附件

中国测绘科学研究院

泄密事件报告登记表

填报部门：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 泄密事件发现过程  (可附页) | 发现时间 |  | 发现地点 |  |
| 发现人姓名 |  | 联系电话 |  |
| 简要经过: | | | |
| 泄密事件基本情况  （可附页） | 责任人姓名 |  | 职务 |  |
| 发生时间 |  | 发生地点 |  |
| 泄密形式 |  | 泄密密级 | 秘密□ |
| 泄密内容及经过： | | | |
| 造成或可能造成的危害 |  | | | |
| 已采取或拟采取的补救措施 |  | | | |
| 初步责任认定及处理意见 |  | | | |
| 事发部门  意见 | 签字：  年 月 日 | | | |
| 保密办公室  意见 | 签字：  年 月 日 | | | |
| 保密工作  领导小组  意见 | 签字：  年 月 日 | | | |

注：此表保密办留存。

备份与恢复预案

**一、总则**

（一）编制目的

为建立健全涉密信息系统电源、设备、应用系统及网络的备份与恢复工作机制，提高应对意外突发事件的组织指挥和应急处置能力，最大限度地减少意外事故带来的损失，及时修复系统和恢复数据，保障信息系统的正常运行。

（二）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》、《中华人民共和国计算机信息网络国际联网安全保护管理办法》等有关法规文件精神，结合实际情况，特制定本预案。

（三）适用范围

本预案适用于涉密信息系统中电源的备份与恢复、设备的备份与恢复、应用的备份与恢复、网络的备份与恢复。

**二、组织机构及职责**

（一）保密工作领导小组负责协调各部门处理备份与恢复事件；

（二）信息中心负责进行备份与恢复；

（三）保密办负责防止备份与恢复过程中出现泄密事件。

**三、备份与恢复机制**

信息中心应从制度建立、技术实现、业务管理等方面建立健全网络安全的备份与恢复机制，在备份与恢复过程中，应全面考虑信息系统运行的安全保密和影响范围等因素，安全产品优先于应用系统，涉密系统优先于非涉密系统，影响范围大的系统优先于范围小的系统。

（一）备份与恢复顺序

安全产品：首先备份和恢复防火墙系统；其次备份和恢复身份认证及访问控制系统；再次备份和恢复防病毒系统；最后进行其它安全管理系统的备份与恢复。

应用系统：首先备份和恢复数据库系统，其次备份和恢复应用服务器系统。

网络设备：首先备份和恢复核心交换机，其次备份和恢复安全管理交换机，最后备份和恢复楼层接入交换机。

（二）备份

根据信息系统需要备份的内容，可以分为硬件备份、操作系统备份、数据库备份、策略备份、软件备份和其它数据备份等类别。

1．硬件备份

关键设备必须有硬件备份，保证在应急情况下有设备能够进行即时恢复。

①电源必须采用UPS备份，并且随时有充足的电能存储能够进行半小时电源保障，以便能有充足时间能够进行设备关机；

②关键设备服务器需要进行备份，备份服务器需要提前预装好操作系统，以便在出现紧急情况能及时恢复关键设备服务器。

2．操作系统备份

服务器操作系统应有备份，每半年至少备份一次。操作系统备份可采用光盘启动服务器，使用GHOST软件将操作系统备份至其它分区，每半年至少一次将备份的操作系统刻录成光盘或转到其它地方进行备份。

3．数据库备份

数据库分为MYSQL数据库、SQL SERVER数据库，数据不同的数据库采取不同的备份方式。

MYSQL数据库

方法一：暂停MYSQL数据库，拷贝MYSQL数据库文件（默认在D:\mysql\data目录下）至最后一个分区进行备份；

方法二：DOS模式下进入D:\mysql\bin目录，运行命令（“mysqldump -u username – p password – all - databases>b ackupfile.sql”）进行备份，把此命令写成批处理文件并且使用操作系统的计划任务，操作系统定期执行备份。

