佛山市联合图书馆体系指导性技术文件

FSUL/Z 60—2024

网络信息安全应急处理规范

（报批稿）

2024 - XX - XX 发布　　2024 - XX - XX 实施

佛山市文化广电旅游体育局 发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由佛山市文化广电旅游体育局提出并归口。

本文件起草单位：

本文件主要起草人：

网络信息安全应急处理规范

1 范围

本文件规定了网络信息安全应急处理的事件划分、机构和职责、事件预防、应急处理、事件报告的要求。

本文件适用于联合图书馆体系的网络信息安全应急处理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

FSUL/Z 2 联合图书馆体系术语

3 术语和定义

FSUL/Z 2 界定的术语和定义适用于本文件。

4 事件划分

4.1 事件分类

网络信息安全事件主要分为以下四类：

a) 人为破坏：指网络线路、通信设施被人为破坏，以及恶意程序、网络攻击、数据篡改假冒、违规操作等引起的网络与信息系统的损坏。

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

c) 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。

d) 其他事件：指未归为上述分类的网络安全事件。

4.2 事件分级

根据业务系统和数据保障要求，按照事件严重程度和影响范围等因素，分为特别重大事件、重大事件、较大事件和一般事件 4 个级别，由高到低分别为Ⅰ级、Ⅱ级、Ⅲ级和Ⅳ级：

a) 特别重大事件（Ⅰ级）为：

1) 特别重要信息系统和网络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。

2) 其他对社会秩序、经济建设和公众利益造成特别严重社会影响的网络安全事件。

b) 重大事件（Ⅱ级）为：

1) 重要信息系统和网络遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

2) 其他对社会秩序、经济建设和公众利益造成严重社会影响的网络安全事件。

c) 较大事件（Ⅲ级）为：
   1) 信息系统和网络遭受较大的系统损失，造成系统中断，明显影响系统效率。
   2) 其他对社会秩序、经济建设和公众利益造成较严重影响的网络安全事件。
d) 一般事件（Ⅳ级）为：
   除上述情形外，对社会秩序、经济建设和公众利益构成一定威胁、造成一定社会影响的网络安全事件，为一般网络安全事件。

5 机构和职责

5.1 机构

5.1.1 中心馆、区总馆应组建本单位的网络信息安全领导小组和工作小组，负责本单位的网络信息安全应急处理工作。

5.1.2 中心馆、区总馆应共同组建联图系统安全应急处理小组，负责联图系统的网络信息安全应急处理工作。

5.1.3 其他成员馆应指定专人配合开展网络信息安全应急处理工作。

5.2 职责

5.2.1 网络信息安全领导小组

工作内容包括但不限于：
a) 负责本单位网络信息安全应急响应工作的整体规划、组织协调和决策指挥；
b) 负责向主管部门和公安机关汇报应急处理进展情况和总结报告；
c) 组织、协调和指导网络信息安全的宣传、普及教育工作。

5.2.2 网络信息安全工作小组

工作内容包括但不限于：
a) 负责贯彻落实网络信息安全领导小组关于网络信息安全工作的要求和规定；
b) 负责定期检查网络信息安全状况，当出现安全事件时，对发生的安全事件及时上报，并配合相关的调查和纠正工作；
c) 应定期组织演练，检验应对网络安全事件的能力、应急工作的准备情况及各部门的协同配合；
d) 负责对内部人员进行网络信息安全的教育、培训，提高内部人员的网络信息安全意识。

5.2.3 联图系统安全应急处理小组

工作内容包括但不限于：
a) 负责按照本文件第 7.1 条响应并处理网络信息安全事件；
b) 通报与联图系统相关的网络信息安全事件；
c) 决定联图系统应急预案的启动，负责现场指挥，并组织相关人员排除故障，恢复系统。

