重庆医药(集团)股份有限公司现代物流中心系统安全保障方案

|  |  |  |
| --- | --- | --- |
| 版本 | 修改时间 | 修改人 |
| 0.9 | 2016-7-24 | 曾睿 |
| 1.0 | 2016-12-24 | 张艺严 |

# 1 系统安全方案

## 1.1 物理级安全解决方案

物理安全解决方案主要保护计算机网络设备、设施以及其它媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏。它主要包括三个方面：

### 1.1.1 环境安全

针对系统所在环境采取了如下安全举措：

#### 1.1.1.1 机房设计

机房设计时选择时处于XXXXX，对于地震、水灾等自然灾害具有天然的防护性。

#### 1.1.1.2 火灾防护

机房配备了XXX防火系统，并全部安装防火门，做到对火灾的快速应对。

#### 1.1.1.3 火灾防护

机房安装了XXX空调系统，保证设备处于事宜的运行环境。

#### 1.1.1.4 异地灾备

土主机房在贵州机房具有异地实时备份，共同构成异地容灾系统。

### 1.1.2 设备安全

针对系统所需设备采取了如下安全举措：

#### 1.1.2.1 断电保护

机房配备了xxxxUPS系统，保护设备在突然断电情况下安全

#### 1.1.2.1 门禁控制

机房配备了XXX门禁系统，严格控制人员进出情况。

#### 1.1.2.1 安全意识教育

严格遵照《重庆医药（集团）股份有限公司土主机房管理条例》规范管理机房。加强教育，提高员工的整体安全意识。

## 1.2 网络级安全解决方案

### 1.2.1 隔离与访问控制

#### 1.2.1.1 严格的管理制度

公司统一发布并执行 《重庆医药集团(股份)有限公司信息系统口令及帐户管理规范》、 《重庆医药集团(股份)有限公司信息系统权限管理制度》、 《重庆医药集团(股份)有限公司信息系统安全责任制度》等。

#### 1.2.1.3 防火墙

在互联网与内网之间架设了防火墙，防止外部攻击。通过制定严格的安全策略实现内外网络或内部网络不同信任域之间的隔离与访问控制。

#### 1.2.1.4 区域隔离

数据库，应用服务器，防火墙之间设置DMZ区域，保证数据安全。

### 1.2.2 入侵检测

系统服务器统一配置了XXXX入侵检测系统，对进出网段的所有操作行为进行实时监控、记录，并按制定的策略实行响应（阻断、报警、发送 E-mail ）。从而防止针对网络的攻击与犯罪行为。

### 1.2.3 病毒防护

系统服务器统一按照了XXX防毒软件，并根据安全等级设定定期的安全扫描，上一旦发现病毒，防毒程序会采取相应处理措施（清除、更名或删除），防止病毒进入网络进行传播扩散。

## 1.3 系统级安全解决方案

### 1.3.1 网络结构安全

土主机房网络结构采用XXXX结构，网络拓扑结构合理；路由采用冗余设计，防止单点失败等。

### 1.3.2 操作系统安全

操作系统全部采取如下安全策略：

1. 操作系统根据应用需求进行了详细的安全配置，关闭一些起不常用却存在安全隐患的应用。
2. 操作系统根据应用需求开放必要的端口，关闭其他端口，降低端口扫描风险。
3. 遵照《重庆医药集团(股份)有限公司信息系统口令及帐户管理规范》，在系统中配置对应权限的账户，统一进行管理。采用加强型口令字，并开启密码策略，定期更换口令。
4. 定期进行系统升级，加装安全补丁，修复系统安全漏洞。

### 1.3.3 应用系统安全

重庆医药(集团)股份有限公司现代物流中心主要包括仓库管理系统，物流业务管理系统，药监报告系统等多个应用系统，采用了如下安全保障措施：

#### 1.3.3.1 身份认证

应用系统均由服务端统一进行认证，防止本地篡改的方式，同时相关认证信息进行加密存储，防止泄露。

#### 1.3.3.2 授权/访问控制

应用系统采用严格的授权/访问控制，系统不仅控制应用/用户访问哪些信息，而且控制应用或用户有权执行哪些操作。

#### 1.3.3.3 事务处理

应用系统采用事务的方式处理系统中重要的业务流程，这样可以保证在系统遇到意外状况（比如掉电）发生的时候，系统不会对数据库作任何修改，达到控制和维护数据库数据的一致性和完整性，维护业务数据不会丢失。