SQL SERVER数据库

依次打开开始菜单→程序→Microsoft SQL Server 2008 → SQL Server Management Studio→选择需要备份的数据库（如：OA\_System\_db），点击鼠标右键→任务→备份→在打开的“备份数据库OA\_System\_db”对话框中，先点击删除，然后点击“添加”→在弹出的“选择备份目标”对话框中，单击“文件名（F）”下方文件路径框右侧的按钮选择备份文件存放路径→文件类型选择“所有文件”→“文件名”填写备份数据库的名字（最好在备份的数据库名字后面加上日期，以方便日后查找）→连续点击“确定”按钮即可，直至备份完成。

4、策略备份

涉密信息系统策略备份根据软件不同采取不同的备份方式，可以导出策略文件的，采用导出策略文件方式进行备份，不能导出策略文件的，采用文档的方式将策略内容记录在文档中进行备份。

5．软件备份

采用将软件拷贝至服务器最后一个分区存放进行备份或采用将软件光盘集中存放的方式进行备份。

6．其它数据备份

数据备份除采用将数据备份至最后一个分区进行备份外，还应每六个月至少一次将数据刻成光盘或者使用其它方式导出进行异地备份。

（三）恢复

根据信息系统需要恢复的内容可以分为硬件恢复、操作系统恢复、数据库恢复、策略恢复、软件恢复和其它数据恢复等。

1．硬件恢复

关键设备必须有硬件备份，在恢复时首先在原硬件基础上尝试恢复，不能进行恢复时应当能提供备用设备，在备用设备上恢复原设备策略。没有备用设备时，应及时上报保密工作领导小组，协调联系硬件厂商进行紧急采购，在有效时间内采购设备并进行恢复。

2．操作系统恢复

操作系统恢复时首先使用光盘启动计算机，然后通过GHOST软件进行恢复，恢复之前应当首先确定原系统内没有需要导出的数据。

3．数据库恢复

数据库分为MYSQL数据库、SQL SERVER数据库，数据不同的数据库采取不同的恢复方式。

1）MYSQL数据库

方法一：暂停MYSQL数据库，拷贝MYSQL数据库备份文件至数据库目录（默认在D:\mysql\data目录下）；

方法二：DOS模式下进入D:\mysql\bin目录，运行命令（“mysql - u username – p password – all - databases>b ackupfile.sql”）进行恢复。

2）SQL SERVER数据库

选择需要还原的数据库（如：OA\_System\_db），点击鼠标右键→任务→还原→在打开的“还原数据库OA\_System\_db”对话框中选择“源设备”，单击文件路径框右侧的按钮→在出现的“指定备份”对话框中，点击“添加”按钮，找到数据库备份的路径，选择需要还原的数据库“XX”（注意：文件类型选择所有文件），然后连续“两次”点击“确定”按钮→在出现的“还原数据库—OA\_System\_db”对话框中，勾选上“选择用户还原的备份集”下的数据库前的复选框→然后选择“选项”，勾选上“覆盖现有数据库”→连续点击“确定”按钮即可，直至还原成功。

4、策略恢复

信息系统策略恢复根据软件不同采取不同的恢复方式，可以导入策略文件进行恢复的，采用按照策略文档进行手动配置进行恢复。

**四、后期处置**

备份与恢复过程中应首先考虑安全保密，确保在安全保密的情况下进行备份与恢复，备份与恢复过程中做好登记与记录，保证在下次进行备份与恢复时能够及时有效的进行。

**五、保障措施**

信息中心应保障备份存储设备的安全，确保有效、可用，保密办负责监督管理部门正常执行备份与恢复工作。

**六、附则**

本预案由信息中心负责解释。

本预案发布之日起施行。

应急响应预案

**一、总则**

（一）编制目的

为建立健全的系统保障应急工作机制，提高应对突发事件的组织指挥和应急处置能力，顺利应对突发事件，妥善处置紧急情况，最大限度地减少意外事故带来的损失，保障网络安全，确保网络安全畅通。

（二）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》、《中华人民共和国计算机信息网络国际联网安全保护管理办法》等有关法规文件精神，结合实际情况，特制定本应急预案。

