**XXX单位**

**安全管理组织规范**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479441245)

[2 适用范围 1](#_Toc479441246)

[3 安全组织 1](#_Toc479441247)

[3.1 信息安全管理中心 1](#_Toc479441248)

[3.2 信息安全工作组 1](#_Toc479441249)

[4 审批管理 2](#_Toc479441250)

[4.1 审批权限 2](#_Toc479441251)

[4.2 审批内容 2](#_Toc479441252)

[4.3 审批程序 2](#_Toc479441253)

[5 安全职责 2](#_Toc479441254)

[5.1 安全主管 3](#_Toc479441255)

[5.2 安全管理员 4](#_Toc479441256)

[5.3 安全审计员 5](#_Toc479441257)

[5.4 系统管理员 6](#_Toc479441258)

[5.5 网络管理员 7](#_Toc479441259)

[5.6 数据库管理员 8](#_Toc479441260)

[5.7 应用管理员 9](#_Toc479441261)

[5.8 机房管理员 10](#_Toc479441262)

[5.9 资产管理员 11](#_Toc479441263)

[6 附则 11](#_Toc479441264)

# 目的

为加强XXX单位信息安全管理，明确信息安全责任，保障信息化建设的稳步发展，特制定本规范。

# 适用范围

本规范适用于XXX单位信息系统安全组织。

# 安全组织

建立专门的信息安全管理中心和安全工作组。

## 信息安全管理中心

信息安全管理中心负责领导落实信息系统安全建设的总体规划，制定本单位安全工作规划的制定与实施，承担如下职责：

(一) 在信息系统网络与信息安全总体方针的指导下，负责组织制定信息系统安全策略并审批部门上报的信息系统安全策略；

(二) 负责组织细化上级规章制度，制定相应程序指南，并监督落实规章制度；

(三) 负责信息系统安全管理层人员权限授予工作；

(四) 负责审阅部门信息安全工作报告；负责信息部门重大安全事故查处与汇报工作。

## 信息安全工作组

信息安全工作组从事具体的安全工作，建立和维持信息安全管理体系，在信息系统内部开展和控制信息安全的管理实施，并承担如下职责：

(一) 调整并制定所有必要的信息安全管理规程、制度以及实施指南等；

(二) 配合执行信息安全相关的实施方法和程序，如风险评估、资产分级分类方法等；

(三) 主动采取部门内的信息安全措施，如安全意识培训及教育等；

(四) 审批信息化建设项目规划及设计的安全部分，并监督其实施落实；

(五) 审查信息安全策略的遵循性；

(六) 审查、监控、协调信息安全相关事件的评估和响应；

(七) 辅助领导机构进行安全方面的决策；

(八) 根据信息安全管理体系的要求，定期向上级主管领导和信息安全管理中心报告。

# 审批管理

## 审批权限

对本部门或科室各项重要活动的审批。

## 审批内容

审批内容（重要活动）包括网络系统、应用系统、数据库管理系统、重要服务器和设备等重要资源的访问，系统变更，网络系统的接入，重要管理制度的制定和发布，人员的配备、培训，产品的采购，第三方人员的访问、管理，与合作单位的合作项目等。

## 审批程序

相关部门或科室将相关需要审批的内容，提交信息安全管理中心审核，并填写对应审批表，按审批权限进行逐级审批。经相关部门或科室负责人审批通过后，方实施。

# 安全职责

网络与信息安全责任分配的基本原则是“谁主管、谁负责；谁运维、谁负责；谁使用、谁负责”。

信息安全相关工作应遵循职责分离的原则，以减少误用或滥用权力带来风险的概率，在无法实现职责充分分离的情况下，应采取其他补偿控制措施并制定流程文档记录在案。

## 安全主管

（一）岗位职责

1）严格维护及遵守国家的一切法律、条例、带头遵循公司、部门各项规章制度；

2）准确传达执行单位各项工作指令，全面主持部门安全工作；

3）组织对的信息安全工作制度和技术操作策略进行审查，拟订信息安全总体策略规划，并监督执行；

4）负责协调、督促各部门和有关单位的信息安全工作，参与信息系统工程建设中的安全规划，监督安全措施的执行；

5）组织信息安全工作检查，分析信息安全总体状况，提出分析报告和安全风险的防范对策；

6）负责接受各部门的紧急信息安全事件报告，组织进行事件调查，分析原因、涉及范围，并评估安全事件的严重程度，提出信息安全事件防范措施，并及时向上级有关部门、单位报告信息安全事件；

7）跟踪先进的信息安全技术，组织信息安全知识的培训和宣传工作；

8）完成领导交办的其它工作.

