**资鼎(上海)互联网金融信息服务有限公司**

**安全管理制度**

（v1.0）

|  |  |  |  |
| --- | --- | --- | --- |
| 文档编制单位： | 资鼎(上海)互联网金融信息服务有限公司 | 文档编制时间： |  |
| 文档总页数： | 231页 | 文档编制： |  |
| 文档审核人： |  | 审核时间： |  |

**信息安全管理机构制度版本记录**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本记录 | | | | | |
| 版本 | 修改日期 | 修改摘要 | 修改人 | 审批人 | 审批日期 |
| 1.0 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**目录**

[第一章 信息安全管理制度总则 8](#_Toc489607028)

[1.1 概述 8](#_Toc489607029)

[1.2 总体原则 8](#_Toc489607030)

[1.3 总体目标 9](#_Toc489607031)

[1.4 总体框架 9](#_Toc489607032)

[1.4.1 系统信息运维安全策略 9](#_Toc489607033)

[1.4.2 信息系统安全管理安全策略 10](#_Toc489607034)

[1.5 适用范围 12](#_Toc489607035)

[第二章 安全管理体系文件 13](#_Toc489607036)

[2.1 目的 13](#_Toc489607037)

[2.2 范围 13](#_Toc489607038)

[2.3 职责 13](#_Toc489607039)

[2.4 管理细则 14](#_Toc489607040)

[2.4.1 体系文件生命周期流程 14](#_Toc489607041)

[2.4.2 体系文件策划 14](#_Toc489607042)

[2.4.3 体系文件的评审 15](#_Toc489607043)

[2.4.4 体系文件的作废 15](#_Toc489607044)

[第三章 信息安全管理体系 16](#_Toc489607045)

[3.1 信息安全管理体系 16](#_Toc489607046)

[3.1.1 信息安全管理体系建立 16](#_Toc489607047)

[3.1.2 信息安全管理体系实施 17](#_Toc489607048)

[3.1.3 信息安全管理体系监察 17](#_Toc489607049)

[第四章 信息安全组织机构制度 18](#_Toc489607050)

[4.1 信息安全组织机构 18](#_Toc489607051)

[4.1.1 信息安全职能部门职责 18](#_Toc489607052)

[4.1.2 信息安全领导小组职责 19](#_Toc489607053)

[4.1.3 信息系统安全小组职责及要求 19](#_Toc489607054)

[4.1.4 信息安全小组权限 27](#_Toc489607055)

[4.1.5 信息安全管理人员 27](#_Toc489607056)

[4.1.6 关键岗位协议 29](#_Toc489607057)

[第五章 信息安全授权及审批管理制度 34](#_Toc489607058)

[5.1 信息安全授权及审批管理制度 34](#_Toc489607059)

[第六章 审核与检查管理制度 35](#_Toc489607060)

[6.1 审核与检查管理制度 35](#_Toc489607061)

[6.1.1 定期安全检查 35](#_Toc489607062)

[6.1.2 文件审批与发布管理制度 36](#_Toc489607063)

[第七章 办公环境管理制度 38](#_Toc489607064)

[7.1 办公环境管理制度 38](#_Toc489607065)

[第八章 沟通与合作管理制度 40](#_Toc489607067)

[8.1 沟通与合作管理制度 40](#_Toc489607068)

[8.1.1 信息安全例会管理 40](#_Toc489607069)

[8.1.2 外部协作管理 41](#_Toc489607070)

[第九章 人员入岗管理制度 42](#_Toc489607072)

[9.1 信息安全条款 42](#_Toc489607073)

[9.2 保密协议 42](#_Toc489607074)

[9.3 人员录用和上岗安全管理 42](#_Toc489607075)

[第十章 人员在岗管理制度 44](#_Toc489607077)

[10.1 人员在岗信息安全管理 44](#_Toc489607078)

[10.1.1 岗位信息安全检查 44](#_Toc489607079)

[10.1.2 信息安全违规纪律处理 44](#_Toc489607080)

[10.2 人员考核 44](#_Toc489607081)

[10.3 关键岗位考核制度 44](#_Toc489607082)

[第十一章 信息安全培训制度 46](#_Toc489607084)

[11.1 信息安全培训制度 46](#_Toc489607085)

[第十二章 人员离岗管理制度 47](#_Toc489607087)

[12.1 人员离岗离职安全管理 47](#_Toc489607088)

[12.1.1 资产归还 47](#_Toc489607089)

[12.1.2 访问权限回收 47](#_Toc489607090)

[12.1.3 离职后信息安全职责的追踪和管理 47](#_Toc489607091)

[第十三章 外来人员管理制度 49](#_Toc489607093)

[13.1 第三方人员安全管理 49](#_Toc489607094)

[13.2 外来人员信息安全管理 49](#_Toc489607095)

[第十四章 工作人员安全守则 51](#_Toc489607098)

[14.1 工作人员安全守则 51](#_Toc489607099)

[第十五章 信息系统建设安全管理制度 54](#_Toc489607102)

[15.1 安全设计需求分析及评估 54](#_Toc489607103)

[15.1.1 应用系统基本安全需求 54](#_Toc489607126)

[15.1.2 硬件系统基本安全需求 55](#_Toc489607127)

[15.1.3 总体安全设计 63](#_Toc489607128)

[15.1.4 安全建设规划 69](#_Toc489607129)

[15.2 系统工程实施 71](#_Toc489607130)

[15.2.1 产品采购管理制度 71](#_Toc489607131)

[15.2.2 安全服务商选择 72](#_Toc489607132)

[15.2.3 硬件采购和安装 73](#_Toc489607133)

[15.2.4 软件采购和安装 73](#_Toc489607134)

[15.2.5 系统软件开发管理 74](#_Toc489607135)

[15.3 系统测试验收 75](#_Toc489607136)

[15.4 系统交付 76](#_Toc489607137)

[15.5 系统备案 76](#_Toc489607138)

[第十六章 硬件设备运维管理制度 77](#_Toc489607140)

[16.1 硬件设备运维管理制度 77](#_Toc489607141)

[16.1.1 机房安全管理制度 77](#_Toc489607142)

[16.1.2 办公环境安全管理制度 79](#_Toc489607143)

[16.1.3 资产安全管理制度 80](#_Toc489607144)

[16.1.4 介质安全管理制度 85](#_Toc489607145)

[16.1.5 设备管理制度 90](#_Toc489607146)

[16.1.6 网络安全管理制度 92](#_Toc489607147)

[第十七章 系统软件运维管理制度 96](#_Toc489607148)

[17.1 系统软件运维管理制度 96](#_Toc489607149)

[17.1.1 系统安全管理制度 96](#_Toc489607150)

[17.1.2 恶意代码防范管理制度 103](#_Toc489607151)

[17.1.3 密码使用管理制度 104](#_Toc489607152)

[17.1.4 信息系统变更管理制度 105](#_Toc489607153)

[第十八章 备份与恢复管理制度 109](#_Toc489607155)

[18.1 备份与恢复管理制度 109](#_Toc489607156)

[18.1.1 备份制度流程图 110](#_Toc489607158)

[18.1.2 资产识别 110](#_Toc489607159)

[18.1.3 备份方案 111](#_Toc489607160)

[18.1.4 备份计划实施 112](#_Toc489607161)

[18.1.5 备份的介质标识 112](#_Toc489607162)

[18.1.6 备份介质的安全存放 112](#_Toc489607163)

[18.1.7 信息恢复 112](#_Toc489607164)

[第十九章 信息系统安全事件管理制度 114](#_Toc489607166)

[19.1 信息系统安全事件管理制度 114](#_Toc489607167)

[19.1.1 安全事件定义 114](#_Toc489607168)

[19.1.2 安全事件等级划分 115](#_Toc489607169)

[19.1.3 安全事件处理流程 116](#_Toc489607170)

[19.1.4 安全事件报告流程 130](#_Toc489607171)

[第二十章 硬件维护日常操作管理规程 132](#_Toc489607173)

[20.1 硬件维护日常操作管理规程 132](#_Toc489607174)

[20.1.1 交换机 132](#_Toc489607175)

[20.1.2 路由器 132](#_Toc489607176)

[20.1.3 防火墙 132](#_Toc489607177)

[20.1.4 小型机 133](#_Toc489607178)

[20.1.5 PC服务器 133](#_Toc489607179)

[20.1.6 审计系统 133](#_Toc489607180)

[第二十一章 信息系统操作规程 135](#_Toc489607182)

[21.1 信息系统操作规程 135](#_Toc489607183)

[21.1.1 服务器设备操作规程 135](#_Toc489607184)

[21.1.2 网络设备操作规程 136](#_Toc489607185)

[第二十二章 应急机构 138](#_Toc489607187)

[22.1 应急机构及角色设置 138](#_Toc489607188)

[22.1.1 应急领导小组 138](#_Toc489607189)

[22.1.2 应急协调小组 138](#_Toc489607190)

[22.1.3 应急实施小组 139](#_Toc489607191)

[22.1.4 外部应急协助组 139](#_Toc489607222)

[第二十三章 应急预案 140](#_Toc489607223)

[23.1 信息系统应急预案 140](#_Toc489607224)

[23.1.1 应急预案分类 140](#_Toc489607225)

[23.1.2 应急预案启动 140](#_Toc489607226)

[23.1.3 应急处理流程 143](#_Toc489607227)

[23.1.4 系统恢复 145](#_Toc489607228)

[23.1.5 故障总结及报告 146](#_Toc489607229)

[23.1.6 应急演练 146](#_Toc489607230)

[23.2 附录 148](#_Toc489607231)

[23.2.1 附1：体系文件建立申请表 148](#_Toc489607232)

[23.2.2 附2：体系文件更改申请表 149](#_Toc489607233)

[23.2.3 附3：体系文件评审记录表 150](#_Toc489607234)

[23.2.4 附4：体系文件作废申请表 151](#_Toc489607235)

[23.2.5 附5：专家论证表 152](#_Toc489607236)

[23.2.6 附6：专家意见书 153](#_Toc489607237)

[23.2.7 附7：专家论证会会议纪要 154](#_Toc489607238)

[23.2.8 附录8 :安全评估报告 155](#_Toc489607239)

[23.2.9 附录9 资产清单 156](#_Toc489607240)

[23.2.10 附录10 :系统的操作手册 158](#_Toc489607241)

[23.2.11 附录11：信息系统安全检查表单 158](#_Toc489607242)

[23.2.12 附录12：备份管理员操作变更申请单 159](#_Toc489607243)

[23.2.13 附录13：密码变更记录表 161](#_Toc489607244)

[23.2.14 附录14：审计记录 163](#_Toc489607246)

[23.2.15 附录15：授权与审批流程 165](#_Toc489607247)

[23.2.16 附录16：系统配置变更审批单 166](#_Toc489607248)

[23.2.17 附录17: 安全检查表 168](#_Toc489607249)

[23.2.18 附录18: 安全检查报告与通报 170](#_Toc489607250)

[23.2.19 附19:外联单位联系表 171](#_Toc489607252)

[23.2.20 附20:会议记要 172](#_Toc489607253)

[23.2.21 附21:信息安全专家聘任书 173](#_Toc489607254)

[23.2.22 附录22 :保密协议 173](#_Toc489607255)

[23.2.23 附录23: 上岗人员情况登记表 178](#_Toc489607260)

[23.2.24 附录24: 人员入岗审核表 180](#_Toc489607261)

[23.2.25 附录25: 岗位协议书 （需打印） 181](#_Toc489607262)

[23.2.26 附录26：信息安全岗位人员考核记录 185](#_Toc489607264)

[23.2.27 附录27：安全技能考核纪录 186](#_Toc489607265)

[23.2.28 附录28：关键岗位审查情况表 187](#_Toc489607279)

[23.2.29 附录29：信息安全培训计划 193](#_Toc489607281)

[23.2.30 附录30：安全教育培训签到表 195](#_Toc489607282)

[23.2.31 附录31: 安全教育培训评价表 196](#_Toc489607283)

[23.2.32 附录32：年度信息安全培训计划 197](#_Toc489607284)

[23.2.33 附录33：培训考题 198](#_Toc489607285)

[23.2.34 附录34：培训考核记录表 202](#_Toc489607289)

[23.2.35 附录35: 人员离岗/职审批表 204](#_Toc489607290)

[23.2.36 附录36: 人员离岗工作交接表 206](#_Toc489607291)

[23.2.37 附录37: 离职保密承诺书 208](#_Toc489607292)

[23.2.38 附录38: 机房进出申请单 209](#_Toc489607293)

[23.2.39 附录39: 机房进出记录表 211](#_Toc489607294)

[23.2.40 附录40：机房出入登记表 213](#_Toc489607295)

[23.2.41 附录41：机房设备出门单 214](#_Toc489607296)

[23.2.42 附录42：设备维护档案 215](#_Toc489607297)

[23.2.43 附录43：信息安全存储介质领用/借用申请单 216](#_Toc489607298)

[23.2.44 附录44：介质销毁审批表 217](#_Toc489607299)

[23.2.45 附录45：信息安全存储介质维修记录 218](#_Toc489607300)

[23.2.46 附录46：设备领用表 219](#_Toc489607302)

[23.2.47 附录47：计算机设备责任人变更审批表 220](#_Toc489607303)

[23.2.48 附录48：特权用户申请表 221](#_Toc489607304)

[23.2.49 附录49：服务器补丁升级记录 222](#_Toc489607305)

[23.2.50 附录50：变更申请单 223](#_Toc489607306)

[23.2.51 附录51：备份记录 225](#_Toc489607307)

[23.2.52 附录52：恢复记录 226](#_Toc489607308)

[23.2.53 附录53：备份与恢复演练记录单 226](#_Toc489607309)

[23.2.54 附录54：安全事件记录报告 227](#_Toc489607310)

[23.2.55 附录55：信息安全事件调查报告 228](#_Toc489607311)

[23.2.56 附录56：硬件维护 229](#_Toc489607312)

[23.2.57 附录57：工作日志 230](#_Toc489607313)

[23.2.58 附录58：信息系统巡检 231](#_Toc489607314)

# 信息安全管理制度总则

## 概述

信息系统安全等级保护管理制度体系是对实现信息系统安全等级保护所采用的安全管理措施的描述。本制度体系从信息安全管理机构制度、信息安全人力资源管理制度、信息系统建设安全管理制度、信息安全系统运维管理制度和信息系统操作规程及应急预案等方面，针对资鼎(上海)互联网金融信息服务有限公司的“马上贷”系统，从信息安全管理和信息系统运维两个方面做出规定。

## 总体原则

本制度的信息安全总体原则如下：

* 全面贯彻国家和上海市关于信息安全工作的要求文件和相关指导性文件精神，在部门内建立符合国家要求完善的信息安全管理体系；
* 建立由安全策略、管理制度、操作规程等构成的全面信息安全管理制度体系，并落实信息安全管理责任到个人，使信息安全管理有章可循；
* 定期进行信息安全培训，提高相关人员信息安全意识及能力；
* 实行预防为主，应急为辅的信息安全理念，对可能存在的信息安全隐患进行提前预防性排查和处理；对于突发性信息安全事件，可以按照应急预案进行快速响应，将事件影响降到最低；
* 定期对信息系统进行风险评估和控制，将信息安全风险控制在可接受的水平，以降低突发性事件出现的概率；
* 持续改进信息安全管理所要求包含的各项工作，为系统提供可靠的安全信息服务。

## 总体目标

* 明确资鼎(上海)互联网金融信息服务有限公司信息安全管理机构和人力资源管理制度；
* 按照等级保护三级要求规范资鼎(上海)互联网金融信息服务有限公司的“马上贷”系统建设和运维；
* 制定资鼎(上海)互联网金融信息服务有限公司的“马上货”系统应急预案，并定期进行应急演练；
* 定期开展全系统范围的信息系统安全检查和信息安全管理制度宣传，并按需开展第三方信息安全风险评估。

## 总体框架

本制度的安全策略包括信息安全管理安全策略和信息系统运维安全策略，如下图所示：



### 系统信息运维安全策略

系统信息运维安全策略包括信息安全管理机构制度和信息安全人力资源管理制度。

#### 信息安全管理机构制度

* 建立资鼎(上海)互联网金融信息服务有限公司的“马上货”系统信息安全管理组织机构

明确网络管理员、主机管理员、系统管理员、安全管理员、安全审计员等安全管理相关岗位及职责。

* 加强信息安全的授权和审批

对于系统变更（包含软件和硬件）实施审批，并记录在案。

* 定期审查信息安全管理体系

监督各项安全控制措施的落实情况，并针对有偏差的地方进行纠正，以保证信息安全管理体系持续有效。

* 规范产品采购和使用管理制度流程

明确产品所有者、使用者与维护者；对所有产品进行标记，实现信息资产从采购、安装、调试、使用、变更到报废整个周期的安全管理，并且密码相关产品符合国家密码主管部门的要求。

* 定期评估安全风险

根据评估结果选择适当的安全策略和控制措施，保证安全风险可控。

#### 信息安全人力资源管理制度

* 加强人员安全管理

包含人员录用前考察、人员在岗和离岗的安全控制、人员考核、奖惩措施等内容；对于关键岗位的工作人员，需签订保密协议。

* 保密协议签署

对于外包的软件开发，需与服务提供商签署保密协议；在信息系统立项和审批过程中，同步考虑信息安全需求和目标。系统开发完成后，要求通过第三方安全机构对软件安全性的测评。

### 信息系统安全管理安全策略

信息系统安全管理安全策略包括信息建设安全管理制度、信息安全系统运维管理和信息系统操作规程及应急预案。

#### 平台信息系统安全管理

* 公司的平台信息系统需要满足《GB/T 22239-2008信息安全技术信息系统安全等级保护基本要求》相对应的安全指标要求，安全管理程序也要符合国际公认的标准，并需要通过独立第三方审计的验证。通过系统的、持续的方法来管理信息安全风险，以保障自身及客户信息的保密性、完整性和可用性。
* 平台信息系统要从网络层、应用层、到主机层三个层面对系统进行全面的防护，包括但不限于：木马扫描、远程登录密码破解、异地登录检测、DDoS、CC攻击防护、漏洞扫描、端口安全、SQL注入和XSS等。
* 平台信息系统所使用的多层体系架构，需要将不同层级的访问隔离，屏蔽系统攻击风险、提升访问性能和高可用性。
* 服务器管理员要加强对服务器的安全防护工作，及时查毒、杀毒，不得在服务器上使用带有病毒和木马的移动存储设备，防止因病毒导致公司网上对外业务的中断。
* 任何个人在未经公司授权的情况下，不得擅自删除、移动、更改服务器上的重要数据，也不能随意更改服务器的系统时间。
* 服务器上的重要数据必须做好实时备份，必要时将备份异地存放，确保系统一旦发生故障时能快速恢复。
* 数据库（如MySQL）要采用集群化布署，并通过读写分离等主备机制提升系统性能和保障数据安全，并隔日在云端做全量备份，实时做日志增量备份。
* 数据库账户及其权限应依据“最小授权”原则进行设置，不同用途的账户应分设，并应对授权的再次传播进行控制。
* 数据库正式启用后，严禁随意变更修改系统配置，如确需变更，必须制定完备的操作方案、回退计划，进行充分的风险评估，并经审批通过后，方可实施。

#### 信息建设安全管理制度

* 文档发布制度化

制定文档发布规范制度，统一文档版本、格式等，并定期按照制度对文档进行更新，以保证所有文档的时效性。

#### 信息安全系统运维管理

* 保障机房物理与环境安全

实施多种手段对机房安全进行监控（如，门禁、视频监控、红外线报警等安全防范措施），确保机房物理安全。部署机房专用空调、UPS，灭火设备等环境保障设施；每天对机房设施运转情况进行定期巡检和维护。控制机房人员和设备的出入管理，非管理人员无法进入主机房，外部人员进入机房需填写出入记录并且由管理人员全程陪同。

* 维护和操作规程文档化

对系统维护和操作规程实施文档化操作，降低和避免因误操作所引发信息安全事件的可能性。

* 定期备份重要系统和数据

对重要的数据和信息系统进行每日增量备份每周全量备份，并对备份介质进行安全地保存，以及对备份数据每季度进行备份还原测试，保证各种备份信息的保密性、完整性和可用性，确保所有重要信息系统和重要数据在故障、灾难后及其它特定要求下进行可靠的恢复。

#### 信息系统操作规程及应急预案

* 信息安全事件应对机制

建立对各类信息安全事件的预防、预警、响应、处置、恢复机制，编写针对网络、数据库、系统和恶意代码等的应急预案，并每年两次进行测试和演练。

## 适用范围

本手册按照ISO/IEC 27001：2005 《信息安全管理体系要求》，结合资鼎(上海)互联网金融信息服务有限公司的“马上货”系统的实际编制而成，符合ISO/IEC 27001：2005 标准的全部要求。本管理制度适用于资鼎(上海)互联网金融信息服务有限公司的“马上货”系统建设和运维过程。

# 安全管理体系文件

## 目的

为规范资鼎(上海)互联网金融信息服务有限公司（以下简称“资鼎金服”）的信息安全管理体系文件的制订、修订及评审，特制定本制度。

## 范围

本管理规范适用于信息安全领导小组和工作小组对信息安全管理体系文件的维护管理。

## 职责

由信息安全工作小组的主体部门资鼎金服负责信息安全管理体系文件的维护，包括制订、修订和评审，由信息安全领导小组负责体系文件的批准、发布和作废。

## 管理细则

### 体系文件生命周期流程



体系文件流程图

### 体系文件策划

信息安全工作小组组织相关人员，根据《信息安全技术 信息系统安全等级保护基本要求（GBT 22239-2008）》、 《信息安全技术 信息系统安全管理要求（GBT 20269-2006）》、《ISO/IEC 27001：2005 信息安全管理体系》的要求， 结合实际的职责和工作流程，策划制定信息安全管理体系文件，并形成《资鼎(上海)互联网金融信息服务有限公司信息安全管理体系文件汇编》。

信息安全工作小组将制定的《资鼎(上海)互联网金融信息服务有限公司信息安全管理体系文件汇编》汇报给信息安全领导小组，信息安全领导小组进行审批确认。

### 体系文件的评审

信息安全工作小组应定期发起对体系文件的评审, 应填写《体系文件建立申请表》(详见附1)。对体系文件的评审应至少每年进行一次。评审流程如下：

(1) 信息安全工作小组发起对体系文件的评审申请，信息安全领导小组确认后批准评审要求。

(2) 信息安全工作小组制定评审计划。计划中应确定各文档对应的评审责任人以及实施评审的时间计划。

(3) 各评审责任人根据时间计划，结合内部审核、管理评审、风险评估及日常记录的结果，评估现有文件的有效性和充分性。如果确定文档有必要进行修改，应填写《体系文件更改申请表》(详见附2)。

(4) 如果修改的内容只涉及研发部，则由信息安全工作小组组长进行审批，在审批同意后，由文档评审责任人进行修改。

(5) 如果修改的内容涉及到研发部以外的部门，需要所有涉及部门的会签。会签后，由文档评审责任人进行文档修改。如需要，可邀请专家对体系文件进行专家评审（详见附5、附6、附7）。

(6) 修改完毕之后，各责任人将《体系文件评审记录表》(详见附3)和完善后的体系文件版本一并报送信息安全工作小组，由信息安全工作小组进行标识和保存。

(7) 信息安全工作小组最终对评审结果向信息安全领导小组进行汇报。

### 体系文件的作废

(1) 在体系文件的评审过程中，如果评审责任人认为文件应当作废，则填写《体系文件作废申请表》(详见附4)，由信息安全工作小组审批后，报信息安全领导小组进行审批。

(2) 信息安全领导小组审批完成后，信息安全工作小组负责通知所有相关人员，并对《资鼎(上海)互联网金融信息服务有限公司信息安全管理体系文件》进行废除。

# 信息安全管理体系

## 信息安全管理体系

以ISO/IEC 27001：2005 《信息安全管理体系要求》为依据，建立信息安全管理体系，并形成相关的信息安全管理体系文件。由资鼎(上海)互联网金融信息服务有限公司主管领导批准发布，在资鼎(上海)互联网金融信息服务有限公司范围内实施并保持，利用内部审核、管理评审、定期检查、定期更新和预防措施以及持续改进的手段，确保信息安全管理体系的有效性。

### 信息安全管理体系建立

#### 管理体系范围

根据资鼎(上海)互联网金融信息服务有限公司系统业务特点、组织机构、物理位置确定本公司“马上货”系统信息安全管理体系的范围为：

* 所有部门和正式工作人员，包括资鼎(上海)互联网金融信息服务有限公司所有成员；
* 资鼎(上海)互联网金融信息服务有限公司研发部主要负责本公司的“马上货”系统建设和运行工作及系统维护和管理；
* 与系统业务活动相关的应用系统及其包含的全部信息资产，其中应用系统包括：资鼎(上海)互联网金融信息服务有限公司的“马上货”系统；信息资产包括：与上述业务应用系统相关的数据、硬件、软件、服务及文档等。

#### 风险评估

在体系建立过程中，资鼎(上海)互联网金融信息服务有限公司确定信息安全风险评估方法，对本公司的“马上货”系统实施风险评估(详见附8)，识别本公司的“马上货”系统所面临的风险，并根据风险进行相应的处理。

#### 风险处置

在风险评估后，根据风险评估的结果，确定风险处置的策略，包括：

* 采用风险控制措施，以降低面临的信息安全风险；
* 在满足信息安全方针和风险接受准则的前提下，有意识地、客观地接受风险；
* 转移相关业务风险到其他方面，如：购买产品维保，运维服务外包等；
* 根据风险处置策略，制定风险控制措施，对已识别出的风险进行分类处理，并对残余风险进行了批准。

### 信息安全管理体系实施

在实施和运行信息安全管理体系中所开展的工作包括：

* 通过风险管理方法来控制信息系统中存在的信息安全风险，配置资源、明确职责和优先级别，实施适当的管理措施；
* 实施各信息安全管理体系文件中包括的控制措施，以达到各控制目标；
* 实施培训和意识教育计划，具体内容参见《培训制度》；
* 实施能迅速检测安全事件和响应安全事故的程序。

### 信息安全管理体系监察

严格执行监视和评审程序以及其它相关措施，以达到：

* 迅速检测信息安全管理体系运行过程中的缺陷和弱点；
* 迅速识别潜在的和已发生的信息安全违规和事故；
* 确保管理者分配给各人员的信息安全活动或通过信息技术实施的信息安全活动能如期执行；
* 确定信息安全措施的有效性；
* 定期进行信息安全管理评审，以判断信息安全管理体系的有效性；
* 定期进行信息安全风险评估的评审；
* 定期对信息安全管理体系进行管理评审；
* 依据监视和评审活动的结果，对信息安全管理体系进行修改和完善；
* 记录可能影响信息安全管理体系有效性或执行情况的措施和事件。

# 信息安全组织机构制度

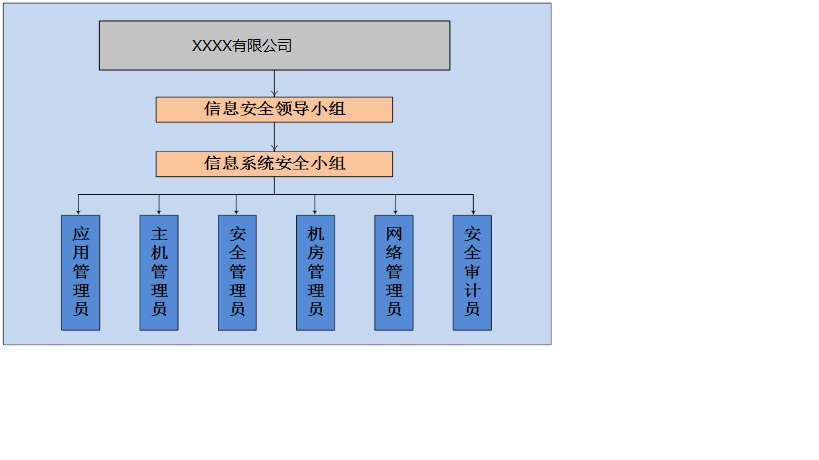
## 信息安全组织机构

资鼎(上海)互联网金融信息服务有限公司针对本公司的“马上货”系统的信息安全组织机构包括信息安全领导小组和信息系统安全小组。

信息系统安全小组的成员包括：机房管理员、主机管理员、网络管理员、应用管理员、安全管理员、安全审计员。

根据各个职位职责不同，对于安全管理员与安全审计员应配备专职人员，不可兼任；对于关键事务岗位应考虑多人共同管理。

资鼎(上海)互联网金融信息服务有限公司信息安全体系组织机构图如下：



### 信息安全职能部门职责

信息安全职能部门为研发部，主要职责如下：

* 保障机房信息系统的安全运行；负责机房的环境维护和物理访问管理；负责机房的设备维护及设备管理；负责机房内任何事故的上报及处理；负责制定及修订有关机房安全管理制度。
* 负责对机房值班人员及技术维护人员（外包方）进行日常工作管理和检查；
* 负责本公司的“马上货”系统的使用控制及处置管理。
* 介质的使用人负责在单位内部介质的使用控制及处置管理。
* 各相关接待人负责其接待的外来人员的介质的使用及监督。
* 负责本公司网络系统安全管理。
* 负责本公司基础平台系统安全管理，应用系统安全管理。
* 负责本公司信息系统的恶意代码防范工作，及发生恶意代码攻击时的应急处理。
* 负责本公司信息系统的密码使用管理工作，包括密码的保管、分配、修改、授权。
* 负责本公司信息系统数据备份与恢复管理工作。
* 负责本公司信息系统安全事件管理工作。

### 信息安全领导小组职责

信息安全领导小组主要职责如下：

* 负责关于信息安全方面工作的方针政策；
* 审定资鼎(上海)互联网金融信息服务有限公司的“马上货”系统的安全建设规划；
* 对信息系统安全工作的重大事项做出决策；
* 研究审定资鼎(上海)互联网金融信息服务有限公司的“马上货”系统安全建设和管理工作中的制度、标准及相关政策，并协调相关部门监督制度、政策的实施情况；
* 组织、协调和指导信息安全的宣传、普及教育工作。

### 信息系统安全小组职责及要求

* 负责贯彻落实信息安全领导小组关于信息系统安全工作的要求和规定，并落实各项安全工作；
* 负责信息系统的安全管理体系和规章制度的建立、实施；
* 建设、技术保障和操作规范等各方面的逐步建成；
* 组织制订和贯彻信息系统运行安全保障和维护工作制度。

#### 机房管理员职责及要求

**机房管理员主要职责如下：**

* 负责保障机房物理与环境的安全建设管理
* 负责制定机房基础设施的相关资产清单(详见附9)

内容包括资产名称、重要程度、所处位置等。

* 明确产品所有者、使用者与维护者；对所有产品进行标记，实现信息资产从采购、安装、调试、使用、变更到报废整个周期的安全管理，并且密码相关产品符合国家密码主管部门的要求。
* 令相关人员能够按照维护规程对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性。
* 负责保障机房物理与环境安全

实施包括门禁、视频监控、报警等安全防范措施，确保机房物理安全。部署机房专用空调、UPS等环境保障设施，对机房设施运转情况进行每日至少一次巡检、维护、故障处理和变更管理。严格对机房人员和设备的出入管理，进出需登记，外来人员需由相关管理人员陪同方能访问机房。

* 在机房基础设施变更、重要操作、物理访问等的进行逐级审批，负责日常审批，重大变更需上报到资鼎(上海)互联网金融信息服务有限公司领导小组负责人进行核准和审批后，方可进行变更；
* 负责组织实施机房基础设施各类事故（故障）的应急处理。

