# 人员信息系统管理制度

来源：网络 作者：紫陌红尘 更新时间：2025-07-08

*第一篇：人员信息系统管理制度人员信息系统管理制度为确保人员信息准确与更新及时性特制订本规定1、上海大众经销商人力资源管理系统分为售前和售后两个网址，是上海大众对所有经销商进行人员管理、信息沟通的平台，包括两大模块：经销商人员管理、信息发布...*

**第一篇：人员信息系统管理制度**

人员信息系统管理制度

为确保人员信息准确与更新及时性特制订本规定

1、上海大众经销商人力资源管理系统分为售前和售后两个网址，是上海大众对所有经销商进行人员管理、信息沟通的平台，包括两大模块：经销商人员管理、信息发布。进行人员管理时，售前网在“人员管理”模块中，售后网在“人力资源”模块中。

2、人员信息系统管理的归口部门为行政管理部。行政管理部人事培训主管拥有人力资源管理系统的操作权限，人事培训主管定期登陆系统，查看最新通知，对系统人员进行维护；其他人员无权进行系统信息修改。行政经理负责监督检查人员系统维护的时效性，人力资源管理指标信息的准确性、规范性、指标达成率等。

3、维护时间

3.1 常规自查：人事培训主管根据《人员信息系统管理规定》要求对相应岗位的信息进行维护和管理，做到准确、无误、及时。人事培训主管每月20日进行人员系统维护，每月25日根据劳动合同花名册进行自查，行政经理每月28日对上月系统操作的规范性进行检查和核实。（签订合同审批表，调岗通知、调岗表）

3.2 变更时限:人员入职应该在员工签订正式劳动合同的30个工作日内进行维护。转岗应填写人员内部调动申请表，批准后30个工作日内将人员工作状态维护成转岗。离职维护应在员工办理完毕离职手续后30个工作日内将人员工作状态维护成离职。

4、售前网维护内容

4.1员工入职：在“添加新员工”模块中依次维护员工信息，重要岗位需上传相关证明材料，包括学历证明、身份证明、驾驶证等。

4.2转岗：在“查看员工信息”模块中选择员工姓名，在“工作状态”一项中选择“转岗”，最后点击“修改”。员工转入的新岗位和替代者按员工入职上报。

4.3离职：在“查看员工信息”模块中选择员工姓名，在“工作状态”一项中选择“离职”，最后点击“修改”。

4.4重要岗位人员维护：按照DOS规定要求，已获得认证的岗位人员（销售

顾问除外）出现变更（已从公司离职），包括以下人员（总经理、销售总监、服务总监、市场总监、客户总监、内训师）需公司行政部填写《重要岗位人员信息变更申请表》，总经理签字并加盖公章邮寄到分销中心，由分销服务中心、区域经理、网络部逐级审批，以上三级全部审批通过，最终状态才会显示通过。

5、售后网维护内容

5.1人员查看：在“人力资源信息查看”中可以看到售后所有在职人员的信息，也可以通过员工姓名进行搜索。

5.2人员申请：在“人力资源信息申请”中，“新建人员”进行员工入职录入，“修改人员信息”进行员工信息变更，“人员调动申请”进行人员转岗录入，“人员离职申请”进行员工离职录入。带有\*号项目为必须录入项。

5.3平台信息共享：在“离职公告中”可以查询到全国经销商离职人员信息，便于信息共享。

6、经销商基本信息维护：经销商名称、经营地址、总经理及销售总监座机、客服热线、销售热线、网络代码、销售服务中心、邮编、法人等必须与公司实际相符。不相符时，不涉及\*标识的经公司行政管理部经理批准后直接进行修改，涉及\*标识的通过RSSC、网络部审批，由上端进行维护。

7、重要岗位审批情况查看：是对公司重要岗位人员信息、资料上传审批情况和最终状态的查询模块。

8、人力资源管理指标查询：是对本经销商的销售顾问、重要岗位配置率、认证率进行查询，该信息由行政管理部进行管理，并指导自身工作的开展。

9、经行政经理审核并报总经理批准后，人事培训主管才能对人员信息进行修改。人事培训主管要根据岗位、工作状态、测评状态、认证状态、年审状态、培训状态对人员信息进行筛选。

10、所有员工的信息以EXCEL格式下载，下载处在信息列表的右下方。

11、行政经理每月28日对上月人员系统操作规范性的进行检查和核实，如发现人事培训主管违规操作一次罚款50元。如发现行政经理没有实行检查和核实一次罚款50元。

**第二篇：信息系统管理制度**

信息系统管理制度

第一章 用户和密码管理

第一条 对于网络设备、主机、操作系统、数据库、业务应用程序，系统用户都必须通过用户和密码认证方可访问。

第二条 用户权限分为普通用户、维护用户与超级用户三个级别。普通用户为各应用系统的使用者，维护用户为各层面系统维护者，超级用户为各层面的管理员用户。

第三条 具有重要权限的帐号密码设置必须符合以下安全要求:

