忻州经济开发区党工委文件

忻开党发〔2023〕7号

忻州经济开发区
网络与信息安全应急预案

区直各单位、各派驻单位：

为切实加强机关网络运行安全与信息安全的防范，做好应对网络与信息安全突发公共事件的应急处理工作，进一步提高预防和控制网络突发公共事件的能力和水平，减轻或消除网络突发公共事件的危害和影响，做好网上舆论管理和信息安全保障工作，确保网络运行安全与信息安全，结合我区工作实际，制定《忻州经济开发区网络与信息安全应急预案》，经党工委同意，现下发各单位，请遵照执行。

中共忻州经济开发区工作委员会

2023年2月8日

忻州经济开发区
网络与信息安全应急预案

一、编制依据

《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指南》、《省网络与信息安全事件应急预案》。

二、适用范围

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，对单位门户网站其中的数据造成危害，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。

本预案适用于网络安全事件的应对工作。

三、事件分级

网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

特别重大网络安全事件是指：OA和门户网站遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

重大网络安全事件是指：OA和门户网站遭受严重的系统损失，造成系统中断或局部瘫痪，业务处理能力受到极

大影响。

较大网络安全事件是指：OA和门户网站遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

一般网络安全事件是指：除上述网络安全事件以外的构成一定威胁、造成一定影响的网络安全事件。

四、工作原则

坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；坚持谁主管谁负责、谁运行谁负责，充分发挥各方面力量共同做好网络安全事件的预防和处置工作。

五、领导机构与职责

网络安全应急处置在开发区网络安全和信息化工作领导组领导下进行，领导组办公室协调各部门积极参与应对，负责安全应急技术支撑工作和联络工作。各部门要及时将网络安全突发事件上报领导组办公室进行处置。

六、预警分级、监测、研判、发布、响应、解除

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、一般网络安全事件。

领导组办公室负责对门户网站的监测工作，各科室、分局、中心要积极配合监测工作，不得以任何理由拒绝。

领导组办公室组织对监测信息进行研判，认为需要立

即采取防范措施的，应当及时通知有关部门并上报网络安全领导组，对可能发生较大及以上网络安全事件的信息及时向市网安应急办报告。

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、发布机关等。

领导组办公室组织预警响应工作，做好风险评估、应急准备和风险控制工作。

领导组办公室根据实际情况，确定是否解除预警，及时发布预警解除信息。

七、应急处置与事后评估

网络安全事件发生后，应立即启动应急预案，实施处置并及时上报信息。对特别重大网络安全事件，及时将有关情况报市网安应急办指挥部。网络安全突发事件发生后，首先要尽快控制事态，有针对性地加强防范，防止事态蔓延；其次要根据事件发生原因，有针对性的采取措施，及时备份数据，保护设备，排查隐患，尽快恢复信息系统正常运行；再次，在应急恢复过程中应保留相关证据，对于人为破坏活动要及时联系市公安局、市保密局进行调查取证；最后，要根据处置结果及时发布信息，不得在未经批准的情况下擅自发布信息。

应急响应结束后30日内，应进行总结评估工作，将事件的起因、性质、影响、责任等进行分析评估，提出处理

意见和改进措施。

八、预防工作

日常要做好网络安全检查、隐患排查、风险评估和容灾备份，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高应对网络安全事件的能力。要定期组织开展演练，检验和完善预案，提高实战能力。要充分利用各种传播媒介和其他有效宣传形式，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传，开展网络安全基本知识和技能的宣传活动。要加强网络安全事件应急知识的培训工作，提高全体工作人员防范意识和技能。

九、保障措施与监督管理

（一）应急装备保障。对于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，保证重要数据在遭到破坏后，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）要充分利用各种传播媒介及有效的形式，加强网络与信息安全突发公共事件应急和处置的有关法律法规

和政策的宣传。

（四）建立应急预案定期演练制度。通过演练，发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

（五）对在网络与信息安全突发公共事件应急处置中作出突出贡献的集体和个人，给予表彰奖励；对在网络与信息安全突发公共事件预防和应急处置中有玩忽职守、失职、渎职等行为，依法依规追究责任。

十、附则

本预案自印发之日起实施，由开发区网络安全工作领导组负责解释，根据情况适时修订。

忻州经济开发区管委会党群工作部　　2023年2月8日印发

共印30份