

NAUTILUS CONSULTORIA DE INVESTIMENTOS LTDA.

**POLÍTICA DE PROTEÇÃO DE DADOS, SEGURANÇA DA INFORMAÇÃO
E CIBERNÉTICA**

OUTUBRO / 2025

ÍNDICE

APRESENTAÇÃO	2
CONFIDENCIALIDADE E ACESSOS	3
AMEAÇAS CIBERNÉTICAS	3
TESTES DE SEGURANÇA E INTEGRIDADE.....	3
MONITORAMENTO	7
PLANO DE RESPOSTA	7
PROTEÇÃO DE DADOS PESSOAIS	8
VIGÊNCIA E ATUALIZAÇÃO	12
ANEXO I.....	13

APRESENTAÇÃO

A Política de Proteção de Dados, Segurança da Informação e Cibernética (“Política”) da Nautilus Consultoria de Investimentos Ltda. (“Nautilus Wealth” ou “Sociedade”), aplica-se a todos os sócios, colaboradores, prestadores de serviços relevantes e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Nautilus Wealth, ou que acesse informações a ela pertencentes (“Colaboradores”).

Além disso, todo e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática da Sociedade, estando sujeito à presente Política.

Em linha com as principais discussões e preocupações do mercado, esta Política tem como base princípios e procedimentos que asseguram a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados pela Sociedade. A efetividade desta Política depende da conscientização de todos os Colaboradores e dos terceiros contratados que tenham acesso a informações relevantes, bem como do esforço constante para que seja feito bom uso das Informações Confidenciais e dos ativos disponibilizados pela Sociedade ao Colaborador e aos terceiros que necessitem do acesso a tais informações.

A Sociedade deverá assegurar que seus profissionais e terceiros contratados assinem, de forma manual ou eletrônica, documento de confidencialidade sobre as informações confidenciais e privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais ou assegurar que o contrato de prestação de serviço do profissional ou do terceiro contratado contenha cláusula de confidencialidade.

Serão compreendidas como “Informações Confidenciais”:

- (a) *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador, relatórios e informações técnicas, analíticas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes;
- (b) Operações estruturadas, demais operações e seus respectivos valores analisadas em favor dos clientes da Sociedade; e
- (c) Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Nautilus Wealth e/ou de seus sócios e clientes.

CONFIDENCIALIDADE E ACESSOS

São princípios fundamentais da presente Política a proteção às Informações Confidenciais e o controle de acesso a tais informações. Nesse sentido, a Sociedade, independentemente de qualquer situação, deverá assegurar que apenas os Colaboradores que tenham necessidade de acesso às Informações Confidenciais assim tenham, evitando que outros Colaboradores e Terceiros que não necessitem do acesso, possam conhecer Informações Confidenciais.

Além disso, será assegurado pela Nautilus Wealth um controle do fluxo de tais Informações Confidenciais de forma a mitigar riscos de acesso de tais informações por Terceiros. Assim, a Sociedade, consoante será destrinchado nesta Política, é capaz de rastrear o fluxo de informações e manter a integridade das informações e de quem teve acesso a elas.

Ainda, em caso de disponibilização de Informações Confidenciais por plataformas em nuvem, tal compartilhamento deverá ser supervisionado pela Área de Compliance e PLD, quem deverá definir as pessoas com acesso à pasta compartilhada em nuvem e torná-la inacessível para as demais pessoas.

AMEAÇAS CIBERNÉTICAS

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, nível de informações ou característica dos ativos. As consequências para as instituições podem ser significativas em termos operacionais, de risco de imagem, danos financeiros ou perda de vantagem concorrencial, podendo tais danos serem irreparáveis.

Diante desse cenário, a Sociedade reconhece como métodos mais comuns de ataques cibernéticos os seguintes: (i) *Malware* (incluindo, vírus, cavalo de troia, *spyware* e *ransomware*, (ii) Engenharia Social (incluindo, *pharming*, *phishing*, *vishing*, *smishing* e acesso pessoal), (iii) Ataques de *DDos* (*distributed denial of services*) e *botnets* e (iv) Invasões (*advanced persistent threats*).

A Nautilus Wealth conta com sistemas anti-vírus em todos os ativos tecnológicos utilizados por seus profissionais, assim como possui auxílio externo de empresa de TI para auxiliar em demandas eventuais. Ainda, além de ataques cibernéticos, a Sociedade pode estar sujeita a mal funcionalidades dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar o perdimento e/ou adulteração de dados e Informações Confidenciais.

