内蒙古艺术学院校园网络安全事件应急预案

一、总则

（一）编制目的

为健全完善学校网络安全事件应急工作机制,规范网络安全事件工作流程，提高学校网络安全应急处置能力,预防和减少网络安全事件造成的损失和危害，维护学校安全稳定，制定本预案。

（二）编制依据

本预案根据《中华人民共和国网络安全法》《国家网络安全事件应急预案》《教育系统网络安全事件应急预案》《河北省教育系统突发公共事件应急预案》的有关要求编制。

（三）工作原则

（1）**统一领导，分级负责**。学校网络安全工作领导小组统筹协调学校网络安全应急指挥工作，各部门按照“谁主管谁负责，谁运维谁负责”的原则，明确落实应急处理部门和各级部门的安全责任，共同提高我校网络安全事件应急处置水平。

（2）**快速反应，科学处置**。快速响应，及时获取信息、跟踪研判、科学决策、果断处置，最大限度地降低网络安全事件所造成的危害和影响。

（3）**预防为主，加强监控**。坚持事件处置和预防工作相结合，做好网络安全事件的预防、预判、预警工作，充分发挥各方面力量，强化应急支撑保障能力和安全态势感知能力建设，做到早发现、早报告、早控制、早解决。

（四）适用范围

本预案适用于学校和各二级学院、管理教辅部门、附属单位。按照《教育系统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。网络舆情与信息内容安全事件的应对，按照《河北师范大学网络舆情报告处置与管理管理办法》等有关规定执行。

二、网络安全事件分级

根据《教育系统网络安全事件应急预案》事件分级规定，根据学校工作特点，可能造成的危害，可能发展蔓延的趋势等，将网络安全事件分为以下四级：

特别重大网络安全事件（I 级）：学校校园网与多个核心业务系统发生全校性大规模瘫痪、信息系统被黑客入侵篡改造成非常严重的影响（例如被敌对黑客组织篡改内容并被其网站发布）、学校核心业务数据丢失、泄露、被篡改，对

学校正常工作造成特别严重损害，且事态发展超出学校控制能力的安全事件；

重大网络安全事件（II级）：学院校园网与多个核心业务系统发生全校性瘫痪、信息系统（网站）被黑客入侵篡改损害学校形象、大量师生个人信息泄露、重要部门业务数据丢失、泄露、被篡改，对学校正常工作造成严重损害，需学校多个部门协同处置，事态发展未超出学校控制能力的安全事件；

较大网络安全事件（III级）：学校某区域校园网络、部门重要业务系统瘫痪、部门业务数据丢失、泄露、被篡改，对学校正常工作造成一定损害，有关部门和信息化中心配合可以解决的安全事件；

一般网络安全事件（IV级）：上述情形以外，发生在个别学院、部门，无扩散性，损害轻微，依靠二级单位自身力量可以解决的安全事件。

三、组织机构与职责

学校网络安全工作领导小组统筹协调全局性网络安全应急处置工作，决定Ⅰ级和II级网络安全事件应急预案的启动，督导检查各有关单位在网络安全事件处置工作中履行职责情况。发生特别重大网络安全事件时，成立专门工作组，负责组织指挥和协调事件处置，并根据实际情况吸纳相关部门、人员参加应对工作。

学校网络安全工作领导小组办公室（党委宣传部）负责网络安全工作的组织、协调，制定相关制度和应急预案；根据校内发生的网络安全事件危害程度提出相应响应级别，组织协调相关单位落实应急预案，共同做好处置工作；负责及时收集、通报和上报网络安全事件处置的有关情况，对外发布相关信息。

信息化中心具体负责学校网络安全基础条件建设和网络安全事件处置过程中的技术保障。

安全工作部（处）负责联系公安部门，配合做好网络安全事件的处置工作。

各二级单位参照成立本单位网络安全工作领导小组，建立上下联动的网络安全事件应急处置工作机制，明确相关人员工作责任。

四、预防监测

建立健全学校网络安全事件预警预报体系。各单位严格执行校园网络与信息系统安全各项管理制度，对本部门所负责管理的信息系统采取相应安全保障措施，及时修复上级通报、学校自查发现的各类网络安全漏洞、隐患。

信息化中心加强对校园网络的监控和安全管理，做好相关数据日志记录，同时做好数据中心的数据备份及登记工作，建立灾难性数据恢复机制。

特殊时期，根据工作需要，由学校网络安全工作领导小组办公室进行统一部署和安排，组织专业技术人员对校园网络和信息系统采取加强性保护措施，对校园网络通信及信息系统进行不间断监控，重要信息系统（网站）责任单位24小时安排人员值守。

