**XXX单位**

**恶意代码防范管理制度**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479446683)

[2 适用范围 1](#_Toc479446684)

[3 岗位职责 1](#_Toc479446685)

[4 管理细则 2](#_Toc479446686)

[4.1 防病毒、恶意代码策略 2](#_Toc479446687)

[4.2 防病毒、恶意代码管理 3](#_Toc479446688)

[4.3 预防恶意软件的通用要求 5](#_Toc479446689)

[4.4 对重要系统的防范恶意软件的特殊要求 5](#_Toc479446690)

[5 响应时限 5](#_Toc479446691)

[6 附则 6](#_Toc479446692)

# 目的

为防止计算机病毒、网络蠕虫、特洛伊木马及逻辑炸弹等恶意软件对XXX单位信息处理设备的攻击造成信息的保密性、完整性、可用性被破坏和业务中断，特制定本制度来保护信息处理设备正确、安全使用，保障信息系统和日常工作的正常进行。

# 适用范围

本制度适用于XXX单位对计算机病毒、网络蠕虫、特洛伊木马及逻辑炸弹等恶意软件的防范和管理。

所谓恶意软件/代码，是指编制或者在计算机程序中插入的破坏计算机功能、毁坏数据、窃取数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。主要是指各类计算机病毒、木马及恶意移动代码等。所谓批处理(Batch)，也称为批处理脚本。批处理就是对某对象进行批量的处理。

# 岗位职责

信息中心负责XXX单位恶意软件/代码防范管理制度的制定、审查及修订工作。负责恶意软件/代码的防治、病毒库的更新、恶意软件/代码引起的信息安全事件的处理、系统故障恢复等工作，为XX单位信息系统提供安全的技术性支持。信息中心以下设安全管理员和网络管理员岗位。

**安全管理员工作职责：**

1）贯彻和落实上级及本单位相关管理制度，开展信息安全管理

2）组织开展信息安全体系建设，组织实施信息安全管理工作，制定和落实安全策略

3）组织开展信息系统等级保护和安全风险管理工作，开展关键业务系统的应急演练工作

4）实施全局IP地址规划、设置、管理工作

5）落实防病毒系统等信息安全措施及日常管理工作，实施防火墙、入侵检测、审计等安全专用设备的日常维护和运行管理工作

6）完成领导交办的其它工作

**网络管理员工作职责：**

1）贯彻和落实上级及本单位相关管理制度，开展网络管理工作

2）开展本单位网络基础设施等规划、建设及日常运行维护工作

3）负责网络的部署以及网络产品、网络安全产品的配置、管理与监控，并对关键网络配置文件进行备份，及时修补网络设备的漏洞

4）在网络及设备异常或故障发生时，详细记载发生异常时的现象、时间和处理方式，并及时上报

5）编制网络设备的维修、报损、报废等计划，报主管领导审核

6）完成领导交办的其他任务

各相关管理员负责所辖防病毒系统相关各类技术资料、运行记录等文档的归档工作以及文件数据的备份工作。

# 管理细则

## 防病毒、恶意代码策略

应通过服务器自动安装客户端计算机防病毒和恶意代码防护软件，定期对防病毒软件、恶意代码防护软件进行版本升级，及时更新病毒库、恶意代码特征库。

应通过管理工具平台统一设置防病毒策略，实时防治病毒，获取完整的病毒活动日志。

应指导、帮助计算机用户使用防病毒和恶意代码防护软件查杀病毒、清理恶意插件，并对本单位计算机信息系统使用人员进行计算机病毒防治教育和培训。

信息中心组织各部门进行有关防病毒及其他后门程序等恶意软件预防工作的培训，使各部门明确病毒及其他恶意软件的管理程序及责任，具体执行出现重大病毒疫情时，达到启动应急预案要求的应启动应急预案，并立即向上级领导报告。

## 防病毒、恶意代码管理

单位所有接入生产网络的服务器及个人计算机必须安装统一要求的防病毒软件。在使用计算机的任何时间必须运行防病毒软件，进行定期病毒检测和清除。各部门或科室、各用户不允许自行安装非统一选型的防病毒软件。

各部门或科室和个人从互联网上下载程序、数据以及购置、维修、借入信息处理设备时，应当进行病毒检测。

各部门或科室和个人不得故意制作计算机病毒、编写恶意代码和攻击工具；不得向社会发布虚假的计算机病毒疫情。各部门或科室和个人不得故意输入计算机病毒，危害计算机信息系统安全；不得向他人提供含有计算机病毒的文件、软件、媒介。用户必须遵守防病毒系统管理规定，不得故意制造或传播病毒，不得散布计算机病毒疫情、处理工具或处理办法。