1.4.1.5 操作日志

系统提供日志功能，将用户登录、退出系统，以及重要的模块所有的操作

都记录在日志中，并且重要的数据系统采用回收站的方式保留，系统管理员能

够恢复被删除的数据，有效追踪非法入侵和维护系统数据安全。

1.4.1.6 数据备份容错

双机热备份保证 7\*24 小时应用不间断。

为了满足办公自动化系统的持续运行能力的高要求。在继续进行信息化建

设的同时保障系统的高可用性我们可以建议使用双机热备份的方案。提供高可

用性让系统无论是硬件或是软件失效，保证办公应用服务不间断的能力。高可

用性软件简单的说是两种功能的综合：监控功能、切换功能，其基本工作原理

是服务器间通过软件监控服务器，当某服务器硬件或是软件失效，软件的切换

功能发生作用将中断服务器的工作在指定服务器上启动起来使服务器的工作得

以继续。 高可用性软件从功能上分可以分为热备、 容错两种， 细分为双机热备、

双机容错、集群热备、集群容错。热备与容错的区别在于容错软件是应用级的

监控，而热备是主机级的监控。容错软件有着比热备软件更高的不间断性，具

有保护业务关键数据和维持和应用程序高可用的能力， 做到坚持 24\*7 的运作将

保证系统的安全运行。 Legato 公司提供的系列双机软件被认为是当今性价比极

高的产品。同时也是可用于各种不同操作系统环境中的可用性数据备份与灾难

恢复的解决方案。

1.4.1.7 磁盘阵列

磁盘阵列是由一个硬盘控制器来控制多个硬盘的相互连接，使多个硬盘的

读写同步，减少错误，增加效率和可靠度的技术。

磁盘阵列可以通过两种方法来实现：软件阵列与硬件阵列。软件阵列是通

过网络操作系统自身提供的磁盘管理功能将连接的普通 SCSI 卡上的多块硬盘配

置成逻辑盘，组成阵列，可以提供数据冗余功能，但是磁盘子系统的性能会有

所降低。硬件阵列是使用专门的磁盘阵列卡来实现的。硬件阵列能够提供在线

扩容、动态修改阵列级别、自动数据恢复、驱动器漫游、超高速缓冲等功能。

并且磁盘阵列卡拥有一个专门的处理器和存贮器，这样服务器对磁盘的操作就

直接通过磁盘阵列卡来进行处理，不会降低磁盘子系统的性能。

1.4.2 安全管理体系

1.4.2.1 管理目标

网络安全管理目标是：采取集中控制、分级管理的模式，建立由专人负责

安全事件定期报告和检查制度，从而在管理上确保全方位、多层次、快速有效

的网络安全防护。

1.4.2.2 管理框架

考虑到管理体系建立需要有详细的组织架构、人员配备及网络结构等方面

的信息，所以此建议书中仅就网络安全规范提供一个框架性建议，具体管理规

范有待我们对系统进行全面、详细的调查后，与信息中心合作或独立完成。

根据管理规范内容的重要程度和安全管理的复杂性特点，我们认为管理规

范应包括技术、人员与组织结构、应急事件、安全响应服务、安全培训五个方

面的内容，如下图：

1.4.2.3 安全技术规范

1.4.2.3.1 日常操作管理办法：

日常操作规范主要是对日常工作职责、内容、操作流程所做的规定，从而XUNJIAN

实现安全防护的程序化和统一化管理，主要内容包括：

? 各种软件安装、调试、维护、卸载权限和流程；

? 管理员日常监管职责划分；

? 安全扫描评估方式选择；

? 安全事件发现后的分析与记录；