宁波市档案馆网络安全应急预案

一、总则

（一）编制目的

为提高我馆处置网络安全突发事件能力，形成科学、有效、反应迅速的应急工作机制，确保重要网络与信息系统的实体安全、运行安全和数据安全，最大限度地减轻网络安全事件的危害，保障数字档案馆和其他信息系统长期安全稳定运行，为人们群众提供良好的档案信息服务。

（二）编制依据

根据《中华人民共和国网络安全法》、《国家网络安全事件应急预案》、《浙江省关键信息基础设施网络安全事件应急处置指南（试行）》、《宁波市委网信办网络安全事件和安全漏洞处置细则》等有关法规、规定，制定本预案。

（三）适用范围

本预案适用于我馆档案数据中心机房、数字档案馆、宁波档案网、办公自动化系统、监控系统等重要网络与信息系统发生的突发网络安全事件和存在的高危安全漏洞。

（四）分类分级

本预案所指的网络安全事件，是指由于人为原因、软硬件缺

陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件。网络安全漏洞是引发网络安全事件的重要原因。

网络安全漏洞是指网络和信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷。这些缺陷以不同形式存在于网络和信息系统的各个层次和环节之中，一旦被恶意主体所利用，会对网络和信息系统的安全造成损害，从而影响网络与信息系统的正常运行。

1、事件分类

网络安全事件分为有害程序事件、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、灾害性事件和其他网络安全事件共七种。

（1）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（2）网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

（3）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（4）信息内容安全事件是指通过网络传播法律法规禁止信息，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。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

（7）其他事件是指不能归为以上分类的网络安全事件。

2、事件分级

根据我馆网络和重要信息系统特点，除以下事件定义为较大网络安全事件外，其余事件定为一般网络安全事件:

（1）未开放电子档案发生大规模泄露的。

（2）重要网络与信息系统发生故障后，不能在 48 小时内恢复的。

（3）集中保存国家秘密信息、重要敏感信息的信息系统数据被窃取、篡改、假冒的。

（4）遇到台风等不可抗力或黑客攻击造成较严重影响的。

（5）市委网信办认为应当定为较大网络安全事件的。

（五）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；坚持电子档案安全优先。

二、工作机构与职责

（一）领导机构

设立馆网络安全应急领导小组，由馆长和分管档案信息化的副馆长分别兼任组长和副组长。主要职责:

贯彻落实国家、省、市网络安全相关法律、法规和政策措施；监督、协调和指导网络安全事件预防、监测、报告和应急处置工作；决定较大网络安全事件应急响应的启动，组织力量对较大网络安全事件进行处置；研究决定网络安全事件和高危安全漏洞急工作的有关重大问题。

（二）工作机构

设立网络安全应急响应小组，由馆信息技术处、市电子文件备份中心相关人员组成。主要职责：

接收到预警信息后，立即组织开展应急响应，依照本预案确认是否为网络安全事件；决定一般网络安全事件应急响应的启动，组织力量对一般网络安全事件和高危安全漏洞进行处置；做好网络安全应急处置的技术支撑工作；向领导机构报告网络安全事件预防、检测和应急处置情况；按要求向市委网信办进行信息报送；按照领导机构的要求进行应急响应应对工作。

（三）各处室

各处室的主要职责包括：监测各自负责的重要信息系统和数据安全状况；及时上报发现的网络安全事件；办公室提供应急所需的人力、后勤和经费等保障；做好秩序维护、安全保障、支援等工作。

三、监测与预警

（一）信息监测

工作机构应定期监测档案数据中心机房硬件设备、操作系统、数据库、虚拟化软件和重要信息系统的运行状态信息、日志信息

和资源使用情况；应定期检查网络和安全设备策略设置情况和服务器补丁更新和防火墙设置情况；应定期检查在线档案数据资源备份情况和安全性；应及时收集第三方运维服务单位提供的运维报告。

（二）研判响应

工作机构应及时接收上级部门通报下发或市委网信办、市公安局等部门监测发现的网络安全事件和安全漏洞信息，及时收集运维单位和馆内工作人员报告的网络和信息系统服务故障。收到预警信息后，应马上组织研判，分析我馆可能存在的网络安全风险，预估已经造成或可能造成的损害程度，确认是否为网络安全事件，提出初步处置意见，并每隔24小时向领导机构汇报一次预警响应情况，直到预警解除。同时，工作机构应根据市委网信办的相关要求，做好24小时值班、每日零报告等工作。

四、应急处置

（一）应急指挥

网络安全事件发生后，应急指挥员应根据《浙江省关键信息基础设施网络安全事件应急处置指南（试行）》第2节“应急处置”，确定监控组、执行组人员。应急指挥员应尽快处于移动或有线高速网络环境中，可与现场建立远程视频实时动态了解应急处置过程；当发生重大安全事件后，如有需要应将相关信息准确通报给系统设备及服务提供商、电信、电力部门等组织，以获得适当的应急响应支持，必要时需联系市应急办请求市安全专家协助应急处置。同时，工作机构负责人应将安全事件简要向领导机

