普定县人民政府办公室文件

普府办发〔2022〕62号

普定县人民政府办公室关于印发《普定县人民政府门户网站应用系统安全保障应急预案》的通知

各民族乡、镇人民政府、街道办事处，县人民政府有关工作部门：

《普定县人民政府门户网站应用系统安全保障应急预案》已经县政府领导同意，现印发给你们，请认真贯彻落实。

普定县人民政府办公室

2022年10月8日

普定县人民政府门户网站应用系统安全保障应急预案

一、总则

（一）编制目的

为全面做好计算机应用系统网络安全保障工作，妥善应对和处置应用系统信息安全突发事件，提高处置网络与信息安全突发事件的能力，为应用系统的正常运行创造安全、稳定、可靠的网络环境，结合使用单位实际情况，特制定本预案。

（二）编制依据

《中华人民共和国电信条例》、《国家通信保障应急预案》、《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》、《非经营型互联网信息服务备案管理办法》、《互联网 IP 地址资源备案管理办法》和《中国互联网域名管理办法》等有关法规和规章制度。

（三）适用范围

本预案针对是普定县人民政府门户网站应用系统信息安全保障专项预案，适用于在重大活动及国家节假日期间应用系统的突发情况，可能导致网络与信息安全突发事件的安全应急处置方案。

（四）应急处置原则

（1）统一领导、规范管理；应用系统突发事件由网络安全

保障应急指挥小组统一协调领导，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）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，重点监控是否被篡改、信息发布是否异常、运行是否异常等问题。

（3）快速处理，确保恢复；突发信息安全事件时，能够及时发现、预警并准确判断和快速、及时采取有效措施，迅速控制事件影响范围，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。尽可能减少信息安全事件给带来的影响或造成的损失。

（4）及时总结，全面高效；应急处置结束后，应及时对人员、经费、设备、通信、后勤等保障措施是否得力进行评估，对应急处置流程操作是否熟练、应急处置能力是否充足、预案内容是否贴合实际等进行总结和优化，并将总结、建议进行归档备案。

二、应急组织体系及职责

设立网络与信息安全事故应急指挥小组，负责应用系统及网络与信息安全事故应急处置工作。网络与信息安全事故应急指挥小组组长由龚从超担任，戴祥龙、彭林、任副组长。网络与信息安全事故应急指挥小组主要负责全面指导排查系统与信息安全风险隐患，强化安全防范和值班值守工作的督促检查，组织和协

调各方资源处置各类突发安全事件。

网络与信息安全事故应急指挥小组下设系统安全保障组、信息安全保障组、资源保障工作组 3 个工作组，并明确小组成员与责任分工，具体如下:

（一）系统安全保障组

负责组织、协调各部门对公司开发、运维管理的网站及系统进行安全隐患排查，组织处理有关网站、系统存在的安全事件，对有关资源进行安全监控和管理，保障网站、系统运行安全和稳定。

组　长：龚从超　　县人民政府办公室主任

副组长：戴祥龙　　县人民政府机关党组成员

　　郭露露　　公司运维人员

组　员：赵恩华　　县人民政府办公室工作员

　　姚贤森　　公司运维人员

（二）信息安全保障组

负责网站、系统的日常巡查、错敏词、信息发布三审三校等信息安全保障工作，及时将客户单位安排的安全工作部署对接公司安全专职人员及时完成。

组　长：龚从超　　县人民政府办公室主任

副组长：戴祥龙　　县人民政府机关党组成员

组　员：赵恩华　　县人民政府办公室工作员

（三）资源保障工作组

负责客户联络，协调、组织第三方资源保障安全工作顺利开展。

组　长：龚从超　　县人民政府办公室主任

副组长：戴祥龙　　县人民政府机关党组成员

组　员：赵恩华、郭露露、王友花、云上贵州胡春虹18008515380、北京拓尔思罗洪海13027880860（网站工作人员、运维公司人员、第三方公司支撑人员）

三、预测、预警机制

（一）危险源分析及预警级别划分

（1）危险源分析

根据网络与信息安全突发公共事件的发生过程、性质和机理，网络与信息安全突发公共事件主要分为以下三类:

1）自然灾害。指地震、台风、雷电、火灾、洪水等引起的网络与信息系统的损坏。

2）事故灾难。指电力中断、网络损坏或是软件、硬件设备故障等引起的网络与信息系统的损坏。

3）人为破坏。指人为破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖袭击等引起的网络与信息系统的损坏。

（2）预警级别划分

根据预测分析结果，预警划分为三个等级：Ⅰ级（特别严重）、Ⅱ级（严重）、Ⅲ级（一般）。

Ⅰ级（特别严重）：因特别重大突发事件引发的，有可能造

成整个应用系统重要数据遭到恶意篡改、重要数据意外丢失等情况，导致应用系统无法访问以及无法进行数据恢复的情况，及其他需要网络与信息安全事故应急指挥小组应急准备的重大情况。

II级（严重）：因重大突发事件引发的，有可能造成应用系统数据遭到篡改、挂马以及SQL注入等，导致应用系统出现不良、不正确信息展现给公众造成恶劣影响的，及其他需要网络与信息安全事故应急指挥小组应急准备的情况。

III级（一般）：因一般突发事件引发的，有可能造成应用系统安全隐患以及其他可能的造成数据丢失的情况；此类故障可能升级为造成重大突发事件故障的情况。

（二）预防机制

网络与信息安全事故应急指挥小组应加强对各级通信保障机构及应用系统的数据安全防护工作和应急处置工作的监督检查，保障应用系统的安全且良好运行环境。

（三）预警监测

各应用系统负责人和主管部门要按照“早发现、早报告、早处置”的原则，加强对各类网络与信息安全突发事件和可能引发网络与信息安全突发事件的有关信息的收集、分析判断和持续监测。

四、应急响应

当发生网络与信息安全突发事件时，发现事故的人员在按规定向相关系统管理员报告的同时，及时向网络与信息安全事故应

急指挥小组相关领导报告。负责人员在接手事故报告后要向网络与信息安全事故应急指挥小组进行应急工作进程报告和事故分析报告。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施等。

（一）应急响应流程

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、总结分析、事件上报及备案。

（二）应急处理措施

应急处理措施应围绕预警级别划分，划定事故预警级别，并第一时间向网络与信息安全事故应急指挥小组进行汇报。

（三）安全事件处置预案

（1）应用系统内容被篡改，出现非法言论事件紧急处置措施。

- 发现应用系统出现非法信息或内容被篡改，由维护人员立即向应急指挥工作组负责人汇报，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。
- 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。
- 值班人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，并将应用系统重新投入运行。
- 将处理结果向公安机关汇报。

（2）系统软件遭受破坏性攻击、入侵，导致应用系统瘫痪的紧急处置。

● 系统软件遭到破坏性攻击，导致应用系统瘫痪，由维护人员立即向应急指挥小组，并协调将系统停止运行。

● 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。

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

● 修复系统，重新配置运行环境，恢复数据。

● 做好相应的记录，实施必要的安全加固措施，将应用系统重新投入运行。

（3）应用系统出现安全漏洞的应急处理

● 发现应用系统出现安全漏洞问题后，由运维公司安全部门协调相关部门和技术人员进行漏洞修复，做好安全漏洞处理结果的验证工作。

● 漏洞修复处理完成后一个工作日内由公司安全部门出具相关安全漏洞处理报告，并向应急指挥小组负责人进行汇报。

● 做好漏洞修复情况的记录。

（4）硬件故障或以外情况的应急处理

● 出现线路问题，由运维公司网络部门组织相关人员恢复并切换。

● 网络设备、计算机系统、网络系统出现故障，由运维公司网络部门负责处理。

● 以上情况均做好必要的记录，并妥善保存。

五、分级处置流程

（一）应急处置分级和应急处置程序

突发事件发生时应急通信保障工作和通信恢复工作，按照快速、机动、灵活的原则，根据响应的预警级别分别进行处置。

Ⅰ级：突发事件造成应用系统相关数据遭到恶意篡改、重要数据意外丢失等情况，及接到相关部门下达的通信保障任务，由网络与信息安全事故应急指挥小组负责组织和协调。负责人员要迅速准确的定位故障源，如果是核心设备故障要及时切换到备用核心设备上并测试调通。

