数据库管理制度

第一章　总则

第一条 为加强公司构数据库管理，保障评级数据库正常、有效运行，确保数据库安全，使数据库能更好地服务于信用评级工作，特制定本制度。

第二条 本制度所称的数据库数据是指纳入公司管理系统中的所有信用评级业务数据。

第三条 本制度适用于公司所有信用评级业务的数据管理，包含但不限于评级信息采集、累计分析数据、业务管理等数据内容。

第四条 评级业务数据库录入的数据源主要包括产权状况、管理层素质、从业人员素质、行政监管、司法监管、管理制度、管理体系、行业产业政策、成长性和抗风险能力、财务数据等。

第二章　管理机构和职责

第五条 数据库实行专业责任制。各部门负责人为专业负责人，全面负责本部门专业数据模板的制作、数据采集和日常维护的管理。部门内分工负责，责任到人。

第六条 公司总经理负责对数据库使用者进行权限审批。

第七条 公司技术专员负责评级数据库的日常维护和运营管理。

第八条 客服专员负责初步调查数据的录入。

第九条 评级项目组组长负责评级信息的录入。评级项目组组长应在评级报告出具后三十日内将该评级项目的相关评级信息输入数据库。

在评级档案归档前，评级项目组组长负责对录入数据资料进行格式和内容进行一级核审，部门负责人二级复审。

若信用评级项目在评级过程中因故终止或暂停，已录入的数据资料永久保存。

第三章 数据保存

第十条 数据保存方式

本制度所指的所有信用评级业务的数据均以电子数据的方式保存，其他类型数据的管理依据《评级档案管理制度》执行。

第十一条 数据保存期限

在公司评级业务存续的情况下，评级业务建立的数据库将永久保存。

第十二条 公司解散或者被依法宣告破产的，应当向备案机构报告，并按照以下方式处理信用评级数据库系统：

（一）与其他信用评级机构约定，转让给其他信用评级机构；

（二）不能依照前项规定转让的，移交给备案机构指定的信用评级机构；

（三）不能依照前两项规定转让、移交的，在备案机构的

监督下销毁。

公司应按照上级监管主体的要求制定数据库数据的处理方案，并指定专人负责对数据库数据进行处理，且相关人员将对数据库数据继续负有保密义务。

公司员工离职时，综合部应将离职人员信息及时通知技术专员，技术专员应在离职人员离职后，及时将其系统权限等关闭，将载有保密信息的任何文件、资料或软件、程序按公司要求归还或予以销毁，删除任何有记忆装置中的保密信息。

第四章　标准管理

第十三条 数据库要严格执行统一的数据库逻辑结构标准，统一的指标库标准，统一的数据模板标准。各部门不得擅自在统一执行的表结构中增加、删除、修改有关字段；不得擅自增加、删除、修改指标库中的指标。

第十四条 各部门认为数据库标准有错误或不合理的地方，应及时通知技术专员。相关信息化项目的数据库调整需经部门负责人审批通过后由技术专员统一处理。对于未信息化项目数据模版修改由相关部门负责人审批通过后，相关部门自行调整，调整后数据模版提交技术专员备案。

第十五条 技术专员统一下发数据库模板标准，数据库数据严格按模板标准采集。

第十六条 数据库数据源为信息化项目流程采集以及相关

部门自行采集、定义。

第十七条 各部门应根据管理要求、业务要求按时提交数据。

第十八条 各部门全面负责采集数据的质量。按模板格式采集数据后，方可载入数据库。

第十九条 技术专员每月定期对入库的数据进行技术性检查，检查数据存储的位置、格式和数据完整性等。

第二十条 各部门接到技术专员的数据审核情况反馈后，若无差错则本月数据校验完成；若有错误，则重新采集、调整，期限不得超过两日。

第五章　权限管理

第二十一条 技术专员拥有数据库服务器及数据库的管理员权限，对数据库的日常运作进行全面管理维护。

第二十二条 技术专员应当确定数据库各类数据的修改权限，避免数据库的人为损坏。

第二十三条 本数据库用户权限分为普通用户和高级用户。

本数据库的数据分为非加密数据和加密数据两大类。普通用户享有对数据库中非加密数据的查询权限，并拥有录入数据和修改本人录入数据的权限；高级用户享有对加密数据的查询权限。

评估师和各部门负责人根据事先确定的权限使用数据库和其中的评级信息。

第二十四条 公司数据库使用人员在进行严格的身份验证后，方可按照相应权限进行数据录入、更新或查询操作。

第六章 用户管理

第二十五条 用户有权使用授权许可范围内的数据库数据，且负有该数据的安全保密义务。

第二十六条 用户口令必须设置 6 位以上字符，并包含既有字母、数字，又有如“@”、“#”、“$”等的特殊字符。口令应至少每个月更改一次。用户名和口令为个人专用，不得给予他人使用，如确有事情外出并要委托他人代办，回来后应及时更改口令。

第七章 安全管理

第二十七条 技术专员负责数据库系统的安全管理，保证安全管理软件的及时升级。

第二十八条 为保证公司数据库的安全运行，技术专员必须遵守下列安全操作规定：

（一）严格按照预先设定的操作权限操作，严禁越权操作，技术专员须对自己用户名下的所有操作负责；在数据库系统上进行的操作要留痕以方便追溯；

（二）制定备份策略，隔天进行一次完整备份，备份数据至少保持三份并场外存放，备份介质包括网络存储、专用移动硬盘灯，保存期限至少半年以上；

（三）数据库运行期间，技术专员应对数据库的运行日志及使用情况进行监控，以便及时发现存在的问题，同时采取严格的安全措施，禁止无关人员接触数据服务器；

（四）数据库使用人员对数据库汇总的信息内容负有保密义务，未经本公司允许，不得将数据库中的信息泄露给其他机构和个人；

（五）技术专员不得进行数据的录入、修改和更新，如确需对数据实时维护，应报请公司总经理批准后方可实施。

第二十九条 技术专员要保证数据库出现异常时能快速恢复，避免或尽量少数据丢失。

第八章　防火墙管理

第三十条 防火墙设备部署位置的环境应满足相应的国家标准和规范，以保证防火墙设备的正常运行。

第三十一条 防火墙设备应定期检测和维护：

（一）每月定期安装、更新厂家发布的防火墙补丁程序，及时修补防火墙操作系统的漏洞，并做好升级记录；

（二）一周内至少审计一次日志报表；

（三）一个月内至少重新启动一次防火墙；

（四）根据入侵检测系统、安全漏洞扫描系统的提示，适时调整防火墙安全规则；

（五）及时修补防火墙宿主机操作系统的漏洞；

（六）对网络安全事故要及时处理，保证信息网络的安全运行。

第三十二条 防火墙设备安全规则的设置、更改，由技术专员具体负责实施。

更改防火墙安全规则之前对正在运行的安全规则必须进行备份，以便于修改防火墙安全规则失败后能够快速恢复正在运行的安全规则。

技术专员应定期和不定期地检查防火墙设备的运行状况，及时查看防火墙日志，对异常情况的发生，及时上报，并做好记录。

第九章　附则

第三十三条 本制度由综合部负责解释。

第三十四条 本制度自发布之日起执行。