**XXX单位**

**人员安全管理制度**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479444226)

[2 适用范围 1](#_Toc479444227)

[3 人员安全管理 1](#_Toc479444228)

[3.1 人员安全管理策略 1](#_Toc479444229)

[3.2 人员安全管理分工原则 2](#_Toc479444230)

[4 外部人员安全管理 3](#_Toc479444231)

[4.1 外部信息技术人员物理访问 3](#_Toc479444232)

[4.2 外部信息技术人员信息访问 3](#_Toc479444233)

[5 第三方驻场运维人员管理 4](#_Toc479444234)

[5.1 驻场人员日常管理 4](#_Toc479444235)

[5.2 驻场人员网络接入管理 4](#_Toc479444236)

[5.3 驻场人员保密管理 4](#_Toc479444237)

[6 附则 5](#_Toc479444238)

# 目的

本文档规定了XXX单位人员安全管理要求。

# 适用范围

本文档适用于XXX单位信息安全中的人员安全管理。

# 人员安全管理

人员安全管理限定为内部人员安全管理，包括人员录用、调动、离岗、考核、培训教育以及外部人员访问管理。

## 人员安全管理策略

**（一）录用前**

应明确被录用人员的安全技能要求，在录用过程中依据技能要求进行考察，并对技能考核结果进行记录；

对涉及访问关键信息，或者访问处理这些信息系统的工作人员应进行严格的安全背景审核和权限审查；

关键岗位人员应当进行特殊的安全审核、权限管理和保密管理，签署岗位安全协议；

人员相关的安全事项必须包括在工作描述或合同中。

**（二）工作期间**

所有工作人员必须在开始工作前，亲自签订保密协议；

必须对全体工作人员就XXX单位信息安全策略和相关管理规定进行培训，使他们熟悉信息安全的实施并加强安全意识；

在对工作人员授权对某项信息技术服务进行访问前，必须对他们进行培训，确保他们正确使用相关的信息工具和设备；

应根据岗位职责的不同，定期对各个岗位的人员进行不同层面的安全认知和安全技能进行培训；

定期对全体工作人员进行安全技能及安全认知的考核，并将考核结果进行记录并保存；

对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒。

**（三）调离岗**

应严格规范人员调离岗过程，及时调整调离岗人员的所有访问权限；

确保指定的继任者能够从该工作人员处获得与该岗位相关的资料和信息；

收回所有XXX单位系统文档、各种分发物件（身份证件、钥匙、徽章、USB令牌等）以及借走的IT设备（笔记本、U盘等）。

**（四）转岗**

应严格规范人员转岗过程，应分配临时员工的所有访问权限，并定期检查人员变动及权限匹配关系；

关键岗位人员应在转岗期间签署保密协议书。

## 人员安全管理分工原则

为确保信息系统的安全，必须加强人事安全管理，提高安全管理人员的技术水平和安全意识，人员安全管理工作遵循以下原则。

（一）重要安全事件多人负责原则，对一些有较高密级与安全有关的活动，都必须有两人或多人在场。上述所指与安全有关的活动包括：硬件和软件的维护；系统软件的设计、实现和维护；处理保密信息；系统用媒介的发放与回收；访问控制用证件的发放与回收；重要程序和数据的删除和销毁等。

（二）重要岗位人员任期有限原则，不能由一人长期担任安全管理职务。对一些重要安全岗位的工作人员应该不定期循环任职，强制实行轮换、休假制度，并对工作人员进行轮流培训。

（三）人员职责分离原则，非经系统主管领导批准，安全工作人员活动所涉及的范围应是受到限制的，不能越权限访问。

（四）人员工作分开原则，权力不能过于集中在某个人或某些人手里。出于对安全的考虑，下面每组内的两项信息处理工作应该由不同的人员来负责：对计算机操作与计算机编程；机密资料的接收和传送；安全管理和系统管理；应用程序和系统程序的编制；访问证件的管理与其它工作；计算机操作与信息系统使用媒介的保管等。

（五）人员权限随岗原则。根据岗位变动情况及时调整相应的授权，做到在岗有权、离岗失权。

# 外部人员安全管理

## 外部信息技术人员物理访问

外部信息技术人员在访问机房时按照《机房安全管理制度》进行管控。

外部信息技术人员需进入机房进行信息设备运维管理的，需向信息化管理部门提出申请，填写《访问记录表》，并进行审批。由机房管理人员全程陪同，并填写《机房出入登记表》做好相关记录。

访问记录表、机房出入登记表资料须保留1年以便备查。

## 外部信息技术人员信息访问

外部信息技术人员需要访问单位信息系统，包含但不限于设备安装、系统维护、业务网接入，填写《访问记录表》，明确工作内容和计划，并由业务部门和运维管理部门审批。

对外部信息技术人员仅分配其所承担工作的最小权限，并在工作完成后及时注销。

外部信息技术人员必须在规定的范围内工作。未经许可，不得擅自使用单位内部的计算机及网络设备，不得以任何名义获取单位内部有价值的数据、文档、程序等信息资源。

外部信息技术人员工作设备有接入内部网络需求的，须经过运维管理部门的安全检查，未经检查的设备不得联网，并通过堡垒机等对操作过程进行信息安全审计。

外部信息技术人员对服务器、网络设备、应用系统等信息遵守保密义务，不得透露任何关于税务单位的信息技术细节、配置信息等内容。访问信息系统设备需签署《保密协议书》，访问敏感信息资源的需签署《保密协议书》。

严禁外部信息技术人员进行远程操作维护，现场运维操作完成后，应及时清理临时数据，不得将任何数据或资料拷贝带离工作现场。

# 第三方驻场运维人员管理

## 驻场人员日常管理

应为第三方方驻场运维人员办理工作证，工作证需随身佩戴。

第三方驻场运维人员应在指定的办公区域内办公，遵守驻场单位的规章制度及工作守则，准时上下班，办公期间不从事与驻场岗位无关的活动。

驻场人员未征得同意，不得使用他人计算机，不得随意翻看他人办公资料物品。

## 驻场人员网络接入管理

应为第三方驻场人员划分单独的网络接入区域，未经许可，严禁第三方接入系统网络区域。

接入单位系统网络的第三方人员终端设备必须满足系统安全管理相关要求。

应加强第三方人员IT 系统权限管理，严格审核第三方权限的分配，监督其操作行为。

定期梳理IT 系统中第三方人员的账号权限，对不合理的账号权限应及时清理和调整。

## 驻场人员保密管理

第三方单位在签署合同时还应签署第三方保密协议，在第三方人员对系统进行访问或提供服务前还应签署个人保密承诺书。

驻场人员必须妥善保管所持有的文件，所获得的相关资料使用完后，应遵守保密条款交还相关人员。

驻场人员未经授权或批准，不准对外提供敏感文件、技术方案、材料以及其他未经公开的经营情况、业务数据等。

# 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。