6 事件预防

6.1 中心馆

中心馆按照职责落实好以下预防措施：

a) 贯彻落实国家网络安全等级保护制度，开展联图系统安全等级保护测评工作；
b) 制定和完善各项信息安全管理制度，规范信息安全日常管理工作；
c) 制定专项应急预案，健全网络信息安全事件通报机制，每年至少开展一次预案演练；
d) 进行网络信息安全风险评估，识别安全风险，及时整改消除隐患，预防安全事件的发生；
e) 做好系统安全加固、补丁升级和系统备份等工作，预防故障和网络安全事件发生；
f) 配备防火墙、防病毒软件、入侵监测系统等安全设备，监测各类网络安全事件发生；
g) 每年应开展一次网络安全培训，将网络安全事件的应急知识列为工作人员的培训内容，加强网络安全特别是网络安全应急预案的培训，增强防范意识；
h) 在国家和省重要活动、会议期间，加强网络安全监测和分析研判，及时预警可能造成重大影响的风险和隐患。

6.2 区总馆

区总馆按照职责落实好以下预防措施：

a) 贯彻落实国家网络安全等级保护制度，开展本单位重要信息系统安全等级保护测评工作；
b) 制定和完善各项信息安全管理制度，规范信息安全日常管理工作；
c) 做好系统安全加固、补丁升级和系统备份等工作，预防故障和网络安全事件发生；
d) 每年应开展一次网络安全培训，将网络安全事件的应急知识列为工作人员的培训内容，加强网络安全特别是网络安全应急预案的培训，增强防范意识；
e) 在国家和省重要活动、会议期间，加强网络安全监测和分析研判，及时预警可能造成重大影响的风险和隐患。

6.3 镇街分馆

镇街分馆按照职责落实好以下预防措施：

a) 制定和完善计算机管理制度，规范工作人员和读者使用计算机终端的行为，定期对计算机终端进行病毒查杀，保障计算机终端安全；
b) 制定和完善网络管理制度，规范网络接入控制、访问控制、网络使用行为；
c) 配合中心馆开展的联图系统弱口令专项整治工作；
d) 每年宜参与一次网络安全培训，增强防范意识；
e) 在国家和省重要活动、会议期间，及时预警可能造成重大影响的风险和隐患。

7 应急处理

7.1 应急处理程序

7.1.1 网络信息安全工作小组在确认安全事件发生后，做好先期应急处理工作并立即采取措施控制事态，必要时采用断网、关闭服务器等方式防止事态进一步扩大，初步估计安全事件造成的损失，保留相关证据，对安全事件进行分类和定级后，上报网络信息安全领导小组决定是否启动应急预案。

7.1.2 联图系统及相关联的信息系统发生重大事件（Ⅱ级）或特别重大事件（Ⅰ级）时，相关单位应立即报告中心馆、区总馆的信息安全工作小组，及时应对处理。

示例：如区总馆与联图系统数据接口有对接的某业务软件系统突然发生大量读者个人敏感数据泄露的信息安全事件时，区总馆应立即向中心馆的信息安全工作小组报告。

7.1.3 应急预案启动时，有关人员应及时到位，进行现场保护。应采取手工记录、截屏、文件备份和影像设备记录等多种手段，对应急处理的步骤和结果进行详细记录，协助调查取证和系统恢复等工作。

7.2 其他应急处理措施

不同分类的网络安全事件应采用针对性的应急处理措施，各成员馆应判断网络安全事件的分类和级别，结合单位内部情况及预制的应急预案，采用最有效的处理措施加以实施。

7.3 人为破坏应急处理措施

7.3.1 恶意程序事件紧急处理措施

7.3.1.1 当发现有计算机被感染上病毒后，应立即进行网络隔离，并向信息安全相关负责人报告。
7.3.1.2 信息安全相关负责人在接到通报后应立即赶到现场。
7.3.1.3 对该设备的硬盘进行数据备份。
7.3.1.4 启用反病毒软件对该机进行杀毒处理，同时通过病毒检测软件对其他机器进行病毒扫描和清除工作。
7.3.1.5 如果现行反病毒软件无法清除该病毒，应立即向本单位网络信息安全领导小组报告，并迅速联系有关产品商研究解决。

