**北京汇聚融达网络科技有限公司**

**—系统安全控制访问策略**

**文件编码：HJRD-5-12**

**版 本：****V1.0**

**发布日期：2017-11-23**

**文档信息**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **基本信息** | | | | | |
| **文档名称** | 系统安全控制访问策略 | | **保密级别** | 内部 | |
| **文档编号** | HJRD-5-12 | | **牵头部门** | 技术部 | |
| **分发范围** | 制度管控员工 | | | | |
| **版本修订** | | | | | |
| **生效日期** | **版本号** | **版本说明** | **制作** | **复审** | **批准** |
| 上半年 | V1.0 | 第一版 | 刘少会/刘陵镇 | CTO | CEO |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：文档基本信息记录本文档提交时的当前有效的基本控制信息，当前版本文档注有效期将在新版本文档生效时自动结束。文档版本小于1.0 时，表示该版本文档为草案，仅可作为参照资料之目的。

# 目的

为了保护北京汇聚融达网络科技有限公司信息系统资源的安全，防止xxx有限公司的各种信息资产受到非授权访问，造成信息泄露，特制订本管理规定。

# 适用范围

本管理规定适用于北京汇聚融达网络科技有限公司（以下简称“公司”）现有的各种底层操作系统、业务系统以及无人值守设备。

# 职责

信息技术部负责对公司的各种信息资产的访问进行管理；

部门信息管理员负责部门间的协调和配合工作；

各部门主管负责在本部门内部落实此文件的规定。

# 系统访问管理

## 操作系统的访问

1. 对于通用操作系统，必须对系统进行安全设置，保证在进入系统前执行经过验证的登录操作过程，才可以进入系统。
2. 对操作系统进行设置，记录登录成功与失败的日志，以便对系统的审计。
3. 系统要限制登录失败的次数，在3次登录失败之后，就将用户锁定，锁定时间结束后解锁用户。
4. 将管理员账号与普通账号分开，日常使用时只能以普通用户的账号登录，如操作需要管理员权限再提权使用。
5. 所有的用户必须分配有一个唯一的用户ID，用户ID可标识用户名，但不可标识职位与权限。
6. 启用操作系统的口令管理安全策略，保证采用高质量口令。
7. 对于具有身份验证功能的系统程序（如财务系统），程序所属部门应建立登录程序的用户，并对不同用户赋予不同的权限；对于没有用户验证功能的系统，要通过系统的访问权限控制对系统的访问。
8. 对目录和文件设置用户可用的最低权限，并通过属性权限与安全权限控制用户的权限。
9. 操作系统的登录口令必须定期更改，需要符合《xxx有限公司账号、口令和权限管理规定》。

## 应用系统的访问

### 4.2.1业务系统的访问

1. 禁止非法使用他人的账号来进行系统登录。
2. 业务系统采用健壮的身份识别、认证及授权机制。
3. 启用业务系统的登录、注销及关键操作日志记录功能，正确实现操作行为与账号名关联。
4. 对业务系统用户权限进行划分，只给予用户工作需要的最低权限，防止越权操作。
5. 系统管理员定期对应用系统现有的账号、权限进行复查和审计。
6. 应用系统管理员定期对应用系统的登录、操作日志进行审计，及时发现事件并通知责任人和当事人。
7. 需定期备份日志文件。

### 4.2.2企业信息化系统的访问

1. 启用日志记录，日志记录内容包括：登录、注销、系统报警、安全日志、重要应用程序日志和重要文件访问日志等。为保证日志的准确性，需正确设置计算机时钟。
2. 系统管理员必须定期检查日志，依据严重程度对发现的问题进行及时纠正。
3. 可以对系统管理程序或工具设置日志，记录使用用户的情况，包括：用户ID、时间、事件类型、所访问的程序及所使用的文件。
4. 对特权账号实行更严格的日志审查。
5. 发现违反安全策略的情况，需及时处理，并通知责任人和当事人。
6. 需定期备份日志文件。

## 无人值守设备的访问

1. 对于无人值守的设备，必须设置带密码保护的自动屏保程序，同时要求用户在离开时将屏幕锁住。
2. 要定期对无人值守设备的运行状态进行巡检。

# 相关文件

无