（一）密码不得包含常用可以识别的名称或单词、易于猜测的字母或数字序列或者容易同用户发生联系的数据，比如自己、配偶或者子女的生日和姓名等内容。

（二）密码长度至少是六个字符，组成上必须包含大小写字母、数字、标点等不同的字符。

（三）如果数据库系统、应用系统提供了密码安全周期机制，则帐户密码必须至少每120天修改一次。

（四）同一密码不得被给定账户在一年内重复使用。

（五）如果数据库系统、应用系统提供了密码安全机制，则必须在30分钟之内连续出现5次无效的登录尝试，其账户必须锁定15分钟。在此期间，超级用户可以采用经过批准的备用验证机制重新启用账户。

（六）厂商默认密码必须在软件或硬件安装调试完毕后进行修改。

（七）对于操作系统，必须禁用GUEST帐户，并将管理员帐户重命名。

第四条 密码保护与备份策略：

（一）范围：网络设备、服务器操作系统、数据库、应用系统、ADSL帐户拨号信息；

（二）包含项目：网络设备包括访问的IP地址、端口，所有超级用户的用户名以及密码；

服务器操作系统的IP地址、所有管理员帐户名、密码；

数据库中所有具有系统数据库管理员权限的用户的用户名和密码；

应用系统中所有超级用户的用户名以及密码；帐户的用户名以及密码。

第二章 网络安全管理

第五条 需要全面、系统地考虑整个网络的安全控制措施，并紧密协调，一致实施，以便优化公司IT系统运营。明确规定有关网络的规划、实施、运作、更改和监控的安全技术要求，对网络安全状态进行持续监控，保存有关错误、故障和补救措施的记录。

第六条 网络层次管理必须遵循以下要求：

（一）应用系统所有者相关部门必须同集团信息管理部密切合作。

（二）必须编制并保留网络连接拓扑结构。

第七条 网络管理员负责生产网络、办公网络的安全管理，网络管理员必须掌握网络管理和网络安全方面的知识。

第八条 网络管理员必须使用安全工具或技术进行系统间的访问控制，并根据系统的安全等级，相应的在系统的接入点部署防火墙等网络安全产品，保证网络安全。

第三章 操作系统安全管理

第九条 操作系统管理员由信息管理部领导指定专人担任。

第十条 操作系统管理员主要责任包括：

（一）对操作系统登录帐号、权限、帐号持有人进行登记分配管理。

（二）制定并实施操作系统的备份和恢复计划。

（三）管理系统资源并根据实际需要提出系统变更、升级计划。

（四）监控系统运行状况，发现不良侵入立即采取措施制止。

（五）每1个月检查系统漏洞，根据实际需要提出版本升级计划，及时安装系统补丁，并记录。

（六）检查系统CPU、内存、文件系统空间的使用情况等。

（七）检查服务器端口的开放情况。

（八）每月分析系统日志和告警信息，根据分析结果提出解决方案。

第十一条 在信息系统正式上线前，操作系统管理员必须删除操作系统中所有测试帐号，对操作系统中无关的默认帐号进行删除或禁用。

第十二条 操作系统管理员与应用系统管理员不可兼职,当操作系统管理员变化时，必须及时更换管理员口令。操作系统管理员必须创建专门的操作系统维护帐号进行日常维护。

第十三条 本地或远程登录主机操作系统进行配置等操作完成后或临时离开配置终端时，必须退出操作系统。在操作系统设置上，操作系统管理员必须将操作系统帐号自动退出时间参数设置为10分钟以内。

第十四条 操作系统管理员执行重要操作时，必须开启操作系统日志，对于一些系统无法自动记录的重要操作，由操作系统管理员将操作内容记录在《系统维护日志》上。

第四章 数据安全管理

第十五条 数据库管理员由信息管理部领导根据工作需要指定专人担任。数据库管理员与应用系统管理员不能为同一个人，不可兼职。数据库管理员必须创建专门的服务支撑帐号进行日常服务支撑。

第十六条 数据库管理员的职责：

（一）数据库用户注册管理及其相关安全管理。

（二）对数据库系统存储空间进行管理，根据实际需要提出扩容计划。对数据库系统性能进行分析、监测，优化数据库的性能。必要时进行数据库碎片整理、重建索引等。

（三）制定并实施数据库的备份及恢复计划，根据备份计划进行数据库数据和配置备份，并检查数据库备份是否成功。

（四）监测有关数据库的告警，检查并分析数据库系统日志，及时提出解决方案，并记录服务支撑日志。

（五）检查数据库对主机系统CPU、内存的占用情况。

第五章 主机安全管理

第十七条 主机系统管理员由信息管理部领导指定专人负责，主机系统管理员与应用系统管理员不可兼职。主机的访问权限由主机系统管理员统一管理，并为系统应用人员分配与其工作相适应的权限。

