

# 重庆医药(集团)股份有限公司文件

渝药司〔2020〕35号

---

## 重庆医药（集团）股份有限公司 关于印发《计算机信息安全管理办法》的通知

各分、子公司，各部门：

为防止计算机病毒的传播、适应公司对计算机网络信息安全的管理需要，结合我司实际工作，对现行的《计算机信息系  
统安全管理办法》进行了修订，现将修订后的《计算机信息安  
全管理办法》印发给你们，请各单位认真贯彻执行。

特此通知

重庆医药（集团）股份有限公司

2020年2月11日



文件编号：CQP-C-46

发放编号：

版本状态：2020 第 3 版

受控状态：**受控**

# 重庆医药（集团）股份有限公司 计算机信息安全管理办法

## 第一章 总 则

**第一条** 计算机信息安全是企业发展的重要基础，为加强信息管理，根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》等有关法律法规，结合我司实际情况，制定本办法。

**第二条** 本办法所称的计算机信息网络，是指由计算机及配套的设施(含网络)及软件构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

**第三条** 本办法适用范围为集团公司所有单位，包含各职能部门、分公司、子公司（包括控股子公司）（以下统称为“应用单位”），适用人员为各应用单位管理人员和从事开发、科研以及使用计算机信息网络的所有人员。

## 第二章 计算机信息安全管理组织机构及工作职责

**第四条** 公司设立计算机信息安全管理领导小组，组长由公司董事长担任，公司总裁、分管安全的副总裁、分管信息中心的副总裁任副组长，信息中心主任、安全环保部部长为组员。

安全管理领导小组下设计算机信息安全管理办公室，办公室主任由分管信息中心的副总裁担任，副主任由信息中心主任



和安全环保部部长担任，成员由办公室、投资与战略管理部、审计与合规部、财务部、质量管理部负责人组成。办公室设在信息中心。

### **第五条 计算机信息安全管理领导小组职责**

（一）领导小组是全集团信息网络安全管理的领导机构，组长是信息网络安全管理的第一责任人，副组长是具体责任人，组员是直接责任人。

（二）贯彻国家和上级主管部门有关计算机信息安全的法律法规、技术规程、文件要求。

（三）审定公司计算机信息安全管理组织体系、职能职责、规章制度。

### **第六条 计算机信息安全管理办公室职责**

（一）负责公司计算机信息网络的日常安全管理工作。

（二）统一拟定公司计算机信息安全管理策略，制定公司计算机信息安全管理制度的技术规范。

（三）检查应用单位的计算机信息安全管理情况，对违反安全管理规定的行为，由公司安全环保部按本条例相关规定予以处罚。

（四）检测计算机信息网络各类安全隐患，并提出整改意见。

（五）对应用单位相关人员进行计算机信息安全管理培训和技术咨询。

（六）依法开展计算机信息安全监察工作，配合相关机构查处信息网络和计算机违法犯罪案件。

## **第七条 信息网络管理部门职责**

(一) 信息网络管理部门指集团信息中心，分公司及子公司（包括控股子公司）的信息网络管理部门。

(二) 负责集团公司范围内信息化的规划、设计、建设、改造升级、系统维护等内容由集团信息中心统一管理，为确保信息安全，包含一切以现代信息技术为主要手段的信息化基础设施、计算机网络、应用系统、互联网应用（APP、网站、微信公众号）等软硬件系统建设。

(三) 根据本办法制定《重庆医药（集团）股份有限公司计算机信息安全管理办法实施细则》（见附件），并按规定行使执行、监督职责。

## **第三章 计算机信息安全管理规定**

**第八条** 应用单位负责人是本单位计算机信息安全管理第一责任人，应用单位须设立计算机信息安全管理小组，负责本单位计算机信息安全管理工作。计算机信息安全管理小组须设置专职计算机信息安全管理（兼任系统维护员），负责本单位计算机信息网络的日常安全管理工作。

**第九条** 应用单位使用公司拥有或部分拥有知识产权的软件，未经信息网络管理部门批准，严禁添加、修改、删除数据库结构，严禁修改和反编译应用程序。

**第十条** 计算机信息网络的操作人员应接受计算机安全培训并建立培训记录台账，未经培训不得上岗。

**第十一条** 未经批准，严禁对外提供任何数据及资料。



**第十二条** 发现计算机安全事故及安全隐患，立即向本单位计算机信息安全管理或集团信息网络管理部门反映。计算机信息安全管理或信息网络管理部门应立即采取措施进行处置。

**第十三条** 未经本单位负责人或集团信息中心批准，严禁使用外来软件、光盘、软盘、U 盘或其他移动存储设备。经批准使用的，连接到计算机时必须先检测病毒，确认无安全隐患后方可使用。

**第十四条** 应用单位应按集团信息网络管理部门规定部署相应的计算机安全软、硬件。计算机信息安全管理办公室在监察工作中发现存在计算机病毒隐患或者其他影响计算机信息安全的隐患时，应当及时通知应用单位或者个人采取安全保护措施，应用单位和个人接到计算机信息安全管理办公室要求改进安全状况的通知后，在限期内拒不改进的，由计算机信息安全管理办公室处以警告或者停机整顿。

**第十五条 公司计算机网络管理规定**

（一）应用单位的计算机网络规划、建设按集团 2017 年 8 月 23 日印发的 渝药司〔2017〕235 号文《信息化建设管理制度》执行。

（二）局域网，指公司各应用单位使用的计算机，在本单位内能互联互通的计算机网络。包括公司信息中心管理的计算机网络和分、子公司自行管理的计算机网络。

（三）在公司局域网内使用互联网，须采取严格的审批制度和专人专机管理。未经批准的人员或计算机，严禁在公司局

域网内连接到互联网。

(四) 独立互联线路的管理, 各个分支公司如果有需要私自搭建互联网线路, 需要提前向集团提交《互联网备案申请表》, 并严格按照《互联网备案申请表》内容的安全责任书执行。

