

POLÍTICA DE USO ACEITÁVEL – ASERNET

Versão: 2.0

Vigência: setembro de 2026

A presente Política de Uso Aceitável (“Política”) estabelece regras para a utilização adequada, segura e lícita dos serviços, redes, equipamentos, plataformas e demais recursos disponibilizados sob a marca AserNet. Seu objetivo é proteger clientes, usuários, terceiros e a infraestrutura utilizada na prestação dos serviços, preservando qualidade, disponibilidade, segurança e conformidade legal e regulatória.

1. ABRANGÊNCIA

Esta Política aplica-se aos clientes, usuários autorizados e demais pessoas que utilizem serviços ou recursos disponibilizados sob a marca AserNet, conforme a natureza da contratação.

As regras poderão abranger, entre outros, serviços de acesso à internet, conectividade, Serviço Móvel Pessoal (SMP), Wi-Fi profissional, redes, equipamentos fornecidos pela AserNet, plataformas, aplicações e soluções tecnológicas.

A empresa responsável por cada serviço ou operação será aquela identificada nos respectivos documentos contratuais, fiscais ou regulatórios.

2. PRINCÍPIOS DE UTILIZAÇÃO

Os serviços e recursos deverão ser utilizados:

- de forma lícita e compatível com a finalidade contratada;
- sem comprometer a segurança, estabilidade, disponibilidade ou integridade das redes, sistemas e equipamentos;
- sem violar direitos de terceiros, sigilo, privacidade, propriedade intelectual ou demais direitos protegidos por lei;
- de acordo com as condições do plano, serviço, equipamento ou solução contratada;
- com adoção de cuidados razoáveis de segurança pelo cliente e pelos usuários sob sua responsabilidade.

3. USOS PROIBIDOS

É vedada a utilização deliberada dos serviços ou recursos para:

- praticar, facilitar ou promover atividades ilícitas;
- realizar fraude, golpe, phishing, falsificação de identidade, engenharia social maliciosa ou outras formas de obtenção indevida de dados, credenciais ou valores;
- invadir, acessar, testar, explorar ou tentar explorar redes, sistemas, contas, dispositivos ou serviços sem autorização;
- executar varreduras, ataques de negação de serviço, distribuição de malware, ransomware, botnets ou outras atividades destinadas a comprometer sistemas ou terceiros;

- interceptar comunicações, capturar credenciais ou obter dados de terceiros sem autorização ou fundamento jurídico;
- alterar, ocultar ou falsificar identificadores, origem de tráfego ou informações técnicas com finalidade fraudulenta ou abusiva;
- enviar spam, mensagens fraudulentas ou comunicações não autorizadas em desacordo com a legislação ou com regras técnicas aplicáveis;
- armazenar, transmitir, disponibilizar ou distribuir conteúdo ilícito ou cuja circulação viole direitos de terceiros;
- utilizar os recursos de forma deliberadamente incompatível com a modalidade contratada, causando risco relevante, degradação indevida ou comprometimento da infraestrutura;
- burlar mecanismos de autenticação, segurança, controle de acesso, franquia, tarifação, limitação técnica ou proteção implementados legitimamente no serviço.

4. SEGURANÇA DE CREDENCIAIS, REDES E DISPOSITIVOS

O cliente deverá adotar cuidados razoáveis para proteger senhas, credenciais, chips, eSIMs, equipamentos e dispositivos associados aos serviços, evitando compartilhamentos indevidos e mantendo, quando aplicável, sistemas e equipamentos próprios em condições adequadas de segurança.

O cliente não será automaticamente responsabilizado por toda atividade originada de sua conexão ou linha quando houver indícios de fraude, invasão, comprometimento ou fato fora de seu controle. A apuração deverá considerar as circunstâncias do caso, os registros disponíveis e as obrigações efetivamente atribuíveis às partes.

Suspeitas de comprometimento, perda, furto, roubo ou uso indevido de credenciais, chip, eSIM ou equipamento deverão ser comunicadas pelos canais de atendimento assim que razoavelmente possível.

5. EQUIPAMENTOS E CONFIGURAÇÕES

É vedado adulterar, violar mecanismos de proteção, modificar firmware de forma não autorizada ou realizar intervenções em equipamentos fornecidos, administrados ou locados pela AserNet quando tais ações possam comprometer segurança, integridade, suporte, gerenciamento ou funcionamento do serviço.

O cliente poderá utilizar e configurar equipamentos próprios, observadas compatibilidade, segurança, limitações técnicas e condições da contratação.

Configurações realizadas pelo cliente em equipamentos próprios ou em recursos cuja administração lhe tenha sido disponibilizada serão de sua responsabilidade, sem prejuízo do suporte contratado e das responsabilidades da AserNet sobre os serviços que lhe competirem.

6. COMPARTILHAMENTO, REDISTRIBUIÇÃO E USO COMERCIAL

O compartilhamento de conectividade dentro da finalidade e do ambiente previstos na contratação é permitido quando compatível com o serviço, inclusive em redes domésticas, empresariais, Wi-Fi de visitantes e soluções profissionais.

É vedada a revenda, redistribuição pública ou exploração comercial do serviço de forma não prevista na modalidade contratada ou sem autorização quando exigida.

Projetos que envolvam disponibilização coletiva, redes de visitantes, condomínios, estabelecimentos, eventos ou outras formas de acesso por terceiros poderão possuir condições específicas de arquitetura, autenticação, segurança e responsabilidade.

7. SERVIDORES, VPN, IoT, CÂMERAS E APLICAÇÕES EMPRESARIAIS

A utilização de servidores, VPN, câmeras, equipamentos IoT, acesso remoto, serviços em nuvem, automações e aplicações empresariais não é proibida por esta Política, desde que seja compatível com o plano e a solução contratados e não represente abuso, risco indevido ou violação legal.

