KINGFA

信息安全应急预案

信息安全应急预案

信息中心

2024 年 10 月

KINGFA

文档修订记录表

文档版本号	V1.0
修订者	谢栩键
修订内容要点	首次编制
审核者	周盛佳
批准者	顾均勇
批准日期	2024 年 10 月 15 日

信息安全应急预案

目录

1 说明..... 1

2 编制目的..... 1

3 编制依据..... 1

4 适用范围..... 1

5 组织架构与职责..... 1

6 应急响应程序..... 3

6.1 应急响应流程..... 3

6.2 应急升级流程..... 4

6.3 技术处理流程..... 5

7 应急处置结果及上报..... 6

8 预防和预警..... 6

9 附录..... 7

9.1 附录 1：勒索病毒应急预案..... 7

9.2 附录 2：邮件安全应急预案..... 8

9.3 附录 3：数据泄漏应急预案..... 9

9.4 附录 4：应用系统被攻击篡改应急预案..... 10

9.5 附录 5：应急人员联系方式..... 11

信息安全应急预案

1 说明

表 1-1 应急预案说明

预案编号	KF-YJ-007
预案名称	信息安全应急预案
适用范围	本预案作为集团应急预案体系的第三级执行指导性文件，用于金发科技内部发生信息安全事件时的应急响应工作
涉及部门	应急组织、信息中心、应用系统责任部门、本地安全服务商

2 编制目的

为提高金发科技股份有限公司信息安全事件应急处置能力，加强信息安全保障工作，形成科学、有效、反应迅速的应急工作机制，确保重要公司信息系统等实体安全、运行安全和数据安全，最大限度地减轻突发信息安全事件的危害。

3 编制依据

根据《中华人民共和国计算机信息系统安全保护条例》、《互联网信息服务管理办法》、《计算机病毒防治管理办法》等相关法规、规定、文件精神，制定本预案。

4 适用范围

本预案适用于金发科技股份有限公司各分子公司、部门的信息安全事件。

5 组织架构与职责

表 2-1 人员职责表

序号	应急人员/组织	职责定义
1	应急领导小组	总体指挥和决策
2	信息安全组	负责安全事件的原因分析和方案策略制定 安全事件完整应急过程的执行

信息安全应急预案

		安全事件汇报和归档
3	网络组	协助信息安全组排查网络层面的攻击定位 根据处置方案配置网络访问控制策略 防火墙等网络资源的配置处理
4	服务管理组	提供终端的运行状态分析 协助信息安全组对终端攻击记录进行溯源分析 终端的配置及恢复操作
5	数据中心组	提供应用系统的运行状态分析 协助信息安全组对服务器攻击记录进行溯源分析 数据的配置及恢复操作
6	本地安全服务提供商	作为二线支持提供应急技术支持 对应急事件进行深入调查，协助解决事件、对事件溯源 提供安全加固建议方案
7	当事人	提供信息安全事件经过 协助信息安全组配合调查、执行相关工作
8	当事人部门领导	协助信息安全组配合执行相关工作
9	保密专员	协助信息安全组配合调查、执行相关工作

表 2-2 人员组成表

序号	应急组织	人员组成
1	应急领导小组	一级事件：CEO、CIO、基地总经理 二级事件：信息中心部长、应用系统相关部门长 三级事件：信息中心主管、应用系统相关部门主管
2	应急处置小组	一级事件：信息中心部长、主管、相关模块组长、保密办公室主任、保密专员 二、三级事件：信息中心相关主管、相关模块组长
3	对外联系人	信息中心主管、安全组长