#### 第四章 罚 则

**第十六条** 违反本办法规定, 尚不构成犯罪的, 由计算机信息安全管理办公室将处理意见报计算机信息安全管理领导小组审批后执行。

**第十七条** 违反本办法规定, 构成违反治安管理行为或构成犯罪的, 由集团公司移送有关国家机关依法处理。

#### 第五章 附 则

**第十八条** 本办法凡与法律法规和上级规定相抵触的, 从其规定。本办法未做出要求和规定的, 执行国家有关的要求和规定。

**第十九条** 本办法自发文之日起执行, 2008 年 1 月 8 日发布的《重庆医药股份有限公司计算机信息系统安全管理办法》、《计算机信息系统安全管理办法实施细则》同时废止。原集团有关规定所涉内容与本办法不一致的, 按本办法执行。本办法由集团公司计算机信息安全管理领导小组办公室负责解释。

附件: 重庆医药(集团)股份有限公司计算机信息安全管理  
办法实施细则



# 重庆医药（集团）股份有限公司 计算机信息安全管理办法实施细则

## 第一章 总 则

**第一条** 根据《重庆医药（集团）股份有限公司计算机信息安全管理办法》（下称《安全管理办法》）制定本细则。

## 第二章 应用单位使用计算机信息安全管理规定

**第二条** 根据《安全管理办法》应用单位须设立计算机信息安全管理小组，负责本单位计算机信息安全工作。计算机信息安全管理小组须设置专职计算机信息安全管理（兼任系统维护员），负责本单位计算机信息系统的日常安全管理工作。

应用单位计算机信息安全管理职责

（一）接受应用单位负责人和集团信息中心对计算机信息安全管理相关工作的安排。

（二）对本单位上机人员至少每季度进行一次计算机信息安全管理教育或培训，并建立安全管理教育、培训记录台帐。

（三）负责本单位所有计算机杀毒软件的安装及升级检查工作，至少每周须对每台计算机进行一次杀毒软件的升级检查和杀毒情况检查，并对检查情况作书面记录。发现未升级成功的应立即处理。

发现病毒时，须立即断开有病毒机器与网络的连接，并报告集团信息中心，病毒完全清除后方可接入使用。

（四）至少每月检查一次本单位接入互联网计算机的使

用情况并做台帐记录。发现违规使用行为，须及时向单位负责人和集团信息中心报告。

（五）使用具有权限管理的应用系统，应根据本单位使用人员工作需要及岗位调整，及时调整其使用权限。

（六）对专供外单位客户查询数据的计算机，承担安全管理责任。

（七）及时为本单位所有计算机的操作系统打补丁。

（八）全面掌握信息系统运行规程要求，正确处理上机运行的一切业务事项，指导和培训本单位员工按流程要求操作。

（九）各单位应每月开展系统对账工作，检查信息系统中有无流程未完成单据、数据错误、库存差异等情况，如发现问题立即联系集团信息中心处理。

**第三条** 计算机信息安全管理（兼任系统维护员）应具备的能力

熟悉应用单位网络架构，能够独立安装工作站的操作系统，独立安装并配置信息系统客户端，独立配置本单位所使用的信息系统，并对修改后的信息系统能下载并更新。独立解决工作站和打印机故障，简单判断及处理网络故障。

**第四条** 应用单位计算机需要报废，应先封存并报集团信息中心签注意见，再按集团公司规定程序报批。对已报废计算机做剩余信息清除的技术处理。

**第五条** 应用单位和个人严禁在公司计算机上制造、修改、研究、传播、买卖、传递计算机病毒。

按“谁使用，谁负责”的原则，应用单位须对本单位每台



信息化设备明确使用责任人。

## **第六条** 计算机信息系统使用人员应遵守的规定

（一）严格按照计算机信息系统流程规范要求，正确处理机内业务。

（二）严禁向他人透露任何密码或用他人密码进入计算机信息系统。操作系统应设立屏幕保护，人机分离时，操作系统应处于屏幕锁定状态。

（三）每天对所用计算机杀毒，发现杀毒异常或计算机染毒，立即断开网络并向本单位系统安全管理员或集团信息中心反映。严禁染毒计算机在公司局域网内继续使用。

每天检查杀毒软件是否更新，发现未及时更新，应立即向本单位系统安全管理员或公司信息中心反映。

（四）严禁使用公司计算机玩游戏、聊天、观看视频、淫秽图像或做其他与工作无关的事。

## **第三章 公司局域网内使用互联网的规定**

**第七条** 局域网，指公司各应用单位使用的计算机，在本单位内能互联互通的计算机网络。包括公司信息中心管理的计算机网络和分、子公司自行管理的计算机网络。

分、子公司及应用单位原则上不允许私自搭建互联网，如因特殊情况需要独立上网的计算机，使用前须报公司信息中心备案，进行使用申请流程，由信息中心领导进行审批，严禁独立上网的计算机接入公司局域网。

## **第八条** 使用互联网的申请审批程序

(一) 严格控制上网用户数量,确属工作需要,应选择素质较高、责任心强的人员使用国际互联网,并在上网申请前对选定的使用责任人进行安全教育。

(二) 应用单位负责人通过公司“互联网使用申请”流程进行逐级审批,原则上不得在流程完成前要求信息中心进行互联网开通操作。

(三) 应用单位上网申请的内容应包括“互联网使用申请”流程中的所有必填项目包括:使用目的、使用责任人及其使用国际互联网的安全教育情况、使用计算机的 IP 地址。如果流程填写内容存在问题或不明确的情况,信息中心原则上不予以开通。

