防灾科技学院信息化管理中心

信息中心〔2021〕28 号

关于印发《防灾科技学院密码安全事件处理应急预案》的通知

学校各部门、各单位：

为应对系统发生密码安全事件，缩小密码安全事件的影响，尽可能保障与用户感知密切相关、受理量较大的业务平稳运行。特制定《防灾科技学院密码安全事件处理应急预案》，现予印发，请遵照执行。

防灾科技学院信息化管理中心

2021 年 12 月 3 日

防灾科技学院密码安全事件处理应急预案

一、适用范围

本预案适用于防灾科技学院系统。如果系统发生密码安全事件，此预案将作为处理安全事件的流程依据。

二、目标

在发生安全事件时，依据此预案快速响应密码安全事件，缩小密码安全事件的影响，尽可能保障与用户感知密切相关、受理量较大的业务平稳运行。

三、组织设置

应急领导组

组长：学校主要负责人

成员：办公室、党委办公室、党委宣传部(党委统战部)、信息化管理中心、发展与财务处、教务处(学位办公室)、党委学生工作部(学生工作处、学生资助管理中心)、学科与研究生处、团委(大学生艺术活动指导中心)、党委安全工作部(安全工作处)、人事处、资产管理处、基建处、图书馆（档案馆)、高等教育研究所（《防灾科技学院学报》编辑部)、信息工程学院等部门负责人

接口人：办公室主任

职责：应急响应领导小组是网络安全应急响应工作的组织领导机构，负责领导和决策网络安全应急响应的重大事宜，并为应急响应工作提供支持。包括：

1.负责对应急响应工作的承诺和支持，如发布正式文件和协调必要的人财物资源等；

2.负责审核并批准应急响应预案；

3.负责启动和指挥应急响应预案的执行；

4.负责启动应急响应预案的定期评审和修订；

5.负责外部协调工作；

6.负责领导和决策安全事件响应的重大事宜；

四、事件处理

密码安全事件应急处理根本目的在于以最短时间消除或降低事件对公司和业务产生的负面影响。为此应急处理过程中可以不遵从日常管理和操作流程，但是处置完成后应按照相关日常管理和操作流程补充相关记录。

应急响应后，首先应确认是否有对应场景的应急预案，如有响应预案，则按照计划执行。如无响应预案，则参照以下步骤执行：

1.响应确认：事件发生后响应事件，判断事件是否为恶意攻击，以及对系统是否存在影响。 获取各关键环节的告警信息和日志信息，以便分析事件使用。

2.缓解抑制:依据分析结果制定补救措施,对事件进行控制，缩小事件对正常业务的影响。

3.汇报沟通：对安全事件形成初步的报告，汇报至应急领导组，并请示下一步安排。同时，必要情况下需与外界沟通，表明

积极响应安全事件的态度，避免宣传上的被动局面。

4.分析阶段：在事件得到初步缓解抑制的状态下，利用前期获取的日志信息、告警信息做充分详细的分析，以便完全掌握事件的原委始末。

5.系统恢复：问题得到初步缓解抑制后，应急处置团队应组织相关部门，按照事件发生前的状态，对受影响的服务和业务进行有序的恢复。通知所有可能受到本事件影响的相关方，共同商讨制定并执行解决措施。通常应包括的相关方：外部客户、内部用户、业务维护方、系统维护方。

6.后续工作及总结:安全事件响应结束后,应采取有效措施，防止系统再次遭受攻击。举一反三，对可能遭受类似攻击的系统实施安全加固。同时对安全应急预案做适当的修补更新。

对于各类安全事件，具体处理过程会有所差别。因此，下面按各种风险场景单列具体处置预案。

4.1 密码泄露处置预案

4.1.1 响应确认阶段

对密码信息泄露事件做出响应，判断安全事件是否为恶意行为，是否对学校造成不良影响。

1.当通过媒体、互联网、或者其他渠道得知发生密码信息泄露事件时，安全团队应紧急响应事件，安排人员核实泄露事件的真实性。应用负责人、数据库负责人比对数据，确定信息泄漏的出处，以及根据日志研判信息泄漏的规模、泄漏的时间、途径。