**机房管理员任职要求如下：**

1、遵守资鼎(上海)互联网金融信息服务有限公司的各项规章制度；具有良好的职业道德和敬业精神；

2、爱岗敬业，吃苦耐劳，愿意长期从事机房管理工作；

3、服从分配与管理，团结协作具有良好的团队精神；能全心全意为资鼎(上海)互联网金融信息服务有限公司服务，言行举止形象文明；

4、了解计算机软硬件安装及维护，动手能力强；

5、具有一定的组织能力和语言表达能力。

6、具备保密意识。

#### 主机管理员

**主机管理员主要职责如下：**

* 负责保障主机（包括服务器设备、操作系统、数据库系统、数据备份）；
* 信息安全日常管理

包括系统口令管理、无人值守设备管理、屏幕保护、便携机管理等，促使每位人员的日常工作符合资鼎(上海)互联网金融信息服务有限公司的“马上货”系统 的信息安全策略和制度要求。负责主机运行维护体系和主机技术支持平台的建设与运行管理，建立服务器设备、操作系统、数据库系统、数据备份文档化的操作和维护规程，使得各个相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性。

* 重要信息和信息系统备份

定期进行重要信息和信息系统备份，并对备份介质进行安全地保存，以及对备份数据定期进行备份测试验证，保证各种备份信息的保密性、完整性和可用性，确保所有重要信息系统和重要数据在故障、灾难后及其它特定要求下进行可靠的恢复。

* 负责统一部署防病毒软件，并每周更新病毒库；
* 负责全系统的计算机恶意代码防治和主机安全的管理工作，制定检查计划（包含在主机巡检工作中），督促检查工作；
* 负责重要信息系统的访问控制管理，对系统特殊权限和系统实用工具的使用进行严格的审批和监管；
* 负责组织实施主机各类事故（故障）的应急处理。

**主机管理员任职要求如下：**

1、一年以上相关工作经验。

2、了解熟悉服务器软件和运行系统(Apache、Windows /UNIX),和网络故障排除，熟悉了解安全措施，能主动学习和聆听良好的时间安排能力，出色的沟通能力以及客户服务能力，完美解决问题，灵活且可靠，以及独立工作能力。

3、具备保密意识

#### 网络管理员

**网络管理员主要职责如下：**

* 负责保障网络安全建设管理；
* 规范网络管理流程；
* 采用技术和管理两方面的控制措施，加强对应用系统的安全控制，提高网络的安全性和稳定性；
* 对重要网络设备应有文档化的操作和维护规程，使得维护人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性；
* 负责保障网络安全，协助安全管理员部署网络安全产品，确保网络安全；对网络设备设施运转情况进行定期巡检、维护、故障处理和变更管理；
* 在网络系统变更、重要操作、访问等的进行逐级审批，负责日常审批，重大变更需报到资鼎(上海)互联网金融信息服务有限公司领导小组进行核准和审批后，方可进行变更；
* 负责组织实施网络各类事故（故障）的应急处理。

**网络管理员任职要求如下：**

1、大专以上学历，计算机、通信等相关专业

2、二年以上网络管理员工作经验

3、熟悉常用服务器设备，具备故障诊断和处理能力

4、熟练掌握Windows 操作系统的管理、维护

5、了解主流厂商的设备和技术发展

6、具备保密意识

7、具备良好职业道德与工作态度，善于沟通

#### 应用管理员

**应用管理员主要职责如下：**

* 负责保障软件开发管理

在资鼎(上海)互联网金融信息服务有限公司的“马上货”系统系统立项和审批过程中，同步考虑信息安全需求和目标。应保证系统设计、开发过程的安全，重点加强对软件代码安全性的管理。属于外包软件开发的，应与服务提供商签署保密协议。系统开发完成后，应要求通过第三方安全机构对软件安全性的测评。

* 负责建立重要应用的文档化操作和维护规程（详见附10），使得各个相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性；
* 负责信息安全日常管理，包括应用系统口令管理、授权审批管理等，促使每位人员的日常工作符合资鼎(上海)互联网金融信息服务有限公司的“马上货”系统系统信息安全策略和制度要求。
* 在应用系统变更、重要操作、访问等的进行逐级审批，负责日常审批，重大变更需报到资鼎(上海)互联网金融信息服务有限公司领导小组进行核准和审批后，方可进行变更；
* 负责组织实施应用系统各类事故（故障）的应急处理。

**应用管理员任职要求如下：**

1、全日制大学本科及以上学历；

2、3年以上信息项目管理或软件开发及维护工作经验；

3、工作责任心强，有良好的团队合作精神，沟通表达能力、文字表达能力及组织、协调能力较强；

#### 安全管理员

**安全管理员主要职责如下：**

负责安全制度的贯彻执行；

* 负责制订信息系统安全规划，并在实施过程中逐步完善；
* 负责制定安全设备或系统的相关资产清单。内容包括资产名称、重要程度、所处位置等；
* 负责制定安全设备或系统的文档化的操作和维护规程，使得运维人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性；
* 负责对安全设备或系统运行维护管理，对安全设备或系统运转情况进行定期巡检、维护、故障处理和变更管理。负责组织实施安全设备或系统各类事故（故障）的应急处理；
* 每年进行风险评估，根据评估结果会同其他负责人进行风险处置；
* 负责协助领导安排安全培训，负责协助负责制定每年安全教育计划，加强信息系统的安全教育，通过各种方式进行宣传和培训，提高全系统安全防范意识；
* 负责制定安全检查计划包括检查职责、检查周期、检查范围、检查内容、检查报告的编制、检查整改、检查通报等内容。对信息系统安全检查并进行情况通报。对记录进行收集、整理、归档。(详见附11)
* 当出现安全事件时，负责对发生的安全事件及时上报，并配合相关的调查和纠正工作；
* 当信息系统运行发生重大问题时，协助相关部门正确判断原因，根据指令立即采取安全措施启动相关处理程序；
* 负责与外部安全机构的协调联系，在发生重大安全事件时以协调获取外部安全机构的支持；
* 负责对介质的管理，对介质的归档、查询和借用进行记录，对介质进行定期盘点并记录，对故障介质的进行送修和销毁并记录，对于保密性高的介质销毁需要申报领导批准，并进行记录。对介质物理传输的交接进行记录。
* 加强对信息系统外包业务与外包方的管理，在与信息系统外包方签署的服务协议中，对信息系统安全加以要求。通过审批、访问控制、监控、签署保密协议等措施，加强外部方访问“资鼎(上海)互联网金融信息服务有限公司的“马上货”系统系统”的管理，防止外部方危害信息系统安全。
* 重视对IT服务连续性的管理，建立对各类信息安全事件的预防、预警、响应、处置、恢复机制，并编写相应的应急预案；
* 在符合国家密码管理相关规定的条件下，合理使用密码技术和密码设备，严格密钥生成、分发、保存等方面的安全管理，保障密码技术使用的安全性。(密码变更记录表见附13)

**安全管理员任职要求如下：**

1、大专以上学历，计算机、通信等相关专业

2、二年以上网络管理员工作经验

3、熟悉常用服务器设备，具备故障诊断和处理能力

4、具备保密意识

5、具备良好职业道德与工作态度，善于沟通

#### 安全审计员

**安全审计员的主要职责：**

* 参与制定资鼎(上海)互联网金融信息服务有限公司规章制度和流程，规章制度和流程培训与宣传；
* 根据资鼎(上海)互联网金融信息服务有限公司的审计要求制定审计计划，定期或不定期的开展审计工作，撰写审计报告，开展风险评估，发现安全漏洞或隐患，提交处理报告和切合实际可操作的处理方案，指导实施；
* 负责机房安全审计，负责数据库服务器、数据备份与灾难恢复审计；
* 负责操作系统安全审计，关键系统的用户角色权限审计；（安全审计员安全审计工作报告每月）
* 负责日常信息安全规章制度和流程的执行审计，信息系统环境安全审计等；
* 对被审计部门提供咨询、建议、协调等服务和公司领导安排的相关工作；
* 负责对系统管理员、安全管理员的操作行为进行审计跟踪分析和监督检查，及时发现违规行为，每月向安全管理中心汇报工作情况；(详见附14)

**安全审计员任职要求如下：**

1、大专以上学历，计算机、通信等相关专业

2、二年以上安全管理员工作经验

3、熟悉常用服务器设备，具备故障诊断和处理能力

4、具备保密意识

5、具备良好职业道德与工作态度，善于沟通

#### 专家小组

**专家小组主要职责:**

* 专家应符合有关资历要求和知识要求，具有高度的事业心和责任心，认真履行检查职责；检查中坚持客观公正，实事求是，不走过场，不弄虚作假，不隐瞒真实情况。对检查结果和所提的意见和建议负责。
* 受资鼎(上海)互联网金融信息服务有限公司委托，定期对其生产作业场所进行安全检查。检查时做到全面细致，不留死角。确保经检查、整改和复查，安全制度、应急救援、消防设施、安全设施等重要设施，屏蔽机房等重要场所部位符合相关规范要求。
* 对安全检查中查出的问题和隐患应逐一向资鼎(上海)互联网金融信息服务有限公司交底，并提出整改意见和建议；对查出的重大事故隐患应及时通报资鼎(上海)互联网金融信息服务有限公司结束后，应如实记录检查情况，并在检查记录上签字。
* 针对资鼎(上海)互联网金融信息服务有限公司信息安全事故隐患，适时对整改情况进行复查，整改复查情况应如实记录并由资鼎(上海)互联网金融信息服务有限公司存档。

**专家小组任职要求：**

1、硕士以上学历；

2、了解并熟悉信息工程及相关领域知识；

2、熟悉相关法律法规及规范/标准；

3、了解ISO9001管理体系；

4、具备注册安全工程师、注册安全评价师、注册风险评价师等资质证书优先考虑；

5、熟悉国家及地方政府对环境、健康与安全方面的政策法规

6、具备良好的组织协调能力、沟通能力及团队协作能力；

7、良好的语言表达、交流能力。

8、具备保密意识

### 信息安全小组权限

* 系统管理员

系统管理员拥有最高的管理权限，包括更改系统和网络配置，新增用户。

* 网络管理员、主机管理员

网络和主机管理员的权限仅次于系统管理员，包括更改系统和网络配置，但无法新增用户。

* 安全管理员

安全管理员只拥有管理权，包括查看安全日志，安全设备配置的变更、备份、环境的安全等。

* 机房管理员

机房管理员只拥有对硬件设备的操作权，但无法对硬件配置进行任何更改，机房管理员登录硬件设备的帐号只有查看权。

* 安全审计员

安全管理员只拥有审计权，包括查看审计日志，审核审查系统和网络配置更改，审查各种数据库记录等。

### 信息安全管理人员

资鼎(上海)互联网金融信息服务有限公司设置有系统管理员、安全管理员和安全审计员、应用管理员、主机管理员、机房管理员，配备多名管理人员和技术人员承担信息系统日常运行维护和管理任务。资鼎(上海)互联网金融信息服务有限公司将部分工作委托给专业技术公司完成，并和公司签订保密协议。

资鼎(上海)互联网金融信息服务有限公司应用管理员、主机管理员、安全管理员、机房管理员、网络管理员以及安全审计员，承担信息系统日常运行维护和管理任务。(备份管理员操作变更 详见附12: 备份管理员操作变更申请单)

各机构人员情况如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **资鼎(上海)互联网金融信息服务有限公司信息安全领导小组** | | | |
| 角 色 | 职务 | 姓名 | 联系电话 |
| 组长 | VP | 姚力 | 13916347636 |
| 副组长 | CPO | 刘逸凡 | 17717393229 |
| **资鼎(上海)互联网金融信息服务有限公司信息安全小组** | | | |
| 主机管理员 | 技术经理 | 徐垚鑫 | 13262509737 |
| 机房管理员 | 运维工程师 | 吴姜为 | 17612124551 |
| 网络管理员 | 运维工程师 | 吴姜为 | 17612124551 |
| 应用管理员 | 开发经理 | 温健根 | 15921587198 |
| **资鼎(上海)互联网金融信息服务有限公司信息安全后备小组** | | | |
| 备份系统/主机管理员 |  |  |  |
| 备份机房管理员 |  |  |  |
| 备份网络管理员 |  |  |  |
| 备份应用管理员 |  |  |  |

| **资鼎(上海)互联网金融信息服务有限公司信息小组信息化三员** | | | |
| --- | --- | --- | --- |
| 角 色 | 职务 | 姓名 | 联系电话 |
| 系统管理员 | 开发经理 | 温健根 | 15921587198 |
| 安全管理员 | 技术经理 | 徐垚鑫 | 13262509737 |
| 安全审计员 | CPO | 刘逸凡 | 17717393229 |

### 关键岗位协议

涉及到核心系统、数据库的管理人员为关键岗位管理人员，如主机，安全管理人员需要明确其职责，并需要签订岗位职责协议书，在岗人员只能从事协议书内相关的工作，不能有越权行为。

**资鼎(上海)互联网金融信息服务有限公司系统管理员岗位协议书**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名字 |  | | 部门 |  |
| 职责范围：   1. 负责保障主机（包括服务器设备、操作系统、数据库系统、数据备份）； 2. 信息安全日常管理   包括系统口令管理、无人值守设备管理、屏幕保护、便携机管理等，促使每位人员的日常工作符合资鼎(上海)互联网金融信息服务有限公司的“马上货”系统 的信息安全策略和制度要求。   1. 负责主机运行维护体系和主机技术支持平台的建设与运行管理   建立服务器设备、操作系统、数据库系统、数据备份文档化的操作和维护规程，使得各个相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性。   1. 重要信息和信息系统备份   定期进行重要信息和信息系统备份，并对备份介质进行安全地保存，以及对备份数据定期进行备份测试验证，保证各种备份信息的保密性、完整性和可用性，确保所有重要信息系统和重要数据在故障、灾难后及其它特定要求下进行可靠的恢复。   1. 负责统一部署防病毒软件，并定期更新病毒库； 2. 负责全系统的计算机恶意代码防治和主机安全的管理工作，制定检查计划（包含在主机巡检工作中），督促检查工作； 3. 负责重要信息系统的访问控制管理，对系统特殊权限和系统实用工具的使用进行严格的审批和监管； 4. 负责组织实施主机各类事故（故障）的应急处理。 5. 严格遵守保密协议。 | | | | |
| 签字确认： | |  | | \_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日 |
| 备注：资鼎(上海)互联网金融信息服务有限公司永久存档 | | | | |

**资鼎(上海)互联网金融信息服务有限公司安全管理员岗位协议书**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名字 |  | | 部门 |  |
| 职责范围：   1. 负责我局安全制度的贯彻执行； 2. 负责制订信息系统安全规划，并在实施过程中逐步完善； 3. 负责制定我局安全设备或系统的相关资产清单。内容包括资产管理的责任部门、资产名称、重要程度、所处位置等； 4. 负责制定安全设备或系统的文档化的操作和维护规程，使得相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性； 5. 负责我局安全设备或系统运行维护管理，对安全设备或系统运转情况进行定期巡检、维护、故障处理和变更管理。负责组织实施安全设备或系统各类事故（故障）的应急处理； 6. 每年进行风险评估，根据评估结果会同其他负责人进行风险处置； 7. 负责协助领导安排安全培训，负责协助负责制定每年安全教育计划，加强信息系统的安全教育，通过各种方式进行宣传和培训，提高全系统安全防范意识； 8. 负责制定安全检查计划   包括检查职责、检查周期、检查范围、检查内容、检查报告的编制、检查整改、检查通报等内容。对信息系统安全检查并进行情况通报。对记录进行收集、整理、归档。   1. 当出现安全事件时，负责对发生的安全事件及时上报，并配合相关的调查和纠正工作； 2. 当信息系统运行发生重大问题时，协助相关部门正确判断原因，根据指令立即采取安全措施启动相关处理程序； 3. 负责与外部安全机构的协调联系，在发生重大安全事件时以协调获取外部安全机构的支持； 4. 负责对介质的管理   对介质的归档、查询和借用进行记录，对介质进行定期盘点并记录，对故障介质的进行送修和销毁并记录，对于保密性高的介质销毁需要申报领导批准，并进行记录。对介质物理传输的交接进行记录。   1. 加强对信息系统外包业务与外包方的管理   在与信息系统外包方签署的服务协议中，对信息系统安全加以要求。通过审批、访问控制、监控、签署保密协议等措施，加强外部方访问“健康档案”的管理，防止外部方危害信息系统安全。   1. 重视对IT服务连续性的管理，建立对各类信息安全事件的预防、预警、响应、处置、恢复机制，并编写相应的应急预案； 2. 在符合国家密码管理相关规定的条件下，合理使用密码技术和密码设备，严格密钥生成、分发、保存等方面的安全管理，保障密码技术使用的安全性。 3. 严格遵守保密协议。 | | | | |
| 签字确认： | |  | | \_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日 |
| 备注：资鼎(上海)互联网金融信息服务有限公司永久存档 | | | | |

**资鼎(上海)互联网金融信息服务有限公司安全审计员岗位协议**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名字 |  | | 部门 |  |
| 职责范围：   1. 参与制定我局规章制度和流程，规章制度和流程培训与宣传； 2. 根据我局的审计要求制定审计计划，定期或不定期的开展审计工作，撰写审计报告，开展风险评估，发现安全漏洞或隐患，提交处理报告和切合实际可操作的处理方案，指导实施； 3. 负责我局机房安全审计，负责数据库服务器、数据备份与灾难恢复审计； 4. 负责我局操作系统安全审计，关键系统的用户角色权限审计； 5. 负责我局日常信息安全规章制度和流程的执行审计，信息系统环境安全审计等； 6. 对被审计部门提供咨询、建议、协调等服务和公司领导安排的相关工作； 7. 负责对系统管理员、安全管理员的操作行为进行审计跟踪分析和监督检查，及时发现违规行为，每月向信息安全中心汇报工作情况；   8、严格遵守保密协议。 | | | | |
| 签字确认： | |  | | \_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日 |
| 备注：资鼎(上海)互联网金融信息服务有限公司永久存档 | | | | |

# 信息安全授权及审批管理制度

## 信息安全授权及审批管理制度

在系统运维过程中，对信息系统的访问、变更等授权给资鼎(上海)互联网金融信息服务有限公司的“马上货”系统运维管理人员。具体为机房管理员负责机房相关事务的授权和审批；网络管理员负责网络相关事务的授权和审批；主机管理员负责主机相关事务的授权和审批；应用系统管理员负责应用相关事务的授权和审批。

授权审批流程如下：

* 由相关信息安全组长判断职责、并授权给相应的管理人员；
* 由外包服务公司申请，相应的管理员进行授权、审批（见附15）；
* 填写授权审批表（见附16）；
* 组织资鼎(上海)互联网金融信息服务有限公司人员每季度审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息，保存审批文档。

需授权的审批事项如下：

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |

# 审核与检查管理制度

## 审核与检查管理制度

### 定期安全检查

* 由安全领导小组组织专门人员每三个月进行安全检查；
* 对包括网络、安全设备、系统、文档等各方面的安全检查；

检查完毕后提交检查报告，并由资鼎(上海)互联网金融信息服务有限公司安全管理员进行检查报告复核，确定安全检查结果，并对于不符合要求的地方提出整改措施并规定整改期限，以电子邮件或书面形式通知被检查人员；（详见附17）

检查时针对上一次的检查结果进行复查，若发现仍未整改的，需上报信息安全领导小组并进行书面通告。（详见附18）

安全检查流程



### 文件审批与发布管理制度

安全管理员根据ISO/IEC 27001：2005《信息安全管理体系要求》，结合部门职责及信息安全管理流程，负责组织编制信息安全管理体系文件，形成初稿；

* 安全管理员负责组织对信息安全管理体系文件的评审，并将审核后的文件报资鼎(上海)互联网金融信息服务有限公司，由信息安全领导小组领导对信息安全管理体系文件进行核准，形成最终的报审稿；
* 安全管理员负责对信息安全管理体系文件的报审稿进行登记、核稿后，报送领导审阅、签批；
* 组织相关人员进行评审，领导审阅、签批后发布；
* 信息安全管理体系文件由安全管理员发放到各负责人，由各负责人按规定的发放范围发至相关职属范围人员，由安全管理员按规定的发放范围发至相关各部门，程序文件、信息安全管理手册封面加盖“受控”章进行标识，统一编号；
* 岗位人员变动时，由文件主管部门及时收回原岗位各类文件，发放现岗位工作所依据的文件，以保证信息安全管理体系的有效运行；
* 岗位人员调离或退休时，应先向资鼎(上海)互联网金融信息服务有限公司交回其所领用的文件后，方可办理有关手续；
* 信息安全管理手册和程序文件制发后，需保留1份，连同签批原件和电子版一并归安全管理员存档；
* 文件更换新版后，由安全管理员收回作废的文件，并做好回收记录；
* 由安全管理员定期检查文件的适用情况，并对现有文件的有效性进行评审。对不合适的地方进行修订，必要时更换新版；
* 外来文件由相应的责任部门负责接收和管理。

# 办公环境管理制度

## 办公环境管理制度

* + 1. **总体要求：**
  1. 各类物品摆放整齐、有序，功能布局清晰。
  2. 所有区域应保持清洁卫生。
  3. 标识统一规范，不随意张贴。
  4. 员工应严格遵行《岗位行为规范》要求。
  5. 爱护公共设备设施；
  6. 遵循ISO环境管理体系要求。
  7. 工作人员调离办公室应立即交还该办公室钥匙
  8. 不在办公区接待来访人员等
     1. **个人办公区域标准**

1. 办公桌椅排放整齐，椅子不得放在走道内阻碍通行；
2. 桌面上允许摆放的物品包括：电脑、茶杯、常用办公用品、小饰物（1－2件）及1个月内常用资料和工作文件。
3. 台式电脑放置于两条桌边垂直角上，立式主机放置于桌底下；
4. 文件资料摆放在办公桌侧边处；
5. 常用办公用品、茶杯、小饰物放置在正前方区域；
6. 1个月以上不常用物品应整理放置于橱柜内；
7. 不乱贴乱钉与工作无关的物品，隔断类办公桌区域内粘贴纸张不得超过隔断上边缘；
8. 抽屉内物品摆放整齐有序，常用物品随手可取；
9. 与工作无关的物品须整齐存放于隐蔽地方；
10. 每日下班离岗前须整理桌面物品、文件资料，恢复标准放置状态；
11. 办公文件资料须分门别类整理、有标识的存放，便于查找和取拿；
12. 保持个人区域范围内的清洁，；
13. 电器线路整齐束扎，下班、双休、长假期关闭拖线板总电源；
14. 爱护公物，做好贵重物品的妥善保管和看护；
    * 1. **公共区域环境标准**
15. 办公桌椅、文件柜、储物柜、办公设备、绿化摆放整齐、布局清晰有序，顶部角落无杂物堆放；
16. 地面、柜面、桌面、公共设备表面清洁无灰尘；
17. 文件柜内文件资料和各类物品分类摆放，有标识；
18. 在指定区域内张贴。
    * 1. **办公行为**
19. 上班着装整洁得体。
20. 工作时间不做与工作无关的事；
21. 公共办公区域内禁止吸烟；
22. 保持防火、防盗安全意识；
23. 遵守环境体系要求，节约能源纸张，垃圾分类投放。
24. 离开办公室应注意关闭电脑、电灯、空调、饮水机、打印机、复印机等设备设施电源，并检查门窗是否关闭上锁。
25. 爱护公用设备设施，按规定正确使用。
    * 1. **办公设备管理**
26. 办公设备属公司国家财产，主要包括办公桌椅、电脑及电脑的各种组件、电脑软件、网络设备、打印机、复印机、扫描仪、存储柜等；
27. 办公设备分配到个人后，使用人须自觉妥善放置和保管，并爱护使用；
28. 爱护公共设备设施，不浪费或故意损坏；
29. 使用人未能合理使用而造成设备损坏的则需照价赔偿；
30. 借用公用办公设备须及时归还，如有丢失或损坏，由借用人负责照价赔偿。
31. 未经允许，不得随意挪用他人或公用办公设备；
32. 设备使用人须配合办公设备管理员的工作；

# 沟通与合作管理制度

## 沟通与合作管理制度

### 信息安全例会管理

(一) 中层信息安全例会由信息安全工作小组负责发起，至少每月需要组织一次常规的信息安全例会，例会参会人员至少要包括信息安全工作小组主要成员和执行层各角色的管理人员。在发生小范围内信息安全事件时如需要，信息安全工作小组可随时召集发起信息安全工作会议，通知相关人员参加，就信息安全管理各项制度和执行情况做出及时调整和部署。

(二) 常规的中层信息安全例会的主要内容是就各阶段的信息安全检查结果进行上会检查和审批，对信息安全检查中发现的各项问题提出解决办法和规避措施，对外包运维人员的工作内容进行确认和审核，就发现的各类信息安全问题及时提出解决方案并落实到相关责任人。

(三) 遇有工程或项目时，可根据工程和项目进度情况或者工程和项目的需要随时召开信息安全例会，且可不拘泥于信息安全工作小组范围，可召集相关的合作单位、合作方、内部相关部门的相关人员一起参加信息安全例会，并由研发部做好例会的记录工作。

(四) 高层信息安全例会由信息安全领导小组负责发起，至少每季度需要组织一次常规的高层信息安全例会，例会参会人员包括信息安全领导小组主要成员。在发生大范围的信息安全事件、有重大信息安全事件发生、或者有重大信息系统建设项目时，如有必要，由信息安全领导小组发起，或者由信息安全工作小组提议，由信息安全领导小组发起高层信息安全领导小组会议，通知相关人员参加，及时协调各方资源，共同协作，解决相关问题，或完成各项部署。

(五) 常规的高层信息安全例会的主要内容是听取信息安全工作小组的信息安全工作季度报告，就信息安全各项工作根据报告提出调整和解决方案，并协调各方资源，共同协作，完成各项信息安全工作。高层信息安全例会的另一重要内容是就信息安全管理体系的各项管理制度，根据运行中发现的问题，及时进行调整和部署，不断完善信息安全管理体系。

### 外部协作管理

(一)由信息安全工作小组负责建立并保持与兄弟单位的合作与沟通，就兄弟单位的成熟经验、政策法规、当前的信息热点事件展开交流与合作。如交流与合作内容比较正式，且有正式的会议形式，则需要由研发部做好会议记录工作，会议记录的模板可用信息安全例会的模板代替，但会议主题需注明为“合作沟通”。

(二)由信息安全工作小组负责建立并加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通，就最新信息安全技术、信息热点事件等进行交流和咨询（详见附19）。如交流与合作内容比较正式，且有正式的会议形式，则需要由研发部做好会议记录工作（详见附20），会议记录的模板可用信息安全例会的模板代替，但会议主题需注明为“合作沟通”。

# 人员入岗管理制度

## 信息安全条款

信息安全相关条款包括以下方面：

* 岗位相关的法律职责和权利；
* 信息系统相关资产的管理职责；
* 操作其他组织和机构信息的职责；
* 保护个人信息方面的安全职责，包括对个人隐私保密，不滥用个人信息等；
* 在办公区域外和正常工作时间之外的职责；
* 信息安全违规将受到的惩戒措施。

## 保密协议

根据岗位安全职责，对重要岗位制定相应的保密协议。保密协议包括以下方面的内容(详见附22)：

* 岗位所要保护的信息；
* 协议有效期；
* 协议终止时所应采取的措施；
* 为避免泄密，签字人的职责和行为；
* 保密协议与知识产权保护、商业秘密保护的关系；
* 协议终止时信息的归档或销毁的措施；
* 违反协议后应采取的措施。

## 人员录用和上岗安全管理

* 指定或授权专门的部门或人员负责人员录用，每位入岗人员都必须如实填写个人相关情况（见附23）；
* 严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行审核（见附24）；
* 岗位人员在任用之前应签署保密协议（见附22）；
* 从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议；（见附25）
* 各单位（部门）应通过教育和培训活动，确保本单位（部门）员工、外来人员在上岗前，理解其岗位信息安全角色和职责；
* 各单位（部门）应确保在针对本单位员工的岗前培训中，包括信息安全管理体系和相关管理制度、岗位信息安全职责等信息安全相关的内容。

# 人员在岗管理制度

## 人员在岗信息安全管理

### 岗位信息安全检查

* 资鼎(上海)互联网金融信息服务有限公司全体成员应提高安全意识，定期对本部门岗位进行信息安全检查，确保信息安全规定得到了有效地执行；
* 资鼎(上海)互联网金融信息服务有限公司的“马上货”系统安全小组不定期抽查各部门的岗位信息安全职责的落实情况，确保各部门的岗位信息安全职责的落实。

### 信息安全违规纪律处理

* 对于信息安全事故和在信息安全检查中发现的违规行为，由根据有关考核规定对该人员进行处罚；
* 对于情节特别严重的违规行为，需向全体人员进行通报和宣传，避免同类问题再次发生。

## 人员考核

* 定期对各个岗位的人员进行安全技能及安全认知的考核；（详见附26）
* 对关键岗位的人员进行全面、严格的安全审查和技能考核；
* 对考核结果进行记录和保存（详见附27）。
* 对于考核不合格人员进行补充安全教育，如超过两次不合格者将采用一定程度处罚措施，情节严重者将严肃处理。

## 关键岗位考核制度

* 关键岗位需要由研发部领导直接考核；
* 对关键岗位人员需要从政治面貌，工作态度，业务能力等方面入手进行考核与审查，每年度一次（附28）；
* 关键岗位业务能力的考核根据岗位要求每年度有所变动，但基本安全要求不变，都需要通过人员考核中相关考核内容；

# 信息安全培训制度

## 信息安全培训制度

* 对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训（附29）；
* 对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；
* 对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训；
* 对于定期举办的信息安全培训资鼎(上海)互联网金融信息服务有限公司相关员工都必须参加，每位培训人员都必须填写培训签到表格予以确认（见附30）；
* 对安全教育和培训的情况和结果进行记录并归档保存（见附31）；
* 培训手段多样化，包括讲座、观看影视资料、学习信息安全材料等。不断的提高信息安全防范意识；
* 年初由组织统一制定全年的安全意识教育和培训计划；统一发布至各部门，并在组织年内具体落实；（见附32）
* 每半年举行一次信息安全培训，培训对象包括资鼎(上海)互联网金融信息服务有限公司所有员工；
* 培训内容包括信息安全基础、信息安全岗位操作流程等；对于新录用的员工，需要单独进行安全培训；
* 培训手段多样化，包括讲座、观看影视资料、学习信息安全材料等。不断的提高信息安全防范意识；
* 培训结束后，需要每个参与人员填写信息安全培训结果反馈和心得体会，并统一归档保存。并对培训内容进行考核（见附33）并记录（见附34）；

# 人员离岗管理制度

## 人员离岗离职安全管理

离职人员应当提出辞职书面申请，并填写《人员离岗/职审批表》（见附36）一式二份，经其所在部门、信息安全小组逐级审核通过方可办理离职手续。

明确人员离职和转岗时的手续，明确离职和转岗管理职责。职责一般包括：

* 归还资产方面各相关单位（部门）的职责；
* 撤销访问权方面各相关单位（部门）的职责；
* 岗位人员变动方面各相关单位（部门）的职责；
* 离开岗位后还应承担的责任，如保密限制等。