#### **第九条 使用互联网的开通程序**

(一) 申请流程中各级领导审批完成后,由流程对应的操作人员进行开通操作。

(二) 信息中心在申请内容完备,审核、审批手续齐全的情况下,通过上网行为管理设备进行互联网权限开通。记录使用人、IP 地址并匹配相应权限策略。

(三) 若应用部门因特殊原因需要增加外网访问权限,需要依照第五条进行重新申请。原则上不允许在流程审批完成前要求信息中心人员进行权限增加。

**第十条** 集团安全环保部适时对使用责任人进行互联网开通后的安全教育检查,发现不符合要求的,应及时通知集团信息中心关闭该 IP 地址接入互联网的权限,同时通知应用单位负责人。



## **第十一条 互联网安全使用规定**

(一) 上网使用责任人对计算机上网安全负直接责任, 应用单位负责人、计算机信息安全管理与使用人共负连带责任。

(二) 上网使用责任人严禁利用国际互联网从事危害国家与公司安全、泄露国家与公司秘密等活动。严禁利用国际互联网查阅、复制、制造和传播危害国家和公司安全, 妨碍社会治安和淫秽色情的信息。

(三) 上网使用责任人应在本机上设置开机密码, 人机分离时退至密码输入处, 无关人员一律严禁上网使用。

(四) 上网计算机在公司局域网外使用互联网后, 重新进入公司局域网, 或采用独立上网形式后重新进入公司局域网时, 使用责任人必须首先检测确认计算机无病毒后才能进入。

(五) 使用责任人严禁在互联网上下载任何可执行程序 (包括各种应用程序、游戏等)。下载与工作相关的文件, 须先保存文件, 采用杀毒软件检测, 确认无病毒后再打开文件。严禁在互联网上打开来历不明的邮件及其附件。

(六) 上网使用即时通软件, 须经应用单位负责人批准并报公司信息中心备案; 严禁使用即时通信软件进行非工作交流。

(七) 严禁擅自更改 IP 地址上网。

## **第四章 通过 VPN 接入公司局域网的安全规定**

### **第十二条 应用单位及使用责任人应遵守的规定**

(一) 由集团信息中心管理或分、子公司自行管理的计算机网络, 通过 VPN 接入的审批、开通等按本条第二款至第五款执行。

(二) 分、子公司需要通过 IPSEC VPN 接入公司局域网, 必须通过“分、子公司开通专用通道 VPN (ipsec-vpn) 申请”流程进行申请

集团信息中心审批同意后, 由各个分、子公司计算机管理员联系当地网络公司进行设备安装和调试, 由集团信息中心人员配合完成。

(三) 个人用户需要通过 SSLVPN 接入公司局域网必须通过“个人用户开通专用通道 VPN 申请”流程进行申请

信息中心审批同意后, 各个分、子公司以及集团总部必须对使用责任人进行安全教育, 并由各个分、子公司计算机管理员或申请 VPN 的个人自行查看安装教程文档, 进行 VPN 客户端的安装。

(四) 分、子公司计算机信息安全管理必须负责管理通过 IPSEC 接入集团内网的终端设备, 保证接入终端 (包括 PC、服务器) 的安全。内容包括开启防火墙、安装杀毒软件、定期进行病毒扫描和查杀、配合进行集团下达的网络安全相关配置要求, 严格把控使用人员的外网权限。

如集团信息中心通过网络安全设备发现分、子公司终端设备流量异常, 或存在攻击行为, 将立即中断网络连接, 并由分、子公司计算机信息安全管理进行处理, 处理完成后重新进行 IPSECVPN 连接。



(五) SSLVPN 原则上仅提供给在外办公人员使用，不得在集团内部或与集团有专线或 IPSECVPN 连接的分、子公司总部办公室进行使用。原则上一人一账号，使用人即为责任人，需对使用 SSLVPN 的终端负责，保证终端的安全。内容包括内容包括开启防火墙、安装杀毒软件、定期进行病毒扫描和查杀，对离职人员或职位调动后工作中不需要 VPN 权限的人员，需要及时上报集团信息中心注销账号。

如集团信息中心通过网络安全设备，发现有 SSLVPN 账号存在流量异常或存在攻击行为，将临时冻结该账户，并由账号责任人对使用终端进行杀毒处理。若账号责任人无能力进行处理的，可携带设备至信息中心，由信息中心人员协助处理。

## 第五章 计算机机房管理规定

**第十三条** 集团信息中心管理的机房，安全管理责任由集团信息中心承担。应用单位管理的机房，安全管理责任由应用单位承担，集团信息中心承担技术指导、监督责任。

### 第十四条 机房管理的设备

机房管理的设备主要有：UPS 设备、机房空调、小型机及存储设备、微机服务器、备份系统设备及附属设备等。

### 第十五条 机房安全管理

#### 物理环境安全管理

(一) 严禁在机房内吸烟及使用电热器具或明火操作，机房内使用的测试仪器、吸尘器等电器设备，用完后必须及时切断电源并带出机房。

(二) 严禁将易燃品、易爆品、含有腐蚀性的物品、强磁物品及其他与机房工作无关的物品带入机房，维修中使用酒精等易燃物品时，必须有人在场，用完后必须剩余部分应立即带出机房。

