附件 5

中卫市教育系统网络与信息安全事件应急处置预案

为提高中卫市教育系统网络与信息安全公共事件的应对能力，有效预防、及时控制和最大限度地消除信息安全各类突发事件的危害和影响，保障教育系统信息系统的实体安全、运行安全和数据安全，特制定本预案。

一、制定依据

依据《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》《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》《政府信息系统安全检查办法》《中卫市网络安全事件应急处置预案》等相关法律法规制定。

二、工作原则

（一）积极防御，综合防范。立足安全防护，加强预警，抓好预防、监控、应急处理、应急保障和打击犯罪等环节，在管理、技术、人才等方面，采取各种措施，充分发挥各方作用，共同构筑中卫教育系统网络与信息安全保障体系。

（二）明确责任，分级负责。按照“谁主管谁负责，谁运维谁负责”的原则，分级分类建立和完善安全责任制度、协调管理机制和联动工作机制。

（三）科学决策，快速反应。加强技术储备，规范应急处置措施和操作流程，网络与信息安全突发公共事件发生时，要快速

反应，及时获取准确信息，跟踪研判，及时报告，果断决策，迅速处理，最大限度地减少危害和影响。

三、适用范围

本预案适用于中卫市教育系统发生的网络与信息安全突发公共事件和可能影响安全运行的网络安全预防和处置等应对工作。

四、组织机构

市教育局成立网络与信息安全应急领导小组和应急工作小组。

（一）应急领导小组

组　长：市教育局局长

组　员：市教育局分管副局长，沙坡头区教育局局长，中宁县教育体育局局长，海原县教育体育局局长

（二）应急领导小组职责

研究制定全市教育系统网络与信息安全应急处置工作规划、年度计划和政策措施，协调推进教育系统网络与信息安全应急机制和工作体系建设。发生网络与信息安全突发公共事件时，启动本预案，组织应急处置。

（三）应急工作小组

组长：市教育局分管副局长

组员：局办公室、信息化服务中心、教育督导科、规划财务科负责同志，各县（区）教育（体育）局分管负责人，应急工作小组由市教育局办公室牵头。

（四）应急工作小组职责

1.负责和处理应急领导小组的日常工作，检查、督促、落实应急领导小组决定事项。

2.研究和制订网络与信息安全应急处置的技术方案，检查、指导和督促各县（区）、学校的网络与信息安全工作，组织开展相关演练。

3.负责教育系统网络安全事件的预防、监测、报告和应急处置工作。

五、监测与预警

（一）预警分级

网络安全事件预警等级分为四级，由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。

（二）预警监测

按照“谁主管谁负责、谁运行谁负责”的原则，组织对本县（区）、学校管理范围内建设运行的网络和信息系统开展网络安全监测工作，及时将重要监测信息报市教育局。

（三）预警信息发布

各县（区）、学校组织对监测信息进行研判，需要立即采取防范措施的，应当及时报告上级教育行政部门，对可能发生重大及以上网络安全事件的信息及时向市教育局、市委网信办报告。发布橙色或以上预警和涉及多地区、多部门、多行业的预警需逐级报请网信部门组织研判。

预警信息包括事件的类别、预警级别、起始时间、可能影响范围、警示事项、应采取的措施和时限要求、发布部门等。

（四）预警响应

1.红色、橙色预警响应。市委网信办统筹组织预警响应工作，市教育局及有关县（区）和学校网络安全事件应急指挥机构实行24小时值班，相关人员保持通信联络畅通，准确及时将相关情况报市委网信办。

2.黄色、蓝色预警响应。相关县（区）和学校启动应急预案，立即采取预防措施，检查可能受到影响的信息系统，做好相关安全漏洞的修复工作。加强网络安全威胁监测频率，及时掌握本县（区）、学校网络系统安全状况，按照早发现、早报告、早处置的原则，对可能演变为网络安全事件的威胁及时报告市教育局，同时报市委网信办。

（五）预警解除

预警发布县（区）或学校根据实际情况，确定是否解除预警，及时发布预警解除信息。

六、应急处置

（一）先期处置

当发生网络与信息安全突发公共事件时，值班人员应做好先期应急处置工作，立即采取措施控制事态，同时向应急工作小组组长报告。

应急工作小组组长接到报告后，应加强与网信、公安等有关方面的联系，掌握最新发展动态。对一般的突发事件，应组织应

急处置工作，有关情况报应急领导小组；对发生重大和有可能演变为重大的网络与信息安全突发公共事件的，要立即报告应急领导小组，并做好启动本预案的各项准备工作。

应急领导小组在接到报告后，要根据网络与信息安全突发公共事件发展态势，视情况决定赶赴现场指挥，协调相关部门应急支援。

（二）应急指挥

本预案启动后，要抓紧收集相关信息，掌握现场处置工作状态，分析事件发展态势，研究提出处置方案，统一指挥网络与信息应急处置工作。需要成立现场指挥部的，应立即在现场开设指挥部，现场指挥部根据事件性质组建各类应急工作组，开展应急处置工作。必要时，向相关部门申请应急支援。

（三）信息处理

应急工作小组对事件进行动态监测、评估，不得隐瞒、缓报、谎报。要做好信息分析、报告和发布工作，及时向领导小组提供事件动态信息，必要时组织专家和有关技术人员研判并提出对策，完善应急处置措施。

（四）信息发布

当网络与信息安全突发公共事件发生后，应急工作小组应及时做好信息发布工作，引导舆论和公众行为，增强公众的信心，接受群众咨询，释疑解惑，稳定人心。

（五）扩大应急

经应急处置后，事态难以控制或有扩大发展趋势时，应实施

扩大应急行动。要迅速召开应急领导小组会议，根据事态情况，研究采取有利于控制事态的非常措施，并向公安、网信等相关部门请求支援。

（六）善后处理

在应急处置工作结束后，应急工作小组要迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作。统计各种数据，查明原因，对事件造成的损失和影响以及恢复重建能力进行分析评估，制定恢复重建计划并组织实施，且将善后处置的有关情况报应急领导小组。

（七）调查评估

应急处置工作结束后，应急工作小组应立即组织有关人员和专家组成事件调查组，对事件发生及其处置过程进行全面的调查，查清事件发生的原因及损失情况，总结经验教训，写出调查评估报告，报应急领导小组。

七、保障措施

（一）应急装备保障

重要网络与信息系统在建设系统时应事先预留一定的应急设备，建立信息网络硬件、软件、应急救援设备等应急物资库。在网络与信息安全突发公共事件发生时，报应急领导小组同意后，由应急工作小组负责统一调用。

（二）数据保障

重要信息系统均应建立容灾备份系统和相关工作机制，保证重要数据在受到破坏后，可紧急恢复。各容灾备份系统应具有一

定的兼容性，在特殊情况下各系统间可互为备份。

（三）应急队伍保障

各级教育行政部门和各级各类学校要重视本单位的网络与信息安全工作，加强网络技术人员队伍建设，强化本单位网络安全设备及系统的常态化运维，每年开展一次网络安全应急演练，切实提高网络与信息安全的保障能力。

（四）经费保障

各级教育行政部门和各级各类学校应利用现有政策和资金渠道，支持网络安全应急技术支撑队伍建设、基础平台建设、预案演练、物资保障等工作开展，为网络安全应急工作提供必要的经费保障。

（五）责任追究

网络安全事件应急处置工作实行责任追究制。在网络安全事件应急管理工作中不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者在应急管理工作中有其他失职、渎职行为的，依照相关规定对相关责任人给予处分，构成犯罪的，依法追究刑事责任。