如果是重要数据遭到恶意篡改故障要第一时间通知网站主管部门进行数据恢复并切换到备用线路上测试调通。

面对黑客攻击或恶意破坏等人为造成的网络故障，及时通知公安机关，同时采取紧急行动如切断数据源网络等将损失控制在最小范围。

对于发现的重大自然灾害隐患，及时汇报网络与信息安全事故应急指挥小组并迅速通知相关部门和领导，准备好临时处理灾情需要用到的工具和应急页面。

Ⅱ级：突发事件造成应用系统数据遭到篡改、挂马以及SQL注入时，由网络与信息安全事故应急指挥小组负责组织和协调。

负责人员要迅速准确的定位故障源，如果是关键数据故障要及时切换到备用设备上并测试调通。

III级：突发事件造成应用系统安全隐患以及看可能会造成数据丢失的情况时，由运维公司安全部门协调进行安全漏洞的修复，并更新相关系统的升级补丁，保障故障及时顺利的处理，如有需要可要求相关负责人进行配合，同时及时报告工作进程给网络与信息安全事故应急指挥小组。

（二）应急保障任务结束

事故现场得以控制，应用系统符合有关标准，导致次生、衍生事故隐患消除后可确认网络通信保障和通信恢复应急工作任务完成。由网络与信息安全事故应急指挥小组下达解除任务通知，现场应急指挥机构收到通知后，任务正式结束。

事件处置完成后，及时向上级主管领导、同级的密码主管部门报告事件发生情况及处置情况。

（三）调查、处理、后果评估与监督检查

网络与信息安全事故应急指挥小组负责对重大安全事故原因进行调查、分析和处理，对事故后果进行评估，并对事故责任处理情况进行监督检查。

（四）信息发布

网络与信息安全事故应急指挥小组负责有关信息的发布工作。

（五）通讯

在突发事件的应急响应过程中，要确保应急处置系统内部机构之间的通信畅通。通信联络方式主要采用固定电话、移动电话、传真等。

六、后期处置

在突发事件应急响应过程中，网络与信息安全事故应急指挥小组应做好突发事件中应用系统数据损失情况的统计、汇总、原因分析、应急处置情况总结等，并按程序上报、处理和详细备案。

七、保障措施

（一）物资保障

网络与信息安全事故应急指挥小组应建立应用系统数据安全保障应急资源的保障机制，根据应用系统安全保障应急工作要求，配备必要的应急设备和资源，加强对应急资源及设备的管理、维护和保养，以备随时紧急调用。

（二）人员保障

安全保障应急队伍主要由运维公司网络安全部门相关人员组成。网络与信息安全事故应急指挥小组人员要不断提高自身专业水平并听从组长的指挥，如遇网站发生安全事件，相关技术人员在接到通知后 24 小时紧急响应，做好安全事件的应急处置工作。

（三）网络安全保障应急工作监督检查制度

网络与信息安全事故应急指挥小组应加强对通信保障应急

工作的监督和检查，做到居安思危、常备不懈。

（四）需要其它部门保障的工作

（1）畅通的网络保障

突发事件发生时，为了保证相关技术人员在第一时间到达现场后尽快了解并摸清故障原因，需网络安全部门的积极配合。

（2）技术保障

突发事件发生时，为了保证应用系统的正常运行，由网络与信息安全事故应急指挥小组与相应平台技术提供商保持良好的合作意愿，并及时取得技术支持。

附件：政府网站网络安全保障（技术维护）工作值班表

抄送：县委办，县人大办，县政协办，法院，检察院。

普定县人民政府办公室　　2022年10月8日印发