(三) 机房落实专人进行定期检查放火、防水、防盗、防尘设施，并按指南更换，并保持良好状态。

设备及系统安全管理

(四) 建立完整的计算机运行日志、操作记录及其他有关的资料保存机制。

(五) 定期检查安全保障设备，确保其处于正常工作状态。

(六) 机器带电运行时严禁开启机箱维修，拆卸机器附件时，必须采取防静电措施。

(七) 对不能停机的主机必须按指南配备定额容量的UPS等设施。

(八) 计算机设备必须有可靠接地，接地电阻不大于相应设备的技术要求，并装置必要的防雷设施。

(九) 可用性要求较高的计算机系统，配置必要的备份设备，以便保障时切换使用。对于重要系统和数据应定时做好备份。

(十) 做好定期的查病毒工作，对于重要的应用和服务应建立防病毒体系。

## **第十六条 机房日常管理**

(一) 机房环境条件

1. 按有关指南控制机房的温度和湿度；



2.机房地板、墙壁应完整无损，防止各类小动物进入；

3.凡与机房无关的任何物品不得存放在机房内；

## （二）机房卫生要求

1.机房应保持清洁，每周清扫一次，每月大扫除一次；

2.进入机房应更换鞋套，并要定期清洗，不准在机房外使用；

3.机房内不准吸烟，不准用膳，不准会客，不准存放食品。

## （三）机房出入要求

1.任何人必须经过授权，并填写《机房出入授权申请单》，方可进入机房；

2.经授权人员进入机房必须填写《机房出入登记表》；

3.外单位进入机房时，须经机房负责人同意，并报集团信息中心负责人审批通过，在由机房负责人指定人员的陪同下进行相关活动；

## 第十七条 机房设备操作指南

（一）机房管理员如需对机房设备进行操作，必须严格遵守操作规程，确保人身、设备安全，认真填写《服务器与网络设备检查记录单》。

（二）操作中发现异常情况应立即报告机房负责人，及时采取相应措施。

（三）任何人不得擅自移动机房内的一切设备。

## 第十八条 故障处理

机房主要设备，如主机和网络设备等，发生故障时，应及时向机房负责人报告，由机房负责人通知相关运维人员进

行简单故障排查,并填写《服务器与网络设备故障报告单》。  
若简单故障排查无法解决问题,则应该启动相关应急响应程序。

### **第十九条 机房保密管理**

权限管理严格权限管理,机密数据按权限查阅,机房管理员不准利用工作方便,查看超越自己权限范围的机密数据。

### **第二十条 口令管理**

系统口令应落实到人,并定期进行修改,严禁泄露用户口令及机密数据。具体参见《密码管理规定》。

### **第二十一条 文档管理**

应保密的软件、文档资料、数据等不准随意打印、复制和转移,确因工作需要时,需经过相关领导批准后方可办理。

### **第二十二条 设备启停操作管理**

#### **(一) 设备启停原则**

组织服务器所运行的系统为 24h 运转系统,正常情况下不得停机。如出现异常、增减设备或检修维护而必须停机的,须提前提出申请,经相关领导同意后,在指定时间内完成。

#### **(二) 设备启停需遵循的规则**

1. 启停程序必须由运维人员协同完成;
2. 停机前 24h 需对网上用户发出停机通知,紧急停机须提前半小时通知;
3. 在服务器停机前须由机房管理员确认网上无用户,停止数据库运行后,停止操作系统运行,然后关机;
4. 服务器停机后,再停止网络设备运行;



5.网络系统停止运行后才可停止 UPS 的运行，然后切断电源，通知有关人员进行停机后的各项工作；

6.在工作完成后，检查所有设备的接地、电源及各连线正常后，开启电源，启动 UPS；

7.确认设备状态正常后启动网络设备，检查网络是否正常；

8.在网络正常启动后，确认服务器状态正常后开启服务器，判断服务器自测结果正常后启动操作系统，观察是否正常；

9.在服务器操作系统正常启动后，启动数据库系统，观察是否正常。在数据库正常启动后，通知用户恢复使用；

10.以上各步骤中如有异常，必须立即停止，协同解决后继续，如有重大事件必须及时反映汇报，不得隐瞒。

### **第二十三条 机房巡检管理**

为保证机房内信息系统能够正常工作，确保计算机网络系统安全、良好地运行，充分发挥计算机系统的效益，做到信息传递的适时、准确和连续，必须进行机房巡检。

### **第二十四条 巡检范围**

对各机房内的所有网络设备（路由器、交换机、集线器）及信息设备（服务器、小型机）等进行巡检。

### **第二十五条 巡检规程**

（一）严格按照各机房巡检路线（巡检路线由集团信息中心制定）进行巡检。

（二）检查各信息设备的运转情况，检查是否有异常的声音，各指示灯是否正常。

（三）检查各网络设备（路由器、交换机、集线器）指

示灯是否正常，可对照设备的常态指示灯来巡检。

（四）对于重要的设备，应按照各系统操作规范，在客户端进行应用测试以验证服务器状态是否正常。

## **第二十六条 巡检结果**

由当天的巡检人员填写《机房巡检记录表》，如各项都正常则在相应的栏目中填写“正常”，否则在相应的栏目中填写“不正常”，并在备注栏中填写出现的情况。如发现突发性系统故障严重影响系统的正常运行，应立即启动相应的应急预案并根据应急预案进行汇报，不得隐瞒或谎报。

# **第六章 信息系统生命周期安全管理规定**

## **第二十七条 可行性分析阶段安全管理**

信息网络管理部门应明确系统的安全建设范围和内容，设定安全性指标要求，合理判断信息系统是否符合公司的网络及信息安全要求。给出评估结论，提出存在的安全风险、初步安全建议以及后续注意事项。

## **第二十八条 立项阶段安全管理**

### **（一）供应商评估**

对供应商的安全防护能力与水平进行评估，并将供应商的安全评估结果作为选择供应商的重要依据。

### **（二）合同安全条款评估**

参与合同安全条款的制定，涉及外包或合作开发的项目应签订正式的合同，合同中应包含保密性、信息安全以及隐私保护等方面的条款。

### **（三）项目安全管理**



项目立项完成后，成立项目组，指定信息安全员。信息安全员负责创建安全风险档案，记录系统在其生命周期阶段存在的问题、漏洞、历史整改情况，便于项目组及时了解和确认系统当前的安全风险情况。

## **第二十九条 需求分析阶段安全管理**

信息安全员在业务需求分析阶段同时提出适合系统的安全需求，项目组参照安全性指标要求进行分析。对安全需求进行完整识别，安全需求的识别范围包括但不限于：行业监管与合规安全要求、公司安全策略与标准、行业安全实践经验等。

## **第三十条 设计阶段安全管理**

### **（一）身份认证**

对用户身份进行识别，并根据安全策略配置相关参数，确保系统不被非法用户进入。认证失败处理，连续失败登录后锁定该账号，账号锁定后可由系统管理员解锁，也可以在一段时间后自动解锁。

