POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CONFIDENCIALIDADE

Política de Segurança e Confidencialidade do aplicativo Me Cuidar

Aplicativo	Me Cuidar	**Código**	PS-ECS-001
Versão	1.0 (preliminar)	**Elaborado em**	12 de novembro de 2026
Publicação / vigência	13/11/2026	**Responsável**	ECS Assessoria em Vendas Treinamento e Negócios Ltda

Esta Política estabelece regras de comportamento e diretrizes de proteção para usuários, administradores, empresas contratantes e equipes autorizadas da ECS no uso do aplicativo Me Cuidar.

1. Objetivos

Proteger a confidencialidade, a integridade e a disponibilidade das informações; reduzir riscos de acesso, alteração, perda ou divulgação não autorizados; e estabelecer responsabilidades compartilhadas. Os controles devem ser proporcionais à sensibilidade dos dados e aos riscos.

2. Classificação das informações

- Públicas: informações aprovadas para divulgação.
- Internas: informações de operação e gestão destinadas a usuários autorizados.
- Confidenciais: dados de clientes, profissionais, agendas, preços, relatórios e documentos internos.
- Sensíveis ou de acesso restrito: dados de saúde, credenciais e informações cuja exposição possa causar dano relevante.

O usuário deverá acessar, compartilhar, exportar ou imprimir somente as informações necessárias à sua função e finalidade autorizada.

3. Identidade e controle de acesso

- Cada pessoa deverá utilizar conta individual. É proibido compartilhar usuário, senha, token ou código de autenticação.
- Senhas devem ser fortes, exclusivas e mantidas em sigilo. Quando disponível, utilizar autenticação multifator.
- Aplicar o princípio do menor privilégio: cada usuário recebe somente as permissões necessárias.
- Administradores devem revisar usuários e permissões e revogar acessos em desligamentos ou mudanças de função.
- Acesso administrativo ou técnico deverá ser restrito, justificado e, quando viável, registrado e temporário.

4. Segregação e proteção de dados

Dados de empresas diferentes devem permanecer isolados por controles efetivos no backend, no banco de dados e nos mecanismos de autorização. Ocultar botões ou telas na interface não é suficiente. Se houver projetos, instalações ou repositórios separados, a separação deverá alcançar credenciais, ambientes, backups, logs e processos de suporte.

É proibido tentar acessar dados de outra empresa ou usuário, contornar permissões, extrair bases, explorar vulnerabilidades ou realizar testes sem autorização formal.

5. Dispositivos e ambiente

- Manter computadores e celulares protegidos por senha, bloqueio automático e atualizações.
- Evitar redes públicas ou inseguras para acessar informações confidenciais.

- Não armazenar dados em dispositivos pessoais, mídias removíveis ou nuvens particulares sem autorização.
- Não deixar telas, documentos ou impressões com dados pessoais expostos.
- Comunicar perda, roubo ou comprometimento de dispositivos imediatamente.

6. Compartilhamento e confidencialidade

Informações somente poderão ser compartilhadas com pessoas ou fornecedores autorizados, para finalidade legítima e pelo canal aprovado. Antes de enviar arquivos, mensagens, fotografias, orçamentos ou relatórios, conferir destinatário e conteúdo. É vedado encaminhar dados para e-mails pessoais, grupos, redes sociais ou serviços externos não aprovados.

Usuários, colaboradores, prestadores e administradores devem manter sigilo sobre as informações acessadas em razão de suas funções, inclusive após o encerramento do vínculo, respeitadas as obrigações legais.

7. Regras específicas do Me Cuidar

Informações de saúde, alergias, contraindicações, histórico de procedimentos e fotografias relacionadas ao atendimento exigem cuidado reforçado. O acesso deve ficar restrito aos profissionais que necessitem dessas informações. É proibido consultar por curiosidade, divulgar em redes sociais ou utilizar em marketing sem autorização e fundamento próprios.

8. Desenvolvimento, manutenção e suporte

A ECS deverá manter práticas proporcionais de desenvolvimento e manutenção segura, incluindo separação de ambientes, proteção de segredos, revisão de permissões, atualização de dependências, backups, monitoramento e tratamento de vulnerabilidades. Chaves e tokens não devem ser expostos em repositórios públicos ou em código executado no navegador.

Dados reais devem ser utilizados em testes somente quando necessário e autorizado, preferindo-se dados fictícios ou anonimizados. O acesso de suporte deve ser limitado ao chamado e encerrado após a necessidade.

9. Incidentes

Suspeita de acesso indevido, envio incorreto, perda de dispositivo, exposição de arquivo, comprometimento de senha ou alteração não autorizada deve ser comunicada imediatamente ao administrador e ao canal de suporte/segurança da ECS.

A ECS registrará o evento, buscará conter o incidente, preservará evidências, avaliará sistemas e dados afetados e apoiará a controladora. Quando operadora, comunicará a contratante sem demora injustificada, buscando fazer o aviso inicial em até 24 horas sempre que viável. A controladora decidirá sobre as comunicações regulatórias e aos titulares, conforme a regulamentação.

10. Retenção, descarte e encerramento

Informações não deverão ser mantidas indefinidamente sem finalidade. O descarte deverá ocorrer por processo aprovado e seguro. Ao término do vínculo, credenciais devem ser revogadas e cópias locais eliminadas, respeitadas as obrigações legais e contratuais. Backups devem ter prazo de expiração e controles de acesso.

11. Condutas proibidas e responsabilidades

- Compartilhar credenciais ou permitir o uso da conta por terceiros.
- Consultar, copiar, alterar ou divulgar dados sem autorização.
- Enviar dados pessoais ou confidenciais a canais não aprovados.
- Desativar mecanismos de segurança ou instalar software não autorizado.
- Realizar engenharia reversa, varreduras ou testes sem autorização.
- Utilizar dados para fins particulares, publicidade própria ou prospecção não autorizada.

Cada usuário é responsável pelo uso de sua conta. A contratante administra permissões e orienta sua equipe. A ECS responde pelos controles e obrigações que lhe cabem conforme sua função e contrato. Violações poderão resultar em bloqueio de acesso e medidas administrativas, contratuais ou legais.

12. Ciência e compromisso

Ao marcar a caixa de ciência/compromisso, o usuário confirma que teve acesso a esta Política e se compromete a observar as regras aplicáveis ao seu perfil. Esse registro não substitui consentimento específico quando exigido por lei.

Empresa: ECS Assessoria em Vendas Treinamento e Negócios Ltda — CNPJ 35.032.080/0001-41

Canal de suporte e segurança: contato@ernestocostasantos.com.br · WhatsApp (11) 99726-1900