2.应急协调组根据泄露信息的条数，对泄露事件定级，并按应急响应预案流程执行。

责任分工表

序号	责任任务	责任人
1	核实客户信息泄露事件	安全团队
2	核实客户信息泄漏源、途径、时间	应用负责人、数据库负责人
3	根据信息泄露条数对事件定级	应急协调组

4.1.2 抑制缓解阶段

在确定密码信息泄漏事件后，应采取必要的缓解抑制操作。应用负责人、数据库负责人应从技术角度，对信息泄漏的路径、方法进行有效封堵，避免密码信息泄漏事件进一步扩大。

若需要其他单位协助消除密码信息泄漏事件的负面影响，应急协调组应报请应急领导组批准，尽快抑制信息泄露事件的负面影响。

责任分工表

序号	责任任务	责任人
1	封堵密码信息泄漏的路径、方法	应用负责人、数据库负责人
2	协调外部门降低泄漏事件负面影响	应急协调组

4.1.3 事件汇报阶段

在安全事件得到初步抑制，负面影响得到初步缓解后，应急协调组应就事件形成书面的完整报告。报告需提交应急领导小组核准。之后，报告作为对外交代事件的统一口径对外发布。详细格式见章节七。

4.1.4 事件分析阶段

分析阶段主要目的是将事件的成因、过程、造成的损失评估等详细信息做周密的调查分析，形成详细报告。详细报告一方面作为与外部部门沟通联系的材料依据，另一方则支撑下一步恢复修复工作。

通过分析阶段，需明确下列内容：

1.确定密码信息泄漏事件的时间、泄漏信息的详细清单、数据量。

2.详细分析信息泄漏事件期间的应用日志、中间件日志、主机日志、静态防篡改设备、抗 DDOS 设备、waf、防火墙、防毒墙/IPS 日志，对攻击者进行溯源分析

3.导出系统的部署文件，进行本地木马查杀，检查是否存在webshell。

4.对系统进行渗透测试，复现密码信息泄露的完整过程。

5.同时确认在密码信息泄漏的同时，数据库数据是否遭到破坏。

6.核实用户资料文件信息、系统文件信息是否出现被破环、

篡改等现象，对有差异的文件进行筛选，形成清单，以便在恢复阶段做文件恢复操作。

责任分工表

序号	责任任务	责任人
1	确定攻击时间范围	安全团队
2	分析设备、主机、中间件等日志	审计团队
3	对部署文件进行 webshell 查杀	安全团队
4	对被攻击主机进行渗透测试	安全团队
5	核实数据库是否遭到破坏	数据库负责人
6	核实用户资料信息	应急技术组

4.1.5 恢复阶段

在处理密码信息泄漏事件的同时，应判断是否存在其他诸如数据损坏，系统损坏的事件发生。若数据损坏、系统损坏也同时存在，应考虑以下恢复步骤：

1.应急协调组负责分析恶意操作的影响，并就是否重新部署系统、是否启用灾备提出建议。

2.若需启动灾备系统，由应急协调组提请应急领导组批准，由应急技术组具体操作实施。

3.若生产环境需要重建部署，由应急协调组提请应急领导组

批准，由工程团队与运维团队共同实施。

4.若需要升级主机、中间件，由信息化管理中心来完成具体的升级工作。

5.如果数据库遭到破坏，数据库负责人负责恢复数据库备份文件。

6.对入侵者利用的（应用、主机、中间件）漏洞进行修复，重新部署应用服务，恢复业务正常运行。

7.若文件资料遭到删除或者破坏，需利用备份数据恢复用户文件资料。

责任分工表

序号	责任任务	责任人
1	对是否需要重新安装操作系统提出建议	应急协调组
2	启用灾备系统	应急技术组
3	重新部署生产环境	工程团队\应急技术组
4	升级主机、中间件补丁	应急技术组
5	恢复数据库	数据库负责人
6	修复系统漏洞、重新部署应用系统	应急技术组
7	恢复用户文件资料	应急技术组

