包头市人民防空办公室
网络安全应急预案

为妥善应对和处置包头市人民防空办公室网络安全突发事件及重大活动安全保障任务，确保网络正常运行，根据《中华人民共和国计算机信息系统安全保护条例》、国务院办公厅《关于加强政府信息系统安全和保密管理工作的通知》等有关精神，结合包头市人防办实际情况，特制定本应急预案。

本预案主要立足防范和消除以下危害情况的出现：一是包头市人民防空网站因病毒感染、黑客攻击导致数据被篡改、丢失、泄密，系统不能正常运行；二是因硬件故障、自然灾害、失窃等原因造成数据丢失、系统瘫痪；三是防范网络与信息安全漏洞。

一、应急组织机构

为及时处置网络信息安全突发事件，确保网络与信息安全，由包头市人民防空办公室网络安全工作领导小组负责对网络突发事件的协调领导工作、网络与信息安全事件的应急处置，协助制定应急处置方案，及时向上级相关部门汇报情况，必要时与公

安机关联系，获得必需的技术支持。

二、应急处置工作原则

1. 统一领导、规范管理。网络安全突发事件由包头市人民防空办公室网络安全领导小组统一协调领导，遵照“统一领导、综合协调、各司其职”的原则协同配合、具体实施，完善应急工作体系和机制。

2. 明确责任，分级负责，保证对网络与信息安全事件做到快速觉察、快速反应、及时处理、及时恢复。

3. 预防为主，加强监控。积极做好日常安全工作，提高应对突发网络与信息安全事件的能力。建立和完善信息安全监控体系，加强对网络与信息安全隐患的日常监测，重点监控网站网页是否被篡改、信息发布是否异常、网站运行是否异常等问题。

三、应急预防保障措施

1. 建立健全网络与信息安全管理预案，加强对网络信息的日常监测、监控，强化安全管理，对可能引发网络与信息安全事件的有关信息，要认真收集、分析判断，发现有异常情况时，及时处理并逐级报告。

2. 做好网站文件和数据库备份。备份采用完全备份策略与部分备份策略相结合，网站管理员负责每个月对网站文件及数据库进行一次完整备份，备份介质、移动硬盘或光存储介质刻录盘。

3. 特殊时期启动网络与信息安全应急值班制度。在特殊时期进行 24 小时应急值班，对网络和信息数据加强保护，进行不间

断监控，一旦发生网络与信息安全事件，立即启动应急预案，判定事件危害程度，采取应急处置措施，并立即将情况报告有关领导。在处置过程中，及时报告处置工作进展情况，直至处置工作结束。属于重大事件或存在非法犯罪行为的，及时向公安机关报告。

4.保持与网站开发商沟通渠道的畅通，确保在应急处理过程中遇到困难或问题时能及时获得网站开发商的技术支援。

四、应急响应流程

网络安全应急响应流程主要分为:分析确认、启动应急预案，故障修复、恢复运行、详细备案。

五、应急处理措施

1.网站、网页出现非法言论事件紧急处置措施

（1）发现网站出现非法信息或内容被篡改，立即通知网站管理员和主管领导，将非法信息或篡改信息从网络中隔离出来，必要时断开网络服务器。

（2）情况严重，保护现场，保存非法信息或篡改页面，并断开网络服务器，立即向公安机关报警。

（3）网站管理员应同时作好必要记录，追查非法信息来源，清理或修复非法信息，妥善保存有关记录，强化安全防范措施，并将网站重新投入运行。

（4）将处理结果向公安机关汇报。

2.系统软件遭受破坏性攻击、网络及网站瘫痪的紧急处置

（1）系统软件遭到破坏性攻击，网络及网站瘫痪，立即向网络技术维护人员和主管领导报告，并将系统停止运行。

（2）情况严重的，要保护好现场，保存非法信息或篡改页面，并断开网络服务器，立即向公安机关报警。

（3）待公安部门提取相关资料后，技术维护人员会同技术服务商检查日志等资料，确认攻击来源。

（4）修复系统，重新配置运行环境，恢复数据。

（5）做好相应的记录，实施必要的安全加固措施，将网站重新投入运行。

3. 网络硬件故障或以外情况的应急处理

（1）出现线路问题，由电信运营商负责处理。

（2）网络设备、计算机系统、网络系统出现故障，由包头市人民防空指挥信息中心、包头市云计算中心、北京正通博瑞有限公司负责维护。

（3）机房遇到失火、盗窃，及时向主管领导报告，必要时请公安部门或消防部门提供帮助。

（4）以上情况均做好必要的记录，并妥善保存。

本预案从制定之日起执行。

包头市人民防空办公室

2022年1月18日