武汉资信管理有限公司

计算机系统安全管理规定

第一章　总则

第一条　为了加强武汉资信管理有限公司（以下简称“公司”）计算机系统管理，保证计算机系统的安全运行，特制定本办法。

第二条　本办法所称计算机系统包括计算机设备、网络、信息和软件。

第三条　计算机设备包括主机服务器、存储设备、台式计算机、笔记本电脑、打印机、网络设备、安全设备、不间断电源、专用空调、其他外围设备等，网络包括局域网、专网和互联网等，信息包括业务数据、管理数据、系统参数等，软件包括系统软件、平台软件、应用软件等。

第四条　本管理规定包括安全管理的组织、人员管理、信息安全管理、网络安全管理、设备安全管理、口令管理、安全技术应用管理、安全事件处理、罚则等内容。

第二章　安全管理的组织

第五条　信息安全管理委员会为信息安全管理的领导组织，负责全公司计算机系统安全运行管理的组织协调及决策工作。公司主要负责人任信息安全委员会主任，安全总监任信息安全委员会副主任，由信息安全委员会副主任主持日常工作。

第六条　信息技术部为信息安全业务管理部门，负责与计算机系统运行相关的信息、设备、网络、软件的安全管理工作。信息技术部门

设置与计算机系统安全管理相关的岗位，分别为系统管理员、网络管理员、数据管理员、安全管理员。

系统管理员负责主机系统、存储系统、系统软件、管理软件、各种应用软件的运行维护工作。

网络管理员负责网络设备、网络访问控制、网络通信线路的运行维护工作。

数据管理员负责数据整理、数据加工、数据备份、数据库管理和数据分析等工作。

安全管理员负责安全设备的运行维护工作，负责设备安全检查、网络安全检查、应用软件系统安全检查、数据安全检查、安全管理制度落实情况检查、机房环境安全检查、信息系统使用权限检查等工作，负责所有安全密码的管理工作。

第七条 组织原则

一、严格授权

对于每一个业务环节都应实行严格的授权制度。操作人员必须在授权范围内进行业务操作。特殊情况下需在授权范围以外进行业务操作的，均应获得公司分管领导书面授权。

二、双人上岗

对关键的业务环节，如数据采集和传递、数据加工处理、软件系统测试、信用报告查询、数据分析、数据备份、数据库维护、设备维护、信息系统的机构和人员维护、系统设置等，应同时指定双人上岗操作，以便形成互相监督、互相制约的机制。

三、岗位分设

对以下业务应分设岗位，由不同的人员进行操作：

1. 系统管理与业务操作

2. 档案资料的使用和保管

3. 安全管理和系统管理

4. 业务经办和业务审批

5. 系统管理和数据管理

第三章　人员管理

第八条 涉及计算机系统运行的所有人员应明确职责和权限。计算机系统的关键岗位必须使用专职人员，须通过严格的政审和业务能力考核。

第九条 应定期对从事操作和维护计算机系统的工作人员进行培训，包括计算机操作维护培训、应用软件操作培训、信息系统安全培训等，保证只有经过培训的人员才能上岗。

第十条 要定期组织对计算机系统所有的工作人员从政治思想、业务水平、工作表现、遵守安全规程等方面进行考核。对于有违反安全法规行为的人员或不适于接触计算机系统关键环节的人员要及时调离岗位。

第十一条 对所有进入信息系统工作的人员，均应签订保密合同，承诺其对系统应尽的安全保密义务，保证在岗工作期间和离岗后，均不得违反保密合同、泄露系统秘密。

第十二条 对调离人员，必须严格办理调离手续，进行调离谈话，明确其调离后的保密义务，收回所有钥匙、密码、证件、技术手册、软件及有关资料，并在系统中撤销其使用权限。

第四章　信息安全管理

第十三条 公司计算机系统信息具体指征信数据、征信指标、系统参数、系统日志、用户权限、征信系统软件等。

第十四条 必须采用必要的安全技术手段保障公司计算机系统信息安全，包括信息加密、设置防火墙、使用用户数字认证、采用入侵检测和防御技术、使用网闸进行网络物理隔离、使用防病毒软件、采用双机热备技术、采用数据备份和恢复技术、对系统操作进行审计等。

