河北传媒学院文件

院信字〔2019〕5号

网络与信息安全事件应急预案

各学院（部）、处（室）：

为提高我校网络与信息系统处理突发事件的能力，形成科学、有效、反应迅速的应急工作机制，减轻或消除突发事件的危害和影响，确保我校信息系统安全运行，最大限度地减少网络与信息安全突发公共事件的危害，特制定本预案。

一、适用范围

本预案适用于我校信息系统安全突发事件的应急响应。当发生重大信息安全事件时，启动本预案。

二、工作原则

统一领导，快速反应，协同工作，科学处置。坚持“谁主管谁负责、谁负责谁落实”的原则，充分发挥各方面力量，共同做好网络与信息安全事件的应急处置工作。

三、编制依据

根据《国家通信保障应急预案》、《中华人民共和国计算机信息系统安全保护条例》、《计算机病毒防治管理办法》、《信息安全应急响应计划规范》、《信息安全技术信息安全事件分类分级指南》、《中华人民共和国网络安全法》相关法规、规定、文件精神，制定本预案。

四、组织机构与职责

1、学校网络与信息安全事件应急响应由河北传媒学院网络与信息安全事件应急处置领导小组统一领导（以下简称信息安全领导小组），负责全校网络与信息安全应急工作的领导、决策和重大工作部署。

2、信息安全领导小组组长由主管副校长担任，成员由各部门主要负责人组成。

3、信息安全领导小组下设应急响应工作办公室，承担领导小组的日常工作。应急响应工作办公室设在信息管理中心，主要负责协调网络与信息安全保障工作，并根据网络与信息安全事件的发展态势和实际控制需要，具体负责现场应急处置工作。办公室应当经常召开会议，对近期发生的事故案例进行研究、分析，并积极开展应急响应实施方案的研究、制定和修订完善。

五、预防与预警机制

1、学校应从制度建立、技术实现、业务管理等方面建立健全网络与信息安全的预防和预警机制。

2、信息监测及报告

（1）应加强网络与信息安全监测、分析和预警工作。学校应每天定时利用自身监测技术平台实时监测和汇总重要系统运行状态相关信息，如：出口路由器、服务器、上网行为、安全设备的访问、运行、报错及流量等日志信息，分析系统安全状况，及时获得相关信息。

（2）建立网络与信息安全事件通报机制。发生网络与信息安全事件后应及时处理，并视严重程度向各院系、处室网络与信息安全事件的应急响应执行负责人及上级主管部门报告。

3、预警

应急响应办公室成员在发生网络与信息安全事件后，应当进行初步核实及情况综合，快速研究分析可能造成损害的程度，提出初步行动对策，并视事件的严重程度决定是否及时报信息安全领导小组负责人。

信息安全领导小组在接受严重事件的报告后，应及时发布应急响应指令，并视事件严重程度向上级相关部门汇报。

（1）预警范围：

易发生事故的设备和系统；存在事故隐患的设备和系统；重要业务使用的设备和系统；发生事故后可能造成严重影响的设备

和系统。

（2）预防措施：

建立完善的管理制度，并认真实施；设立专门机构或配备专人负责安全工作；适时分析安全情况，制定、完善应急响应具体实施方案。

4、预防机制

积极推行信息系统安全等级保护，逐步实行网络与信息安全风险评估。基础信息网络和重要信息系统建设要充分考虑抗毁性与故障恢复，制定并不断完善网络与信息安全应急响应具体实施方案；及早发现事故隐患，采取有效措施防止事故发生，逐步建立完善的监控系统，保证预警的信息传递准确、快捷、高效。

六、事件分类与分级

1、事件分类

河北传媒学院网络与信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件等7个基本分类。

有害程序事件：蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的网络与信息安全事件。

网络攻击事件：通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的网络与信息安全事件。

信息破坏事件:通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的网络与信息安全事件。

信息内容安全事件:利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件，利用网络从事违法犯罪活动的情况，网络恐怖活动的嫌疑情况和预警信息。

设备设施故障:由于信息系统自身故障或外围保障设施故障而导致的网络与信息安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的网络与信息安全事件。

