Manifold

PLANO DE SEGURANÇA, PRIVACIDADE E REGRAS DE EXECUÇÃO

Plataforma Moola

Preparado por: Manifold, Lda

Nome institucional: MANIFOLD

Preparado para: Cliente

Referência do documento: MFD-MOOL-AUD-2026-ROE-A1

Revisão: A1

Data de emissão: 15/07/2026

Estado: Final para aprovação antes dos testes

Classificação: Confidencial

---

1. Controlo do Documento

Revisão	Data	Descrição	Preparado por	Revisto por	Aprovado por
A1	15/07/2026	Revisão final do plano, ativos-base e regras de execução	MANIFOLD	Vayile Fumo	Rogerio Casimiro

1.1 Documentos de referência

Documento	Descrição	Estado
Statement of Work	Ativos, atividades, limites e responsabilidades.	Documento associado
Pacote Contratual - NDA e DPA	Obrigações de confidencialidade e proteção de dados.	Documento vinculativo
Proposta Executiva e Técnica	Metodologia e workstreams.	Documento associado
Inventário de ativos autorizado	Ativos e ambientes efetivamente abrangidos.	A produzir na Fase 0

2. Objetivo e Aplicação

Este documento define as medidas de segurança, privacidade, tratamento de informação, autorização, execução e interrupção aplicáveis à auditoria da plataforma Moola. As regras são vinculativas para a MANIFOLD, o Cliente e quaisquer terceiros formalmente autorizados.

> **Regra de ouro**

> Nenhum teste intrusivo, exploração controlada ou acesso a dados sensíveis será iniciado antes da aprovação do inventário, da autorização formal para testes, dos contactos de emergência e das condições de paragem.

3. Classificação da Informação

Classe	Exemplos	Tratamento
Pública	Informação aprovada para divulgação.	Sem restrições adicionais.
Interna	Informação operacional não pública.	Acesso apenas a pessoas com necessidade.
Confidencial	Arquitetura, código, contratos, configurações e resultados.	Encriptação, controlo de acesso e distribuição restrita.
Altamente Confidencial	Credenciais, segredos, dados pessoais, vulnerabilidades críticas e provas de conceito.	Acesso nominativo, MFA, repositório segregado e canal seguro.

Por defeito, todo o material da auditoria será tratado como Confidencial. Credenciais, dados pessoais e vulnerabilidades críticas serão tratados como Altamente Confidencial.

4. Princípios de Tratamento

- Necessidade e menor privilégio: aceder apenas ao necessário para o procedimento aprovado.
- Minimização: recolher a menor quantidade possível de dados e evidências.
- Segregação: separar materiais por Cliente, projeto, ambiente e nível de sensibilidade.
- Encriptação: proteger dados em trânsito e em repouso.
- Rastreabilidade: registar concessão de acesso, transferência, consulta, exportação e eliminação relevante.
- Retenção limitada: conservar apenas durante o período contratual ou legal aplicável.
- Divulgação controlada: partilhar vulnerabilidades apenas com destinatários autorizados.
- Segurança por defeito: proibir ferramentas ou canais não aprovados.

5. Gestão de Acessos e Credenciais

Controlo	Regra
Identidade	Contas nominativas; nenhuma conta partilhada.
MFA	Obrigatório sempre que tecnicamente disponível.
Privilégio	Acesso de leitura e menor privilégio por defeito; elevação temporária quando necessária.
Concessão	Aprovada pelo owner do ativo e registada na Matriz de Acessos.
Credenciais	Transmitidas por cofre ou canal seguro; nunca em texto aberto ou no corpo de e-mail.
Chaves/tokens	Temporários, com escopo mínimo, rotação e revogação após utilização.
Revogação	Imediata na conclusão, substituição de recurso, incidente ou pedido do Cliente.
Revisão	Revisão periódica durante a execução e confirmação no encerramento.

6. Ambiente de Trabalho da MANIFOLD

Área	Requisito
Endpoints	Dispositivos geridos, bloqueio automático, encriptação de disco, proteção antimalware e patches.
Rede	Ligação segura; VPN quando acordada; proibição de redes públicas não protegidas.
Repositório	Armazenamento segregado, encriptado, com MFA e controlo por grupo.
Cópias locais	Minimizadas; eliminadas após sincronização e conclusão.
Removíveis	Proibidos salvo autorização e encriptação.
Impressão	Evitada; quando necessária, controlo físico e destruição segura.
Backups	Limitados ao necessário e sujeitos às mesmas regras de segurança e retenção.

7. Ferramentas, IA e Serviços de Terceiros

- Ferramentas serão selecionadas com base na finalidade, segurança e licenciamento.
- Nenhum código-fonte, credencial, log, dado pessoal ou finding será submetido a ferramentas públicas de inteligência artificial.
- SaaS, scanners cloud, repositórios externos ou plataformas de colaboração só serão utilizados após aprovação do Cliente e avaliação do tratamento de dados.
- Sempre que uma ferramenta envie dados para terceiros, serão documentados o fornecedor, finalidade, localização, retenção e categorias de dados.
- Resultados automatizados serão validados por profissionais antes de serem reportados.
- A MANIFOLD manterá inventário das ferramentas relevantes utilizadas no projeto.

8. Gestão de Evidências

Campo/Controlo	Requisito
ID da evidência	Identificador único e ligação ao procedimento/finding.
Origem	Ativo, ambiente, data, utilizador e método de recolha.
Conteúdo	Captura, configuração, log, excerto de código ou resultado de teste.
Integridade	Hash ou outro mecanismo quando material.
Minimização	Redação de segredos e dados pessoais não necessários.
Acesso	Restrito ao workstream e reviewers autorizados.
Retenção	90 dias de calendário após o relatório final ou reteste, salvo instrução de eliminação antecipada ou obrigação legal.
Destruição	Eliminação segura e certificado quando contratualmente exigido.

9. Privacidade e Dados Pessoais

Tema	Regra
Papéis das partes	O Cliente atua como responsável pelo tratamento; a MANIFOLD atua como operador/subcontratante quando tratar dados por instrução, sem prejuízo de atividades em que atue como responsável autónomo por obrigações legais.
Categorias de dados	Identificadores de conta, contactos, perfis, telemetria, logs, dados de dispositivo, conteúdo técnico e amostras mínimas necessárias.

Tema	Regra
Titulares	Utilizadores da Moola, colaboradores e prestadores do Cliente e membros da equipa MANIFOLD.
Finalidade	Executar procedimentos de auditoria, produzir evidência e entregar resultados.
Minimização	Preferir dados sintéticos; evitar exportação de bases completas.
Ambientes não produtivos	Dados reais não serão copiados para ambientes não produtivos sem necessidade, autorização e controlos equivalentes.
Retenção/eliminação	Retenção de 90 dias após relatório final/reteste e eliminação segura, salvo obrigação legal documentada.
Incidentes	Notificação por canal seguro, imediata para risco crítico e no máximo em 24 horas após confirmação de incidente material.
Transferências	Tratamento preferencial em Moçambique; nenhuma transferência internacional ou subprocessador sem aprovação escrita do Cliente.

10. Subcontratantes e Pessoal

- Pessoal sujeito a dever de confidencialidade e need-to-know.
- Subcontratantes apenas com autorização e obrigações equivalentes.
- Acesso revogado quando a participação termina.
- Formação e briefing específico antes de receber acesso.
- Lista nominal de recursos e subcontratantes disponível ao Cliente.

11. Regras de Execução - Identificação do Teste

Campo	Informação aprovada
Cliente	Cliente
Projeto	Auditoria Técnica Integral da Plataforma Moola
Período autorizado	30 dias úteis a partir de T0; janelas sensíveis autorizadas entre 18h00 e 22h00 CAT
Fuso horário	Africa/Maputo
Ambientes	Desenvolvimento e staging para testes; produção apenas leitura e técnicas não destrutivas
IPs de origem da MANIFOLD	Endereços IP estáticos da MANIFOLD comunicados por canal seguro na Fase 0
Contactos de emergência do Cliente	Sponsor e contacto técnico do Cliente registados no kickoff e no canal de emergência
Contacto de emergência MANIFOLD	Vayile Fumo | +258 84 044 3592 | geral@manifold.co.mz
Canal seguro para findings críticos	Cofre/repositório seguro e chamada direta aos contactos autorizados
Kill switch / ordem de paragem	Mensagem "STOP MOOLA" no canal seguro ou chamada direta; suspensão imediata e confirmação por voz

12. Ativos Autorizados

Tipo	Identificação	Ambiente	Autorização
Aplicação móvel/builds	Moola Android e iOS; até 2 builds candidatas	Desenvolvimento/staging	Revisão, instrumentação e testes controlados; produção não destrutiva
APIs e domínios	Até 40 endpoints registados no inventário da Fase 0	Desenvolvimento/staging/produção	Testes autorizados; produção com baixo volume e sem stress

Tipo	Identificação	Ambiente	Autorização
Projetos Firebase/GCP	Até 3 project IDs comunicados por canal seguro	Dev/staging/prod	Leitura de configuração; alterações apenas com autorização
Firestore/Storage	Até 25 collections e 3 buckets	Dev/staging/prod	Regras e acesso; amostra mínima de dados; sem eliminação
Cloud Functions	Até 30 funções e triggers	Dev/staging/prod	Revisão e invocação controlada; sem consumo intencional de quotas
Painel web/admin	Não incluído na baseline; APIs administrativas permanecem abrangidas	Não aplicável	Inclusão apenas por Change Request
Integrações externas	Até 8 integrações na fronteira sob controlo do Cliente	Conforme integração	Configuração e fluxo; sem teste direto ao terceiro

13. Técnicas Permitidas

- Revisão de código, configuração, documentação, logs e arquitetura.
- Análise estática de código e dependências em ambiente controlado.
- Testes autenticados e não autenticados de APIs e aplicação móvel.
- Validação de autenticação, autorização, sessão, regras Firestore/Storage e App Check.
- Manipulação controlada de pedidos, parâmetros, tokens e fluxos de negócio.
- Provas de conceito mínimas, reversíveis e necessárias para demonstrar impacto.
- Criação e utilização de contas e dados de teste aprovados.
- Análise de performance sem carga destrutiva e conforme os limites acordados.

14. Atividades Proibidas sem Autorização Adicional

- Negação de serviço, flooding, stress, brute force de larga escala ou consumo intencional de quotas.
- Eliminação, corrupção ou alteração de dados reais.
- Persistência, backdoors, malware, cryptomining ou movimentação lateral fora do âmbito.
- Exfiltração de dados além da amostra mínima necessária.
- Acesso intencional a conteúdo de utilizadores reais sem necessidade.
- Engenharia social, phishing, chamadas, testes físicos ou ataques a pessoas.
- Testes a terceiros, lojas de aplicações, operadores, pagamentos ou provedores sem autorização.
- Divulgação pública de findings ou contacto com utilizadores.

15. Regras Específicas para Produção

Condição	Regra
Autorização	Documento adicional ou indicação expressa no inventário.
Janela	Data e período definidos; evitar picos de negócio.
Monitorização	Cliente acompanha logs, disponibilidade, quotas e alertas.
Backups	Confirmação de backup e capacidade de recuperação antes do teste.
Técnicas	Não destrutivas, baixo volume e prova mínima.

Condição	Regra
Paragem	Interrupção imediata a qualquer sinal de impacto inesperado.
Comunicação	Canal síncrono disponível durante atividades sensíveis.

16. Condições de Paragem

- Degradação, indisponibilidade ou comportamento anómalo não previsto.
- Risco de perda, corrupção ou exposição de dados reais.
- Identificação de ativo não autorizado ou sistema de terceiro.
- Incidente de segurança em curso não relacionado com a auditoria.
- Instrução do Cliente ou do contacto de emergência.
- Impossibilidade de manter comunicação durante atividade sensível.
- Descoberta que exija coordenação executiva antes de continuar.

17. Comunicação de Vulnerabilidades Críticas

Etapa	Ação
Validação	Confirmar evidência e reduzir falsos positivos sem ampliar o impacto.
Notificação	Contactar imediatamente os destinatários autorizados por canal seguro.
Conteúdo mínimo	Ativo, impacto, evidência mínima, risco imediato e ação de contenção recomendada.
Embargo	Não incluir em canais amplos até confirmação dos destinatários.
Acompanhamento	Registar decisão, contenção, owner e prazo.
Relatório final	Incorporar de forma controlada com histórico e estado.

18. Gestão de Incidentes Relacionados com a Auditoria

1. Interromper a atividade e preservar evidências.
2. Notificar os contactos definidos e classificar o incidente.
3. Apoiar contenção e investigação sem ultrapassar o âmbito autorizado.
4. Registar cronologia, ações, decisões e impacto.
5. Emitir relatório de incidente e ações preventivas, quando aplicável.

19. Retenção, Devolução e Destruição

Momento	Tratamento
Durante o projeto	Conservar apenas o necessário em repositório aprovado.
Versões finais	Entregar pelos canais acordados e restringir acesso.
Encerramento	Revogar acessos, eliminar cópias temporárias e encerrar formalmente os itens em aberto.
Período residual	90 dias após o relatório final ou reteste para suporte, controlo de qualidade e resposta a questões.
Destruição	Método seguro adequado ao meio; emissão de certificado se requerido.
Exceções legais	Documentar obrigação, escopo, prazo e controlos.

20. Checklist de Pré-Teste

Verificação	Estado
Contrato, NDA e DPA assinados	Obrigatório antes de T0; cópia no repositório contratual
Autorização formal para testes assinada	Obrigatório antes de qualquer teste intrusivo
Inventário e exclusões aprovados	Obrigatório antes de T0; baseline assinada
Contas, MFA e acessos validados	Obrigatório antes de T0; teste de acesso concluído
Dados de teste disponíveis	Obrigatório antes dos testes funcionais
Backups e monitorização confirmados	Obrigatório antes de atividade em produção
Janelas e contactos de emergência confirmados	Obrigatório antes de cada janela sensível
IPs/ferramentas e canais seguros aprovados	Obrigatório antes de T0; lista registada
Kill switch testado/compreendido	Obrigatório; simulação durante o kickoff
Riscos e limitações iniciais aceites	Obrigatório; aceitação no SOW e no presente RoE

21. Autorização para Execução

Ao assinar, o Cliente confirma que possui autoridade sobre os ativos identificados, autoriza a MANIFOLD a executar exclusivamente as atividades permitidas, reconhece os riscos controlados inerentes e aceita as condições de paragem e comunicação.

Pela Manifold, Lda

Nome: Rogerio Casimiro

Função: Representante Autorizado

Assinatura: _____

Data: na data da assinatura

Pelo Cliente

Nome: Cliente

Função: Representante Autorizado

Assinatura: _____

Data: na data da assinatura