4.2 密码数据篡改事件处置预案

4.2.1 应急响应确认阶段

密码系统数据疑似遭受攻击，被恶意篡改时，应急协调组对此作出响应，确认影响范围，以及影响程度。

1.数据库负责人确认被篡改数据是否有备份。

2.数据库负责人确认被篡改数据的数量。

3.数据库负责人确认可以直接连接被篡改数据库的 IP 清单，并报备至应急协调组，方便进行下一步排查。

4.密码系统各环节负责人收集被篡改数据相关的日志信息，包括但不局限于:静态防篡改设备、抗 DDOS 设备、web 应用、中间件、主机、waf、防火墙、防毒墙/IPS 日志以及数据库操作日志（如果没有被删除）

责任分工表

序号	责任任务		责任人
1	确定被篡改数据库是否有备份		数据库管理员
2	确认被篡改数据的数量		数据库管理员
3	确认可以直接连接被篡改数据库的 IP 清单，并报备至应急协调组		数据库负责人
4	日志收集	静态防篡改设备告警日志	安全设备负责人
		抗 DDOS 设备告警日志	安全设备负责人
		web 应用自身登陆、登出、查询或办理业务日志	应用负责人
		中间件（自身操作、告警、错误日志）	应用负责人

		主机日志	主机负责人
		waf 告警日志	安全设备负责人
		防火墙告警日志	网络负责人
		防毒墙/IPS 告警日志	安全设备负责人

4.2.2 抑制缓解阶段

场景 1：内网人员违规操作，数据篡改

1.应急协调组对篡改的影响做充分的分析，并就是否重新部署系统、是否启用灾备数据库提出建议。

2.由应急协调组提请应急领导组批准是否启动灾备系统，由应急技术组具体操作实施。

3.若数据篡改量较大，影响业务系统正常运行，系统主页发布系统维护公告静态页面:XX 系统于 20xx 年 xx 月 xx 日 hh:mm:ss 进行系统升级，给您带来不便敬请谅解。

4.应急响应联络员与外部门保持联络，通报事件处理进展。

责任分工表

序号	责任任务	责任人
1	对恶意操作的影响做充分的分析，并就是否重新部署系统、是否启用灾备提出建议	应急协调组
2	启用灾备系统	应急技术组
3	发布系统升级维护公告	应用负责人
4	保持外部门联系，通报事件处理进展	应急响应联络员

场景 2：通过外网入侵，利用漏洞控制主机，或直接通过 SQL 注入漏洞进行数据篡改

1.应急协调组对数据篡改操作的影响做充分的分析，并就是否重新部署系统、是否启用灾备提出建议。

2.由应急协调组提请应急领导组批准启动灾备系统，由应急技术组具体操作实施。

3.若数据篡改量较大，影响业务系统正常运行，系统主页发布系统维护公告静态页面:XX 系统于 20xx 年 xx 月 xx 日 hh:mm:ss 进行系统升级，给您带来不便敬请谅解；

4.数据库负责人核实被篡改的数据与互联网及其他系统的网络连接情况；

5.应急响应联络员与新闻媒体等保持联络，以确保在网络安全事件发生时能及时通报准确情况和获得适当支持，以以下口径介绍：

a)系统按原定计划开展应急演练,服务预计于 xx 时间点恢复正常。

b)系统维护升级，服务预计于 xx 时间点恢复正常。

责任分工表

序号	责任任务	责任人
1	对恶意操作的影响做充分的分析，并就是否重新部署系统、是否启用灾备提出建议	应急协调组
2	启用灾备系统	应急技术组

3	发布系统升级维护公告	应用负责人
4	核实被篡改的数据库与互联网及其他系统的网络连接情况	数据库负责人
5	保持与外部门联系，通报事件处理进展	应急响应联络员

4.2.3 事件汇报阶段

在安全事件得到初步抑制，负面影响得到初步缓解后，应急协调组应就事件形成书面的完整报告。报告需提交应急领导小组核准。之后，报告作为对外交代事件的统一口径对外发布。详细格式见章节 7。

