康 复 大 学 文 件

康大校发〔2025〕99号

关于印发《康复大学网络安全事件应急预案（试行）》的通知

各部门、单位:

《康复大学网络安全事件应急预案（试行）》已经学校校长办公会议研究通过，现予以印发，请认真遵照执行。

康复大学

2025年12月24日

康复大学网络安全事件应急预案（试行）

为建立学校网络安全事件应急响应工作机制，有效预防并科学应对网络安全突发事件，确保校园网络与信息系统正常运行，根据《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》等法律法规，以及《信息安全事件分类分级指南》（GB/Z 20986-2007）等相关规定，结合学校工作实际，制定本预案。

第一章　总则

第一条　学校网络安全事件是指学校信息化基础设施、应用系统、网站和相关数据等因各种因素遭到破坏，对学校教学、科研和管理等工作秩序造成负面影响的事件。

第二条　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，最大可能地降低危害和减少影响。

第二章　网络安全事件分级

第三条　网络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、窃取等而导致的网络安全事件。

（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、网络瘫痪等导致的网络安全事件。

（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）：

1.造成校园网络与信息系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于学校是不可承受的。

2.威胁国家安全，引起社会动荡，对学校有恶劣的负面影响，或者严重损害公众利益。

（二）Ⅱ级（重大）：

1.造成校园网络与信息系统长时间中断或局部瘫痪，使其业务处理能力受到重大影响，或系统关键数据的保密性、完整性、

可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于学校是可承受的。

2.引起社会恐慌，对学校有重大的负面影响，或者损害到公众利益。

（三）III级（较大）：

1.造成校园网络与信息系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但学校是完全可以承受的。

2.可能影响到国家安全，扰乱社会秩序，对学校有一定的负面影响，或者影响到公众利益。

（四）IV级（一般）：

1.造成校园网络与信息系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性受到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

2.对国家安全、社会秩序、学校和公众利益基本没有影响，但对个别学生、教职工、法人或其他组织的利益会造成损害。

第三章　组织机构及职责

第五条　网络安全与信息化领导小组（以下简称领导小组）

为网络安全事件应急处理领导机构，网络安全与信息化领导小组办公室（以下简称领导小组办公室）负责具体处置工作。

第六条 学校党政管理部门的处级机构，教学科研实体单位的二级学院、研究院，教辅机构，直属单位（以下统称各部门）负责本部门网站和业务系统的网络安全事件的处置工作，应对照本预案，建立本部门应急处置机制。

第四章 预防措施和处置程序

第七条 加强网络与信息系统安全管理，健全工作制度和建立预报预警监测体系，有效防范和减少网络安全事件的发生。

第八条 启动预案：发生网络安全事件后，信息网络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、收集相关证据，并报告本部门负责人和信息网络中心负责人。

第九条 事件定级：领导小组办公室组织有关单位和部门，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，确认事件的类别和等级。

第十条 应急响应：根据事件等级采取相应的响应方式。

Ⅰ至Ⅱ级：领导小组办公室立即上报网络安全与信息化领导小组，由学校报告山东省教育厅和当地公安机关，公安部门指挥协调有关单位和学校协同进行应急处置。

Ⅲ级：领导小组办公室应立即上报网络安全与信息化领导小组，由领导小组指挥、协调相关二级部门进行应急处置。涉及人为主观破坏事件时由学校安保主管部门报告当地公安部门。

Ⅳ级：领导小组办公室组织相关单位和部门及时、自主进行应急处置，做好处置记录。

第十一条 应急处理方式：根据网络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地址或其他网络用户信息。在彻底清除威胁并确认安全后，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，评估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，迅速协调技术力量尽快抢修故障设备，优先保证校园网主干网络和核心业务系统的运转。

（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）其他类事件：指不能归为以上分类的网络安全事件。

第十二条 后续处理程序

（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化。

（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，要及时恢复数据、服务，恢复工作应避免出现误操作导致的数据丢失。

第十三条 安全事件报告

（一）系统恢复运行后，领导小组办公室对事件造成的损失、事件处理流程等进行分析评估，总结经验教训，撰写事件处理报告。

（二）发生Ⅰ至Ⅱ级事件，在报告学校的同时，应按照教育部办公厅《信息技术安全事件报告与处置流程（试行）》（教技厅函〔2014〕75号）报告山东省教育厅。

第十四条 报告流程

（一）事发紧急报告：事件发生后立即以口头通讯方式报山东省教育厅，涉及人为主观破坏的事件应同时报当地公安机关。报告内容包括：时间地点，简要经过，事件类型与分级，影响范围，危害程度，初步原因分析，已采取的紧急措施。

（二）事中处置报告：应在事件发生后8小时内以书面报告形式报送。

（三）事后整改报告：应在事件处置完毕后5个工作日内以书面报告形式报送。

第五章 保障措施

第十五条 加强队伍建设，不断提高工作人员的网络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。

第六章 附则

第十七条 本预案由信息网络中心负责解释。

第十八条 本预案自公布之日起施行。

附件：网络安全事件应急响应报告

附件

网络安全事件应急响应报告

部门名称:（公章）　　事发时间:　　年　月　日

<table>
<tr><td rowspan="2">联系人姓名</td><td rowspan="2"></td><td>移动电话</td><td></td></tr>
<tr><td>电子邮箱</td><td></td></tr>
<tr><td>事件分类</td><td colspan="3">☐网络攻击事件-病毒传播　☐网络攻击事件-外部入侵
☐网络攻击事件-内部入侵　☐设备故障事件
☐灾害性事件　　☐信息内容安全事件
☐其他类事件</td></tr>
<tr><td>事件分级</td><td colspan="3">☐I级　☐II级　☐III级　☐IV级</td></tr>
<tr><td>事件概况</td><td colspan="3">（包括：事件发生的原因、造成的危害和影响、初步处置措施。可加页附文字、图片以及其他补充说明）</td></tr>
<tr><td>处理和整改情况</td><td colspan="3"></td></tr>
<tr><td>部门主要负责人意见</td><td colspan="3">签名:
年　　月　　日</td></tr>
</table>

康复大学党政办公室　　2025年12月26日印发