POLÍTICA DE SEGURANÇA CIBERNÉTICA E TRATAMENTO DE DADOS DA AGROLEND SOCIEDADE DE CRÉDITO DIRETO S.A.

VERSÃO **1**, APROVADA EM 5 DE OUTUBRO DE 2021.

INTRODUÇÃO

A presente Política de Segurança Cibernética e Tratamento de Dados (a "Política") orienta e estabelece as diretrizes corporativas da Agrolend Sociedade de Crédito Direto S.A., sociedade anônima inscrita no Cadastro Nacional da Pessoa Jurídica do Ministério da Economia sob o nº 43.774.196/0001-84 ("AGROLEND"), para assegurar a confidencialidade, a integralidade, a disponibilidade e o tratamento dos dados e dos sistemas de informação da **AGROLEND**. Deve ser cumprida e aplicada em todas as áreas da **AGROLEND** e de seu grupo econômico ("Grupo AGROLEND"), por todas as pessoas físicas e jurídicas, sejam eles sócios, diretores, administradores, empregados, funcionários, prestadores de serviços, parceiros e/ou quaisquer outros terceiros (em conjunto, os "Colaboradores") que, no âmbito dessa relação, possam vir a ter acesso às áreas, equipamentos, informações, arquivos, redes e dados de titularidade da **AGROLEND** e/ou por ela obtidos, cujo acesso seja controlado.

Para fins da presente Política, deve-se entender como Grupo **AGROLEND** todas as empresas do grupo econômico da **AGROLEND**, incluindo controladas e controladoras, bem como a própria **AGROLEND** Sociedade de Crédito Direto S.A.

SUMÁRIO

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 do Grupo **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 que tem 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 os clientes, as práticas e as escolhas de privacidade que possuem para a utilização dos serviços da **AGROLEND**.

ABRANGÊNCIA

Esta Política aplica-se a todos e quaisquer dados relativos à **AGROLEND**, incluindo, mas não se limitando a dados sobre seus negócios, dados sobre operações de crédito, dados de clientes, dados pessoais e dados sensíveis, os quais podem ser coletados sobre as pessoas físicas relacionadas à **AGROLEND**, incluindo seus Colaboradores e clientes.

Aplica-se a todo o Grupo **AGROLEND**, na utilização de dispositivos, acesso e tratamento de sistemas de informações, aos servidores, conexões à rede e à internet e quaisquer outros recursos tecnológicos ou que contenham informações da **AGROLEND**.

Neste sentido, respeitada a legislação e se necessário, a **AGROLEND** poderá monitorar, gravar e registrar os ambientes, sistemas, serviços, computadores e redes, para garantir a disponibilidade e a segurança das informações utilizadas. É obrigação de cada Colaborador manter-se atualizado em relação a esta Política, aos procedimentos e às normas relacionadas aplicáveis.

1. COMITÊ DE SEGURANÇA CIBERNÉTICA

O Comitê de Segurança Cibernética (o "CSC"), é o comitê área de segurança da informação ("Área de Segurança da Informação"), responsável pela elaboração e atualização desta Política, o órgão com a função de discutir e deliberar sobre assuntos relacionados à segurança cibernética da **AGROLEND**. Toda e qualquer dúvida sobre o conteúdo desta Política deve ser encaminhada ao CSC, através do correio eletrônico (*e-mail*): csc@agrolend.agr.br.

A Área de Segurança da Informação é a responsável pela implementação das diretrizes e obrigações previstas nesta Política e/ou definidas pelo CSC, sendo que quaisquer questões sobre a implementação das obrigações aqui previstas devem ser encaminhadas à Área de Segurança da Informação através do correio eletrônico (*e-mail*): si@agrolend.agr.br.

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 e por escrito pelos representantes legais da **AGROLEND**.

