网络与信息安全应急预案

为加强我校信息技术安全工作，及时掌握和处置信息技术安全事件，降低安全事件带来的损失与影响，有效预防并科学应对网络信息安全突发事件，确保校园网络与信息系统正常运行，根据国家有关法律法规和标准规范，参照教育部有关规定，制定本流程。

**第一条** 信息技术安全事件定义。根据《中华人民共和国计算机信息系统安全保护条例》、《信息安全事件分类分级指南》（GB/T20986-2007，以下简称《指南》），本流程中所称的信息技术安全事件（以下简称安全事件）是指除信息内容安全事件以外的有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件。如校园信息化基础设施、应用系统、网站、信息化数据等因各种因素遭到破坏，对学校工作、学习、生活秩序造成负面影响的事件。

**第二条** 适用范围。本流程适用于我校信息技术安全事件的报告与处置工作，涉及信息内容安全事件的报告与处置工作仍按相关规定执行。应急处置遵循“统一领导，预防为本,快速反应，科学处置”的原则，最大可能的降低危害和影响。

**第三条** 网络信息安全事件依据发生过程、性质和特征不同，可分为以下四类：

**（一）网络攻击事件：**由于遭受有害程序感染、非法入侵或其他技术手段攻击，造成校园网络和信息系统运行异常或存在潜在危险，或造成信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。

**（二）设备故障事件：**由于信息系统或外围软硬件设施故障、人为误操作等，造成信息系统破坏、业务中断、系统宕机、网络瘫痪等导致的信息安全事件。

**（三）灾害性事件：**因洪水、火灾、雷击、地震、台风、非正常停电等外力因素造成网络与信息系统损毁，导致业务中断、系统宕机、网络瘫痪等安全事件。

**（四）信息内容安全事件：**利用校园网络在校内外传播法律法规禁止的信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

**第四条** 网络信息安全事件按照可控性、严重程度和影响范围不同,可划分为四级：

**（一）Ⅰ级（特别重大）：**事件导致发生全校性大规模瘫痪，或由于网站非法信息引发学校大规模群体性事件，对学校正常工作造成特别严重损害，事态发展超出学校控制能力。

**（二）Ⅱ级（重大）：**事件导致校园网发生全校性瘫痪，或由于网站非法信息引发师生反应强烈并有过激行为，对学校正常工作造成严重损害，事态发展超出学校网络安全和信息化领导小组控制能力，需要跨单位协同处置。

**（三）Ⅲ级（较大）：**事件导致校园网某一区域的重要网络与信息应用系统瘫痪，或由于网站敏感信息、谣言等，对学校正常工作造成一定损害，学校网络安全和信息化领导小组可以自行处理。

**（四）Ⅳ级（一般）：**事件导致某一局部网络或信息应用系统受到一定程度损坏，学校工作受到一定影响，但不危害学校整体工作，学校网络安全和信息化领导小组办公室（以下简称网信办）可以自行处理。

**第五条** 安全事件自主判定。一旦发生安全事件，各部门应根据《指南》，视信息系统重要程度、损失情况以及对工作和社会造成的影响，自主判定安全事件等级。

**第六条** 学校网络安全和信息化领导小组为网络信息安全事件应急处理领导机构，网络安全和信息化领导小组办公室（设在信息中心）负责具体处置工作。其职责包括：

（一）负责网络信息安全工作的组织、协调和监督，制定相关制度和应急预案；

（二）根据网络信息安全事件严重程度启动相应级别的预案，组织协调成员部门落实应急预案，共同做好处置工作；

（三）负责及时收集、通报和上报网络信息安全事件处置的有关情况；

（四）对全校各部门贯彻执行预案以及在事件处置工作中履行职责情况进行检查督办。

**第七条  相关部门职责包括：**

**（一）党委办公室、学校办公室：**牵头组织重大敏感时期、重要活动、重要会议期间发生的信息安全事件的协调处置；负责涉密级信息网络泄密类事件的处理。

**（二）信息中心：**负责校园基础网络系统安全，保证校园网络服务不中断；负责网络攻击、设备故障类事件的处置；负责全校网络信息安全事件处置的技术支持工作。

**（三）宣传部：**负责学校舆情监测和信息内容安全类事件的处置，对于涉及师生政治思想方面的预警性、倾向性、苗头性的问题，要加强分析研判，妥善有效应对。

**（四）保卫处：**密切联系公安部门，负责涉及人为破坏类事件的处置，配合重大安全事件的处置。

**第八条** 加强网络与信息系安全管理，健全工作制度和建立预报预警监测体系，避免和减少网络信息安全事件发生。健全技术防护体系，在校园网出入口、数据中心、重要信息系统等重要部位，安装必要的安全防御检测工具，进行实时监测和定期扫描，发现异常情况及时处理并逐级报告。同时做好操作系统升级杀毒，数据备份、安全审计等日常管理工作。