信息安全应急预案

6 应急响应程序

6.1 应急响应流程

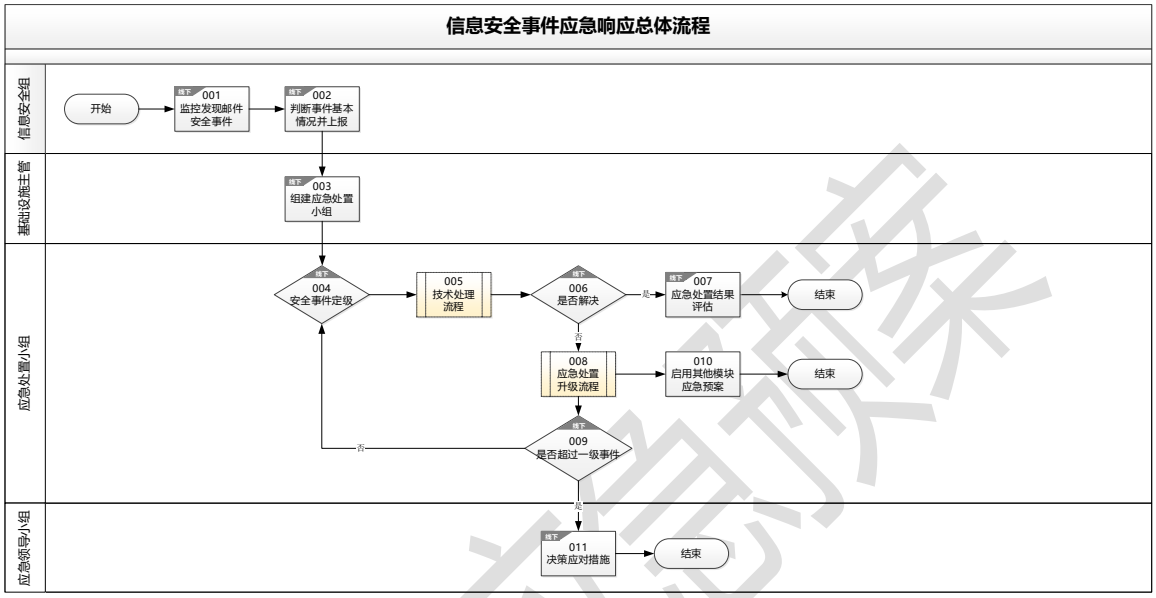


图 6-1 信息安全事件应急响应总体流程

1、发现信息安全事件（可由其他人员报障或信息安全小组主动发现），由信息安全组判断攻击基本情况并上报；

2、基础设施主管根据汇报信息，组建应急处置小组，将实施人员、系统责任部门或使用部门、基础设施组等人员纳入。

3、分析攻击影响情况，参考二级文件进行定级。

4、如果攻击在可控范围内，信息安全组与网络组及时控制，隔离攻击对象消除隐患；

5、启动技术处置流程（见 6.3 技术处理流程）。