第十八条 主机系统管理员必须每日检查主机机房工作环境是否满足主机的工作条件，包括不间断电源、温度、湿度、洁净程度等。若主机机房的工作条件不能满足主机的工作要求，应及时向上级主管部门反映，提出改善主机机房的要求，以保障主机设备的安全。

第十九条 主机系统管理员负责系统安全措施的设置，系统用户管理和授权，制定系统安全检查规则，实施对生产系统服务器的访问控制、日志监测、系统升级，防止非法入侵。

第六章 终端安全管理

第二十条 各计算机终端用户不允许进行任何干扰网络用户、破坏网络服务和破坏网络设备的活动，不得私自调整网络参数配置。

第二十一条 计算机终端设备为公司生产设备，不得私用，转让借出，除笔记本电脑外，其它设备严禁无故带出生产工作场所。

第二十二条 计算机终端设备均应用于与公司办公生产相关的活动，不得安装与办公生产无关的软件和进行与办公生产无关的活动。

第二十三条 所有计算机终端设备必须统一安装网络防病毒软件，接受公司防病毒服务器的统一管理，未经网络管理员同意，不得私自在计算机中安装非公司统一规定的任何防病毒软件及个人防火墙。对于特殊专业使用的终端设备必须安装适合的防病毒软件，符合防病毒安全管理规定。长期在外使用的计算机终端设备，必须及时升级操作系统补丁和防病毒软件。

第二十四条 信息管理部采取必要的管理工具或手段，检查终端设备是否及时升级操作系统补丁、是否及时更新防病毒软件的病毒库信息。

第二十五条 信息管理部定期组织检查办公用机器上是否安装或使用非办公软件及任何与工作无关的软件，定期检查是否访问反动、不良网站。

第二十六条 各计算机终端用户负责自己所拥有的一切口令的保密，并根据密码管理的要求及时修改口令。不得将自己所拥有系统帐号转借他人使用。

第二十七条 禁止在计算机终端上开放具有“写”权限的共享目录，如果确实必要，可临时开放，必须设置基于用户的共享，禁止将共享权限赋予“Everyone”，在共享使用完之后应立刻取消。在下班时将自己使用的个人计算机关机。

第二十八条 禁止在个人计算机操作系统分区或卷上存放重要数据，以及以软盘、移动存储设备、红外设备或手提电脑等形式将重要数据带出系统。如需要将移动存储设备连接到个人计算机，需征得信息管理部同意并进行病毒查杀后方可接入，未经同意使用U盘、移动硬盘等设备造成机器故障或网络故障的，根据情节，将提交领导进行行政处理或其它处罚。

第二十九条 如因工作需要，需将非公司计算机或者笔记本电脑接入公司内部，必须经信息管理部同意并检查后，方可接入。

第七章 病毒防治

第三十条 信息管理部应在信息系统的主机和终端上统一安装性能优良的防病毒软件，并及时对其进行更新。因硬件或操作系统比较生僻而无法安装防病毒软件的主机应注意升级系统补丁、关闭不使用的系统服务和配置相应的访问控制规则。

第三十一条 网络管理员通过人工或者系统自动提醒的方式完成定期（每天一次）更新终端防毒软件内的病毒码。

第三十二条 网络管理员必须了解最新的病毒信息和病毒动向，及时检查并下载杀毒防毒补丁。

第三十三条 公司内部计算机终端用户必须启用防病毒产品的实时检测功能，任何主机系统和终端在加载任何软件或数据前，先对该软件或数据进行病毒检查。

第三十四条 信息管理部网络管理员定期（至少每月一次）对系统中的程序或数据文件进行病毒检查，填写《病毒扫描记录》提交本部门主管领导审阅。

由于个人计算机系统漏洞或者误操作导致计算机感染病毒程序的，必须及时切断本机网络连接。在病毒发作时，必须进行相应的诊断、分析和记录，对于因计算机病毒而引起的重要信息系统瘫痪、程序和数据损坏等重大事故，及时报告信息管理部领导以及相关信息系统应用部门及时进行处理。

第八章 机房安全管理

第三十五条 机房的电源系统、空调系统、门禁系统、消防系统的服务支撑以及对电源电压，地线、接地，环境温、湿度，各种电缆走线，清洁度，防静电，防霉，防虫害，防火，防水，防易燃、易爆品，防电磁波等方面都应当符合国家标准及国家和集团有关规定。