### **（二）职责与权限设计**

系统必须具有基于人员职责的用户授权管理以确保用户仅可访问其权限范围内的系统部分，严格限制用户访问其权限范围以外的系统部分。

### **（三）日志与审计**

系统中应设置严格的日志记录，以利回溯、追踪、审计。

### **（四）通信安全**

传输过程中的充分考虑数据加密，防止数据和信息在传输中被窃取和篡改。

### **第三十一条 开发阶段安全管理**

#### **(一) 开发过程要求**

##### **1. 输入验证**

对用户输入项进行数据验证，除常见的数据格式、数据长度外，还需要对特殊的危险字符进行处理，特殊字符包括并不限于 <>"' % ( ) & + \ \ \ " 等关键字符，防止注入攻击、脚本攻击等恶意攻击行为。

##### **2. 访问控制**

系统必须具备授权访问控制功能，确保授权的用户仅可访问权限范围内最小的系统功能。

##### **3. 错误处理**

严禁错误响应时将系统核心信息暴露给用户，例如：服务器的 IP 地址、操作系统的类型和版本、会话标识符、账号信息等，从而避免增加服务端被黑客攻击的可能性。

##### **4. 会话管理**

禁止在系统、错误信息或日志中暴露会话标识符，会话信息存储方式以缓存服务器存储,禁止采用文件存储。

##### **5. 数据加密处理**

程序代码中不能直接写入数据库连接串、访问用户和密码等敏感信息，对于无法规避的情况，应当使用配置文件对敏感信息进行配置，并对配置文件的敏感信息进行对称加密处理，在程序中解密后再使用。



在涉及接口交互的过程中，应采用各种加密算法对传输的数据进行签名校验，防止数据被篡改。在条件允许的情况下，可采用 RSA 等非对称加密算法加密请求数据，确保数据传输过程中的保密性。对于公网（互联网）站点，应申请 HTTPS(SSL)证书，采用数字证书的机制来确保数据传输的安全。

## 6. 文件处理

在文件上传处理中，应限制符合要求格式的文件，严禁用户直接上传可执行文件并在服务器端限制可执行文件的执行权限。在文件下载时禁止列举服务器上的文件，同时禁止将服务器端的路径作为参数进行传递，防止用户非法获取服务器端文件。

### （二）开发中运用到的生产数据处理

开发平台上如需使用来自生产环境的敏感数据，必须是通过脱敏处理后的数据，并保留数据导入的处理记录。

### （三）源代码管理

对源代码的访问和修改严格控制，需使用配置管理工具进行代码访问及代码版本控制。

## 第三十二条 测试阶段安全管理

### （一）测试前安全检查

对所有拟上线系统，组织开发人员进行代码审核，检查、消除程序代码潜在的安全漏洞，并由开发人员提交书面审核记录。

（二）测试人员应设计测试计划、测试范围、测试方法和测试工具，充分考虑与其他系统的互操作性。测试中对其

他系统的影响，选择适当的时间、方法。并对应用系统存在的弱点威胁进行安全检查，如：假冒身份、恶意篡改、信息泄露等，测试人员对全过程进行书面记录。

（三）测试与需求设计进行比对和确认，并记录测试结果，记录中需包含对信息安全方面的测试结果，并符合系统设计及信息安全要求。

### **第三十三条 系统上线阶段安全管理**

（一）系统上线部署前，通过开展安全漏洞检查、安全防护配套设施检查等检查手段，确认所有系统相关补丁或改进措施已全部实施，并将此过程及结果进行确认记录。

（二）制定恰当的上线时间，并制定可能产生的影响对应的预案。

（三）为用户提供指南，确保系统上线后业务的操作性、持续性、稳定性。

（四）系统运行后一个月，评估系统在信息安全等方面的符合情况、控制措施的运行效果和效率、以及潜在的需要改进的信息安全措施。并提供书面报告，根据评估情况制定措施持续改进。

### **第三十四条 系统运营阶段安全管理**

#### **（一）变更管理**

应当建立变更控制审批流程，对变更计划的提出和实施进行严格管控，确保变更不会对系统的安全性和完整性造成影响，具体管理流程见附件二《计算机信息系统变更管理》。

#### **（二）安全状态监控**



通过监控预警系统对应用程序服务、网络连接、基础环境等安全运行状态进行实时监控。通过配置各种监控项实现自动报警，确保系统运行安全。

### （三）业务连续性管理

针对应用系统部署保证业务连续运行所需的相关高可用系统，并制定信息系统安全事件应急预案，预案中明确组织机构及工作职责，并定期进行应急演练。

### （四）安全测评与改进

定期进行安全评估，挖掘系统存在的安全漏洞并持续改进。

## **第三十五条 系统退役阶段安全管理**

系统退役时，需对系统数据信息进行妥善转移、转存、销毁，避免发生信息安全事件。包括信息转移或清除、设备迁移或废弃、介质清除或销毁等。系统退役主要经过以下三个阶段：

### （一）系统退役计划

1.系统退役计划形成所需的信息包括：

（1）对历史数据的保存和销毁需求。

（2）对当前软硬件配置，以及带有接口的设备或仪器的识别。

（3）对所有依赖于本系统的数据的外部系统识别。

2.系统退役计划内容包括：

（1）角色和职责

系统退役流程中涉及的角色以及相应责任都应该在计划中以文件形式存档，其中应该包括系统所有者、系统退役

小组及其成员，以及其他所有在退役过程的起作用的相关部门或个人。

## （2）业务流程描述

退役前的业务流程应该从流程、用户群和数据/记录等几个方面进行考虑与文件化。这有助于确保我们已经识别出所有对业务流程可能的影响，并且确保各种对流程的支持措施都已经可以适应系统退役后的状态。