TESTES DE SEGURANÇA E INTEGRIDADE

Para manter a segurança e integridade dos sistemas a Nautilus Wealth adota rotinas que abrangerão testes de contingência que serão realizados na periodicidade necessária, de modo a permitir que a Sociedade esteja preparada para a continuação de suas atividades. Sendo estes os seguintes:

- a) Acesso aos sistemas e aos *e-mails* remotamente, dos *notebooks* e/ou computadores de contingência;
- b) Acesso aos dados armazenados;
- c) Testes para verificação de segurança, especialmente nos requisitos de acesso via VPN, níveis de autenticação e validação *back up*; e
- d) Outros testes necessários à continuidade das atividades.

(i) Disponibilização e uso

A Nautilus Wealth poderá disponibilizar computadores para seus Colaboradores para o desempenho das atividades profissionais na Sociedade e, nesta hipótese, o computador não poderá ser utilizado para quaisquer outros fins.

O uso dos computadores pelos Colaboradores da Nautilus Wealth respeita as seguintes regras:

- a) A cada novo Colaborador, o Diretor de Compliance e PLD autorizará, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos;
- b) Todos os equipamentos, *softwares* e permissões de acessos necessários para o Colaborador devem ser testados, homologados e autorizados pelo Diretor de Compliance e PLD;
- c) O Diretor de Compliance e PLD autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário;
- d) A identificação do usuário é feita através do *login* e senha, que através do registro de *logs* utilizado pela Nautilus Wealth é sua assinatura eletrônica no servidor da Sociedade; e
- e) Todos os eventos de *login* e alteração de senhas são auditáveis e rastreáveis.

(ii) Softwares

A implantação e configuração de *softwares* da Nautilus Wealth respeitam as seguintes regras:

- a) Todos os *softwares*, programas básicos (sistema operacional e ferramentas) e componentes físicos necessários para o desempenho de suas atividades são implantados e configurados sob supervisão do Diretor de Compliance e PLD;
- b) É vedado aos usuários alterar as configurações dos *softwares* disponibilizados direta ou indiretamente pela Sociedade sem a permissão formalizada do Diretor de Compliance e PLD; e
- c) É proibido ao usuário implantar ou alterar componentes físicos em seus computadores sem prévio conhecimento do Diretor de Compliance e PLD.

(iii) Registros

A Nautilus Wealth mantém por 5 (cinco) anos todos os *logs* de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores dos Colaboradores, arquivos em rede, sejam *softwares*, *hardwares* ou acessos que não sejam autorizados.

Nesse sentido, através dos *logs* realizados pela Sociedade, a Nautilus Wealth consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme Resolução CVM nº 19/2021.

(iv) Responsabilidades do usuário

O Colaborador é o custodiante dos recursos disponibilizados a ele, devendo este cuidar adequadamente do equipamento. O Colaborador também deve garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela Sociedade.

Ainda, o Colaborador deve adotar um comportamento seguro condizente com a Política, devendo:

- a) Não compartilhar nem divulgar sua senha com terceiros;
- b) Não transportar Informações Confidenciais da Sociedade em qualquer meio (CD, DVD, *pendrive*, papel, etc.) sem as devidas autorizações e proteções;
- c) Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);
- d) Não abrir mensagens de origem desconhecida, ou *links* suspeitos mesmo que advindos de origem conhecida;
- e) Armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contêm Informações Confidenciais, evitando utilizar redes públicas desconhecidas; e
- f) Seguir corretamente a política para uso de internet e correio eletrônico estabelecida pela Nautilus Wealth.

(v) Regras e responsabilidades do uso da Internet

O Colaborador é responsável por todo acesso realizado com a sua autenticação.

Quando o usuário se comunicar através de recursos de tecnologia ligados a Nautilus Wealth, este deve sempre resguardar a imagem da Sociedade, evitando entrar em sites de fontes não seguras, assim como abrir *e-mails* de fontes não conhecidas.

(vi) Uso de correio eletrônico particular

É proibido a utilização profissional de correio eletrônico particular para o desempenho das atividades da Sociedade. A Nautilus Wealth disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex.: @nautiluswealth.com.br).

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à Sociedade, devendo ser o mesmo durante todo o seu período de vínculo com a Nautilus. Se houver necessidade de troca de endereço, a alteração será realizada pela área responsável, mediante autorização e supervisão do Diretor de Compliance e PLD.

(vii) Endereço eletrônico de programas ou de comunicação corporativa

É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico. Nesse caso, é obrigatória a existência de um usuário da Área de Compliance e PLD responsável por acompanhar as mensagens emitidas e recebidas por esse endereço.

É permitida a existência de endereços de correio eletrônico para o envio de mensagens tipo comunicação interna da Nautilus Wealth, porém, é obrigatória a identificação do usuário que encaminhou a mensagem.

O endereço de correio eletrônico disponibilizado para os Colaboradores e as mensagens associadas a este correio eletrônico são de propriedade da Nautilus Wealth.

(viii) Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pela Sociedade mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via internet.

O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico da Sociedade.