7.3.2 网络攻击事件紧急处理措施

7.3.2.1 当发现遭受网络攻击并严重影响工作环境时，首先将被攻击的服务器等设备从网络中隔离出来，保护现场，并将有关情况向本单位网络信息安全领导小组汇报。
7.3.2.2 信息安全相关负责人应在接到通知后立即赶到现场，对现场进行分析，并做好记录，必要时上报主管部门。
7.3.2.3 恢复与重建被攻击或破坏的系统。
7.3.2.4 网络信息安全领导小组召开会议，如评定为III级及以上安全事件，则立即向公安部门报警。

7.3.3 网站、网页出现非法言论事件紧急处理措施

7.3.3.1 信息安全部门值班人员定期监视网站、网页信息内容。
7.3.3.2 网站、网页内容被篡改或出现非法信息时，值班人员应立即向本单位信息安全相关负责人通报情况；情况紧急的，首先中断服务器网络连接，再按程序报告。
7.3.3.3 信息安全相关负责人应在接到通知后立即赶到现场，做好必要记录，清理非法信息，妥善保存有关记录及日志或审计记录，强化安全防范措施，并将网站、网页重新投入使用。
7.3.3.4 追查非法信息来源，并将有关情况向本单位网络信息安全领导小组汇报。
7.3.3.5 网络信息安全领导小组召开会议，如认为事态严重，则立即向公安部门报警。

7.3.4 软件系统遭破坏性攻击的紧急处理措施

7.3.4.1 重要的软件系统平时必须存有备份，与软件系统相对应的数据必须按本单位容灾备份规定。
7.3.4.2 一旦软件遭到破坏性攻击，应立即向信息安全相关负责人报告，并将该系统停止运行。
7.3.4.3 检查信息系统的日志等资料，确定攻击来源，并将有关情况向本单位网络信息安全领导小组汇报，再恢复软件系统和数据。
7.3.4.4 网络信息安全领导小组召开会议，如评定为III级及以上安全事件，则立即向公安部门报警。

7.4 事故灾难应急处理措施

7.4.1 电力中断应急处理措施

7.4.1.1 馆内线路故障，应通知维修人员迅速恢复。

7.4.1.2 馆外线路故障，值班人员应立即向信息安全部门负责人汇报情况，宜做如下安排：

a) 预计停电 1 小时以内，由 UPS 供电；

b) 预计停电 1～4 小时，关掉非关键设备，确保各主机、路由器、交换机供电；

c) 预计停电超过 4 小时，白天工作时间关键设备运行，晚上所有设备停机。

7.4.2 数据库故障应急处理措施

7.4.2.1 主要数据库系统应定时进行数据库备份。

7.4.2.2 一旦数据库崩溃，应立即进行数据及系统修复。

7.5 自然灾害应急处理措施

当发生的灾害为自然灾害时，应根据当时的实际情况，在保障人身安全的前提下，首先保障数据的安全，然后是设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

8 事件报告

8.1 收集信息

8.1.1 应及时收集相关信息，包括事件发生时间、地点、涉及的系统、涉及的用户等。

8.1.2 宜拍照或录像记录事件过程。

8.2 反馈信息

8.2.1 整理收集到的信息，并及时向成员馆的网络信息安全工作小组反馈。

8.2.2 反馈内容应包括事件的简要描述、紧急程度评估、可能的影响范围等。

8.3 事件确认

网络信息安全工作小组对收到的反馈信息进行分析和评估，确认其是否为真实的信息安全事件，并及时作出回复。

8.4 事后调查处理

8.4.1 安全事件应急处理结束后，应组成事件调查组对安全事件进行调查，形成事件调查报告，由网络信息安全工作小组按规定上报。

8.4.2 调查要准确、及时、公正地查清事件性质、原因和责任，并对责任者提出处理意见。

8.5 事后整改

事件相关部门应组织研究网络信息系统各类安全事件发生的原因和特点，综合分析网络信息系统中存在的关键点和薄弱点，及时总结应急响应工作的经验和教训，提出整改措施，制定整改实施方案并予以落实。

参 考 文 献

[1] GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南
[2] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 38645-2020 信息安全技术 网络安全事件应急演练指南
[4] LD/T 04-2022 人力资源社会保障网络安全监测和应急处置规范