**北京汇聚融达网络科技有限公司**

**—系统安全管理制度**

**文件编码：HJRD-5-06**

**版 本：****V1.0**

**发布日期：2017-11-23**

**文档信息**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **基本信息** | | | | | |
| **文档名称** | 系统安全管理制度 | | **保密级别** | 内部 | |
| **文档编号** | HJRD-5-06 | | **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。

**第一条【目标】**为了保护北京汇聚融达网络科技有限公司系统资源的安全，确保北京汇聚融达网络科技有限公司信息系统的安全运行，防止信息系统数据的丢失、破坏和失密；硬件破坏、失效等灾难性故障，特制订本管理规定。

**第二条【职责】**网络与信息中心负责对北京汇聚融达网络科技有限公司的各种信息系统安全进行管理，各部门主管负责在本部门内部落实此文件的规定。

**第三条【 操作系统的访问】**

（一）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。

（二）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。

（三）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。

（四）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。

（五）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。

（六）启用操作系统的口令管理安全策略，保证采用高质量口令。

（七）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。

（八）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。

**第四条【业务系统的访问】**

（一）禁止非法使用他人的账号来进行系统登录。

（二）业务系统采用健壮的身份识别、认证及授权机制。

（三）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关联。

（四）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。

（五）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。

（六）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。

（七）需定期备份日志文件。

**第五条【业务系统的日志管理】**

（一）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。

（二）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。

（三）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。

（四）对特权账号实行更严格的日志审查。

（五）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。

（六）需定期备份日志文件。

**第六条【系统监控方法】**

（一）由网络与信息中心自行监控的对象，其方法：

①服务器每周点检运行状态与日志，北京汇聚融达网络科技有限公司IT系统运行状态检查，详细记录见《服务器日常检查记录》（见附件五十）；

②防病毒产品监控报警 ：适用于业务系统和办公网络系统的防病毒管理，实现北京汇聚融达网络科技有限公司自我管理。

③网络连接测试：适用于业务系统和办公网络系统的网络异常事件、拒绝服务事件；

④服务访问测试：适用于业务系统和办公网络系统的拒绝服务事件、木马等；

⑤防火墙与网络监控设备监控：适用于北京汇聚融达网络科技有限公司办公网络的数据的流入、流出监视与控制；

**第七条【系统监控日志的备份与保护】**

（一）由北京汇聚融达网络科技有限公司信息中心自行监控的对象，其日志的备份与保护实施主要包括：

①为保证日志的准确性，应对业务系统与服务器设置时钟同步；

②系统人员每周检查服务器系统，并对所产生的日志进行收集与备份，以供分析；

③对于服务器支持服务系统的运行日志，系统日志每周打包保存，操作日志每三个月备份一次，目前备份日志在本机保存；

④为确保日志备份信息的完整性，备份日志仅保存在机房，查看人员需经信息中心许可后进入机房查看，不得通过远程访问形式进行查看。

**第八条【系统补丁安装管理】**

所涉及的补丁包括操作系统补丁、数据库补丁和应用系统补丁。

（一）补丁由系统管理员统一进行下载、测试，测试通过后由各系统使用部门自行安装，未经许可，不可私自下载安装。

（二） 补丁来源须为原厂商官方网站或原厂商工作人员，对于非法的补丁禁止安装 。

（三） 补丁安装前，应先做好系统和数据备份工作，避免出现问题进行回退，经严格测试通过后方可安装，对测试不成功的补丁严禁安装。

（四） 测试中发现的问题应做详细分析，判断发生问题的原因并及时解决，如果不能解决，须记录发生问题的环境，立即反馈给原厂商。

（五） 对于刚发布的严重等级漏洞（无补丁）或未通过测试的补丁，可采用临时解决办法消除漏洞的威胁或者暂时接受该风险。

（六）制订补丁修补计划，须先分析信息资产、IT系统环境、IT网络环境和信息资产重要等级，确定需要安装的补丁和相应严重等级，同时明确修补时间、修补方式和修补范围。

（七） 补丁安装前须由相应的补丁管理员和应用系统管理员对变更的必要性、风险和修补计划进行评审，评审通过后，由应用系统管理员安排运维人员全过程配合补丁安装，应用系统管理完成补丁的安装和应用系统的测试。

（八） 补丁安装顺序遵循“资产价值大、威胁等级高优先安装”的原则。对于漏洞级别为严重的补丁，无特殊情况须在补丁发布后1星期内安装。

（九） 补丁安装完成后应进行全面检查，以确认补丁安装情况，同时制定补丁清单列表。

**第九条 【系统安全检查管理】**

(一)系统管理员定期对系统进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况，并对其进行服务器停机申请/操作表（见附件十八）和备份结果检查表（见附件三十五）。

（二）系统管理员定期进行漏洞扫描。