## （3）数据和记录迁移、存档和销毁

计划中应该明确指出哪些数据需要进行转移、存储或销毁。

## （4）系统维护和支持终止

系统退役后，将不再对其他系统提供支持，应计划所有和退役系统相关的系统支持。

## （5）进度表

系统退役过程中的各项工作都应该连同相应的责任人、需完成任务的到期日一起形成进度表，进度表中还应该包括重要的检查点。

## （二）系统退役实施

1.选择适当的实际进行退役实施，可能会包括向替换系统的切换（可能是分阶段进行的，也可能是同时进行的，或者直接切换过去）。

2.有业务持续性计划，以防在进行退役工作或迁移工作时出现问题。另外，可编制一个后备计划，其中包括配置和重新安装系统的详细步骤或者参考资料，以使在确实需要时可以重新安装已退役的系统。



### (三) 系统退役报告

在实施完系统退役计划后，应编制一个总结报告来描述计划实施过程，及其结果。报告中需包括所有和已退役系统相关的文件索引或记录表。

**第三十六条** 集团员工利用公司资源研制的程序，其版权归重庆医药（集团）股份有限公司所有，员工严禁以个人名义享有与出让公司拥有的版权。

**第三十七条** 对于委托第三方开发的应用系统（或功能、模块等）的代码文件或设置文件，在需要对其进行修改时，必须经过信息网络管理部门批准后才能交给执行人进行修改。第三方修改过程严格按照以上“信息系统生命周期安全管理规定”所列要求执行。

## 第七章 密码管理规定

### 第三十八条 密码适用范围

（一）服务器：操作系统管理员密码。

（二）数据库：管理员密码（Sybase 和 SQL Server 为 Sa 密码；Oracle 为 SYS 和 SYSTEM 密码）；应用程序调用数据库的密码。

（三）应用服务程序：三层架构的应用程序中，应用服务的密码。

（四）网站：网站管理员密码。

（五）网络设备：路由器、交换机、防火墙等密码。

### 第三十九条 密码的设置

(一) 服务器、网络设备的密码，由集团信息中心管理确定。已纳入堡垒机管理范围的设备，由堡垒机随机设置并更新。

(二) 服务器、网络设备的密码，须集团信息中心负责人在场时由使用人员记录封存留底。

(三) 办公计算机、应用系统的密码，由使用人自行设置，并报本部门负责人记录封存留底。

(四) 密码内容设置规则：必须由数字、字符和特殊字符组成；密码长度不能少于 8 个字符；机密级计算机设置的密码长度不得少于 10 个字符；设置密码时应尽量避开有规律、易破译的数字或字符组合作为自己的密码。

(五) 重要服务器需要操作系统开机登录密码。

#### **第四十条 密码的修改**

(一) 密码要定期更换：一般服务器密码更换周期不得多于 180 天；重要服务器密码更换周期不得超过 90 天，办公计算机、应用系统的密码更换周期不得多于 90 天。

(二) 服务器、数据库、应用服务器、交换机、路由器、防火墙等所有设备/软件的密码在添加或修改后做好备案，相关人员定期做好密码有效性检查。相关人员工作变化或离职后交出密码，接管人员确认密码后方能完成工作交接。

(三) 修改密码后应更新相应应用程序设置，需对应用、系统进行检查，验证在密码修改后各应用的有效性。

#### **第四十一条 密码的保存**



(一) 设置的用户密码由使用者自行保存, 严禁将自用密码转告他人; 若工作需要必须转告, 应请示上级领导批示。

(二) 服务器、网络设备的非系统管理员使用密码完成后, 系统管理员应该及时更改密码, 保证密码安全。

(三) 所有设置的用户密码须登记造册, 服务器、网络设备的密码集团信息中心负责人记录封存留底。办公计算机、应用系统的密码报本部门负责人记录封存留底。留底文件必须密封保存, 防止密码外泄。

(四) 密码更换后需将新密码或口令记录登记封存。

(五) 如发现密码有泄密迹象或黑客入侵, 发现人要立刻报告集团信息中心, 集团信息中心负责人应及时修改密码, 并严查泄密源头修补系统漏洞, 将详细情况以书面形式上报公司领导。

## **第八章 信息系统数据备份管理制度**

**第四十二条** 备份分为日常备份与更新备份。其中, 日常备份由各应用单位就实际情况建立备份规范, 包括备份周期、备份范围、备份技术等; 更新备份应在系统或软件更新前对现有的重要文件进行备份。

**第四十三条** 信息网络管理部门(指集团信息中心, 分公司及子公司(包括控股子公司)的信息网络管理部门)负责服务器数据管理和备份。

**第四十四条** 信息网络管理部门负责路由器、交换机及其他网络设备数据管理和备份。设备需备份的数据包括配置、

日志、关键数据、应用及其他快速部署系统并保证系统正常生产的必要数据。

**第四十五条** 应用单位需对本单位的各种数据信息的管理和备份负责。应用单位计算机信息安全管理员负责本单位数据备份工作。

**第四十六条** 数据分为一般数据和重要数据两种。一般数据主要指：个人或应用单位的各种信息及办公文档、电子邮件、通讯录等；重要数据主要包括：应用单位数据、应用数据、网站数据、数据库数据等。

一般数据由应用单位自行备份，由本单位计算机信息安全管理员实际操作，由信息网络管理部门提供技术支持。实行“谁备份，谁负责”原则。

重要数据，包括秘密数据由专业人员负责备份；机密文档和人事数据由相关保密人员负责，财务数据由财务人员负责，网站数据、数据库数据等其他数据由信息网络管理部门负责。

**第四十七条** 数据实行三重备份制度，除在本地计算机硬盘上备份外，并应进行异地存储。

一般数据每半年进行一次备份，由应用单位自行存放，保存周期 1 年。应用单位数据、业务应用数据、网站数据、数据库数据每月进行一次备份，保存周期 3 年。

**第四十八条** 所有服务器、主干交换机及其他系统主要设备配置更新变化时及时进行备份

（一）应用系统、软件每次修改后均进行备份，并保存



最新版本。

(二) 每周完全备份服务器上的相关文档。

(三) 每周完全备份数据库中的所有数据。

(四) 每季度将主要数据作为历史数据保存。

(五) 如遇系统有重大改动或更新时，需在改动当天进行备份。

**第四十九条** 所有数据备份工作应由操作人员进行详实记录，要求记录备份的内容、时间及次数。

**第五十条** 信息网络管理部门应定期演练恢复操作，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

**第五十一条** 各备份数据由各责任部门留存，未经部门领导批准不得泄露。

**第五十二条** 如遇网络遭受攻击或病毒感染等突发事件，严格按照相关应急响应预案进行处理，需要进行数据恢复时，由信息网络管理部门执行恢复程序，同时将具体情况记录到数据备份及恢复档案中。

## **第九章 附则**

**第五十三条** 本实施细则自发文之日起执行。本实施细则由公司计算机信息安全管理办公室负责解释。

附件：1. 子公司计算机信息安全自查手册  
2. 计算机信息系统变更管理  
3. 计算机信息系统应急预案

附件 1:

## 子公司计算机信息安全自查手册

(一) 该自查手册针对服务器由子公司管理的信息系统, 自查工作由子公司计算机信息安全管理员担当, 要求做好自查书面记录, 每季度向集团信息中心报告一次自查情况。

(二) 网络安全方面

1. 上网用户计算机管理

A、严禁下载可执行文件等。

B、控制网络流量, 防止大数据(大文件)的上传、下载。

C、控制使用 BT、电骡等 P2P 软件。

D、自查时间: 每月一次。

2. 网络文件共享的管理

A、关闭计算机的默认共享。

B、如需共享的目录、文件等, 设置共享权限为“只读”。

C、自查时间: 每月一次。

3. 网络计算机端口的管理

检查系统软件所需开放的协议和端口, 关闭不必要的端口, 以防病毒的攻击。自查时间: 每月一次。

4. 网络计算机的病毒防范

A、安装正版杀毒软件, 检查升级和病毒查杀情况, 做好检查记录。

B、杀毒软件的防火墙和病毒监控模块必须打开, 操作系统防火墙也必须打开。



C、自查时间：每月一次。

### (三) 服务器安全方面

#### 1. 超级用户的口令管理

A、将默认超级用户“administrator”更名。

B、设置强壮密码，密码 8 位以上，采用数字、字符和特殊字符等共同组成。

C、定期（三个月）更换密码。

#### 2. 服务器上其他用户的管理

A、禁用 Guest 用户。

B、其他用户不得授予超级用户和超级用户组的权限。

C、其他用户只能授予访问特定功能权限，不得滥授权。

D、自查时间：三个月一次。

#### 3. 共享权限的管理

A、关闭计算机的默认共享。包括默认的管理共享如 IPC\$、ADMIN\$和各目录的默认共享。

B、如需共享的目录、文件等，设置共享权限为“只读”。

C、自查时间：三个月一次。

#### 4. 操作系统的补丁升级

A、检查操作系统的补丁升级情况(服务器、工作站等)，做好记录。

B、安装 WSUS 系统，作为补丁分发服务器。

C、自查时间：每月一次。

#### 5. 杀毒软件的安装、升级等

安装正版杀毒软件，并检查升级情况。杀毒软件的防火

墙和病毒监控模块必须打开。操作系统防火墙必须打开。启用单机防火墙（系统和杀毒软件）。自查时间：每月一次。

#### 6.相关端口的关闭

关闭易受攻击的端口，如：135、445、57、1080、3128、6588、8080、161、1433、53、67、2847。自查时间：三个月一次。

#### （四）数据备份方面

- 1.每月一次数据库份（恢复）的有效性检查。
- 2.将数据备份到多个（至少两个不同）地方。
- 3.季度刻盘（或其他方式）异地存放。

#### （五）数据库管理方面

##### 1.Sa 口令的定期更换

设置强壮密码，密码 12 位以上，采用大、小写字母、数字、符合等共同组成。定期（三个月）更换密码。此工作由信息中心负责完成。

##### 2.系统用户权限清理

对各系统用户只授予必须使用模块的权限，用户工作调整后，及时调整权限。

##### 3.数据库安全检查

定期检查各应用单位数据库日志，针对存在问题适当进行调整。此工作由集团信息中心负责完成。



附件 2:

## 计算机信息系统变更管理

### 一、目的

为对信息系统、设备设施等永久性或暂时性的变更进行有计划的、规范的控制，加强信息系统变更风险管理，消除和减少由于变更而引起的隐患，保障信息系统安全稳定运行，特制订本制度。

### 二、变更范围

软件系统功能、数据库、网络硬件系统等改造、升级、更新等。

### 三、角色与职责

变更申请人：负责申请变更，配合相关人员进行变更需求调研，并确认变更需求。在执行计划中，确认变更实施计划满足时间、成本和质量等要求。变更申请人由提出变更需求的部门或个人担任。

变更实施组：负责对用户进行变更需求调研，根据需求给出初步的解决方案，并组织变更评审。在执行计划中，负责制定和组织执行变更实施计划。根据变更内容确定实施人员组成。

变更评审人：负责对最终是否进行变更给出评价，并确定最终变更方案。

### 四、变更管理流程

1.变更申请：变更申请人负责变更申请提起。

2.变更需求调研：由变更实施组组织调研，在变更申请人配合下，完成对变更需求的调研分析，给出初步的方案建议。由变更申请人对方案中的功能、性能、时间、成本等进行确认。并根据确认结果，制定变更计划，对变更过程进行风险分析，确定变更产生的风险，制订控制措施。

3.方案评审：变更评审人员负责评审变更方案的可行性。

4.执行变更计划：变更实施组组织实施变更计划。

5.变更执行完成后，变更申请人对变更情况进行验收，验收通过则变更流程结束。



附件 3:

## 计算机信息系统应急预案

### 应急预案 1

#### 双机系统管理及故障预案

为防止双机运行期间出现异常情况而影响业务正常运行,特制定以下应急方案。

和平物流中心数据库服务器双机系统管理及应急预案

##### (一) 和平物流中心双机简介

双机系统主要是运行 WMS 系统数据。双机主机: PC SERVER DELL R930, 4CPU, 内存 512GB。操作系统是 LINUX 64 位, 数据库使用的是 Oracle 11g。双机软件使用的是 Oracle 数据库自身的 RAC 集群服务。

