POLÍTICA DE SEGURANÇA CIBERNÉTICA E TRATAMENTO DE DADOS

DA AGROLEND SOCIEDADE DE CRÉDITO, FINANCIAMENTO E INVESTIMENTO S.A

SUMÁRIO

1. OBJETIVO

Promover a disseminação dos princípios gerais de conduta e obrigações a serem seguidas pelos Colaboradores, a fim de mitigar riscos relacionados às ameaças externas ou internas, deliberadas ou acidentais, que possam impactar os dados e sistemas de informação da **AGROLEND**, quanto à sua integridade, confidencialidade e disponibilidade.

A presente Política explica como a **AGROLEND** coleta, guarda, processa, trata e compartilha os dados pessoais e outros dados sensíveis a que têm acesso, os quais podem ser coletados sobre as pessoas físicas relacionadas à **AGROLEND**, incluindo seus Colaboradores e clientes. Foi elaborada para indicar aos Colaboradores e/ou clientes, as práticas e as escolhas de privacidade que possuem para a utilização dos serviços da **AGROLEND**.

2. ABRANGÊNCIA

A Política deve ser observada e cumprida pela **AGROLEND** e empresas do Grupo, membros da administração, conselho, colaboradores, prestadores de serviços e parceiros ("Partes Interessadas").

3. BASE LEGAL

A base normativa inclui, mas não se limita, à Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018) e à Resolução CMN nº 4.893, de 26 de fevereiro de 2021.

4. DEFINIÇÕES

AGROLEND: Agrolend Sociedade de Crédito, Financiamento e Investimento S.A., instituição financeira inscrita no Cadastro Nacional da Pessoa Jurídica do Ministério da Economia sob o nº 43.774.196/0001-84.

BCB: Banco Central do Brasil.

CLIENTE: Pessoa natural ou jurídica que utiliza os serviços, celebra operações de crédito relacionadas à produção rural no Brasil, com a **AGROLEND** ou acessa o Site, após ter seu cadastro junto à **AGROLEND** aprovado pela Diretoria desta.

CMN: Conselho Monetário Nacional.

COLABORADOR: Pessoa natural contratada sob regime da CLT ou aquela pessoa jurídica contratada para este fim específico, bem como seus administradores.

DIRETOR RESPONSÁVEL: (i) Diretor responsável pela função de conformidade, indicado nos termos do artigo 5º, inciso IV, da Resolução 4.595**;** e (ii) Diretor responsável pelo sistema de controles internos, indicado nos termos do artigo 10º, da Resolução 4.968.

NORMAS APLICÁVEIS: A Resolução nº 4.595, de 28 de agosto de 2017 e a Resolução nº 4.968, de 25 de novembro de 2021, e demais normas editadas pelo Congresso Nacional, pelo CMN, pelo BCB e por quaisquer órgãos nacionais ou internacionais que editem normas ou orientações aplicáveis à política de conformidade e controles internos de instituições financeiras brasileiras, quando mencionadas em conjunto.

REGRAS: O conjunto de políticas, manuais e procedimentos internos aprovados pela Diretoria da **AGROLEND**.

SISTEMA DE CONTROLES INTERNOS: Conjunto de práticas e estrutura de governança adotadas pela **AGROLEND**, com o fim de dar cumprimento às Normas Aplicáveis e às Regras da **AGROLEND**, reduzindo a possibilidade de sofrer perdas financeiras, desgaste da imagem institucional e incrementar a qualidade das informações contábeis, financeiras e gerenciais**.**

SITE: Página da **AGROLEND** na rede mundial de computadores, disponível no seguinte endereço eletrônico: www.agrolend.agr.br.

5. DIRETRIZES

5.1. DIRETORIA DE SEGURANÇA CIBERNÉTICA

O Diretor de Segurança Cibernética é responsável pela elaboração e atualização desta Política, também com a função de discutir e deliberar sobre assuntos relacionados à segurança cibernética da **AGROLEND**.

5.2. INFORMAÇÕES PROTEGIDAS

Todo e qualquer dado e/ou informação relativa à **AGROLEND**, incluindo, mas não se limitando aos seus negócios, operações, parcerias, Colaboradores e clientes que o Colaborador desenvolva ou venha a ter acesso em virtude do seu vínculo com o **Grupo AGROLEND** ou em virtude do desempenho de suas atividades contratadas pela **AGROLEND** (as "Informações Protegidas"), será considerada informação confidencial, de sua exclusiva propriedade, salvo disposição contratual diversa, sendo expressamente proibida a reprodução, divulgação, publicação, transmissão, cessão ou facilitação de quaisquer acessos a terceiros, direta ou indiretamente, total ou parcialmente, salvo se autorizado previamente pelos representantes legais da **AGROLEND**.

As Partes Interessadas poderão ser responsabilizadas por eventual uso indevido da Informação Protegida, pelo que a **AGROLEND** se reserva o direito de monitorar o uso das Informações Protegidas e analisar todos dados e evidências relacionados, para fins de obtenção de provas que poderão ser eventualmente utilizadas nos processos investigatórios e na adoção das medidas legais cabíveis.

