Q/SYY

中 科 大 数 据 研 究 院 企 业 标 准

Q/SYY BZ202.04—2022

数据安全事件应急预案

Emergency Plan for Data Security Incidents

2022－07－15 发布　　2022－08－01 实施

中科大数据研究院　　发 布

数据安全事件应急预案

1 范围

本文件规定了中科大数据研究院数据安全事件应急响应组织机构、处置、应急保障等内容。本文件适用于中科大数据研究院数据安全事件应急处理。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

本文件没有需要界定的术语和定义。

4 应急响应组织机构

4.1 数据安全事件应急响应领导小组

组织构成与职责如下：

数据安全事件应急响应领导小组组长由副院长担任，组长的职责主要有：

1) 负责应急响应的整体协调、指挥和领导工作。
2) 监督总体应急管理流程的有效执行。
3) 负责应急响应处置总体决策。
4) 负责数研院数据安全应急事件的上报。

4.2 安全应急响应技术专家

由安全大数据中心副主任担任安全应急响应技术专家，职责主要有：

1) 对重大数据安全事件进行评估，提出启动应急响应的建议。
2) 研究分析数据安全事件的相关情况及发展趋势，为应急响应提供咨询或提出建议。
3) 分析数据安全事件原因及造成的危害，为应急响应实施提供建议支持。

4.3 应急响应安全技术小组

由安全大数据中心技术人员组成应急响应安全技术小组，其职责主要有：

1) 分析应急响应需求(如风险评估、业务影响分析等)。
2) 编制应急预案文档。
3) 实施应急响应，如应急事件的分析排查、溯源等。
4) 进行应急预案测试、培训、演练等。
5) 总结应急响应工作，提交应急响应总结报告。

4.4 应急响应恢复人员

由运维部门技术人员担任应急响应恢复人员，主要职责有：

1) 进行业务系统的灾难恢复。
2) 系统备份与恢复的日常管理。

3) 参与应急预案的测试、培训、演练等。
4) 数据安全事件发生时的损失控制和损害评估。

5 数据安全事件处理

5.1 数据泄露事件

数据泄露事件指的是系统由于受到外部攻击或者内部人员故意泄密等原因，造成的数据泄露事件。

1) 紧急措施：发现有数据泄露时，应报告数据安全事件应急响应领导小组，由应急响应领导小组组织协调人员进行检查，及时防止数据泄露范围扩大影响。
2) 抑制处理：由应急响应日常运行部门组织排查系统及数据库、应用系统等相关日志，及时下线或切断相关业务系统外联网络，并保留证据，必要时公安机关介入。
3) 根除：应急响应领导小组组织协调相关部门、厂商工作人员对业务系统和相关日志进行检查，分析事件原因，并进行总结。

5.2 数据篡改事件

数据篡改事件，如业务系统不具有数据完整性保护能力，无法确保重要数据不被篡改，从而可能导致的重要数据被篡改的安全事件。

1) 紧急措施：发现核心数据库数据或业务系统大规模被篡改后，应立即报送数据安全事件应急领导小组，由应急响应领导小组指定数据库管理员或运维人员进行检查确认，同时启动应急预案，暂停相关业务服务，并通知相关业务中心。
2) 抑制处理：使用备份数据恢复数据后重新启动服务，并立即迫查原因。如属外部攻击原因的，应立即通过日志等分析攻击来源，必要时请公安机关介入。
3) 根除：总结经验教训，分析具体原因核，加固核心数据库系统安全，并报领导小组。

5.3 数据丢失事件

数据丢失事件，比如业务系统数据库或业务系统文件、办公文件数据等被非法删除。

1) 紧急措施：当发现数据丢失时，应立即报告数据安全事件应急响应领导小组，由应急领导响应小组统一指挥，组织协调相关部门进行检查，排查数据丢失影响范围，评估对业务的影响。
2) 抑制处理：应急响应领导小组立即组织相关业务部门、数据安全工程师等进行解决，从近的有效备份恢复数据及业务系统服务等。
3) 根除：总结经验，分析具体原因，加固涉敏数据安全处理，并报告应急领导小组。

5.4 敏感数据泄露事件应急响应处理

敏感数据包括：用户个人信息相关数据、用户服务内容相关数据、企业运营管理相关数据等，当发生数据泄露事件时，各系统应组织人员对事件进行确认，评估事实与事件影响范围，并启动应急处置措施。

敏感数据泄露事件应急流程如下：

数据备份还原工具、数据恢复工具、日志分析工具、数据库审计系统等。

应急步骤：

1) 应急启动，当发现黑客通过网络攻击窃取核心信息、内部员工或合作伙伴人员利用职务之便窃取机密信息、监控部门发现数据泄露等情况时，启动应急预案。
2) 数据泄露确认，当发现数据泄露时，立即组织人员核实欵据泄露情况，确认数据泄露影响范围，并定位数据库IP、关联业务等，根据泄密的用户信息判断哪些业务的用户信息被泄露。
3) 应急处置

如有备份系统，应迅速切换到备用系统，并将在线设备脱网，作好安全审计及系统恢复的准备。

若无备份系统，则请示应急领导小组组长将相关系统进行下线处理，防止数据进一步泄露。

4) 事件排查分析

通过将遭受攻击的主机上系统日志、应用日志等导出备份，并加以分析判断。

进一步分析系统日志、数据库日志等，确定安全事件发生的原因、窃取过程及可能造成的影。

若发现是内部员工或支撑厂商人员造成数据泄露，必要情况下，立即组织人员现场开展调查，通过分析内部员工或支撑厂商计算机的系统痕迹记录(浏览器痕迹、软件使用痕迹、U盘使用痕迹等)，进一步收集和分析相关证据。

日志分析外，还应分析数据收集链路、数据下载、数据分发等情况的审批记录，进一步分析处置措施，确认安全事件发生的原因、窃取过程及可能造成的影响。

5) 风险消除

及时修复发现的安全漏洞。

对数据进行加密传输，根据数据敏感级别进行加密存储，并对前台敏感数据进行脱敏处理。

定期开展数据安全流程制度落实情况安全检查及漏洞检查。

定期组织内部员工、支撑厂商人员开展安全意识培训。

定期开展安全合规检查和安全审计工作。

6 安全事件应急保障

应急响应保障是数据安全应急预案的重要组成部分，是保证数据安全事件发生后能够快速有效地实施应急预案的关键要素。

人力保障：人力保障由数据安全事件应急响应领导小组统一规划和管理。数据安全应急保障人员，详见附件。

技术保障：通过建立应急响应安全技术小组来进行为应急响应技术保障，应急响应领导小组应依据应急响应的需要，制定数据安全事件技术应对表，全面考察和管理相关技术基础，选择合适的技术服务者，明确职责和沟通方式。定期开展数据安全相关技术研究，不断完善“事前可防范、事中可阻断、事后可追溯”的数据安全技术保障体系，开展对数据安全事件的预警、预测、预防和应急处理的技术研究，加强技术储备。

物质保障：包括通信保障、资金保障等，应急响应工作中产生的所有物质、资金需求由应急响应领导小组统一统筹提供。