6、未解决的话按照升级流程进行升级，根据二级文件的定义判断是否需启动其他应急预案；

7、应急响应人员恢复遭受攻击的系统；追查非法来源，消除安全隐患；

8、事件回顾、跟踪和总结，调整安全策略，加强防范措施；

9、信息安全小组与应用系统责任人/部门共同评估损失，归档记录；

10、应急结束。

信息安全应急预案

6.2 应急升级流程

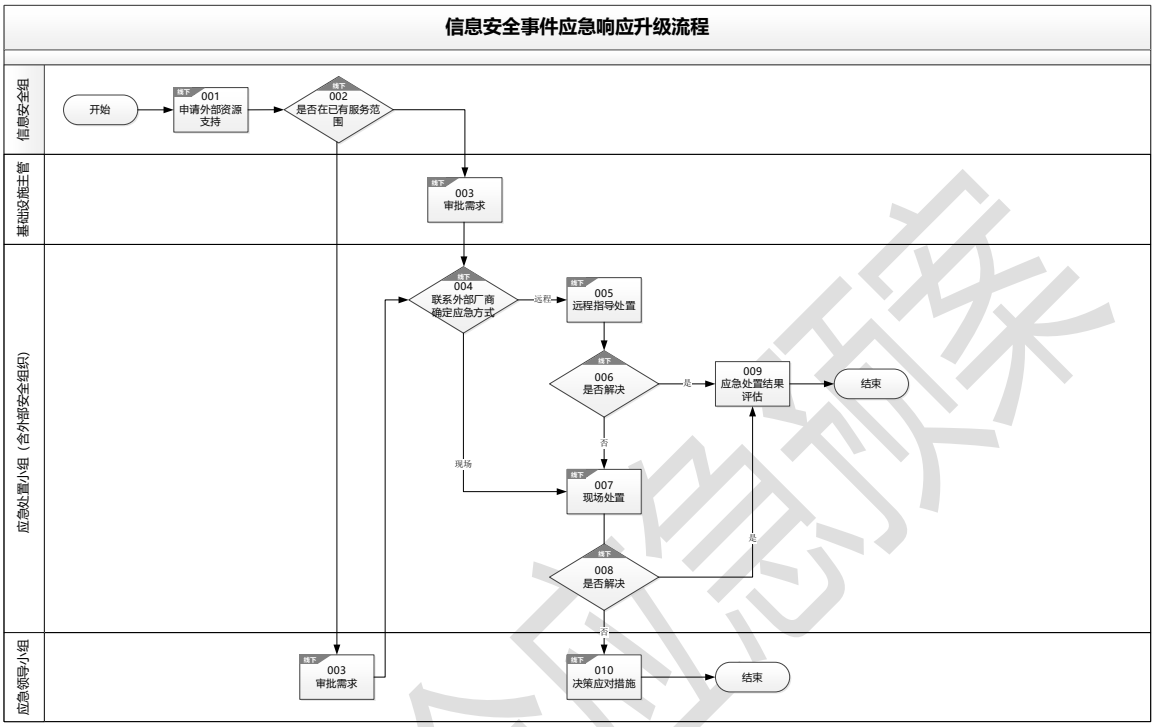


图 6-2 信息安全事件应急响应升级流程

1、由信息安全组判断是否需要向申请外部资源技术支持，填写《应急响应支持申请单》若已购或有外部服务时，由基础设施主管审批即可，若无相关服务且需产生费用时，需提交应急领导小组审批；

