|  |
| --- |
| **网络安全应急响应控制程序** |

|  |  |
| --- | --- |
| 编号 |  |
| 编制 |  |
| 审核 |  |
| 批准 |  |
| 发布日期 |  |

**XXX公司**

**修改记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 文件更改内容  | 修改日期 | 修改人 | 版本 |
| 1 | A |  |  | V1.0 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. 新增，M-修改，D-删除）

目录

[1.目的 3](#_Toc14258820)

[2.范围 4](#_Toc14258821)

[3.职责 4](#_Toc14258822)

[4.术语 4](#_Toc14258823)

[5.程序 4](#_Toc14258824)

[5.1网络安全事件风险管理 4](#_Toc14258825)

[5.2应急响应措施验证 4](#_Toc14258826)

[5.2.1黑客攻击事件紧急处置措施 4](#_Toc14258827)

[5.2.2病毒事件紧急处置措施 5](#_Toc14258828)

[5.2.3软件系统遭破坏性攻击的紧急处置措施 5](#_Toc14258829)

[5.2.4数据库安全紧急处置措施 6](#_Toc14258830)

[5.2.5广域网外部线路中断紧急处置措施 6](#_Toc14258831)

[5.2.6局域网中断紧急处置措施 7](#_Toc14258832)

[5.2.7设备安全紧急处置措施 7](#_Toc14258833)

[5.3用户告知、召回 8](#_Toc14258834)

[6.相关文档 8](#_Toc14258835)

[7.相关记录 8](#_Toc14258836)

# 1.目的

为切实做好网络突发事件的防范和应急处理工作，提高预防和控制网络突发事件的能力和水平，减轻或消除突发事件的危害和影响，确保网络与信息安全，特制定本应急程序。

# 2.范围

本程序适用于XXX公司医疗网络安全应急。

# 3.职责

# 4.术语

# 5.程序

## 5.1网络安全事件风险管理

网络安全事件应纳入风险管理的范围，正确识别网络安全事件引入的风险，进行风险评估，必要时制订适当的风险控制措施降低风险等级到合理可接受水平。产品上市后，应对实际发生的网络安全事件进行评估，以确认既有的风险控制措施是否充分。

## 5.2应急响应措施验证

## 5.2.1黑客攻击事件紧急处置措施

5.2.1.1当发现黑客正在进行攻击时或者已经被攻击时，首先将被攻击的服务器等设备从网络中隔离出来，保护现场，并将有关情况向本单位信息化领导小组汇报。

5.2.1.2信息安全相关负责人应在接到通知后立即赶到现场，对现场进行分析，并做好记录，必要时上报主管部门。

5.2.1.3恢复与重建被攻击或破坏系统。

5.2.1.4信息化领导小组召开会议，如认为事态严重，则立即向市政府信息化办公室和公安部门报警。

## 5.2.2病毒事件紧急处置措施

5.2.2.1当发现有计算机被感染上病毒后，应立即向信息安全负责人报告，将该机从网络上隔离开来。

5.2.2.2信息安全相关负责人员在接到通报后立即赶到现场。

5.2.2.3对该设备的硬盘进行数据备份。

5.2.2.4启用反病毒软件对该机进行杀毒处理，同时通过病毒检测软件对其他机器进行病毒扫描和清除工作。

5.2.2.5如果现行反病毒软件无法清除该病毒，应立即向本单位信息化领导小组报告，并迅速联系有关产品商研究解决。

5.2.2.6信息化领导小组开会研究，认为情况严重的，应立即市政府信息化办公室和公安部门报警。

## 5.2.3软件系统遭破坏性攻击的紧急处置措施

5.2.3.1重要的软件系统平时必须存有备份，与软件系统相对应的数据必须按本单位容灾备份规定的间隔按时进行备份，并将它们保存于安全处。

5.2.3.2一旦软件遭到破坏性攻击，应立即向信息安全负责人报告，并将该系统停止运行。

5.2.3.3检查信息系统的日志等资料，确定攻击来源，并将有关情况向本单位信息化领导小组汇报，再恢复软件系统和数据。

5.2.3.4信息化领导小组召开会议，如认为事态严重，则立即市政府信息化办公室和公安部门报警。

## 5.2.4数据库安全紧急处置措施

5.2.4.1对于重要的信息系统，主要数据库系统应按双机设备设置，并至少要准备两个以上数据库备份，平时一个备份放在机房，另一个备份放在另一安全的建筑物中。

5.2.4.2一旦数据库崩溃，值班人员应立即启动备用系统，并向信息安全负责人报告。

5.2.4.3在备用系统运行期间；信息安全工作人员应对主机系统进行维修并作数据恢复。

5.2.4.4如果两套系统均崩溃而无法恢复，应立即向有关厂商请求紧急支援。

## 5.2.5广域网外部线路中断紧急处置措施

5.2.5.1广域网线路中断后，值班人员应立即向信息安全负责人报告。

5.2.5.2信息安全相关负责人员接到报告后，应迅速判断故障节点，查明故障原因。

5.2.5.3如属我方管辖范围，由信息安全工作人员立即予以恢复。

5.2.5.4如属电信部门管辖范围，立即与电信维护部门联系，要求修复。

5.2.5.5如有必要，向本单位信息化领导小组汇报。

## 5.2.6局域网中断紧急处置措施

5.2.6.1设备管理部门平时应准备好网络备用设备，存放在指定的位置。

5.2.6.2局域网中断后，信息安全相关负责人员应立即判断故节点，查明故障原因，并向网络安全组组长汇报。

5.2.6.3如属线路故障，应重新安装线路。

5.2.6.4如属路由器、交换机等网络设备故障，应立即从指定位置将备用设备取出接上，并调试通畅。

5.2.6.5如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调测通畅。

5.2.6.6如有必要，向本单位信息化领导小组汇报。

## 5.2.7设备安全紧急处置措施

5.2.7.1服务器等关键设备损坏后，值班人员应立即向信息安全负责人报告。

5.2.7.2信息安全相关负责人员立即查明原因。

5.2.7.3如果能够自行恢复，应立即用备件替换受损部件。

5.2.7.4如属不能自行恢复的，立即与设备提供商联系，请求派维护人员前来维修。

5.2.7.5如果设备一时不能修复，应向本单位信息化领导小组汇报。

## 5.3用户告知、召回

发生网络安全事件后，研发生产部应及时评估事件对软件产品安全有效性的影响，以及如何采取措施降低该影响。当措施影响已注册发布的软件产品时，应遵照《不良事件、忠告性通知及召回管理程序》通知客户或进行产品召回。

# 6.相关文档

《不良事件、忠告性通知及召回管理程序》

# 7.相关记录