灾害性事件:由于不可抗力对信息系统造成物理破坏而导致的网络与信息安全事件。

其他信息安全事件:不能归为以上6个基本分类的网络与信息安全事件。

2、事件定级

河北传媒学院网络与信息安全事件级别分为四级：一级(特别重大)、二级(重大)、三级(较大)和四级(一般)。

一级（特别重大)：指能够导致特别严重影响或破坏的网络与信息安全事件。

二级（重大)：指能够导致严重影响或破坏的网络与信息安全事件。

三级（较大)：指能够导致相对严重影响或破坏的网络与信息安全事件。

四级（一般）：指能够导致较小影响或破坏的网络与信息安全事件。

七、应急响应的流程

在发生信息安全事件时，启动下列应急响应流程。

1、事件分析

事件分析主要完成如下工作：

（1）在发生信息安全事件后，应急响应办公室对事件进行确认。

（2）确认为信息安全事件后，根据应急处理事件分类规则对事件进行定性、定级和上报。

（3）根据对事件的初步分析，确定应急处理方式，如果应急响应办公室以自身力量无法处理的事件，由其向上级领导或上级主管部门提出应急支援请求。

2、事件处理

事件处理主要包括以下内容：

（1）泄密安全事件发生时，要及时的用口头或书面的形式向保密工作部门如实报告，同时采取断开网络、改变或终止用户权限等措施切断泄密源头，控制泄密范围，并及时对系统隐患进行修补。在对系统的泄漏隐患或风险进行重新评估，确认安全后，系统方能重新运行，对事件类型、发生原因、影响范围、补救措施和最终结果进行详细纪录。

（2）系统运行安全事件发生时，应分析是否存在针对该事

件的特定系统预案，如果存在则启动特定系统应急预案，如果涉及多个特定系统预案，应同时启动所有涉及的特定系统预案。分析是否存在针对该事件的专题预案，如果存在则启动专题预案，如果事件涉及多个专题预案，应同时启动所有涉及的专题预案。

（3）如果没有针对该事件的应急预案，应根据事件具体情况，采取抑制措施，抑制事件进一步扩散，并根除事件影响，恢复系统运行；

3、结束响应

系统恢复运行后，应急响应办公室对事件造成的损失、事件处理流程、应急预案进行评估，对响应流程、预案提出修改意见，撰写事件处理报告。应急响应办公室应根据《信息安全应急预案》要求，确定是否需要上报该事件及其处理过程，需要上报的应及时准备相关材料，上报上级机关。

对于蠕虫、病毒等易造成大范围传播的信息安全事件，应及时向应急工作小组提交预警信息。

4、应急处置演练制度

为保证应急行动的能力，应每年至少组织一次应急行动演练，以提高处理应急事件的能力，检验物资器材的完好情况。

应急响应演练按如下步骤进行：

（1）由信息安全领导小组确定应急响应演练的目标和应急响应演练的范围；

（2）按信息安全领导小组的要求，由应急响应办公室制定

应急响应演练的方案；

（3）应急响应办公室调配应急响应演练所需的各项资源，并协调应急响应演练过程中涉及的部门和单位；

（4）应急响应办公室组织进行应急演练；

（5）信息安全领导小组总结经验，根据演练结果对应急预案进行更新，并对本单位的应急工作整改。

在应急响应演练结束之后，应急响应办公室应针对应急响应工作过程中遇到的问题，分析应急响应预案的科学性和合理性，针对预案中的问题向应急工作小组提出修改建议。应急工作小组组织对修改意见进行评估，修改后的预案应经评估通过后，上报领导小组，经批准后发布实施。

在上级机关预案或相关的法律标准修改后，本预案应进行调整与其保持一致。调整后，应急工作小组应组织专家组对其评审，评审通过后上报领导小组，经批准后发布实施。

5、应急响应总结制度

应急处置结束后，须进行以下工作：

（1）召开应急事件总结会议。

（2）分析异常事件发生的原因，形成信息安全事件原因分析报告。

（3）有关人员编制安全事件处置报告。报告内容包括事件发生时间、地点，监测到事件的时间、地点，事件的处理过程，事件的处理方法，事件造成的影响，可吸取的经验教训。

（4）对相关责任人员进行严肃的批评和教育，指出其工作中的缺陷，并让其提供总结报告。情节严重的，按照学院规定给予处罚。

（5）针对发生的事件的起因，分析改进的措施和补救方法，从技术和管理上加以改进，坚决杜绝类似事件在今后发生。

（6）技术改进措施：

①针对脆弱性或漏洞，检查涉密信息系统的其他位置，找出并进行改进或加固；

②改进应急方案内容，使应急方案满足今后的日常监测和应急需要；

③增加可能出现故障设备的备份设备，增加单点设备的备份设备；

④更换或升级经常出故障的产品；

⑤对本次应急处理的处理方法进行归档，作为知识经验进行保管。

（7）管理改进措施：

①修改相关制度和岗位工作任务和职责；

②落实人员的岗位职责；

③进一步做好系统的日常运维工作；

④加强教育，培养人员的安全意识；

⑤进一步加强安全检查，以检查促安全。

八、附则

本预案由信息管理中心负责解释，自发布之日起施行。

二〇一九年十一月五日

河北传媒学院院长办公室　　2019年11月5日印发