（二）任职要求

1）教育背景：计算机相关专业；本科及以上学历

2）工作经验：3年及以上本企业工作经验，1年及以上基层工作经验

3）职业资质：具备相应专业中级及以上专业技术资格，或技师及以上技能等级，具备岗位胜任能力合格证书

4）岗位胜任能力：

* 熟悉计算机、网络、安全、信息系统专业知识，了解企业运营管理知识
* 具备较强的计划、组织、沟通、协调、学习、分析、团队领导和文字表达导能力，具有较强的敬业意识和责任心

## 安全管理员

（一）岗位职责

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。

（二）任职要求

1）教育背景：计算机相关专业；大专及以上学历

2）工作经验：1年及以上相关工作经验

3）职业资质：具备相应专业员级及以上专业技术资格，或中级工及以上技能等级，具备岗位胜任能力合格证书

4）岗位胜任能力：

* 了解计算机、网络和信息系统专业知识，了解信息安全知识
* 具备一定的学习、分析和沟通能力，具有较强的敬业意识和责任心

## 安全审计员

（一）岗位职责

1）负责指导并监督系统管理员（包括主机系统管理员、网络管理员、数据库管理员和应用管理员等）及普通用户与安全相关的工作；

2）负责定期对主机系统、网络产品、应用系统的日志文件进行分析审计，发现问题及时上报；

3）负责组织信息系统的安全风险评估工作，并定期进行系统漏洞扫描，形成安全评估报告；

4）根据本单位的信息安全需求，定期提出本单位的信息安全改进意见，并上报信息安全管理部门主管；

5）定期查看信息安全站点的安全公告，跟踪和研究各种信息安全漏洞和攻击手段，在发现可能影响信息安全的安全漏洞和攻击手段时，及时做出相应的对策，通知并指导系统管理员进行安全防范；

6）负责组织审议安全方案、安全审计报告、应急计划以及整体安全管理制度；

7）完成领导交办的其它工作。

（二）任职要求

1）教育背景：计算机相关专业；大专及以上学历

2）工作经验：1年及以上相关工作经验

3）职业资质：具备相应专业员级及以上专业技术资格，或中级工及以上技能等级，具备岗位胜任能力合格证书

4）岗位胜任能力：

* 了解计算机、网络和信息系统专业知识，了解信息安全知识
* 具备一定的学习、分析和沟通能力，具有较强的敬业意识和责任心

## 系统管理员

（一）岗位职责

1）贯彻和落实上级及本单位相关管理制度，负责系统的运行和维护管理；

2）负责主机操作系统的安全配置（包括及时修补系统漏洞）和日常审计，系统应用软件的安装，从系统层面实现对用户与资源的访问控制；

3）负责对所管辖的服务器操作系统进行安全配置，并定期对所管辖的服务器操作系统进行安全检查；

4）在主机系统异常或故障发生时，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）编制主机设备的维修、报损、报废计划，报主管领导审核；