构进行通报。

（二）信息报送

网络安全事件发生后原则上要在 2 小时内向市委网信办提交《宁波市网络安全事件信息报告表》（附件 3），在网络安全事件处置结束后，应向市委网信办提交网络安全事件处置报告。发现网络安全漏洞后，应在漏洞排除后并于 2 天内将网络安全漏洞处置报告报送市委网信办。

（三）先期处置

网络安全事件发生或发现网络安全漏洞后，工作机构应立即采取紧急措施，控制事态发展，防止事件蔓延；并快速判断事件性质及危害程度，提出初步应对建议；同时，做好事件发生、发展、处置的记录和证据留存。

（四）应急处置流程

1、网络安全事件

发现网络安全事件后，应急响应处置流程如附件 1 所示。工作机构应立即组织先期处置，指派技术人员 2 小时内赶赴现场进行应急处置，在先期处置的基础上，组织力量研究判断事件级别，重大网络安全事件由领导机构组长启动预案并由副组长担任指挥，一般网络安全事件由工作机构组长启动预案并担任指挥，与重要网络与信息系统相关的一般网络安全事件如48小时内未处置完，则升级为重大网络安全事件。应急恢复处置方法详见《浙江省关键信息基础设施网络安全事件应急处置指南（试行）》第 2 节“应急处置”。如有特殊处置要求的，按照附件 4 要求进行。

必要时由外部技术力量或请求市委网信办协调网络安全专家提供支持。

如果我馆发生的网络安全事件和我市其他同类网络安全事件一起升级为特别重大或重大网络安全事件的，按照国家、浙江省网络安全事件应急处置预案处置。

2、高危安全漏洞

本预案高危安全漏洞中的“高危”含义为：CNNVD 编号对应的安全等级为“高危”、“超危”，或者 CVE 编号对应的安全等级为“高危”。

高危安全漏洞应急响应处置流程如附件 2 所示。发现高危漏洞后，先根据漏洞编号查找国家信息安全漏洞或 CVE 漏洞信息库获取漏洞详细描述信息，然后分析漏洞是否已被攻击者利用，如果已被利用则转为网络安全事件应急响应处置流程，如果未被利用，则由工作机构组织力量立即进行打补丁、修改安全策略、关闭必要的端口等安全加固，最后进行漏洞修复验证，有条件的应聘请第三方安全服务公司对已修补的漏洞进行安全性验证。

五、后期处置

（一）整改和预防

工作机构对网络安全事件的原因、经过，以及对应处置的方法、措施进行分析和总结。对系统功能、安全机制、管理规定、应急预案进行改进，防止同类事件再次发生。

（二）总结和报告

属较大网络安全事件的，工作机构应综合相关结果向市委网

信办提交完整的网络安全事件总结和调查报告，总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施，事件的总结和报告原则上应在应急响应结束后 20 天内完成。

六、保障措施

（一）应急物资保障

在信息化经费中，安排一定的资金用于预防或应对信息安全突发事件，提供必要的常备冗余设备，优化信息安全应急处理工作的物资保障条件。

（二）技术支撑保障

建立和完善机房“云”运维机制，7*24 小时实时监测 UPS 参数、空调温湿度和蓄电池状况，进一步相关网络安全事件响应速度和处置能力。建立应急技术资料档案并及时更新，包括网络拓扑结构、重要系统或设备的型号及配置、主要设备厂商信息、使用维护信息，以保证与实际系统的一致性。

（三）合作机制建设

工作机构应与相关管理部门、安全设备和安全服务厂商、设备及服务提供商、软件开发商、电信、电力等支持单位保持联络与协作，以确保在网络安全事件发生时能及时获得适当外部技术支持。

七、预防工作

（一）培训

工作机构应当定期组织技术人员和各处室相关人员开展基础

网络与信息安全应急管理、应急处置等培训，提高信息化管理人员、应急处置人员、系统使用人员防范意识及技能。监督和指导软件开发商和系统集成商等运维单位提高安全运维水平。

（二）演练

工作机构应每两年组织一次网络与信息系统安全演练。模拟处置影响较大的网络安全事件，检验预案的可执行性。通过演练，及时发现和改进应急体系和工作机制存在的问题，完善应急预案，提供应急处置能力，检验应急物资的完好情况。

