漯河市第三初级中学文件

漯三中〔2022〕18号

漯河市第三初级中学网络应急安全预案及流程

一、预防措施

1、加强领导，健全组织，强化工作职责，完善各项应急预案的制定和各项措施的落实。

2、充分利用各种果道进行网络安全知识的宣传教育，组织、指导全校网安全常识的普及教育，广泛开展网络安全和有关技能训练，不断提高广大师生的防范意识和基本技能。

3、认真搞好各项物资保障，严格按照预案要求积极配备网各安全设施设备，落实线路、交换设备、网络安全设备等物资，强化管理，使之保持良好工作状态。

4、采取一切必要手段，组织各方面力量全面进行网络各安全事故理工作，把不良影响与损失到最低点。

5、调动一切积极因素，全面保证和促进学校网各安全稳定地运行。

二、现场处置及救援措施

1、发现出现网络恶意攻击，立刻确定该攻击来自校内还是校外；受攻击的设备有哪些；影响范国有多大。并迅速推断出此次攻击的最坏结果，判断是否需要紧急切断校园网络的服务器及公网的同连接，以保护重要数据及信息。

2、如果攻击来自校外，立刻从防火墙中查出对方 IP 地址并过滤，同时对防火墙设置对此攻击的过滤，并视情况严重程度决定是否报警。

3、如果攻击来自校内，立刻确定攻击源，查出该攻击出自哪台交换机，出自哪台电脑，出自哪位教师或学生。接看立刻赶到现场，关闭该计算机网连接，并立刻对该计算机进行分析处理，确定攻击出于无意、有意还是被利用。暂时扣留该电脑。

4、重新启动该电脑所连接的网络设备，直至完全恢复网络通信。

5、对该电脑进行分析，清除所有病毒、恶意程序、木马程以及垃圾文件，测试运行该电 5 小时以上，并同时进行监控，无问

题后归还该电脑。

6、从事故一发生到处理事件的整个过程，必须保持向领导小组组长汇报、解释此次事故的发生情况、发生原因、处理过程。

三、事故报告及现场保护

1、确保 WEB 网站信息安全为首要任务：关闭 WEB 服务器的外网连接、学校公网连接。迅速发出紧急警报。所有相关成员集中进行事故分析，确定处理方案。

2、分析网络，确定事故源：使用各种网络管理工具，迅速确定事故源，按相关程序进行处理。

3、事故源处理完成后，逐步恢复网络运行，监控事故源是否仍然存在。

4、针对此次事故，进一步确定相关安全措施、总结经验，加强防范。

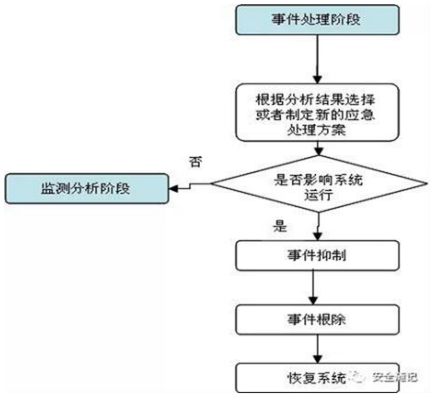
5、从事故一发生到处理的整个过程，必须及时向领导小组组长以及教务处以及校长汇报，听从安排，主意做好保密工作。

四、事故调查及处理

1、在应急行动中，各部门要密切配合，服从指挥，确保政令畅通和各项工作的落实。

2、事后迅速查清事件发生原因，查明责任人，并报领导小组根据责任情况进行处理。

五、处置流程



漯河市第三初级中学

2022 年 4 月