第三十六条 信息管理部配合公司物业安全保卫部门对防火、防盗、防雷、应急出口、应急照明等系统定期检查，并记录检查结果。

第三十七条 机房环境管理

（一）机房附近不应有污染气体、强电磁场、强震动源、强噪声源及所有危害系统正常运行的因素。

（二）机房的洁净程度必须满足设备制造厂家要求的工作条件，地面要最大程度的达到整洁，机房门窗必须封闭。

（三）机房必须保持清洁，排列正规，布线整齐，仪表正常，工具到位，资料齐全，设备有序，使用方便。机房周围应保持清洁，凡路口、过道、门窗附近，不得堆放物品和杂物妨碍交通。

（四）机房内核心设备与服务器必须配备UPS，至少保证断电情况下UPS可对核心设备与服务器持续供电30分钟。

（五）必须严格遵守设备制造商有关设备保护的要求。

（六）信息管理部应监控及调节机房的环境条件，保证机房的温度在18---25摄氏度内。

（七）机房有足够的照明设备、通信设施和良好的防静电设施。

第三十八条 用电防火安全管理

（一）机房必须配备灭火装置等防火设施。

（二）严禁在机房使用与生产无关的各种电器，非电气人员不准装、修电气设备和线路，不准带电作业。

（三）加强机房施工监护，防止人为事故的发生，各种安装施工禁止使用UPS电源，施工人员撤离现场后应关闭工具电源。

（四）机房内电器设备外壳要接地良好，高压操作时必须使用绝缘防护工具，并注意人身和设备安全。

（五）机房应设置灭火装置和安全防护用具，安放在指定位置，并有专人负责定期检查。维护人员必须熟悉一般的消防和安全操作方法。

（六）消防系统需要定期委托请公司消防部门进行检查验收。

（七）机房内严禁存放易燃易爆物品。严禁在机房内大面积使用化学溶剂。

（八）雷雨季节要加强对机房内部安全设备、地线及防护电路的检修。

第三十九条 机房内部管理：

（一）机房管理实施安全责任人制度，信息管理部安排专人负责机房管理。

（二）机房管理人员应保持机房内整洁。

（三）机房管理人员不做与工作无关的事情。

（四）未经上级主管部门同意，任何人不得操作与自己不相关的设备。

（五）检修设备由相关人员进行，他人不得随意操作。需停设备检修时，应经设备主管部门领导批准方能进行。

**第三篇：信息系统管理制度\_定稿**

信息系统管理制度 第一章 总则

第一条

为明确岗位职责，规范操作流程，保障本中心信息系统安全、有效运行，根据有关法律、法规和政府有关规定，结合信息统计中心实际情况，特制定本制度。

第二条

目的：使信息化建设工作规范化进行，做到统一规划、统一标准、统一建设、统一管理。使用范围：适用于本中心信息化建设。

第三条 利用信息系统实施内部控制至少应当关注下列风险：

（一）信息系统缺乏或规划不合理，可能造成信息孤岛或重复建设，导致中心管理效率低下。

（二）系统开发不符合内部控制要求，授权管理不当，可能导致无法利用信息技术实施有效控制。

（三）系统运行维护和安全措施不到位，可能导致信息泄漏或毁损，系统无法正常运行。

第四条 职责：

（一）信息统计中心负责中心信息化管理总体规划，建立统一的信息化建设标准、规范。负责中心各科（所）信息化项目总体协调及中心办公自动化网络和系统软硬件的维护工作。

（二）各科（所）负责指定专人担任本专业信息化网络工作，并负责本科（所）日常信息管理工作。

第五条

工作要求：

（一）各科(所)在开展涉及信息化建设及申报信息化建设项目之前，需报主管领导审批后，将业务需求、建设规划等报信息统计中心，信息统计中心应按照中心信息化建设规划及相关要求进行审核。

（二）经信息统计中心审核同意后的信息化建设项目，由信息中心提出信息化技术要求及软硬件需求，同意规划整合后报市卫生局信息中心。

（三）各科（所）申报的信息化项目批准后，信息统计中心技术人员全程参与项目的招标、实施、验收。

第二章 信息系统的开发

第六条 信息统计中心根据信息系统建设整体规划提出项目建设方案，明确建设目标、人员配备、职责分工、经费保障和进度安排等相关内容，按照规定的流程报批通过后配合相关公司实施。