4.2.4 事件分析阶段

分析阶段主要目的是将事件的成因、过程、造成的损失评估等详细信息做周密的调查分析，形成详细报告。详细报告一方面作为与外部部门沟通联系的材料依据，另一方则支撑下一步恢复修复工作。

通过分析阶段，需明确下列内容：

1.确定密码数据篡改事件的开始时间、结束时间、持续时间。

2.细致化分析应用日志、中间件日志、主机日志、静态防篡改设备、抗 DDOS 设备、waf、防火墙、防毒墙/IPS 日志以及数据库操作日志，对攻击者进行溯源分析。

3.对恶意篡改密码数据的 IP 进行定位，确认是内部人员所为

还是外部人员做的。

4.分析是否存在数据库全量数据导出行为。

5.导出系统的部署文件，进行本地网马查杀，检查是否存在webshell。

6.对系统进行渗透测试，分析恶意篡改事件所利用的漏洞。

7.核实用户资料文件信息、系统文件信息是否出现被破坏、篡改等现象。对有差异的文件进行筛选，形成清单，以便在恢复阶段做文件恢复操作。

责任分工表

序号	责任任务	责任人
1	确定数据库篡改事件的开始时间、结束时间、持续时间	安全团队
2	日志分析、定位源头	审计团队
3	对恶意篡改数据库的 IP 进行定位	安全团队 审计团队
4	分析是否存在数据库脱库行为	数据库管理员
5	对部署文件进行 webshell 查杀	安全团队
6	渗透测试	安全团队
7	核实用户资料信息	应急技术组

4.2.5 恢复阶段

依据分析阶段的结果，对被破坏的系统、数据、用户文件资

料进行恢复，对漏洞进行修复，恢复系统正常运行。恢复步骤按如下方式进行：

1.应急协调组负责分析恶意操作的影响，并就是否重新部署系统、是否启用灾备提出建议。

2.若需要升级主机、中间件，由维护室来完成具体的升级工作。

3.数据库负责人负责恢复数据库备份文件。

4.对入侵者利用的（应用、主机、中间件）漏洞进行修复，重新部署应用服务，恢复业务正常运行。

5.若用户文件资料遭到删除或者破坏，需利用备份数据恢复用户文件资料

责任分工表

序号	责任任务	责任人
1	重新部署生产环境	工程团队\应急技术组
2	升级主机、中间件补丁	应急技术组
3	恢复数据库	数据库负责人
4	修复系统漏洞、重新部署应用系统	应急技术组
5	恢复用户文件资料	应急技术组

4.3 密码系统破坏事件处置预案

4.3.1 响应确认阶段

当密码系统遭到疑似系统破坏攻击时，应急协调组对此作出

响应，确认影响范围，以及严重程度。

1.确认事件的真实性。

2.应急协调组根据事件的性质、影响，确定安全事件级别，并按应急响应预案流程执行。

3.主机管理员、应用管理员核实受影响的密码主机 IP 清单，并报备至应急协调组，方便进行下一步排查。

4.系统负责人负责确认主机的用途。

5.系统各环节负责人收集被破坏系统的日志信息，包括但不局限于:静态防篡改设备、抗 DDOS 设备、web 应用、中间件、主机、waf、防火墙、防毒墙/IPS 日志（由于此次事件属于恶意系统破坏，各个环节的日志尽可能的收集）。

责任分工表

序号	责任任务		责任人
1	当得到系统主机、web 系统早点破坏的通知或信息时，确定事件的真实性		安全团队
2	根据事件的性质、影响确定安全事件级别，并按应急响应预案流程执行		应急协调组
3	核实受影响的主机清单，并报备至应急协调组		主机管理员 应用管理员
4	确认造破坏主机的作用		系统负责人
5	日日志收集	静态防篡改设备告警日志	安全设备负责人
		抗 DDOS 设备告警日志	安全设备负责人

		web 应用自身登陆、登出、查询或办理业务日志	应用负责人
		中间件（自身操作、告警、错误日志）	应用负责人
		主机日志	主机负责人
		waf 告警日志	安全设备负责人
		防火墙告警日志	网络负责人
		防毒墙/IPS 告警日志	安全设备负责人

