第一章 总则
第一条 为加强和规范木头云交易平台，以及各部门网络信息和交易安全工作，提高平台交易安全系统防护水平，实现网络信息安全的可控、能控、在控，依据国家有关法律、法规的要求，特制定本方针。
第二条 本文档汇编的目的是为木头云交易平台网络安全管理提供一个总体的策略性架构文件，以便提高整体网络安全水平，确保安全控制措施落实到位，保障平台的网络通信畅通和各类业务系统的正常运营。
第三条 本文档适用于确保本平台用户交易的整体安全：
第二章 方针、目标和原则
第四条 平台交易安全管理坚持“安全第一、预防为主，管理和技术并重，综合防范”的总体方针，实现可控、能控、在控。依照“分区、分级、分域”总体安全防护策略，执行网络安全等级保护制度。管理信息网络分为信息内网和外网，实现“双机双网”，内网定位为承载涉密数据，外网定位为对外业务网络和访问互联网用户终端网络。内、外网之间实施强逻辑隔离的措施。
第五条 网络信息安全总体目标是确保信息系统持续、稳定、可靠运行和确保信息内容的机密性、完整性、可用性。
（一）防止因信息系统本身故障导致信息系统不能正常使用和系统崩溃；
（二）防止数据尚未进行严格加密造成的数据泄露风险；
（三）防止缺乏有效可行的网络安全组织管理制度，所导致的信息系统操作权限混乱和开发运维工作人员不拆分造成的潜在风险；
（四）抵御黑客、病毒、恶意代码等对信息系统发起的各类攻击和破坏；
（五）防止各种意外突发事件造成信息系统内容及数据丢失和失密；
（六）防止有害信息在网上传播；
（七）防止本平台对外服务中断和由此造成的系统运行事故；
第六条 信息安全工作的总体原则
（一）基于安全需求原则
平台技术部门应根据其信息系统设立理念，积累的信息资产的重要性，可能受到的威胁及面临的风险分析安全需求，按照信息系统等级保护要求确定相应的网络信息安全保护等级，遵从相应等级的规范要求，从本平台网络信息安全需求上恰当地平衡安全投入与效果；
（二）主要领导负责原则
主要领导应确立其组织统一的信息安全保障的宗旨和政策，负责提高员工的安全意识，组织有效安全保障队伍，调动并优化配置必要的资源，协调安全管理工作与各部门工作的关系，并确保其落实、有效；
（三）全员参与原则
信息系统所有相关人员应普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障网络信息安全；
（四）系统方法原则
按照系统工程的要求，识别和理解信息安全保障相互关联的层面和过程，采用管理和技术结合的方法，提高实现安全保障的目标的有效性和效率；
（五）持续改进原则
安全管理是一种动态反馈过程，贯穿整个安全管理的生存周期，随着安全需求和系统脆弱性的时空分布变化、威胁程度的提高、系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进信息安全管理体系的有效性；

（六）依法管理原则
信息安全管理工作主要体现为管理行为，应保证网络信息安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响；
（七）分权和授权原则
对特定职能或责任领域的管理功能实施分离、独立审计等实行分权，避免权力过分集中所带来的隐患，以减小未授权的修改或滥用系统资源的机会。任何实体（如用户、管理员、进程、应用或系统）仅享有该实体需要完成其任务所必须的权限，不应享有任何多余权限；
（八）选用成熟技术原则
成熟的技术具有较好的可靠性和稳定性，采用新技术时要重视其成熟的程度，并应首先进行多轮测试后才能逐步推广，以减少或避免可能出现的失误；
（九）分级保护原则
按等级划分标准确定信息系统的安全保护等级，实行分级保护；对多个子系统构成的大型信息系统，确定系统的基本安全保护等级，并根据实际安全需求，分别确定各子系统的安全保护等级，实行多级安全保护；
（十）管理与技术并重原则
坚持积极防御和综合防范，全面提高安全防护能力，采用管理与技术相结合，管理科学性和技术前瞻性结合的方法，保障信息系统的安全性达到所要求的目标。
第七条 在规划和建设信息系统时，防护措施应按照“三同步”原则，与信息系统建设同步规划、同步建设、同步投入运行。
第三章 总体安全策略
第八条 物理安全策略
物理层的安全设计应从三个方面考虑：环境安全、设备安全、线路安全。采取的措施包括：机房屏蔽、电源接地、布线隐蔽、传输加密。
第九条 网络安全策略
（一）网络中必须部署路由器、交换机、防火墙、防毒墙、IPS 设备和内网网络管理、补丁分发等系统；
（二）网络设备除接入交换机之外，必须进行双机热备，除接入交换机链接工作终端的线路外，其他线路必须进行双线冗余；
（三）整体网络不能出现流量瓶颈，保证带宽充足；
（四）各部门必须划分不同网段的 IP 地址；
（五）划分网络带宽，突出优先级；
（六）网络边界处必须部署防火墙、IPS 等安全设备；
（七）网络设备必须开启日志审计功能。
第十条 主机安全策略
（一）本平台所有技术人员，在登录操作系统和数据库系统的用户时必须进行身份标识和鉴别；
（二）操作系统和数据库系统管理用户身份标识不能出现同名用户，口令应有复杂度要求并定期更换；
（三）操作系统和数据库系统必须启用登录失败处理功能；
（四）对服务器进行远程管理时，必须采取必要措施，防止鉴别信息在网络传输过程中被窃听；
（五）为操作系统和数据库系统设置操作权限，不同用户分配不同的权限，进入信息系统不同操作模块；

（六）为用户设置不同的用户名，确保用户名具有唯一性，不能出现重名情况；
（七）操作系统和数据库必须及时删除多余的、过期的账户，避免共享账户的存在；
（八）主机必须开启日志审计功能；
（九）主机必须安装防恶意代码产品，并进行统一管理。
第十一条 应用安全策略
（一）应用系统必须在登录时要求输入用户名和口令；
（二）登录应用系统必须进行两种或两种以上的复合身份验证（如用户名口令+Ukey 或用户名口令+IP 与 MAC 地址绑定方式）；
（三）应用系统中设置的用户都必须是唯一用户，不能有相同名称，且不能出现多人使用同一账户的情况；
（四）应用系统必须开启登录失败处理功能；
（五）应用系统必须开启登录连接超时自动退出等措施；
（六）应用系统必须开启身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数；
（七）应用系统必须开启日志审计功能；
（八）应用系统存储用户信息的设备在销毁、修理或转其他用途时，必须清除内部存储的信息。
第十二条 数据安全策略
（一）业务应用数据和设备配置文档都必须进行备份，以便发生问题时可以恢复；
（二）数据备份至其他设备上时，必须使用专门的备份数据链路，保证数据传输的完整性；
（三）数据本机备份时应检测其完整性；
（四）数据备份时必须使用专业的备份设备和工具，在数据传输和数据存储时，都必须是加密传输和存储；
（五）数据进行异地备份时，必须利用通信网络将关键数据定时批量传送至备用场地；
（六）为应对突发事件，除日常常规数据备份外，还必须着手搭建应用级异地灾备系统设施。
第四章 附则
第十三条 本办法由本平台网络与信息安全领导小组负责解释并督促执行。
第十四条 本平台各部门可根据本办法制定实施细则，报本平台网络与信息安全领导小组备案。
第十五条 本办法自发布之日起执行。

东莞市木头云供应链有限公司
2019 年 1 月 6 日