信息统计中心负责监督开发流程，明确系统设计、安装调试、验收、上线等全过程的管理要求。

第七条 信息统计中心需要深入了解各个业务科（所）的业务流程、关键控制点、处理规则、用户范围以及手工环境下难以实现的控制功能等较为核心的信息系统需求点。在系统开发过程中，应当按照不同业务的控制要求，通过信息系统中的权限管理功能控制用户的操作权限，避免将不相容职责的处理权限授予同一用户。

应当针对不同数据的输入方式，考虑对进入系统数据的检查和校验功能。对于必需的后台操作，应当加强管理，建立规范的流程制度，对操作情况进行监控或者审计。

应当在信息系统中设置操作日志功能，确保操作的可审计性。对异常的或者违背内部控制要求的操作，应当设计系统自动报告并设置跟踪处理机制。

第八条 信息统计中心需要组织开发单位或开发人员与各科（所）的日常沟通和协调，督促开发单位或开发人员按照建设方案、计划进度和质量要求完成编程工作。

第九条 信息统计中心应根据配备的硬件设备和系统软件的具体情况，组织安排相应的硬件厂家或软件开发商的技术人员入场安装调试。对于关键的软硬件设备，应安排专人负责跟踪、记录整个安装调试过程；在完成软硬件设备的安装调试后，应注意做好有关文档的验收及归档保存工作。

第十条 信息系统上线前，需要对信息系统进行等保定级，没有定级的信息系统不能正式上线。另外，信息统计中心都应当切实做好上线的各项准备工作，应查验设备厂商或软件开发商或开发人员提交的有关运行维护资料，包括技术手册、操作手册等，并负责监督设备厂商或软件开发商提供对相关岗位人员的技术培训。制定科学的上线计划和新旧系统转换方案，考虑应急预案，确保新旧系统顺利切换和平稳衔接。系统上线涉及数据迁移的，还应制定详细的数据迁移计划。第十一条 未经安全检测的信息系统不能为其配置外网地址，信息安全的投入原则上不低于信息系统项目总投资的10%。此外，对于信息技术软件，应注意母盘或源代码的保存登记工作，并由专人管理。日常工作中应尽量使用母盘的复制品，避免造成对母盘或源代码的破坏。

第三章 信息系统的运行与维护

第十二条 信息系统投运前，信息统计中心要掌握有关设备所提供的各种系统监控、维护工具，并检查其安全性和完整性。

第十三条 信息系统投运前，信息统计中心应与软件开发商和设备的供应商共同制定系统投运实施方案以及应急处理方案，并尽可能在测试环境中测试通过后，再在实际运行环境中实施。

第十四条

信息系统的日常管理和维护由信息统计中心负责。信息统计中心按实际情况制定各模块子系统的具体操作规范，及时跟踪、发现和解决系统运行中存在的问题，确保信息系统按照规定的程序、制度和操作规范持续稳定运行。

信息统计中心对服务器等关键信息设备指定专人负责检查维护，及时处理异常情况。未经授权，任何人不得接触关键信息设备。机房设备发生故障时，应及时联系设备供应厂商解决。

第十五条

信息系统需求变更应当严格遵照管理流程进行操作。信息系统操作人员不得擅自进行系统软件的删除、修改等操作；不得擅自升级、改变系统软件版本；不得擅自改变软件系统环境配置。

对于重大信息系统配置的更改，应先形成方案文件，经信息统计中心讨论确认可行，报信息统计中心领导批准后执行。方案中应包括系统备份方式、调试运行期限、更改和操作记录、应急措施等相关内容。

第十六条 根据业务性质、重要性程度、涉密情况等确定信息系统的安全等级，建立不同等级信息的授权使用制度。

（一）建立用户管理制度，根据工作岗位需求严格控制重要业务系统的访问权限。合理分配用户权限，避免授权不当或存在非授权账号，禁止不相容岗位用户账号的交叉操作。

（二）每周备份信息系统数据库，确保信息系统一旦发生故障能够快速恢复。第十七条

信息统计中心人员必须严格遵守信息传递操作流程，严禁外泄网络用户密码及共享权限密码。严禁擅改他人文件。

第十八条

信息统计中心全体人员均有权制止违反规定、可能损害信息系统安全的行为，并有义务及时向信息统计中心领导汇报。在出现违反规定的可疑情况，应立即向信息统计中心领导通报。

第十九条

信息系统设备完成安装调试后，未经信息统计中心同意，任何个人或部门不得擅自移动或拆除。如因工作需要，确实要对有关设备进行移动或拆除，需报信息统计中心审批同意后，由信息统计中心组织有关技术人员实施，并做好相应的登记变更工作。关键硬件设备完成安装后，运行地点要相对固定，移动或拆除要在完成审批程序后，方可实施。