（三）评估

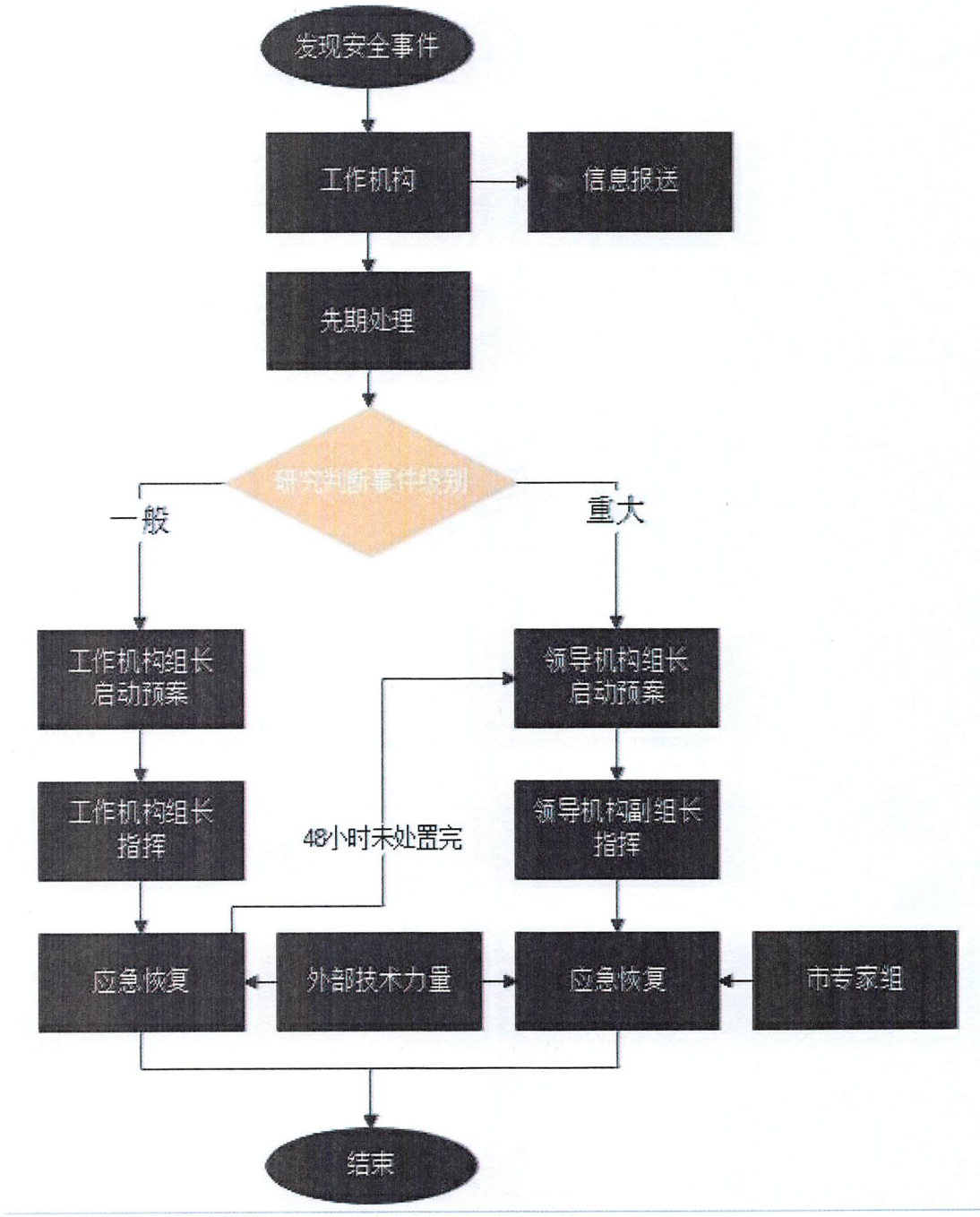
工作机构应定期聘请专业安全公司对网络和重要信息系统进行安全评估，针对我馆网络、系统、应用、业务提供全面的安全检测，发现存在的安全隐患，并提供详细的整改建议。同时，根据市委网信办、市公安局、市经信局等部门要求，做好年度网络安全自查、自评等相关工作。