O Colaborador poderá ser responsabilizado por eventual uso indevido da Informação Protegida, pelo que a **AGROLEND** se reserva o direito de monitorar o uso das Informações Protegidas pelo Colaborador 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 a **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 pelo Grupo **AGROLEND** com terceiros somente poderá ser divulgada após análise e validação do Comitê de Segurança Cibernética da **AGROLEND**.

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 do Grupo **AGROLEND**, designadas para tal. Embora o Grupo **AGROLEND** não tenha interesse em divulgá-la a indivíduos externos, a disponibilização dessa informação não tem o potencial de causar danos sérios ao Grupo **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 o Grupo **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 ao Grupo **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 do Grupo **AGROLEND**, sempre serão consideradas Informações Secretas.

Além das Informações Protegidas, há também a informação Pública, destinada ao público em geral e já divulgada pelo Grupo **AGROLEND**, cuja utilização por quaisquer indivíduos independe de autorização e não é passível de prejuízos para o Grupo **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, abaixo indicados:

(a) documentos impressos: a classificação da informação deve ser indicada no topo de todas as páginas, de forma visível, quando o documento for gerado dentro do Grupo **AGROLEND**, ou marcado com uma etiqueta ou carimbo quando o documento for gerado externamente por outras organizações;

(b) documentos eletrônicos: a classificação da informação deve ser indicada no nome do arquivo. Caso o arquivo eletrônico possa ser impresso, as regras descritas no subitem (i) deverão ser observadas;

(c) correio eletrônico (*e-mail*): a classificação da informação deve ser indicada em letra maiúscula no assunto do correio eletrônico (*e-mail*) e o rodapé de todos os correios eletrônicos (*e-mails*) enviados deve conter *disclaimer* equivalente: "*A informação contida nesta mensagem e seus anexos é restrita e/ou confidencial, para uso exclusivo de seu destinatário. Caso você não seja o destinatário desta mensagem, notifique o remetente e descarte esta mensagem.";*

(d) bancos de dados e aplicações: a classificação deve estar indicada nos "metadados" dos registros. Eventuais relatórios oriundos dessas aplicações e banco de dados deverão seguir os padrões mencionados nos tópicos supra; e

(e) outros tipos de mídia: a classificação deverá ser visível pelos recursos que se façam necessários.

Caso o Colaborador receba uma informação que não esteja 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 CSC. A classificação das Informações Protegidas é de extrema importância para a sua rastreabilidade.

A **AGROLEND** coletará informações sobre seus clientes e/ou Colaboradores quando estes usarem seus aplicativos digitais ou acessarem o(s) seu(s) sítio(s) eletrônico(s) (disponíveis sob o nome de domínio agrolend.agr.br) ou celebrarem com 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.

4. PRIVACIDADE E PROTEÇÃO DE DADOS

A **AGROLEND** coletará informações sobre seus clientes e/ou Colaboradores quando estes acessarem o seu sítio eletrônico (disponível no endereço eletrônico agrolend.agr.br) ou celebrarem com 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 do Grupo **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 do Grupo **AGROLEND**.

O Grupo **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 (*firewalls)*, gestão de criptografia de dados, uso de autenticação e controles de acesso físico a centros de dados, uso de autenticação e controles de autorização de acesso a informações, uso de políticas de senha, de sistemas de detecção de intrusão (IDS) e sistemas de prevenção a intrusão (IPS), execução testes de penetração e *scans* de vulnerabilidade periódicos, modelagem de segurança de aplicações e desenvolvimento seguro, gestão de mudanças e de liberação, gestão de dispositivos móveis e fingerprinting e monitoramento de segurança.

Os Colaboradores declaram-se cientes do compromisso do Grupo **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. DADOS PESSOAIS

Os dados pessoais ("Dados Pessoais") são informações que podem ser associadas a uma pessoa identificada ou identificável, e podem ser identificados como: nome, endereço (incluindo endereços de cobrança e entrega), número de telefone, correio eletrônico (*e-mail*), número do cartão de pagamento, informações financeiras, número da conta, data de nascimento e credenciais emitidas pelo governo (por exemplo, número da carteira de motorista, nº do RG, informações do passaporte, nº do Cadastro da Pessoa Física do Ministério da Economia (CPF/ME) e nº do Cadastro Nacional da Pessoa Jurídica do Ministério da Economia - CNPJ/ME).