A qualquer tempo, caso seja solicitado pela **AGROLEND**, ou em caso de término da relação do Colaborador, independentemente da causa, o Colaborador restituirá à **AGROLEND** todas as cópias, bancos de dados, reproduções ou adaptações que tiver das Informações Protegidas. O Colaborador reconhece que as obrigações

e proibições previstas nesta Política permanecerão válidas durante toda a existência do vínculo do Colaborador com a **AGROLEND** e mesmo após o término de tal vínculo, independentemente do motivo.

Qualquer Informação Protegida cuja divulgação seja exigida por Lei, ordem judicial, determinação de autoridades administrativas competentes ou acordos celebrados pela **AGROLEND** com terceiros somente poderá ser divulgada após análise e validação do Diretor de Segurança Cibernética da **AGROLEND**.

5.3. CLASSIFICAÇÃO DAS INFORMAÇÕES PROTEGIDAS

As Informações Protegidas são classificadas de acordo com a importância que representam para os negócios da **AGROLEND**, aplicando-se o grau de sigilo necessário, conforme a sua classificação:

(i) Interna: informação relacionada a assuntos exclusivamente pertinentes a questões internas da **AGROLEND**, cujo acesso é liberado tão somente às pessoas internas da **AGROLEND**, designadas para tal. Embora a **AGROLEND** não tenha interesse em divulgá-la a indivíduos externos, a disponibilização dessa informação não tem o potencial de causar danos sérios à **AGROLEND**;

(ii) Confidencial: informação sigilosa que não deve ser divulgada, estando restrito o seu uso a um determinado número de pessoas (para desempenharem as suas atividades), sendo que a divulgação não autorizada pode causar prejuízos para a **AGROLEND** (tais como perda de clientes, danos financeiros, depreciação da imagem etc.), propiciando vantagens aos concorrentes e clientes, bem como, revelando estratégias e resultados de negócios; e

(iii) Secreta: informação sigilosa com acesso controlado e liberado apenas às pessoas designadas para tal, que contém matérias de ordem vital para a **AGROLEND** ou seus clientes, cuja divulgação, inexatidão e disponibilidade (total ou parcial) podem causar danos graves à **AGROLEND**, incluindo, mas não se limitando a morais e/ou patrimoniais. Todos os procedimentos de segurança, dados pessoais e as outras informações de notável sensibilidade para os negócios da **AGROLEND**, sempre serão consideradas Informações Secretas.

Além das Informações Protegidas, há também a informação Pública, destinada ao público em geral e já divulgada pela **AGROLEND**, cuja utilização por quaisquer indivíduos independe de autorização e não é passível de prejuízos para a **AGROLEND** ou para terceiros.

Assim, o Colaborador responsável por gerar ou obter tal informação, antes de divulgá-la a qualquer pessoa, obrigatoriamente deverá classificá-la em Interna, Confidencial ou Secreta, de acordo com o tipo de suporte, quais sejam: documentos impressos, documentos eletrônicos, correio eletrônico (*e-mail*), bancos de dados e aplicações - quando cabível -, eventuais relatórios oriundos dessas aplicações e banco de dados devem seguir os padrões mencionados no tópico, além de outros tipos de mídia. A classificação deve estar visível pelos recursos que se façam necessários.

Caso o Colaborador receba uma informação não classificada, ele deve considerar tal informação como sendo uma Informação Confidencial. E ao ter conhecimento de que Informações Internas, Confidenciais ou Secretas estejam sendo tratadas inadequadamente, o Colaborador deverá imediatamente comunicar o Diretor de Segurança da Informação. A classificação das Informações Protegidas é de extrema importância para a sua rastreabilidade.

5.4. PRIVACIDADE E PROTEÇÃO DE DADOS

A **AGROLEND** pode coletar informações sobre seus clientes e/ou Colaboradores quando estes acessarem o seu sítio eletrônico (disponível no endereço eletrônico agrolend.agr.br) ou celebrarem quaisquer instrumentos de vínculo comercial, de emprego, de prestação de serviços, de parceria e/ou diversos, sempre se valendo de base legal válida, legítima e adequada.

É vedado o uso dos dados para finalidades diversas das estabelecidas nesta Política e/ou diversas dos motivos que ensejaram a coleta, o uso, o armazenamento e qualquer outra hipótese de tratamento dos dados.

O Colaborador garante a não divulgar os dados pessoais a que tiver acesso ou compartilhá-los sem autorização expressa da **AGROLEND**, bem como, transmiti-los ou acessá-los por terceiros não autorizados. O Colaborador garante, ainda, a adotar as melhores práticas de segurança da informação durante todo o ciclo de vida dos dados dentro da **AGROLEND**.