2、无法通过远程应急支持、远程指导解决，应急升级，向请求现场应急支持；

3、通过外部高级技术支持，阻断或隔离攻击，并清理已感染区域，恢复被攻击应用系统，结束应急升级流程。

信息安全应急预案

6.3 技术处理流程

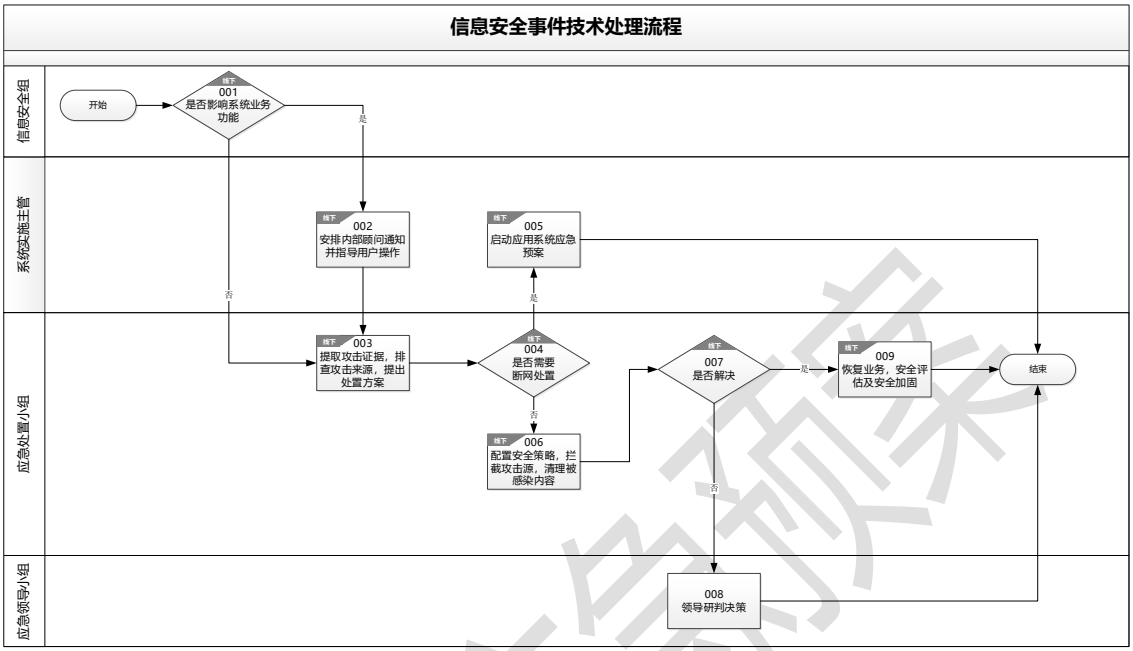


图 6-3 信息安全事件技术处置流程

1、 发现信息安全事件时，启用信息安全应急预案，信息安全组和模块系统负责人判断是否影响系统业务功能；

2、 若对业务系统造成功能影响，由内部联络组及内部顾问通知业务部门做好手工替代，暂时断开与网络的连接，应用系统脱机运行，达到应用系统预案启动条件时，需同步启动其他模块系统的应急预案；当发生大范围感染事件，应由信息安全组立即开展全集团通知，并联调保密专员配合执行相关事项；

3、 若不对业务系统造成功能影响，则由内部应急小组对应用系统进行溯源分析和定位攻击来源，并提出处置方案；

4、关闭被攻击/破坏的系统，提取现场证据，手工恢复被破坏内容，封堵攻击的来源途径，应急处置小组检查是否完成解决，若无法解决需上升至应急领导小组进行研判决策；

5、通过处置方案解决消除信息安全事件后，试运行恢复应用系统并进行安全评估和安全加固，最后结束事件处理。

信息安全应急预案

7 应急处置结果及上报

1、对于无法修复的应用系统入侵可能会需要重新安装操作系统，重新部署应用服务，并重新注册，重新做数据迁移工作，所需要的时间会延长和需要相关人员（至少系统管理员），需要相关模块/部门之间的配合，甚至启动其他模块系统应急预案。

2、感染处理可能导致系统负载较高。

3、对于系统被攻击破坏的情况，有可能会导致系统数据丢失，系统责任人、业务部门、数据中心要有日常数据备份工作，以备应急。

4、在切换备份服务器的过程中出现不能访问应用服务的情况，系统负责人需提前告知业务部门准备。

5、因应急处置需重新启动系统，会出现网络服务访问较慢的现象，系统负责人需提前告知业务部门做好准备。

6、处置过程的汇报应遵守二级应急预案文件《金发科技信息系统应急预案》的相关规定。

8 预防和预警

1、信息安全组需做好技术能力知识和应急知识储备；

2、信息安全组对应用系统加强实时监控和安全风险管理，定期进行例行安全检查和安全评估加固（包括但不仅限于漏洞加固、应用系统权限最小化访问等）；

3、

3、应用系统责任人和数据中心组实时监控应用系统运行情况，出现问题应及时上报；

4、数据中心组对于应用系统应做好备份工作，以便在系统被攻击、数据被破坏/篡改时可及时主备切换、数据恢复等；

信息安全应急预案

5、确保和外部维保或信息安全组织沟通渠道的畅通，在信息安全事件超出内部处理能力范畴时可及时获得外部技术支援；情节严重的外部服务系统可及时向公安单位协助。

9 附录

9.1 附录 1：勒索病毒应急预案



信息安全应急预案-勒索病毒.doc

信息安全应急预案

9.2 附录 2：邮件安全应急预案



信息安全应急预案-
邮件安全.doc

信息安全应急预案

9.3 附录 3：数据泄漏应急预案



信息安全应急预案-数据泄漏.doc

信息安全应急预案

9.4 附录 4：应用系统被攻击篡改应急预案



信息安全应急预案-
应用系统被攻击篡改

信息安全应急预案

9.5 附录 5：应急人员联系方式

应急组织	角色	姓名	所属部门及职称	联系方式
应急处置小组	组长	***	信息管理部	***
	组员	***		***
	组员	***		***
	组员	***		***
网络小组	应急组组员	***		***
服务管理组	应急组组员	***		***
数据中心小组	应急组组员	***		***
系统责任人	应急组组员	***		***

信息安全应急预案