第十五条 从计算机局域网或专网导入导出信息必须登记，并经信息技术部门负责人审批，导入导出信息时必须双人上岗操作。

第十六条 从计算机局域网或专网导入导出信息时，只能使用专用媒介，并须做好查毒、杀毒工作，确保信息文件无毒交换。

第十七条 计算机中的涉密文件未经领导批准，不可设置为共享。

第十八条 公司内所有计算机设备必须安装防病毒软件。

第十九条 公司计算机系统信息必须按月备份，并采取有效的防盗、防火、防潮措施，保证备份的安全。

第二十条 系统管理员应对操作系统和数据库管理系统中的系统运行记录（Log）和数据库运行记录进行转储保存以备查。

第二十一条 通过磁盘等媒介人工传递信息，必须实行双人上岗。接收信息的人员拷贝完毕后应立即清空媒介上的文档。

第二十二条 信息技术部门指定专人负责对计算机系统安全进行

每周巡查，发现安全问题及时处理，并向公司领导汇报。

第二十三条 系统的数据必须按照操作规程进行采集、存储、处理、传递、使用和销毁，销毁必须有效且不可恢复。

第二十四条 涉密信息应按相应密级文件进行管理，其复制、分发、输出必须经过公司领导审批。

第二十五条 对于征信信息的数据库，必须有与征信信息密级相适应的安全保密措施，确保征信信息在建库、检索、修改、输出等环节中的安全保密，包括：

（一）使用身份验证机制对用户进行鉴别；

（二）对不同的用户设置不同的用户权限，控制用户对数据的操作权限和访问范围；

（三）建立系统日志和数据库备份。

第五章 应用系统安全管理

第二十六条 应用系统的运行维护由系统管理员负责维护，未经允许任何人不得对信息系统进行任何操作。

第二十七条 根据应用系统的设计要求及实施细则安装、调试、配置应用系统，建立信息系统管理员账号，设置管理员密码，密码要求应符合口令管理要求。

第二十八条 对应用系统的基本配置信息做详细记录，包括系统配置信息、用户帐户名称，系统安装目录、数据文件存贮目录，在应用系统配置信息发生改变时及时更新记录。

第二十九条 当应用系统用户发生增加、减少、变更时，新建用户

帐户需经相关部门审批，并填写系统用户申请单或系统用户变更申请单，审批通过后，由系统管理员进行操作，并做详细记录。

第三十条 根据用户需求设置应用系统各功能模块访问权限，并提交技术部门负责人审批。

第六章　主机安全管理

第三十一条　系统主机由系统管理员负责维护，未经允许任何人不得对系统主机进行操作。

第三十二条　根据系统设计方案和应用系统运行要求进行主机系统安装、调试，建立系统管理员账户，设置管理员密码，建立用户账户，设置系统策略、用户访问权利和资源访问权限，并根据安全风险最小化原则及运行效率最大化原则配置系统主机。

第三十三条　建立系统设备档案包括系统主机详细的技术参数，如：品牌、型号、购买日期、序列号、硬件配置信息、软件配置信息、网络配置信息、系统配置信息，妥善保管系统主机保修卡，在系统主机软硬件信息发生变更时对设备档案进行及时更新。

第三十四条　每月通过系统性能分析软件对系统主机进行运行性能分析，并做详细记录，根据分析情况对系统主机进行系统优化，包括磁盘碎片整理、系统日志文件清理，系统升级等。