Recursos que demandem características específicas de disponibilidade, endereçamento, portas, capacidade, segurança, suporte ou nível de serviço poderão exigir plano ou solução apropriada.

8. ASERNET MÓVEL

Nos serviços AserNet Móvel, o titular e os usuários autorizados deverão utilizar a linha, chip ou eSIM de forma lícita e compatível com a oferta contratada.

É especialmente vedada a utilização deliberada da linha para:

- golpes, fraude, phishing, spam ou envio abusivo de mensagens;
- automação ou geração artificial de chamadas, mensagens ou tráfego que viole regras aplicáveis ou comprometa a rede;
- adulteração ou utilização irregular de identificadores, credenciais, chip, eSIM ou mecanismos de autenticação;
- atividades destinadas a contornar controles técnicos, regulatórios ou de segurança.

Medidas relacionadas à linha observarão as responsabilidades da prestadora responsável pelo SMP, os documentos específicos da contratação e a regulamentação aplicável.

9. PROTEÇÃO DA REDE E MEDIDAS TÉCNICAS

Quando forem identificados indícios consistentes de ataque, fraude, comprometimento, abuso técnico ou risco relevante à rede, a clientes ou a terceiros, poderão ser adotadas medidas técnicas de contenção compatíveis com a natureza e a urgência do evento.

As medidas poderão incluir, conforme tecnicamente aplicável:

- orientação ou solicitação de correção ao cliente;
- bloqueio ou redefinição de credenciais comprometidas;
- isolamento ou restrição de equipamento, porta, protocolo, endereço, tráfego ou recurso afetado;
- limitação temporária estritamente necessária à contenção do risco;
- outras medidas técnicas proporcionais e necessárias à proteção da infraestrutura.

Sempre que a urgência permitir, o cliente será informado e terá oportunidade razoável para correção. Em situação de risco imediato, a medida técnica necessária poderá ser adotada antes da comunicação, com registro e posterior informação quando cabível.

As medidas de segurança deverão buscar atingir o recurso afetado e evitar restrição desnecessária de outros serviços ou funcionalidades.

10. SUSPENSÃO, INADIMPLÊNCIA E CANCELAMENTO

A suspensão ou rescisão contratual não decorrerá automaticamente de qualquer evento descrito nesta Política. Essas medidas somente serão aplicadas quando houver fundamento contratual, legal ou regulatório e observados os procedimentos cabíveis.

As consequências da inadimplência observarão o Regulamento Geral dos Serviços AserNet, os documentos específicos da contratação e a regulamentação aplicável, não sendo esta Política instrumento autônomo para criar hipóteses adicionais de suspensão por falta de pagamento.

Violações graves ou reiteradas desta Política poderão resultar em medidas contratuais cabíveis, observados gravidade, proporcionalidade, possibilidade de correção, segurança da rede, direitos do cliente e legislação aplicável.

11. REGISTROS TÉCNICOS, SEGURANÇA E PRIVACIDADE

Para operar, proteger e manter os serviços, poderão ser tratados registros técnicos, eventos de segurança, identificadores, dados de autenticação, conexão ou acesso e outras informações necessárias às finalidades legítimas da operação.

O tratamento deverá observar a Política de Privacidade e Tratamento de Dados AserNet, a legislação aplicável, os princípios de necessidade e segurança e, quando pertinente, as regras relativas ao sigilo das comunicações.

Esta Política não autoriza inspeção irrestrita do conteúdo das comunicações dos usuários.

12. COOPERAÇÃO COM AUTORIDADES E TERCEIROS

A AserNet poderá preservar registros, fornecer informações ou adotar medidas quando houver obrigação legal ou regulatória, ordem válida de autoridade competente ou necessidade de exercício regular de direitos, observados os limites legais e a proteção dos dados envolvidos.

Denúncias ou notificações recebidas de terceiros serão avaliadas de acordo com sua consistência, elementos disponíveis e obrigações aplicáveis, não implicando responsabilização automática do cliente.

13. RESPONSABILIDADES

Cada parte responderá pelos atos e omissões que lhe forem legal ou contratualmente atribuíveis.

O cliente é responsável por orientar usuários aos quais conceda legitimamente acesso aos serviços e por adotar cuidados razoáveis na administração de suas credenciais, equipamentos e redes próprias.

A AserNet é responsável pelas obrigações que lhe competirem na prestação dos serviços, inclusive pelas medidas de segurança, operação, atendimento e tratamento de incidentes previstas nos documentos aplicáveis e na legislação.

14. ATUALIZAÇÕES DESTA POLÍTICA

Esta Política poderá ser atualizada para refletir mudanças legais, regulatórias, tecnológicas, operacionais ou relacionadas aos serviços.

A versão vigente será disponibilizada nos canais oficiais da AserNet. Alterações que afetem condições essenciais de contratos vigentes observarão os documentos contratados, a legislação, a regulamentação e, quando exigível, os procedimentos de comunicação ou manifestação aplicáveis.

15. DISPOSIÇÕES FINAIS

Esta Política integra a contratação quando expressamente incorporada pelo Termo de Adesão, contrato, regulamento ou outro documento aplicável.

Condições específicas de determinado serviço, produto, plano ou projeto poderão complementar esta Política e prevalecer quanto às particularidades validamente contratadas, desde que compatíveis com a legislação e a regulamentação aplicáveis.

Em caso de dúvida sobre a utilização adequada dos serviços ou sobre uma medida de segurança aplicada, o cliente poderá utilizar os canais oficiais de atendimento da AserNet.