4.3.2 抑制缓解阶段

场景 1：内网人员执行危险命令、或者失误操作引起的

1.应急协调组对恶意操作的影响做充分的分析，并就是否重新部署系统、是否启用灾备提出建议。

2.由应急协调组提请应急领导组批准是否启动灾备系统，由应急技术组具体操作实施。

3.系统主页发布系统维护公告静态页面：XX 系统于 20xx 年 xx 月 xx 日 hh:mm:ss 进行系统升级，给您带来不便敬请谅解。

4.应急响应联络员与外部门保持联络，通报事件处理进展。

责任分工表

序号	责任任务	责任人
1	对恶意操作的影响做充分的分析，并就是否重新部署系统、是否启用灾备提出建议	应急协调组
2	启用灾备系统	应急技术组
3	发布系统升级维护公告	应用负责人
4	与外部门保持联络，通报事件处理进展	应急响应联络员

场景 2：通过外网入侵，利用漏洞控制主机，进行的恶意破坏行为

1.应急协调组分析恶意操作的影响，并就是否重新部署系统、是否启用灾备提出建议

2.由应急协调组提请应急领导组批准启动灾备系统，由应急技术组具体操作实施。

3.系统主页发布系统维护公告静态页面：：XX 系统与 20xx 年 xx 月 xx 日 hh:mm:ss 进行系统升级，给您带来不便敬请谅解；

4.网络管理员核实被恶意破坏系统与互联网及其他系统的网络连接情况；

5.应急响应联络员与外部门保持联络，通报事件处理进展。

责任分工表

序号	责任任务	责任人
1	对恶意操作的影响做充分的分析，并就是否重新部署系统、是否启用灾备提出建议	应急协调组
2	启用灾备系统	应急技术组
3	发布系统升级维护公告	应用负责人
4	核实被恶意破坏系统与互联网及其他系统的网络连接情况	网络管理员
5	与外部门保持联络，通报事件处理进展	应急响应联络员

4.3.3 事件汇报阶段

在安全事件得到初步抑制，负面影响得到初步缓解后，应急协调组应就事件形成书面的完整报告。报告需提交应急领导小组核准。之后，报告作为对外交代事件的统一口径对外发布。详细格式见章节 7。

4.3.4 事件分析阶段

分析阶段主要目的是将事件的成因、过程、造成的损失评估等详细信息做周密的调查分析，形成详细报告。详细报告一方面作为与外部部门沟通联系的材料依据，另一方则支撑下一步恢复修复工作。

通过分析阶段，需明确下列内容：

1.确定恶意破坏事件的开始时间、结束时间、持续时间。

2.细致化分析应用日志、中间件日志、主机日志、静态防篡改设备、抗DDOS设备、waf、防火墙、防毒墙/IPS日志，对攻击者进行溯源分析

3.导出系统的部署文件，进行本地网马查杀，检查是否存在webshell。

4.对系统进行渗透测试,分析恶意破坏事件利用了什么漏洞。

5.核实数据库是否遭到破坏。

6.核实用户资料文件信息、系统文件信息是否出现被破坏、篡改等现象。对有差异的文件进行筛选，形成清单，以便在恢复阶段做文件恢复操作。

责任分工表

序号	责任任务	责任人
1	确定恶意破坏事件的开始时间、结束时间、持续时间	安全团队
2	日志分析、定位源头	审计团队
3	对部署文件进行webshell查杀	安全团队
4	渗透测试	安全团队
5	核实数据库是否遭到破坏、篡改	数据库管理员
6	核实用户资料信息	应急技术组