6）完成领导交办的其它工作。

（二）任职要求

1）教育背景：计算机相关专业；大专及以上学历

2）工作经验：1年及以上相关工作经验

3）职业资质：具备相应专业员级及以上专业技术资格，或中级工及以上技能等级，具备岗位胜任能力合格证书

4）岗位胜任能力：

* 了解计算机、网络和信息系统专业知识
* 具备一定的学习、分析和沟通能力，具有较强的敬业意识和责任心

## 网络管理员

（一）岗位职责

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。

（二）任职要求

1）教育背景：计算机相关专业；大专及以上学历

2）工作经验：1年及以上相关工作经验

3）职业资质：具备相应专业员级及以上专业技术资格，或中级工及以上技能等级，具备岗位胜任能力合格证书

4）岗位胜任能力：

* 了解计算机、网络和信息系统专业知识
* 具备一定的学习、分析和沟通能力，具有较强的敬业意识和责任心
  1. 数据库管理员

（一）岗位职责

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）对数据库系统进行安全配置，修补已发现的漏洞；

3）负责数据库系统的用户账号管理，对系统中所有的用户进行登记备案；对数据库系统的用户、口令的安全性进行管理；对数据库系统登录用户进行监测和分析；

4）负责业务数据及系统其它重要数据的备份与备份数据管理工作；

5）为安全审计员提供完整、准确的数据库系统运行活动的日志记录，详细记载发生异常时的现象、时间和处理方式，并及时上报；

6）在发生安全问题导致数据损坏或丢失时，进行数据的恢复；

7）根据业务发展的需求，提交数据存储介质购买或存储系统扩容计划；

8）完成领导交办的其他任务。

（二）任职要求

1）教育背景：计算机相关专业；大专及以上学历

2）工作经验：1年及以上相关工作经验

3）职业资质：具备相应专业员级及以上专业技术资格，或中级工及以上技能等级，具备岗位胜任能力合格证书

4）岗位胜任能力：

* 了解计算机、网络和信息系统专业知识
* 具备一定的学习、分析和沟通能力，具有较强的敬业意识和责任心
  1. 应用管理员

（一）岗位职责

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）对业务应用系统进行安全配置；督促软件开发商提供补丁来修补已发现的漏洞；

3）对业务应用系统的用户、口令的安全性进行管理；对业务应用系统的登录用户进行监测和分析；

4）负责提出数据的备份要求，制定数据备份策略，督促数据库管理员按照备份方案按时完成，并恢复所需数据；

5）实施系统软件版本管理，应用软件备份和恢复管理；

6）完成领导交办的其他任务。

（二）任职要求

1）教育背景：计算机相关专业；大专及以上学历

2）工作经验：1年及以上相关工作经验

3）职业资质：具备相应专业员级及以上专业技术资格，或中级工及以上技能等级，具备岗位胜任能力合格证书

4）岗位胜任能力：

* 了解计算机、网络和信息系统专业知识
* 具备一定的学习、分析和沟通能力，具有较强的敬业意识和责任心
  1. 机房管理员

（一）岗位职责

1）贯彻和落实上级及本单位相关管理制度，开展机房管理工作，其它人员未经允许不得入内；

2）填写机房的值班记录和运行日志，提高设备的完好率和利用率，保证计算机运行可靠性；

3）随时监测机器和网络状况，处理临时出现的故障，确保计算机和网络安全运转；

4）机房内必须保持环境清洁，做好防潮、防尘、防水、防热、 防火、防盗等工作；并定期为服务器及交换机等设备除尘；

5）完成领导交办的其他任务。

（二）任职要求

1）教育背景：计算机相关专业；大专及以上学历

2）工作经验：1年及以上相关工作经验

3）职业资质：具备相应专业员级及以上专业技术资格，或中级工及以上技能等级，具备岗位胜任能力合格证书

4）岗位胜任能力：

* 了解计算机、网络和信息系统专业知识
* 具备一定的学习、分析和沟通能力，具有较强的敬业意识和责任心
  1. 资产管理员

（一）岗位职责

1）贯彻和落实上级及本单位相关管理制度，负责设备管理的日常事务；

2）负责建立和完善设备资料档案；

3）负责信息技术部门全部资产的采购、登记、分发、回收、废弃等管理；

4）协助相关专业主管对重要设备安装、改造、更新、维护、维修计划的制定和组织实施；

5）完成领导交办的其他任务。

（二）任职要求

1）教育背景：计算机相关专业；大专及以上学历

2）工作经验：1年及以上相关工作经验

3）职业资质：具备相应专业员级及以上专业技术资格，或中级工及以上技能等级，具备岗位胜任能力合格证书

4）岗位胜任能力：

* 了解计算机、网络和信息系统专业知识
* 具备一定的学习、分析和沟通能力，具有较强的敬业意识和责任心

# 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。