Os Dados Pessoais dos clientes e/ou Colaboradores são armazenados para cumprir obrigações legais, regulatórias, contratuais, de prevenção à fraude e lavagem de dinheiro e questões relacionadas aos negócios do Grupo **AGROLEND**.

A **AGROLEND** poderá 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 ao Grupo **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 por que os clientes e/ou Colaboradores visitam os serviços da **AGROLEND**.

5.1. Utilização de Cookies

A **AGROLEND** e seus Colaboradores podem usar informações de navegação coletadas por *Cookies* para:

- reconhecer o cliente, o Colaborador e/ou o visitante;
- personalizar suas experiências online, os serviços que o cliente e/ou o Colaborador utiliza e outros conteúdos de publicidade;
- avaliar a eficiência de promoções; e
- reduzir riscos, evitar fraudes potenciais e promover confiança nos serviços do Grupo **AGROLEND**.

Caso o cliente e/ou o Colaborador opte por desativar ou recusar os *Cookies*, o uso dos serviços poderá ser limitado ou, em alguns casos, impossibilitado em razão de certos aspectos e recursos só estarem disponíveis através do uso de *Cookies*.

5.2. Opções de Privacidade Disponíveis

O cliente e/ou o Colaborador tem 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 pode 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.

- Registro do cliente e/ou o Colaborador e informações da conta: Se tiver uma conta, o cliente e/ou o Colaborador geralmente pode revisar e editar os Dados Pessoais ao acessá-la, atualizar as informações de forma direta, ou entrar em contato com a **AGROLEND**.

- 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 pode gerenciar suas preferências no respectivo dispositivo.

- Informativos: A **AGROLEND** enviará comunicações necessárias ou obrigatórias a respeito dos serviços, o 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.

6. MONITORAMENTO E AUDITORIA DO AMBIENTE

Com o objetivo de apurar o cumprimento das normas de segurança da **AGROLEND**, respeitados a legislação em vigor, **TODO AMBIENTE FÍSICO E DIGITAL DO GRUPO AGROLEND É OU PODERÁ 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** poderá monitorar todos os servidores, redes, conexões de internet, *softwares*, equipamentos e dispositivos corporativos, móveis ou não, conectados à rede corporativa; 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 poderá identificá-lo e apresentar dados sobre o seu uso da infraestrutura técnica do Grupo **AGROLEND** e do material e conteúdo manipulado, sendo certo que todas as informações coletadas no curso do monitoramento são guardas nos *back-ups* do Grupo **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 do Grupo **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.

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.

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.

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.

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.

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 do Grupo **AGROLEND**, seja através de equipamentos de propriedade do Grupo **AGROLEND** para o uso do Colaborador ou até mesmo equipamentos do próprio Colaborador, caso autorizado pelo Grupo **AGROLEND** nos termos das regras definidas no item 15, abaixo - "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 do Grupo **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 ao Grupo **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**.

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 pelo Grupo **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 na rede corporativa do Grupo **AGROLEND**, em diretório específico, que inviabilize o acesso por Colaboradores não autorizados. Eventuais arquivos a serem armazenados em dispositivo móvel (a exemplo, em *notebooks*, por conta de reuniões externas), serão 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 do Grupo **AGROLEND**, observados 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, a **AGROLEND**, o direito de guardar e acessar os dados pessoais que coletar pelo tempo necessário para cumprir as leis e regulamentações aplicáveis.

7.6. Descarte de Informações

O descarte dos documentos físicos e/ou a exclusão de arquivos digitais da rede do Grupo **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 a área de Segurança da Informação, 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.