（三）适用范围

本预案适用于下述网络保障、网络恢复和泄密事件的处理工作：1、网络布线系统；２.机房；３.网络系统各管理部门；４.网络系统服务器和交换设备；５.泄密事件的处理。

**二、组织机构及职责**

（一）部门负责人负责协调各部门处理应急事件；

（二）信息中心负责了解突发事件情况，向保密工作领导小组报告并提出处理建议，按照指令实施网络应急处理工作；

（三）保密办负责网络泄密事故的具体处理工作；

（四）保卫处、保密办和信息中心负责网络设备失窃的处理工作和机房失火的扑救工作；

（五）重大突发事件造成网络通信中断或网络通信严重受阻时，任何职工和部门都有义务通过各种途径向部门领导和信息中心报告情况。

**三、预防和预警机制**

信息中心及各部门应从制度建立、技术实现、业务管理等方面建立健全网络安全的预防和预警机制。

（一）预防机制

网络应急工作应坚持早预防、早发现、早报告、早处置的方针。各有关部门要对应急保障的重点网络、重点环节、重点场所、重点地区进行监测，分析可能出现的各种紧急情况，建立和完善安全预警信息预测预报机制，并加强重点监管。

（二）预警监测

信息中心应提交网络正常运行具备的条件保障报告，供相关部门配置参考；应贯彻落实系统安全规划和工作要求，不断提高网络自愈与抗毁能力。加强重点保障目标的应急预防和演练，增强应对突发事件的保障能力。不断完善系统保障准备工作。

（三）预警分级和发布

1．预警分级

预警划分为三个等级：1、Ⅰ级(重大)：因特别重大突发事故引发的，可能造成研究院网络运行全面中断的情况，出现泄密事件；2、Ⅱ级(较大)：因较大设备事故及突发网络事件引发的，可能造成研究院基础网络通信多点通信故障； 3、Ⅲ级(一般)：因一般设备故障件引发的，有可能造成研究院局部网络通信故障的情况。

响应分级对应预警等级的划分。

2．预警发布

保密工作领导小组得到网络突发事件信息后，可以确认并发布Ⅰ级预警信息；信息中心得到网络突发事件信息后，应初步判断事件性质、级别，确认并发布Ⅱ级和Ⅲ级预警信息并决定是否启动应急预案、启动相应级别的应急预案。

**四、应急响应**

1．应急预案启动

有下列情况应启动应急预案：1、计算机机房、各配线间发生火灾；2、交换系统设备故障；3、服务器故障；4、发现系统遭到攻击；5、网络设备发生被盗或人为损坏；6、发现系统泄密；7、系统出现病毒；8、临时停电。

2．应急处置

发生火灾事故、交换系统设备故障、服务故障、系统遭到攻击、网络设备被盗或人为损坏、系统泄密、系统出现病毒、临时停电及其他事件时，应启动应急处置程序。

1、火灾事故发生时处理办法

报警程序：①当火灾发生时，立即切断电源，根据火势如需报警立即就近用电话或手机报告消防中心（电话：119），报告内容为：“中国测绘大厦（北京市海淀区莲花池西路28号）发生火灾，请迅速前来扑救”，待对方放下电话后再挂机，同时将火情通知保密工作领导小组；②备好应急灯（或手电筒）；③向保卫处值班人员报告，并派人等待引导消防车辆。

组织实施：①在消防车到来之前，先尽量使用现有消防设备将火势控制在最小；②消防车到来之后，院人员配合消防专业人员扑救或作好辅助工作；③使用器具：灭火器、水桶、脸盆等；④迅速组织人员逃生，原则是“先救人，后救物”。

扑救方法：可用大楼配备的灭火器灭火。

注意事项：①火灾事故首要的一条是保护人员安全，扑救要在确保人员不受伤害的前提下进行；②发现火灾时应掌握的原则是边救火，边报警；③人员在逃生时应掌握正确的逃离方法；④相关领导配合有关部门调查分析火灾原因，进行防火措施改进。

2、交换系统设备故障发生，应启动应急处置程序

①交换机发生故障时，用同系列备机替换，替换下来的交换机及时送修，等修好将备机进行替换；②光纤收发器出现故障时，用同型号的光纤收发器替换，故障机报修。

3、服务器故障

①首先尝试修复故障，不能快速修复故障时，应及时联系相关人员协助；②当办公应用服务器和安全管理服务器同时出现问题，应首先解决安全管理服务器故障；③服务器发生故障如不能恢复，应立即在备份服务器上提取相应的数据，及时将所有数据恢复到另外一台备用服务器上，替换原来的配置，提供服务；如果没有备用设备，应及时联系相关人员紧急调配备用设备。