### 资产归还

* 离岗人员在离岗时归还其使用的资产，包括所有先前发放的软件、访问卡、文件和设备等。相关单位（部门）应与离岗人员进行离岗交接，并做好记录（见附36）；

离岗人员应就其涉及到的专利、技术文档等及时向所在单位（部门）上交；

* 人员在离岗时，应对正在实施的项目中的相关信息形成文档并提交给相关单位（部门），进行项目交接。

### 访问权限回收

* 各单位（部门）在人员任用终止时，应按照离岗手续，通知相关单位（部门）对该人员使用信息和信息系统的权限进行调整；

信息安全中心依照相关人员的个人权限清单和业务部门授权文件的要求，修改、限制或删除相关信息和信息系统的访问权限，包括物理访问、逻辑访问、密钥及ID卡等，并作相应记录；

信息安全中心应立即撤销或停用离岗人员所使用的账户，或者修改离岗人员所掌握的系统帐户口令。

### 离职后信息安全职责的追踪和管理

离职人员应明确其离职后仍需担负的安全责任和义务，以及违反安全责任和义务所引发的后果；

* 如发生有离职人员违反其应负的安全责任，按照有关规定和离职保密承诺书（见附37）追究其法律责任；

# 外来人员管理制度

## 第三方人员安全管理

第三方人员主要为与我委有业务往来的外单位人员，如项目相关单位、服务商单位等相关人员。

* 第三方在访问前需签订责任书或保密协议；
* 第三方进出机房等重要区域前需提交申请，并提交安全管理员签字确认；审批通过后需登记进出时间，事件内容等信息，并注明陪同人员（见附38）；
* 第三方人员进入机房作业时，需由机房管理员全程陪同，不得允许第三方人员单独在机房内作业；
* 对于需要登录主机或网络设备时，第三方人员需提交给主机管理员或网络管理员操作指南，经主机或网络管理员确认并提交安全管理员审批后，由主机管理员或网络管理员代为操作；
* 不得允许第三方人员独自改动主机或网络配置；对于需要变更的操作，需先向安全管理员提出申请并审批通过后方可进行；
* 对于第三方携带的移动存储设备如移动硬盘、U盘等，未经病毒扫描不得直接插在主机上；确有需要的，由主机管理员确认后代为操作。

## 外来人员信息安全管理

* 外来人员来本单位访问、参观时，应对其进行信息安全意识教育，确保其理解和遵守访问、参观时应注意的信息安全规定；
* 外来人员访问受控区域时应提交书面申请，并在批准后由机房管理员陪同并登记备案；（见附39）
* 各单位（部门）应要求外部方根据制度要求，对其人员进行安全职责的宣传和教育，确保外来人员理解其应担负的安全责任和义务；
* 各单位（部门）应按照有关信息安全管理规定以及制度要求，对所有外来人员进行监督和检查，并就安全违规情况按管理制度条款中的要求进行处理；

# 工作人员安全守则

## 工作人员安全守则

* 保护信息资产的安全是每位工作人员的责任。每个工作人员必须认识到信息资产的价值，负责保管好自己所辖的涉及资鼎(上海)互联网金融信息服务有限公司的数据和信息；
* 每个工作人员必须遵守资鼎(上海)互联网金融信息服务有限公司信息保密策略规定，了解信息的重要度级别。对于不能确定是否为涉密信息或重要信息的，在对外披露时，必须征得安全责任人的同意；
* 工作人员必须遵守资鼎(上海)互联网金融信息服务有限公司制定并下发的安全保密管理体系；
* 工作人员必须了解安全事件处理流程，并能遵守和使用；
* 研发部有权对工作人员的计算机设备定期审查；
* 工作人员登录或使用资鼎(上海)互联网金融信息服务有限公司核心网络和系统的所有操作，都将被记录形成日志备查；
* 对于自己的计算机必须设置开机口令（所有计算机在使用之前必须修改由厂商所设置的原始口令）；若怀疑口令泄露或经过厂商维修后必须修改口令；
* 当离开计算机时，必须激活带口令的屏幕保护程序，或将系统锁定，或返回登录状态，或关机；
* 设置的任何口令，必须是字母、数字和符号组合，且不少于8位。必须不易被猜测（不得是自己的生日、电话号码、姓名的拼音等），口令每三个月更改一次，必须牢记自己的口令；
* 必须使计算机设备与食物、饮料、水、磁性物质等保持一定距离，防止计算机设备遭受污染和损坏；
* 对手提计算机、软盘、移动硬盘、闪存等便携设备，必须及时清理锁入柜中，防止被盗；
* 必须确保所有个人重要数据（如电子邮件、个人文档等）及时备份，并将备份数据保存在安全地点；
* 计算机必须安装统一的防病毒软件，并由防病毒服务器统一管理，不得安装非信息安全中心指定的防病毒软件或其它安全软件；
* 外来存储介质在使用之前、电子邮件等在打开之前必须先查杀病毒；
* 当认为自己的计算机可能已感染病毒时，必须立即报告信息安全中心部门处理；
* 软盘、光盘、闪存、磁带等存储介质上的数据不再需要时，必须及时对数据予以清除；
* 当用户的计算机出现故障，在维修人员到场维修时，必须现场监督维修人员无拷贝数据或打开文件的行为，需要送外维修时应当确保所有重要信息已经备份并在计算机上已经物理删除；
* 当非本单位人员到本部门办公区时，员工必须询问来访目的，不允许非本单位人员无故逗留；
* 员工必须对自己使用的电子邮件系统、办公系统以及其他应用系统的帐号、口令及进行的一切活动和事件负全部责任；
* 转发涉及资鼎(上海)互联网金融信息服务有限公司信息的电子邮件到外部地址必须事先经过信息拥有人同意或有关部门的授权；
* 用户若发现任何非法使用本人帐号以及其他威胁信息系统安全的情况，必须立即报告信息安全管理部门；
* 用户必须经常对电子邮件进行备份，把电子邮件中的重要信息导入文字处理文档、数据库或其它文件中，防止被用户本人错误删除或当系统发生问题时丢失。同时，电子邮件系统不是被用来存储重要信息的，管理员保留对电子邮件服务器中储存的信息定期维护的权利；
* 对涉及重要信息的电子文件，应当设置口令；
* 不得共享或透露个人用户名和口令，不得将内部用户名和口令借与外单位人员登录资鼎(上海)互联网金融信息服务有限公司应用系统；
* 不得传播任何非法的、骚扰性的、中伤他人的、辱骂性的、恐吓性的、伤害性的、淫秽的等信息数据；
* 不准传播任何教唆他人构成犯罪行为的信息数据；
* 不得传输助长国家不利因素、涉及国家安全，以及任何不符合国家法律、法规、规章的信息数据；
* 未经许可不得非法进入其他的邮件系统；
* 不得盗用他人的邮件帐号；
* 不得随意在自己的计算机内设置共享目录，如确有必要，必须设置口令保护，并在共享完毕后立即取消共享功能；
* 工作人员不得随意安全软件，所有相关软件都必须由研发部人员安装，并由信息安全中心人员确认无安全危害；
* 非研发部人员不得随意拆卸计算机设备，更改计算机系统配置。
* 不得将有重要资料的软盘、光盘、磁带等存储介质随意存放或随意带出办公地点。
* 在使用应用系统时，必须遵守应用系统的权限管理，不得企图获取别人的口令或其它认证方式，不得攻击内部网络或企图侵入无权限的应用系统；
* 未经授权，不得向外部网络传输涉密信息及重要信息；

# 信息系统建设安全管理制度

## 安全设计需求分析及评估

### 应用系统基本安全需求

* 身份鉴别层面需求，包括但不限于以下方面：
* 身份鉴别信息是否具有不易被冒用的特点，例如复杂性（如规定字符应混有大、小写字母、数字和特殊字符）；
* 具有登录失败处理功能，如结束会话、限制非法登录次数，当登录连接超时，自动退出；
* 具有鉴别警示功能（如系统有三次登录失败则锁定该用户的限制，则应给用户必要的提示）；
* 具有抵抗渗透性测试的能力，如通过暴力破解或其他手段进入系统，或对WEB系统采用SQL注入等绕过身份鉴别的方法。
* 访问控制层面需求，包括但不限于以下方面：
* 系统应能够提供访问控制机制，实现依据安全策略控制用户对客体（如文件和数据库中的数据）的访问；
* 由授权主体设置对系统功能操作和对数据访问的权限；
* 应实现应用系统特权用户的权限分离（如将系统管理员、安全员和审计员的权限分离），权限之间确保相互制约（如系统管理员、安全管理员等不能对审计日志进行管理，安全审计员不能管理审计功能的开启、关闭、删除等重要事件的审计日志等）。
* 安全审计层面需求，包括但不限于以下方面：
* 安全审计应记录应用系统重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统功能的执行等；
* 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；
* 为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；
* 审计记录应受到保护避免受到未预期的删除、修改或覆盖等。
* 软件容错层面需求，包括但不限于以下方面：
* 对通过人机接口输入或通过通信接口输入的数据进行有效性检验；
* 对通过人机接口方式进行的操作提供“回退”功能，即允许按照操作的序列进行回退；
* 有状态监测能力，当故障发生时，能实时检测到故障状态并报警；
* 有自动保护能力，当故障发生时，自动保护当前所有状态。
* 资源控制层面需求，
* 应限制单个用户的多重并发会话；
* 应对应用系统的最大并发会话连接数进行限制；
* 应对一个时间段内可能的并发会话连接数进行限制；
* 应根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式。

### 硬件系统基本安全需求

* 物理威胁及需求，包括但不限于以下方面：
* 雷击、地震和台风等自然灾难，需要通过对物理位置进行选择、建立数据备份和恢复系统、实行备份与恢复管理，以及采取防雷击措施等来解决雷击、地震和台风等威胁带来的问题；
* 水患和火灾等灾害，需要采取防水、防潮、防火措施、建立数据备份和恢复系统、实行备份与恢复管理，来解决水患和火灾等威胁带来的安全威胁；
* 高温、低温、多雨等原因引起温度、湿度异常，应该采取温湿度控制措施，同时，建立数据备份和恢复系统、实行备份与恢复管理来解决因高温、低温和多雨带来的安全威胁；
* 电压波动，需要合理设计电力供应系统，同时，建立数据备份和恢复系统、实行备份与恢复管理来解决因电压波动带来的安全威胁；
* 供电系统故障，需要合理设计电力供应系统，如：购买UPS系统或者建立发电机机房来保障电力的供应，同时，建立数据备份和恢复系统、实行备份与恢复管理来解决因供电系统故障带来的安全威胁；
* 静电、设备寄生耦合干扰和外界电磁干扰，需要采取防静电和电磁防护措施来解决静电、设备寄生耦合干扰和外界电磁干扰带来的安全威胁；
* 强电磁场、强震动源、强噪声源等污染，需要通过对物理位置的选择、采取适当的电磁防护措施，同时，建立数据备份和恢复系统、实行备份与恢复管理来解决强电磁场、强震动源、强噪声源等污染带来的安全隐患；
* 线路老化等原因导致通信线路损坏或传输质量下降，需要通过采取对网络进行安全管理，对网络通信线路的传输能力进行必要的监控，以及建立数据备份和恢复系统、实行备份与恢复管理来解决因线路老化等原因导致通信线路损坏或传输质量下降带来的安全问题；
* 存储介质使用时间过长或质量问题等导致不可用，需要通过对存储介质存放的环境进行管理，对介质和设备进行管理，检查通信的完整性和数据的完整性，建立数据备份和恢复系统、实行备份与恢复管理来解决存储介质使用时间过长或质量问题等导致不可用带来的安全问题；
* 网络设备、系统设备及其他设备使用时间过长或质量问题等导致硬件故障，需要通过对产品采购、自行软件开发、外包软件和测试验收进行管理，网络设备、系统设备存放的环境进行管理，对存储介质进行管理，对网络和系统设备以及其他设备进行管理，建立一套监控管理体系，建立数据备份和恢复系统、实行备份与恢复管理，通过上述措施来解决网络设备、系统设备及其他设备使用时间过长或质量问题等导致硬件故障带来的安全问题；
* 攻击者利用非法手段进入机房内部盗窃、破坏等，需要通过进行环境管理、采取物理访问控制策略、实施防盗窃和防破坏等控制措施，建立数据备份和恢复系统、实行备份与恢复管理来解决非法手段进入机房内部盗窃、破坏等带来的安全问题；
* 攻击者采用在通信线缆上搭接或切断等导致线路不可用，需要通过采取物理访问控制策略、实施防盗窃和防破坏等控制措施，建立数据备份和恢复系统、实行备份与恢复管理来解决在通信线缆上搭接或切断等导致线路不可用带来的安全问题；
* 攻击者利用工具捕捉电磁泄漏的信号，导致信息泄露，需要通过采取防电磁措施，加强对产品采购的管理，加强对密码的管理，加强通信的保密性和数据的保密性，来解决电磁、信息泄漏带来的安全问题。
* 攻击者非法物理访问系统设备、网络设备或存储介质等，需要通过数据保密、通信保密性、防盗窃和防破坏、物理访问控制、产品采购、密码管理等技术手段完成。
* 网络威胁及需求，包括但不限于以下方面：
* 内部人员未授权接入外部网络，需要通过边界的完整性检查、网络审计、主机审计、应用审计等手段解决；
* 网络设计不合理，需要通过优化设计、安全域改造完成；
* 设施、通信线路、设备或存储介质因使用、维护或保养不当等原因导致故障，需要通过线路状态检测、线路冗余、数据备份与恢复等技术手段解决；
* 攻击者利用分布式拒绝服务攻击等拒绝服务攻击工具，恶意地消耗网络、操作系统和应用系统资源，导致拒绝服务，需要通过主机资源优化、网络入侵检测与防范、网络结构调整与优化等技术手段解决；
* 攻击者利用网络协议、操作系统、应用系统漏洞，越权访问文件、数据或其他资源，需要通过恶意代码防护、控制台审计、漏洞扫描、访问控制、身份鉴别、GB17859二级以上操作系统、网络和主机审计系统等技术手段解决；
* 攻击者利用网络协议存在的漏洞进行可躲避检测的攻击（如碎片重组，协议端口重定位等），需通过网络入侵检测、防病毒系统、控制台审计、访问控制等技术手段解决；
* 攻击者利用网络结构设计缺陷旁路安全策略，未授权访问网络，需通过网络入侵检测、访问控制、身份鉴别、网络结构优化和调整等技术手段解决；
* 攻击者利用通用安全协议/算法/软件等缺陷，获取信息、解密密钥或破坏通信完整性，需要通过控制台审计、恶意代码防范、国密办认证的算法及协议产品；
* 攻击者盗用授权用户的会话连接，需通过身份鉴别、访问控制、通信加密等技术手段解决。
* 系统威胁及需求，包括但不限于以下方面：
* 攻击者在软硬件分发环节（生产、运输等）中恶意更改软硬件，需通过恶意代码方法、控制台审计等技术手段解决；
* 攻击者利用网络扩散病毒，需通过恶意代码方法、控制台审计等技术手段解决；
* 内部人员下载、拷贝软件或文件，打开可疑邮件时引入病毒。需通过恶意代码防范技术手段解决；
* 授权用户对系统错误配置或更改。需通过安全审计、数据备份和恢复等技术手段解决；
* 由于授权用户的不正确启动和恢复导致安全机制失效，需通过系统加固、安全审计、软件容错、备份与恢复等技术手段解决；
* 攻击者利用通过恶意代码或木马程序，对网络、操作系统或应用系统进行攻击，需通过恶意代码防护、网络入侵检测、身份鉴别、访问控制、控制台审计等技术手段解决。
* 应用威胁及需求，包括但不限于以下方面：
* 攻击者否认自己的操作行为，需要采取抗抵赖性措施，以及通过加强网络安全审计以及软件应用系统的自身的安全审计来解决抵赖行为带来的安全问题；
* 系统软件、应用软件运行故障，需要通过对产品采购、自行软件开发、外包软件和测试验收进行管理，系统软件和应用软件应具备容错能力，对系统和软件进行保护，并对系统软件和应用软件监控管理，对入侵系统和软件的行为进行监测和报警，此外，建立数据备份和恢复系统、实行备份与恢复管理等措施，来解决此类安全问题；
* 系统软件、应用软件过度使用内存、CPU等系统资源，需要对系统软件和应用软件进行入侵行为的防范，并进行实时的监控管理，同时，对系统使用的资源进行管理控制来解决过度使用带来的安全问题；
* 应用软件、系统软件缺陷导致数据丢失或运行中断，需要通过对产品采购进行管理、加强自软件开发管理、加强外包软件开发管理、加强代码安全管理，加强通信完整性和数据完整性，以及建立数据备份和恢复系统、实行备份与恢复管理等措施来解决应用软件、系统软件缺陷导致数据丢失或运行中断带来的安全问题；
* 攻击者利用应用系统、操作系统中的后门程序攻击系统，需要加强产品采购管理、加强软件外包开发的管理、对软件进行充分的测试和验收管理、对恶意代码采取有效的防范措施，对网络设备进行防护、对访问网络的用户进行访问控制、对访问网络的用户身份进行鉴别、对系统或应用实行自主访问控制和强制的访问控制来加强访问控制措施，采取措施对入侵行为进行监测和防范，通过采取上述措施来解决应用系统和操作系统中的后门程序带来的安全隐患；
* 攻击者利用各种工具获取身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问网络、系统，或非法使用应用软件、文件和数据，需要加强产品采购管理、加强密码管理、保证数据传输的通信的保密性和数据的保密性、对网络设备进行防护、对拨号访问用户进行控制、对访问网络的用户进行访问控制、对访问网络的用户身份进行鉴别、对系统或应用实行自主访问控制和强制的访问控制来加强访问控制措施，通过采取上述措施来解决攻击者利用工具分析和解剖信息带来的安全问题；
* 攻击者利用非法手段获得授权用户的鉴别信息或密码介质，访问网络、系统，或使用应用软件、文件和数据，需要加强密码管理、保证数据传输的保密性、对网络设备进行防护、对拨号访问用户进行控制、对访问网络的用户进行访问控制、对访问网络的用户身份进行鉴别、对系统或应用实行自主访问控制和强制的访问控制来加强访问控制措施，同时，加强员工安全意识的教育和培训，加强系统的安全管理，来解决攻击者带来的安全问题；
* 攻击者利用伪造客户端进入系统，进行非法访问，需要对网络设备进行防护、对拨号访问用户进行控制、对访问网络的用户进行访问控制、对访问网络的用户身份进行鉴别、对系统或应用实行自主访问控制和强制的访问控制来加强访问控制措施，来解决攻击者伪造客户端带来的安全问题；
* 攻击者提供伪造的应用系统服务进行信息的窃取，需要加强网络边界完整性检查，加强对网络设备进行防护、对访问网络的用户身份进行鉴别，此外，加强数据保密性来解决攻击带来的安全问题。
* 数据威胁及需求，包括但不限于以下方面：
* 内部人员利用技术或管理漏洞，未授权修改重要系统数据或修改系统程序，需要通过网络安全审计、恶意代码防范、审核和检查、网络安全管理、系统安全管理、网络设备防护、网络访问控制、身份鉴别、自主访问控制、强制访问控制、拨号访问控制、通信完整性、数据完整性、入侵防范、应用系统身份鉴别等技术手段解决；
* 内部人员未授权访问敏感信息，将信息带出或通过网络传出，导致信息泄露，需要通过网络安全审计、网络设备防护、网络访问控制、身份鉴别、自主访问控制、强制访问控制、数据保密性、通信保密性、产品采购、密码管理、资产管理、介质管理等技术手段解决；
* 攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失，需要通过通信完整性、数据完整性、通信保密性、数据保密性、产品采购、密码管理、抗抵赖等技术手段解决；
* 通信过程中受到干扰等原因发生数据传输错误，需要通过通信完整性、数据完整性等技术手段解决；
* 授权用户操作失误导致系统文件被覆盖、数据丢失或不能使用，需要通过网络安全审计、软件容错、数据备份和恢复、备份与恢复管理、管理制度、人员录用、人员离岗、人员考核、第三方人员访问管理、安全意识教育和培训、外包软件开发、产品采购、监控管理等手段解决；
* 攻击者截获、读取、破解介质的信息或剩余信息，进行信息的窃取，需要通过通信保密性、数据保密性、剩余信息保护、介质管理、产品采购、密码管理、网络访问控制、拨号访问控制、自主访问控制、强制访问控制等安全措施；
* 攻击者截获、读取、破解通信线路中的信息，需要通过通信保密性、数据保密性、产品采购、密码管理等技术手段解决；
* 攻击者利用通信干扰工具，故意导致通信数据错误，需要通过结构安全和网段划分、通信完整性、数据完整性等技术手段解决。

#### 管理层面安全需求

安全是不能仅仅靠技术来保证，单纯的技术都无法实现绝对的安全，资鼎(上海)互联网金融信息服务有限公司必须要有相应的组织管理体制配合、支撑，才能确保信息系统安全、稳定运行。

管理安全是整体安全中重要的组成部分。信息系统安全管理虽然得到了一定的落实，但由于人员编制有限，安全的专业性、复杂性、不可预计性等，在管理机构、管理制度、人员安全、系统建设、系统运维等安全管理方面存在一些安全隐患：

* 管理机构
* 需要建立安全职能部门，设置安全管理岗位，配备必要的安全管理人员、网络管理人员、系统管理人员；
* 需要配备相应的安全管理员、网络管理员、系统管理员；
* 需要建立相应的审批部门，进行相关工作的审批和授权；
* 需要建立定期和不定期的协调会，就信息安全相关的业务进行协调处理；
* 需要建立相应的审核和检查部门，安全人员定期的进行全面的安全检查。
* 管理制度
* 需要制定信息安全工作的总体方针、政策性文件和安全策略等，说明机构安全工作的总体目标、范围、方针、原则、责任等；
* 需要建立安全管理制度，对管理活动进行制度化管理，制定相应的制定和发布制度；
* 需要对安全管理制度进行评审和修订，不断完善、健全安全管理制度；
* 需要各功能部门协调机制，进行必要的沟通和合作；
* 需要建立相关工作的审批和授权机制，进行必要活动的审批和授权；
* 需要建立恰当的联络渠道，进行必要的沟通和合作，在必要的时候，进行事件的有效处理；
* 需要建立审核和检查的制度，对安全策略的正确性和安全措施的合理性进行审核和检查；
* 需要建立备案管理制度，对系统的定级进行备案；
* 需要建立产品采购，系统测试和验收制度，确保安全产品的可信度和产品质量。
* 人员安全
* 需要对人员的录用进行必要的管理，确保人员录用的安全；
* 需要对人员的离岗进行有效的管理，确保人员的离岗不会带来安全问题；
* 需要对人员的考核进行严格的管理，提高人员的安全技能和安全意识；
* 需要对人员进行安全意识的教育和培训，提高人员的安全意识；
* 需要对第三方人员访问进行严格的控制，确保第三方人员访问的安全。
* 系统建设
* 需要具有设计合理、安全网络结构的能力；
* 需要密码算法和密钥的使用符合国家有关法律、法规的规定；
* 需要任何变更控制和设备重用要申报和审批，并对其实行制度化的管理；
* 需要对信息系统进行合理定级，并进行备案管理；
* 需要安全产品的可信度和产品质量；
* 需要自行开发过程和工程实施过程中的安全；
* 需要能顺利地接管和维护信息系统；
* 需要安全工程的实施质量和安全功能的准确实现；
* 需要对软硬件的分发过程进行控制；
* 需要信息安全事件实行分等级响应、处置。
* 系统运维
* 需要机房具有良好的运行环境；
* 需要对信息资产进行分类标识、分级管理；
* 需要对各种软硬件设备的选型、采购、发放、使用和保管等过程进行控制；
* 需要各种网络设备、服务器正确使用和维护；
* 需要对网络、操作系统、数据库系统和应用系统进行安全管理；
* 需要用户具有鉴别信息使用的安全意识；
* 需要定期地对通信线路进行检查和维护；
* 需要硬件设备、存储介质存放环境安全，并对其的使用进行控制和保护；
* 需要对支撑设施、硬件设备、存储介质进行日常维护和管理；
* 需要系统中使用的硬件、软件产品的质量；
* 需要提供足够的使用手册、维护指南等资料；
* 需要软硬件中没有后门程序和隐蔽信道；
* 需要在事件发生后能采取积极、有效的应急策略和措施。

### 总体安全设计

#### 总体安全策略设计

* 根据系统的安全定级规划，明确该等级对应的的总体防护描述；
* 根据系统和子系统划分结果、安全定级结果将保护对象归类，并组成保护对象框架；
* 根据方案的设计目标来建立整体保障框架，来指导整个安全保护方案的设计，明确关键的安全要素、流程及相互关系；在安全措施框架细化后将补充到整体保障框架中；
* 根据系统受到的威胁对应出该等级的基本保护要求（即需求分析），并分布到物理层、网络层、系统层、数据层、应用层、管理层等不同的层面上；
* 根据由威胁引出的安全保护基本要求、安全保护实施过程、整体保障框架来确定总体安全策略（即总体安全目标），再根据安全保护的基本要求将总体安全策略细分为不同的具体策略（即具体安全目标），包括安全域内部、安全域边界和安全域互联的策略，并分布到物理层、网络层、系统层、数据层、应用层、管理层等不同的层面上；
* 根据保护对象框架、等级化安全措施要求、安全措施的成本来选择和调整安全措施；根据安全技术体系和安全管理体系的划分，各安全措施共同组成了安全措施框架；
* 各安全保护对象根据系统的功能特性、安全价值以及面临威胁的相似性来进行安全区域的划分，各安全区域将保护对象框架划分成了不同部分，即各安全措施发生作用的保护对象集合。
* 根据选择好的各保护对象的安全措施、安全措施框架、实际的具体需求来设计安全解决方案。

设计思路及主要过程的示意图如下：



#### 安全技术体系结构设计

* 清晰定义模型的原则

在设计资鼎(上海)互联网金融信息服务有限公司的“马上货”系统信息安全保障体系时，首先要对信息系统进行模型抽象，这样既能相对准确地描述信息体系的各个方面的内容及其安全现状，又能代表绝大多数地区和各种类型的信息系统。把信息系统各个内容属性中与安全相关的属性抽取出来，参照IATF（美国信息安全保障技术框架），建立“保护对象框架”、“安全措施框架”、“整体保障框架”等安全框架模型，从而相对准确地描述信息系统的安全属性和等级保护的逻辑思维。

* 分域防护、综合防范的原则

任何安全措施都不是绝对安全的，都可能被攻破。为预防攻破一层或一类保护的攻击行为无法破坏整个信息系统，需要合理划分安全域和综合采用多种有效措施，进行多层和多重保护。

* 需求、风险、代价平衡的原则

对任何类型网络，绝对安全难以达到，也不一定是必须的，需正确处理需求、风险与代价的关系，等级保护，适度防护，做到安全性与可用性相容，做到技术上可实现，经济上可执行。

* 技术与管理相结合原则

资鼎(上海)互联网金融信息服务有限公司的“马上货”系统的信息安全涉及人、技术、操作等各方面要素，单靠技术或单靠管理都不可能实现。因此在考虑信息系统信息安全时，必须将各种安全技术与运行管理机制、人员思想教育、技术培训、安全规章制度建设相结合。

* 动态发展和可扩展原则

随着网络攻防技术的进一步发展，资鼎(上海)互联网金融信息服务有限公司的“马上货”系统的网络安全需求会不断变化，以及环境、条件、时间的限制，安全防护一步到位，一劳永逸地解决信息安全问题是不现实的。信息安全保障建设可先保证基本的、必须的安全性和良好的安全可扩展性，今后随着应用和网络安全技术的发展，不断调整安全策略，加强安全防护力度，以适应新的网络安全环境，满足新的信息安全需求。

#### 安全管理体系结构设计

安全体系框架是按照结构化原理描述的安全措施的组合，依据“积极防御、综合防范”的方针，以及“管理与技术并重”的原则进行设计的。

资鼎(上海)互联网金融信息服务有限公司的“马上货”系统安全措施框架包括安全技术措施、安全管理措施两大部分。安全技术措施包括安全防护系统（物理防护、边界防护、监控检测、安全审计和应急恢复等子系统）和安全支撑系统（安全运营平台、网络管理系统和网络信任系统）。

安全技术措施、安全管理措施各部分之间的关系是人（安全机构和人员），按照规则（安全管理制度），使用技术工具（安全技术）进行操作（系统建设和系统运维）。安全措施框架示意图如下：安全措施框架是按照结构化原理描述的安全措施的组合。本方案的安全措施框架是依据“积极防御、综合防范”的方针，以及“管理与技术并重”的原则进行设计的。

资鼎(上海)互联网金融信息服务有限公司的“马上货”系统安全措施框架包括安全技术措施、安全管理措施两大部分。安全技术措施包括安全防护系统（物理防护、边界防护、监控检测、安全审计和应急恢复等子系统）和安全支撑系统（安全运营平台、网络管理系统和网络信任系统）。

安全技术措施、安全管理措施各部分之间的关系是人（安全机构和人员），按照规则（安全管理制度），使用技术工具（安全技术）进行操作（系统建设和系统运维）。安全措施框架示意图如下：



### 安全建设规划

#### 安全建设目标确定

一般而言，信息系统的安全保护能力主要分为对抗能力和恢复能力。能够应对威胁的能力构成了系统的安全保护能力之一——对抗能力。能够在一定时间内恢复系统原有状态的能力构成了系统的另一种安全保护能力——恢复能力。对抗能力和恢复能力共同形成了信息系统的安全保护能力。

基于资鼎(上海)互联网金融信息服务有限公司的“马上货”系统的具体安全需求、以国内外先进的信息安全模型等理论为基础，同时结合资鼎(上海)互联网金融信息服务有限公司信息系统的目前现状，将安全理论转化为具体安全需求，将安全体系分为两个方面，五个层次来考虑。两个方面主要是安全技术体系和安全管理体系，五个层次包括物理层、网络层、系统层、应用层、数据层。再依据现有比较成熟的安全技术，将安全需求转化为可以实现的技术和管理安全防护手段，为资鼎(上海)互联网金融信息服务有限公司的“马上货”系统全面性、及时性、准确性、完整性、保密性、无障碍性等业务要求提供安全保障。

通过技术手段和管理手段相结合来增强资鼎(上海)互联网金融信息服务有限公司的“马上货”系统的安全保护能力是本系统建设的核心目标，具体包括如下：

* 核心应用服务不受攻击
* 公共服务信息不被篡改
* 敏感资料不被窃取

#### 安全建设内容规划

针对信息系统自身的业务特点，依托并结合适应政府行业电子政务特点且已经行之有效的业务管理体系，开展信息安全管理工作，达到与现有的业务管理体系及安全技术体系相互依托、高度融合，更好地发挥技术体系作用，同时安全管理体系将融入到日常的运维体系当中，也争取将关键指标纳入到正常的绩效考核体系中，从组织、人员、运维等方面进行体现管理本质的信息安全管理体系建设。

信息系统的安全等级保护是依据信息系统的安全等级情况保证它们具有相应等级的基本安全保护能力，不同安全等级的信息系统要求具有不同的安全保护能力。实现基本安全保护能力将通过选用合适的安全措施或安全控制来保证，根据等级保护要求，可以使用的安全措施或安全控制依据实现方式的不同，分为技术要求和管理要求两大类。

技术类安全要求通常与信息系统提供的技术安全机制有关，主要是通过在信息系统中部署软硬件并正确的配置其安全功能来实现；管理类安全要求通常与信息系统中各种角色参与的活动有关，主要是通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现。

基本建设内容从物理安全、网络安全、主机系统安全、应用安全和数据安全几个层面提出安全要求；基本管理要求从安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理几个方面提出安全要求。