A **AGROLEND** prioriza a privacidade dos dados dos seus clientes, portanto compromete-se com a proteção e o sigilo dos dados pessoais, utilizando avançadas tecnologias de proteção de dados para tanto. Mantém medidas de segurança técnicas, físicas e administrativas, elaboradas para proporcionar proteção aos dados em razão de perda, mau uso, acesso não autorizado, divulgação, alteração e exclusão, e incluem filtros de acesso de origens não desejadas, gestão de criptografia de dados, uso de autenticação e controles de acesso físico aos ambientes restritos, uso de autenticação e controles de autorização de acesso a informações, uso de políticas de senha e a manutenção de cópias de segurança. A **AGROLEND** realiza testes periódicos visando garantir que seu ambiente está adequado às necessidades de segurança

Os Colaboradores, como peça-chave no processo de gestão da segurança cibernética, estão cientes e assumem o compromisso da **AGROLEND** quanto a tal obrigação, e garantem os melhores esforços no sentido de proteger e guardar sigilo dos dados pessoais a que tiverem acesso no exercício de suas funções.

5.5. DADOS PESSOAIS

São considerados dados pessoais (“Dados Pessoais”) as informações que podem ser associadas a uma pessoa identificada ou identificável

A **AGROLEND** adota medidas para garantir que os dados armazenados de seus clientes e/ou Colaboradores são aqueles estritamente necessários para cumprir obrigações legais, regulatórias, contratuais, de prevenção à fraude e lavagem de dinheiro e questões relacionadas aos negócios da **AGROLEND**.

A **AGROLEND** pode compartilhar os dados pessoais e outros dados sensíveis a que tiver acesso, observadas as normas e regulamentações aplicáveis:

- com outras empresas do **Grupo AGROLEND**;
- com os Colaboradores que prestarem serviços à **AGROLEND**, e desde estritamente necessário à prestação do serviço;
- com outras instituições financeiras com quem possuir parceria para criar ou oferecer produto ou serviço conjuntamente;
- com as outras partes negociais no âmbito das operações de crédito celebradas pela **AGROLEND**;
- com terceiros, para negócios com a **AGROLEND** ou conforme permitido/exigido por lei;
- com o consentimento e/ou orientação do cliente; e
- para fornecer dados estatísticos anonimizados agregados a terceiros sobre como, quando e porque os clientes e/ou Colaboradores visitam os serviços da **AGROLEND**.

5.5.1. Opções de Privacidade Disponíveis

O cliente e/ou o Colaborador têm opções de privacidade e comunicações ao utilizar os serviços da **AGROLEND**, sendo que algumas opções são explicadas quando da realização do cadastro ou utilização de um serviço, tais como:

- Dados Pessoais: O visitante pode se recusar a fornecer os Dados Pessoais quando solicitados pela **AGROLEND**. Neste caso, todos os Serviços ficam indisponíveis para o visitante, pois o fornecimento dessas informações é necessário para a realização do cadastro.
- Opções de Cookies: O cliente e/ou o Colaborador podem gerenciar suas preferências de Cookies por meio da exclusão, desativação ou bloqueio diretamente em seu navegador ou dispositivo de internet. Neste caso, muitos recursos e funções importantes disponíveis podem ficar indisponíveis. Ainda, o cliente e/ou o Colaborador pode ser questionado se deseja que o aplicativo ou o sítio eletrônico salve certas informações para otimização de seu uso. Neste caso, a **AGROLEND** utiliza Cookies apenas com autorização expressa do cliente e/ou do Colaborador.

- Comunicação e Marketing: A **AGROLEND** pode enviar ao cliente e/ou ao Colaborador conteúdo de marketing sobre os serviços e produtos que oferece em conjunto com instituições financeiras, bem como, produtos e serviços de terceiros não afiliados. O conteúdo de marketing é enviado por meio de vários canais de comunicação, tais como: mensagem de texto, correio eletrônico (e-mail), pop-ups, notificações e aplicativos de mensagens. O cliente e/ou Colaborador podem optar por cancelar o recebimento do conteúdo de marketing ao ajustar suas preferências de comunicação em configurações da conta. Para mensagens enviadas por notificações, o cliente e/ou o Colaborador podem gerenciar suas preferências no respectivo dispositivo.

- Informativos: A **AGROLEND** enviará comunicações necessárias ou obrigatórias a respeito dos serviços, os quais o cliente e/ou o Colaborador não podem cancelar o recebimento, podendo tão somente ajustar a mídia e o formato que recebe tais avisos.

5.6. MONITORAMENTO E AUDITORIA DO AMBIENTE

Com o objetivo de apurar o cumprimento das normas de segurança da **AGROLEND**, respeitada a legislação em vigor, todo ambiente físico e digital da **AGROLEND** pode ser monitorado, incluindo, mas não se limitando ao acesso, uso ou tráfego de informações em tal ambiente por qualquer meio (como por exemplo, correio eletrônico - *e-mail*).