8. E-MAIL CORPORATIVO

Os endereços de correio eletrônico (*e-mail*) fornecidos pela **AGROLEND** ou pelo Grupo **AGROLEND** aos Colaboradores, são individuais e destinados para fins exclusivamente corporativos e relacionados às atividades do Colaborador dentro do Grupo **AGROLEND**.

As mensagens de correio eletrônico (*e-mail*) sempre deverão incluir assinatura com o formato padrão da **AGROLEND** ou do Grupo **AGROLEND**, conforme aplicável, sendo proibido aos Colaboradores o uso do correio eletrônico (*e-mail*) para:

- enviar mensagens não solicitadas para vários destinatários, exceto se relacionadas a uso legítimo da **AGROLEND**;
- enviar qualquer mensagem por meios eletrônicos que torne o remetente e/ou qualquer empresa do Grupo **AGROLEND** vulneráveis a ações civis, trabalhistas ou criminais;
- divulgar informações não autorizadas, incluindo, mas não se limitando a imagens de tela, sistemas, documentos e afins, sem a expressa autorização do responsável;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas; e
- apagar mensagens pertinentes de correio eletrônico (e-mail) quando sujeito a algum tipo de investigação.

9. 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, será julgada inadequada 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 no Grupo **AGROLEND** e deverão providenciar a regularizar a licença e o registro de tais *softwares*, com orientação e a aprovação da área de Tecnologia da Informação (TI).

É proibido:

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

(ii) efetuar *upload* (“subir”) de qualquer *software* licenciado ao Grupo **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.

10. 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, 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 do Grupo **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 o Grupo **AGROLEND** recomenda o uso de navegação anônima para aplicações particulares em equipamentos de propriedade do Grupo **AGROLEND**.

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

11. COMUNICAÇÃO INTERNA

O Grupo **AGROLEND** pode disponibilizar para uso do Colaborador, por meio dos equipamentos corporativos, uma ou mais aplicações de comunicação colaborativa (ex.: Google Meeting, Microsoft Teams, Atlassian 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 do Grupo **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.

12. ACESSO À REDE DE ARQUIVOS

O acesso às informações armazenadas na infraestrutura técnica do Grupo **AGROLEND** poderá ser realizado de maneira diferente (por meio físico, lógico ou remoto), a depender do tipo de formato, ao qual serão aplicadas regras de conduta distintas.

12.1. Acesso Físico ao Datacenter

Os locais de instalação dos *datacenters* da **AGROLEND** são considerados parte crítica da sua infraestrutura tecnológica, e por tal motivo o cuidado com a proteção e segurança deve ser redobrado. Dentre os diferentes tipos de acessos, tem-se para cada, diferentes regras e restrições:

(i) permanente: acesso permitido somente aos empregados do Grupo **AGROLEND** que tenham a necessidade de acesso liberado para executar suas atividades;

(ii) esporádico: acesso permitido a outros Colaboradores ou a visitantes externos, mediante autorização prévia da **AGROLEND**, com acesso registrado pela equipe de TI, com indicação de nome, data e horário, e desde que haja acompanhamento em tempo integral pela equipe responsável; e

(iii) externos: acesso permitido àqueles que não sejam Colaboradores do Grupo **AGROLEND** (externos), mediante autorização e desde que tenham contrato vigente com o Grupo **AGROLEND** que justifique tal acesso.

12.2. Acesso Lógico

O acesso às informações armazenadas na infraestrutura tecnológica do Grupo **AGROLEND** será restrito a cada Colaborador, a depender do perfil de acesso que lhe for atribuído pela área de TI, conforme as regras dispostas no item 13 – "Autenticação, Identificação e Senhas". É pressuposto que cada perfil tenha liberação do acesso de determinados diretórios dentro da rede do Grupo **AGROLEND**, que são definidos a exclusivo critério da área de TI, ou seja, as informações poderão ser acessadas de acordo com o nível de acesso definido pelo Grupo **AGROLEND**.

