南开大学网络与信息安全类突发公共事件

应急处置预案

（试行）

　　为加强南开大学信息技术安全工作，及时掌握和处置信息技术安全事件，协调相关力量做好应急响应处理，降低安全事件带来的损失与影响，维护正常工作秩序和营造健康的网络环境，根据国家有关法律法规，以及相关标准文件，结合我校实际情况，制定本预案。

　　第一条 信息技术安全事件定义。根据《信息安全事件分类分级指南》（GB/T 20986-2007，以下简称《指南》），本流程中所称的信息技术安全事件（以下简称安全事件）是指除信息内容安全事件以外的有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件。

　　第二条 适用范围。本预案适用于在南开大学发生的网络与信息安全类事件的报告与处置工作。涉及信息内容安全事件的报告与处置工作需按信息内容安全相关规定执行。

第三条 安全事件等级划分。根据《指南》并结合我校实际情况，将安全事件划分为四个等级。

1. 特别重大事件（I级）

信息系统发生大规模瘫痪，信息泄漏或损坏，事态发展超出管理单位的控制范围，对国家安全、社会秩序、经济建设和公共利益造成特别严重损害的突发公共事件，超过24小时不能恢复。

1. 重大事件（Ⅱ级）

业务系统发生较大规模瘫痪，信息泄漏或损坏，对国家安全、社会秩序、经济建设和公共利益造成严重损害，超过12小时未能恢复，需要跨部门协同处置的突发公共事件。

1. 较大事件（Ⅲ级）

业务系统发生瘫痪，信息泄漏或损坏，对国家安全、社会秩序、经济建设和公共利益造成一定损害，但在8小时内可以恢复，不需要跨部门协同处置的突发公共事件。

1. 一般事件（Ⅳ级）

业务系统部分瘫痪，信息泄漏或损坏，对系统用户的权益有一定影响，但在4小时内可以恢复，不危害国家安全、社会秩序、经济建设和公共利益的突发公共事件。

　　第四条 安全事件自主判定。一旦发生安全事件，应根据第三条所述，视信息系统重要程度、损失情况以及对工作和社会造成的影响自主判定安全事件等级。

　　第五条 I至Ⅲ级安全事件的报告与处置。报告与处置分为三个步骤：事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置。

（一）事发紧急报告与处置

　　1．网络与信息系统运维操作人员一旦发现上述安全事件，应根据实际情况第一时间采取有效措施进行处置，将损害和影响降到最小范围，保留现场，并报告本单位安全责任人和主要负责人。

　　2．本单位安全责任人接到报告后，应立即组织技术人员赶赴现场进行紧急处置，同时以口头通讯的方式将相关情况通报至信息化建设与管理办公室（以下简称信息化办）。涉及人为主观破坏事件应同时报告学校保卫处。

　　3．信息化办接到报告后，负责组织技术人员协同报告单位人员进行应急处置。同时，应进一步判定安全事件等级，对确认属I至Ⅲ级安全事件的,应报告学校宣传部，由宣传部负责上报有关部门领导。

　　4．紧急报告内容包括：（1）时间地点；（2）简要经过；（3）事件类型与分级；（4）影响范围；（5）危害程度；（6）初步原因分析；（7）已采取的应急措施。

　　6．信息办应及时跟进事件发展情况，出现新的重大情况应及时补报。

（二） 事中情况报告与处置

　　1．事中情况报告应在安全事件发现后12小时内以书面报告的形式进行报送，报送内容和格式见附件1。

　　2．事中情况报告由事件发生单位的安全负责人组织相关人员，运维单位共同填写，由事件发生单位主要负责人审核后，签字并加盖公章报送信息化办和宣传部。

　　3．安全事件的事中处置包括：及时掌握损失情况、查找和分析事件原因，修复系统漏洞，恢复系统服务，尽可能减少安全事件对正常工作带来的影响。如果涉及人为主观破坏的安全事件应积极配合保卫处和公安部门开展调查。