技术要求与管理要求是确保信息系统安全不可分割的两个部分，两者之间既互相独立，又互相关联，在一些情况下，技术和管理能够发挥它们各自的作用；在另一些情况下，需要同时使用技术和管理两种手段，实现安全控制或更强的安全控制；大多数情况下，技术和管理要求互相提供支撑以确保各自功能的正确实现。

#### 安全建设项目计划

项目建设的实施进度可规划为以下几个阶段，具体设计如下：

* 第1阶段

完成项目招投标的评审论证，确定项目实施中标单位，并完成合同签订等相关工作。

* 第2阶段

根据评标委员会专家组评审意见完善方案细节，执行项目深化调研以确保方案的可实施性，为正式建设作充分的技术准备。同步完成项目建设涉及的软硬件安全产品的采购订货工作。

* 第3阶段

项目涉及的各个软硬件设备到货，集中进行安全集成与实施；同步进行用户技术培训等工作。

* 第4阶段

系统建设实施完毕，准备相关资料，同步进行系统等级保护安全测评。

* 第5阶段

安全测评通过后，上报等级保护相关主管部门审批备案，并同步根据测评单位给出的反馈意见实施整改优化。通过等保测评，可启动项目验收流程，正式进入系统运维周期。

## 系统工程实施

* 指定或授权专门的部门或人员负责工程实施过程的管理，必要时可引入外部信息工程监理机构进行工程实施的监理；
* 由实施方制定详细的工程实施方案控制实施过程，由资鼎(上海)互联网金融信息服务有限公司认可并要求工程实施单位能按计划执行工程实施；
* 由实施方制定工程实施方面的管理规范，明确说明实施过程的控制方法和人员行为准则，及时向资鼎(上海)互联网金融信息服务有限公司提交相关表单文档。

### 产品采购管理制度

说明负责产品采购的部门

* 我单位计算机设备，包括PC机、笔记本电脑、打印机、电话机、服务器及辅助外设，计算机软件包括系统软件、应用软件和其他通用软件（包括开发工具、办公自动化等），由行政部按照单位的预算制度和审批流程购买及管理。
* 选用的计算机硬件和软件及相关产品的种类、型号必须符合符合国家的有关规定和我单位的各项技术规定，密码产品采购和使用符合国家密码主管部门的要求；并且定期检查安全产品采购和使用的国家有关规定及行业相关要求，及时更新组织的相关规定。
* 公司采购计划必须包含在每年预算范围内。超出预算范围内的采购计划必须向上级管理层及财务部解释原因，并须批准。
* 业务部门和个人需要购买计算机设备或软件，首先须由本部门领导审批同意，然后向行政部提出申请。行政部在考虑统一规划和综合评估后，如确实需要购买，经研发部选配计算机设备或软件规格、型号，行政部确定价格后，申请人根据此价格完成财务审批手续。
* 对于有特殊性能和功能要求但没有相应数据证明满足该要求的产品，应组织人员进行专项测试，并保留测试数据；重要部位的产品委托国家认可的专业测评单位进行专项测试，并将测试结果作为选用产品的重要因素。
* 付款前应填写财务付款审批表，然后根据单位的付款流程处理。
* 购买物品到货后，由购买经手人负责清点验货。
* 购买经手人完成清点验货后，签署验收单；如果厂商提供验收单，可以直接签署厂商验收单，保留原件；如果厂商没有验收单，则厂商送货人及验收人签署本单位的到货验收单。此到货验收单复印件送交财务部作为资产入账凭据。
* 购买经手人完成清点验货后，对购买物品进行资产登记编号，如果购买物品属于固定资产，应录入单位及部门的资产清单。
* 单位职工领用IT设备及软件时，行政部做好领用登记，如不在使用范围的员工申请，须经本部门领导及相关负责人确认后方可领用。

### 安全服务商选择

* 确保系统建设服务商的选择符合国家信息安全的有关规定，必要时应选择有安全集成的相关资质的服务商；
* 与选定的系统建设服务商签订与安全相关的保密协议，明确约定相关责任；
* 确保选定的系统建设服务商提供技术培训和服务承诺，必要的与其签订服务合同。

### 硬件采购和安装

* 应确保产品采购和使用符合国家信息安全的有关规定；
* 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；
* 尽量采用我国自主开发研制的信息安全技术和设备；
* 采用境外信息安全产品时，产品必须通过国家信息安全测评机构的认可；
* 严禁使用未经国家密码管理部门批准和未通过国家信息安全质量认证的密码设备；
* 设备符合系统选型要求并获得批准后，方可购置；
* 凡购回的设备均应在测试环境下经过连续72小时以上的单机运行测试和联机48小时的应用系统兼容性运行测试；
* 通过上述测试后，设备才能进入试运行阶段。试运行时间的长短可根据需要自行确定；
* 通过试运行的设备，才能投入系统，正式运行。

### 软件采购和安装

* 信息系统所使用的操作系统、应用软件、数据库、安全软件、工具软件必须是正式版本，严禁使用测试版和盗版软件；
* 重要的操作系统和主要应用软件必须在安全管理员的监督之下进行安装；
* 软件的参数设置由应用管理员设置，并进行相关备份。

### 系统软件开发管理

#### 软件自主开发管理

说明负责软件开发的部门名称

* 系统应用软件的开发必须根据信息密级和安全等级，同步进行相应的安全设计，并制定各阶段安全目标，按目标进行管理和实施；
* 系统应用软件的开发，必须有安全管理专业的技术人员参加，其主要任务是：对系统方案与开发进行安全审查和监督，负责系统安全设计和实施；
* 软件设计方案、数据结构、安全管理、操作监控手段、数据加密形式、原代码等，只能在有关开发人员及有关管理机构中流动，严禁散失或外泄；
* 应用软件开发必须符合软件工程规范；
* 确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制；
* 制定代码编写安全规范，要求开发人员参照规范编写代码；
* 确保提供软件设计的相关文档和使用指南，并由应用管理员负责保管；
* 确保对程序资源库的修改、更新、发布进行授权和批准。

#### 外包软件开发管理

* 应要求开发单位提供软件设计的相关文档和使用指南；
* 在委托开发过程中，应加强开发过程中的安全管理和监控，重点考虑资质、许可证、代码所有权和知识产权；审核工作质量和访问权限，代码质量和安全功能达到合同要求；
* 应要求软件开发商在所开发的信息系统内设计实现了安全控制措施，确保信息在系统中得到了正确处理；
* 在开发过程中，应采取控制措施，减少信息泄露的可能性，重点考虑：规范开发过程中的通信行为，以减少第三方从这些行为中推断信息的可能性；在现有法律或法规允许的情况下，定期监视个人和系统的活动；监视计算机系统的资源使用；防止非授权的网络访问；对程序源代码的防护管理；
* 应要求软件开发商对程序源代码进行管理与控制

程序源代码应集中保存在代码库中，对代码库实施安全保护。保护措施主要包括：建立程序源代码和源程序库管理规范；对访问源程序库人员进行授权管制；程序列表应保存在安全的环境中；建立对源程序库所有访问的审核日志；维护和拷贝源程序库应受严格的限制。

* 测试数据的管理

在测试数据选择过程中，应避免使用包含个人信息或其它敏感信息的运行数据库用于测试。其控制措施包括：运行信息每次被拷贝到测试系统时应有独立的授权；测试完成后，应立即从测试系统中清除运行信息或进行授权访问控制；记录运行信息的拷贝和使用日志。

* 信息系统安全整体测试

开发完成的系统须用户在离线测试环境下对所开发信息系统进行安全测试。经过测试确认后，方可转入正式环境，并组织评估测试结果的安全符合性。

## 系统测试验收

说明测试验收负责部门

* 委托第三方测试单位对系统进行安全性测试，并出具安全性测试报告，要求建设单位根据测试结果及时进行整改；
* 在测试前应根据设计方案或合同要求等制订测试方案，在测试过程中应详细记录测试结果，并形成测试报告，测试通过后方可进行验收；
* 对系统测试验收的控制方法和人员行为准则进行书面规定；
* 指定或授权专门的部门或人员负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；
* 形成系统安全性测试报告，报告给出测试通过的结论（如果报告中提出了存在的问题，则检查是否有针对这些问题的改进报告），有第三方测试机构的签字或盖章。

## 系统交付

说明负责系统交付的部门

* 对系统交付的控制方法和人员行为准则进行书面规定；
* 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作；
* 制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点和确认；
* 对负责系统运行维护的技术人员进行相应的技能培训，以及对系统最终用户的操作进行相应的培训。

## 系统备案

* 建立和归档系统等级相关材料报主管部门备案的记录或备案文档；
* 建立和归档系统等级相关备案材料报相应公安机关备案的记录或证明；
* 建立和归档系统定级相关材料的使用控制记录。

# 硬件设备运维管理制度

## 硬件设备运维管理制度

### 机房安全管理制度

* 机房管理员负责机房的安全管理，主要包括：

1. 保障机房信息系统的安全运行；
2. 负责机房的环境维护和物理访问管理；
3. 负责机房的设备维护及设备管理；
4. 负责机房内任何事故的上报及处理；
5. 负责制定及修订有关机房安全管理制度。

* 机房管理员负责对机房值班人员及技术维护人员（外包方）进行日常工作管理和检查；
* 机房内无人时应当关门；
* 任何人未经机房管理员许可不得进入机房、不得擅自操作或移动机房内设备；
* 外来人员进出机房需有机房管理员全程陪同，不得单独留外来人员在机房操作；
* 机房内的一切公用物品未经主管部门负责人许可一律不得挪用和外借；
* 保持良好的卫生环境，机房内不得抽烟，不得带入食品和饮料；
* 保持机房肃静，不要大声喧哗；
* 严禁携带易燃、易爆、易碎、易污染以及强磁物品进入电脑机房；
* 机房温度应保持在20℃~23℃左右，不得任意调整机房温度、湿度；
* 相关文件与记录为：《资鼎(上海)互联网金融信息服务有限公司进入机房人员登记表》（详见附40），《资鼎(上海)互联网金融信息服务有限公司机房设备出门单》（详见附41）。

#### 机房出入访问控制安全管理

* 资鼎(上海)互联网金融信息服务有限公司机房管理员负责机房日常的管理；
* 任何人进入机房都需经研发部授权，任何人必须办理有关登记手续方能进入机房，否则不得私自进入机房。特殊情况下，对于没有机房出入证的人员可由机房管理员进行电话确定，经研发部相关负责人授权同意后方可进入机房；
* 任何人进入机房应主动配合机房管理员填写《机房出入登记表》，明确填写进、出时间，进入事由，陪同人、物品携带情况及是否有敏感操作行为；
* 机房值班人员应严格把好设备、物品进出关，严禁将对机房有害设备、物品带入机房。任何人携带非机房设备进入机房须登记；
* 凡出入机房的物理设备均须经机房管理员确认后方可出入机房。有设备进入机房时，机房值班人员应及时通知资产管理员，得到其确认后方可允许设备进入；有设备移出机房时，相关人员应主动出具盖章后的《资鼎(上海)互联网金融信息服务有限公司机房设备出门单》，经机房人员查验同时得到机房资产管理员确认后方可移出；
* 凡进入机房核心区域的非机房长期工作人员须由机房相关工作人员全程陪同，否则不允许出入机房核心区域和进行任何操作；
* 非机房工作人员进出机房时，机房人员必须做好相关记录，并在进出时进行登记。

#### 机房设备访问控制管理

* 未经资鼎(上海)互联网金融信息服务有限公司信息领导小组授权和机房资产管理员的当面确认，任何人员不得私自接触、拆卸、移动在机房内的所有服务器、PC或网络设备等以及相关配件；
* 机房管理员负责机房设备日常管理及维护，机房及内部设备应保持干净、整洁，须安排人员定期（每周一次）开展卫生保洁工作；
* 机房设备的安置必须满足设备供应商要求的物理环境；
* 机房设施的日常维护应有维护记录，对失效的设施及时进行维修；
* 任何个人，未经同意，不得擅自更改网络设备及其配置；
* 机房内的重点设施（设备），如UPS电源、服务器、网络设备等应指定专人管理，日常操作由管理员负责,其他人员未经允许严禁上机操作、更改设置及改动相应的关联设备；
* 机房内的管理人员使用的计算机监控设备和工作盘片以及专用U盘和移动硬盘，应定期进行计算机病毒检查。

#### 机房事故处理管理

* 对机房内的关键系统、设施（设备）应制定安全应急预案；
* 机房发生重大问题，如断电、火警、重点设备的异常，应及时采取积极措施排除险情，并按应急预案处理；
* 机房内发生的各类事故，应由事故直接责任人承担。机房管理员和分管负责人也应承担相应的管理责任。造成经济损失的，按损失的大小承担一定的赔偿或处罚；
* 机房内发生的各类事故，应做好相应的事故记录，对重大事故应根据相关事故处理流程处理，同时应向上级管理部门报告。

### 办公环境安全管理制度

资鼎(上海)互联网金融信息服务有限公司研发部负责办公环境的安全管理，同时负责对办公环境日常工作进行管理和检查。

* 对于外来人员，必须验证，问明来意，不在办公区接待来访人员，不允许委托外单位人员来办公室取物品；
* 禁止收旧货、推销物品等闲杂人员进入办公区；从办公室内取走物品，值班人员应索取放行凭据后，方可放行；
* 工作人员最后离开办公室者，应随手关闭冷、暖气、电灯、电扇、电脑，切断电源，锁门；
* 工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件
* 不许在办公室使用电炉及超负荷电器；不许将易燃、易爆、剧毒、放射性等危险品带入办公室；
* 严格管理文件、公章、重要资料、文书档案，及时妥善处理打印废纸；
* 发现不安全隐患要及时报告，认真整改，防患未然。定期组织检查；
* 违反上述规定，导致发生事故的，要逐级追究责任人和当事人的责任。
* 工作人员调离办公室应立即交还该办公室钥匙

### 资产安全管理制度

行政部为资鼎(上海)互联网金融信息服务有限公司信息化资产分类及管理工作的管理部室，负责资产的发放，领用和分类标识。

* 建立设备登记档案，详细记录每台设备的名称、规格、配置、单价、购入日期、供货商、存放地点、耐用年限等参数，关键设备应建立维护档案；（详见附42）
* 根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
* 信息系统硬件资产在使用中，应监测生成的信息，对生成的信息应及时分析并做出分析报告；
* 在监测中如发现重大问题，应立即采取相应控制措施并将有关情况逐级上报；
* 信息系统硬件资产使用中产生的重要报告应备份存档，并按密级资料管理方式履行有关手续；
* 信息系统硬件资产应及时进行升级和维护并登记备案；
* 信息系统硬件资产报废后，应报有关部门审批方可封存或销毁；
* 应对信息系统硬件资产的使用情况进行定期（每季度一次）检查。

#### 信息的分类

* 根据信息在资鼎(上海)互联网金融信息服务有限公司信息系统的重要程度,考虑信息在机密性,完整性和可用性的综合影响,将信息划分为:关键信息、重要信息及一般信息；
  + 1. 关键信息：为资鼎(上海)互联网金融信息服务有限公司信息系统中关键信息，如果遭受破坏或泄露会使导致关键信息系统故障或难以恢复，造成的经济利益、公众信誉受到重大损害，例如：等保二级信息系统中的数据及系统配置信息、IP地址分配表、网络拓扑图等；
    2. 重要信息：为资鼎(上海)互联网金融信息服务有限公司信息系统中重要信息，如果遭受破坏或泄露会导致重要业务系统故障或难以恢复，造成资鼎(上海)互联网金融信息服务有限公司日常工作遭受损害、干扰和影响，资鼎(上海)互联网金融信息服务有限公司的经济利益、公众信誉受到一定损害；例如：等保二级信息系统中合同、合作伙伴信息、管理信息等；
    3. 一般信息：为资鼎(上海)互联网金融信息服务有限公司信息系统中一般信息，如果遭受破坏或泄露不会使资鼎(上海)互联网金融信息服务有限公司研发部日常工作遭受损害，但不宜向外部公开的信息，例如组织架构，规章制度，人员信息；
* 信息载体是指记载有信息或数据的纸类、电磁类及其它媒体（软盘、硬盘、光盘、磁带等）；
* 必须按分类的定义和划分要求，对信息进行分类、标识及管理；
* 对信息进行分类时，应充分考虑该信息的性质及重要程度等因素。

#### 信息的标识

* 信息在确定级别后，应做好标识；
* 资鼎(上海)互联网金融信息服务有限公司研发部仅对关键、重要信息进行标识；
* 信息系统数据类、信息系统配置类信息的标识在所在系统设备的资产识别表中体现；
* 文档类信息的标注位置应在封面、眉头或首页的右上角进行分类标注，或者标注在包装的明显处。

#### 信息的保管

* 关键信息
  + 1. 纸质的重要信息必须落实专人保管并存放于上锁的箱或柜中，有条件的应存放于保险柜中；
    2. 电子（以软盘、光盘、U盘，移动硬盘等媒介存储）的关键信息应设置访问权限，有条件的考虑加密存储，并视同纸制档案进行管理；
    3. 存储在服务器中的关键信息，必须落实相应的保密安全措施、访问权限控制措施，未采取安全保密措施的不得与互联网连接，特权帐号口令必须分段管理及双因素认证；
* 重要信息
  + 1. 纸质、电子（以软盘、光盘、U盘，移动硬盘等媒介存贮的）的重要信息应存放于上锁抽屉中，有条件的应存放于上锁的箱或柜中妥善保管，保证安全；
    2. 存储在服务器中的重要信息，必须落实相应的保密安全措施、访问权限控制措施，未采取安全保密措施的不得与互联网连接；
* 一般信息
  + 1. 纸质、电子（以软盘、光盘、U盘，移动硬盘等媒介存贮的）的内部公开信息应存放于上锁抽屉中，有条件的应存放于上锁的箱或柜中妥善保管，保证安全；
    2. 存储在设备中（如服务器、笔记本电脑等）的一般信息，应有访问权限控制措施。

#### 信息的使用

* 关键和重要的信息系统数据
  + 1. 未经允许和授权，任何人员不得随意查询、更改或删除；
    2. 未经允许和授权，任何人不得借阅信息系统数据；
    3. 如其他部门需维护、更新或获取核心、关键或重要信息，应要求需求提出部门向资鼎(上海)互联网金融信息服务有限公司提出正式申请；对于关键信息，需经资鼎(上海)互联网金融信息服务有限公司领导小组同意，其他信息需经研发部同意后方可由实施；数据获取完成并提交需求部门后，应及时删除。应用于开发测试目的的客户数据，应在使用前对账号、密码、身份证件信息、联络方式等信息进行变形处理；
* 关键和重要的信息系统配置
  + 1. 研发部应根据相关安全要求配置系统；
    2. 系统投入生产后，系统配置不得随意修改；如需修改，需根据制度中系统变更相关要求进行；
    3. 系统配置信息变更前，应做好原配置信息的备份工作；
* 关键和重要的文档类信息
  + 1. 只允许限定人员在资鼎(上海)互联网金融信息服务有限公司内使用；如需扩大使用范围，需经资鼎(上海)互联网金融信息服务有限公司主管领导批准；
* 一般信息
  + 1. 可在资鼎(上海)互联网金融信息服务有限公司内公开使用；如需向资鼎(上海)互联网金融信息服务有限公司以外公开，必须经过研发部负责人批准。

#### 信息的传递

* 对于其他部门提出的信息系统数据获取需求，研发部必须采用加密方式将数据传递给需求提出部门，有条件的可通过机要渠道传递；
* 信息系统数据不得通过互联网传输，其他信息如需在互联网上传输，需经过资鼎(上海)互联网金融信息服务有限公司主管领导同意并采用加密方式传递。

#### 信息的复制

* 信息系统数据严禁打印；
* 关键的非信息系统数据类信息：
  + 1. 原则上严禁打印或复印，如确有需要，需经资鼎(上海)互联网金融信息服务有限公司主管领导批准；
    2. 复印件的使用及管理要求同原件，并须符合本管理程序的要求，使用后及时销毁；
* 重要的非信息系统数据类：
  + 1. 严格限定打印及复印；
    2. 复印件的使用及管理要求同原件，并须符合本管理程序的要求，使用后及时销毁；
* 一般信息：内部人员不作特殊限制，使用及管理同原件，并符合本管理程序的要求。

#### 信息的销毁

* 信息系统数据
  + 1. 如因存储有业务办公系统数据的设备损坏、送修、数据超过保存期限等原因，需销毁数据的，需经资鼎(上海)互联网金融信息服务有限公司研发部领导批准；
    2. 磁盘、磁带应采用消磁方式处理，光盘需采用粉碎方式处理；
* 由安全管理员执行，至少二人以上在场；
* 关键和重要的非信息系统数据类信息
  + 1. 如需销毁，经研发部负责人批准；
    2. 纸质采取粉碎，电子媒介采用消磁方式处理；
* 一般信息如需销毁，纸质应采用粉碎处理，电子媒介采用格式化处理；
* 销毁关键信息应向资鼎(上海)互联网金融信息服务有限公司研发部报备登记。

#### 信息的备份与恢复

* 信息系统数据、信息系统配置信息的备份应参照《备份与恢复管理制度》执行；
* 文档类信息的备份由研发部安全管理员负责。应根据信息级别制定相应的备份策略；
* 各信息责任团队应定期（每月一次）验证备份有效性，验证后应及时删除恢复数据；
* 备份信息的保管要求、恢复后的信息使用及管理要求视同原信息；

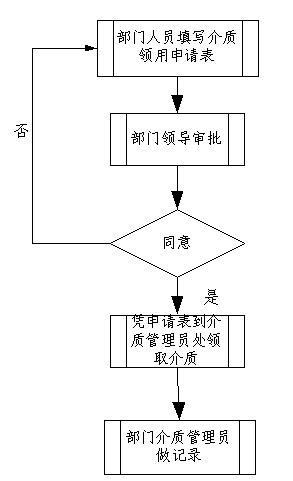
#### 信息级别解除或变更

* 因工作情况变化或随时间推移，信息重要程度发生变化时，可视情形解除或变更信息的级别；
* 信息级别的解除或变更：
  + 1. 关键信息级别的解除或变更需经信息安全领导小组批准；
    2. 重要、一般信息级别的解除或变更需经信息安全领导小组核准；
    3. 信息级别的解除或变更并同时通知相关使用部门，关键信息的级别变更应向研发部报备；
    4. 变更后的信息，应按照相应的级别管理和使用。

### 介质安全管理制度

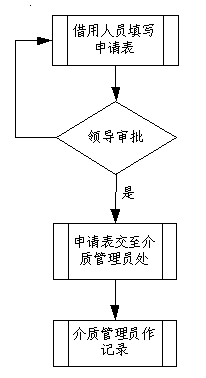
安全管理员负责资鼎(上海)互联网金融信息服务有限公司生产介质的使用控制及处置管理。

**信息安全介质使用流程**

****

* 介质的使用人负责所使用介质的控制及处置管理。
* 各相关接待人负责其接待的外来人员的介质的使用及监督。若需使用信息安全存储介质，需经信息安全领导小组审批同意后由安全管理员统一领用和管理。
* 安全U盘、移动硬盘由安全管理员统一进行保管。
* 内部实行信息安全存储介质借用制度，由借用人填写“信息安全介质借用/领用申请表”（附43）向安全管理员借用信息安全介质，介质使用后应及时归还，如丢失则需追究责任。安全管理员应做好相关的登记管理工作并接受安全审计员的监督检查。

**信息安全介质借用流程**



* 移动介质在接入信息系统前，必须进行恶意代码、木马检测和杀毒处理，防止恶意代码侵入和传染给其它信息系统；
* 如果信息不再需要，需删除可重复使用的移动介质中的信息；
* 如果信息需要保存，则使用人应该保存在个人计算机中，而不应该放在移动介质中；
* 介质在长期保管时，其保管的地点必须满足防火、防水、防震、防潮、防霉、防鼠害、防虫蛀、防静电、防磁等方面的安全要求，介质的保管要符合介质生产商对介质保管的要求；
* 并定期（每季度一次）对介质中的数据进行转存和验证测试，防止由于介质老化、失效而导致的重要数据丢失；
* 内部实行存储介质借用制度，介质使用后应及时归还。安全管理员应做好相关的登记管理工作；
* 存储介质的保管工作必须符合国家相关管理制度。各类存储介质如未经批准严禁由个人私自带离开本单位外；
* 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

#### 介质的存放环境

* 介质由于其体积较小，易于流传的特点，使用时应注意对其安全保管，防止丢失；
* 对于磁带、磁盘等带有磁性介质的介质应注意其保存环境，保证其长期（十年）有效；
* 用于生产网络的介质（如备份光盘、磁带等）应由安全管理员负责保管，存放于机房或办公环境专用柜中，防止其被盗、被毁、被未授权修改以及信息的非法泄漏；
* 应根据数据备份的需要确定须异地存储的备份介质，存储地的环境要求和管理方法应与本地相同。

#### 介质的维护

* 作为重要用途的光盘、磁带、移动硬盘，应按照信息分类原则进行分类管理，做好信息标识，并且由安全管理员保管在安全的地方，不再用其作为信息交换的介质。对重要介质中的数据和软件采取加密存储；
* 应对备份用途的光盘、磁带、移动硬盘建立介质目录清单，由安全管理人员定期（每季度一次）根据目录清单对介质的使用现状进行检查，检查内容包括完整性（数据是否损坏或丢失）和可用性（介质是否受到物理破坏）。

#### 介质的报废

**信息安全载体销毁审批流程图**

申请人填写销毁审批表

核对人清点载体、签字

申请部门领导审核

信息科领导审核

主要领导审批

机房管理员、网络管理员共同押运、外送销毁

否

否

NO

NO

NO

NO

否

否

否

·

否

* 介质损坏后不得自行销毁或丢弃，需交还至资鼎(上海)互联网金融信息服务有限公司研发部进行处理。
* 安全管理员定期（每半年一次）将损坏的介质集中，填写《介质销毁审批表》，经信息安全领导小组批准后，交研发部进行统一销毁（附44）。
* 信息安全介质的销毁工作由安全管理员负责。
* 拟销毁的信息安全介质要登记造册，机房管理员和网络管理员两人核对，主机管理员和应用管理员两人监销。

#### 介质的维修管理

信息安全介质因故障需送外修理，必须经领导批准，由安全管理员负责送修。申请维修的人员陪同，并在修理现场进行监督，当场取回，并填写维修记录表附45

### 设备管理制度

安全管理员为资鼎(上海)互联网金融信息服务有限公司设备管理及发放的人员，负责资产的采购申请、发放、领用和分类。

#### 设备的购置要求

* 购买设备前，应对拟购买的设备进行试用，测试其性能及安全功能是否满足需求，若不能满足，则应考虑其他供应商或采取相应的控制措施；
* 选购信息安全产品，应对产品资质进行审查，选购通过国家权威机构认证的信息安全产品；
* 选购密码类产品，应对产品资质进行审查，使用信息安全主管机构批准的密码类产品；
* 所有采购来的设备，应先由资鼎(上海)互联网金融信息服务有限公司安全管理员进行资产登记，在设备清单记录该设备的品牌、型号、S/N号、详细配置和保修期限等，在设备上粘贴设备标签后，资产入库。

#### 设备的发放与领用

* 信息安全设备及安全防护设施、设备的使用、维护、报废、停用，统一纳入资鼎(上海)互联网金融信息服务有限公司研发固定资产管理范围，由相关部门进行统一购置、统一标识、统一发放。资鼎(上海)互联网金融信息服务有限公司安全管理员负责具体审核，并且进行登记备案工作。（附46）
* 每六个月应对设备和存储介质的数量、用途等进行清查核对和登记，并将结果报资鼎(上海)互联网金融信息服务有限公司信息安全领导小组进行备案，如发现问题应及时向资鼎(上海)互联网金融信息服务有限公司研发部领导报告。
* 信息安全设施、设备的使用管理部门应建立相应的管理制度，严格使用程序和操作规定。对于重要的设施、设备应由专职管理人员负责管理和使用，认真落实各项安全措施，切实做好安全防范工作。
* 信息安全设备与介质应由安全管理员负责对供货方交付的货物进行验收，验收时应对产品型号、数量、配置、检测证书等进行严格核对。查验供应商提供的相关检测证书原件，以验证其真实性。
* 使用的设备和产品，应符合安全管理要求。
* 信息安全设施、设备的使用人员必须严格遵守信息安全纪律，不得泄露有关安全信息，不得擅自携带信息安全设备外出。
* 信息安全设备及防护措施、设备出现故障时，应当及时与指定单位联系维修，并做好维修记录。未经信息安全部门同意，禁止擅自拆卸维修。
* 计算机设备责任人变更时需要按一下变更流程进行变更，通过审批后才能变更。（详见附47）

**计算机设备责任人变更流程**



#### 设备的维护与维修

* 按照信息设备维护要求的时间间隔和规范，对设备进行维护；
* 设备如需升级或维修，因由安全管理员提出申请，经主管领导批准后，进行维修或升级；
* 送外单位维修的设备不得存储内部敏感信息。在送修前应由资鼎(上海)互联网金融信息服务有限公司安全管理员对送修设备是否存有内部敏感信息进行检查。如有，应先拆除硬盘等存储部件，或使用信息清除软件对磁盘信息进行彻底清除后，方能送修；
* 重要设备的维护人员在现场维护过程中，应有资鼎(上海)互联网金融信息服务有限公司相关负责人员在场，外部人员的访问应进行登记，必要时要求其签署保密协议；
* 设备进行升级或维修后，如设备配置进行了变更，则将最新设备配置资鼎(上海)互联网金融信息服务有限公司安全管理员处进行备案，以保证有安全管理员处有最新的设备配置；

#### 设备的报废与销毁

* 设备确因设备老化、性能落后等原因，造成设备无法继续使用的，由安全管理员提出报废申请，相关负责人批准后，实施报废处理，并在资产清单中进行记录；
* 设备在报废处理前，应由安全管理员对其是否存有内部敏感信息进行检查。如有，应对其存储部件进行消磁或物理毁坏，确保不会因设备处置不当造成泄密。

### 网络安全管理制度

* 网络管理员负责资鼎(上海)互联网金融信息服务有限公司网络安全管理，主要包括：
  + 1. 负责网络通信系统的变更、事件处理及日常维护检查等运维管理；
    2. 负责网络通信系统连接安全管理；
    3. 负责网络通信设备的安全防护管理；
    4. 负责网络通信系统用户、日志、补丁等管理；
    5. 负责入侵检测/防御策略制定，日志或报表分析，网络入侵事件处理及网络漏洞扫描工作的组织；
* 对涉及到网络变更方面的需求（如网络结构变更、终端网络需求变更（如Hub的接入）、非常规性网络访问（如外来人员临时性访问），需向资鼎(上海)互联网金融信息服务有限公司研发部提出书面申请，研发部对变更申请进行评审通过后，方可进行操作；
* 在网络边界处采取安全措施进行有效隔离防护，并对违规行为进行检查和阻断；
* 对于网络的VLAN和安全域划分，不同业务应用系统尽量安排在不通的安全域中，各VLAN和安全域间应采取有效的访问控制措施；
* 对网络设备、网络设备之间的连接线缆进行标识，重要网络端口也须进行详细标识；
* 开启网络设备日志，记录与网络安全相关的操作与活动，日志保存时间应至少保证在一个月以上；
* 在网络关键位置采取网络审计手段，对网络访问操作行为进行记录，定期（每半年一次）对记录进行评审，将评审结果进行记录；
* 定期（每季度一次）对网络配置、网络设备日志进行备份，并做好备份记录；
* 定期（每半年一次）对网络设备配置进行检查和评估，确保网络配置与安全策略保持一致，并对检查结果进行记录；
* 定期（每半年一次）对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；
* 定期（每半年一次）对设备口令进行更新。

