|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | 代 号 |  | | 名 称 | 软件安全性评估手册 | |  |  |  |  |  | | --- | --- | | 单 位 |  | | 编 写 |  | | 校 对 |  | | 审 核 |  | | 标 审 |  | | 批 准 |  |  |  | | --- | | 航天恒星科技有限公司 |  |  |  | | --- | --- | | 编 号 |  | | 密 级 |  | | 阶 段 |  | | 页 数 |  |   **会 签** |

目 录

[1 物理安全 1](#_Toc383596150)

[1.1 物理位置选择（机房位置等） 1](#_Toc383596151)

[1.2 物理访问控制（出入刷卡等） 1](#_Toc383596152)

[2 网络安全部分 1](#_Toc383596153)

[2.1 访问控制 1](#_Toc383596154)

[2.1.1 应在网络边界部署访问控制设备，启用访问控制功能 1](#_Toc383596155)

[2.1.2 HTTP、FTP等协议层的网络控制 1](#_Toc383596156)

[2.1.3 。。。 1](#_Toc383596157)

[2.2 安全审计 1](#_Toc383596158)

[2.2.1 网络运行状况，设备等的日志记录 1](#_Toc383596159)

[2.3 入侵防范 1](#_Toc383596160)

[2.3.1 在网络边界处监视： 1](#_Toc383596161)

[2.3.2 恶意代码防范： 1](#_Toc383596162)

[2.3.3 网络设备防护： 2](#_Toc383596163)

[3 主机安全 2](#_Toc383596164)

[3.1 身份鉴别 2](#_Toc383596165)

[3.2 访问控制 2](#_Toc383596166)

[3.3 安全审计 2](#_Toc383596167)

[3.4 入侵防范 2](#_Toc383596168)

[3.5 恶意代码防范 3](#_Toc383596169)

[3.6 资源控制 3](#_Toc383596170)

[4 应用安全 3](#_Toc383596171)

[4.1 身份鉴别 3](#_Toc383596172)

[4.2 访问控制 3](#_Toc383596173)

[4.3 安全审计 3](#_Toc383596174)

[4.4 剩余信息保护 4](#_Toc383596175)

[4.5 通信完整性 4](#_Toc383596176)

[4.6 通信保密性 4](#_Toc383596177)

[4.7 软件容错 4](#_Toc383596178)

[4.8 资源控制 4](#_Toc383596179)

[5 数据安全 4](#_Toc383596180)

[5.1 数据完整性 4](#_Toc383596181)

[5.2 数据保密性 5](#_Toc383596182)

[5.3 数据备份恢复 5](#_Toc383596183)

[6 其他安全管理要求 5](#_Toc383596184)

# 物理安全

## 物理位置选择（机房位置等）

## 物理访问控制（出入刷卡等）

# 网络安全部分

## 访问控制

### 应在网络边界部署访问控制设备，启用访问控制功能

### HTTP、FTP等协议层的网络控制

### 。。。

## 安全审计

### 网络运行状况，设备等的日志记录

## 入侵防范

### 在网络边界处监视：

1. 端口扫描
2. 强力攻击
3. 木马后门攻击
4. 拒绝服务攻击
5. 缓冲区溢出攻击
6. IP碎片攻击、
7. 网络蠕虫攻击等

攻击出现时，网络端需记录类型目的时间等

### 恶意代码防范：

1. 网络层对恶意代码进行检测清除
2. 维护恶意代码库的升级检测系统更新

### 网络设备防护：

1. 登录网络设备的用户进行身份鉴别
2. 应对网络设备的管理员登录地址进行限制

# 主机安全

## 身份鉴别

1. 应对登录操作系统和数据库系统的用户进行身份标识和鉴别
2. 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换
3. 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施
4. 。。。

## 访问控制

1. 启用访问控制功能，依据安全策略控制用户对资源的访问
2. 应实现操作系统和数据库系统特权用户的权限分离
3. 应及时删除多余的、过期的帐户，避免共享帐户的存在
4. 。。。

## 安全审计

1. 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户
2. 。。。

## 入侵防范

1. 能够检测到对重要服务器的入侵行为，记录IP，类型，目的，时间等
2. 。。。

## 恶意代码防范

1. 安装防恶意代码软件（杀毒软件）并定期更行软件版本和恶意代码库
2. …

## 资源控制

1. 对重要服务器进行监视，包括CPU硬盘等资源
2. 限制单用户的最大或最小使用限度

# 应用安全

## 身份鉴别

1. 应提供专用的登录控制模块对登录用户进行身份标识和鉴别
2. 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别
3. 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施
4. 。。。

## 访问控制

1. 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问
2. 应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限
3. 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施

## 是否有超时限制，也就是说，用户登陆后在一定时间内（例如15分钟）没有点击任何页面，是否需要重新登陆才能正常使用上传控制

### 上传类型限制

### 上传文件大小限制

## 安全审计

1. 审计记录的内容至少应包括事件的日期、 时间、发起者信息、类型、
2. …

## 剩余信息保护

1. 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除无论这些信息是存放在硬盘上还是在内存中
2. 。。。

## 通信完整性

1. 应采用密码技术保证通信过程中数据的完整性

## 通信保密性

1. 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证
2. 应对通信过程中的整个报文或会话过程进行加密

## 软件容错

1. 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中
2. …

## 资源控制

1. 当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话
2. 应能够对系统的最大并发会话连接数进行限制；
3. …

# 数据安全

## 数据完整性

1. 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施
2. …

## 数据保密性

1. 应采用加密或其他有效措施实现系统管理数据、 鉴别信息和重要业务数据传输保密性

## 数据备份恢复

1. 应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放
2. …

# 其他安全管理要求

…我在网上看到的资料，显示有一些很常见的WEB安全测试都要包含的内容，如：SQL注入测试；跨站点脚本攻击；跨站点伪造请求；邮件标头注入；目录遍历。。。。考虑一下这些测试是否可行，把这些也加进去。