Neste sentido, os Colaboradores têm ciência que a **AGROLEND** pode monitorar todos os servidores, redes, conexões de internet, *softwares*, equipamentos e dispositivos corporativos, móveis ou não; e realizar inspeções físicas nos equipamentos e nas estações de trabalho do Colaborador, periodicamente ou sob fundada suspeita de infração às normas internas da **AGROLEND**.

O Colaborador declara, ainda, estar ciente que o monitoramento pode identificá-lo e apresentar dados sobre o seu uso da estrutura tecnológica da **AGROLEND** e do material e conteúdo manipulado, sendo certo que todas as informações coletadas no curso do monitoramento são guardadas nos *backups* da **AGROLEND** para fins de auditoria e poderão ser utilizadas como provas de eventual violação das regras e condições estabelecidas pela **AGROLEND** ou pela legislação em vigor. As informações oriundas do monitoramento poderão ser divulgadas na medida em que houver razão legal ou determinação judicial para tanto, caso solicitadas pelos órgãos competentes.

O monitoramento é realizado para resguardar a segurança não só dos sistemas da **AGROLEND** e das Informações Protegidas, como também do próprio Colaborador, sendo que os dados e as informações monitoradas somente poderão ser acessadas pelas áreas competentes e para finalidades legítimas, como a apuração de denúncias e condução de investigações no ambiente de trabalho. Todo e qualquer tratamento de dados para estes fins será fundamentado no relatório de auditoria ou em outro instrumento apropriado para tanto, e cumprirá as normas específicas sobre privacidade e proteção de dados pessoais.

5.7. MANUSEIO DAS INFORMAÇÕES PROTEGIDAS

O Colaborador é responsável pelo uso que fizer das Informações Protegidas, portanto as regras quanto ao manuseio das informações protegidas deverão ser observadas para garantir o nível mínimo de Segurança da Informação.

5.7.1. Impressoras e Copiadoras

Os Colaboradores têm ciência que todo e qualquer uso dos equipamentos, tais como impressoras e copiadoras, deve ser feito exclusivamente para as suas atividades profissionais, sendo proibido o uso para fins pessoais. A impressão de documentos com Informações Secretas deve ser evitada, sendo que a impressão de documentos contendo outros tipos de Informações Protegidas deve ser imediatamente retirada dos equipamentos.

5.7.2. Uso de Informações Protegidas

O Colaborador tem ciência quanto ao cuidado que deve empregar para o uso das Informações Protegidas, não deixando anotações ou manipulando documentos que contenham tais informações em locais de circulação, tais como salas de reunião ou locais públicos (a exemplo, cafés, aviões etc.). A reutilização de papéis para rascunho que contenham Informação Protegida é proibida.

O compartilhamento de Informações Protegidas somente ocorrerá após a formalização de Acordo de Confidencialidade ("Acordo de Confidencialidade") ou de outro instrumento equivalente, nos casos envolvendo a contratação de serviços de terceiros que justifiquem a necessidade.

5.7.3. Comunicação Verbal

Caso ocorra a transmissão de Informações Protegidas através de comunicação verbal, o Colaborador deverá respeitar as regras dispostas abaixo, de acordo com o meio de transferência da informação:

(i) Presencial: Informações Internas, Confidenciais e Secretas devem ser discutidas em locais privados de acesso controlado, para impedir que terceiros não autorizados escutem a conversa e tenham acesso a tais informações. Em caso de inviabilidade de comunicação em ambiente privado, o Colaborador tomará, no mínimo, as seguintes cautelas: *(a)* observar se alguém está escutando a conversa; e *(b)* nunca identificar a **AGROLEND**, o cliente e/ou terceiro relacionado.

(ii) Telefones, Celulares e Rádios: É vedada a transmissão de Informações Confidenciais e Secretas por telefone (fixo ou móvel) ou rádio. Caso não se possa evitar que tais informações sejam transmitidas por ligações telefônicas ou pelos outros meios de transmissão, o Colaborador deve redobrar o cuidado, sendo objetivo e discreto ao transmitir tais informações. Da mesma forma, não deve fornecer informações como senhas, telefones, endereços (físicos e eletrônicos) ou outras informações de acesso restrito por telefone ou outros meios de transmissão e deve estar atento para não repetir em

voz alta essas informações quando forem lhe passadas por terceiros. Ainda, o Colaborador compreende e concorda que é vedada a gravação de Informações Confidenciais e Secretas em equipamentos eletrônicos, como caixa postal, secretária eletrônica, áudios em aplicativos de conversa etc.

5.7.4. Recebimento, Envio e Compartilhamento de Arquivos

O Colaborador é responsável pelos arquivos que envia, recebe e compartilha por meio eletrônico e pela infraestrutura tecnológica da **AGROLEND**, seja através de equipamentos de propriedade da **AGROLEND** para o uso do Colaborador ou até mesmo equipamentos do próprio Colaborador, caso autorizado pela **AGROLEND** nos termos das regras definidas na presente Política – ("Dispositivos"), ou ainda, serviços de *cloud* (nuvem).