（三）事后整改报告与处置

　　1．事后整改报告应在安全事件处置完毕后5个工作日内以书面报告的形式进行报送，报送内容和格式见附件2。

　　2．事后情况报告由事件发生单位的安全负责人组织相关人员，运维单位共同填写，由事件发生单位主要负责人审核后，签字并加盖公章报送信息化办和宣传部。

　　3．安全事件事后处置包括：进一步总结事件教训，研判安全现状、排查安全隐患，进一步加强制度建设，提升安全防护能力。如涉及人为主观破坏的安全事件应继续配合保卫处和公安部门开展调查。

第六条 一般安全事件报告与处置。相关单位发生一般安全事件，应及时、自主组织应急处置工作，在事件处置完毕后7天内报送整改报告信息化办和宣传部，报告内容和格式见附件2。

第七条 安全事件参考处置方案。当发生网络与信息安全事件时，首先应区分事件性质，然后再根据不同情况分别进行处置。

1. 根据事件性质，网络与信息安全事件可划分为三类

　　1．自然灾害。指地震、雷电、火灾、洪水等灾害引起的计算机网络与信息系统的损坏。

　　2．事故损毁。指电力中断、网络损坏或是软件、硬件设备故障等引起的计算机网络与信息系统的损坏。

　　3．人为破坏。指人为破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖袭击等引起的计算机网络与信息系统的损坏。

1. 针对上述三类事件的处置办法

　　1．属自然灾害类事件时，应根据实际情况，在保障人身安全的前提下，首先保障数据安全，然后再保障设备安全（包括硬盘拔出与保存、设备断电与拆卸、搬迁设备等）。

2．属事故损毁类事件时，应迅速分析故障特征，查明原因，若事件发生单位不能独立处理，必须立刻通知相关单位（供电局、网络运营商、软硬件产品维护单位等），马上组织人员进行系统修复。

（1）外电中断处置。外电中断后，立即切换到备用电源；迅速查明断电原因，如因内部线路故障，马上组织恢复；如因供电部门原因，立即与供电单位联系，尽快恢复供电；如被告知将长时间停电，应做好以下工作：（a）预计停电1小时以内的，由UPS供电；（b）预计停电1-4小时的，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小时的，做好数据备份工作，及时关闭有关设备。

（2）机房火灾处置。一旦机房发生火灾：首先切断所有电源，按响火警警报；其次，检查自动喷淋系统是否启动，并使用灭火器进行灭火；最后，如果需要，应通过119电话向公安消防部门请求支援。

（3）网络线路中断处置。网络线路中断后：首先，应迅速判断故障节点，查明原因、尽快修复。如属网络运营商负责维护运营的线路，立即与运行商维护部门联系，及时进行修复。如属局域网内部线路故障，应立即判断故障节点，查明故障原因，迅速组织修复；如属路由器、交换机等网络设备故障，立即与设备供应商联系修复；如属路由器、交换机配置文件破坏，迅速按照要求重新配置；其次，如遇本地技术无法解决的技术问题，应立即向有关厂商请求支援。

（4）设备故障处置。发现服务器等关键设备损坏，应立即查明设备故障原因；能自行恢复的，立即用备件替换受损部件；难以自行恢复的，立即与设备供应商联系，请求派维修人员前来维修；若设备一时不能修复，应及时采取必要措施，并发布通知告知有关单位暂缓上传、上报数据。

3．属人为破坏类事件时，应首先判断破坏来源与性质，然后断开影响安全的网络设备，断开与破坏来源的网络连接，跟踪并锁定破坏来源IP地址或其它用户信息，修复被破坏的信息，恢复信息系统。

（1） 有害信息处置。首先，尽快采取屏蔽、删除等有效措施对有害信息进行清理，并做好相关记录；其次，指派专人对存在问题的网站、网页及邮件信息等进行全时监控；再次，采取技术手段追查有害信息来源；最后，如发现涉及国家安全、稳定的重大有害信息，还要及时向保卫处或公安局网警支队报告。

（2） 黑客攻击处置。当发现网页内容被篡改或通过入侵检测系统发现黑客攻击时:首先,将被攻击服务器等设备从网络中隔离；其次,组织相关人员对事件进行安全评估，评估破坏程度，并视其严重程度对事件进行定级并上报相关部门；再次，采取技术手段追查非法攻击来源；最后，恢复或重建被破坏的系统。