#### 网络维护

* 维护人员负责定期对网络设备及主干通信线路进行例行检查，并将检查内容写进日报里；
* 外部公司（设备厂商、集成运维商等）技术人员实施系统维护前必须填写书面申请，由安全管理员签字批准后执行，维护完毕后再由资鼎(上海)互联网金融信息服务有限公司研发部相关负责人签字确认；
* 应根据网络设备供应商建议的维护周期和规范进行维护，设备维护人员必须具备相应的技术技能并应经过授权。

#### 网络变更

* 网络与信息系统的任何变更必须受到严格控制，变更后需对相关文档记录进行更新，对相关配置信息进行备份，并定期（间隔不少于1个月）存档；
* 涉及网络架构调整、软件版本升级、导致应用系统服务中断等重大网络变更实施前，需开展变更风险分析并制定应急处理预案。

#### 网络检查

* 每半年一次定期对网络进行全面检查，填写检查记录，并重启相关核心交换机。

#### 事件处理

* 网络管理员根据网络集中监控系统告警、用户报障等对网络事件进行分析处理；
* 影响正常业务和办公、大范围用户报障、网络设备故障等网络事件，网络管理员应及时向信息安全领导小组报告，并通知相关人员处理；
* 维护人员负责将每日网络异常事件及处理情况和结果记录到日报中；

#### 网络日志管理

* 网络通信系统日志收集范围至少需包括：资鼎(上海)互联网金融信息服务有限公司生产网络及安全设备的日志信息及操作日志；
* 网络日志应每月备份并存档，保存周期至少为一年。

# 系统软件运维管理制度

## 系统软件运维管理制度

### 系统安全管理制度

* 主机管理员负责资鼎(上海)互联网金融信息服务有限公司的基础平台系统安全管理，主要包括：
  + 1. 负责信息系统中操作系统、数据库系统用户新增、删除、变更的审核及实施；
    2. 负责信息系统基础平台的安全配置、参数变更、事件处理等运维管理工作；
    3. 负责信息系统基础平台系统用户、权限、日志、补丁等管理工作。
    4. 负责信息系统基础平台系统漏洞扫描工作的组织实施。
* 应用管理员负责资鼎(上海)互联网金融信息服务有限公司业务应用系统安全管理，主要包括：
  + 1. 负责信息系统中业务应用系统用户新增、删除、变更的审核及实施；

负责信息系统业务应用系统的安全配置、参数变更、事件处理等运维管理工作；

* + 1. 负责信息系统业务应用系统用户、权限、日志、补丁等管理工作。
    2. 负责信息系统业务应用系统漏洞扫描工作的组织实施；
* 对网络和信息资源实行专人管理、监督和调度，由专人对网络和信息资源进行维护和配置（对资源访问须为不同访问者设置相应权限）；
* 必须负责配置、审计、备份重要、敏感信息资源；
* 未经主管部门许可，任何人不准私自拆卸、搬移PC设备或网络设备，不得以任何方式改变系统的配置参数；
* 未经主管部门许可，任何人员不准私自更改PC机配置（包括硬件配置、操作系统及网络设置）、不准安装未经许可的软件、不准卸载必须安装的软件（如系统补丁和防病毒软件）；
* 未经主管部门许可任何人不准对非相关人员泄漏相关应用程序的登录帐号以及口令；
* 不得利用工作之便随意浏览、泄漏平台内非本职工作范围内的其它信息资料；
* 访问互联网时，不得从事违反法律、法纪、法规及各项规章制度的活动，也不能从事与工作无关的其他一切活动；不能随意下载受版权保护的软件或资料等；严禁访问不良站点；
* 对冗余数据定期清除，并监督系统的工作情况；
* 应适当审计服务器登录使用情况；
* 所有服务器需统一安装杀毒软件，并定期（每季度一次）更新。

#### 系统访问控制

* 应根据业务需求和安全要求制定访问控制策略，明确访问控制的具体要求，清楚地说明信息系统的访问控制准则和用户的访问权限；
* 访问控制策略应考虑以下内容：
  + 1. 每个系统的安全要求；
    2. 同系统间，访问控制与信息分级的一致性；
    3. 符合相关法律法规及合同义务；
    4. 访问权限的管理；
    5. 信息发布和授权的管理，如根据工作需要确定信息发布和授权范围，并明确信息的安全级别；
    6. 普通用户所能访问的基本信息。
* 访问控制准则应明确规定禁止事项和允许事项，应注意以下几点：
  + 1. 区分强制执行的准则与可选或条件性的准则；
    2. 以“除非明确许可，否则必须禁止”为基础建立准则，而不是“除非明确禁止，否则通常允许”；
    3. 信息标签的变更，包括系统自动生效的和用户决定的；
    4. 涉及用户权限的变更，包括系统自动生效的和管理员批准生效的；
    5. 访问规则需经系统管理员审查批准方可执行。

#### 系统帐号管理

* 帐号使用要求
  + 1. 所有操作系统、业务系统、数据库等均需要支持基于帐号的访问控制功能；
    2. 应用系统用户按个人创建单独的用户帐号，并赋予相应的权限，以避免共享帐号的产生；
    3. 系统管理员应对帐号申请者提供适当的培训与指导，以确保申请者能够进行正确的操作，避免对系统安全造成隐患；
    4. 系统正式投入使用前，必须更改原来系统中的缺省帐号的所有口令，以保证正式环境的安全；
    5. 帐号使用人在使用的过程中，不得使用帐号访问与自己工作无关的资源；
* 特权用户的新增、变更和注销
  + 1. 如需在系统中新增特权用户、变更或注销已有特权用户的，申请人需填写《特权用户申请表》（见附48），并提交系统管理员进行审批；
    2. 审批通过后，系统管理员安排技术人员实施并将实施结果通知申请人；
* 操作系统、数据库系统帐号管理要求
  + 1. 操作系统级和数据库超级用户帐号，由系统管理员统一进行管理、设置和分配，帐号需报管理员批准；
    2. 超级权限应基于“使用需要”，逐个事件进行授权，即以完成其工作职责的最低要求为依据，超级权限在完成特定任务后应被立即收回；
    3. 操作系统普通用户帐号由由具体使用人员向系统管理员申请，系统管理员对普通帐号统一进行管理、设置和分配。帐号的申请和审批必须有正式的书面审批表；
    4. 系统管理员需通过安全途径将帐号初始口令告知用户，用户收到初始口令后，应在初次登陆系统时修改初始口令；
* 帐号权限管理要求
  + 1. 对帐号的授权须遵守“最小权限”原则，即以其能进行系统管理、操作的最小权限进行授权，权限与具体人员的职责匹配，并根据岗位变更进行相应调整；
    2. 从帐号管理的角度，可以进行基于角色的访问控制权限的设定，即对资源的访问控制权限是以角色或组为单位进行授予，角色定义基本不随人员和管理岗位的变更而变更。

#### 系统操作安全管理

* 使用新操作系统必须向系统管理员申请，由系统管理员确定该服务器的访问地址及域名，IP等信息后，再进行安装。
* 操作系统安装完成后，在接入网络前，必须由系统管理员检查安全配置，只有经过系统管理员认可后，才能接入网络。
* 为保证计算机系统和数据库的安全，禁止同一人掌管操作系统和数据库系统口令；
* 所有用户都必须设置口令，口令应具备一定长度要求，且不可选择常用易猜的名字或单词，口令应定期更换，并应以文字形式封存。管理员用户口令文档交由安全管理员保管，普通用户口令文档由技术文档管理员保管；
* 严格按岗位职责设置各岗位工作人员的操作权限。系统管理员应定期检查操作员的权限，对于权限设置不合理的操作员，应按规定向相关人员、部门提出；
* 对于已调离的工作人员，应及时清理其操作权限；
* 应删除系统中的来宾用户，服务器及应用系统中其它的冗余用户或过期用户也需定期清理；
* 对核心数据库有写操作权限的关键用户，须设置登录站点限制，还可根据需要设置连接个数、登录时间等限制；
* 对于应用系统及其它系统设备的日常使用和维护应严格按照操作流程进行，不得违反规范随意操作；
* 对于信息系统的重要维护操作应坚持复核制度，即一人进行操作，另一人进行复核，以保证操作的正确性；
* 信息系统出现重大技术故障，应及时向上级主管部门负责人汇报，同时按应急计划实施应急措施。

#### 系统软件维护

* 系统软件维护
  + 1. 系统管理员发现操作系统有安全补丁需要安装时，应判断安全补丁的安装对现有应用系统的影响程度，并由管理员决定是否可以安装，确定允许安装后由系统管理员和安全管理员一起实施安装；
    2. 安全补丁安装之前应当对当前操作系统进行一次完全备份，安装之后对操作系统再做一次完全备份，并提交安装情况报告存档备案；
* 应用软件维护
  + 1. 应用软件有新版本需要进行升级时，应判断新版本决定是否可以在现有平台上安装，并由相关部室负责人决定是否可以安装，确定允许安装后由系统工程师应当联系软件供应商获取最新稳定版会同安全管理员一起实施安装；
    2. 应用软件升级之前应当对当前操作系统及应用软件配置和数据进行一次完全备份，安装完成之后向相关部室负责人提交安装情况报告存档备案；
    3. 应用软件系统配置、参数需要变更时，由系统管理员向相关部室负责人提交变更需求报告，组织相关技术人员进行讨论决定是否进行变更。确定允许变更以后，由系统管理员首先进行试变更，试变更应只在少数几台设备上进行，并保证这几天设备上数据的安全，保证做好数据备份。试变更经过测试未发现问题后由系统管理员会同安全管理员进行正式变更，变更前做好数据备份，变更后向相关部室负责人提交变更情况报告存档备案。

#### 系统日志管理

* 系统日志管理对象包括资鼎(上海)互联网金融信息服务有限公司信息系统的操作系统日志、应用系统日志及数据库日志；
* 维护人员应对网络设备、主机系统、安全设备的各种日志内容每周进行检查，从中分析可能存在的安全风险；
* 业务应用系统的责任部室负责每月对应用系统日志实施检查及分析工作；
* 系统日志应每月备份并存档，保存周期至少为半年。

#### 漏洞扫描

* 对重要业务系统需定期进行漏洞扫描以发现系统潜在的安全隐患，扫描对象包括服务器操作系统及数据库系统，并扫描完毕后提交扫描报告；
* 漏洞扫描工作由安全管理员负责组织实施，并负责扫描工具的管理工作。

#### 测试补丁回退

发现更新的补丁影响到了系统的正常运行，则需要进行回退工作，具体如下：

* 小型机系统恢复

小型机的系统退回，需要从备份磁带中导入已经备份好的操作系统，步骤如下：

* CMDFILE=/backup/bak/bak
* LOGFILE=/backup/bak/log
* su - oracle -c "rman nocatalog target / cmdfile $CMDFILE msglog $LOGFILE"
* bak
* run{
* sql 'alter session set NLS\_LANGUAGE = AMERICAN';
* CONFIGURE RETENTION POLICY TO REDUNDANCY 3;
* CONFIGURE CONTROLFILE AUTOBACKUP ON;
* CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '/backup/bak/%F';
* sql 'alter system archive log current';
* backup database format '/backup/bak/%d-D-%I-%T\_%t\_%s';
* crosscheck archivelog all;
* delete expired archivelog all;
* delete noprompt expired archivelog all;
* crosscheck backup;
* delete noprompt obsolete;
* backup current controlfile format '/backup/bak/%d\_C\_%I\_%T\_%t\_%s';
* backup spfile format='/backup/bak/%d-SP-%I-%T\_%t\_%s';
* }WINDOWS系统回退方案

从已经备份好的系统镜像中还原。

* ORACLE数据库回退方案
  + - 还原shen-db和shen-dw操作系统相关配置，同小型机；
    - 还原shen-db和shen-dw上/oracle/app/oracle下所有oracle软件，使用UNIX的tar命令，将备份的版本还原；
      * 清空/oracle/app/oracle目录
      * 通过如下指令还原老版本的oracle软件
      * Vgchange –a y vgrmantmp
      * Mount /dev/vgrmantmp/lvrmantmp /rmantmp
      * Cd /oracle/app/oracle
      * Tar xvf /rmantmp/shen-db\_oracle.tar
* 系统测试
  + - 按照《资鼎(上海)互联网金融信息服务有限公司-日常测试巡检操作手册》对设备和系统进行巡查。

### 恶意代码防范管理制度

安全管理员负责资鼎(上海)互联网金融信息服务有限公司的恶意代码防范工作，及发生恶意代码攻击时的应急处理。

* 统一设置IE浏览器中的Internet选项中的 Internet区域的安全级别，设定为高等级，并禁止用户修改；
* 一般情况下，不通过服务器直接登录公共站点访问，如有必要，须事先在其他电脑中登记访问网站，确保该网站的安全性；
* 在所有服务器中，如非必需，禁止开启ActiveX插件和控件、JAVA脚本等；
* 确保各服务器及工作站安装并及时更新网络防火墙，并确保“实时监控功能”的开启状态；
* 任何人不得擅自停用杀毒软件；
* 任何外来介质在接入计算机时均需要进行扫描防病毒处理；
* 不得擅自打开来路不明的邮件中的任何文件，在打开外来邮件包含的任意文件时均需要进行防病毒扫描；
* 严禁访问可能包含恶意代码的网站；
* 不得擅自启用未知网站的插件；
* 做好Windows 相关注册表的备份工作；
* 网络管理员要对IE或其他网络浏览器进行定期得打补丁或更新工作，在补丁更新前对补丁程序进行严格测试，在确保无危害情况下才可着手准备在生产环境中进行补丁升级。
* 在补丁升级前要填写补丁升级上报相关表格（附49），并得到上级领导批准后方可实施；
* 做好服务器和客户端计算机的防病毒工作。所购买使用的防病毒产品必须获得国家防病毒产品销售许可证；
* 做好防病毒产品的升级管理工作，并在每次病毒库升级前需要对升级库进行安全评估，确保无问题方可在生产环境中进行升级，并做好相关记录
* 每次对病毒查杀后需要进行汇总。
* 每周进行一次恶意代码安全性评估，对根据安全评估结果进行相关安全修补工作。
* 定期就恶意代码安全防护对所有工作人员进行培训教育工作，并体现在资鼎(上海)互联网金融信息服务有限公司年度培训计划表中；

### 密码使用管理制度

安全管理员负责资鼎(上海)互联网金融信息服务有限公司的密码使用管理工作，包括密码的保管、分配、修改、授权。

* 服务器、网络设备及其他相关设备由专人管理，服务器无人操作时应置于锁定状态；
* 对服务器、网络设备及其他相关设备的任何软、硬件修改都必须事先向主管部门提交书面申请，征得主管部门负责人许可并签字后方可进行，并按规定书写管理日志，经操作人员签字后备案；
* 服务器、网络设备及其他相关设备的超级用户的口令由专人设置、统一保管、定期更改；
* 未经主管部门许可任何人不准对非相关人员泄漏服务器、网络设备及其他相关设备的登录帐号以及口令；
* 服务器、网络设备及其他设备的远程接入或远程管理帐户与口令由专人设置、统一保管，使用前必须事先向主管部门提交书面申请，征得主管部门负责人许可并签字后方可使用，使用完毕应立刻告知系统管理员，由系统管理员收回并重新设置；
* 凡掌握服务器、网络设备及其他设备的高权限帐户的人员离职或调离岗位，必须通知主管部门以及时更换相应口令。

### 信息系统变更管理制度

资鼎(上海)互联网金融信息服务有限公司信息安全领导小组负责一级变更的审核。

资鼎(上海)互联网金融信息服务有限公司信息安全工作小组负责二级变更的审核。

资鼎(上海)互联网金融信息服务有限公司信息系统管理员负责系统的变更实施。

* 变更申请人识别具体的变更需求（如范围、可交付成果、时限、组织等），填写《变更申请表》，交给变更审批人进行审批；
* 相应的变更审批人对变更申请进行审核，如判断此变更属于日常变更，由日常变更审批人审批后自行组织实施；如属于重大技术变更，则提交资鼎(上海)互联网金融信息服务有限公司信息安全领导小组审批；
* 变更审批人组织制定变更实施计划，包括变更前的备份、变更计划、实施人员、实施流程、所用工具、回退计划、回退不成功的应急预案等；
* 变更实施前由变更实施人员进行备份，变更实施后进行变更情况记录；
* 如为重大变更，变更实施前由相关人员进行实施测试，并对测试情况进行记录，测试通过后方可实施；
* 变更实施前通知所有将受变更影响的用户；
* 如变更不成功，立即按照变更实施计划中的回退计划实行变更回退过程，使其状态回到变更前的状态，并进行记录；
* 变更完成后由变更实施人员进行后期跟踪及反馈，并进行记录。

#### 变更的分级和审核

根据变更的规模、变更的风险、变更的范围等要素，将变更分为二级，针对二级变更的分类准则及审核要求为：

* 一级变更

涉及到应用系统核心部分的变更，包括软硬件及应用系统几个方面，主要有硬件的变更、安全配置的变更、体系架构的变更、系统软件的变更等，一级变更是指资鼎(上海)互联网金融信息服务有限公司系统核心设备的变更、或该变更会影响到整个系统，一级变更必须经管理员审核，资鼎(上海)互联网金融信息服务有限公司主任审批。

* 二级变更

涉及到应用系统的重要变更，包括软硬件及应用系统几个方面，主要有硬件的变更、安全配置的变更、体系架构的变更、系统软件的变更等，二级变更是指资鼎(上海)互联网金融信息服务有限公司系统重要设备的变更、或该变更会对系统由局部影响，二级变更必须经过安全工作小组审批。

* 三级变更

涉及到健康档案应用系统的一般变更，包括软硬件及应用系统几个方面，主要有硬件的变更、安全配置的变更、体系架构的变更、系统软件的变更等，二级变更仅对部室内部产生影响，三级变更必须经过系统管理员审批。

#### 变更管理控制

* 主机变更
  + 1. 资鼎(上海)互联网金融信息服务有限公司主机硬件变更和硬件配置的变更需求根据中心业务发展的需要提出，填写《变更申请表》（见附50），制定变更方案；
    2. 资鼎(上海)互联网金融信息服务有限公司相关负责人应进行业务及技术可行性分析，要求保证关键业务的可靠性和处理性能。交资鼎(上海)互联网金融信息服务有限公司相关审核人审核，必要时需组织相关部室和专家评审。并根据变更的级别进行审批后实施；
    3. 实施结束后，资鼎(上海)互联网金融信息服务有限公司相关负责人应组织测试与验收，将相应报告报资鼎(上海)互联网金融信息服务有限公司相关审核人，必要时资鼎(上海)互联网金融信息服务有限公司相关审核人可组织对结果进行再确认；
* 网络变更
  + 1. 管理中心网络硬件、网络设备配置、网络架构的变更根据业务发展的需要提出，并填写《变更申请表》。
    2. 涉及网络硬件、网络设备配置、网络构架改造，复杂的变更应制定变更方案，资鼎(上海)互联网金融信息服务有限公司相关负责人应进行业务及技术可行性分析，必须考虑改造对现有业务的影响，并制定有效的风险控制措施，交资鼎(上海)互联网金融信息服务有限公司相关审核人审核，必要时需组织相关部室和专家评审，并根据变更的级别进行审批后实施；
    3. 管理中心网络硬件、网络设备配置、网络架构的变更后，变更管理部室应组织测试与验收，将相应报告报网络管理员，必要时网络管理员可组织对结果进行再确认；
* 系统软件的变更
  + 1. 资鼎(上海)互联网金融信息服务有限公司相关负责人负责管理中心系统软件的安装及升级，保证安装过程的完整安全；
    2. 资鼎(上海)互联网金融信息服务有限公司核心主机和网络设备的操作系统的安装及升级，必须制定安装及升级方案，交资鼎(上海)互联网金融信息服务有限公司相关审核人审核，必要时需组织相关部室和专家评审,并根据变更的级别进行审批后实施；
    3. 变更实施前应进行安全测试，确保变更不会影响到当前业务系统的运行；
    4. 变更实施前应制定好不成功变更的恢复措施；
    5. 一般情况下，不允许员工使用其自行下载的升级包，以保证员工工作机的安全。
    6. 设置完备的测试环境。软件、补丁等软件变更实施之前，在测试服务器中安装及测试，测试完成之后对系统的稳定性及软件运行情况进行评估，满足使用要求并对系统无影响，再进行变更。

#### 变更实施的安全要求

* 在变更实施之前，将重要的数据、系统软件进行备份，以便变更不成功之后的恢复；
* 在变更实施之前，应和各部门协商，以便确定适当的变更时间，尽可能的将对业务的影响减至最低。
* 在变更实施之前，需要准备相应设备的备品备件，以防实施过程中因设备故障对业务造成影响。

#### 变更验收与记录

* 当变更成功提交后，需由相关人员进行验收，确认其是否已完成所提的要求，达到预期的效果，并记录此次变更操作。

#### 变更后软件和资料的备份要求

* 变更完成后，需将此次所运行的软件进行备份，包括其相关资料，以便下次的再一次变更以及资料查询；
* 对变更涉及到的资料文档，作好相应的变更并存档。

#### 变更不成功的恢复措施

* 取消所做变更，从备份资料中获得原始软件资料，重新运行，恢复原始状态；
* 根据变更操作记录，查找变更失败原因，以便再次做变更操作时避免同样的错误发生。

# 备份与恢复管理制度

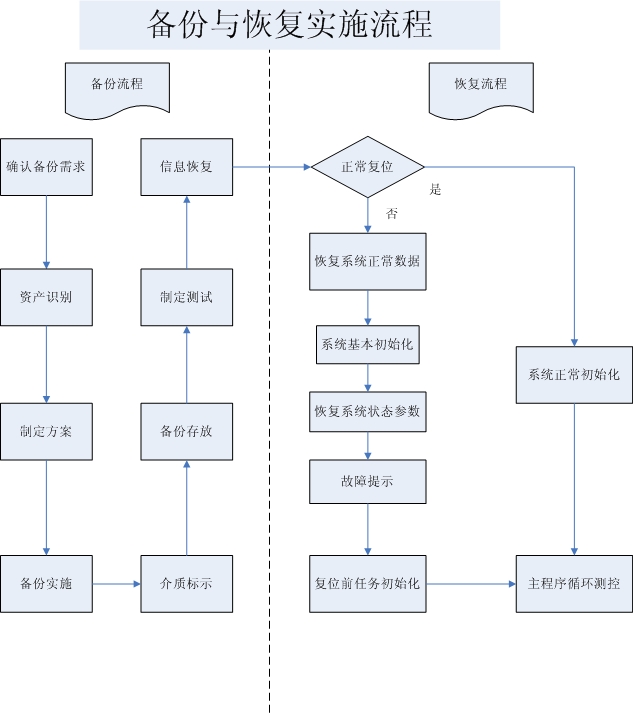
## 备份与恢复管理制度

主机管理员负责资鼎(上海)互联网金融信息服务有限公司数据备份与恢复管理工作，主要包括：

* 负责执行资鼎(上海)互联网金融信息服务有限公司数据备份与恢复管理工作，针对不同类型的数据制定相应的备份及恢复策略；
* 负责系统备份和恢复性测试具体实施工作，负责备份介质的选择、恢复性测试、日常维护等工作。

### 备份制度流程图

备份制度流程图如下所示：



### 资产识别

* 收集需要备份的资产相关信息，主要包括资产的重要性、资产的保护级别等属性；对确定的重要业务数据、操作系统、应用系统、数据库等进行备份。需要检查的信息资产可能包括：业务运作数据；重要的信息数据；操作系统；系统配置参数；技术文件；档案资料；应用软件；软件源代码等；
* 无法备份的信息，尽量多使用其复制件，保存原件。

### 备份方案

* 确定备份周期

根据信息更新速度、易损坏成度及备份介质的有效期，确定周期。

* 确定备份介质类型

确定备份使用的介质，一般是光盘、软盘或硬盘，要同时考虑成本与可靠性。

* 确定备份方式

一般采用复制、双系统同步、转储、压缩复制等。

* 确定备份工具

备份使用的工具，如光盘记录机、复印机、压缩软件等，选择工具时，要确定在信息失效之前，对应的恢复工具可用。

* 确定备份数量

确定备份的数量，一般信息备份一份即可，对于特别重要的信息需要备份多份。

* 存放位置

备份信息须与原始信息分开存放，要根据信息保密级别有相应的保密措施。

* 命名规则

对于备份文件命名，应遵循备份设备名+备份内容+备份时间的方式来命名。

* 责任人：确定备份的责任人。
* 备份方案需提交给相关部门负责人，经部门主任确认并批准后予以实施。
* 当责任人没有足够的工具或条件时，可要求相关工程师协助。

### 备份计划实施

对分散的信息进行整理、归类；处理信息，在备份信息前，先将其复制到有备份工具的计算机上；执行备份程序；检查备份数据的可用性；清理过程数据。

### 备份的介质标识

* 标识应依据介质本身的特点，加标签或直接手写在介质上；对于已经有标识的纸面文档的复印件，可不用再另加标识；各部门应采取适宜的方法对备份信息介质进行标识，防止备份信息的误用，标识的内容包括：备份信息的名称；备份的日期；版本号；必要时，备份还原工具；
* 考虑信息本身在被使用时的特点，确定标识的内容；
* 做好数据备份的文卷管理，所有备份应有明确标识、包括卷名、运行环境、备份人。

### 备份介质的安全存放

* 备份完毕，备份操作员需向部门主任或备份管理人员提交备份成果：备份介质；备份过程中的相关文件，如：备份记录文件(详见附51)、备份恢复工具或软件等；将备份介质保存到指定的位置，需按时间顺序存放；

备份介质须保存在适宜的环境中；对备份介质进行异地存储，以避免主要场地发生灾难时资产受到损坏；备份介质存储场地的物理和环境保护；分配专人对备份介质进行管理，对备份介质的访问进行控制；

* 定期(每半年一次)测试备份介质，以确保应急使用时可以使用这些备份介质。

### 信息恢复

当重要信息被篡改、破坏或丢失时，使用备份数据恢复信息；当存在多份备份时，应根据需要选择合适的备份；备份信息使用前，应检查备份信息的完整性和可用性。

应对重要业务数据建立备份数据的恢复程序，如遇服务器遭受攻击或网络病毒，造成数据丢失或系统崩溃，需要进行数据恢复，应由系统管理员执行恢复程序，同时将具体情况做记录。（详见附52）

* 备份数据的恢复测试：
  + - 备份数据的恢复测试是指定期对已备份的重要业务数据进行恢复测试，以验证备份恢复策略及备份文件的可用性及准确性，测试完成后应由系统管理员对测试结果进行记录，并由相关负责人检查确认。
    - 系统管理员应每半年进行一次备份恢复演练，并记录演练的结果，填写《备份与恢复演练记录单》（详见附53），按演练实际情况更改相关的备份与恢复文档，以准确反映操作过程。
    - 系统管理员应定期或不定期抽样部分备份数据进行恢复，以检查备份数据是否可用，是否被更改或删除。

# 信息系统安全事件管理制度

## 信息系统安全事件管理制度

安全管理员负责资鼎(上海)互联网金融信息服务有限公司信息系统安全事件管理工作，主要包括：

* 负责重大信息安全事故的处理和信息安全的奖惩；
* 负责中等信息安全事故和信息安全故障的处理，负责组织信息安全薄弱点的识别和预防措施的实施；
* 负责有关计算机系统平台、系统软件的安全事故的处理和纠正；
* 负责有关计算机系统应用软件以及相关工具软件的安全事故的处理和纠正；
* 负责有关计算机系统数据库以及相关工具软件的安全事故的处理和纠正；
* 负责消防、供电有关安全事故的调查、处理和纠正，确保对主机房的能源支持；
* 负责涉及资鼎(上海)互联网金融信息服务有限公司信息泄露调查、处理及纠正；
* 负责定期对薄弱点、故障及事故的相关记录进行分析、总结和学习。

### 安全事件定义

网络与信息安全事件一般可以分为攻击类、故障类和灾害类等，可能造成的后果是业务中断、系统宕机、网络瘫痪、信息破坏等。根据资鼎(上海)互联网金融信息服务有限公司的“马上货”系统系统安全事件的发生原因、性质和机理，网络与信息安全事件主要分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障和灾害性事件五类：

* 有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件；
* 网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件；
* 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件；
* 设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障；
* 灾害性事件是指自然灾害等其他突发事件导致的网络和信息系统故障。

### 安全事件等级划分

根据信息安全事件的分级考虑要素，将信息安全事件划分为四个级别：特别重大事件、重大事件、较大事件和一般事件。

* **特别重大事件**

指能够导致特别严重影响或破坏的信息安全事件，包括以下情况：会使特别重要信息系统遭受特别严重的系统损失；产生的社会影响会波及到全市的大部分地区，威胁到国家安全，引起社会动荡，对经济建设有极其恶劣的负面影响，或者严重损害公众利益。

* **重大事件**

指能够导致严重影响或破坏的信息安全事件，包括以下情况：

会使特别重要信息系统遭受严重的系统损失；或使重要信息系统遭受特别严重的系统损失；产生的社会影响波及到全区的大部分地区，对经济建设有重大的负面影响，或者损害到公众利益。

* **较大事件**

指能够导致较严重影响或破坏的信息安全事件，包括以下情况：会使特别重要信息系统遭受较大的系统损失；或使重要信息系统遭受严重的系统损失、一般信息信息系统遭受特别严重的系统损失；扰乱社会秩序，对经济建设有一定的负面影响，或者影响到公众利益。

* **一般事件**

指能够导致较小影响或破坏的信息安全事件，包括以下情况：会使特别重要信息系统遭受较小的系统损失；或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重的系统损失；对国家安全、社会秩序、经济建设和公众利益基本没有影响，但对个别公民、法人或其他组织的利益会造成损害。

### 安全事件处理流程

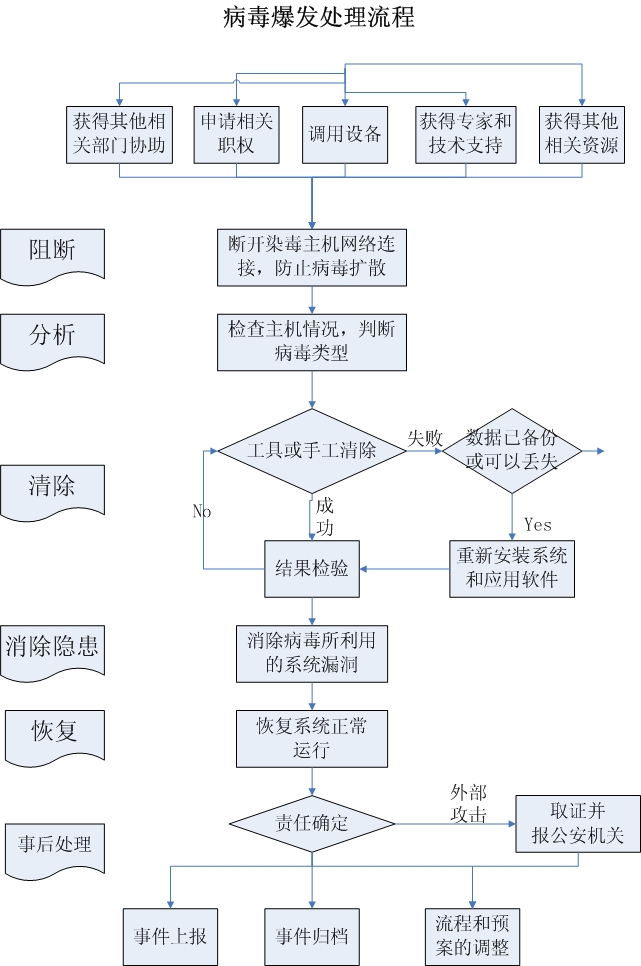
出现事件后安全管理员要及时通过电话、传真、邮件、短信等方式通知单位领导及相关技术负责人。

