教育技术中心文件

教育技术中心发〔2021〕1号

教育技术中心
关于印发《承德医学院网络安全事件应急预案》的通知

各单位、各部门:

根据“庆祝中国共产党成立一百周年网络安全保障方案”，对《承德医学院网络安全事件应急预案》进行了修订，发生网络安全事件时按照此预案执行。

特此通知。

教育技术中心

2021年5月12日

承德医学院网络安全事件应急预案

第一章　总则

第一条 编制目的 为了切实做好我校网络与信息系统安全事件（以下简称网络安全事件）的防范和应急处理工作，进一步提高处理网络安全事件的能力，形成科学、有效、反应迅速的应急工作机制，减轻或消除网络安全事件的危害和影响，确保校园网络及信息系统的实体安全、运行安全和数据安全，制定本预案。

第二条 编制依据《中华人民共和国计算机信息系统安全保护条例》、《国家信息化领导小组关于加强信息安全保障工作的意见》和公安部、国务院信息化工作办公室等单位《关于信息安全等级保护工作的实施意见》，依据 GB/T 24363-2009《信息安全技术 信息安全应急响应计划规范》。

第三条 适用范围 本预案适用于承德医学院网络安全事件，按照《国家网络安全事件应急预案》规定，本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害性事件和其他事件。信息内容安全事件的应对，参照有关规定和办法。

第四条 工作原则 统一领导、统一指挥、各司其职、快速有效、保障安全。

第二章　组织机构与职责

第五条 学校网络安全事件应急响应由承德医学院网络安全和信息化领导小组统一领导，负责全校网络安全事件应急处置工作的领导、决策和重大工作部署。

第六条 教育技术中心成立学校网络安全事件应急响应工作小组，主要负责综合协调网络与信息安全保障工作，并根据网络安全事件的发展态势和实际控制需要，协助各单位完成应急处置工作。工作小组应当对近期发生的事件案例进行研究、分析，并积极开展应急响应具体实施方案的研究、制定工作。

第七条 各单位党组织负责人为本单位网络与信息系统安全管理责任人，同时也是本单位网络安全事件应急响应执行责任人，负责网络安全事件的具体处置和管理工作。

第三章　预防与预警机制

第八条 学校从制度建立、技术实现、业务管理等方面建立健全网络与信息系统安全的预防与预警机制。

第九条 预防机制 严格执行网络安全等级保护制度；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；及早发现网络和系统安全隐患，采取有效措施防止事件发生。

第十条 预警机制

（一）加强网络与信息系统安全监测、分析和预警工作。学校定期对重要信息系统和设备运行状态进行监测，主要包括路由器、交换机、服务器、存储设备、安全设备、信息系统、数据库

系统、机房管理系统等，收集访问、运行、报错及流量等日志数据，分析系统安全状况。

（二）对各单位潜在的网络安全事件进行不定期通报，网络安全事件应急响应工作小组协助进行处置。

第四章　网络安全事件分类与分级

第十一条 网络安全事件分为以下七类。

（一）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安全事件。

（二）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安全事件。

（三）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安全事件。

（四）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。

（五）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安全事件。

（六）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安全事件。

（七）其他信息安全事件：不能归为以上6个基本分类的网络安全事件。

第十二条 网络安全事件级别分为以下四级。

一级(特别重大)：指能够导致特别严重影响或破坏的网络安全事件。

二级(重大)：指能够导致严重影响或破坏的网络安全事件。

三级(较大)：指能够导致相对严重影响或破坏的网络安全事件。

四级(一般)：指能够导致较小影响或破坏的网络安全事件。

第五章　应急响应流程

第十三条 当发生网络安全事件时，启动下列应急响应流程，流程图如下。

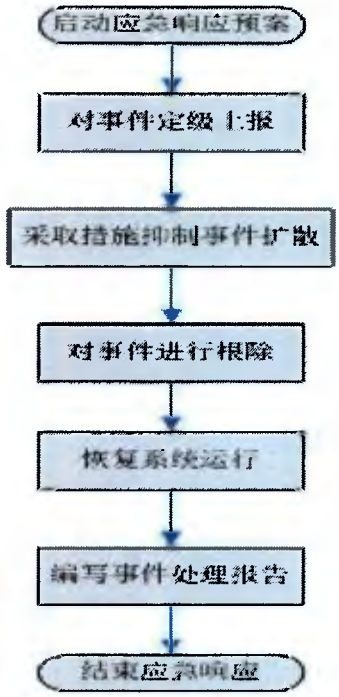

图 1. 应急响应流程图

（一）网络安全事件发生后，应急响应工作小组根据事件分类和事件定级规则，对事件进行定性、定级，并向主管校领导或相关单位报告。

（二）应急响应执行责任人指定网络与信息安全管理员采取关闭系统、断开网络、改变或终止用户权限等措施切断事件源头，控制事件范围，并及时对系统隐患进行处置，报应急响应工作小组对系统存在的隐患或风险进行重新评估。确认安全后，系统方能重新运行。

（三）系统恢复运行后，应急响应执行责任人撰写网络安全事件处置报告，交应急响应工作小组。小组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。

（四）网络安全事件处置报告内容包括事件发生时间、地点、事件造成的影响、事件的处理过程和处理方法、分析事件发生的原因及可吸取的经验。应急响应工作小组分析改进的措施和补救方法，从技术和管理上加以改进，坚决杜绝类似事件再次发生。

承德医学院教育技术中心　　2021年5月12日印发