12.3. Acesso Remoto

O Colaborador poderá acessar a rede privada do Grupo **AGROLEND** de forma remota, por meio de tecnologias autorizadas, que pode incluir o uso de VPN. O acesso remoto somente será concedido ao Colaborador nos casos em que houver necessidade comprovada, através de aprovação formal do Grupo **AGROLEND** ou somente a implantação de Política específica de *Home Office*.

O acesso remoto é permitido para execução das atividades profissionais do Colaborador vinculadas ao Grupo **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.

No caso de furto, roubo ou extravio do equipamento móvel que tenha o acesso remoto à VPN do Grupo **AGROLEND** configurado, o Colaborador deverá imediatamente procurar uma autoridade policial para lavrar um boletim de ocorrência e, na sequência, comunicar o incidente à equipe de TI, apresentado cópia do boletim de ocorrência lavrado.

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

13. AUTENTICAÇÃO, IDENTIFICAÇÃO E SENHAS

Os privilégios de acesso a Informações Protegidas são concedidos ao Colaborador, de acordo com o cargo e suas atribuições. A exemplo, o acesso externo ao correio eletrônico (*e-mail*), liberação ao acesso à Internet e no acesso lógico, utilização externa de alguns equipamentos do Grupo **AGROLEND**, liberação de espaço em disco rígido, utilização de dispositivos móveis, entre outros.

O Colaborador receberá um login e uma senha, de acordo com o perfil que lhe for atribuído, que permitirá ser identificado quando do acesso à infraestrutura do Grupo **AGROLEND**. Assim, o Colaborador somente terá acesso às áreas da infraestrutura do Grupo **AGROLEND** que forem autorizadas conforme o seu perfil. 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 ao Grupo **AGROLEND**.

De acordo com o perfil, além do login do Colaborador, também receberá uma identificação física que lhe concederá acesso a determinadas áreas físicas do Grupo **AGROLEND**, que poderá ser realizada através de crachá, cujo uso é pessoal e intransferível, e terá por finalidade registrar a entrada e saída das dependências das empresas do Grupo **AGROLEND**.

14. 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 do Grupo **AGROLEND**, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse único de exclusivo do Grupo **AGROLEND**, cumprindo as recomendações constantes nos procedimentos operacionais fornecidos pela área de TI.

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 habilitada 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 do Grupo **AGROLEND** (fotos, músicas, vídeos etc.) não deverão ser copiados/movidos para os *drives* de rede, pois podem sobrecarregar o armazenamento no disco do computador. 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 deverão ser salvos em diretório centralizado seja em data center físico (via sftp ou ssh ou outro protocolo seguro de transferência de arquivos), ou salvos em serviços de armazenamento em nuvem (*cloud*), como, por exemplo: Amazon AWS S3, Google Drive ou a Suíte de Documentos em Nuvem do Google (Planilhas, Documentos, etc.), desde que seja garantido o *back-up* e a disponibilidade por meio de qualquer computador. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), 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.

O Colaborador entende que é o responsável por todo e qualquer dano que causar nos equipamentos, por dolo, negligência ou culpa, e está ciente e concorda em observar as regras:

- o Colaborador é responsável pelos equipamentos utilizados e se compromete a empregar os cuidados necessários, como se o dispositivo fosse seu;
- os computadores de uso individual deverão ter senha de BIOS para restringir o acesso de Colaboradores não autorizados, sendo que tais senhas serão definidas pela área de TI do Grupo **AGROLEND**, que terá acesso a elas para manutenção dos equipamentos;
- os dispositivos devem estar sempre em seu alcance e não podem ser deixados em locais públicos, em veículos ou em qualquer outro local fora das dependências das empresas do Grupo **AGROLEND** em que possa haver acesso do equipamento por pessoas não autorizadas, a fim de evitar o furto e/ou roubo destes equipamentos, bem como o vazamento das Informações Protegidas nele contidas;
- os Colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;