4.3.5 恢复阶段

依据分析阶段的结果，对被破坏的系统、数据、用户文件资料进行恢复,对入侵者利用的漏洞进行修复,恢复系统正常运行。恢复步骤按如下方式进行：

1.应急协调组负责分析恶意操作的影响，并就是否重新部署系统、是否启用灾备提出建议。

2.若需要升级主机、中间件，由维护室来完成具体的升级工作。

3.如果数据库遭到破坏，数据库负责人负责恢复数据库备份文件。

4.对入侵者利用的（应用、主机、中间件）漏洞进行修复，重新部署应用服务，恢复业务正常运行。

5.若用户文件资料遭到删除或者破坏，需利用备份数据恢复用户文件资料。

责任分工表

序号	责任任务	责任人
1	重新部署生产环境	工程团队\应急技术组
2	升级主机、中间件补丁	应急技术组
3	修复系统漏洞、重新部署应用系统	应急技术组
4	恢复数据库	数据库负责人
5	恢复用户文件资料	应急技术组

4.2 应急协调组

组长：办公室主任

成员： 党委宣传部、信息化管理中心负责人

接口人：办公室主任

职责：应急响应协调小组主要负责为应急响应提供专业的技术支持和组织协调工作，包括：

1.负责对重大网络安全事件进行评估，对应急响应级别提出建议；

2.负责研究分析网络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.负责分析网络安全事件原因及造成的危害，为应急响应提供技术支持。

