信息系统安全管理办法

East credit

评级内控制度

制度编号：PJ/NK.011
制度版本：V3.0
生效日期：2020年8月1日
修订日期：2023年10月11日
2024年12月30日

声 明

本版本制度基于 2023年10月11日发布的《信息系统安全管理办法》修订，经东方资信资信评估有限公司（以下简称“东方资信”或“公司”）总经理办公会审议通过，自发布之日起取代原版本文件执行。此制度生效日前已完成的项目，不再变更和追溯。

东方资信享有对本制度的最终解释权。本制度执行过程中，东方资信有权根据外部环境变化、公司治理需要对制度进行修订、增补、废止。监管政策变化导致与本制度不一致时，在本制度变更前，应首先依据监管规定执行。

本制度文件是东方资信评级业务管理一般性规范文件，用于业务指导，具体业务开展与完成可在本制度指引下另立细则。如因本制度规定而导致某项具体项目或业务开展受到局限时，东方资信将针对具体情况给予特别说明。

本制度的制定符合中华人民共和国相关法律、法规规定，东方资信将根据国家法律法规、监管规定的变化适时调整本制度文件，同时会定期针对本制度执行情况进行评估和内部审核，并依据评估结果适当更新制度版本。

信息系统安全管理办法

第一章 总 则

第一条 为加强公司评级系统和信息的安全管理，提高信息资源的运作成效，防范各种来自内部和外部的信息安全隐患，杜绝各类信息安全事故的发生， 制订本制度。

第二条 本制度适用于公司各部门。

第三条 制度所指的评级信息设备和评级信息系统和评级信息，是指公司内由涉及评级的各种网络设备、运用服务器、办公电脑、终端设备和各种数据库、程序、图表等电子文档及必要的系统软件、应用软件构成。

第四条 公司设专职信息管理员及评级部负责人，负责管理涉及评级信息的所有信息设备、信息系统、信息安全管理工作。

第二章 设备管理

第五条 信息设备实行“谁使用谁负责”的原则（公用设备责任落实到人）。使用人要保持清洁、安全、良好的设备工作环境，禁止在计算机应用环境中放置易燃、易爆、强腐蚀、强磁性等有害计算机设备安全的物品。

第六条 严禁擅自移动和装拆各类设备及其他辅助设备；严禁擅自请人维修；严禁使用假冒伪劣产品；严禁擅自调整部门内部信息设备的安排；严禁在私人电脑上处理与工作相关的数据。

第七条 凡登记在案的信息设备，由信息管理员统一管理并张贴设备卡。设备卡作为相应设备的标识，各使用人有义务保证贴牌的整洁与完整，不得遮盖、撕毁、涂画。

第八条 员工因工作需要发生调动，需要继续使用该计算机的应在信息管理员处作变更备案；因离职等原因不继续使用该计算机的，部门领导需监督责任人将计算机及相关设备及时退回。

第九条 公司员工因工作需要，确需购买信息设备或配件的，可向公司提出申请，由公司进行调配或购置。若因工作需要对设备配置有特殊要求的，需说明。

第十条 设备硬件或操作系统等故障报信息管理员进行处理。非本公司人员对我单位的设备、系统等进行维修、维护时，必须由本公司相关人员现场全程监督。信息设备送外维修的，须经公司负责人批准。

第三章 用户管理

第十一条 用户分为管理员与普通用户两种。管理员分为网络管理员、系统管理员、子系统管理员、分模块管理员等级别，不同级别的用户拥有不同的使用权限。

第十二条 系统管理员账号由信息管理部管理和使用，普通账号由用户自行保管。用户应保管好自己的登录帐号和密码，严禁随意向他人泄露、借用自己的帐号和密码；严禁使用他人账号登录系统。用户应定期更改密码、 使用安全性较高的密码。

第十三条 新员工入职或岗位变更，由综合管理部向信息管理员报送员工基础信息，分配相应的系统账号和登录密码、设置对应的使用权限。 员工离职，由公司综合管理部向信息管理员报送员工信息，由

信息管理部删除其相应系统的账号和使用权限。

第十四条 网络管理员、系统管理员、操作员调离岗位后一小时内由接任人员监督检查更换新的密码；厂方设备调试人员调试维护完成后一小时内，由系统管理员关闭或修改其所用帐号和密码。

第四章 操作管理

第十五条 严禁利用公司网络和计算机从事与工作无关的事情；严禁非信息管理人员随意更改各种信息设备配置。

第十六条 评级用计算机未经允许不准安装其它软件、不准使用来历不明的载体（包括软盘、光盘、U 盘、移动硬盘等）。

第十七条 凡涉及业务类的专业软件、程序、文件，具体业务操作和人员培训由使用部门和个人自行负责。

第十八条 信息管理员将有针对性地对员工的计算机应用技能进行定期或不定期的培训，由信息管理部收集计算机信息系统常见故障及排除方法并整理成册，

供公司员工学习参考。

第十九条 公司指定专人负责计算机病毒的防范工作，建立公司的计算机病毒防治管理制度，经常进行计算机病毒检查，发现病毒及时清除。

第五章 数据管理

第二十条 用户计算机内的资料涉及评级信息的，应该为计算机设定开机密码或将文件加密；凡涉及评级信息的数据或文件，非工作需要不得以任何形式转移，更不得透露给他人。

第二十一条 工作范围内的重要数据（重要程度由各部门经理核定）由计算机终端用户定期更新、备份，并提交给所在部门经理，由部门经理负责保存。各部门经理在一个季度开始后 10 天之内，将本部门上一季度的工作数据交综合管理部，统一汇集后采用磁性介质或光盘保存，并归档造册。数据的查阅和复制必须严格按照程序进行逐级审批，做好详细登记，严禁擅自复制外传。

第二十二条 终端用户务必将有价值的数据存放在除系统盘（电脑 C 盘）以外的盘上。计算机系统发生故障，应及时与信息管理员联系并采取保护数据安全的措施。

第二十三条 终端用户未做好备份前不得删除任何硬盘数据。对特别重要的数据应备份双份，存放在不同的地点；对采用磁性介质或光盘保存的数据，要定期进行检查，每使用依稀就进行复制，防止由于磁性介质损坏，而使数据丢失；做好防磁、防火、防潮和防尘工作。

第二十四条 任何业务数据的使用及存放数据的设备或介质的调拨、转让、废弃或销毁必须严格按照程序进行逐级审批，以保证备份数据安全完整。

第二十五条 数据恢复前，必须对原环境的数据进行备份，防止有用数据的丢失。数据恢复后，必须进行验证、确认，确保数据恢复的完整性和可用性。

第六章 处罚措施

第二十六条 有以下情况之一者，视情节严重程度给予相应的经济处罚。触犯国家法律的，移交司法机关处理。

（一） 制造或者故意输入、传播病毒以及其他有害数据的；

（二） 非法复制、截收、篡改评级信息系统中的数据危害信息系统安全的；

（三） 对网络和信息设备进行恶意攻击；

（四） 访问未经授权的文件、系统或更改设备设置；

（五） 擅自与他人更换使用计算机或相关信息设备；

（六） 简易故障出现三次以上（包括三次）仍无法自行处理的；

（七） 擅自调整部门内部计算机的安排且未向信息管理部备案；

（八） 日常抽查、岗位调动、离职时检查到计算机配置与该计算机档案不符、设备卡被撕毁、涂画或遮盖等；

（九） 擅自下载、安装或存放与工作无关的文件；

（十） 未经许可擅自将公司内部资料对外传阅或发布到互联网上，情节严重的；

（十一） 工作时间利用公司网络和计算机做与工作无关的事情如：炒股、聊天、网购、打游戏、看电影等;

（十二)因工作需要长时间(五个小时以上)离开办公位置或下班后无故未将计算机关闭；

第二十七条 计算机终端用户因主观操作不当对设备造成破坏两次以上或蓄意对设备造成破坏的，视情节严重，按所破坏设备市场价值的 50%-80% 赔偿，并给予行政处罚。 。