**第九条** 建立灾害险情巡查制度。网站管理员应随时监控网站内容，做好校园网络与信息安全的日常巡查及日志保存工作，以保证最先发现灾害并及时处置突发性事件。

**第十条 启动预案**：发生网络信息安全事件后，信息中心和涉事部门应第一时间采取断网等有效措施，将损害和影响降低到最小范围，保留现场，并报告网信小组。

**第十一条 事件定级：**信息中心组织有关单位，尽最大可能收集事件相关信息，鉴别事件性质，确定事件来源，弄清事件范围，评估事件带来的影响和损害，确认事件的类别和等级。

**第十二条 应急响应：**根据事件等级采取相应的响应方式

**IV级：**信息中心组织相关部门及时、自主进行应急处置，做好处置记录。

**III至II级：**信息中心应立即上报网络安全和信息化领导小组，由领导小组指挥、协调相关部门进行应急处置。涉及人为主观破坏事件时由学校保卫处报告当地公安部门。

**I级：**信息中心立即上报网络安全和信息化领导小组组长，由学校报告教育厅科技处和当地公安部门，公安部门指挥协调有关单位和我校协同进行应急处置。

**第十三条  应急处理方式：**根据网络与信息安全事件分类采取不同应急处置方式。

**（一）网络攻击事件：**判断攻击的来源与性质，关闭影响安全的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的IP地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照事件发生的性质采取以下方案：

**病毒传播：**及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口，甚至相应楼层的网络，及时请有关技术人员协助进行杀毒处理。

**外部入侵：**判断入侵的来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价威胁很小的外网入侵，定位入侵的IP地址，及时关闭入侵的端口，限制入侵的IP地址的访问。对于已经造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和影响。  
 **内部入侵：**查清入侵来源，如IP地址、所在办公室等信息，同时断开对应的交换机端口，针对入侵方法调整或更新入侵检测设备。对于无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

**（二）设备故障事件：**判断故障发生点和故障原因，迅速联系IT运维公司尽快抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

**（三）灾害性事件：**根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

**（四）信息内容安全事件：**接到校内网站出现不良信息的报案后，应迅速屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息传播，查找信息发布人并做好善后处理。对公安机关要求我校协查的外网不良信息事件，根据校园网上网相关记录查找信息发布人。

**（五）其它不确定安全事件：**可根据总的安全原则，结合具体情况，做出相应处理，不能处理的及时请示省教育厅科技处。

**第十四条  后续处理**

（一）安全事件最初应急处置后，应及时采取措施，抑制其影响进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。

(二)安全事件被抑制后，通过对有关事件或行为的分析结果，找出问题根源，明确相应补救措施并彻底清除。

（三）安全事件解决后，要及时清理系统，恢复数据、程序、服务，恢复工作应避免出现误操作导致的数据丢失。

**第十五条  报告流程**

**（一）事发紧急报告与处置**

　　1.发现安全事件，网络与信息系统运维操作人员应根据实际情况第一时间采取断网等有效措施进行先期处置，将损害和影响降到最小范围，保留现场，并报告信息中心安全分管责任人和主要负责人。

2.信息中心安全分管责任人接到报告后，应立即组织技术人员赶赴现场进行紧急处置，同时以口头方式将相关情况报告教育厅科技处。涉及人为主观破坏事件应同时报告当地公安机关。

　　3.紧急报告内容包括：（1）时间地点；（2）简要经过；（3）事件类型与分级；（4）影响范围；（5）危害程度；（6）初步原因分析；（7）已采取的应急措施。

　　4.应及时跟进事件进展情况，出现新的重大情况应及时补报。

**（二）事中情况报告与处置**

　　1.事中情况报告应在安全事件发现后8小时内以书面报告的形式进行报送（报送内容和格式见附件1）。

　　2.事中情况报告由信息中心负责人组织技术人员、系统使用部门和运维单位共同编写，由校领导审核后，签字并加盖公章报送省教育厅科技处。

　　3.安全事件的事中处置包括：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。如果涉及人为主观破坏的安全事件应积极配合公安部门开展调查。

**（三）事后整改报告与处置**

　　1.事后整改报告应在安全事件处置完毕后5个工作日内以书面报告的形式进行报送（报送内容和格式见附件2）。

　　2.事后整改报告由信息中心负责人组织技术人员、系统使用部门和运维单位共同编写，由校领导审核后，签字并加盖公章报送省教育厅科技处。

　　3.安全事件事后处置包括：进一步总结事件教训，研判信息安全现状、排查安全隐患，进一步加强制度建设，提升安全防护能力。如涉及人为主观破坏的安全事件应继续配合公安部门开展调查。

**（四）一般安全事件报告与处置。**单位发生一般安全事件，应及时、自主组织应急处置工作，在事件处置完毕后5日内向省教育厅科技处报送整改报告（报告内容和格式见附件2）

**（五）预警类信息的报告与处置。**信息中心要认真做好省教育厅、公安厅等信息安全部门发布的预警类信息的应急处置工作，并及时将执行情况同时报告教育厅科技处和省教育信息安全监测中心。

**（六）信息安全问题整改类信息的报告与处置。**学校相关部门要认真做好教育部、省教育厅、省公安厅、省工业和信息化委员会、省互联网应急办公室等信息安全部门发布的漏洞整改类信息的应急处置工作，并及时将整改报告同时报送教育厅科技处和省教育信息安全监测中心。（报送内容和格式见附件3）