- é vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico de TI do Grupo **AGROLEND** ou por terceiros devidamente contratados para o serviço;
- o Colaborador deverá manter a configuração do equipamento disponibilizado pelo Grupo **AGROLEND**, seguindo os devidos controles de segurança exigidos pela presente Política e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;
- é expressamente proibido o fumo na mesa de trabalho e próximo aos equipamentos;
- deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados;
- os recursos tecnológicos adquiridos pelo Grupo **AGROLEND** devem ter imediatamente suas senhas padrões (default) alteradas;
- quando o Colaborador usar um dispositivo em um local público, deve utilizar película protetora em tal dispositivo, a fim de impedir a visualização de conteúdo por terceiros;
- todos os dispositivos devem ser protegidos por senha e não devem ficar logados quando o Colaborador não estiver presente;
- caso, no decorrer do uso do dispositivo, o Colaborador tiver dúvidas sobre o seu manuseio ou constatar falhas que impliquem na necessidade de sua substituição ou manutenção, o Colaborador deverá abrir um chamado junto a área de TI que, por sua vez, além de fornecer os esclarecimentos necessários, deverá orientá-lo a entregar o equipamento no local indicado para sua substituição ou conserto;
- caso o uso de um dispositivo seja esporádico, o Colaborador deverá devolvê-lo a área de TI em perfeitas condições de uso, juntamente com eventuais acessórios lhe tenham sido entregues, como bolsas, cases, películas etc., tão logo termine o período necessário para o uso. Em caso de não devolução do equipamento, no prazo e local determinado, o Colaborador será responsável por restituir os custos de tal equipamento ao Grupo **AGROLEND**, sem prejuízo de outras medidas legais e administrativas a serem tomadas pelo Grupo **AGROLEND**; e
- no caso de perda, furto, roubo ou dano ao equipamento, o Colaborador deve comunicar imediatamente a área de TI, que procederá com a remoção do conteúdo corporativo contido no dispositivo. O Colaborador também deverá procurar as autoridades policiais e realizar um boletim de ocorrência, que obrigatoriamente deverá ser apresentado ao quando da comunicação do incidente.

A utilização indevida dos dispositivos do Grupo **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, como, por
- exemplo, analisadores de pacotes (sniffers);

- 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.

É proibida a utilização, pelo Colaborador, de dispositivos móveis particulares ou de terceiros (tais como celulares, *smartphones*, *notebook*s, *tablets*, entre outros) para o desenvolvimento das atividades profissionais vinculadas à **AGROLEND**, a exceção de quando previamente autorizado pelo Grupo **AGROLEND**, que auxiliará o Colaborador na instalação do mesmo.

15. DATACENTER E *CLOUD*

O Grupo **AGROLEND** utiliza diversos *softwares* próprios ou de terceiros no curso de suas operações, assim o Colaborador não poderá:

(i) utilizar tais *software*s para fins pessoais ou de qualquer forma que comprometa a segurança da infraestrutura do Grupo **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 na rede ou nos dispositivos do Grupo **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.

O Grupo **AGROLEND** disponibiliza apenas o(s) recurso(s) Amazon WebServices e Google Workspace para o armazenamento externo de arquivos, *software*s e sistemas. Desta forma, é proibida a utilização pelo Colaborador de serviços de armazenamento na nuvem não disponibilizados por meio da infraestrutura tecnológica do Grupo **AGROLEND**, como por exemplo, Dropbox e iCloud.

A contratação de serviços de Datacenter e nuvem (*cloud*) (*outsourcing*) deverá ter certificações de segurança, como exemplo SSAE 16, ISAE 3402, ISO 27001 e PCI DSS, conforme o tipo de serviço que será hospedado ou novos padrões de certificações que surgirem no mercado.