4、发现系统遭到攻击

①当发现服务器或涉密计算机遭到攻击时，用户应及时通告系统管理员；②系统管理员确认后立即阻断攻击，确认攻击源，记录相关网络行为；③通知保密办，提交攻击源资料。

5、网络设备发生被盗或人为损害处理办法

报警程序：①发现案件时应及时向保卫处报警；②根据案情报告保密办和保密工作领导小组；③经领导同意后向公安机关报案。

处置措施：保护现场。

注意事项：①注意保护现场，以便为侦破案件提供条件；②积极协助公安人员勘察现场，为侦破提供条件。

6、发现系统泄密处理办法

以下情况视为泄密事件：①在非密计算机中处理、存储涉密信息；②私自将涉密计算机连接到其它网络；③在非密计算机使用涉密载体；④在互联网网站发布涉密信息以及通过电子邮件、论坛等方式处理、传输涉密信息。

报警程序：①向保密办报告；②向保密办和保密工作领导小组报告；③经领导同意后向国家保密局报告。

处置措施：①阻断传播端口；②保存泄密事件网络行为证据；③锁定违法者的人员信息、IP地址等；④清除泄密信息，直至网络处于安全状态；⑤报告保密办。

注意事项：①遇事一定要冷静，果断采取措施；②网络泄密突发事件处理原则是：先查封违法者的IP地址，后报警，及时控制事态的发展。

7、系统出现病毒处理办法

系统管理员定期下载更新病毒库，如发现有新的不明病毒传播，系统管理员应立即上网查询相关信息，确认病毒类型，并上网更新病毒库，然后通告所有用户防病毒方法，督促各部门进行杀毒处理，直至网络处于安全状态。

对不良信息追查信息来源，对擅自发布信息而造成不良影响者，按照有关规定给予处分。触犯法律者，移交执法机关追究法律责任。

8、临时停电的处理办法

临时停电事件发生时，应先等待10分钟，如果在10分钟之内没有来电，则首先关闭应用服务器、交换机，然后关闭安全服务器，最后关闭UPS。

当来电时应首先启动安全产品，保障安全产品正常运行的情况下恢复应用系统。

9、其它事件

当发生其他影响系统正常运行的事件时，首先应查明情况，了解解决问题的最快时间和造成的影响，根据情况首先停用应用系统，最后停用安全服务器。

**五、后期处置**

网络运行和服务恢复应急工作完成后，信息中心应及时写出调查报告，报保密工作领导小组。调查报告主要内容包括：事故发生的时间、地点、原因、影响程度和直接、间接经济损失情况；应急救援参加单位、投入人员、设备情况；应急救援过程、经费决算、实际效果；诱发事件或应急救援不力的主要责任部门和个人。

对重大和特大网络突发事件，由研究院组织相关领导、专家负责对网络事故原因进行调查、分析和处理，对事故后果进行评估，并对事故责任处理情况进行监督检查。

**六、保障措施**

（一）网络建设基础资料

定期备份、及时更新网络系统的建设时的相关技术图纸、网络拓扑结构图、网络资产清单、网络设备分布图和相关部门及主管领导联系方式。

（二）技术储备与保障

信息中心平时应加强技术储备与保障管理工作，建立网络安全技术知识库，定期组织相关人员认真学习。适时组织相关专家和机构分析当前网络通信安全形势，对网络保障应急预案及实施进行评估，开展网络保障的现场研究，加强技术储备。

（三）宣传、培训和演习

各级网络通信保障应急管理机构，应加强对网络通信安全和网络通信保障应急的宣传教育，定期或不定期地对有关网络通信保障应急指挥管理机构和保障人员进行技术培训和应急演练，保证应急预案的有效实施，不断提高网络通信保障应急的能力。

**保密应急演练记录表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 演练时间 |  | | 演练地点 |  |
| 演练名称 |  | | 指挥人 |  |
| 参加人： | | | | |
| 演练过程记录： | | | | |
| 演练存在的问题及整改措施： | | | | |
| 演练评价人签字/日期： | | 保密总监签字/日期： | | |

**附注：本制度汇编中的表格将根据国家保密有关规定和院实际情况适时调整，最新**

**版本以保密办提供的为准。**