(ix) Cópias de segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria a cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área responsável, mediante supervisão do Diretor de Compliance e PLD.

(x) Armazenamento em Nuvem (Cloud)

A Nautilus Wealth poderá realizar o armazenamento das Informações Confidenciais e quaisquer outros dados na Nuvem (Cloud).

De forma a possuir um ambiente seguro de nuvem, considerando aplicações *Web*, se prezará pela confiabilidade, disponibilidade e integridade do armazenamento da mesma.

(xi) Contratação de Terceiros para Serviços de Armazenamento na Nuvem

Fornecedores, prestadores de serviços e parceiros (“Terceiros”) podem representar uma fonte significativa de riscos para a Nautilus Wealth em relação à Cibersegurança. Neste sentido, é necessário adotar certos procedimentos que devem ser realizados previamente a contratação de Terceiros para serviços de Armazenamento na Nuvem.

Assim sendo, será dever da Sociedade verificar se o Terceiro segue políticas, programas e procedimentos formais relativos à segurança da informação e cibersegurança, priorizando, quando possível e viável, a contratação de prestadores de serviços renomados e consolidados em seu respectivo segmento de atuação.

Em caso de qualquer incidente constatado pelo Terceiro, este deverá de imediato enviar uma notificação relatando o ocorrido à Sociedade, a qual, dependendo da situação, poderá reavaliar e inclusive rescindir de imediato o contrato do Terceiro.

Outros serviços com utilização da tecnologia em Nuvem também devem ser considerados para fins das regras aqui presentes, tais quais, (i) *Software as a Service (SaaS)*, (ii) *Platform as a Service (PaaS)* e (iii) *Infrastructure as a Service (IaaS)*.

MONITORAMENTO

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados sob supervisão do Diretor de Compliance e PLD. Os Testes de Contingência serão realizados periodicamente, de modo a permitir que a Nautilus Wealth esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais.

Ademais, serão realizados Testes Periódicos de Segurança da Informação e Cibernética na Sociedade, com especial enfoque em segregação lógica-informacional, testes de penetração, eventos de vazamento de dados, rastreabilidade dos *logs* de acessos às informações sensíveis, tratamento de dados, dentre outros, sempre objetivando a preservação dos dados mantidos pela Nautilus Wealth, em especial os confidenciais.

PLANO DE RESPOSTA

Na hipótese de verificação de indícios, suspeita fundamentada, vazamento de Informações Confidenciais ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, a Sociedade deverá contratar profissional ou empresa especializada para verificar

a falha de segurança e a extensão dos danos causados à Sociedade, bem como dos dados pessoais acessados.

Sendo averiguado a existência de falha de segurança, a Nautilus Wealth deverá adotar todas as medidas necessárias para corrigir tal falha, seja diretamente ou por meio da contratação de terceiros, e reforçar a segurança de seus sistemas de informação, ao passo que deverá procurar mitigar os efeitos negativos oriundos de tal falha.

Todo e qualquer incidente ocorrido, assim como os resultados do plano de resposta a ser adotado pela Sociedade deverão ser devidamente classificados por nível de severidade, arquivados e documentados pela Área de Compliance e PLD.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Manual de Ética, Controles Internos e Compliance da Nautilus Wealth.

PROTEÇÃO DE DADOS PESSOAIS

Escopo e Abrangência:

A Sociedade está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis que forem coletados ou aos quais tiver acesso em função do uso do site ou por conta do desempenho de suas atividades, e com o cumprimento das leis e regulamentos em vigor.

Por esta razão, estabeleceu, as diretrizes, princípios e regras previstas nesta Política, as quais servirão de guia para a coleta, registro, processamento, armazenamento, uso, compartilhamento e eliminação de dados pessoais, fornecendo o arcabouço para o correto tratamento e proteção dos dados pessoais em seu poder.

Essas diretrizes, princípios e regras se aplicam a todos os Colaboradores da Nautilus Wealth, e englobam os dados pessoais que se encontrem armazenados em qualquer meio, e abrangem toda e qualquer forma de tratamento que possa ser empregada e esteja disponível para a Sociedade.

É importante observar que o escopo da proteção de dados pessoais no âmbito da Nautilus Wealth está, em grande parte, limitado aos dados pessoais de seus Colaboradores e de pessoas físicas e jurídicas com as quais tiver estabelecido relações jurídicas. Também estão abrangidos por esta proteção os dados de candidatos às vagas na Sociedade, de fornecedores e outros com os quais a Nautilus Wealth manteve contato para atender alguma demanda relevante e específica.