##### (二) 故障处理流程

1. 首先检查和平物流中心局域网网络是否正常, 若有异常时应告知相关人员检查。

2. 若和平物流中心局域网网络正常但故障仍存在, 检查集群服务是否都有故障, 如果只是单机有故障且集群服务正常, 对有故障单机进行相应处理。

3. 检查服务器硬件各个指示灯是否异常, 若有异常时应告知相关人员处理。

4. 若硬件各个指示灯正常但故障仍存在, 应检查操作系

统日志以及操作系统是否有异常，检查服务器连接阵列的盘是否正常，若有异常时应告知相关人员处理。

### （三）故障处理注意事项

1.及时判断故障处理时间。应将故障处理所需时间明确告知和平物流中心领导和公司分管副总经理。若两台服务器均有故障且在2个小时内不能解决时应考虑应用转移。

2.转移应用，尽量保证数据完整。若不能保证应尽量采用最后备份的数据。对应备份数据后续的数据，只能通过盘点的方式解决库存的问题。单据则根据接口表内容传输。其他数据关系只能手工在数据库中调整。

3.转移的应用应转到备用服务器。

4.故障处理过程要求小心操作，并对每个步骤做好记录。必要时需双人确认故障处理过程。处理过程要求数据库服务提供商到场一起处理。



## 应急预案 2

### 单机系统管理及故障预案

随着公司单位增多，各应用商务系统的应用单位也大幅增加。为了提高系统的稳定性和减少数据丢失的可能性，制定本方案

#### 一、公司联网服务器

##### （一）含义

公司联网服务器是指通过网络与公司中心机房实时连接的服务器，包括中心机房的服务器。

##### （二）故障处理流程（由信息中心完成）

1.首先检查局域网网络是否正常。如果不正常，告知相关人员检查局域网网络设备。

2.如果局域网网络正常但问题还存在，检查服务器硬件各个指示灯，看是否有异常。如有异常，告知相关人员处理。

3.如果硬件各个指示灯正常但问题仍存在，检查操作系统日志，检查操作系统是否有异常，检查服务器连接阵列的盘是否正常。如果有异常告知相关人员处理。

##### （三）故障处理注意事项

1.及时判断故障处理时间。故障处理时间明白无误告知应用部门领导和公司分管副总。服务器都有故障且在2个小时内不能解决应考虑应用转移。

2.转移应用：尽量保证数据完整。如不能保证，尽量采用最后备份的数据。对应备份数据后续的数据，只能通过补

录数据的方式解决

3.手工单据完整无误。对于与和平物流接口的数据通过接口表打印，关掉与和平物流的传输，然后录入商务系统。新录入的单据不传输到和平物流系统。

4.转移的应用转到备用服务器。

5.故障处理过程要求小心操作，并对每个步骤做好记录。必要时双人确认故障处理过程。

## 二、异地应用单位服务器

（一）含义：异地应用单位服务器是指不能通过网络与公司信息中心机房实时连接的服务器。

（二）故障处理流程（由信息中心协助故障单位系统维护人员共同完成）

1.首先检查局域网网络是否正常。如果不正常应告知相关人员（本单位维护人员）检查局域网网络设备。

2.如果局域网网络正常但问题还存在，检查服务器硬件各个指示灯，看是否有异常。如有异常，告知相关人员（本单位系统维护人员）处理。

3.如果硬件各个指示灯正常但问题还存在，检查操作系统日志，检查操作系统是否有异常，检查服务器磁盘是否正常。若有异常应告知相关人员（本单位系统维护人员）处理。

## （三）故障处理注意事项

1.及时判断故障处理时间。故障处理时间明白无误告知应用部门领导和公司分管副总。服务器都有故障且在2个小时内不能解决应考虑应用转移。



2.转移应用：尽量保证数据完整。如不能保证，尽量采用最后备份的数据。对应备份数据后续的数据，只能通过补录数据的方式解决

3.手工单据完整无误。对于与和平物流接口的数据通过接口表打印，关掉与和平物流的传输，然后录入商务系统。新录入的单据不传输到和平物流系统。

4.转移的应用转到备用服务器。若无备用服务器，可用PC代替。

5.故障处理过程要求小心操作，并对每个步骤做好记录。必要时双人确认故障处理过程。

## 应急预案 3

### 网络故障应急预案（主要针对数据传输故障）

#### 一、和平物流中心

检测物理链路（联通、移动、电信等）是否同时中断，如不是同时都中断将所有业务数据迁移到未中断线路上，并且拨打 ISP 电话报修通断线路。如果同时都中断就拨打 3 家 ISP 电话进行报修。

电信报修电话：10000

联通报修电话：10010

移动报修电话：10086

#### 二、分子公司

1.如果分子公司拥有 2 条互联网线路（IPSECVPN 专用一条互联网线路，办公上网另一条互联网线路）。如何 IPSECVPN 线路中断，分子公司拨打当地 ISP 电话报修，并使用 SSLVPN 拨号连接到公司内网进行业务访问。

2.如果分子公司拥有 1 条互联网线路（IPSECVPN 和办公上网公用一条互联网线路）。如何 IPSECVPN 线路中断，分子公司拨打当地 ISP 电话报修，并让电脑连接热点（如手机热点）使用 SSLVPN 拨号连接到公司内网进行业务访问。

#### 三、门店

1.重庆本地门店专线线路中断，检测物理链路 ISP 专线是否中断，如果中断立即拨打 ISP 电话报修通断线路。（由于重庆本地医保政策，目前门店还没有备用线路和方式）



2.非重庆本地门店互联网线路中断，检测物理链路互联网线路是否中断，如果中断立即拨打 ISP 电话报修通断线路，并让电脑连接热点（如手机热点）