第三十五条　定期检查系统主机各硬件设备是否正常运行，并做详细记录。

第三十六条　定期检查系统主机各应用服务系统是否运行正常，并

做详细记录。

第三十七条 在系统主机发生故障时应及时通知用户，用最短的时间解决故障，保证系统主机尽快正常运行，并对系统故障情况做详细记录。

第三十八条 每周对系统日志、系统策略、系统数据进行备份，做详细记录。

第三十九条 每月对系统主机运行情况进行总结、并出具系统主机运行维护月报。

第七章 网络安全管理

第四十条 公司的网络分为征信生产网，征信开发网，互联网。各类网络之间必须物理隔离。互联网上未经批准，严禁存储、运行、传递和发布公司机密信息。

第四十一条 网络设备安装在中心机房内。网络内 IP 地址由信息技术部门统一分配和管理，任何人不得擅自更改。

第四十二条 网络的信息系统在规划和建设时，必须同步规划和落实安全保密管理制度和技术措施。已建成投入使用的信息系统，应完善安全保密管理制度和技术措施。

第四十三条 严禁通过串口、并口、红外、USB 等通讯端口与其它计算机系统（含单机、局域网和广域网）连接。

第四十四条 所有连接到互联网的计算机必须安装相关监控软件。

第四十五条 计算机连接互联网须报公司领导批准，并安装相关监

控软件。

第四十六条 禁止任何人携带非工作用笔记本电脑接入本单位计算机网络。

第四十七条 网络相关安全设备的软硬件配置情况及在网上运行的有涉密内容的各种应用软件，不得对外进行交流。

第四十八条 网络系统应当采取身份鉴别技术，防止冒充、非法访问、重演，并应具备防伪造、防猜测等手段。

第四十九条 网络系统的访问应按权限控制，不得进行越权操作。处理不同密级信息的系统，访问应当按照用户类别控制。

第五十条 网络系统的通信应采用数字签名技术，以验证信息的完整性，对抗冒充、抵赖等威胁。

第五十一条 网络系统应具有审计功能，能够对网络操作进行完整记录。审计跟踪应符合以下要求：

（一）核心业务系统应当有详细的系统日志，记录每个用户的每次活动（访问时间、地址、数据、程序、设备等）以及系统出错、配置修改等信息；

（二）处理征信信息的系统，信息安全管理人员应当定期审查系统日志并作审查记录；

（三）日志由信息技术部门负责人签字，定期上报公司主要领导。

第五十二条 网络上选用的信息安全设备必须使用国家主管部门认可批准的产品。安全设备由安全管理员负责管理，不得随意移动，不得随意更改设置参数。

第五十三条 连接互联网的计算机必须安装防火墙和防病毒软件。

第五十四条 网络管理员应当做好记录，定期检查网络设备运行情

况。

第五十五条 如遇网络故障，应由网络管理员做常规处理，无法修复时，应及时报告并通知厂商处理。

第八章 终端安全管理

第五十六条 公司使用的所有终端必须由信息技术部门登记备案，明确设备责任人，严禁将没有备案的计算机接入网络。

第五十七条 个人办公用终端的保管和日常维护由使用者负责。

第五十八条 终端使用者应做好防尘、防水、防磁、防震等工作。严禁在计算机上运行与业务无关的程序，不得随意更改系统和网络设置、变更网线、加装设备和变更计算机的使用位置。

第五十九条 禁止在工作终端上安装、使用与本职工作无关的软件、硬件系统。禁止利用工作计算机、网络或上网工作站玩游戏、看影碟。

第六十条 终端若出现故障，指定的使用者应及时向系统管理员反映，由系统管理员及时查明原因，组织维修。

第六十一条 对未特别指定使用者的终端由信息技术部门负责保管和维护。

第六十二条 员工原则上只能使用分配给本人的终端。未经当事人同意，不能擅自在他人的终端上进行任何操作。

第六十三条 所有终端设备，未经授权同意，不得擅自改变位置、拆换任何零件、配件、外设。

第六十四条 个人不得擅自将私有或外来的零件、配件、设备，加

入到本办公区终端或网络中。

第六十五条 所有连接到公司信息网络的终端必须封闭所有的 IO 接口，封闭机箱，任何人不得擅自开启。

第六十六条 任何人未经相关领导批复，禁止外借终端及其附件给其它单位和个人使用。

第六十七条 终端在使用完毕后应及时关闭终端和电源。

第六十八条 信息技术部门指定专人每周对所有终端进行全面的安全检查，并做好检查记录。

第九章 口令管理

第六十九条 计算机、网络设备须使用口令对用户的身份进行验证和确认。对于重要系统，由安全管理员负责日常的密码管理工作。安全管理员将密钥资源等级造册，每月修改密码一次，将现行可用的密钥记载并装入密码封中交公司主要领导封存保管。

第七十条 安全管理员负责为新增加的用户分配初始口令，指导用户正确使用口令；检查用户使用口令情况，帮助用户开启被锁定的口令；对非法操作及时查明原因；解决口令使用过程中出现的问题；协助用户保护信息不受侵害。