五、应急处置流程

（一）分析研判

对上级主管部门通报及自主检测的网络安全问题和隐患，责任单位要及时进行信息的收集、校验、跟踪、确认。初判为较大以上（含较大）的网络安全事件，应立即向学校网络安全工作领导小组办公室报告。

（二）前期处置

确认网络安全事件发生后，责任单位应立即启动应急预案，立即组织本单位的网络安全技术人员采取科学有效的应急处置措施，尽最大努力将影响降到最低，并注意保存网络攻击、网络入侵或网络病毒等证据。经学校网络安全工作领导小组办公室初步研判为特别重大、重大网络安全事件的，应立即向学校网络安全工作领导小组组长报告。

（三）应急响应机制

网络安全事件发生后，在前期处置基础上，学校网络安全工作领导小组办公室组织协调各有关部门，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，确认突发事件的类别和等级，并按照以下响应机制对突发事件进行处置。

Ⅰ级突发事件响应：立即上报学校网络安全工作领导小组，领导小组再上报省教育厅相关部门和石家庄市公安局，由上级相关部门、属地公安机关会同学校网络安全工作领导小组统一组织、协调指挥应急处置。

Ⅱ级突发事件响应：立即上报学校网络安全工作领导小组和分管校领导，由分管校领导协调指挥进行应急处置。

Ⅲ级或Ⅳ级突发事件响应：由信息化中心协助突发安全事件的信息系统（网站）建管部门完成应急处置工作，做好相关记录工作，如发生影响扩大等突发状况，及时将有关情况报分管校领导。

（四）应急处置方式

根据网络安全事件分类，采取不同应急处置方式。

1.有害程序与网络攻击事件：判断有害程序与网络攻击的来源与性质，关闭影响安全与稳定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，寻找并公布病毒攻击信息，以及杀毒、防御方法。

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。

2.信息破坏事件：一般性信息破坏事件，应迅速屏蔽信息系统（网站）的网络端口或拔掉网络连接线，阻止信息进一步被破坏或有害信息更大范围的传播，根据信息系统（网站）相关日志记录查找破坏来源并做好记录；发现政治性有害信息，首先拔掉网络连接线，上报学校网络安全工作领导小组办公室，由学校网络安全工作领导小组决定后续处理方式。

3.设备故障事件：判断故障发生点和故障原因，迅速联系相关公司抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

4.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。

（五）善后工作

网络安全事件进行最初的应急处置后，应及时采取进一步行动，清理系统，恢复数据、程序、服务，恢复工作中应避免出现误操作导致设备损坏、数据丢失。

通过对网络安全事件的分析结果，找出问题根源，明确相应补救措施，彻底清除漏洞、隐患。由事发单位负责组织制定恢复、整改或重建方案，特别重大、重大网络安全事件的工作方案，报学校网络安全工作领导小组办公室审核后实施。

（六）记录上报

网络安全事件处置过程中，有关人员应作好完整的过程记录，保存各相关系统日志，及时报告处置工作进展情况。

网络安全事件处置结束后，较大以上（含较大）网络安全事件由学校网络安全工作领导小组办公室会同相关部门，对事件的起因、性质、影响、损失、责任等问题进行调查评估，撰写事件处理报告，总结事件处理经验和教训，需要向

上级部门报告的应及时提供相关材料。一般网络安全事件由责任单位自行进行调查评估并向网络安全工作领导小组办公室备案。

六、监督检查

学校网络安全工作领导小组办公室负责对本预案的执行情况进行监督、检查。对违反本预案操作程序，导致严重不良后果的部门和责任人，交由有关部门追究其责任。

七、保障措施

网络安全事件应急处置是一项长期的、随时可能发生的工作，必须做好各项应急保障工作。

（一）队伍保障

加强队伍建设，不断提高部门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。

（二）技术保障

不断完善网络安全防护工作方案，加强管理，确保信息系统的稳定与安全。根据工作需要聘请信息安全顾问为应急处置过程和重建工作提供咨询和技术支持。

（三）资金保障

信息化中心、各单位应根据实际需要申报购置关键设备及软件的运行维护专项资金，纳入单位年度预算，由学校给予资金保障。

（四）安全培训和演练

信息化中心定期组织对相关工作人员进行网络与信息系统安全的培训，增强预防意识和应急处置能力。有针对性地开展应急演练，确保相关措施的有效落实。

保卫工作部（保卫处）

2024 年