4.在应急工作中起到协调、督导作用，负责应急领导组决策的落地实施，协调应急响应技术组完成各方面技术操作。

4.3 应急响应技术组

组长：信息化管理中心负责人

成员： 部门相关人员

应急响应技术小组主要负责应急响应的具体技术实施工作，包括：

1.负责编制应急响应预案；

2.负责实施应急响应预案；

3.负责组织应急响应预案的测试、培训、演练；

4.负责执行应急响应预案的评审和修订任务；

5.负责总结应急响应工作，提交应急响应总结报告。

4.4 应急响应联络员：

应急联络员： 信息化管理中心负责人

应急响应联络员主要负责应急响应中对内部和外部的各项联系工作，包括：

1.负责建立维护应急响应内部和外部联系清单。负责定期更新联络清单，确保事件发生时可及时联系到外部相关部门；

2.负责与相关人员或部门联系，及时发布事件进展的最新情况，以确保在网络安全事件发生时能及时准确通报情况和获得适当支持与理解。

外部联系人清单

序号	部门	姓名	电话	联系场景

4.5 各部门

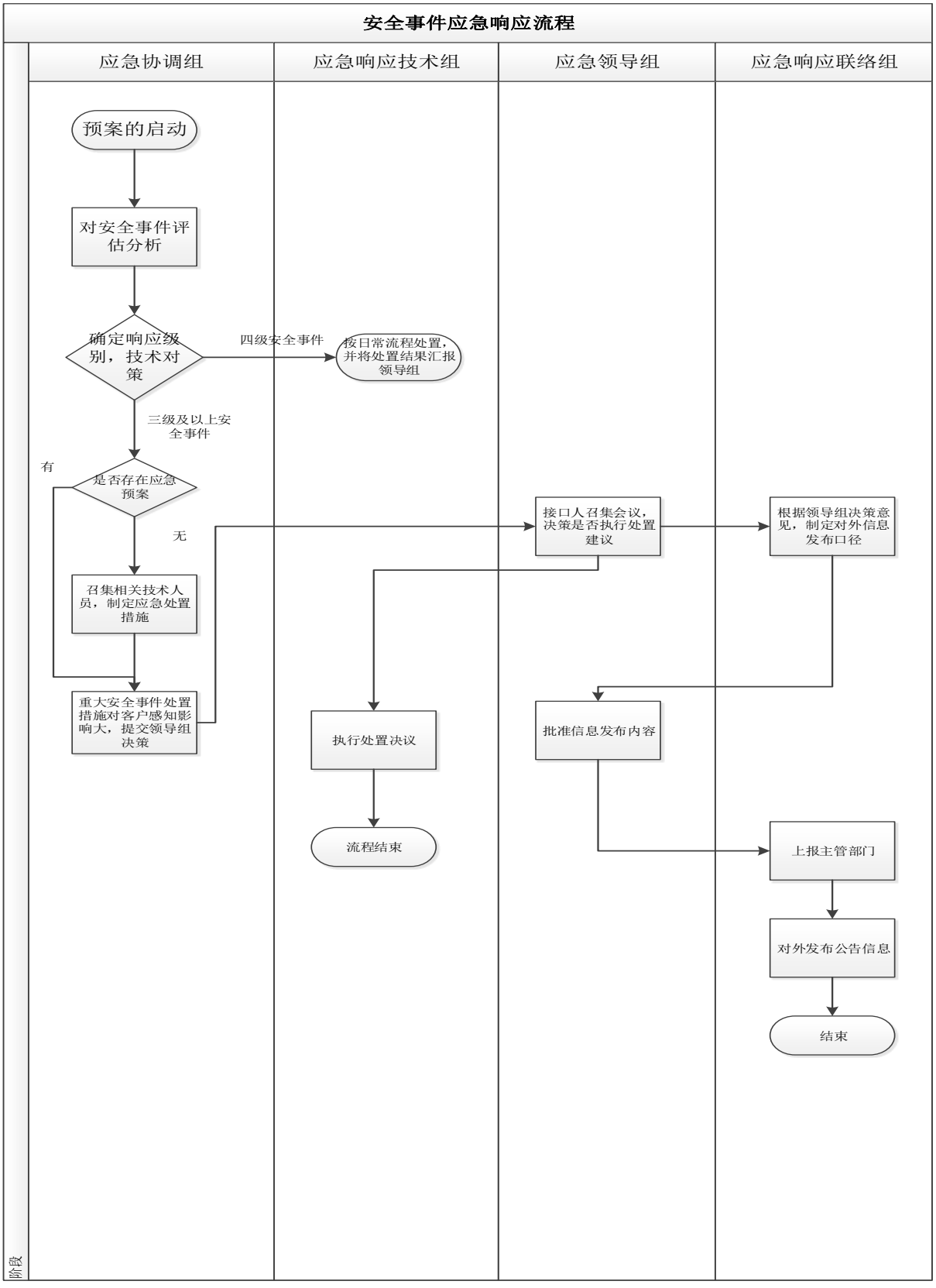
1.负责配合应急响应工作；

2.负责日常监控,将疑似攻击行为的事件向应急协调组报告。

负责人清单：

序号	角色	姓名	电话

五、应急响应流程图


安全事件应急响应流程
应急协调组
应急响应技术组
应急领导组
应急响应联络组
预案的启动
对安全事件评估分析
确定响应级别，技术对策
四级安全事件
按日常流程处置，并将处置结果汇报领导组
三级及以上安全事件
有
是否存在应急预案
无
召集相关技术人员，制定应急处置措施
重大安全事件处置措施对客户感知影响大，提交领导组决策
接口人召集会议，决策是否执行处置建议
根据领导组决策意见，制定对外信息发布口径
执行处置决议
流程结束
批准信息发布内容
上报主管部门
对外发布公告信息
结束
阶段

六、预案的启动

本应急预案自事件发生时启动，完成对事件的响应、严重性分析、修复方法研究，风险的初步遏制消除、信息的汇总上报，并在系统恢复、启动容灾切换中提供技术咨询，直至事件处理完毕为止。

事件来源：

安全类投诉；

上级部门或其他部门通报的安全事件；

下级部门上报的安全事件；

系统运行的告警信息；

安全监控设备的告警信息；

执行日常安全作业计划时所发现的问题；

审计分析发现的异常情况。

当疑似网络安全事件发生时，应由应急协调组接收处理。协调组收到事件报告后，应首先按照附件二对事件级别进行确认。

协调组应依据事件的影响和处理的时间要求等，判断是否需要启动应急响应流程。如无需启动应急流程，应提出处置建议，进行常规处理，并报应急领导组知晓。

七、汇报沟通

在安全事件的处理过程中，应及时汇总上报掌握的情况、处理进展等信息，以便领导层对于事件的性质、内容、风险以及可能造成的内外部的影响有充分的掌握和准确的预判。

在事件初步判定为安全事件后，应急协调组应就事件形成初步报告，以邮件、电话、信息等方式汇报至领导层。汇报内容应包括但不局限于以下内容：

事件发生的时间、报告人、事件内容、影响系统范围、潜在风险、事件定级、处置建议等。

安全应急事件报告模版

事件时间	20xx/xx/xx xx:xx:xx	报告人	xxxxx
事件类别	网页篡改/	事件定级	
事件内容	**系统与通过安全类投诉 XXXX 年 XX 月 XX 日 hh:mm:ss 发生网页篡改事件,经过应急响应技术组确认,XXXX 年 XX 月 XX 日 hh:mm 开始应急响应。		
影响系统范围			
危害及影响			
处置建议			