第二十条 硬件设备的报废应由使用部门提出书面申请，信息统计中心根据设备的使用情况进行审核，提出设备报废清单，按固定资产报废程序办理。

**第四篇：医院信息系统管理制度**

郏县中医院

信息系统安全等级保护管理制度

发布人：郏县中医院信息科 发布时间：2025-01-01

第一章 总则

第一条 为规范信息安全等级保护管理，提高我院信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设，根据《中华人民共和国网络安全法》文件要求，制定本制度。

第二条 根据国家制定的信息安全等级保护管理规范和技术标准，对本部门所使用和运营的信息系统分等级实行安全保护。

第三条 在我院信息化领导小组的领导下，信息科负责医院信息系统安全定级和保护的指导、上报和检查工作。

第四条 各科室依照本制度及相关标准和规范进行本科室运营和使用的信息系统的定级保护工作。

第五条 各科室应当依照本制度及相关的标准规范，对运营和使用的信息系统履行安全等级保护的义务和责任。

第二章 等级划分和保护

第六条 信息等级保护坚持坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

第七条 信息系统的安全保护等级分为以下五级：

第一级为自主保护级，适用于一般的信息系统，其受到破坏后，会对公民、法人和其他组织的合法权益产生损害，但不损害国家安全、社会秩序和公共利益。

第二级为指导保护级，适用于一般的信息系统，其受到破坏后，会对社会秩序和公共利益造成轻微损害，但不损害国家安全。

第三级为监督保护级，适用于涉及国家安全、社会秩序和公共利益的重要信息系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成损害。

第四级为强制保护级，适用于涉及国家安全、社会秩序和公共利益的重要信息系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成严重损害。

第五级为专控保护级，适用于涉及国家安全、社会秩序和公共利益的重要信息系统的核心子系统，其受到破坏后，会对国家安全、社会秩序和公共利益造成特别严重损害。

第三章 等级保护的实施与管理

第八条 信息系统运营、使用科室依照本制度和《信息系统安全等级保护定级指南》确定信息系统的安全保护等级，报到信息中心。信息中心审核后，统一上报到郏县卫生健康委信息工作股。根据上级主管部门的审核和指导意见，按照国家规范，完成我院信息系统的安全定级工作。并完成相应的安全保护和制度建设工作，对定为二级以上的信息系统按照相关规定报平顶山市公安局备案。

第九条 信息系统的安全保护等级确定后，运营、使用部门应当按照国家信息安全等级保护管理规范和技术标准，使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品，开展信息系统安全建设或者改建工作。

第十条 在信息系统建设过程中，运营、使用部门应当按照《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息系统安全等级保护基本要求》等技术标准，参照《信息安全技术信息系统通用安全技术要求》（GB/T20271-2025）、《信息安全技术网络基础安全技术要求》（GB/T20270-2025）、《信息安全技术操作系统安全技术要求》（GB/T20272-2025）、《信息安全技术数据库管理系统安全技术要求》（GB/T20273-2025）、《信息安全技术服务器技术要求》、《信息安全技术终端计算机系统安全等级技术要求》（GA/T671-2025）等技术标准同步建设符合该等级要求的信息安全设施。

第十一条 运营、使用部门应当参照《信息安全技术信息系统安全管理要求》（GB/T20269-2025）、《信息安全技术信息系统安全工程管理要求》（GB/T20282-2025）、《信息系统安全等级保护基本要求》（GB/T22239-2025）等管理规范，制定并落实符合本系统安全保护等级要求的安全管理制度。

第十二条 信息系统运营、使用部门及其主管部门应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。经自查，信息系统安全状况未达到安全保护等级要求的，运营、使用部门应当制定方案进行整改。

第四章 附 则

第十三条 各部门对本部门运营和使用的信息系统进行梳理，按照本制度的要求确定信息系统的安全保护等级；新建信息系统在设计、规划阶段确定安全保护等级。

**第五篇：计算机信息系统管理制度**

计算机信息系统管理制度

一、目的

为加强对信息系统的管理,确保公司信息系统正常运行，防止各种因素对信息系统造成危害，严格信息系统授权管理，确保信息系统的高效、安全运行。

二、适用范围

适用于公司所有信息系统的管理,包括单机和网络系统。

三、职责

计算机管理员负责监督本制度实施。

四、定义

IT设备指除PC外的信息系统设备。

五、内容

1、硬件管理 1.1计算机设备购置

1.1.1各部门根据工作需要提出计算机设备购买申请，填写《设备设施购置申请表》交办公室、财务部签署意见后报总经理审批；

1.1.2计算机管理员根据总经理的批复后实施。购买时至少挑选3家供应商进行比较，考虑：价格、供应商的合法性、质量承诺和售后服务的信誉度、设备能否满足使用部门的需要、设备是否易于调整且可靠性高；

