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 灾害防护

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。并严格按照《重庆医药集团股份有限公司灾害应急预案》进行准备，并定期组织演练。

#### 1.1.1.3 环境控制

机房安装了温湿度检测与XXX空调系统，保证设备处于事宜的运行环境。当发生温湿度异常时，系统会自动短信通知对应维护人员处理问题。

#### 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，共同构成异地容灾体系。

### 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，保护设备在电力供应突然切断的情况下安全。

#### 1.1.2.1 门禁控制

机房配备了XXX门禁系统，并由安全环保部门定时巡查，严格控制人员进出情况，防止盗窃、破坏等人为事故的发生。

#### 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。

#### 1.2.1.5 网络层加密

信息系统所在的网络不能直接与公共网络进行联通，当外部网络想要访问内部网络时，只能通过VPN建立专用安全通道，保证传输的机密性与稳定性。

### 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、发送短信提醒等）。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：

#### 1.3.2.1 安全配置

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。

#### 1.3.2.2 端口管理

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。

#### 1.3.2.3 账户控制

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。

#### 1.3.2.4 修复漏洞

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，根据操作者的不同角色赋予不同等级的操作权限。

#### 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。

#### 1.3.3.4 操作日志

应用系统提供日志功能，所有的重要操作均记录在日志中，保证重要操作可查。

#### 1.3.3.5 数据备份容错

应用系统数据库均严格按照《重庆医药集团(股份)有限公司信息中心数据库备份策略》执行定时备份策略，保证数据的安全与可追溯性。

## 1.4 安全管理体系

### 1.4.1 管理框架

现代物流中心信息系统采取集中控制、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、快速有效的安全防护。

### 1.4.2 运维组织

信息中心针对现代物流中心信息系统建立了完整的运维组织，根据相关安全管理制度巡检维护软件系统及相关设备，并定期组织安全培训，根据应急预案进行安全演练，提高人员素质及警惕性部分运维成员如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **部门** | **人员** | **联系方式** | **职责** |
| 信息中心 |  |  | 总体安全责任人 |
| 物流中心 |  |  | 总体安全责任人 |
| XXX公司 |  |  | 安全顾问 |
| 信息中心 | 曾睿 |  | 硬件设备安全责任人 |
| 信息中心 | 雷剑 |  | 应用系统安全责任人 |
| 信息中心 | 刘勇 |  | 数据库安全责任人 |
| 信息中心 |  |  | 网络系统安全责任人 |
| 物流中心 | 安环部的人 |  | 安环设备安全责任人 |
| 物流中心 |  |  | 电力保障安全责任人 |
| 信息中心 |  |  | 硬件设备安全巡检员 |
| 信息中心 |  |  | 硬件设备安全巡检员 |
| 信息中心 |  |  | 硬件设备安全巡检员 |
| 信息中心 | 张艺严 | TEL:15730364985 | 应用系统安全巡检员 |
| 信息中心 |  |  | 应用系统安全巡检员 |
| 信息中心 |  |  | 应用系统安全巡检员 |
| 信息中心 |  |  | 应用系统安全巡检员 |
| 信息中心 |  |  | 数据库安全巡检员 |
| 信息中心 |  |  | 数据库安全巡检员 |
| 物流中心 |  |  | 安环设备安全巡检员 |
| 物流中心 |  |  | 安环设备安全巡检员 |

### 1.4.3 安全规范

安全规范为实现安全防护的程序化和统一化管理，主要内容包括：

#### 1.4.3.1 日常巡检规范

运维组织成员根据《重庆医药（集团）股份有限公司土主机房管理条例》中对工作职责、巡检内容、操作流程等进行日常巡检工作，保障现代物流中心硬件设备与网络系统的稳定运行。

#### 1.4.3.2 应用系统维护规范

运维组织成员遵循《重庆医药（集团）股份有限公司应用系统开发流程》对现代物流中心各类应用系统进行安装、调试、维护等运维工作，保障应用系统的稳定运行。

#### 1.4.3.3 灾害应对规范

现代物流中心遵循《重庆医药（集团）股份有限公司灾害应急预案》进行定期灾害演练。当灾害发生时，快速响应，即使抢救，最大限度的维护重庆医药（集团）股份有限公司与其客户的利益。

#### 1.4.3.4 安全审计规范

运维组织成员定期聘请第三方安全评估现代物流中心信息系统进行安全审计，扫描安全隐患，分析日志记录，定期生成安全审计报告。