档案信息安全事件应急响应预案的编制要点

摘　要：编制档案网络与信息安全事件应急响应预案是为了有效防范档案信息系统在进行业务处理、运行管理和内部控制过程中产生的风险，预防和减少突发事件造成的危害和损失。文章从 5 个方面就档案信息安全事件应急响应预案的编制要点加以论述。

关键词：档案信息　安全　应急　预案　编制

◇ 崔振玲

为有效防范档案信息系统在业务处理、运行管理和内部控制过程中产生的风险，预防和减少突发事件造成的危害和损失，建立健全档案信息系统突发事件应急机制，提高档案网络与信息安全事件应急处理和保障能力，保证应急指挥调度工作迅速、高效、有序进行，及时处置档案网络及信息安全事件，确保档案网络与信息系统安全、持续、稳定运行。笔者结合多年工作经验，就档案信息安全事件应急响应预案的编制方法作以简要探讨。

1.明确组织体系和职责。档案信息系统应急组织指挥体系一般由领导机构、日常办事机构及现场应急处理工作组组成。领导机构组长一般由单位主要负责人担任，副组长由单位分管信息化的领导担任。职责是：⑴ 全面负责档案信息系统应急管理的领导工作，统一协调和组织开展档案信息系统应急管理工作，部署和指导应急预案和各项制度的建设。⑵ 发生特别重大档案信息系统突发事件时，负责启动本预案，下达应急保障任务，指挥应急保障行动，及时向相关部门报告有关情况。⑶ 规划和制订档案信息系统应急保障策略，研究和评估应急体系和实施成效，部署和督查各项应急计划、培训、演练等事宜。⑷ 对应急方案的实施、计划和预算进行审议和决策。对每次实施应急预案后的应急情况及时进行总结和分析，并对实施情况进行评估。

2.明确安全事件分级原则和等级划分。遵循《信息安全技术信息安全事件分类分级指南（GB/Z 20986- 2007）》，分级原则一般为：⑴ 影响因素，包括档案信息系统的重要程度、社会影响和资产损失等。⑵ 从高原则，按相对较高一级突发事件处理。⑶ 升级原则。在处置过程中事态和影响进一步扩大时，达到上一级标准的，应作升级处理。根据安全事件的影响程度，安全级别从低到高分为预警预报事件（IV级）、一般突发事件（III 级）、重大突发事件（II 级）、特别重大突发事件（I 级）。

3.明确预防措施。目前，信息安全预防主要技术手段为：⑴ 边界防护：采用防火墙入侵防御等安全设备，实行内外网的物理隔离等。⑵ 病毒安全防范：计算机设备均应配备正版的防病毒软件。⑶ 软件系统安全防范：计算机和网络设备必须使用正版操作系统和应用软件，杜绝使用盗版软件，对开发的应用软件进行安全性能评估。⑷ 数据安全防范：建立相应的数据备份、恢复机制，原则上备份介质的存储不能与主机系统在同一地域。⑸ 设备安全防范：采购的计算机设备都必须有较高的可靠性，尤其是主机、服务器及中心网络设备、网络安全设备等关键设备都要有冗余备份或相应配件。

4.明确应急响应等级和基本流程。档案信息系统应急保障和恢复响应行动一般划分为 4 个响应等级。⑴ I 级响应：当出现 I 级突发事件，由应急领导小组决定启动 I 级保障应急预案，由应急办发布全局性应急通告，单位进入临时应急处理状态，并及时向当地公安部门报告，争取支援。⑵ II 级响应：当出现 II 级突发事件，由应急办决定启动 II 级保障应急预案，并及时向应急领导小组报告，由应急办发布全局性应急通知，单位进入应急预备状态，并及时向当地信安办和公安部门网警机构报告。⑶ III 级响应：当出现 III 级突发事件，由技术部门决定启动 III 级保障应急预案，并及时向应急办报告，各事发相关部门进入应急处理状态。⑷ IV 级响应：当出现IV级突发事件，由技术部门启动IV级保障应急预案，并及时发出预警预报，隐患消除后取消预警预报。突发事件发生后，应急保障工作要分轻重缓急，按照“先核心、后外围，先对外服务，后对内服务”的原则组织实施，实行一盘棋策略，按规定、流程有序进行。应急预案启动后，应急领导小组应迅速了解事件的基本情况和先期处置情况，并部署应急办组织相关应急业务小组和职能部门按预案部署处置方案，责成各方严格按照应急联动和职责分工，立即开展处置和保障工作，确保组织到位、应急保障措施到位、应急保障设备和应急保障人员到位，控制事件的蔓延和发展。现场应急处理时应尽最大可能收集事件相关信息，明确事件类别，确定事件来源，保护证据，以便缩短应急响应时间。主要措施：⑴ 检查威胁造成的结果，评估事件带来的影响和损害。如检查系统、服务、数据的完整性、保密性或可用性，检查攻击者是否侵入了系统，以后是否能再次随意进入等。⑵ 抑制事件的影响进一步扩大，限制潜在的损失与破坏。可能的抑制策略一般包括：关闭服务或所有的系统，从网络上断开相关系统，修改防火墙和路由器的过滤规则，封锁或删除被攻破的登录账号，阻断可疑用户得以进入网络的通路，提高系统或网络行为的监控级别，设置陷阱，启用紧急事件下的接管系统，实行特殊“防卫状态”安全警戒，反击攻击者的系统等。⑶ 根除。在事件被抑制之后，通过对有关恶意代码或行为的分析结果，找出事件根源，明确相应的补救措施并彻底清除。与此同时，执法部门和其他相关机构将对攻击源进行定位并采取合适的措施将其中断。⑷ 清理系统、恢复数据、程序和服务。把被攻破的系统和网络设备彻底还原到它们正常的任务状态。恢复工作要十分小心，应避免出现误操作导致数据的丢失，对涉密系统特别需要遵照涉密系统的恢复要求，以加强信息安全保密工作。

5.明确后期处置办法。⑴ 核实突发事件造成的各种损失。⑵ 落实资金、设备和技术保障，做好各项恢复工作，确保档案信息系统的正常运行。⑶ 根据损坏设备的情况，及时做好相关设备的补充和备份。时间要求是在 I 级突发事件发生后的一星期内，应急办必须向应急领导小组提交书面分析报告；在 II 级、III 级突发事件发生后的一星期内，各应急业务小组必须向应急办提交书面分析报告。

[责编　赵晶莹]