Os relatórios pertinentes as certificações devem ser apresentados anualmente, contendo os detalhes sobre o nível de implementação dos controles, sendo que os relatórios das certificações SSAE 16 e ISAE 3402, por exemplo, devem ser apresentados nos formatos SOC2 e SOC3.

16. DESLIGAMENTO OU MOVIMENTAÇÃO DE COLABORADOR

Ao término do vínculo do Colaborador com o Grupo **AGROLEND**, o acesso à infraestrutura tecnológica do Grupo **AGROLEND** será imediatamente revogado, momento em que o Colaborador deverá devolver todos e quaisquer dispositivos de propriedade do Grupo **AGROLEND** que estejam em sua posse, em perfeitas condições de uso, juntamente com eventuais acessórios lhe tenham sido entregues. Todas e quaisquer obrigações de sigilo e a não reprodução das Informações Protegidas, assumidas pelo Colaborador nessa Política, permanecerão em vigor mesmo após o término de referido vínculo.

Em caso de não devolução de quaisquer equipamentos, no prazo e local determinado, o Colaborador será responsável por restituir os custos respectivos ao Grupo **AGROLEND**. Em caso de perda, furto ou roubo de equipamentos, serão aplicadas as regras previstas do item 14 – "Dispositivos".

O Colaborador que tenha acesso à conta de correio eletrônico (*e-mail*) corporativa ou a qualquer outro *software* instalado em seu dispositivo pessoal, deverá apresentar esse dispositivo para a área de TI, que procederá à sua desinstalação.

Caso o Colaborador mude de área ou de função dentro do Grupo **AGROLEND**, este também deverá ter seus acessos revistos, passando a visualizar apenas os sistemas e pastas de rede necessários ao desempenho de sua nova função.

17. REPORTE DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O Grupo **AGROLEND** emprega medidas de segurança para evitar a exposição indevida das Informações Protegidas, tanto internas quanto externas, as quais atendem as 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.

O Colaborador, caso tome conhecimento ou suspeite de qualquer acontecimento que viole as regras desta Política ou coloque em risco a segurança das informações da **AGROLEND**, deverá imediatamente comunicar o CSC da **AGROLEND**. A **AGROLEND**, por meio do CSC, 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, conforme o Plano de Resposta a Incidentes de Segurança da Informação da **AGROLEND**.

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.

18. SANÇÕES

O descumprimento das regras estabelecidas na presente Política sujeitará o Colaborador à aplicação de sanções que serão determinadas pela direção da **AGROLEND** de acordo com o grau de gravidade da conduta praticada, podendo variar entre: (i) advertência; (ii) suspensão; ou (iii) encerramento do contrato.

Os Colaboradores que cometerem infração às regras desta Política serão comunicados por escrito, através de comunicação contendo a regra violada, a conduta praticada pelo Colaborador e a sanção aplicada pela **AGROLEND**, sem prejuízo de eventual indenização paga pelo Colaborador a ser apurada judicialmente.

19. 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 (a exemplo, acordo de confidencialidade), 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 pelo Grupo **AGROLEND**, mediante a assinatura do Colaborador, física ou digital, ou por meio de mecanismo de consentimento digital.

20. DISPOSIÇÕES FINAIS

As exceções às regras estabelecidas por esta norma específica para atender alguma demanda específica devem ser apresentadas ao CSC para avaliação e aprovação.

Essa Política foi elaborada em 26 de fevereiro de 2021, aprovada em reunião de Diretoria realizada em 5 de outubro de 2021.[1] Poderá ser revista, atualizada e alterada anualmente ou a qualquer tempo, a exclusivo critério da **AGROLEND**, sempre que algum fato relevante ou evento motive sua revisão antecipada.

[1] Versão 1, elaborada em 26 de fevereiro de 2021, aprovada em Reunião de Diretoria realizada em 5 de outubro de 2021, após aprovação do Banco Central do Brasil publicada no Diário Oficial de 16 de setembro de 2021 e registro na Junta Comercial.