四 川 农 业 大 学

信息与教育技术中心文件

信教发〔2022〕 5 号

四川农业大学网络安全监测预警通报制度

（试行）

为规范四川农业大学网络安全管理工作，提高网络安全事件监测、预警、通报和应急响应水平，结合当前实际情况，制定本制度。

第一章 责任分工

第一条 信息与教育技术中心对学校信息系统运行情况进行常态化监测，组织定期对学校信息系统进行安全扫描，将所发现问题通报相关单位。

第二条 信息与教育技术中心负责接收上级有关单位下发的网络安全漏洞、隐患、事件通报，通报相关单位，协助完成整改并上报整改结果。

第三条 各信息系统责任单位在通报规定期限内实施信息系统漏洞、隐患整改，并撰写整改报告。

第四条 各信息系统责任单位应指定专人负责不定时对信息系统（网站）的运行情况进行检查，做到安全事件早发现、早报告、早控制、早解决。

第二章 通报处置程序

第五条 信息与教育技术中心接到上级有关部门安全事件通报或自主发现各单位信息系统发生安全事件后，第一时间以口头方式将相关情况通报给相关单位网络安全员。相关单位接到通知后，应立即组织技术人员进行紧急处置。随后信息与教育技术中心以书面形式，将安全事件详情、要求整改内容及时限通报给相关单位。

第六条 相关单位主管领导、信息与教育技术中心根据发生安全事件的信息系统重要程度、损失情况以及对学校工作和社会秩序造成的影响判定安全事件等级，安全事件划分为四个等级:

特别重大网络安全事件（I 级）：学校校园网与多个核心业务系统发生全校性大规模瘫痪、信息系统被黑客入侵篡改造成非常严重的影响（例如被敌对黑客组织篡改内容并被其网站发布）、学校核心业务数据丢失、泄露、被篡改，对学校正常工作造成特别严重损害，且事态发展超出学校控制能力的安全事件;

重大网络安全事件（II 级）：学院校园网与多个核心业务系统发生全校性瘫痪、信息系统（网站）被黑客入侵篡改

损害学校形象、大量师生个人信息泄露、重要部门业务数据丢失、泄露、被篡改，对学校正常工作造成严重损害，需学校多个部门协同处置，事态发展未超出学校控制能力的安全事件;

较大网络安全事件（Ⅲ级）：学校某区域校园网络、部门重要业务系统瘫痪、部门业务数据丢失、泄露、被篡改，对学校正常工作造成一定损害，有关部门和信息化中心配合可以解决的安全事件;

一般网络安全事件（Ⅳ级）：上述情形以外，发生在个别学院、部门，无扩散性，损害轻微，依靠二级单位自身力量可以解决的安全事件。

对特别重大事件和重大事件，应及时上报学校网络安全和信息化领导小组，对涉及人为故意破坏的事件应同时报告公安机关。

第七条 安全事件处置过程中要及时掌握损失情况，查找和分析事件原因，修复系统漏洞，恢复系统服务，尽可能减少安全事件对正常工作带来的影响。如果涉及人为故意破坏应积极配合公安机关开展调查。

第八条 网络安全事件整改报告应在通报规定时限内以书面形式报送信息与教育技术中心，上级有关单位没有明确时限的，一般应在事件处置完毕后 3 个工作日内报送。信息与教育技术中心及时将整改报告上报上级有关单位。

第九条 网络安全事件相关责任单位应进一步总结事件教训，研判安全现状、排查安全隐患，加强制度建设、安全设施建设，全面提升安全防护能力。

第三章 通报与整改报告内容

第十条 网络安全事件通报应包含上级有关单位安全通报主要内容、漏洞详情、整改建议、整改时限与其他应当知晓的情况。

第十一条 网络安全事件整改报告应包含通报基本情况描述、针对通报漏洞所采取的整改措施与其他应当报告的情况。

第四章 附 则

第十二条 本制度自发布之日起施行，由信息与教育技术中心负责解释和修订。

信息与教育技术中心

2022 年 4 月 22 日