Vale ressaltar que todo o tratamento de dados pessoais feito pela Sociedade está pautado nos requisitos do artigo 7º da LGPD, assim como nas premissas do artigo 11 da mesma lei, quando

aplicável. Dessa maneira, o tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

- a) Quando o titular consentir, de forma específica e clara, para finalidades específicas;
- b) Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
 - i) Cumprimento de obrigação legal ou regulatória pelo controlador;
 - ii) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
 - iii) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
 - iv) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
 - v) Proteção da vida ou da incolumidade física do titular ou de terceiros;
 - vi) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
 - vii) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Princípios Norteadores:

A Sociedade compromete-se a obter dados pessoais de maneira justa e legal, e suas ações serão norteadas no princípio da boa-fé e nos princípios abaixo, os quais estão elencados no art. 6º da Lei 13.709/2018:

- a) Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- b) Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- c) Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- d) Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

- e) Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- f) Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- g) Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- h) Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- i) Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- j) Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Responsável pela Proteção de Dados Pessoais:

Em consonância com o artigo nº 42 da Lei nº 13.709/2018, a Nautilus Wealth salienta que o responsável por essa Política, bem como por todos os preceitos concernentes à Proteção de Dados Pessoais é o Diretor de Compliance e PLD da Sociedade.

Direitos:

Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18, da Lei 13.709/2018, o titular dos dados pessoais tem direito de solicitar à Nautilus Wealth, em relação aos seus dados, a qualquer momento e mediante requerimento expresso. Esses direitos estão exemplificados abaixo, todavia o seu exercício em face da Sociedade deve ser analisado em cada caso concreto.

- a) Confirmação de existência de tratamento;
- b) Acesso aos dados;
- c) Correção de dados incompletos, inexatos ou desatualizado;
- d) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- e) Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

- f) Eliminação dos dados pessoais tratados com o consentimento do titular, exceto em determinadas situações e respeitados os limites técnicos das atividades, conforme determinado na Lei;
- g) Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- h) Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e
- i) Revogação do consentimento, nos termos da Lei.

A Nautilus Wealth disponibiliza canal de comunicação específico para esse tema, através do endereço leonardo@nautiluswealth.com.br. O Diretor responsável pelo Tratamento de Dados Pessoais receberá quaisquer requisições, solicitações, comunicações e/ou manifestações dos titulares de dados pessoais para exercício dos direitos estipulados na LGPD.

O Encarregado pelo Tratamento de Dados Pessoais, também conhecido como *Data Protection Officer* (DPO), é o responsável por auxiliar os controladores de dados pessoais em relação ao cumprimento de suas obrigações legais referentes à privacidade. Dessa forma, o DPO atua como uma ponte entre a Sociedade, os titulares dos dados (pessoas físicas) e a Autoridade Nacional de Proteção de Dados (ANPD).

Período de Armazenamento dos Dados Pessoais:

Os dados pessoais serão armazenados pela Sociedade durante o período de tempo necessário para o atingimento dos objetivos para os quais foram coletados. Porém, este período poderá ser ampliado para o cumprimento de obrigação legal, regulatória ou contratual.

Cooperação com Autoridades:

A divulgação de dados pessoais para o cumprimento de lei, determinação judicial, regulatória ou de órgão competente ao qual a Nautilus Wealth estiver sujeita somente ocorrerá nos estritos termos e nos limites requeridos para o cumprimento da obrigação, sendo que os titulares dos dados, na medida do possível e desde que não configure infração, inadimplemento ou cause prejuízo à Sociedade, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a Nautilus Wealth cooperará com a Autoridade Nacional de Proteção de Dados (ANPD) em qualquer problema em relação à proteção de dados e dentro dos limites previstos na Lei e nas demais regulamentações sobre a matéria, porém sem renunciar a quaisquer defesas e/ou recursos disponíveis.

Governança:

As matérias relacionadas aos dados pessoais, dados confidenciais e aos tratamentos destes serão apresentados pelo Encarregado pelo Tratamento de Dados Pessoais para deliberação.

Obrigação de Reporte:

Os Colaboradores estão obrigados a comunicar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais sobre toda e qualquer suspeita ou indício de evento que possa ter comprometido os dados pessoais de posse da Sociedade para a devida apuração. Caso necessário, o Encarregado pelo Tratamento de Dados Pessoais notificará, em prazo compatível com a severidade do evento, a Autoridade Nacional de Proteção de Dados.

Registro de Eventos:

Os eventos reportados que tenham sido apurados e tiverem resultado no comprometimento de dados pessoais serão registrados nos termos dispostos na LGPD.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada anualmente e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

ANEXO I
TERMO DE ADESÃO À POLÍTICA DE
PROTEÇÃO DE DADOS, SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Nesta data, eu, _____, inscrito no CPF/MF sob o nº _____, declaro que li e estou plenamente de acordo com as disposições da Política de Proteção de Dados, Segurança da Informação e Cibernética da Nautilus Consultoria de Investimentos Ltda. Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

[Cidade], [Data]

[CLIENTE/COLABORADOR/TERCEIRO]