**第十六条**加强技术保障，不断完善网络安全整体方案，加强技术防护，确保信息系统的稳定与安全。加强队伍建设，不断提高工作人员的信息安全防范意识和技术水平，确保安全事件应急处置科学得当。

**第十七条**  加强资金保障，信息中心根据校园网安全防护和应急处置工作实际需要，提出用于安全的软硬件设备及运行维护经费预算，报财务处纳入年度经费预算，以专项经费列支。

**第十八条**  加强安全培训和演练，信息中心应定期组织相关部门和信息员信息安全知识培训，增强防范意识和应急处置能力。开展应急处置演练，确保相关措施的有效落实。

**第十九条** 本预案自发布之日起施行。

**第二十条**  本预案由信息中心负责解释。

郑州测绘学校信息中心联系电话：0371-56665901

河南省教育厅科技处联系电话：0371—69691286、69691767（传真）

　　河南省教育信息安全监测中心应急值守电话：0371—67761893、67763297

　　附件：[1.信息技术安全事件情况报告（样式）](http://www.haedu.gov.cn/UserFiles/File/201705/20170525120439915.doc)

[2.信息技术安全事件整改报告（样式）](http://www.haedu.gov.cn/UserFiles/File/201705/20170525120445884.doc)

[3.信息安全隐患整改报告（样式）](http://www.haedu.gov.cn/UserFiles/File/201705/20170525120454196.doc)

附件1

信息技术安全事件情况报告

单位名称：（加盖公章） 事发时间： 年 月 日 分

|  |  |  |  |
| --- | --- | --- | --- |
| 联系人姓名 |  | 手机 |  |
| 电子邮箱 |  |
| 事件分类 | □有害程序事件 □网络攻击事件  □信息破坏事件 □设备设施故障  □灾害事件 □其他 | | |
| 事件分级 | □I级 □II级 □III级 □IV级 | | |
| 事件概况 |  | | |
| 信息系统基本情况（如涉及请填写） | 1.系统名称：  2.系统网址和IP地址：  3.系统主管单位/部门：  4.系统运维单位/部门：  5.系统使用单位/部门：  6.系统主要用途：  7.是否定级 □是 □否，所定级别：  8.是否备案 □是 □否，备案号：  9.是否测评 □是 □否  10.是否整改 □是 □否 | | |

|  |  |
| --- | --- |
| 事件发现与处置的简要经过 |  |
| 事件初步估计的危害和影响 |  |
| 事件原因的初步分析 |  |
| 已采取的应急措施 |  |
| 是否需要应急支援及需支援事项 |  |
| 信息技术安全分管负责人意见（签字） |  |
| 主要负责人意见（签字） |  |

附件2

信息技术安全事件整改报告

单位名称： （加盖公章） 报告事件： 年 月 日

|  |  |  |  |
| --- | --- | --- | --- |
| 联系人姓名 |  | 手机 |  |
| 电子邮箱 |  |
| 事件分类 | □有害程序事件 □网络攻击事件  □信息破坏事件 □设备设施故障  □灾害事件 □其他 | | |
| 事件分级 | □I级 □II级 □III级 □IV级 | | |
| 事件概况 |  | | |
| 信息系统基本情况（如涉及请填写） | 1.系统名称：  2.系统网址和IP地址：  3.系统主管单位/部门：  4.系统运维单位/部门：  5.系统使用单位/部门：  6.系统主要用途：  7.是否定级 □是 □否，所定级别：  8.是否备案 □是 □否，备案号：  9.是否测评 □是 □否  10.是否整改 □是 □否 | | |

|  |  |
| --- | --- |
| 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 |  |
| 存在问题与建议 |  |
| 信息技术安全分管负责人意见（签字） |  |
| 单位主要负责人意见（签字） |  |

附件3

信息技术安全隐患整改报告

单位名称：（加盖公章） 报告时间： 年 月 日

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 联系人姓名 | |  | 手机 |  |
| 电子邮箱 |  |
| 信息安全隐患  名称 | |  | | |
| 信息安全隐患类别 | | □安全漏洞 □暗链 □网页篡改 □弱口令  □信息泄露 □系统后门 □网页挂马  □其它 | | |
| 隐患级别 | | □高危 □中危 □低危 | | |
| 接收到整改通知时间 | |  | | |
| 信息系统基本情况（如涉及请填写） | | 1.系统名称：  2.系统网址和IP地址：  3.系统主管单位/部门：  4.系统运维单位/部门：  5.系统使用单位/部门：  6.系统主要用途：  7.是否定级 □是 □否，所定级别：  8.是否备案 □是 □否，备案号：  9.是否测评 □是 □否  10.是否整改 □是 □否 | | |
| 存在隐患主要原因 |  | | | | |
| 简要处置过程 |  | | | | |
| 处置结果 |  | | | | |
| 信息技术安全主管部门审核意见（签字） |  | | | | |
| 信息技术安全分管负责人审定意见（签字） |  | | | | |

备注：接到安全隐患告知通知后，按规定时限将该报告提交至教育厅科技处和省教育信息安全监测中心。