1.1.3设备购置后，计算机管理员会同供应商进行设备安装，试运行正常，计算机管理员建立《计算机设备管理台账》，将设备编号后交与使用部门；

1.1.4计算机硬件设备的原始资料（光盘、说明书及保修卡、许可证协议等）根据档案保管要求保管。使用者必需的操作手册由使用者保管。

1.2计算机的使用

1.2.1各部门的计算机只能由计算机管理员授权及培训的员工操作使用； 1.2.2使用者应保持设备及其所在环境的清洁。下班时，需关机切断电源； 1.2.3使用者的业务数据，应严格按照要求妥善存储在网络上相应的位置上； 1.2.4未经许可，使用者不可增删硬盘上的应用软件和系统软件； 1.2.5严禁使用计算机玩游戏。1.3计算机设备维护

1.3.1计算机设备不准私自随意拆装,必须由计算机管理员对计算机设备进行维护，对

使用人员的报修及维修需填写《硬件设备故障及维修记录》；

1.3.2一切硬件设备不准带出机房及办公场所(如必要时必须经过公司相关部门领导同意)。

1.4计算机设备的报废

1.4.1计算机设备需要报废时，使用部门提出申请，填写《设备报废申请单》，交财务部审核后，报总经理批准；

1.4.2财务部根据总经理批复，实施财务核销；

1.4.3使用部门将已同意报废的设备与《设备报废申请单》一起计算机管理员；不得随意乱放处置，应按照清单办理报废销毁手续，由计算机管理员统一处理；

1.4.4计算机管理员注销《计算机设备管理台帐》，并将已报废的设备按照清单办理销毁手续。

1.5硬件安全管理 1.5.1 PC安全

◆任何个人未经计算机管理员许可，不得擅自拆装电脑机箱；

◆员工应尽力防止任何液体进入机箱，显示器，键盘、鼠标及外部设备。一旦发生此类情况，须立即关闭相关设备电源，并报告计算机管理员。键盘进水请立即将键盘倒置以减轻损害程度；

◆计算机管理员应建立《计算机设备管理台帐》，详细记录每台PC的编号，IP地址，使用人及所属部门；发生变更时及时更改记录。

1.5.2机房安全

◆无人值守时机房必须上锁；

◆机房钥匙由计算机管理员，备用钥匙由办公室保管；计算机管理员不得擅自将钥匙交于他人使用，离开机房后应锁闭机房；

◆任何人不得携带饮料或其他液体、未包装的食品进入机房，任何人不得在机房内进食或打开食品包装；

◆机房内严禁吸烟；

◆机房温度应保持在18℃25℃；计算机管理员应经常注意机房空调设备的运行状况，一旦空调设备发生运行故障，须及时通知办公室进行修理；

◆机房内设备放置应合理有序，线路连接应保持整洁，相关标签清晰。1.5.3 IT设备安全

◆服务器的开机前，负责硬件安全检查，作《计算机安全值班记录》。必须由计算机管理员单独负责并进行操作，并做《服务器使用记录》；

◆计算机管理员应建立《IT设备及供应商、报修电话一览表》，详细记录每种设备的型号，供货商及维修电话，以在设备发生故障时可以第一时间联系到供货商或生产厂家。

2、软件管理 2.1备份

2.1.1所有系统软件和应用软件,由公司计算机管理员列表登记《软件一览表》，备制二份,一份使用,一份保存；

2.1.2所有信息数据,应当按《服务备份管理细则》进行复制备份,并由计算机管理员负责保管。

2.2维护更新

软件维护更新必须按规定的要求执行。2.3文件病毒防治

2.3.1计算机管理员负责在服务器及个人微机上统一安装防病毒软件并将不定期检查员工的计算机。任何个人未经许可不得卸除或关闭防病毒程序，如发现有私自卸除或关闭防病毒程序的情况，将立即制止并上报该部门主管；

2.3.2计算机管理员负责定期发布更新的防病毒软件及其病毒库，并根据需要通知员工执行必要的防范措施。员工应积极配合信息系统管理员的工作；

2.3.3员工一旦发现或怀疑自己的计算机被病毒感染时，应该立即停止一切操作，断开网络，并向计算机管理员报告；

2.3.4计算机管理员接到病毒报告后，应立即检查被感染情况，作必要的记录，并清除病毒。同时，应通知相关人员，以协助防止病毒的扩散。

2.4电子邮件病毒防治

2.4.1应在电子邮件服务器上安装邮件病毒扫描程序；

2.4.2计算机管理员应确保邮件病毒扫描程序正常运行，并能有效拦截邮件病毒； 2.4.3因工作需要使用外部邮件系统，应确认防病毒程序正常工作。对可疑邮件应先联系计算机管理员再作处理。

