

Segurança de Acesso e Autenticação

Responsabilidades para proteger contas e autorizar operações.

O essencial para consulta

- Use contas individuais e autenticação em duas etapas.
- Nunca envie senhas em formulários públicos.
- Recuperação de acesso exige verificação proporcional.

Resumo de consulta. As cláusulas completas abaixo prevalecem.

1. Responsabilidades e escopo

A política cobre conta de cliente, painéis, acessos administrativos, integrações e pessoas autorizadas. A Zovvi protege os componentes que administra; o cliente protege dispositivos, aplicativos e permissões sob sua gestão. Um incidente será apurado conforme causa e obrigações de cada parte, sem atribuição automática de toda responsabilidade ao titular.

2. Senhas, fatores e dispositivos

Use senha exclusiva e longa, gerenciador confiável e autenticação em duas etapas onde disponível. Guarde recuperação separada e não reutilize códigos. Não exigimos troca arbitrária periódica de senha como substituto de segurança; altere-a diante de comprometimento ou orientação fundamentada.

Acesso administrativo ou operação sensível pode exigir segundo fator ou confirmação adicional, informados no fluxo. Mantenha navegador e dispositivo atualizados e bloqueados. O suporte não solicita senha ou código temporário em abordagem não solicitada.

3. Equipe, delegação e privilégios

Prefira acessos individuais, permissões mínimas e revogação ao fim do vínculo. O titular deve identificar quem pode administrar, contratar ou pedir exclusão. Não compartilhe a credencial principal com agências; use delegação quando disponível ou procedimento autorizado de escopo limitado.

A Zovvi deve verificar autorização para alterações sensíveis. Estar copiado em um e-mail ou conhecer o domínio não comprova titularidade. Disputas de acesso exigem evidências e proteção das partes, sem liberar dados ao primeiro solicitante.

4. Chaves, integrações e acesso técnico

Tokens e chaves devem ter escopo mínimo, armazenamento protegido e rotação quando expostos. Não os publique em código, URL, captura ou chamado aberto. Para suporte ou migração, forneça acesso temporário pelo canal seguro indicado e revogue ao concluir.

Acesso técnico pela Zovvi deve ser necessário ao serviço, limitado e confidencial. Uma autorização de diagnóstico não permite explorar dados para outras finalidades. Alterações que possam sobrescrever conteúdo ou afetar disponibilidade exigem escopo e autorização adequados.

5. Recuperação e suspeita de incidente

Avise pelo atendimento oficial se perder acesso, detectar login suspeito ou sofrer golpe. Informe serviço, horário e fatos, sem expor novos segredos. A recuperação pode exigir confirmação de titularidade proporcional, com proteção dos documentos. Comprovante de pagamento isolado não basta para transferir controle.

Podemos encerrar sessões, revogar tokens ou isolar componente diante de risco concreto, comunicando motivo e próximos passos assim que viável. Medidas não podem impedir indevidamente contestação ou exercício de direitos. Dados de incidentes seguem a Política de Privacidade.

6. Aplicações e revisão

Atualize CMS, plugins e dependências, remova acessos sem uso e mantenha cópias independentes. Certificado SSL protege o transporte, mas não garante ausência de vulnerabilidades ou legitimidade de qualquer mensagem. Exigências adicionais devem ser proporcionais, explicadas e compatíveis com o serviço contratado. Peça revisão se uma medida ou verificação parecer excessiva.