党发〔2022〕34号

沧州师范学院

信息系统技术安全漏洞整改流程

第一条 为加强我校信息系统技术安全保障能力，规范信息系统技术安全漏洞整改流程，降低网络安全风险，维护正常工作秩序和营造健康的网络环境，根据《中华人民共和国网络安全法》和教育部有关网络安全的文件精神，结合学校实际情况，制定本流程。

第二条 信息系统技术安全漏洞的定义。 根据《信息安全技术安全漏洞等级划分指南》((GB/T30279-2013),以下简称《指南》，摘录部分见附件一)，本流程中所称的信息系统技术安全漏洞(以下简称信息安全漏洞)是指计算机信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷。这些缺陷以不同形式存在于计算机信息系统的各个层次和环节之中，一旦被恶意主体所利用，会对计算机信息系统的安全造成损害，从而影响计算机信息系统的正常运行。

第三条 适用范围。本流程适用于我校各类网站、信息系统(包含承载其运行的服务器操作系统、中间件软件和数据库管理系统等)以及网络交换机、网络路由器、网络打印

机、办公及教学用计算机、服务器等其他计算机信息系统(以下均统称为信息系统)信息安全漏洞的发现、处置与整改。

第四条 责任体系。根据《中华人民共和国网络安全法》第二十五条要求，网络运营者应当及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。

现代教育技术中心负责学校各类信息安全漏洞的通知、应急处置、整改督促和学校核心数据中心内的虚拟服务器的操作系统、中间件系统和数据库系统级别信息安全漏洞技术处置，负责学校网站群平台的操作系统及平台级信息安全漏洞的处置，校内其他各系统信息安全漏洞的扫描和技术支持。

学校各单位负责本单位所管理的各类信息系统的信息安全漏洞自查、堵塞整改、复查复测和处置情况报告等。

第五条 信息安全漏洞等级划分。根据《指南》，信息安全漏洞等级划分要素包括访问路径、利用复杂度和影响程度三方面。根据危害程度从低至高，将信息安全漏洞划分为四个等级，依次为低危、中危、高危和超危。

相关机构或相关安全软件有明确定义安全等级的漏洞按照其标准确定等级;没有明确级别的，现代教育技术中心负责对信息安全漏洞的危险等级进行评估，确定漏洞的危害等级。对不同等级的信息安全漏洞，将采取不同的处置措施。

第六条 信息安全漏洞发现。学校信息安全漏洞主要包含：①上级有关部门或其他机构通报的信息安全漏洞；②

学校通过网络安全扫描发现的信息安全漏洞；③信息系统管理员自己发现的信息安全漏洞。

第七条 高危与超危信息安全漏洞的处置。对于高危与超危信息安全漏洞，现代教育技术中心应立刻采取断网措施，根据信息系统的登记备案信息，向信息系统责任单位发出《信息安全漏洞整改通知》(以下简称整改通知)，限定24小时内完成整改，五个工作日内向现代教育技术中心提交《沧州师范学院信息系统漏洞整改报告》。

第八条 中危与低危信息安全漏洞的处置。对于中危和低危信息安全漏洞，现代教育技术中心发送整改通知单告知责任单位进行整改，限定二个工作日内完成整改。单位整改完成后直接回复现代教育技术中心要求重新扫描，现代教育技术中心对整改结果进行检查，确认单位是否已完成整改。对于未按期完成整改的单位，采取断网措施，同时向责任单位发出整改通知。

第九条 信息安全漏洞整改。信息系统责任单位收到整改通知后，可根据实际情况直接整改，或指定信息系统负责人完成整改。整改完成后，填写《沧州师范学院信息系统漏洞整改报告》(以下简称整改报告)。整改报告的主要内容包括:信息系统基本信息、漏洞说明、整改情况说明、整改结果及单位审核，具体内容和格式见附件二。整改报告由本单位主要负责人审核，签字并加盖公章后报送信息化管理部门。

第十条 整改落实机制。各单位收到整改通知后，要认真做好整改工作，坚持做到查清信息安全漏洞原因、按时整改，尽力杜绝类似信息安全漏洞再次发生。

第十一条 整改结果验证。责任单位提交整改报告后，现代教育技术中心对信息系统进行整改结果检测，确认整改完成后才能开放网络连接。

第十二条 人事变更报告。为保障联络通畅，各单位分管信息化建设负责人、信息系统管理员,联络方式等发生变更的，应及时向现代教育技术中心报备。

第十三条 责任追究。各单位应按照流程及时地完成信息安全漏洞整改。如有接到整改通知后不整改或整改不力等情况的，网络安全和信息化工作领导小组将进行通报，情节严重的将问责处理。

第十四条 本流程自发布之日起施行，由网络安全和信息化工作领导小组负责解释。

附件一：信息系统技术安全漏洞等级划分指南

附件二：信息安全漏洞整改报告

附件一

信息安全技术安全漏洞等级划分指南

《信息安全技术安全漏洞等级划分指南》(GB/T30279-2013)信息系统安全漏洞(简称安全漏洞)的等级划分要素和危害程度级别。

一、安全漏洞等级划分要素

安全漏洞等级划分要素包括访问路径、利用复杂度和影响程度三方面。访问路径的赋值包括本地、邻接和远程，通常可被远程利用的安全漏洞危害程度高于可被邻接利用的安全漏洞，可本地利用的安全漏洞次之。

利用复杂度的赋值包括简单和复杂，通常利用复杂度为简单的安全漏洞危害程度高。

影响程度的赋值包括完全、部分、轻微和无，通常影响程度为完全的安全漏洞危害程度高于影响程度为部分的安全漏洞，影响程度为轻微的安全漏洞次之，影响程度为无的安全漏洞可被忽略。影响程度的赋值由安全漏洞对目标的保密性、完整性和可用性三个方面的影响共同导出。

二、安全漏洞等级划分要素

安全漏洞的危害程度从低至高依次为低危、中危、高危和超危，具体危害等级划分方法见表一 。

安全漏洞危害等级划分表

序号	访问路径	利用复杂度	影响程度	安全漏洞等级
1	远程	简单	完全	超危
2	远程	简单	部分	高危
3	远程	复杂	完全	高危
5	邻接	简单	完全	高危
6	本地	简单	完全	高危
7	远程	简单	轻微	中危
8	远程	复杂	部分	中危
9	邻接	简单	部分	中危
10	本地	简单	部分	中危
11	本地	复杂	完全	中危
12	远程	复杂	轻微	低危
13	邻接	简单	轻微	低危
14	邻接	复杂	部分	低危
15	邻接	复杂	轻微	低危
16	本地	简单	轻微	低危
17	本地	复杂	部分	低危
18	本地	复杂	轻微	低危

附件二

沧州师范学院信息系统漏洞整改报告

单位名称		整改通知编号	
网站/系统名称		域名	
IP 地址			
漏洞说明			
整改情况说明			
整改结果	☐整改完成　　☐部分整改完成　　☐未完成		
备注	如未完全整改或有其他说明，请在此备注。		
单位审核	单位主要负责人（签字）： 日期：　　（单位公章）		