2.5保密要求

2.5.1计算机存贮、传输的信息属于企业商业机密,各部门的加密软件盒必须妥善保管,如发生加密盒丢失、信息泄密及因其造成后果的,由计算机管理员负责。如因操作发生失

误所致,其责任由操作员承担；

2.5.2涉密信息的处理应通过单机独立工作,其信息介质应由专人负责保管,并按相应密级的文件进行管理；

2.5.3各部门计算机因故障需要送外修理,必须由计算机管理员办理,同时必须有效清除硬盘信息或卸下硬盘,不得泄密信息；

2.5.4建立账号审批制度，加强对信息系统的访问权限管理，系统访问过程中不相容岗位（或职责）一般应包括：申请、审批、操作、监控；

2.5.5当发生岗位变化或离岗的用户，部门负责人应通知计算机管理员，及时调整其在系统中的访问权限；

2.5.6系统操作人员应当在权限范围内进行操作，不得利用他人的口令和密码进入信息系统。更换操作人员或密码泄密后，必须及时更改密码。操作人员如果离开工作现场，必须在离开前锁定或退出已经运行的程序，防止其他人员越权操作或散发不当信息；

2.5.7对于特权用户，企业应该对其在系统中的操作进行监控，并定期审阅监控日志； 2.5.8计算机管理员应当定期对系统中的账号进行审阅，避免有授权不当或冗余账号存在。

3、网络安全 3.1互联网连接安全

3.1.1计算机管理员应保证公司局域网与国际互联网的网络连接有效；出现故障应及时与网络接入运营商联系，排除故障；

3.1.2计算机管理员应经常察看防火墙或网关设备状态，确保其正常运行； 3.1.3计算机管理员在必要时可更改防火墙规则或网关设备的数据传送规则，以阻止有害信息包的传递；

3.2账号安全

3.2.1用户应使用自己的独立账号访问公司邮件服务器或应用系统，非特殊情况不得与他人共享账号；

3.2.2计算机管理员为每位用户设立初始密码时，密码长度至少为6位，必须包括英文字母、数字、及标点符号三种字符中的至少两种；

3.2.3对于电子邮件账号，计算机管理员应根据实际情况设置账号锁定策略。如登录失败3次则锁定该用户30分钟；

3.2.4对于公司重要账号的密码管理，应加强安全管理，定期检查更新安全措施。

3.3服务器安全

3.3.1服务器管理员密码严禁为空，设置高级密码强度；

3.3.2服务器只安装必要的服务及应用程序；与公司业务无关的服务组件及应用软件不得安装；

3.3.3除非公司关键业务服务器应取消缺省的驱动器共享；

3.3.4必须针对每台服务器提供相应的备份策略，并记录到信息系统备份计划中； 3.3.5计算机管理员应及时为服务器的操作系统及应用软件安装补丁程序，避免因软件漏洞造成黑客或病毒入侵；

3.3.6除非服务器本地登录应处于锁定状态或未登录状态； 3.4局域网安全

3.4.1公司网络结构由计算机管理员统一规划建设并负责管理维护，任何部门和个人不得私自更改。个人电脑及实验环境设备等所用IP地址必须按信息系统管理员指定的方式设置，不得擅自改动；

3.4.2严禁任何人以任何手段，蓄意破坏公司网络的正常运行，或窃取公司网上的保密信息；

3.4.3公司网上服务如DNS、DHCP、WINS等由计算机管理员统一规则，任何部门和个人不得在网上擅自设置该类服务；

3.4.4除计算机管理员外，严禁任何人安装、使用任何包捕获程序、嗅探器及密码破解程序；

3.4.5工作必需软件由计算机管理员负责安装，任何个人未经许可不得擅自安装任何软件；

3.4.6计算机管理员应及时提醒和帮助用户对PC的操作系统及应用软件安装补丁程序，避免因软件漏洞造成黑客或病毒入侵；

4公司计算机信息系统权限管理

4.1公司所使用的计算机信息系统（以下简称CMS）权限管理采用人员控制、部门控制、功能授权、数据导出专项控制限制等功能模块交叉管理，功能授权采用按职能定位设置工作小组，按工作小组分配人员，实现功能授权管理。确保系统和数据的安全；

4.2申请部门填写《信息系统授权申请登记表》，计算机管理员对人员进行核定。4.3计算机管理员对使用授权进行核定。4.4报总经理批准。

4.5计算机管理员实施，建立用户使用账户，并通知用户。4.6计算机管理员存档《信息系统授权申请登记表》。

本DOCX文档由 www.zciku.com/中词库网 生成，海量范文文档任你选，，为你的工作锦上添花,祝你一臂之力！