对于配置低、不适宜安装防病毒软件的计算机（此类机器不得与办公网络相连，否则必须安装防病毒软件），由所属各部门或科室每月至少一次进行病毒查杀和防范控制，并填写人工查杀病毒记录表。

防病毒软件须保持最新病毒定义更新，能自动更新病毒定义的必须接受指定防病毒服务器管理进行更新，不能自动更新病毒定义的须在每次连接互联网时自行更新病毒定义。各部门或科室联网计算机接受防病毒服务器的管理，在每次开机时自动从防病毒服务器上下载最新病毒库。

单位用户须减少高风险操作降低病毒感染的可能性，在安装或使用从其它渠道获得的电脑文件前进行病毒检测，禁止安装或使用未经检测过的软件或带毒软件，避免使用互联网下载文件、打开电子邮件附件以及通过即时通讯工具传送文件等。

对于防病毒系统不能清除的病毒，用户应及时向防病毒管理员报告。在问题处理之前应禁止使用感染该病毒的文件，同时断开网络连接。

应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。

应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

特殊情况，如某种新恶性病毒大规模爆发，网络管理员应立即升级病毒库，并紧急通知信息技术部立即进行病毒库更新升级，同时立即进行病毒扫描，并对病毒情况汇报信息中心负责人。

新购置、借入或维修返回的计算机，软盘、光盘以及其它移动存储介质在使用前应进行病毒检测和清除。

各部门或科室在使用各部门或科室以外的任何电子媒体前都应对其进行病毒扫描，对发现病毒的电子媒体应禁用，待病毒清除后方可使用，对于不能清除的病毒，应及时报告网络管理员处理处理。

各部门或科室用户应在计算机或其它电子信息处理设施的启动后检查是否已启动病毒实时监测系统。如未启动，应在进行其他操作前启动病毒实时监测系统。

各部门或科室在使用电子邮件或下载软件时应启动病毒实时监测系统的实时防护，以便对电子邮件进行病毒检查。

网络管理员需加强对特洛伊木马的探测与防治。通过以下措施予以控制：

(1) 安装正版反病毒软件；

(2) 使用正版软件；

(3) 对软件更改进行控制；

(4) 对软件开发过程及引进过程进行控制；

(5) 其他必要措施。

运行批处理脚本需各部门或科室领导审批。并对其进行测试，确保安全的情况下方可执行。

凡因违反上述规定，致使计算机感染病毒，造成数据丢失或系统瘫痪的人员，将对其行为所产生的后果承担相关责任，依据相关管理条例对其进行处理。

蓄意传播病毒、触犯国家有关法律或规定的人员由相关部门依照国家有关法律、法规进行处罚。

## 预防恶意软件的通用要求

保护不受恶意软件攻击的基础是安全意识，适当的系统权限。所有员工应养成良好的防范恶意软件意识并遵守以下规定：

1）按照本制度规定的要求使用防病毒软件；

2）禁止使用来历不明的软件；

3）禁止计算机在未安装有效防病毒软件的情况下从互联网上下载软件；

4）删除来历不明的电子邮件；

5）使用介质前应进行病毒检查。

## 对重要系统的防范恶意软件的特殊要求

网络管理员应与防火墙供应商保持联系，确保功能及时升级并实施严密的安全策略，确保中心网络的安全。

对于涉及单位机密等重要系统严格实施网络隔离政策，严禁采取其它措施与互联网连接。

信息技术部应按照信息备份的要求进行重要数据和软件的备份。

如果发生信息处理设施受到病毒或其他种类的恶意软件攻击的事故，应由网络管理员确认事故原因后，对被破坏数据或软件进行恢复。

对各部门或科室安装的外购软件在使用前必须测试其安全性。

对测试发现的各种恶意软件立即停止使用，各部门或科室在使用过程中发现有恶意软件及相应迹象应立即通知信息技术部，交由该各部门或科室处理。

各部门或科室如受到各种恶意软件攻击，应及时向信息技术部报告。

# 响应时限

所有病毒防护的负责部门或人员应严格遵守病毒响应时限的要求。如无法在病毒响应时限内完成对病毒的响应工作，应及时上报单位信息安全管理部门进行协调解决并承担相应责任。

办公终端感染病毒的（非蠕虫类），应在发现时（防病毒系统记录或技术支持电话记录）起2小时内进行解决。

办公终端感染蠕虫的，应在发现时（防病毒系统记录或技术支持电话记录）起30分钟内进行解决。

服务器、监控平台等生产设备感染病毒的（非蠕虫类），应在发现时（防病毒系统记录）起1小时内进行解决。

服务器、监控平台等生产设备感染蠕虫的，应在发现时（防病毒系统记录）起30分钟内进行解决。如果该设备会对其他生产设备产生影响时，应立刻切断该设备与网络的连接。

# 附则

本文件由XXX单位信息中心负责解释与修订。

本文件自颁布之日起发布执行。