间关闭电源、切断网络。

信息化管理处启动应急预案，组织相关人员紧急判断网络安全事件的类型和等级，采取相应的应急措施，将损害和影响降到最小范围：

1.初步认定为恶意程序、网络攻击、数据安全事件的，应立即停止涉事信息系统（网站）的所有网络服务，并保存网络病毒、

网络入侵等证据。

2.初步认定为设备设施故障、违规操作、异常行为、不可抗力事件的，应立即联系相关人员进行处理。

第九条 应急响应

网络安全事件应急响应分为Ⅰ级、Ⅱ级、Ⅲ级等三级，分别对应重大、较大和一般网络安全事件。信息化管理处在网信领导小组的指挥下成立应急工作组，开展应急响应工作。

1. Ⅰ级、Ⅱ级响应

应急工作组进入应急状态，工作组成员保持 24 小时联络畅通，Ⅰ级响应应安排相关人员24小时值守。

信息化管理处进一步详细分析事件原因，保留相关证据，涉及人为主观破坏的网络安全事件及时报杨凌示范区公安局，配合开展调查取证工作，涉及在校师生的，由相关单位依据学校规定进行处理。事发单位应排查、整改涉事信息系统（网站）的安全隐患，及时恢复。信息化管理处采取适当技术措施、管控手段，最大限度阻止和控制事态蔓延。党委宣传部做好舆情监测工作。

2. Ⅲ级响应

应急工作组进入应急状态，工作组成员保持 24 小时联络畅通。

信息化管理处协助事发单位做好事件原因分析、证据保留、全面安全排查等工作。事发单位应及时开展隐患排查整改、信息系统（网站）或数据恢复等工作。

第十条 响应结束

网络安全事件整改完毕后，事发单位报应急工作组，工作组批准后，解除响应状态。

事发单位及时编写《网络安全事件整改报告》，报送信息化管理处。信息化管理处审核通过后，恢复涉事信息系统（网站）的网络服务。

第五章 预防工作

第十一条 各单位应做好主管信息系统（网站）的风险评估、安全漏洞修复和数据备份等网络安全事件日常预防工作，提高信息系统（网站）的网络安全防范能力。

第十二条 信息化管理处应建立网络安全监测和通报处置工作机制，提高发现和应对网络安全事件的能力。信息化管理处负责定期对信息系统（网站）进行安全隐患排查、安全漏洞扫描、网络攻击分析，及时发现并指导督促各单位消除网络安全威胁。各单位应及时完成修复、加固工作。

第十三条 信息化管理处每年至少组织开展一次网络安全应急演练，提高实战能力，各相关单位应积极配合。

第十四条 信息化管理处定期组织网络安全培训，将网络安全法规政策、基本知识和技能、事件应急预案列为培训内容，提高师生网络安全意识及防护技能。

第十五条 各单位网络安全第一责任人、直接责任人、信息系统（网站）管理员发生变更的，应及时将变更情况报信息化管

理处。

第六章 附则

第十六条 各单位应按本预案及时、如实报告，妥善处置网络安全事件。

第十七条 本预案由信息化管理处负责解释。

第十八条 本预案自印发之日起实施，原《西北农林科技大学网络安全事件应急预案》（校办发〔2020〕25号）同时废止。

附件：网络安全事件整改报告

附件

网络安全事件整改报告

单位名称（加盖公章）：

联系人姓名		手机	
		电子邮箱	
事件分类	☐恶意程序事件　☐网络攻击事件 ☐数据安全事件　☐设备设施故障事件 ☐违规操作事件　☐异常行为事件 ☐不可抗力事件　☐其他事件		
事件分级	☐I 级　☐II 级　☐III 级		
事发时间	年　月　日　时　分		
事件概况			
信息系统（网站）基本情况（如涉及请填写）	1.系统名称： 2.系统 url 和 IP 地址： 3.系统主管单位： 4.系统运维单位： 5.系统主要用途：		

事件发生的最终判定原因（可加页附文字、图片及其他说明）	
事件的影响及恢复情况	
事件的安全整改措施	
存在问题及建议	
单位网络安全第一责任人意见（签字）	

抄送：校领导。

西北农林科技大学校长办公室　　2026 年 3 月 25 日印发