第七十一条 安全管理员必须有能力更改口令。当口令使用期满、被其他人知悉或认为口令不保密时，安全管理员可按照口令更改程序变换口令。口令更换操作应在保密条件下进行。

第七十二条 信息系统的身份认证应当符合以下要求：

（一） 处理核心信息的系统，口令长度不得少于八个字符，并且应包含英文字母、数字、符号。口令更换周期不得长于一月；

（二） 口令必须加密存储，并且保证口令存放载体的物理安全；

（三） 口令在网络中必须加密传输。

第七十三条 用户应记住自己的口令，不应把它记载在不保密的媒介物上，严禁将口令贴在终端上。输入的口令不应显示在显示终端上。

第十章 安全技术应用管理

第七十四条 安全技术系统包括集中监控与审计系统、补丁分发系统、防火墙、入侵检测系统、漏洞扫描系统、防病毒系统等。

第七十五条 安全技术的应用管理由信息技术部门负责。

第七十六条 安全管理员对安全技术系统的进行监测，及时进行安全技术系统的升级，对出现的异常现象进行处理，保证安全技术系统处于完好可用状态。

第七十七条 安全管理员应根据实际情况及时对安全技术系统的策略进行调整。安全技术系统的任何配置变动，需经过分管领导审批后，由安全管理员进行配置。

第七十八条 对安全技术系统的配置和使用必须做好详细记录。每月对安全技术系统的数据、配置、日志进行备份。安全技术系统日常运行维护相关的日志、文档不得随意涂改，并定期存档。

第七十九条 任何单位和个人不得制作计算机病毒。

第八十条 任何单位和个人不得有下列传播计算机病毒的行为：

（一） 故意输入计算机病毒，危害计算机信息系统安全；

（二） 向他人提供含有计算机病毒的文件、软件、媒体；

（三） 在计算机系统内使用非法软件、无合法版权软件或其他无明确来源的软件系统。

第八十一条 因工作需要在从计算机信息网络上下载程序、数据或者购置、维修、借入计算机设备时，必须进行计算机病毒检测。

第八十二条 禁止使用不知来源的软盘、光盘和程序。所有外来安装软件和升级软件必须经过查毒无误后方可使用。

第十一章 应急预案管理

第八十三条 信息技术部门应制定各种意外事件处置预案，并具体执行，包括线路故障、设备故障、长时间停电、火灾等，每年进行预案演练。

第八十四条 出现安全事件，值班人员应及时报告，并及时采取有效措施，将损失降到最小。对出现的安全事件应作好记录备查。

第八十五条 线路故障应立即拨打线路故障电话，同时上报部门负责人，协助电信部门查找故障原因，尽快使线路恢复正常。

第八十六条 遇到火灾应根据火情采取以下措施：

1. 如火情较轻时，应立即切断机房总电源，并迅速用消防器材，力争把火扑灭、控制在初期阶段，同时上报集团保卫部门。

2. 如火情严重应迅速拨打报警电话“119”，同时通知集团综合管理部门，听从消防工作人员的现场指挥，协助处理有关事项。

第八十七条 如遇机房突发性停电，且超过备用电源可用时间，应及时通知用户，同时关闭设备电源，来电后，及时通知用户，并检测

设备是否正常运行。

第八十八条 系统出现灾难性故障时，系统管理员应立刻通知部门负责人，并按照制定的系统恢复方案执行。

第八十九条 遇紧急情况，值班员应立即通知保密办和系统管理员，保持 24 小时通讯畅通，随时处理紧急事件。

第九十条 水灾发生时，应切断电源，迅速报告有关部门，尽可能地弄清水灾原因，采取关闭阀门、排水、堵漏、清除等措施。

第九十一条 地震发生时，应切断电源，避免引发短路和火灾。

第九十二条 发生紧急事件后，要对信息系统的安全策略、安全结构、安全服务和过程进行全面的检查，并对其进行完善。

第十二章 灾难备份管理

第九十三条 信息技术部门应建立完整的灾难备份系统。完整的灾难备份系统应由数据备份系统、备份数据处理系统、备份通信网络系统和完善的灾难恢复计划所组成。

第九十四条 灾难恢复要求全系统离线冗余备份。备份介质应定期转移到异地保管，保证能够用于灾难恢复。

第九十五条 每月必须对各服务器进行灾难备份，并妥善保管灾难备份磁带。一旦服务器配置发生变化，应立即重新制作灾难备份磁带。

第十三章 罚 则

第九十六条 对公司违反本规定的部门和个人，由信息技术部对有关责任人员进行培训教育，责令其限期整改，对限期整改不到位的有

关责任人员由信息技术部门向公司总经理进行报备，并进行全公司通报批评，扣减当月绩效。

第九十七条 有下列危害公司系统安全行为之一的，给予有关责任人员扣减绩效至记过处分；造成严重后果的，给予记大过至开除处分，触犯法律的，移送国家司法机关处理。

1、私自卸载或屏蔽计算机安全软件的；

2、利用邮件系统传播损害公司形象的；

3、利用公司计算机设备和网络系统制造、传播计算机病毒的；

4、将属于公司的计算机软件、文档、资料、客户信息等据为己有、复制或者借给外单位的；

5、对擅自编制、使用、修改业务应用程序、调整系统参数和业务数据的。