评级业务信息管理制度

标普信用评级（中国）有限公司
生效日期：2019 年 8 月 1 日
最新修订日期：2024 年 6 月 21 日
标普信用评级（中国）有限公司员工应遵守本制度。

第一章 总则

第一条 为加强标普信用评级（中国）有限公司（以下简称“公司”）对评级业务信息的管理，保障在评级项目实施的过程中公司和评级对象等相关方的信息安全，维护信息权利人的合法权益，特制定本制度。

第二章 信息分类、定义与等级划分

第二条 评级业务信息根据保密级别划分为两类：普通信息和保密信息。

第三条 普通信息分类：包括公开信息和仅限内部使用的信息。

1.公开信息

指通过公开途径可获取或已被广泛公开的信息。这类信息通常无需采取保密措施。公开信息的来源多样，包括但不限于：政府及监管机构的官方网站、新闻媒体、行业分析报告以及数据服务提供商等。此类信息涵盖领域广阔，诸如公开发行债券的信用评级报告及结果、上市公司的财务报告以及公司的注册信息、行业归属、业务领域等内容。

2.仅限内部使用的信息

指在公司内部交流使用，不适宜对外公开的信息。“仅限内部使用”是信息的默认分类，该类信息是非敏感的、不受合同机密性限制的，并且根据法律规定无需对其保密。该类信息包括但不限于：基于公开信息整理和加工的评级材料、模型、数据库等。

第四条 保密信息分类：包括机密信息和高度机密信息。

1.机密信息

指对公司日常运营、业务发展、市场竞争力和客户关系等方面具有显著影响的信息，这类信息的泄露可能会对公司的商业利益、市场地位和声誉造成直接的负面影响。机密信息的范围包括但不限于：

- 评级业务委托协议和收费信息、保密协议、承诺函等文件；

- 在评级过程中获取的，涉及委托方或发行人经营、财务状况或者对该公司证券市场价格产生重大影响的未公开信息；
- 根据委托方和监管部门的要求，尚未对外发布和披露的评级报告（包括评级报告的中间稿）、评级结果和数据表格等资料信息；
- 评级项目评审资料、信评委会议纪要、工作记录、表决过程和表决结果等内部文件；

机密信息仅限相关人员（指基于其工作职责和角色，确实需要知道机密信息以完成工作任务的员工）知晓。

2.高度机密信息

指对公司具有极端重要性，一旦泄露，将对公司的长期战略利益、法律合规性以及国家安全等方面造成极其严重后果的信息，属于公司最高级别的保密内容。这类信息通常涉及公司的核心商业秘密、国家安全或国际关系等敏感领域。高度机密信息的范围包括但不限于：

- 军工企业或其他涉及国家安全的评级项目资料；
- 监管机构特别指出的、对外部具有重大敏感性的保密资料和文件。

高度机密信息仅允许在监管部门、信息提供方或公司高级管理层的批准下，由特定人员接触。

第三章 保密协议与保密义务

第五条 公司开展证券评级业务前，应当与评级委托方、受评级机构或受评级证券发行人签订保密协议或在评级协议中约定保密条款。

第六条 除法律法规要求、公开信息渠道获取、受评企业或第三方公开外，公司对于受评企业书面提出保密要求的相关信息应承担保密义务，不得向第三方提供或对外披露。对于在开展信用评级业务过程中知悉的国家秘密、商业秘密和个人隐私，公司应当依法履行保密义务。但下列情况除外：

(一)国家司法机关、政府监管部门和协会等自律组织按照有关规定进行调查取证的；

(二)有关法律、法规要求提供的；

(三)依据保密协议或保密条款可以公开的。

第七条 在评级信息依法披露之前，除用于监管要求、评级协议约定用途、委托方及评级对象外，公司应当履行信息保密义务，不得向内部其他人员和外部泄露相关评级信息。

第八条 评级从业人员在项目结束或离开公司后仍应当履行保密义务。

第四章 信息处理与存储规范

第九条 公司在中国境内采集的评级信息的整理、保存和加工，应当在中国境内进行。向境外组织或者个人提供信息，应当遵守法律法规以及信用评级行业主管部门和业务管理部门的有关规定。

第十条 公司需根据信息的分类进行相应的存储和处理，以保障信息安全得到有效的维护。

第五章 数据管理与安全措施

第十一条 为保障评级业务数据管理的规范性和安全性，数据维护负责人（以下简称“负责人”）需建立信息权限管理要求，明确相关角色员工的数据访问权限，并定期进行权限审查与调整。此外，负责人应参与制定数据安全措施的标准，包括数据加密、访问控制、网络安全等，以及在数据泄露或其他安全事件发生时的事故响应计划，确保能迅速有效地应对并最小化损失。在执行这些职责时，负责人需与分析团队、合规团队、信息技术团队等相关部门进行跨部门协调，确保数据管理流程的顺畅和高效，共同维护公司的数据安全和信息保密。

第六章 数据库建设与运维

第十二条 公司根据评级业务开展和评级技术研究的需要，建设统一的信用评级数据库和技术系统。

第十三条 数据库应包括机构自身采集、数据积累及分析、机构业务管理等数据。数据内容的保存期限、保存方式和更新时间应符合国家相关法律和监管机构相关规定。

第十四条 公司终止信用评级业务时，应当按照国家相关法律和监管机构相关规定，对信用评级数据库进行妥善处置。

第十五条 公司信息技术团队负责信用评级数据库的建设和运维管理。

1. 信息安全团队

- 与相关团队共同制定信息安全领域的制度、规范、标准流程和操作手册并进行版本维护；
- 负责协助员工履行信息安全职责及相关规定，组织信息安全培训和宣传；
- 监督在信息系统访问控制方面的日常工作，维护公司的系统管理员名单；
- 监督日常运维中定期安全检查；
- 在开发生命周期过程中提供信息安全相关建议，监督安全开发相关控制要求；
- 定期执行漏洞扫描和渗透测试工作；
- 负责加密密钥的管理和监督。

2. 信息技术基础架构运维团队

• 负责遵守公司信息安全政策，协助信息安全团队制定相关领域的信息安全流程和操作手册；
• 网络管理员及系统管理员应负责新系统上线前开展对应用系统、操作系统、数据库和网络进行信息安全检查；
• 系统管理员负责系统的日常安全管理，及时向信息安全团队报告信息安全问题；
• 负责服务器的安装、配置和安全管理，监控服务器的运行情况，负责服务器的应急 计划和故障恢复，服务器的资产管理和变更；
• 为信息安全系统的运行和监控提供工具；
• 配合内外部审计，对不符合项实施修正；
• 负责公司数据中心和服务器机房区域物理环境的安全管理；
• 负责公司网络架构的建立、优化和维护，管理日常运营中网络设备的运行安全，并立即响应和解决网络安全事件；
3. 信息技术应用开发团队：
• 根据公司评级业务开展和评级技术研究的需要，建设公司综合信息系统和平台。
• 负责遵守公司信息安全政策，协助信息安全团队制定相关领域的信息安全流程和操 作手册；
• 负责及时报告日常工作中发生的安全事件
• 配合内外部审计，对不符合项实施修正；
• 负责协助制定访问管理规则，并在日常工作中负责系统的访问控制；
• 负责在应用程序开发流程中的信息安全设计、评估等工作。

第七章 附则

第十六条 本制度仅适用于评级业务信息，对于其他类型信息的管理由公司另行规定。

第十七条 本制度由制度评审委员会负责解释、修订，通过之日起执行。