（3） 病毒侵入处置。当发现计算机系统感染病毒后：首先，立即将该计算机从网络上物理隔离，同时备份硬盘数据；其次，启用防病毒软件进行杀毒处理，并使用病毒检测软件对其他机器进行病毒扫描和清除；再次，一时无法查杀的新病毒，要迅速与相关病毒软件供应商联系解决；最后，如感染病毒的是服务器或主机系统，要立即告知使用部门并做好相应清查工作。

（4）数据库安全防范处置。一旦发生数据库崩溃：首先，应关停服务，立即通知有关单位暂缓上传、上报数据；其次，组织技术人员对主机系统进行维修；再次，如遇本地技术人员无法解决的问题，应立即请求软硬件供应商协助解决。最后，系统修复启动后，将最新的备份数据恢复到数据库中。

　　第八条 相关配套机制。各相关单位应根据实际建立本单位值守制度，做到安全事件早发现、早报告、早控制、早解决。各单位应建立健全本单位安全事件应急处置机制，制定安全事件应急预案，定期组织应急演练。

　　第九条 问责制度。各相关单位应按照流程及时、如实地报告和妥善处置安全事件。如有瞒报、缓报、处置和整改不力等情况，将对相关单位进行约谈或通报。

本预案自发布之日起施行。

　　附件：1. 信息技术安全事件情况报告

　　　　　2. 信息技术安全事件整改报告

附件1

南开大学信息技术安全事件情况报告

单位名称：（需加盖公章） 事发时间： 年 月 日 分

|  |  |  |  |
| --- | --- | --- | --- |
| 联系人姓名 |  | 手机 |  |
| 电子邮箱 |  |
| 事件分类 | □ 有害程序事件 □ 网络攻击事件  □ 信息破坏事件 □ 设备设施故障  □ 灾害事件 □其他\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| 事件分级 | □Ⅰ级 □Ⅱ级 □Ⅲ级 □Ⅳ级 | | |
| 事件概况 |  | | |
| 信息系统的基本情况（如涉及请填写） | 1. 系统名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2. 系统网址和IP地址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 3. 系统主管单位/部门：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 4. 系统运维单位/部门：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 5. 系统使用单位/部门：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 6. 系统主要用途：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   1. 是否定级 □是 □否，所定级别：\_\_\_\_\_ 2. 是否备案 □是 □否，备案号：\_\_\_\_\_\_\_\_\_\_ 3. 是否测评 □是 □否 4. 是否整改 □是 □否 | | |
| 事件发现与处置的简要经过 |  | | |
| 事件初步估计的危害和影响 |  | | |
| 事件原因的初步分析 |  | | |
| 已采取的应急措施 |  | | |
| 是否需要应急支援及需支援事项 |  | | |
| 安全负责人意见（签字） |  | | |
| 主要负责人意见（签字） |  | | |

附件2

南开大学信息技术安全事件整改报告

单位名称：（需加盖公章） 报告时间： 年 月 日

|  |  |  |  |
| --- | --- | --- | --- |
| 联系人姓名 |  | 手机 |  |
| 电子邮件 |  |
| 事件分类 | □ 有害程序事件 □ 网络攻击事件  □ 信息破坏事件 □ 设备设施故障  □ 灾害事件 □其他\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| 事件分级 | □Ⅰ级 □Ⅱ级 □Ⅲ级 □Ⅳ级 | | |
| 事件概况 |  | | |
| 信息系统的基本情况（如涉及请填写） | 1.系统名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  2.系统网址和IP地址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  3.系统主管单位/部门：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  4.系统运维单位/部门：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  5.系统使用单位/部门：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  6.系统主要用途：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  7.是否定级 □是 □否，所定级别：\_\_\_\_\_  8.是否备案 □是 □否，备案号：\_\_\_\_\_\_\_\_\_\_  9.是否测评 □是 □否  10.是否整改 □是 □否 | | |
| 事件发生的最终判定原因（可加页附文字、图片以及其他文件） |  | | |
| 事件的影响与恢复情况 |  | | |
| 事件的安全整改措施 |  | | |
| 存在问题及建议 |  | | |
| 安全负责人意见（签字） |  | | |
| 主要负责人意见（签字） |  | | |