宁波市档案馆

2020年4月30日

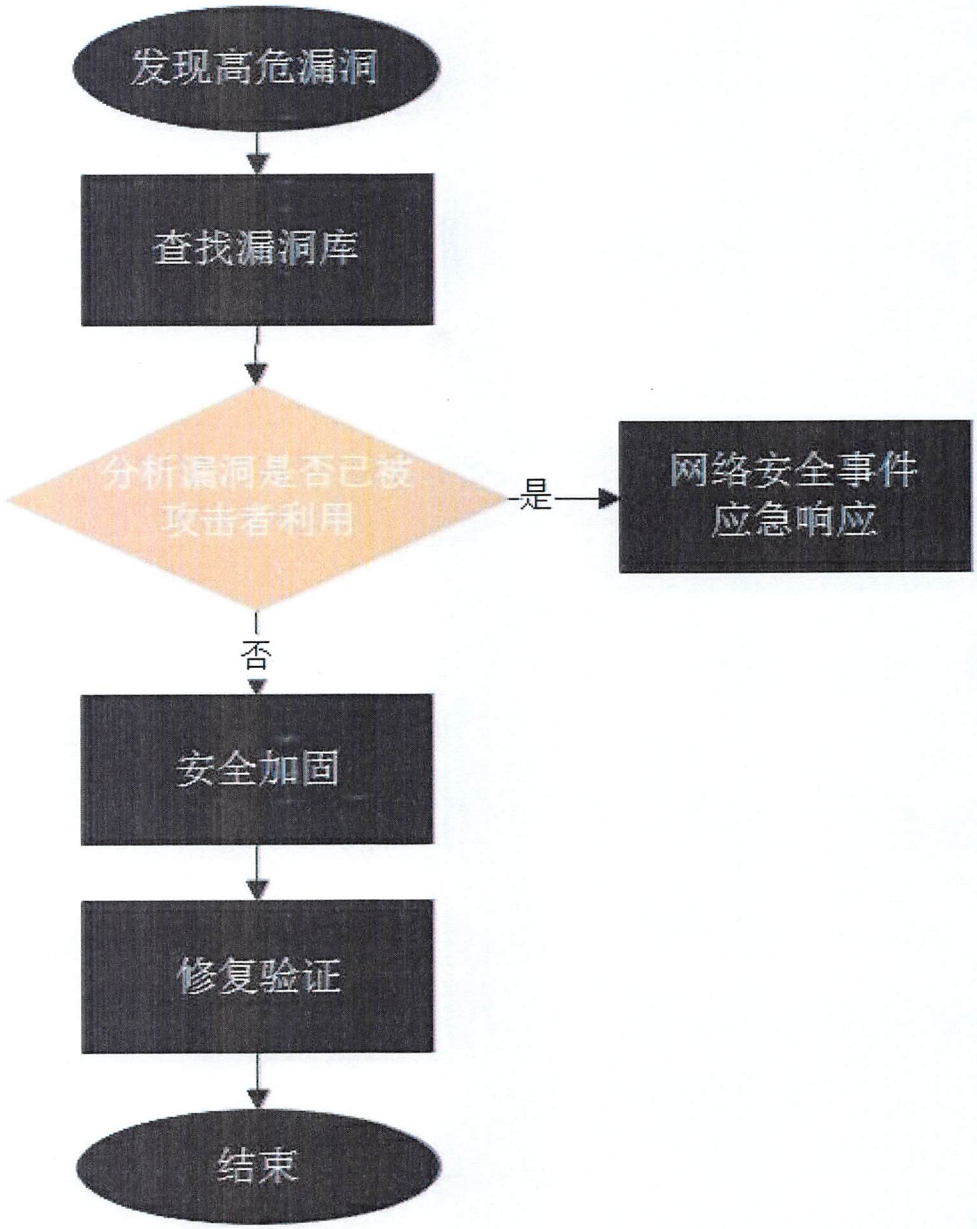
附件 1

网络安全事件应急响应处理流程图



附件 2

高危安全漏洞应急响应处置流程



附录 3

宁波市网络安全事件信息报告表

报告时间：　年　月　日　时　分　　签发人：

报告单位		联系人	
联系电话 （含手机）		传　真	
初判事件类型	□有害程序事件 □网络攻击事件 □信息破坏事件 □设备设施故障 □灾害性事件 □其他事件 □尚无法判定		
初判事件来源	□网信部门 □公安部门 □通管部门 □本单位　□其他		
初判事件级别	□特别重大 □重大 □较大 □一般 □其他		
事发单位及事发网络和信息系统功能描述			
事发时间、事态发展简要经过及初判原因			
事件影响范围和危害（影响程度、影响人数、经济损失等情况）			
已采取的措施及效果			
请求事项及工作建议			
备注			

附件 4

网络安全事件分级分类和特殊处置对照表

序号	内容	分级	分类	特殊处置
1	未开放电子档案发生大规模泄露的	较大	有害程序、网络攻击、信息破坏	检查磁带备份
2	集中保存国家秘密信息、重要敏感信息的信息系统数据被窃取、篡改、假冒的		有害程序、网络攻击、信息破坏	检查磁带备份
3	遇到台风等不可抗力或黑客攻击造成较严重影响的		灾害性事件	
4	机房发生故障	一般	设备设施故障	
5	宁波档案网故障		有害程序、网络攻击、信息破坏、信息内容安全、设备设施故障、灾害性事件	立即断网
6	数字档案馆系统故障		有害程序、网络攻击、信息破坏、设备设施故障、灾害性事件	维保单位到现场
7	办公自动化系统故障		有害程序、网络攻击、信息破坏、设备设施故障、灾害性事件	