安全管理员根据事件信息，初步判定事件等级。能够自身解决，要及时加以解决；如果不能自行解决故障，由相关负责人现场指挥，按照分工负责的原则，组织相关技术人员进入抢险程序。

#### 病毒爆发处理流程

对外服务信息系统一旦发现感染病毒，应执行以下应急处理流程：

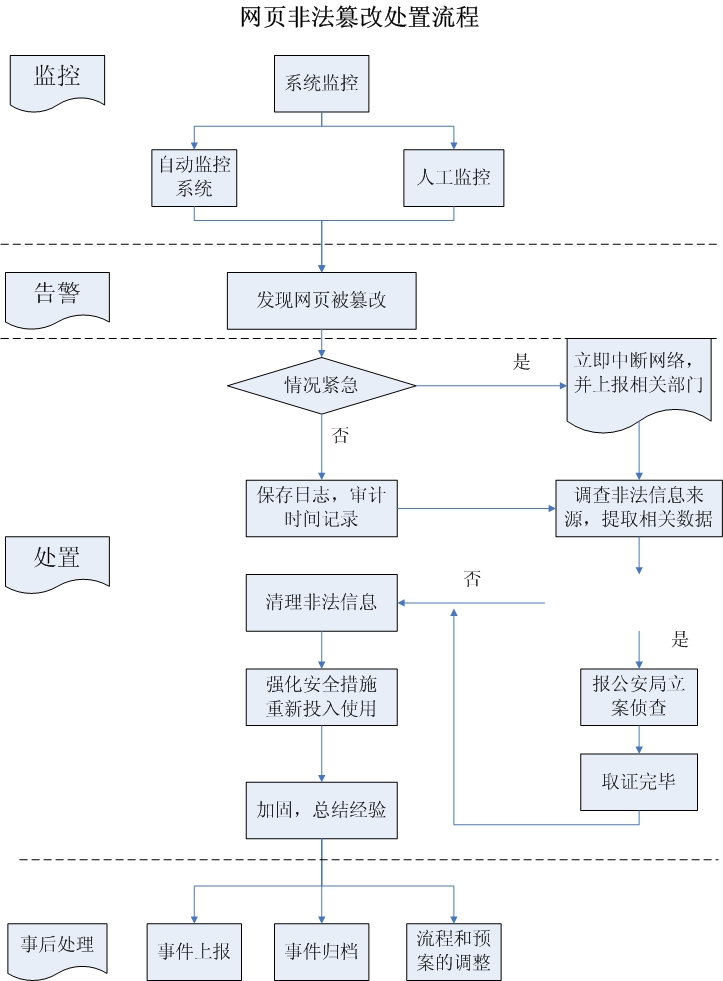
* 立即切断感染病毒服务器与网络的联接；
* 对该服务器的重要数据进行数据备份；
* 启用防病毒软件对该服务器进行杀毒处理，同时通过防病毒软件对其他服务器进行病毒扫描和清除工作；
* 如果满足下列情况之一的，应立即向相关负责人通报情况，并向资鼎(上海)互联网金融信息服务有限公司报告：
* 现行防病毒软件无法清除该病毒的；
* 杀毒软件在2小时内无法处理完毕的；
* 业务系统或办公系统在4小时内无法恢复正常的；
* 恢复系统和相关数据，检查数据的完整性；
* 病毒爆发事件处理完毕，将服务器重新接入网络；
* 总结事件处理情况，并提出防范病毒再度爆发的解决方案；
* 实施必要的安全加固。



#### 网页非法篡改处理流程

对外服务网站一旦发现网页被非法篡改，应执行以下应急处理流程：

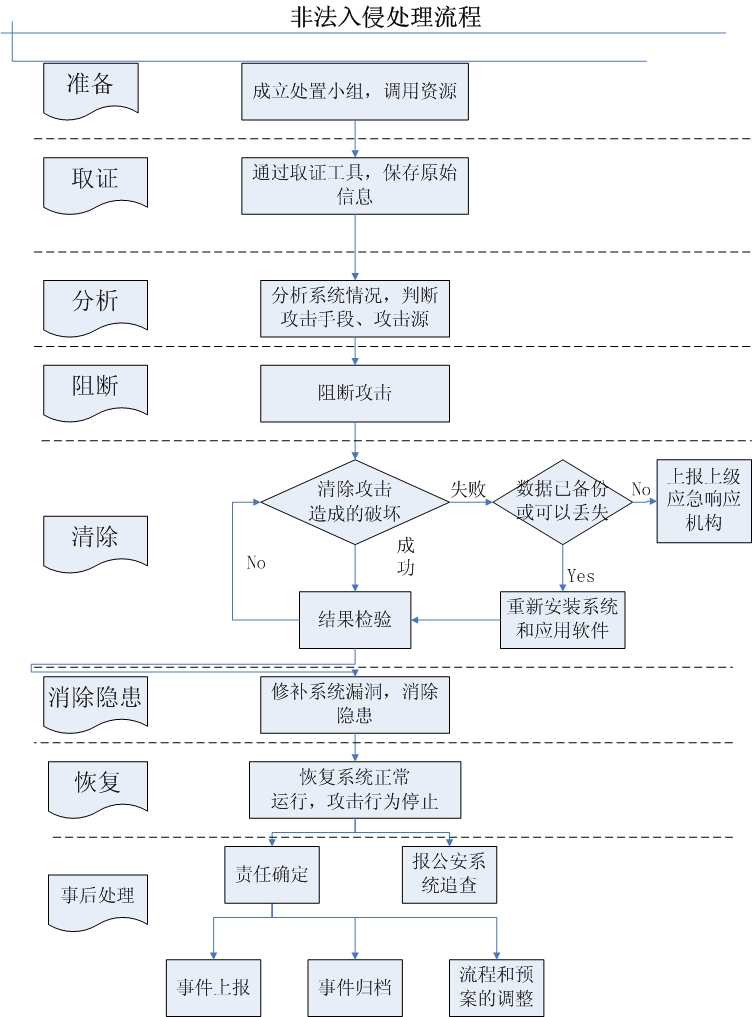
* 发现网站网页出现非法信息时，网络管理员应立即向资鼎(上海)互联网金融信息服务有限公司信息安全负责人通报情况。情况紧急的，应先及时采取断网等处理措施，再按程序报告；
* 信息安全管理员应在接到通知后立即赶到现场，做好必要记录，妥善保存有关记录及日志或审计记录（详见附54）；
* 相关技术人员应在接到报告后2小时内赶到现场，追查非法信息来源。资鼎(上海)互联网金融信息服务有限公司研发部做好各种相关的配合工作，必要时协调相关部门或公司来协助解决；
* 在提取相关数据样本后，清理网站非法信息，强化安全防范措施，然后将网站重新投入使用。如情节严重，构成违法犯罪的，由市公安局网监处立案侦查；
* 总结事件处理情况，向资鼎(上海)互联网金融信息服务有限公司备案，并提出防范再度发生的解决方案；
* 实施必要的安全加固。



#### 非法入侵处理流程

对外服务信息系统一旦发现被远程控制等非法入侵行为，应执行以下应急处理流程：

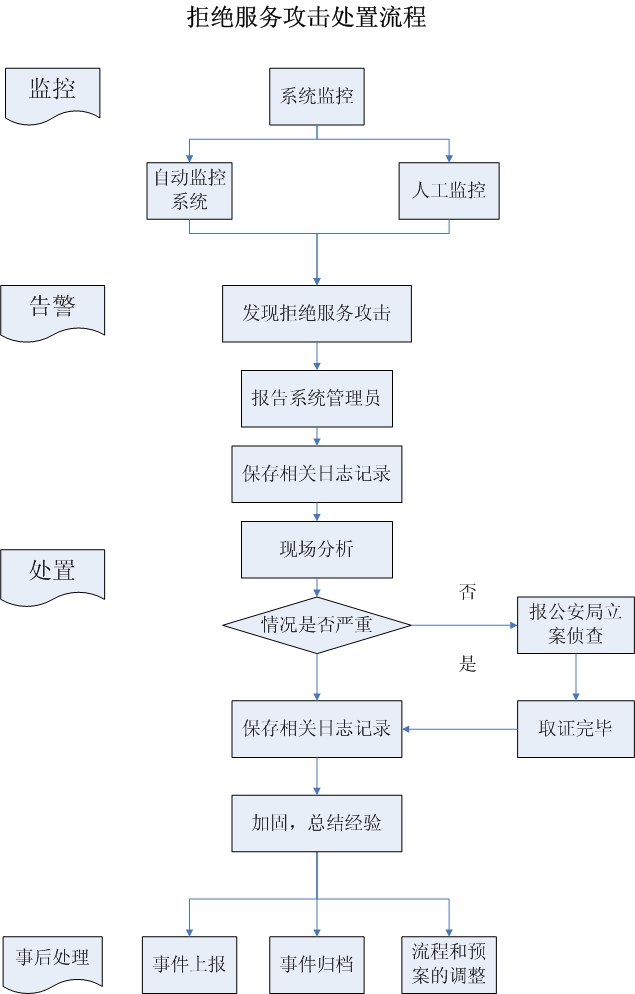
* 发现系统服务器被远程控制、植入后门程序，或发现有黑客正在进行攻击时，应立即向资鼎(上海)互联网金融信息服务有限公司安全管理员通报情况，并立即向市公安局网监处和资鼎金服报告；
* 如服务器已被入侵，将被攻击的服务器等设备从网络中隔离出来，保护现场；
* 信息安全管理员应在接到通知后立即赶到现场，做好必要记录，妥善保存有关记录及日志或审计记录（详见附54）；
* 相关技术人员对入侵事件应在接到报告2小时内赶到现场；对业务系统和办公系统事件应在接到报告4小时内赶到现场，对现场进行分析，追查攻击源，修改防火墙等设备的安全配置阻断黑客继续入侵。相关单位做好相关的配合工作，必要时协调相关部门或公司来协助解决；
* 分析后台数据库操作日志，判断是否发生数据失窃。检查、校验数据的完整性和有效性；
* 在提取相关数据样本后，恢复与重建被攻击或破坏的系统。如情节严重，构成违法犯罪的，由市公安局网监处立案侦查。重新将恢复后的对外服务系统接入网络；
* 总结事件处理情况，向资鼎(上海)互联网金融信息服务有限公司备案，并提出防范再度发生的解决方案；
* 实施必要的安全加固。



#### 拒绝服务攻击处理流程

各单位对外服务信息系统一旦发现遭受DDoS等拒绝服务攻击，无法正常访问时应执行以下应急处理流程：

* 发现对外服务系统访问流量异常、无法正常访问，可能遭受拒绝服务攻击时，应立即向资鼎(上海)互联网金融信息服务有限公司安全负责人通报情况，并立即向市公安局网监处和资鼎金服报告；
* 信息安全管理员应在接到通知后立即赶到现场，做好必要记录，妥善保存有关记录及日志或审计记录（详见附54）；
* 相关技术人员对拒绝服务事件应在接到报告2小时内赶到现场；对业务系统和办公系统事件应在接到报告4小时内赶到现场，对现场进行分析，追查攻击源，修改路由器、防火墙等设备的安全配置，缓解、消除拒绝服务攻击的影响。相关部门做好相关的配合工作，必要时协调专业公司来协助解决；
* 在提取相关数据样本后，恢复对外系统正常运行。如情节严重，构成违法犯罪的，由市公安局网监处立案侦查；
* 总结事件处理情况，向资鼎(上海)互联网金融信息服务有限公司备案，并提出防范再度发生的解决方案；
* 实施必要的安全加固。



#### 机房物理环境事故应急处理流程

* 供电故障

如果出现短路：切断电源，更换短路器件，恢复供电；

如果出现断路：切断电源，连接断开线路，恢复供电；

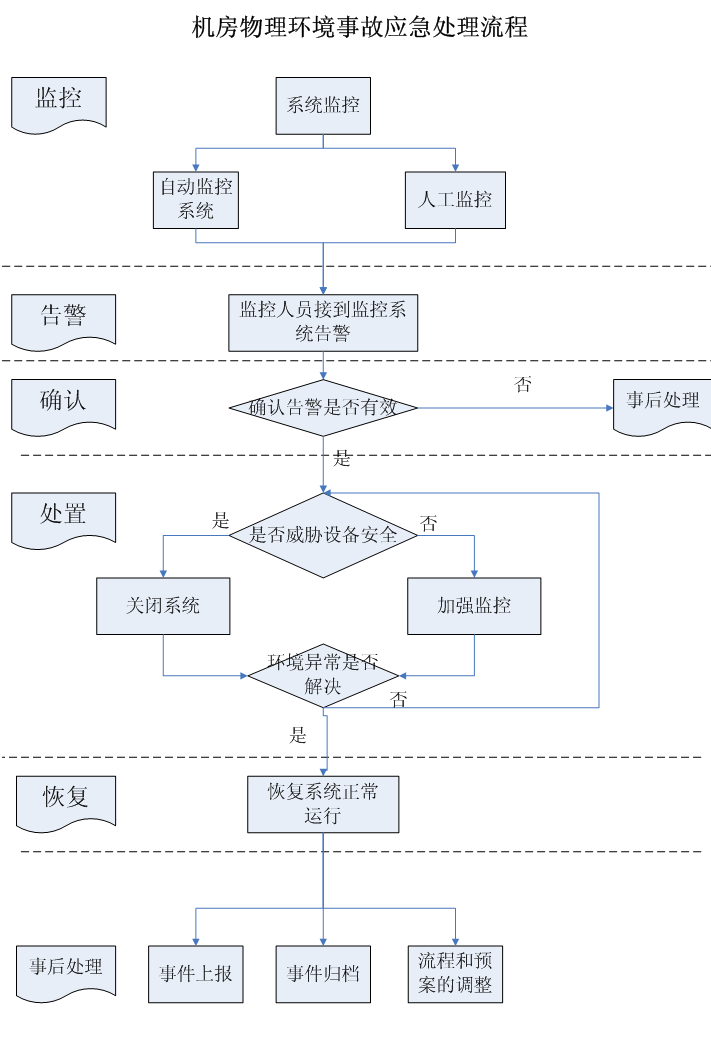
防雷防静电设备故障：切断电源，跳过防雷防静电设备直接供电，及时维修损坏设备并更换；UPS故障，跳过逆变输出，及时维修损坏设备并更换；

* 火灾

切断电源，使用灭火器灭火；向119指挥中心报告火警，请求支援；如有人员遇险，应先救人后救物；

* 水渗故障

切断电源，更换浸水设备，采取防水渗措施。



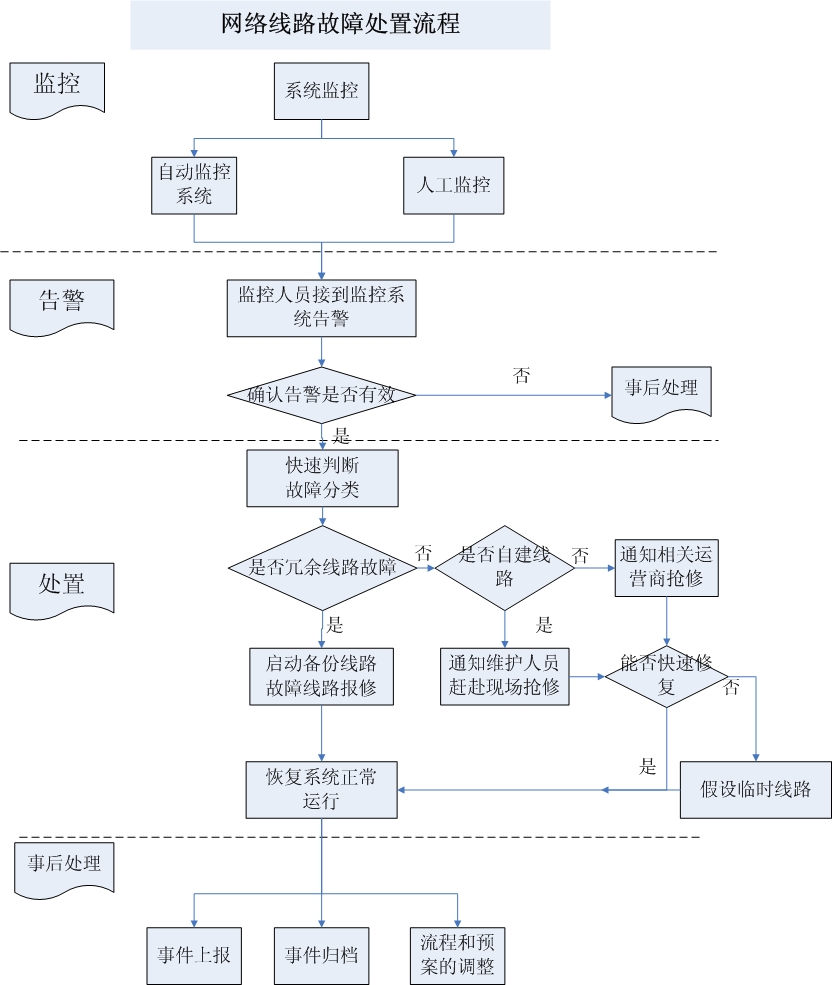
#### 网络线路故障应急处理流程

* 内部线路故障

如果有环路或冗余线路，通过自动路由或手动设置、联接等技术措施保障网络畅通。对于需要抢修的线路，如果属于自建线路，维护人员赶赴现场抢修；如果是租用其它电信运营商的线路，通知相关运营商及时抢修；如果线路无法修复，协调架设临时线路。

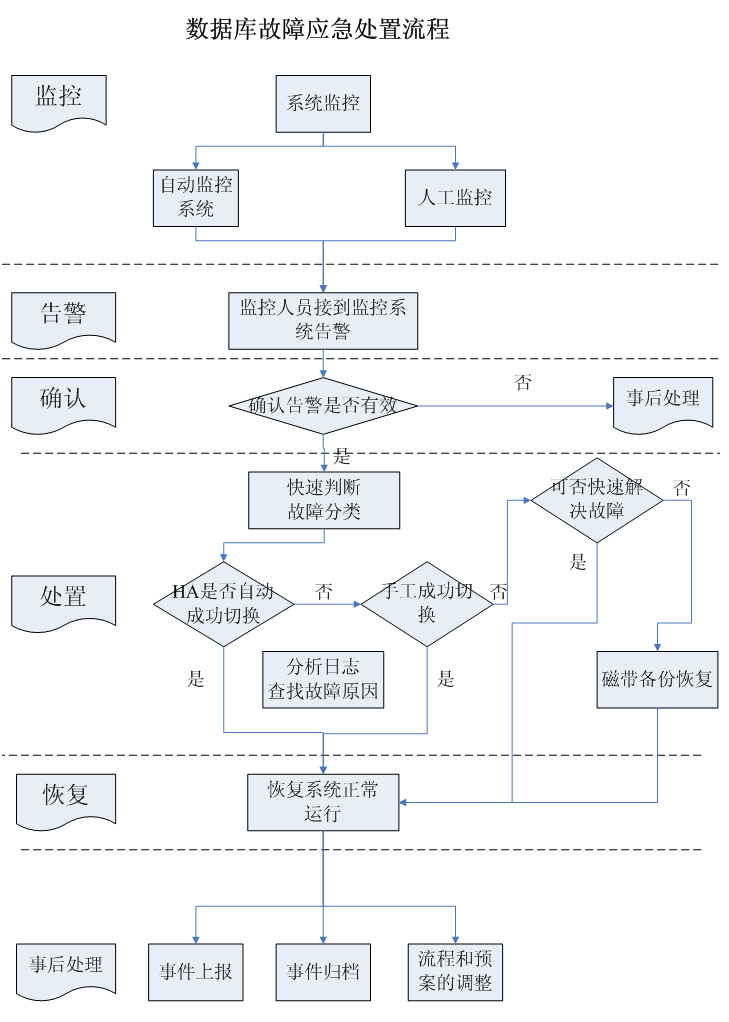
* 互联网出口线路故障

启用备份线路，通知线路维护人员及时抢修。



#### 数据故障应急处理流程

数据丢失或损坏：从数据备份服务器上提取数据，尽快恢复，保证系统在最短时间内能够正常运行；分析造成事故的原因，针对具体问题，采取相应安全策略。



#### 安全事件恢复

* 安全事件的恢复由各系统管理人员负责，并会同各兄弟单位、专家一起对安全事件产生的结果进行尽快恢复；
* 对于病毒、恶意代码、网页、非法入侵、拒绝服务等攻击行为需要对涉及设备进行全面安全检查，因以上原因引起系统不能正常运行则可采用重新安装系统、升级补丁、由供应商人员等方法解决；
* 对于机房、网络线路故障的恢复，需要会同线路提供单位共同解决；
* 当灾难降临、系统或设备发生故障、数据被破坏或丢失时，应及时向上级报告，并在最短的时间内，用备份的数据来恢复整个系统，最低限度减少损失，使系统提供正常的服务。
* 数据的恢复要由专人负责数据恢复工作，并认真填写恢复日志。一旦发生数据丢失或数据破坏等情况，要由应用管理员进行数据的恢复并做好记录。
* 对于安全事件，如短时间不能解决，需要提供备份解决方案，提供备份链路；

### 安全事件报告流程

* 当发生安全事件时，信息系统管理员或维护人应立即在第一时间向研发部口头通知事件情况，说明事件发生的时间、部位、表象、程度和影响；
* 发现安全事件时应立即组织人员开展抢修工作，1小时后仍未恢复时，立即向资鼎(上海)互联网金融信息服务有限公司领导汇报；根据事件严重程度，也可由资鼎(上海)互联网金融信息服务有限公司相关负责人向上级主管领导报告。

#### 事件调查报告

* 发生重大信息安全事件，应在3个有效工作日内将书面《信息安全事件调查报告》报资鼎(上海)互联网金融信息服务有限公司主管领导，由领导审定后，在5个有效工作日内，将审核意见及报告上报上级的分管领导审批。
* 较大信息安全事件，应在5个有效工作日内将书面《信息安全事件调查报告》（详见附55）报资鼎(上海)互联网金融信息服务有限公司领导领导审批。
* 一般信息安全事件，应在3个有效工作日内将书面《信息安全事件调查报告》报资鼎(上海)互联网金融信息服务有限公司负责人审批。
* 信息系统故障，应在当天将故障情况登记在册，内容包括故障发生、处理经过和简要原因分析。在一个月内同一部位连续发生同一故障3次，按一般信息安全事件处理。

#### 安全事件的后期教育与培训

* 安全事件发生以后，需要整理相关资料，并总结经验，就事件处理经验交流，并就事件进行相关人员教育工作，以免再犯此类错误；
* 每半年进行一次安全事件教育工作，并加入到每年度的培训计划中，对全体工作人员进行相关教育；

# 硬件维护日常操作管理规程

## 硬件维护日常操作管理规程

### 交换机

1.用管理员帐号登录交换机，查看系统日志，检查是否有异常和严重的报错信息；

2.在系统内用命令行方式检查交换机每块背板和电源状态是否正常，并做记录（见附56）；

3.在系统内用命令行方式检查交换机硬件资源如CPU、内存的利用率是否正常，并做记录；

4.在系统内用命令行方式检查交换机各个网络接口、VLAN、路由和网络通讯等状态是否正常，并做记录；

5.如果交换机有异常情况或者进行配置修改需要做好记录。

### 路由器

1.用管理员帐号登录路由器，查看系统日志，检查是否有异常和严重的报错信息；

2.在系统内用命令行方式检查交换机每块背板和电源状态是否正常，并做记录（见附56）；

3.在系统内用命令行方式检查交换机硬件资源如CPU、内存的利用率是否正常，并做记录；

4.在系统内用命令行方式检查交换机各个网络接口、路由和网络通讯等状态是否正常，并做记录；

5.如果路由器有异常情况或者进行配置修改需要做好记录。

### 防火墙

1.通过Web界面用管理员帐号登录各个防火墙，查看系统日志，检查是否有异常和严重的报错信息；

2.在系统内检查防火墙硬件资源如CPU、内存的利用率和会话连接数是否正常，并做记录（见附56）；

3.在系统内检查防火墙各个网络接口、路由和网络通讯等状态是否正常，并做记录；

4.在系统内检查防火墙安全策略是否正常，并做记录；

5.如果防火墙有异常情况或者进行配置修改需要做好记录。

### 小型机

1.用管理员帐号登录Oracle核心数据库主机小型机，查看系统日志，检查是否有异常和严重的报错信息；

2.在系统内用命令行方式检查主机CPU、内存、硬盘、网卡、HBA卡和电源等硬件部件状态是否正常，并做记录（见附56）；

3.在系统内用命令行方式检查主机硬件资源如CPU、内存、硬盘、换页空间和文件系统的利用率是否正常，并做记录；

4.在系统内用命令行方式检查主机各个网络接口、网络通讯和群集等状态是否正常，并做记录；

5.如果主机有异常情况或者进行配置修改需要做好记录。

### PC服务器

1.在机房现场查看PC服务器的运行情况，查看液晶面板上是否有报错信息；

2.查看服务器的CPU、内存、硬盘和电源等部件是否有故障；

3.如果有异常情况或者进行配置修改需要做好记录（见附56）。

### 审计系统

1.登录审计系统，查看资鼎(上海)互联网金融信息服务有限公司的“马上货”系统网络设备运行情况；

2.查看资鼎(上海)互联网金融信息服务有限公司的“马上货”系统网络链路情况；

3.如果有异常情况或者进行配置修改需要做好记录。（见附56）

# 信息系统操作规程

## 信息系统操作规程

### 服务器设备操作规程

* 必须放置于通风良好、消防设施齐全的房间，并由专人看管；
* 关键应用提供双机热备机制，提高系统整体可靠性；服务器上的数据定期备份，由相关人员执行备份操作；
* 服务器管理员口令需要定期(每季度一次)更换；
* 定期(每日一次)对服务器运行情况进行监控，包括CPU利用率、磁盘使用情况等；
* 机房内投入工作的服务器中存储有重要的数据，只有经过专业培训的工作人员才允许对服务器参数进行调整或对硬件设施进行维护，任何来宾未经许可不得擅自进行操作、修改，非系统管理员需要对服务器进行操作，在使用前必须征得相关责任人同意方可进行，即便经过允许或授权也要保证计算机内原有数据的完整性可系统的可运行性，否则引起的损失，由当事人承担一切责任；
* 管理员口令必须妥善保管，临时离开管理员界面时必须锁屏；
* 对服务器进行维护前，通知用户服务器需中断的时间；
* 在修改服务器系统的过程中，必须记录详细的工作日志（见附57）；
* 在修改服务器状态前必须确保所作的修改操作或新安装的软件不会对遭受软件功能造成损伤。修改过程中必须对所修改的参数记录，以方便查错和参数恢复；修改后必须对服务器进行功能测试，查看其运行状态是否正常、新软件是否运行正常；
* 软件公司来对服务器数据更新、版本升级、或者安装新软件，必须遵守本制度，方可开展相关工作；

### 网络设备操作规程

* 管理人员必须遵守资鼎(上海)互联网金融信息服务有限公司的各项规章制度，遇到紧急情况，应及时通知有关主管领导，并做好工作日志，日志必须保存60天；
* 只有经过专业培训的工作人员才允许对网络设备参数进行调整或对硬件设施进行维护；
* 路由器、交换机和服务器以及通信设备是网络的关键设备，须放置计算机机房内，不得自行配置或更换，更不能挪作它用；
* 管理人员负责安装、调试、新建、扩建、升级网络中的路由器、各类交换机、集线器及光纤收发器、网络通信线路（包括光缆、双绞线、无线设备）、管理中心接入设备，随时监控网络的运行状态、及时处理网络故障、恢复网络的正常运行；
* 管理人员定期检查网络设备的运行情况。主交换机、防火墙、路由器等重要设备至少每天检查一次，其他设备至少每周检查一次，并做好检查记录；（见附58）
* 管理人员定期备份网络设备的配置，管理人员和主管人员不准透露配置和口令，以保障网络的安全运行，定期(每季度一次)修改网络设备的管理口令；
* 网络设备出现问题应及时解决，并做好相关记录，注明问题的现象、问题的产生原因及其解决方法。若出现重大问题，如违法性网络行为、黑客行为、主干网瘫痪等，应立刻向主管领导汇报；
* 网络设备进行维护前，应通知用户网络需中断的时间；
* 硬件设施维护规程：  替换热插拨器件时，首先从系统中卸载要变更的器件，然后再进行插拨操作；替换的新器件，在固定好后，再通过系统参数使之生效；替换非热插拨器件时，首先关闭电源，然后对替换的器件进行替换操作，替换新器件并固定后，最后在参数界面中配置参数，使之生效；如有可能，在不影响业务的前提下尽量都先关闭电源后操作；
* 网络设备系统参数维护过程：在修改的过程中必须记录详细的工作日志；在修改设备参数前必须记录原始参数状态，备份配置文件；在修改过程中必须对修改的参数记录，以方便查错和参数恢复；修改后，必须对整个设备进行功能测试，保证其运行状态正常；正常运行后，备份配置文件，并整理此次更改日志。

# 应急机构

## 应急机构及角色设置

安全应急小组是安全事件的应急响应机构，细分为应急领导小组、应急协调小组、应急实施小组，以及外部应急协助组。

### 应急领导小组

应急领导小组是信息安全事件应急处理的领导机构，决定和部署应急管理工作，具体负责信息安全事件应急响应过程中的决策指挥。应急领导小组的具体职责是：

（1）提出运行维护和应急响应的具体要求；

（2）监督检查运行维护和应急响应的工作落实情况；

（3）应急预案的批准；

（4）应急预案的启动或终止决定；

（5）应急事件的决策指挥；

（6）对应急处置过程重大事项进行协调；

（7）应急事件信息发布。

|  |  |  |  |
| --- | --- | --- | --- |
| 角 色 | 职务 | 姓名 | 电 话 |
| 应急领导小组组长 |  |  |  |
| 应急领导小组副组长 |  |  |  |

### 应急协调小组

应急协调小组是信息安全事件日常管理和应急响应的行政管理机构。应急协调小组的具体职责是：

（1）负责具体管理信息安全事件应急响应工作，包括平时演练的布置与安排；

（2）负责信息安全事件应急响应中，人力资源、财力资源、运输设备等的调用调度；

（3）负责信息安全事件应急响应中事件现场的秩序管理、安全保卫等；

（4）负责信息安全事件应急结束后的事故调查、责任追究工作。

|  |  |  |  |
| --- | --- | --- | --- |
| 角 色 | 职 务 | 姓 名 | 电 话 |
| 应急协调小组组长 |  |  |  |
| 应急协调小组组员 |  |  |  |
| 应急协调小组组员 |  |  |  |
| 应急协调小组组员 |  |  |  |
| 应急协调小组组员 |  |  |  |