八、后续工作及总结

事件处理完成后，应组织相关部门进行总结，至少应包括事件发生的原因、产生的影响和获得教训等方面，制定并执行相关的检查措施以及今后的改进措施。

1.应跟踪检查活动和改善活动的执行情况。

2.应协同各相关方，根据事件的影响程度对事件责任人进行相应的处罚，如触犯法律，依法移交司法机关处理。

3.组织对事件进行分析，识别公司的网络安全体系存在的不足，进行完善和细化，并进行必要的培训。根据事件的状况，必要时在单位更大范围内进行检查和审核，避免类似事件的再次发生。

4.事件处理完毕后，应整理事件相关的所有记录，修正或补充响应的安全事件应急处理预案。

附件 1.事件分类

密码安全事件分为有害程序事件、网络攻击事件、密码信息破坏事件、设备设施故障、灾害性事件和其他网络安全事件等。

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.密码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。

附件 2.事件定级

根据密码安全的重要程度，将安全事件分为四级：特别重大(I 级)、重大(II 级)、较大(III 级)、一般(IV 级)。

特别重大安全事件 (I 级)

指能够导致特别严重影响或破坏的密码安全事件，包括以下情况：

密码篡改：修改密码系统的相关信息，危害国家安全、社会稳定和公共利益的内容，产生特别重大社会影响；

拒绝服务、系统入侵、恶意代码：因被攻击或设备故障等，导致密码系统业务中断、系统宕机、网络瘫痪等特别严重影响，业务中断已超过或预计超过 2 小时；预计解决故障时间或实际解

决故障时间超过 4 小时；

灾害事件导致的密码系统系统中断、系统宕机、网络瘫痪等事件。

密码信息泄漏：其他对社会秩序和公共利益造成特别严重损害，或对国家安全造成严重损害的网络安全事件。

重大安全事件（II 级）

指能够导致严重影响或破坏的网络安全事件，包括以下情况：

密码篡改：修改密码系统的相关信息，危害国家安全、社会稳定和公共利益的内容，产生重大社会影响；

拒绝服务、系统入侵、恶意代码：因被攻击或设备故障等，导致密码系统业务中断、系统宕机、网络瘫痪等特别严重影响，业务中断已超过或预计超过 1 小时；预计解决故障时间或实际解决故障时间超过 2 小时；

密码信息泄漏：其他对社会秩序和公共利益造成严重损害，或对国家安全造成损害的网络安全事件。

较大安全事件（III 级）

指能够导致较严重影响或破坏的网络安全事件，包括以下情况：

拒绝服务、系统入侵、恶意代码：因被攻击或设备故障等，导致密码系统业务中断、系统宕机、网络瘫痪等特别严重影响，业务中断已超过或预计超过 30 分钟；预计解决故障时间或实际解决故障时间超过 1 小时；

密码信息泄漏:：其他对公民合法权益造成严重损害，或对社会秩序和公共利益造成损害，但不损害国家安全的网络安全事件。

一般安全事件(IV 级)

指不满足以上条件的网络安全事件，包括以下情况：

拒绝服务、系统入侵、恶意代码：因被攻击或设备故障等，导致密码系统业务中断、系统宕机、网络瘫痪等特别严重影响，业务中断已超过或预计不超过 30 分钟；预计解决故障时间或实际解决故障时间不超过 1 小时；

密码信息泄漏：其他对公民合法权益造成损害，但不损害国家安全、社会秩序和公共利益的网络安全事件。

防灾科技学院信息化管理中心　　2021 年 12 月 3 日印发