É vedado ao Colaborador, para garantir níveis mínimos de segurança da infraestrutura tecnológica do **Grupo AGROLEND**:

(i) receber, enviar e compartilhar arquivos que: ***(a)*** tenham finalidades diversas e não relacionadas às atividades de interesse da **AGROLEND** ou relativas aos seus negócios; ***(b)*** contenham pornografia ou conteúdo de cunho racista, discriminatório ou qualquer outro que viole a legislação, a moral e os bons costumes; ***(c)*** violem direitos de terceiros, em especial direitos de propriedade intelectual, autorais, direitos de imagem, entre outros; ***(d)*** caracterizem infração civil ou penal e/ou possam causar prejuízos a **AGROLEND** e a terceiros; e ***(e)*** configurem concorrência desleal ou quebra de sigilo profissional; e

(ii) enviar, compartilhar e baixar: ***(a)*** arquivos que contenham vírus, *malware* ou outros códigos maliciosos; ***(b)*** *Informações* Internas, Confidenciais ou Secretas em ambiente externo; e ***(c)*** qualquer arquivo executável (.exe) que não seja autorizado pelo **Grupo AGROLEND**.

5.7.5. Guarda e Deslocamento de Informações

As Informações Protegidas que devem ser armazenadas em suporte físico ou digital, quando da sua guarda pelo Colaborador, devem respeitar regras de ciclo de vida dos dados da **AGROLEND**, assim como seguir os cuidados de acordo com a classificação da informação:

(i) Suporte físico: Os documentos com Informações Internas, Confidenciais e Secretas devem ser armazenados em arquivos físicos próprios indicados pela **AGROLEND**, de acordo com métodos de identificação do conteúdo, incluindo a data de arquivamento. Os documentos utilizados pelo Colaborador na estação de trabalho, quando não estiverem sendo utilizados, devem sempre ser guardados em gaveta ou armário, que deverão permanecer trancados quando se tratar de Informações Secretas. As anotações relacionadas às Informações Protegidas jamais podem ser deixadas à mostra, mesmo na presença do Colaborador.

(ii) Suporte digital: Todo e qualquer arquivo que contenha Informação Interna, Confidencial ou Secreta, deve ser salvo no repositório corporativo (em nuvem) da **AGROLEND**, em diretório específico, que inviabilize o acesso por Colaboradores não autorizados. Eventuais arquivos armazenados em dispositivo móvel (a exemplo, em *notebooks*, por conta de reuniões externas), devem ser removidos pelo Colaborador após a sua utilização.

Todo e qualquer documento ou arquivo que contenha Informações Confidenciais ou Secretas somente poderá ser movimentado se houver a possibilidade de recuperação ou análise dos registros de tal arquivo ou documento em caso de falhas de segurança que acarretem a perda ou o extravio das Informações Protegidas.

A **AGROLEND** declara que os dados pessoais coletados são armazenados com a finalidade de atender as obrigações legais, regulatórias, contratuais e de prevenção à fraude e lavagem de dinheiro aplicáveis, não obstante propósitos negociais da **AGROLEND**, observadas as normas e regulamentações aplicáveis à matéria.

Caso seja legítimo interesse empresarial da **AGROLEND** e não seja proibido por lei, é possível que os dados pessoais sejam armazenados por períodos mais longos que o mínimo exigido por lei, reservando-se, à **AGROLEND**, o direito de guardar e acessar os dados pessoais que coletar pelo tempo necessário para cumprir as leis e regulamentações aplicáveis.

5.7.6. Descarte de Informações

O descarte dos documentos físicos e/ou a exclusão de arquivos digitais da rede da **AGROLEND**, que contenham Informações Protegidas, deverá seguir as regras:

(i) Suporte físico: os documentos que tiverem Informações Públicas poderão ser descartados no lixo comum, já aqueles que possuírem Informações Internas, Confidenciais e Secretas devem ser destruídos manualmente ou, preferencialmente, através de um aparelho fragmentador, antes do descarte. Em caso de Informações Secretas, o uso de aparelho fragmentador é obrigatório e, na ausência de tal aparelho, o gestor responsável deverá ser acionado.

(ii) Suporte digital: arquivos que contenham Informações Protegidas e estejam armazenados em suporte digital flexível, tais como DVD ou CD, deverão ser destruídos através de aparelho fragmentador e, na ausência de tal aparelho, o Colaborador deverá acionar o gestor responsável. Os arquivos armazenados em suporte digital rígidos, como disco rígido (HD) e pen drive, devem ser encaminhados ao Diretor de Segurança Cibernética, em caixa lacrada, para destruição nos termos do procedimento interno adotado.

O responsável pela geração ou armazenamento do arquivo ou documento a ser descartado, tem competência para descartá-lo ou deletá-lo, salvo no caso de ter atribuído expressa autorização para que terceiro o faça.

Para o fim de se manter o histórico e possibilitar a realização de auditorias, caso necessário, todo descarte deve ser registrado.