### 应急实施小组

应急实施小组是信息安全的日常技术与事务管理部门和事件应急响应的技术支持与保障部门。应急实施小组的具体职责是：

（1）负责信息安全事件应急响应工作的事件分析和先期处置；

（2）负责应急预案选择和应急预案设计；

（3）负责信息安全事件应急响应过程中的技术支持与技术保障；

（4）在领导小组和协调小组的指挥下处置信息安全事件应急响应工作；

（6）负责信息安全事件应急结束后的重建、恢复工作；

（7）负责应急预案测试、复审与维护。



### 外部应急协助组

外部应急协助组是与数据中心建设和运维管理过程中相关的外部技术力量。包括：参与项目论证的专家组，承担项目集成建设的集成商、分包资质单位主要技术负责人，测评机构、监理机构等单位参与本项目的主要技术负责人。这些来自于外部的专家、技术人员共同构成系统应急协助的力量。

|  |  |  |  |
| --- | --- | --- | --- |
| 角 色 | 姓 名 | 职 务 | 电 话 |
| 总集成商 |  |  |  |
| 分集成商 |  |  |  |
| 监理单位 |  |  |  |

# 应急预案

## 信息系统应急预案

### 应急预案分类

按照突发事件的可控性、严重程度和影响范围，原则上按一般（IV级）、较大（III级）、重大（II级）、特别重大（I级）四级启动相应预案。

响应等级的判断标准：

|  |  |  |  |
| --- | --- | --- | --- |
| 等级 | 颜色 | 处置机构 | 判断标准 |
| 一般（IV级） | 蓝色 | 应急实施小组 | 日常维护小组人员可以独立处置，影响范围1-3台非关键设备，对业务单位基本无影响 |
| 较大（III级） | 黄色 | 本单位应急响应小组 | 本单位应急小组可独立处置，影响3-5台非关键设备，对单位业务基本无影响 |
| 重大（II级） | 橙色 | 本单位应急响应 | 影响关键设备或5台以上非关键设备，影响单位业务效率 |
| 特别重大（I级） | 红色 | 上级应急响应机构 | 关键设备瘫痪或整个系统瘫痪，业务无法开展，可能扩散影响到其他单位 |

### 应急预案启动

#### 报告监测

利用资鼎(上海)互联网金融信息服务有限公司研发部现有人工和自动监控系统相结合的方式监控系统运行状态，应对的主要突发事件包括：

* 主机网络设备故障
* 安全故障
* 机房环境异常（停电、失火、进水、空调停机等）

来自监控系统的事件信息应当由负责监控系统的人员先进行信息准确性的判断，当监控人员判断确实有以上事件发生时，应该立即通知安全工作小组的领导。

#### 信息报告

系统的监控及运维人员，包括网络、主机、应用系统等运营维护人员，在工作中发现主机异常、应用或服务异常、网络异常等事件后，经过故障检查确认是系统网络突发事件，应当立即向安全工作小组的领导报告。

当班人员通知安全工作小组的领导，立即进行处置。如安全工作小组的领导判断事件无法独立处置或1小时内无法控制事件影响，需在1小时内通知应急领导小组，由应急领导小组启动应急预案，协调相关资源进行处置。

#### 先期应急处置

* 现场调查

应急实施小组人员接到事件报告之后，应迅速通知外部应急协调小组，并迅速到达事件发生的现场，在系统运维人员的协助下进一步对事件进行调查。

调查的内容包括：

* 故障现象
* 事故影响范围
* 事故原因
* 持续时间
* 相关日志记录
* 相关记录的信息
* 其他相关信息

|  |  |
| --- | --- |
| 系统网络突发事件现场调查表 | |
| 故障现象 |  |
| 事件影响范围 |  |
| 事故原因 |  |
| 持续时间 |  |
| 相关日志信息 |  |
| 分析判断结果 |  |
| 调查人 |  |
| 日期 |  |

* 事件分析判断

应急实施小组成员经过现场调查之后，确认事件，同时也需要对事件产生的后果进行判断，事件的后果定义为四个级别，分别是：一般、较大、重大、特别重大。根据事件后果的轻重来决定该事件是否上报，对于一般的事件只需要现场处理和记录；对于较大的事件应当上报给本单位的应急领导小组，启动预案进行处置。

### 应急处理流程

在发现系统网络突发事件之后，在启动预案之前，需要对事件进行简单的处置。处置的简单流程如下：



#### 分级响应

* 一般事件响应

由应急实施小组根据现场情况进行现场处置。处置流程和结果进行记录备案。

* 较重事件处置
* 成立处置小组

应急实施小组将分析结果上报至应急领导小组之后，对于较大事件，由领导小组决定启动应急预案，召集应急组织成员成立处置小组来负责该次事件的处置。处置小组成员根据事件具体情况从预案确定的名单中选取。

* 协调资源
  + 专家支持

由于系统网络突发事件的特殊性，需要较多的专业知识，因此，在处置事件时可能需要专家的指导。当预案启动后，由协调小组的成员负责联系相关专家，专家提供相应的技术支持，必要的时候，专家需要到现场进行应急响应指导。

* + 设备

在应急响应的处理过程中，信息系统安全小组应有所有设备、服务提供商的联系表，根据事件处理的情况与相关的提供商取得联系，必要时需要提供商派人员到现场给予支持。

* + 相关权限申请

信息系统安全在应急响应过程中，必然会涉及到各个部门，进一步牵涉到相关职权和权限的申请，例如：机房访问权限、服务器操作权限等等。在应急响应事件处理过程中，信息系统安全在需要其他网络资源访问和人员配合权限的时候，由协调小组负责相关权限的申请和人员的调配。

* 执行事件处置

信息系统应急实施小组在获得相应的权限后，可以对事件执行处置。

* 处置结果检验

当处理完毕后，信息系统应急实施小组应当对处置结果进行检验。

* 故障缓解：继续跟踪其状态变化，并对后续解决方案提供建议
* 故障消除：关闭事件并进入下一步程序。
* 处理失败：封锁事故范围，保持跟踪，注明原因并立即向上级应急领导小组报告，请求领导小组进行处置，提交相应报告。
* 重大事件处置

重大事件如果能够独立处置的，处置流程与较重事件相同。如果需要上级应急响应组织处置的，流程如下。

* 事件上报

将事件上报到主管部门，说明事件的现象、影响范围、事件造成的损失严重程度等。

* 由上级响应组织进行处置

在主管部门协调处置的过程中，本单位的应急响应机构负责提供处置所需的相关资料，配合整体的处置。

* 特别重大事件处置

对于特别重大的事件，中心的应急响应机构无法独立进行处置，需立刻上报给上级主管部门，由上级协调有关职能单位进行处置。在上级应急响应组织进行响应之前，中心应急响应小组应该采取措施，缓解事件，阻止事件的扩散。

* 响应的升级与降级

如果突发事件进一步发展，有蔓延扩大的趋势，并且情况复杂难以控制时，应当由应急领导小组决定，及时提升响应级别；如果突发事件已经逐步得到控制，不会进一步扩散，应当由应急领导小组决定，降低响应级别。

#### 应急结束

对于一般事件，应急实施小组在处置完成后，确认事件消除，即可确认应急过程结束。

对于较重和重大事件，在现场处置结束后，由信息系统安全所有成员确认事件的处置结果，确认后由本单位应急机构负责人宣布应急状态的结束。

对于特别重大的事件，在处置结束后，需由上级应急响应组织宣布应急状态的结束。

#### 事件归档

每次应急响应结束后，应该将该次事件所有的文档统一归档保存。

#### 预案更新

在应急响应结束后，需根据应急过程中暴露的问题和调查总结的结果，对预案进行相应的更新。

### 系统恢复

当信息系统被篡改、破坏或丢失时，使用备份数据恢复系统；当存在多份备份时，应根据需要选择合适的备份；备份信息使用前，应检查备份信息的完整性、可靠性、可用性。使用后应观察设备运行一段时间，确保系统恢复正常。

### 故障总结及报告

* 现场维护人员故障现象报告，应急定位报告。

一线维护工程师在判定故障时，可以远程借助二线、厂商技术人员的支持尽快判断故障，故障定位，在排查过程中做相应的记录，包括故障发生时间及详细的故障症状。以便为二线支持提供更多更直接的资料。

* 现场应急实施小组处、理报告

在故障排除之后，由应急实施小组提供故障排除报告，包括故障引起的原因分析，及故障排除过程和故障产生的隐患，以便后期工作的加强，防范类似故障的发生。同时上报相关用户及领导。

* 指挥中心发表故障报告到上层领导。（一、二级故障时）
* 故障总结报告

### 应急演练

资鼎(上海)互联网金融信息服务有限公司定期对资鼎(上海)互联网金融信息服务有限公司的“马上货”系统网络、数据库和信息安全等事件进行应急演练并做详细记录。

应急演练记录

|  |  |
| --- | --- |
| 演练项目： | 演练时间： |
| 演练地点： | |
| 参与人员： | |
| 预演安排： | |
| 应急情况处理过程： | |
| 演练结果： | |
| 记录员：  日期： | |

## 附录

### 附1：体系文件建立申请表

**体系文件建立申请表**

|  |  |  |  |
| --- | --- | --- | --- |
| 文件名称 |  | | |
| 文件编号 |  | | |
| 发起部门 |  | | |
| 建立体系文件目的及内容 |  | | |
| 申请人  签名 |  | 申请日期 |  |
| 审批人  签名 |  | 审批日期 |  |
| 审批人意见 |  | | |
| 备注 |  | | |

### 附2：体系文件更改申请表

**体系文件更改申请表**

|  |  |  |  |
| --- | --- | --- | --- |
| 文件名称 |  | | |
| 文件编号 |  | | |
| 更改原因及内容 |  | | |
| 申请人  签名 |  | 申请日期 |  |
| 审批人  签名 |  | 审批日期 |  |
| 实施结果 |  | | |
| 备注 |  | | |

### 附3：体系文件评审记录表

**体系文件评审记录表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本号 | 文件编号/名称 | 审核人 | 批准人 | 发布日期 | 说明 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### 附4：体系文件作废申请表

**体系文件作废申请表**

|  |  |  |  |
| --- | --- | --- | --- |
| **申请陈述** | | | |
| **信息委领导、信息安全领导小组和信息安全工作小组：**  现申请作废名称为： （版本号为 ） 信息安全管理体系文件。  原因如下： | | | |
| 申请人： |  | 申请日期 |  |
| 信息安全工作小组  审批意见： |  | 审批日期 |  |
| 信息安全领导小组  审批意见： |  | 审批日期 |  |

### 附5：专家论证表

**专家论证会议签到表**

|  |  |  |  |
| --- | --- | --- | --- |
| 会议名称 |  | | |
| 组织单位 |  | | |
| 会议地点 |  | 会议时间 |  |
| 序号 | 姓名 | 单位名称 | 职务 |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |
| 11 |  |  |  |
| 12 |  |  |  |
| 13 |  |  |  |
| 14 |  |  |  |

### 附6：专家意见书

**专家意见书**

|  |  |
| --- | --- |
| 单位名称 |  |
| 单位地点 |  |
| 方案名称 |  |
| 专家意见： | |
| 专家：（签名）  日期： | |

### 附7：专家论证会会议纪要

**专家论证会会议纪要**

|  |  |
| --- | --- |
| 会议名称 |  |
| 会议地点 |  |
| 会议时间 |  |
| 组织单位 |  |
| 列席人数 |  |
| 会议记录 |  |
| 与会人员签名： |  |
| 记录人： |  |
| 审阅人： |  |

### 附录8 :安全评估报告

|  |
| --- |
| **1、简述总体安全形势** |
|  |
| **2、重点安全问题/问题部门分析** |
|  |
| **3、改进建议** |
|  |

报告人： 时间：

### 附录9 资产清单

网络及安全设备清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 网络安全设备名称 | 型号(软件/硬件) | 物理位置 | 所属网络区域 | IP地址/掩码/网关 | 序列号 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

服务器清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 网络安全设备名称 | 型号(软件/硬件) | 物理位置 | 所属网络区域 | IP地址/掩码/网关 | 序列号 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### 附录10 :系统的操作手册

### 附录11：信息系统安全检查表单

**信息系统安全检查表单**

检查周期： 年 月

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **检查单元** | **最近一个月情况** | **系统漏洞情况** | **重要数据备份情况** | **故障受理情况** | **各项制度执行情况** | **其他突出安全问题** | **检查时间** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 操作员 /日期 |  | | | | 审核人  /日期 |  | |

### 附录12：备份管理员操作变更申请单

**备份管理员操作变更申请单**

|  |  |
| --- | --- |
| 申请变更的设备/系统 | *设备/系统名称，版本，日期等信息描述* |
| 变更的内容  及其理由 |  |
| 评估变更将对  设备/系统造成的影响 |  |
| 备份管理员签字 |  |
| 审核人签字 | *审批意见：*  签字 日期 |
| 变更后的系统信息 | *输入名称，版本，完成日期等信息*  操作员 日期 |
| 审批人签字 | □同意投入使用。  □不同意投入使用，原因：  签字 日期 |

### 附录13：密码变更记录表

密码变更记录表-服务器

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **网络安全设备** | **型号(软件/硬件)** | **变更前密码** | **用户名** | **变更后密码** | **日期** |
|
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

密码变更记录表-网络及安全设备

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 网络安全设备 | 型号(软件/硬件) | 变更前密码 | 用户名 | 变更后密码 | 日期 |
|
| 1 |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 2 |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 3 |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 4 |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 5 |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 6 |  |  |  |  |  |  |

### 附录14：审计记录

审计记录

|  |  |  |  |
| --- | --- | --- | --- |
| **审计内容** | | **审计结果** | |
| 漏洞扫描 | | 是否按照规定定期扫描 | 是 口 否 口 |
| 补丁情况 | 服务器系统补丁 | 是否按照规定定期安装补丁 | 是 口 否 口 |
| 数据库补丁 | 是否按照规定定期安装补丁 | 是 口 否 口 |
| 漏洞扫描补丁库审计 | 每月是否更新漏洞扫描补丁库 | 是 口 否 口 |
| 数据备份 | 系统备份 | 是否定期备份 | 是 口 否 口 |
| 数据库备份 | 是否定期备份 | 是 口 否 口 |
| 网络设备配置备份 | 设备变更前是否备份 | 是 口 否 口 |
| 用户权限审计 | 服务器系统权限 | 是否有违规用户 | 是 口 否 口 |
| 数据库用户权限 | 是否有违规用户 | 是 口 否 口 |
| 机房环境安全审计 | | 机房环境是否定时审查 | 是 口 否 口 |
| 系统管理员操作行为审计 | | 系统管理员操作行为是否违规 | 是 口 否 口 |
| 安全管理员操作行为审计 | | 安全管理员操作行为是否违规 | 是 口 否 口 |
| 规章制度流程、执行审计 | | 规章制度流程、执行是否违规 | 是 口 否 口 |
| 审计内容汇报 | | 安全审计员：  日期： | |

### 附录15：授权与审批流程

**授权与审批流程**



### 附录16：系统配置变更审批单

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_信息系统**

**系统配置变更审批单**

编号：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 题目 |  | | | | | 日期 |  |
| 申请方 |  | | 部门 | |  | 申请人 |  |
| 变更描述：（内容包括情况描述、变更目的、建议处理意见等，具体变更和回退方案可附页）  申请方签字： | | | | | | | |
| 变更类型 | | 应用□网络□主机□安全□其他□ | | | | | |
| 维护单位意见：  签字：  年月日 | | | | 资鼎(上海)互联网金融信息服务有限公司相关部门意见  签字：  年月日 | | | |
| 处理过程与结果：（可附页）  处理方签字：年月日 | | | | | | | |
| 维护单位处理结果验证：  签字：  年月日 | | | | 资鼎(上海)互联网金融信息服务有限公司相关部门处理结果验证：  签字：  年月日 | | | |
| 备注 |  | | | | | | |

### 附录17: 安全检查表

**安全检查表格**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 部门 |  | 责任人 |  | | 职务 |  |
| 岗位等级 |  | 地点 |  | | 电话 |  |
| 终端/服务器/安全设备基本情况 | | | | | | |
| 资产编号 |  | 设备/主机名 |  | | 帐号 |  |
| 硬件情况 |  | | | | | |
| 主要检查项目 |  | | | | | |
| 信息安全情况 | 文件状况 | | |  | | |
| 介质状况 | | |  | | |
| 联网状况 | | |  | | |
| 整体安全状况 | | |  | | |
| 检查结论 |  | | | | | |
| 检查人签名 |  | | | | | |
| 部门意见 |  | | | | | |
| 检查日期 |  | | | | | |
| 备注 | 由资鼎(上海)互联网金融信息服务有限公司永久保存 | | | | | |

### 附录18: 安全检查报告与通报

**安全检查报告与通报**

|  |  |
| --- | --- |
| 通告事项 |  |
| 通报内容 |  |
| 通报部门 | 资鼎(上海)互联网金融信息服务有限公司 |
| 通报日期 | 年 月 日 |

### 附19:外联单位联系表

**外联单位联系表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **服务提供商名称** | **联系人** | **联系电话** | **服务内容** | **保密协议** | **备注** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### 附20:会议记要

**会议记要**

记录号：HY01－ －

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **会议类型** | □例会 □部门 □培训/交流 □信息安全会议 □其他： | | | | |
| **议 题** |  | | | **会议用时(h)** |  |
| **时 间** | 年 月 日  **:** | **地 点** |  | | |
| **主持人** |  | **记录人** |  | | |
| **与会人员** | 共计 人。（签到表HY-10 - ） | | | | |
| **关键字** |  | | | | |
| **1. 会议议程** | | | | | |
|  | | | | | |
| **2. 内容纪要** | | | | | |
|  | | | | | |
| **3. 待解决及共识等后续工作** | | | | | |
|  | | | | | |

注：记录号应填写为HY01－YY（年号）MM（月号）－nn（顺序号）

### **附21:信息安全专家聘任书**

信息安全专家聘任书

兹聘请 同志为资鼎金服信息安全专家，聘期自 年 月 日至 年 月 日。聘任期间， 同志作为专家之一指导资鼎金服信息安全建设，参与信息安全规划和安全评审等。

资鼎(上海)互联网金融信息服务有限公司(章)

年 月

### 附录22 :保密协议

保 密 协 议

甲方：（以下简称甲方）资鼎(上海)互联网金融信息服务有限公司

乙方：（以下简称乙方）

甲方工作内容可能涉及交通运输信息，人员隐私等敏感或机密信息，为保护国家和个人的秘密信息，维护国家安全和社会稳定，依据《中华人民共和国保守国家秘密法》、《科学技术保密规定》等相关法规规定，双方就乙方在履行服务期间保守甲方秘密，同时维护公司合作伙伴的技术和商业秘密，签订下列条款共同遵守：

**第一条**双方确认，乙方在甲方服务期间，因履行服务合同或者主要是利用甲方的物质技术条件、业务信息等产生的发明创造、技术秘密和国家秘密等，有关的知识产权均属于甲方享有。甲方可以在其业务范围内充分自由地利用这些发明创造、技术秘密和国家秘密，进行生产、经营或者向第三方转让。乙方应当依甲方的要求，提供一切必要的信息和采取一切必要的行动，包括申请、注册、登记等，协助甲方取得和行使有关的知识产权。

**第二条**乙方在甲方服务期间所完成的、与甲方业务相关的发明创造、技术秘密、公司秘密和国家秘密，乙方主张由其本人享有知识产权的，应当及时向甲方申明。经甲方核实，认为确属于非职责成果的，由乙方享有知识产权，甲方不得在未经乙方明确授权的前提下利用这些成果进行生产、经营，亦不得自行向第三方转让。

乙方没有申明的，推定其属于职责成果，甲方可以使用这些成果进行生产、经营或者向第三方转让。即使日后证明实际上是非职责成果的，乙方亦不得要求甲方承担任何经济责任和法律责任。

乙方申明后，甲方对成果的权属有异议的，可以通过协商解决；协商不成的，通过当地仲裁委员会仲裁解决。

**第三条**乙方在甲方服务期间，须指定乙方代表和乙方派遣人员，该人员须与乙方签定相关保密协议，乙方须以书面通知的形式告知甲方，经甲方同意后，方可进驻甲方履行服务。

**第四条**乙方在甲方服务期间，必须遵守甲方规定的任何成文或不成文的保密规章、制度，履行与其工作职责相应的保密职责。

甲方的保密规章、制度没有规定或者规定不明确之处，乙方亦应本着谨慎、诚实的态度，采取任何必要、合理的措施，维护其于服务期间知悉或者持有的任何属于甲方或者虽属于第三方但甲方承诺有保密义务的技术秘密、公司秘密和国家秘密，以保持其机密性。

保密资料的接触范围严格限制在因本协议规定目的而需接触保密资料的各自负责任的代表的范围内。

**第四条**除了履行职务的需要之外，乙方承诺，未经甲方同意，不得以泄露、公布、发布、出版、传授、转让或者其他任何方式使任何第三方（包括按照保密制度的规定不得知悉该项秘密的甲方的其他职员）知悉属于甲方或者虽属于他人但甲方承诺有保密义务的技术秘密或其他商业秘密信息，也不得在履行职务之外使用这些秘密信息。

**第五条**乙方同意，乙方服务期满之后仍对其在甲方服务期间接触、知悉的属于甲方或者虽属于第三方但甲方承诺有保密义务的技术秘密、公司秘密和国家秘密信息，承担如同服务期间一样的保密义务和不保存、不使用、不外泄有关秘密信息的义务，而无论乙方因何种原因与甲方终止服务。

乙方服务期满之后承担保密义务的期限为自服务终止之日3年内。

**第六条**乙方承诺，在履行职责时，由于乙方的原因，造成甲方的技术秘密、相关信息和国家秘密等秘密信息的泄漏，乙方应当承担全部的法律责任和经济赔偿责任。

**第七条**乙方在履行职责时，不得擅自使用任何属于他人的技术秘密、公司秘密和国家秘密，亦不得擅自实施可能侵犯他人知识产权的行为。

若乙方违反上述承诺而导致甲方遭受第三方的侵仅指控时，乙方应当承担全部的法律责任和经济赔偿责任。

**第八条**乙方在履行职责时，按照甲方的明确要求或者为了完成甲方明确交付的具体工作任务必然导致侵犯他人知识产权的，若甲方遭受第三方的侵权指控，应诉费用和侵权赔偿不得由乙方承担或部分承担。

**第九条**乙方因工作上的需要所持有或保管的一切记录着甲方秘密信息的文件、资料、图表、笔记、报告、信件、传真、磁带、磁盘、光盘、软盘、录像带、幻灯片、仪器以及其他任何形式的载体，均归甲方所有，而无论这些秘密信息有无商业上的价值。

**第十条**乙方应当于服务终止时，或者于甲方提出请求时，返还全部属于甲方的财物，包括记载着甲方秘密信息的一切载体。

但当记录着秘密信息的栽体是由乙方自备的，且秘密信息可以从载体上消除或复制出来时，可以由甲方将秘密信息复制到甲方享有所有权的其他载体上，并把原载体上的秘密信息消除。此种情况乙方无须将载体返还，甲方也无须给予乙方经济补偿。

**第十一条**本协议提及的秘密，包括但不限于：人员信息、交通运输数据、技术方案、工程设计、业务流程、技术指标、计算机软件、数据库、研究开发记录、技术报告、检测报告、系统数据、评测结果、图纸、操作手册、技术文档、相关的函电，等等。

**第十二条**本协议中所称的服务期间，以甲乙双方签订合同为标志，并以该合同的有效期间为服务期间。

**第十三条**如乙方受甲方委派为第三方提供外包服务，乙方对甲方的保密责任和义务同样有效，作用范围自动延伸到外包服务工作的全过程。

**第十四条**因本协议而引起的纠纷，如果协商解决不成，任何一方均有权提交当地仲裁委员会仲裁。

**第十五条**本协议自双方签字或盖章完成之日起生效，本协议一式四份，双方各执两份，具有同等法律效力。

**第十六条**本协议如与双方以前的口头或书面协议有抵触，以本协议为准。本协议的修改必须采用双方同意的书面形式。

甲方（签字/盖章）：　　 乙方（签字）：

地址： 地址：

联系电话：\_\_\_\_\_\_\_\_\_　　　　　　　　　 　联系电话：\_\_\_\_\_\_\_\_\_

传真：\_\_\_\_\_\_\_\_\_　　　　　　　　　　　 　传真：\_\_\_\_\_\_\_\_\_

邮政编码：\_\_\_\_\_\_\_\_\_　　　　　　　　　 　邮政编码：\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日　　　　　　　 　\_\_\_\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日

**岗位安全协议**

甲方：资鼎(上海)互联网金融信息服务有限公司

乙方：

根据《中华人民共和国劳动合同法》规定，经双方协商一致，自愿签订本协议，共同遵守本协议所列条款

一、聘用岗位

甲方根据工作需要，聘任乙方到＿＿＿＿＿＿＿＿部门，＿＿＿＿岗位工作，任＿＿＿＿＿＿职务，岗位级别＿＿＿＿＿＿。

二、协议期限

本协议期限为\_\_\_\_\_年，自\_\_\_\_年＿＿月＿＿日起至\_\_\_\_年＿＿月＿＿日止。

三、岗位职责

乙方应在聘用期内，按照所聘岗位的《岗位协议书》，接受甲方的管理，在规定的时限内完成规定的工作任务，并达到岗位说明书规定的工作标准，以及甲方确定的其他工作指标。

四、岗位协议解除

劳动者发生职务晋升或岗位调整或出现其他情况不得不解除岗位协议的，本协议可以提前解除。

本协议作为劳动合同的附件，与劳动合同一并管理。

本协议一式两份，甲乙双方各执一份，自签订之日起生效。

甲乙双方一经签订协议，公司的各项规章制度，将与本协议一并生效。

甲方（公章）

乙方（签字或盖章）

签订日期：

### 附录23: 上岗人员情况登记表

资鼎(上海)互联网金融信息服务有限公司

上岗人员情况登记表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 姓 名 |  | | | | | 一寸免冠彩照 | |
| 出生年月 |  | | 性 别 | □ 男 □ 女 | |
| 籍 贯 |  | | 民 族 |  | |
| 身份证件号码 |  | | 签发机关 |  | |
| 政治面貌 |  | | 国 籍 |  | |
| 婚 姻 | □已婚 □未婚 □离异 □丧偶 | | | | | | |
| 户籍地址 |  | | | | 邮 编 |  | |
| 居住地址 |  | | | | 邮 编 |  | |
| 工作单位 |  | | | | 邮 编 |  | |
| 职 务 |  | | | | 职 称 |  | |
| 学 历 |  | | | | 学历签发院校 |  | |
| 学 位 |  | | | | 学位证书编号 |  | |
| 联系电话 | 单位电话： 手机： | | | | | | |
| **工作经历** | | | | | | | |
| 起止时间 | 单 位 名 称 | | 职　务 | | 离职原因 | 证明人 | 电话 |
|  |  | |  | |  |  |  |
|  |  | |  | |  |  |  |
| **相关技能** | | | | | | | |
| 与从事业务相关的认证、技能、资质等证书说明 | |  | | | | | |
| **参与项目情况** | | | | | | | |
| 参与的项目及负责的主要任务 | |  | | | | | |
| 本人保证以上所填内容均属实。  签字：  时间： 　 年 　月　 日 | | | | | | | |
| 备注：资鼎(上海)互联网金融信息服务有限公司永久存档 | | | | | | | |

### 附录24: 人员入岗审核表

**资鼎(上海)互联网金融信息服务有限公司**

**人员入岗审核表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **申请人** |  | **工号** |  | **所属部门** |  |
| **入岗时间** | **年月日** | | | | |
| 是否与资鼎(上海)互联网金融信息服务有限公司签订保密协议：是🞏否🞏  是否签订《保密协议（在岗）》：是🞏否🞏  是否填写《人员情况登记表》：是🞏否🞏  **主管领导签字：** | | | | | |
| **承担的角色**：  安全管理工作小组成员🞏项目总监🞏项目经理🞏项目安全管理员🞏  项目开发人员🞏系统集成人员🞏系统维护人员🞏  **承担的主要工作：**  项目管理🞏安全管理🞏软件开发🞏系统集成🞏系统维护🞏 | | | | | |
| **核定程度**：  核心人员🞏重要人员🞏一般人员🞏  **资鼎(上海)互联网金融信息服务有限公司领导签字：** | | | | | |
| 备注：资鼎(上海)互联网金融信息服务有限公司永久存档 | | | | | |

### 附录25: 岗位协议书 （需打印）

**资鼎(上海)互联网金融信息服务有限公司系统管理员岗位协议书**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名字 |  | | 部门 |  |
| 职责范围：   1. 负责保障主机（包括服务器设备、操作系统、数据库系统、数据备份）； 2. 信息安全日常管理   包括系统口令管理、无人值守设备管理、屏幕保护、便携机管理等，促使每位人员的日常工作符合资鼎(上海)互联网金融信息服务有限公司的“马上货”系统的信息安全策略和制度要求。   1. 负责主机运行维护体系和主机技术支持平台的建设与运行管理   建立服务器设备、操作系统、数据库系统、数据备份文档化的操作和维护规程，使得各个相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性。   1. 重要信息和信息系统备份   定期进行重要信息和信息系统备份，并对备份介质进行安全地保存，以及对备份数据定期进行备份测试验证，保证各种备份信息的保密性、完整性和可用性，确保所有重要信息系统和重要数据在故障、灾难后及其它特定要求下进行可靠的恢复。   1. 负责统一部署防病毒软件，并定期更新病毒库； 2. 负责全系统的计算机恶意代码防治和主机安全的管理工作，制定检查计划（包含在主机巡检工作中），督促检查工作； 3. 负责重要信息系统的访问控制管理，对系统特殊权限和系统实用工具的使用进行严格的审批和监管； 4. 负责组织实施主机各类事故（故障）的应急处理。 5. 严格遵守保密协议。 | | | | |
| 签字确认： | |  | | \_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日 |
| 备注：资鼎(上海)互联网金融信息服务有限公司永久存档 | | | | |

**资鼎(上海)互联网金融信息服务有限公司安全管理员岗位协议书**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名字 |  | | 部门 |  |
| 职责范围：   1. 负责我局安全制度的贯彻执行； 2. 负责制订信息系统安全规划，并在实施过程中逐步完善； 3. 负责制定我局安全设备或系统的相关资产清单。内容包括资产管理的责任部门、资产名称、重要程度、所处位置等； 4. 负责制定安全设备或系统的文档化的操作和维护规程，使得相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性； 5. 负责我局安全设备或系统运行维护管理，对安全设备或系统运转情况进行定期巡检、维护、故障处理和变更管理。负责组织实施安全设备或系统各类事故（故障）的应急处理； 6. 每年进行风险评估，根据评估结果会同其他负责人进行风险处置； 7. 负责协助领导安排安全培训，负责协助负责制定每年安全教育计划，加强信息系统的安全教育，通过各种方式进行宣传和培训，提高全系统安全防范意识； 8. 负责制定安全检查计划   包括检查职责、检查周期、检查范围、检查内容、检查报告的编制、检查整改、检查通报等内容。对信息系统安全检查并进行情况通报。对记录进行收集、整理、归档。   1. 当出现安全事件时，负责对发生的安全事件及时上报，并配合相关的调查和纠正工作； 2. 当信息系统运行发生重大问题时，协助相关部门正确判断原因，根据指令立即采取安全措施启动相关处理程序； 3. 负责与外部安全机构的协调联系，在发生重大安全事件时以协调获取外部安全机构的支持； 4. 负责对介质的管理   对介质的归档、查询和借用进行记录，对介质进行定期盘点并记录，对故障介质的进行送修和销毁并记录，对于保密性高的介质销毁需要申报领导批准，并进行记录。对介质物理传输的交接进行记录。   1. 加强对信息系统外包业务与外包方的管理   在与信息系统外包方签署的服务协议中，对信息系统安全加以要求。通过审批、访问控制、监控、签署保密协议等措施，加强外部方访问“健康档案”的管理，防止外部方危害信息系统安全。   1. 重视对IT服务连续性的管理，建立对各类信息安全事件的预防、预警、响应、处置、恢复机制，并编写相应的应急预案； 2. 在符合国家密码管理相关规定的条件下，合理使用密码技术和密码设备，严格密钥生成、分发、保存等方面的安全管理，保障密码技术使用的安全性。 | | | | |
| 签字确认： | |  | | \_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日 |
| 备注：资鼎(上海)互联网金融信息服务有限公司永久存档 | | | | |

