Política de Segurança da Informação PantAI v1.1

Versão 1.1 · 2 de novembro de 2026 · Substitui a versão 1.0 · PANTANO FERNANDES LTDA

Esta versão descreve só as medidas de segurança que o PantAI pratica hoje. As promessas da 1.0 que ainda não são cumpridas saíram e estão listadas no fim.

1. Objetivo e escopo

1.1 Esta Política descreve como a PANTANO FERNANDES LTDA, CNPJ 67.537.675/0001-45 ("PantAI"), protege as informações tratadas no sistema PantAI, em cumprimento aos arts. 46 a 49 da LGPD.

1.2 Vale para o painel, o app do profissional, os complementos e a equipe do PantAI com acesso ao sistema. Complementa o Contrato de Assinatura e a Política de Privacidade.

2. Responsabilidades

2.1 **PantAI**: manter os controles da seção 3, tratar incidentes (seção 6) e dar acesso aos dados só a quem da equipe precisa deles para prestar o serviço.

2.2 **Salão**: a segurança também depende do Salão, que deve:

- criar um login para cada pessoa da equipe, no perfil adequado (administrador, recepção ou profissional);
- não compartilhar login e senha;
- usar senhas fortes e ativar a verificação em duas etapas;
- retirar o acesso de quem deixar a equipe;
- avisar o PantAI em suporte@pantai.tech se suspeitar de acesso indevido.

3. Controles em vigor

Controle	Como funciona hoje
Conexão cifrada	toda a comunicação com o sistema usa HTTPS
Senhas	guardadas apenas com hash, nunca em texto; senha nova com no mínimo 10 caracteres, letra e número, e recusa de senhas comuns
Tentativas de login	bloqueio temporário depois de várias tentativas erradas, com registro do evento
Verificação em duas etapas	disponível para todos os Usuários
Sessão	o acesso expira automaticamente após 8 horas; é preciso entrar de novo

Perfis de acesso	administrador, recepção e profissional, definidos pelo Salão
Isolamento entre salões	cada Salão só vê os próprios dados; o isolamento é feito no banco de dados e conferido por testes automatizados antes de cada entrega
Segredos e certificados	guardados cifrados, incluindo o certificado A1 dos salões
Registros	eventos de acesso e ações administrativas ficam registrados
Cópia de segurança	diária, guardada fora do servidor por 30 dias
Dados de cartão	não passam pelo PantAI; ficam no Asaas
Registros da aplicação	o sistema é feito para não gravar senhas, chaves, CPF e dados de cobrança nos registros técnicos da aplicação

4. Cópias de segurança

4.1 O PantAI faz cópia de segurança diária dos dados e a guarda fora do servidor principal, na Backblaze, nos EUA, por 30 dias.

4.2 Dados apagados de uma conta podem permanecer nas cópias até elas expirarem, sem uso para nenhuma outra finalidade.

5. Certificado A1 e segredos

5.1 O certificado digital A1 enviado pelo Salão é guardado cifrado e usado somente para emitir, cancelar e baixar as notas fiscais do próprio Salão.

5.2 O certificado é apagado quando o Salão o remove no painel ou, no cancelamento da conta, junto com os demais dados, 30 dias após o cancelamento.

5.3 Chaves e senhas de acesso a serviços usados pelo sistema também são guardadas cifradas ou fora do código, apenas no servidor.

6. Incidentes de segurança

6.1 Ao saber de um incidente, o PantAI age para contê-lo, apura o que aconteceu e registra o caso.

6.2 Se o incidente afetar dados de um Salão, o PantAI avisa o Salão sem demora indevida, informando o que souber sobre os dados e as pessoas afetadas, as medidas tomadas e os riscos.

6.3 Quando o PantAI for controlador e o incidente puder causar risco ou dano relevante, comunica a ANPD e as pessoas afetadas e mantém o registro do incidente, nos termos do art. 48 da LGPD e da Resolução CD/ANPD nº 15/2024.

6.4 Suspeitas de incidente ou de falha de segurança podem ser enviadas a privacidade@pantai.tech.

7. Fornecedores

Os fornecedores que recebem dados para o serviço funcionar estão listados na Política de Privacidade, com finalidade e país. O PantAI atualiza essa lista quando inclui ou troca um fornecedor.

8. Revisão e contato

Esta Política é revista quando houver mudança relevante no sistema ou na lei. Dúvidas: privacidade@pantai.tech.

O que foi retirado da 1.0 e por quê

Cada item abaixo era uma promessa que o PantAI não cumpre hoje. Se algum passar a existir, pode voltar numa próxima versão.

Promessa da 1.0	Por que saiu
Adoção da ISO/IEC 27001, NIST CSF 2.0 e OWASP ASVS como referência	sugere conformidade ou certificação que não existe
Classificação da informação em 4 níveis, com aprovação formal de acesso	processo formal não implantado
Revisão anual pela alta administração e indicadores (tempo médio de detecção e resposta)	não há processo nem indicadores medidos
Criptografia dos dados em repouso no banco e nos backups	não implantada; hoje só segredos e certificados são cifrados
Migração de segredos para serviço dedicado com rotação	promessa futura
Expiração de sessão por inatividade	não implantada; a sessão expira por tempo (8 horas)
Bloqueio de senhas vazadas por consulta a bases de vazamentos	não implantado; o sistema recusa senhas comuns
Ambientes separados, proibição de dados reais em teste, revisão de código antes da produção	processo formal não implantado
Auditoria interna OWASP anual	promete periodicidade; houve revisões, sem rotina fixa
Análise estática e dinâmica, prazos de correção por criticidade	não implantado
Teste de invasão externo anual	nunca foi feito
Testes de restauração, metas de RPO e RTO, plano de continuidade	não implantados

Provedor com certificações arquivadas; criptografia de disco nos aparelhos da equipe	não verificado
Treinamento periódico registrado	não implantado
Canal formal para relato de vulnerabilidades	não há canal próprio; suspeitas vão para privacidade@pantai.tech
Trilha de auditoria por 5 anos protegida contra alteração	prazo passa a ser de no mínimo 6 meses, até 5 anos; proteção contra alteração não comprovada
Contato dpopantai@gmail.com	substituído por privacidade@pantai.tech

Entrou na 1.1: verificação em duas etapas, regras de senha e bloqueio de tentativas, expiração da sessão, guarda cifrada do certificado A1, cópias diárias por 30 dias fora do servidor, aviso de incidente ao Salão e responsabilidades do Salão.