5.8. INTERNET

As regras da **AGROLEND** visam ao desenvolvimento de um comportamento ético e profissional no uso da internet, garantindo a utilização racional de tais recursos, bem como a segurança dos dados e sistemas. A **AGROLEND**, se necessário, utilizará ferramentas para verificação do conteúdo de correios eletrônicos (*e-mails*) corporativos e monitoramento do uso da internet e rede corporativa.

Eventuais tentativas de alteração dos parâmetros de segurança, sem autorização para tal, serão julgadas inadequadas e os riscos relacionados serão informados ao Colaborador e ao respectivo gestor. O uso de recursos para atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de ações civis e criminais, sendo que nesses casos a **AGROLEND** cooperará ativamente com as autoridades competentes.

Os Colaboradores com acesso à internet somente poderão fazer o *download* de *softwares* ligados às suas atividades na **AGROLEND** e deverão providenciar a regularização da licença e o registro de tais *softwares*, com orientação e a aprovação da área de Tecnologia da Informação (TI).

Proibido:

(i) utilizar os recursos da **AGROLEND** para fazer *download* ou distribuição de *software* ou dados sem as licenças adequadas;

(ii) efetuar *upload* ("subir") de qualquer *software* licenciado à **AGROLEND** ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo *software* ou pelos dados; e

(iii) utilizar a rede de visitantes (rede de Internet segregada) com seus dispositivos de trabalho, exceto se prévia e expressamente autorizado pelo departamento competente, hipótese em que serão aplicáveis todas as limitações de uso aqui previstas.

5.9. REDES SOCIAIS, WHATSAPP E E-MAIL PESSOAIS

O uso de redes sociais, serviços de correio eletrônico (*e-mail*), WhatsApp e outros mensageiros, para finalidades pessoais em dispositivos disponibilizados pela **AGROLEND**, é autorizado, desde que:

(i) não sejam utilizados para acesso ou divulgação de quaisquer Informações Protegidas;

(ii) não sejam utilizados para acesso ou divulgação de conteúdo não autorizado;

(iii) não atrapalhe o exercício das atividades do Colaborador ou qualquer Colaborador;

(iv) o Colaborador não compartilhe, poste, divulgue ou exponha qualquer imagem, foto, vídeo ou som captado no ambiente interno da **AGROLEND**; e

(v) o Colaborador não compartilhe, poste, divulgue ou exponha qualquer comentário ou texto que revele ou induza terceiros a acreditar que é uma opinião ou posicionamento da **AGROLEND** ou do **Grupo AGROLEND**.

O Colaborador é o único responsável pelo uso e pela guarda de suas senhas de acesso a redes sociais e correios eletrônicos (*e-mails*) pessoais, e a **AGROLEND** recomenda o uso de navegação anônima para aplicações particulares em equipamentos de propriedade da **AGROLEND**.

A utilização e o acesso a tais aplicações, nas dependências físicas ou de rede da **AGROLEND**, a seu exclusivo critério, poderá ser suspensa, temporariamente e sem aviso prévio, por questões de governança e/ou de segurança da informação.

5.10. COMUNICAÇÃO INTERNA

A **AGROLEND** pode disponibilizar para uso do Colaborador, por meio dos equipamentos corporativos, uma ou mais aplicações de comunicação colaborativa (ex.: Google Meeting, Slack, Jira), desde que tais aplicações trafeguem os dados de forma criptografada e exija a autenticação que esteja vinculada conta corporativa da **AGROLEND**. Essas aplicações possibilitam a troca de mensagens de texto, voz e vídeo em tempo real no ambiente de trabalho. O acesso e uso de tal ferramenta é destinado exclusivamente para fins profissionais, sendo vedado qualquer uso para finalidades pessoais, pelo que as informações trocadas estão sujeitas ao monitoramento.

O Colaborador está ciente que, na utilização da ferramenta, não poderá:

(i) enviar mensagens com Informações Confidenciais ou Secretas;

(ii) enviar mensagens que violem a legislação em vigor ou cujo conteúdo verse sobre drogas, violência, racismo ou qualquer forma de discriminação, ameaça, pornografia ou qualquer outro que seja ofensivo e desrespeite a moral e os bons costumes;

(iii) enviar mensagens com propagandas, correntes, boatos ou qualquer tipo de mensagem que, além de sobrecarregar os sistemas da **AGROLEND** com o tráfego excessivo, possa causar danos a terceiros; e

(iv) interceptar mensagens de terceiros ou se fazer passar por qualquer outra pessoa forjando quaisquer mensagens.

5.11. ACESSO À REDE DE ARQUIVOS

O acesso às informações armazenadas na infraestrutura tecnológica (nuvem) da **AGROLEND** é restrito a cada Colaborador, a depender do perfil de acesso que lhe for atribuído pelo responsável pela liberação, conforme as

regras dispostas na presente Política – "Identificação e Senhas". É pressuposto que cada perfil tenha liberação do acesso de determinados diretórios específicos da **AGROLEND**, que são definidos a exclusivo critério do responsável pela liberação, ou seja, as informações poderão ser acessadas de acordo com o nível de acesso definido pela **AGROLEND**.

O acesso remoto é permitido para execução das atividades profissionais do Colaborador vinculadas à **AGROLEND**, motivo pelo qual tal acesso não poderá ser realizado por dispositivo ou *software* particulares do Colaborador ou de terceiros.

É de total responsabilidade do Colaborador as atividades realizadas quando do seu acesso remoto, pelo que responde por qualquer uso irregular, mesmo que seja de outra pessoa na posse de seu acesso.

5.12. AUTENTICAÇÃO, IDENTIFICAÇÃO E SENHAS

Os privilégios de acesso a Informações Protegidas são concedidos ao Colaborador, de acordo com o cargo e suas atribuições, que receberá um login e uma senha, que permitirá ser identificado quando do acesso à infraestrutura da **AGROLEND.** A **AGROLEND** reserva-se o direito de revisar, a qualquer momento e sem aviso prévio, por meio dos departamentos competentes, os privilégios de qualquer Colaborador, a fim de resguardar os níveis de segurança da informação da **AGROLEND**.

O login e a senha do Colaborador são pessoais e, consequentemente, o Colaborador é o responsável pelo sigilo e pela manutenção segura da sua senha vinculada ao login, sendo proibido o compartilhamento de login e senha com terceiros, inclusive outros Colaboradores, sob pena de arcar com as sanções não só previstas nesta Política, mas também as penalidades civis, criminais e trabalhistas, respondendo, ainda, por todo e qualquer dano que causar a **AGROLEND**.

5.13. DISPOSITIVOS

Os dispositivos físicos para armazenamento de Informações Protegidas, como computadores, celulares, *notebooks*, *tablets* e outros, disponibilizados aos Colaboradores para a execução de suas atividades, são de propriedade da **AGROLEND**, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse único e exclusivo da **AGROLEND**, cumprindo as recomendações constantes nos procedimentos operacionais.

Os equipamentos devem ser identificados de forma individual, inventariados e protegidos de quaisquer acessos indevidos. Devem ter o recurso de atualizações automáticas do sistema operacional habilitado por padrão e *software* antivírus instalado, ativado e atualizado frequentemente, sendo que em caso de suspeita de vírus ou problemas na funcionalidade, o usuário deverá acionar imediatamente a área de TI.

Os arquivos pessoais e/ou não pertinentes aos negócios da **AGROLEND** (fotos, músicas, vídeos etc.) não deverão ser copiados/movidos para os *drives* de armazenamento, pois podem sobrecarregar os recursos disponibilizados.

Caso identificada a existência desses arquivos, eles poderão ser excluídos por meio de comunicação prévia ao usuário.

Os documentos imprescindíveis para as atividades dos Colaboradores na instituição devem ser salvos nos espaços disponibilizados pela **AGROLEND**, onde é garantido o *back-up* e a disponibilidade. Tais arquivos, não devem ser gravados nos drives locais dos dispositivos, pois não terão garantia de *back-up* e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio Colaborador a inobservância do procedimento.

No caso de furto, roubo, perda ou extravio do equipamento móvel da **AGROLEND,** ou ainda de dispositivos pessoais configurados com dados da **AGROLEND**, o Colaborador deve imediatamente comunicar o Diretor de Segurança Cibernética e na sequência e, quando cabível procurar uma autoridade policial para lavrar um boletim de ocorrência. A **AGROLEND**, quando julgar necessário pode exigir a cópia do boletim de ocorrência lavrado.

Todos os acessos remotos são registrados pela equipe de TI, e tais registros ficam disponíveis para consulta em caso de auditoria.

A utilização indevida dos dispositivos da **AGROLEND** sujeitará o Colaborador às sanções aplicáveis, a depender da gravidade da conduta praticada, sendo hipóteses de uso indevido:

- tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- burlar ou tentar burlar quaisquer sistemas de segurança;
- acessar informações confidenciais sem explícita autorização do proprietário;
- vigiar secretamente outrem por dispositivos eletrônicos ou softwares;
- interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e/ou a ordem pública; e
- utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

5.14. DATACENTER E CLOUD

A **AGROLEND** utiliza diversos *softwares* próprios ou de terceiros no curso de suas operações, assim o Colaborador não pode:

(i) utilizar tais *software*s para fins pessoais ou de qualquer forma que comprometa a segurança cibernética da **AGROLEND**;

(ii) excluir, modificar, copiar, transferir, realizar engenharia reversa ou ceder o acesso de tais *softwares* a terceiros, ou praticar qualquer ato que esteja em desacordo com a legislação aplicável; e

(iii) instalar nos dispositivos da **AGROLEND** qualquer *software* pirata, não licenciado ou não autorizado pela área TI, sendo que qualquer *software* não autorizado que seja baixado pelo Colaborador, será excluído pela equipe de TI.

Em todos os processos de contratação de serviços de Datacenter e nuvem (*cloud*) (*outsourcing*) a **AGROLEND** exige a apresentação de certificações de segurança, conforme o tipo de serviço que será hospedado.

5.15. REPORTE DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A **AGROLEND** emprega medidas de segurança para evitar a exposição indevida das Informações Protegidas, tanto internas quanto externas, as quais atendem às obrigações legais vigentes. No entanto, tais medidas somente serão eficazes se o Colaborador efetivamente cumprir com as obrigações de segurança assumidas nesta Política, uma vez que tais incidentes podem ocorrer em razão de falhas humanas, tecnológicas ou sistêmicas.

As violações às regras desta Política ou coloquem em risco a segurança das informações da **AGROLEND**, deverão imediatamente ser comunicada ao Diretor de Segurança da Informação da **AGROLEND**. A **AGROLEND**, por meio do Diretor de Segurança da Informação, irá apurar as causas e os efeitos do incidente ocorrido, para então tomar as medidas de contenção, avaliação de impacto e necessidade de comunicação sobre o incidente ao órgão competente e/ou aos titulares das Informações Protegidas.

Para que seja realizada uma auditoria sobre o incidente, a **AGROLEND** analisará toda e qualquer informação, assim como as evidências disponíveis que possam identificar a causa do problema, que serão compiladas e anexadas a um relatório para formalização da ocorrência.

5.16. RELATÓRIO ANUAL SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

Um relatório anual será elaborado demonstrando a implementação do plano de resposta a incidentes, com data-base de 31 de dezembro. O relatório anual deverá abordar, no mínimo:

- A efetividade da implementação das ações descritas nessa política;

- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes descritos nessa Política;

- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

- Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório anual é apresentado à Diretoria da **AGROLEND** até 31 de março do ano seguinte ao da data-base.

5.17. MECANISMOS PARA DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

Os Colaboradores devem cumprir as disposições expressas nesta Política, independentemente de cargo, função, área de atuação ou localidade na qual exerça suas atividades profissionais vinculadas à **AGROLEND**.

Todos os Colaboradores, no ato de sua contratação, receberão uma cópia desta Política, em formato impresso ou digital, conforme estabelecido pela **AGROLEND**, bem como eventual documentação de suporte aplicável, que estabeleça, além dos procedimentos de segurança a serem seguidos pelo Colaborador, regras sobre o correto uso das ferramentas e Informações Protegidas.

Com a ciência do Colaborador e concordância com os termos descritos nesta Política e na documentação suporte, deverá assinar um termo de responsabilidade (por meio de assinatura física ou digital ou por meio de mecanismo de consentimento digital) para formalizar o seu comprometimento quanto as disposições vigentes e suplementares.

Eventuais alterações introduzidas na Política e nos documentos suporte serão comunicadas por escrito ao Colaborador, sendo responsabilidade do Colaborador ler atentamente as atualizações enviadas. A manifestação de aceite, pelo Colaborador, às alterações apresentadas será realizada conforme oportunamente definido pela **AGROLEND**, mediante a assinatura do Colaborador, física ou digital, ou por meio de mecanismo de consentimento digital.

6. PENALIDADES

Atitudes que violem a presente Política serão devidamente apuradas, tratadas e encaminhadas para deliberação da Diretoria de Conformidade e Controles Internos.

Qualquer descumprimento das disposições da presente Política acarretará a adoção das medidas corretivas correspondentes, sem prejuízo da adoção de eventual medida disciplinar em relação à Parte Interessada que tiver contribuído para o descumprimento de forma negligente ou intencional.

As medidas disciplinares a serem adotadas pela Diretoria de Conformidade e Controles Internos poderão incluir, entre outras, as penalidades de: (i) advertência; (ii) suspensão; (iii) demissão por justa causa; (iv) rescisão

contratual; (v) destituição do cargo de diretor, ou, ainda, exclusão do quadro societário; sem prejuízo da adoção das medidas judiciais cabíveis e de o infrator responder civil, trabalhista e/ou criminalmente, conforme previsto na legislação brasileira.

O(s) Colaborador(es)/Parte(s) Interessada(s) que cometerem infração às regras desta Política serão comunicados por escrito, por meio de comunicação contendo a regra violada, a conduta praticada pelo infrator e a sanção aplicada pela **AGROLEND**, sem prejuízo de eventual indenização paga pelo(s) Colaborador(es)/Parte Interessada(s) a ser apurada judicialmente.

7. HISTÓRICO DE ALTERAÇÕES HISTÓRICO DE ALTERAÇÕES

Descrição da Alteração	**Versão**
Atualização dos tópicos relacionados a alteração da regulamentação	2.0
Atualização de layout Atualização da razão social da Agrolend Ajuste do tópico de penalidades	3.0
Atualização de layout Ajuste do número de versão do documento	4.0
Alteração na definição de Colaboradores Ajustes pontuais no texto	5.0

8. APROVAÇÃO

Esta Política foi aprovada pela Diretoria da Instituição em agosto de 2025.