**资鼎(上海)互联网金融信息服务有限公司安全审计员岗位协议**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名字 |  | | 部门 |  |
| 职责范围：   1. 参与制定我局规章制度和流程，规章制度和流程培训与宣传； 2. 根据我局的审计要求制定审计计划，定期或不定期的开展审计工作，撰写审计报告，开展风险评估，发现安全漏洞或隐患，提交处理报告和切合实际可操作的处理方案，指导实施； 3. 负责我局机房安全审计，负责数据库服务器、数据备份与灾难恢复审计； 4. 负责我局操作系统安全审计，关键系统的用户角色权限审计； 5. 负责我局日常信息安全规章制度和流程的执行审计，信息系统环境安全审计等； 6. 对被审计部门提供咨询、建议、协调等服务和公司领导安排的相关工作； 7. 负责对系统管理员、安全管理员的操作行为进行审计跟踪分析和监督检查，及时发现违规行为，每月向信息安全中心汇报工作情况； | | | | |
| 签字确认： | |  | | \_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日 |
| 备注：资鼎(上海)互联网金融信息服务有限公司永久存档 | | | | |

### 附录26：信息安全岗位人员考核记录

**信息安全岗位人员考核记录**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 考核对象 | |  | | | 考核 日期 |  | | |
| 所在岗位 | |  | | |  |  | | |
| 评定项目 | 所占 比重 | 评分标准 | | | | | | |
| 具体指标 | 优秀 100%-90% | 较好 90%-80% | 一般 80%-70% | 较差 70%-60% | 很差 60%以下 | 备注 |
| 安全知识 | 20 | 安全意识10 |  |  |  |  |  |  |
| 参加培训的成绩10 |  |  |  |  |  |  |
| 安全技能 | 40 | 专业知识10 |  |  |  |  |  |  |
| 实际经验5 |  |  |  |  |  |  |
| 应变能力15 |  |  |  |  |  |  |
| 处理难题能力10 |  |  |  |  |  |  |
| 安全制度的执行方面 | 40 | 对安全文件的理解力10 |  |  |  |  |  |  |
| 职业道德5 |  |  |  |  |  |  |
| 执行情况15 |  |  |  |  |  |  |
| 创新能力10 |  |  |  |  |  |  |
| 评分小计 | | |  |  |  |  |  |  |
| 综合评语 | | 级别 标准 | 80分以上胜任 | | | 80分以下不胜任 | | |
| 评价意见 | | 评价人签字： 日期： | | | | | | |

### 附录27：安全技能考核纪录

**资鼎(上海)互联网金融信息服务有限公司安全技能考核纪录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **考核日期** | **考核对象/部门** | **合格（是/否）** | **备注** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 附录28：关键岗位审查情况表

**资鼎(上海)互联网金融信息服务有限公司**

**关键岗位审查情况表**

**单位： 年度**

|  |  |  |  |
| --- | --- | --- | --- |
| **员工姓名** |  | **岗位** |  |
| **考核内容** | | | |
| **政治面貌** |  | | |
| **工作态度：**  **岗位负责人签名：** | | | |
| **专业技能：**  **岗位负责人签名：** | | | |
| **本年度是否有违纪违规行为：**  **岗位负责人签名：** | | | |

**资鼎(上海)互联网金融信息服务有限公司安全审计员岗位协议**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名字 |  | | 部门 | 资鼎(上海)互联网金融信息服务有限公司研发部 |
| 职责范围：   1. 参与制定我局规章制度和流程，规章制度和流程培训与宣传； 2. 根据我局的审计要求制定审计计划，定期或不定期的开展审计工作，撰写审计报告，开展风险评估，发现安全漏洞或隐患，提交处理报告和切合实际可操作的处理方案，指导实施； 3. 负责我局机房安全审计，负责数据库服务器、数据备份与灾难恢复审计； 4. 负责我局操作系统安全审计，关键系统的用户角色权限审计； 5. 负责我局日常信息安全规章制度和流程的执行审计，信息系统环境安全审计等； 6. 对被审计部门提供咨询、建议、协调等服务和公司领导安排的相关工作； 7. 负责对系统管理员、安全管理员的操作行为进行审计跟踪分析和监督检查，及时发现违规行为，每月向信息安全中心汇报工作情况； | | | | |
| 签字确认： | |  | | \_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日 |
| 备注：资鼎(上海)互联网金融信息服务有限公司永久存档 | | | | |

资鼎(上海)互联网金融信息服务有限公司机房管理员岗位协议书

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名字 |  | | 部门 |  |
| 职责范围：   1. 负责保障机房物理与环境的安全建设管理 2. 负责制定机房基础设施的相关资产清单 3. 内容包括资产名称、重要程度、所处位置等。 4. 明确产品所有者、使用者与维护者；对所有产品进行标记，实现信息资产从采购、安装、调试、使用、变更到报废整个周期的安全管理，并且密码相关产品符合国家密码主管部门的要求。 5. 令相关人员能够按照维护规程对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性。 6. 负责保障机房物理与环境安全 7. 实施包括门禁、视频监控、报警等安全防范措施，确保机房物理安全。部署机房专用空调、UPS等环境保障设施，对机房设施运转情况进行每日两次巡检、维护、故障处理和变更管理。严格对机房人员和设备的出入管理，进出需登记，外来人员需由相关管理人员陪同方能访问机房。 8. 在机房基础设施变更、重要操作、物理访问等的进行逐级审批，负责日常审批，重大变更需上报到资鼎(上海)互联网金融信息服务有限公司领导小组负责人进行核准和审批后，方可进行变更； 9. 负责组织实施机房基础设施各类事故（故障）的应急处理。 | | | | |
| 签字确认： | |  | | \_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日 |

资鼎(上海)互联网金融信息服务有限公司主机管理员岗位协议书

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名字 |  | | 部门 |  |
| 职责范围：   1. 负责保障主机（包括服务器设备、操作系统、数据库系统、数据备份） ； 2. 信息安全日常管理   包括系统口令管理、无人值守设备管理、屏幕保护、便携机管理等，促使每位人员的日常工作符合系统的信息安全策略和制度要求。   1. 负责主机运行维护体系和主机技术支持平台的建设与运行管理   建立服务器设备、操作系统、数据库系统、数据备份文档化的操作和维护规程，使得各个相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性。   1. 重要信息和信息系统备份   定期进行重要信息和信息系统备份，并对备份介质进行安全地保存，以及对备份数据定期进行备份测试验证，保证各种备份信息的保密性、完整性和可用性，确保所有重要信息系统和重要数据在故障、灾难后及其它特定要求下进行可靠的恢复。   1. 负责统一部署防病毒软件，并定期更新病毒库； 2. 负责全系统的计算机恶意代码防治和主机安全的管理工作，制定检查计划（包含在主机巡检工作中），督促检查工作； 3. 负责重要信息系统的访问控制管理，对系统特殊权限和系统实用工具的使用进行严格的审批和监管； 4. 负责组织实施主机各类事故（故障）的应急处理。 | | | | |
| 签字确认： | |  | | \_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日 |

资鼎(上海)互联网金融信息服务有限公司网络管理员岗位协议书

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名字 |  | | 部门 |  |
| 职责范围：   1. 负责网络设备等（包括网络设备,安全设备配置,维护及数据备份） ； 2. 负责保障网络安全建设管理； 3. 规范网络管理流程； 4. 采用技术和管理两方面的控制措施，加强对应用系统的安全控制，提高网络的安全性和稳定性； 5. 对重要网络设备应有文档化的操作和维护规程，使得维护人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性； 6. 负责保障网络安全，协助安全管理员部署网络安全产品，确保网络安全；对网络设备设施运转情况进行定期巡检、维护、故障处理和变更管理； 7. 在网络系统变更、重要操作、访问等的进行逐级审批，负责日常审批，重大变更需报到资鼎(上海)互联网金融信息服务有限公司领导小组进行核准和审批后，方可进行变更； 8. 负责组织实施网络各类事故（故障）的应急处理。 | | | | |
| 签字确认： | |  | | \_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日 |

资鼎(上海)互联网金融信息服务有限公司应用管理员岗位协议书

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名字 |  | | 部门 |  |
| 职责范围：   1. 负责保障软件开发管理, 在资鼎(上海)互联网金融信息服务有限公司的“马上货”系统系统立项和审批过程中，同步考虑信息安全需求和目标。应保证系统设计、开发过程的安全，重点加强对软件代码安全性的管理。属于外包软件开发的，应与服务提供商签署保密协议。系统开发完成后，应要求通过第三方安全机构对软件安全性的测评。； 2. 负责建立重要应用的文档化操作和维护规程（详见附录2），使得各个相关人员能够采用规范化的形式对系统进行操作，降低和避免因误操作所引发信息安全事件的可能性； 3. 负责信息安全日常管理，包括应用系统口令管理、授权审批管理等，促使每位人员的日常工作符合资鼎(上海)互联网金融信息服务有限公司的“马上货”系统系统信息安全策略和制度要求。 4. 在应用系统变更、重要操作、访问等的进行逐级审批，负责日常审批，重大变更需报到资鼎(上海)互联网金融信息服务有限公司领导小组进行核准和审批后，方可进行变更； 5. 负责组织实施应用系统各类事故（故障）的应急处理。 | | | | |
| 签字确认： | |  | | \_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_日 |

### 附录29：信息安全培训计划

**信息安全培训计划**

为了使资鼎(上海)互联网金融信息服务有限公司的相关管理和技术人员熟练地掌握系统中产品的基本原理、操作使用和管理维护、及时排除系统故障，并提高网络安全管理能力，将对安全培训有如下计划：

**现场培训方式**

**培训目的：**伴随项目实施的全过程，资鼎(上海)互联网金融信息服务有限公司技术人员和厂商工程师一起进行安全策略的制定、安全产品的安装、系统联调等，并从实际施工操作中获得对产品配置、操作、维护的第一手直观的认识和经验。

**培训对象：**资鼎(上海)互联网金融信息服务有限公司技术人员。

**培训时间：**每半年举行一次

**培训内容：**安全产品安装、调试、配置、使用、维护、管理和故障处理、安全事故处理方法等。

**预备知识：**掌握TCP/IP原理，网络安全基础知识，熟练使用Windows操作系统。

**培训教材：**产品使用手册，现场操作演示。

**《网络安全技术培训》（集中培训）**

**培训目的：**使资鼎(上海)互联网金融信息服务有限公司技术人员和相关管理人员通过学习，掌握网络安全知识，提高网络安全管理能力；了解安全产品基本原理和操作技能，充分掌握独立进行系统管理和维护、解决故障的能力。

**培训对象：**资鼎(上海)互联网金融信息服务有限公司相关安全管理人员和技术人员。

**培训时间：**每半年举行一次

**培训内容：**网络安全基础知识、操作系统安全教程以及安全热点分析、前门攻击和后门渗透、安全弱点分析、Web应用安全、恶意代码等；安全产品的技术原理、操作使用、管理维护和故障处理等。

**预备知识：**掌握TCP/IP原理，网络安全基础知识，熟练使用Windows操作系统。

**培训教材：**专用培训教材

**《系统运维管理培训》（集中培训）**

**培训目的：**让使用者有强烈的安全意识，并将安全目标落实到人，提高安全管理水平。

**培训对象：**系统内管理运维人员。

**培训时间：**每半年举行一次

**培训内容：**根据等级保护管理制度要求对系统内管理运维人员进行教育培训、安全培训、应急响应培训、技能培训等。

**培训教材：**专用培训教材

### 附录30：安全教育培训签到表

**资鼎(上海)互联网金融信息服务有限公司**

**安全教育培训签到表**

|  |  |  |  |
| --- | --- | --- | --- |
| 教育培训名称 |  | | |
| 时间 |  | | |
| 地点 |  | | |
| 参加人员 |  | | |
| 未参加人员 |  | | |
| 主持人 |  | | |
| 部门 | 姓名 | 到会时间 | 签名 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### 附录31: 安全教育培训评价表

资鼎(上海)互联网金融信息服务有限公司

安全教育培训评价表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 培训种类 | □ 外派培训 □ 内部技术培训/交流  □ 新员工培训 □ 其它： | | | | |
| 培训名称及  内容 |  | | | | |
| 考核方式 | □笔试 □口试 □实地操作 □心得报告 □其它 | | | | |
| 主讲人 |  | 培训日期 | |  | |
| 参加人员 | （见会议签到表 ） | | | | |
| 自我评价  及建议 |  | | | | |
| 填写人 |  | | 填写日期 | |  |
| 培训后  考核意见 | 培训效果评估：□合格 □不合格 | | | | |
| 考核/填写人 |  | | 考核/填写日期 | |  |

### 附录32：年度信息安全培训计划

| **年度信息安全培训计划**  部门：资鼎(上海)互联网金融信息服务有限公司研发部 | | | | | | | | | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **培训时间** | | | **培训班名称** | | | **培训对象** | | | **培训人次** | | **培训方式** | | **天数** | **预算（元）** | | | **备注** | | |
| 1 |  | | |  | | |  | | |  | |  | |  |  | | |  | | |
| 2 |  | | |  | | |  | | |  | |  | |  |  | | |  | | |
| 3 |  | | |  | | |  | | |  | |  | |  |  | | |  | | |
| 4 |  | | |  | | |  | | |  | |  | |  |  | | |  | | |
| 5 |  | | |  | | |  | | |  | |  | |  |  | | |  | | |
| 6 |  | | |  | | |  | | |  | |  | |  |  | | |  | | |
| 7 |  | | |  | | |  | | |  | |  | |  |  | | |  | | |
| 8 |  | | |  | | |  | | |  | |  | |  |  | | |  | | |
| 统计数： | | | |  | | |  | | |  | |  | |  |  | | |  | | |
|  | | | | | | | | | | | | | | | | | | | | |
| 编制人 | |  | 日 期 | |  | 审核人 | |  | 日 期 | |  | | 批准人 | | |  | 日 期 | |  |

### 附录33：培训考题

培训考题

一、填空题

1、计算机网络的主要功能有三个：\_\_\_

2、Server/Client的中文意思是指\_\_\_

3、\_\_\_ 的基本做法是把有环路的网络结构生成一个没有环路的逻辑树形网络结构。

4、选取根桥的原则是：根桥必须具有最低的\_\_\_ 地址。

5、一个IP：192.168.4.10/30它所处的网络号是\_\_\_

6、OSPF 是一种\_\_\_ 路径路由选择协议

7、一台10口集线器中有\_\_\_ 个冲突域

一、选择题

1．OSI模型分为几层 ( )

A．4 B．5 C.6 D．7

2．RIP规定一条通路上最多可包含的路由器数量是 ( )。

A．1个 B．16个 C．15个 D.无数个

3．在Windows操作系统中用于路由追踪的命令是？( )

A Netstat B Route Print C Traceroute D Tracert

4．关闭Rip路由汇总的命令是？( )

A．no auto-summary B．auto-summary C．no ip router D．ip router

5．一般连接交换机与主机的双绞线叫做( )

A．交叉线 B．直连线 C．反转线 D．六类线

6. 以下属于C类IP地址的是( )

A、110.33.24.58 B、66.200.12.33 C、210.41.224.36 D、127.0.0.1

7. HTTP协议使用的端口号是？( )

A 20 B 25 C 69 D 80

8．下列哪种协议的目的是从已知IP地址获得相应的MAC地址( )

A TELNET B HTTP C ARP D RARP E ICMP

9．IPv4将IP地址划分为几类( )

A．4 B．2 C．3 D．5

10. 已知对一个标准的C类网络192.168.1.0/24进行了子网划分，每个子网可以容纳6台主机，现有一个主机IP地址为192.168.1.11,请问下列地址中，那一个主机地址与该主机地址在同一个网段( )

A．192.168.1.6 B． 192.168.1.9 C．192.168.1.7 D．192.168.1.15

11．如果子网掩码是255.255.255.192，主机地址为195.16.15.1，则在该子网掩码下最多可以容纳多少个主机？( )

A．254 B． 126 C． 62 D． 30

12、当RIP向相邻的路由器发送更新时，它使用多少秒为更新计时的时间值？( )

A． 30 B． 20 C． 15 D． 25

13、有一个中学获得了C类网段的一组IP 192.168.1.0/24，要求你划分7个以上的子网，每个子网主机数不得少于25台，请问子网掩码该怎么写？( )

A、255．255．255．128 B、255．255．255．224 C、255．255．255．240 D、255．255．240．0

14、通过console口管理交换机在超级终端里应设为( )

A、波特率：9600 数据位：8 停止位：1 奇偶校验：无

B、波特率：57600 数据位：8 停止位：1 奇偶校验：有

C、波特率：9600 数据位：6 停止位：2 奇偶校验：有

D、波特率：57600 数据位：6 停止位：1 奇偶校验：无

15、以下关于TCP/IP 体系结构的描述中，正确的是( ) 。

A. TCP/IP提供无连接的网络服务，所以不适合话音和视频等流式业务

B. TCP/IP定义了OSI/RM的物理层和数据链路层

C. 在TCP/IP体系结构中，一个功能层可以有多个协议协同工作

D. TCP/IP体系结构的应用层相当于OSI/RM的应用层和表示层

16、在路由器里正确添加静态路由的命令是: ( )

A、Red-giant(config)#ip route 192.168.5.0 255.255.255.0 serial 0

B、Red-giant#ip route 192.168.1.1 255.255.255.0 10.0.0.1

C、Red-giant(config)#route add 172.16.5.1 255.255.255.0 192.168.1.1

D、Red-giant(config)#route add 0.0.0.0 255.255.255.0 192.168.1.0

17、在Windows 中，可以提供WWW服务的软件是( ) 。

A. IIS B. ISA C. ISP D. ASP

培训考题答案

一、填空题

1、资源共享、信息交换、分布式管理 2、服务器/客户机

3、STP 4、MAC 5、192.168.4.8 6、开放式最短路径 7、1

二、选择题

1、D 2、C 3、D 4、A 5、B 6、C 7、D 8、C 9、D 10、B   
11、C 12、A 13、B 14、A 15、C 16、A 17、A

### 附录34：培训考核记录表

资鼎(上海)互联网金融信息服务有限公司

培训考核记录表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 培训考核记录表 | | | | | |
| 培训日期 |  | 培训地点 |  | 培训方式 |  |
| 组织单位 |  | 授课人 |  | 培训人数 |  |
| 培训内容 |  | | | | |
| 培训教材 |  | | | | |
| 单位 | 受训人 | 考核成绩 | 单位 | 受训人 | 考核成绩 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### 附录35: 人员离岗/职审批表

人员离岗/职审批表

单位：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 姓 名 |  | | 性别 | |  | 出身年月 |  | |
| 职务、岗位 | |  | | 职称 | |  | 政治面貌 |  |
| 上岗时间 | |  | |  | |  |  |  |
| 离岗原因： 辞职 □ 调动 □ 其他： | | | | | | | | |
| 要求辞职、调动理由、去向： | | | | | | | | |
| 在资鼎(上海)互联网金融信息服务有限公司从事的工作内容： | | | | | | | | |
| 审核意见 | | | | | 主管签字：  年 月 日 | | | |
| 资鼎(上海)互联网金融信息服务有限公司安全领导小组审核意见 | | | | | 主管签字：  年 月 日 | | | |

### 附录36: 人员离岗工作交接表

**人员离岗工作交接表**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 姓名 |  | | | 所在部门 | | |  | | | | |
| 离岗 | □离职 □换岗 □其它 | | | 离岗时间 | | |  | | | | |
| 原因 |
| 原部门 |  | 职务 |  | 现部门 | | (若有) | | 职务 | | |  |
| **项目(业务)交接** | | | | | | | | | | | |
| 应移交事项 | | | 移交人签字 | | 接交人签字 | | | | | 审核人签字 | |
| 经办工作内容交接 | | |  | |  | | | | |  | |
| （具体交接内容附附件） | | |
| 其他事宜 | | |  | | | | | | | | |
| **各类事宜处理意见** | | | | | | | | | | | |
| 详情 | 账号处理意见 | | | 备注 | | | | | 审核人签字 | | |
| 权限 | □注销 □保留 | | |  | | | | |  | | |
| □调整新权限（附申请单） | | |
| 邮箱 | □注销 □调整至新部门 | | |  | | | | |  | | |
| 门卡 | □收回 □调整至新部门 | | |  | | | | |  | | |
| 钥匙 | □收回 □调整至新部门 | | |  | | | | |  | | |
| 办公设备 | □收回 □调整至新部门 | | | 如电脑等 | | | | |  | | |
| 其他事宜 |  | | | | | | | | | | |
| 各类事宜移交处理结果 | | | | | | | | | | | |
| 详情 | | | 处理部门 | | 处理结果 | | | | | 经办人签字 | |
| 财务相关事宜 | | | 财务部 | |  | | | | |  | |
| 权限 | | | 系统管理员 | |  | | | | |  | |
| 邮箱 | | | 系统管理员 | |  | | | | |  | |
| 办公设备 | | | 系统管理员 | |  | | | | |  | |
| 门卡、钥匙 | | |  | |  | | | | |  | |
| 其它事项 | | | 备注： | | | | | | | | |

### 附录37: 离职保密承诺书

**离职保密承诺书**

姓名： 身份证号：

任职单位： 上海市 岗位：

本人承诺，自离职之日起，就本人就在职其间掌握和了解的所有与资鼎(上海)互联网金融信息服务有限公司相关的秘密或需要保密的信息、资料进行保密。本人愿意继续承担《保密协议》中应进行的保密要求。若因为本人泄密等原因造成资鼎(上海)互联网金融信息服务有限公司的损失，愿意承担相关的法律责任，资鼎(上海)互联网金融信息服务有限公司有权向本人追究赔偿的权利。

承诺人（签字）：

承诺人身份证号：

签字日期： 年 月 日

### 附录38: 机房进出申请单

资鼎(上海)互联网金融信息服务有限公司机房进出申请单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **申请人** | |  | **日期** |  |
| **工作事宜** | 集成参数配置（ ） 集成调试 （ ） 更换硬件 （ ）  系统切换或备份（ ） 数据库操作（ ） 其他 （ ） | | | |
| **工作内容描述** | | | | |
| 集成负责人签字：  日期： | | | | |
| **审核意见** | | | | |
| 用户：  签名：  日期： | | | | |

### 附录39: 机房进出记录表

资鼎(上海)互联网金融信息服务有限公司机房进出记录表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 姓名 | 单位名称 | 工作事项 | 手机 | 日期 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |
| 10 |  |  |  |  |  |
| 11 |  |  |  |  |  |
| 12 |  |  |  |  |  |
| 13 |  |  |  |  |  |
| 14 |  |  |  |  |  |
| 15 |  |  |  |  |  |
| 16 |  |  |  |  |  |
| 17 |  |  |  |  |  |
| 18 |  |  |  |  |  |

### 附录40：机房出入登记表

**机房出入登记表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 日期 | 姓名 | 单位名称 | 事由 | 进入时间 | 离开时间 | 陪同人员 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### 附录41：机房设备出门单

资鼎(上海)互联网金融信息服务有限公司机房设备出门单

编号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 申请人 |  | 部 门 |  | 申请时间 |  |
| 设备类型 |  | | | 数量 |  |
| 申请理由： | | | | | |
| 领导审批意见：  签名 年 月 日 | | | | | |
| 注：1. 本表由安全管理员负责填写  2. 本表由安全审计员员负责存查 | | | | | |

### 附录42：设备维护档案

**设备维护档案**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 设备的名称 | 规格 | 配置 | 购入日期 | 供货商 | 存放地点 | 使用年限 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### 附录43：信息安全存储介质领用/借用申请单

**信息安全存储介质领用/借用申请单**

编号：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 领用人 |  | 部 门 |  | 领用时间 | | |  |
| 载体类型 | 磁盘□ 光盘□ U盘□ 其它□（ ） | | | | 数量 |  | |
| 申请理由： | | | | | | | |
| 本部门领导审批意见：  签名 年 月 日 | | | | | | | |
| 注：1. 本表由安全管理员负责填写  2. 本表由主管部门日常执行机构管理员负责存查 | | | | | | | |

### 附录44：介质销毁审批表

信息安全介质销毁审批表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 申请部门： | | | 申请人： | | 核对人： | | |
| 介质物理形态 | | 纸介质□ 磁介质□ 光盘□ 胶片□ 相片□ 其他： | | | | | |
| 序 | 介质内文件、音像、图样名称 | | | 文号、图号 | 编号 | 份数 | 页数 |
|  |  | | |  |  |  |  |
|  |  | | |  |  |  |  |
|  |  | | |  |  |  |  |
| 申请部门领导审核： | | | | 介质产生部门或归口部门领导审核： | | | |
| 主管领导审批： | | | | | | | |
| 送销或销毁经办人： | | | | 资鼎(上海)互联网金融信息服务有限公司监销人： | | | |
| 注：本表由信息安全部门长久保存 | | | | | | | |

### 附录45：信息安全存储介质维修记录

信息安全存储介质维修记录

NO：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 报修部门： | 报修人： | | 报修日期： | 联系电话： | | |
| 设备名称： | 型号： | | 厂编号： |  | | |
| 故障现象（或故障现场情况）：  报修部门盖章  （主管签字）： | | | | | | |
| 内修情况记录：  内修维修人： 年 月 日 | | 维修元件名称（型号） | | | 数量 | 总价 |
|  | | |  |  |
|  | | |  |  |
|  | | |  |  |
|  | | |  |  |
|  | | |  |  |
| 外修情况记录：  外修维修人： 年 月 日 | |  | | |  |  |
|  | | |  |  |
|  | | |  |  |
|  | | |  |  |
|  | | |  |  |
|  | | |  |  |
| 报修部门验收意见：  验收人： 年 月 日 | | 维修费用结算：  材料费：  其 他：  主管部门签字： 年 月 日 | | | | |

### 附录46：设备领用表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **资产名称** | **资产编号** | **品牌** | **规格型号** | **数量** | **单价** | **使用部门** | **签收人** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

### 附录47：计算机设备责任人变更审批表

**计算机设备责任人变更审批表**

|  |  |  |  |
| --- | --- | --- | --- |
| 计算机编号 |  | | |
| 原责任人 |  | 现责任人 |  |
| 申请理由： | | | |
| 现责任人意见：  签字： 年 月 日 | | | |
| 部门领导意见：  签字： 年 月 日 | | | |
| 资鼎(上海)互联网金融信息服务有限公司意见：  签字： 年 月 日 | | | |
| 备注： | | | |

### 附录48：特权用户申请表

特权用户申请表

编号：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 申请人 |  |  | 部 门 |  | 使用时间 |  |
| 权限范围 |  |  | | | | |
|  | 申请理由： | | | | | |
|  | 应用系统管理员审批意见：  签名 年 月 日 | | | | | |
|  | 领导审批意见：  签名 年 月 日 | | | | | |
|  | 注：1. 本表由安全管理员负责填写  2. 本表由应用系统管理员负责存查 | | | | | |

### 附录49：服务器补丁升级记录

服务器补丁升级记录

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 日期 | 更新服务器 | 是否备份 | 备份内容 | 补丁名称 | 补丁类型 | 测试结果 | 备注 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

### 附录50：变更申请单

**变更申请表**

以下内容由发起单位填写

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 发起人 |  | 日期 |  | 要求期限 |  |
| 联系电话 |  | 单位\部门 |  | | |
| 变更内容或需求目标 | 数据变更 应用变更 网络变更 | | | | |
| 业务部门主管意见  （应用变更适用） |  | | | | |
| 分管领导意见  （如有必要） |  | | | | |

以下内容由研发部填写

|  |  |
| --- | --- |
| 系统管理员意见 |  |
| 中心领导审批 |  |
| 承办情况 | 办理人员签字： |

**变更记录表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 变更记录 | | | | | |
| 版本 | 变更日期 | 变更摘要 | 变更人 | 审批人 | 审批日期 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**变更过程记录单**

|  |  |
| --- | --- |
| 变更记录 | |
| 变更任务号：SGBG13- | |
| 变更前描述 | 变更后描述 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 变更实施人： 年 月 日 | |

### 附录51：备份记录

**备份记录**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 备份日期 | 备份时间 | 备份方式 | 存放位置 | 备份人员 | 备份内容 | 备份文件名 | 备注 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 填表说明：备份文件名需要填写备份操作所涉及的备份来源设备（或IP地址、主机名），避免备份文件冲突 | | | | | | | |

### 附录52：恢复记录

**恢复记录**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 恢复日期 | 恢复时间 | 恢复方式 | 恢复文件存放位置 | 恢复人员 | 恢复内容 | 恢复文件名 | 备注 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 填表说明：恢复文件名需要填写恢复操作所涉及的恢复来源设备（或IP地址、主机名），避免误操作 | | | | | | | |

### 附录53：备份与恢复演练记录单

**备份与恢复演练记录**

|  |  |  |  |
| --- | --- | --- | --- |
| 演练名称 |  | 演练时间 |  |
| 组织人 |  | 演练地点 |  |
| 记录内容：  记录人： | | | |
| 参加部门 |  | | |
| 演练结果 |  | | |
| 发现的问题 |  | | |
| 需要改进之处 |  | | |

### 附录54：安全事件记录报告

**安全事件记录报告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 事件发生单位 |  | | | 发生时间 |  |
| 安全事件现象描述  （包括事件发生现象、发生位置、影响范围等） |  | | | | |
| 已经造成的损失和预计损失 |  | | | | |
| 已经采取的措施 |  | | | | |
| 报告人 |  | 报告时间 |  | | |
| 备注 | 发生网络与信息安全事件必须在半小时内口头、1小时内书面报告资鼎(上海)互联网金融信息服务有限公司。较大以上网络与信息安全事件或特殊情况，必须立即报告。 | | | | |

### 附录55：信息安全事件调查报告

|  |  |
| --- | --- |
| 信息安全事件调查报告 | |
| 信息安全事件 |  |
| 信息安全事故描述  轻微：  普通：  重大： |  |
| 信息安全事件  部门/类别及原因分析： |  |
| 控制措施：（可包括资源需求） |  |
| 事件趋势：（和以前相比） |  |
| 汇报人 |  |
| 时间 |  |

### 附录56：硬件维护

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **资鼎(上海)互联网金融信息服务有限公司的“马上货”系统** | | | | |
| **巡检人：** | | **巡检时间** | | |
| **检查内容** | **内存使用率** | **CPU使用率** | **网络状况** | **数据传输** |
|
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 附录57：工作日志

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 工作日志 | | | | | | | |
| 日期 | 序号 | 工作内容 | 完成情况 | 工作详情 | | 实施人员 | 备注 |
| 遇到问题 | 处理情况 |
|  | 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
|  | 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
|  | 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
|  | 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
|  | 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
|  | 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
|  | 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
|  | 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |

### 附录58：信息系统巡检

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **资鼎(上海)互联网金融信息服务有限公司的“马上货”系统** | | | | |
| **巡检人：** | | **巡检时间** | | |
| **检查内容** | **内存使用率** | **CPU使用率** | **网络状况** | **数据传输** |
|
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |