Grupo	***Código***
RECURSOS HUMANOS E INFRAESTRUTURA	C3
Assunto	
POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO	
Aprovação	***Data da aprovação***
DIRETORIA	10/04/2018
Responsabilidade	***Data de vigência***
DIRETORIA, TECNOLOGIA DA INFORMAÇÃO, RISCO, COMPLIANCE	10/04/2018

APRESENTAÇÃO

Esta política de confidencialidade e segurança da informação ("PSI") tem como objetivo definir políticas internas da Vórtx em relação aos procedimentos e fluxos operacionais relativos à preservação da confidencialidade e proteção de informações em posse da empresa. Ele se dirige a todos os Colaboradores, incluídos sócios, associados, funcionários e outras pessoas de interesse. Como procedimento padrão, o presente PSI deve ser entendido em conjunto com os outros manuais, incluindo as normas de proteção à integridade e risco da Vórtx.

O PSI reflete os processos correntes utilizados pela empresa no dia-a-dia. Visa a identificar os principais procedimentos, cumprindo requisitos regulatórios e estabelecendo pontos de checagem e monitoramento de risco.

ÍNDICE

I DEFINIÇÕES

1.1 Principais definições

- "ANBIMA": Associação Brasileira das Entidades do Mercado Financeiro e de Capitais.

- "BCB": Banco Central do Brasil.

- "CVM": Comissão de Valores Mobiliários.

- "Colaboradores": os colaboradores da Vórtx, incluindo fundadores, sócios, conselheiros, diretores, membros de comitês, associados, empregados, consultores, e estagiários.

- "CTO": Chief Technology Officer, o responsável pela área de tecnologia e desenvolvimento de sistemas da Vórtx

- "DC": Diretoria Colegiada, órgão formado por todos os diretores da Vórtx, cujas reuniões se regem de acordo com seu regimento interno.

- "DdC": Diretor de Compliance, o diretor estatutário responsável por cumprimento de normas e regulações.

- "DR": Diretor Responsável, o diretor responsável pelas normas de confidencialidade e segurança da informação.

- "Informação Confidencial":

  a. todos e quaisquer dados, informações e/ou documentos relacionados à Vórtx, seus negócios, investimentos e seus Parceiros, revelados aos Colaboradores em função das atividades desenvolvidas durante seu relacionamento com a Vórtx, seja verbalmente, por escrito ou por quaisquer outros meios, diretos ou indiretos, incluindo mas não se limitando a informações prestadas por ou a respeito à Vórtx, independentemente da designação expressa "Confidencial";

  b. toda e qualquer informação de caráter técnico, financeiro e/ou comercial, incluindo, mas não se limitando a informações sobre negócios ou transações relativos à Vórtx ou qualquer de suas divisões, preços, lista de clientes, planos de ação, estratégias e/ou informações de mercado, modelos de análise, práticas de mercado, orçamentos, previsões comerciais, demonstrativos financeiros, programas de computador, códigos fonte e objeto, know-how, slogans, expressões, ideias, material publicitário, fórmulas, segredos de negócio, produtos, patenteados ou não, processos produtivos, desenhos, projetos, plantas, contratos, e/ou quaisquer outros materiais correlatos transmitidos ao Colaborador ou obtidas por este durante seu relacionamento com a Vórtx; ou

  c. informações pessoais ou financeiras de investidores, incluindo dados cadastrais, comunicações, saldos, posições e qualquer outro tipo de informações relativas a investidores.

- "Manual de Compliance": manual de política de compliance da Vórtx, que faz parte deste

Manual de Escrituração.

- "Manual" ou "PSI": esta política de confidencialidade e segurança das informações.

- "Parceiros" significa todos e quaisquer parceiros comerciais da Vórtx, envolvidos ou não diretamente com seus negócios, incluindo mas não se limitando aos Colaboradores Vórtx, prestadores de serviços da Vórtx, e aos fundos de investimento administrados pela Vórtx, e as respectivas afiliadas, bancos, clientes e potenciais investidores, independentemente da designação expressa "Parceiros".

- "Política de Auditoria": manual de política de auditoria interna e externa (independente) da Vórtx.

1.2 Limitações

Não são consideradas Informações Confidenciais as informações:

a. que sejam ou venham a se tornar de conhecimento público sem violação desta PSI;

b. que sejam de conhecimento do Colaborador anteriormente ao seu relacionamento com a Vórtx, ou em virtude de sua divulgação pelo Vórtx em caráter expressamente não-confidencial;

c. recebidas pelo Colaborador de terceiro(s) que as divulgue(m) de forma não-confidencial; ou

d. desenvolvidas ou utilizadas pelos Colaboradores de maneira independente, sem a utilização das Informações Confidenciais.

Caberá sempre e somente ao Colaborador documentar e provar, caso necessário, a anterioridade de conhecimento, a recepção de terceiro, e o desenvolvimento ou utilização independente referidos acima nas alíneas b., c., e d.

II ASPECTOS GERAIS

2.1 Objeto

Informação é um bem valioso e juridicamente protegido, que constitui em diferencial no mercado. As informações geradas, adquiridas, processadas, armazenadas, transmitidas e descartadas são consideradas patrimônio da Vórtx e devem ser protegidas adequadamente.

Confidencialidade é um princípio fundamental. Aplica-se a quaisquer informações não-públicas referentes aos negócios da empresa, como também a informações recebidas de seus clientes, contrapartes ou fornecedores durante o processo natural de condução de negócios.

Esta política tem por escopo proteger as informações sigilosas, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas, conforme o §8 do Art. 4 da Instrução CVM nº 558/2015, e das normativas do BCB. Deste modo, nenhuma informação considerada sigilosa deve ser divulgada, dentro ou fora da empresa, a quem não

necessite de, ou não deva ter acesso a tais informações para desempenho de suas atividades profissionais.

2.2 Objetivos

A PSI tem como objetivo principal preservar a confidencialidade das informações da empresa para cumprir os deveres fiduciários inerentes a suas atividades e proteger ativos de informação.

A PSI da Vórtx visa a garantir:

• Integridade: Garantir que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

• Confidencialidade: Garantir que o acesso à informação seja obtido somente por pessoas autorizadas.

• Disponibilidade: Garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2.3 Abrangência e escopo específicos

Todos os Colaboradores estão sujeitos à PSI.

2.4 Auditoria interna

Os protocolos da PSI estão sujeitos à auditoria. Para maiores informações, favor observar o manual de auditoria da Vórtx ("Manual de Auditoria").

III GOVERNANÇA

3.1 Responsável

3.1.1 Nomeação

A Diretoria Colegiada ("DC") nomeou o Diretor de Compliance ("DdC") como responsável ("DR") pelo cumprimento das presentes normas. Sempre que agindo como DR, o referido diretor estará subordinado diretamente à DC, gozando de garantias e poderes indicados abaixo.

3.1.2 Atribuições

O DR é responsável pelas seguintes atribuições:
- estabelecer as normas, protocolos e procedimentos relativos à confidencialidade e segurança da informação;
- classificar informações e fluxos de informações como confidenciais, protegidas, privativas e públicas;
- controlar a disseminação de informações;
- realizar as atividades de treinamento e preparação de Colaboradores em relação à proteção da confidencialidade e seguraça da informação;
- divulgar as presentes normas, protocolos e processos; e

- aconselhar e solucionar dúvidas e questionamentos dos Colaboradores em relação a esta PSI.

3.1.3 Poderes especiais e garantias do DR

A DC deverá garantir que o DR tenha todos os poderes e autoridade necessários para cumprir sua missão institucional. O DR, na forma desta política, pode delegar a outros Colaboradores tarefas específicas.

3.2 Chief Technology Officer

3.2.1 Nomeação

A Diretoria Colegiada ("DC") nomeou o *Chief Technology Officer* ("CTO"), responsável por sistemas e desenvolvimento, como o responsável por checar, testar e implementar os protocolos e procedimentos para classificação, proteção e manutenção de informações confidenciais, e pela infraestrutura de segurança da informação.

3.2.2 Atribuições

O CTO é responsável pelas seguintes atribuições:
- desenhar procedimentos e protocolos de confidencialidade e segurança da informacão;
- manter a infraestrutura de proteção à confidencialidade e segurança de informação;
- configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI;
- testar periodicamente o funcionamento dos referidos procedimentos, protocolos e infraestrutura;
- apresentar ao DR, caso solicitado, relatórios e atualizações de procedimentos;
- identificar deficiências e promover, junto com o DR, ações seu saneamento;
- aconselhar a DC e o DR;
- aconselhar e solucionar dúvidas e questionamentos dos Colaboradores em relação aos procedimentos e controles internos; e
- organizar, junto com o DR, sessões de treinamento para os Colaboradores.

IV REGRAS FUNDAMENTAIS

4.1 Princípios básicos

Tratamento confidencial: Informações Confidenciais recebidas são tratadas e arquivadas de forma segura e íntegra, se necessário com métodos de criptografia. Estas apenas serão acessadas por pessoas autorizadas e capacitadas para seu uso adequado; as informações somente serão fornecidas a terceiros, mediante autorização prévia do cliente ou para o atendimento de exigência legal ou regulamentar;

Disponibilidade por necessidade: o uso de informações confidenciais será garantido apenas àqueles que tiverem acesso em vista de sua função ou que solicitarem sua divulgação por necessidade de trabalho, quando essa necessidade aparecer concretamente ("*as-needed*");

Integridade da informação**:** salvaguarda da exatidão e completeza da informação e dos métodos de processamento e arquivamento¸ protegendo as informações contra acesso, modificação, destruição ou divulgação não-autorizada.

Legalidade de uso a informação: garantia de que a informação está em conformidade com a legislação em vigor. Cumprindo as leis e as normas que regulamentam os aspectos de propriedade e assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades aprovadas pela empresa.

Usuário**:** a política aplica-se a qualquer usuário da informação, incluindo qualquer Colaborador, incluindo empregados, contratados, estagiários, prestadores de serviços, parceiros que utilizam as informações da empresa.

4.2 Diretrizes

4.2.1 Proteção da Informação

As medidas de proteção da informação devem considerar:
- os níveis adequados de integridade, confidencialidade e disponibilidade;
- a legislação, as decisões judiciais, as diretrizes e as instruções e procedimentos em vigor;
- o Manual de Compliance, em especial o Código de Ética
- a relação receita versus despesas;
- o alinhamento com as estratégias de cada área;
- as melhores práticas para a gestão da segurança da informação;
- os aspectos comportamentais e tecnológicos

4.2.2 Responsabilidade pela Segurança da Informação

As atividades de Segurança da Informação são exercidas por pessoas com sólidos conhecimentos em Segurança da Informação, inseridas na estrutura organizacional das áreas de Gestão de Riscos e Compliance.

Cada funcionário é responsável pela segurança da informação do grupo e deve cumprir as diretrizes, a declaração de princípios éticos e código de conduta e as instruções de procedimentos e restritos aplicáveis ás suas funções zelando pela correta aplicação das medidas de proteção.

4.2.3 Acesso á informação

O acesso e o uso de qualquer informação da empresa, pelo usuário, deve se restringir ao necessário para o desempenho de suas atividades profissionais no âmbito da Vórtx.

Para acessar informações nos sistemas da empresa deverão ser utilizadas somente ferramentas e tecnologias autorizadas pela empresa.

Senhas são pessoais e intransferíveis, não devem em hipótese alguma ser disponibilizadas a terceiros ou compartilhadas com outros Colaboradores.

As Informações Confidenciais poderão ser classificadas segundo seu grau de confidencialidade.

A segregação de acessos a Informações Confidenciais serão estruturadas a partir de grupos de

perfil de acesso.

4.3 Regras básicas

Dever de preservar. Os Colaboradores não devem transmitir nenhuma informação não-pública a terceiros. Todos os Colaboradores são responsáveis por preservar ativos de informação e devem estar comprometidos com a proteção adequada de informações e sistemas da empresa, considerando que a segurança da informação é um importante diferencial competitivo.

Autorização prévia. Toda e qualquer divulgação de informações estratégicas da empresa deve ser previamente autorizada.

Acesso privilegiado. Colaboradores da empresa deverão guardar sigilo sobre qualquer informação relevante à qual tenham acesso privilegiado, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Operações em andamento. Colaboradores devem preservar a confidencialidade de informações relativas a operações em andamento, bem como informações recebidas de entidades/pessoas cuja publicidade ou posição possa influenciar o mercado.

Divulgação acidental. Colaboradores devem evitar manter em suas mesas papéis e documentos confidenciais, e manter sigilo sobre senhas do computador, rede e sistemas. Funcionários, associados e sócios devem garantir que o acesso à área de trabalho seja feito somente por pessoal autorizado.

Propriedade da informação. Toda informação produzida ou recebida pelos Colaboradores como resultado da atividade profissional ou dentro da empresa pertence ou foi cedido à Vórtx. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Propriedade de equipamentos. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da empresa, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento da PSI.

Autorização para gravação e uso. Esta PSI dá ciência a cada Colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

Autorização para monitoramento de rede. O Colaborador está ciente de que a Vórtx pode e monitorará a rede interna para garantir a integridade dos dados e programas.

Autorização para monitoramento mensagens. O Colaborador está ciente de que a Vórtx pode e monitorará mensagens de e-mails ou qualquer outra forma de comunicação eletrônica a que o Colaborador tiver acesso na empresa para garantir a integridade das informações e mensagens repassadas.

Usos inadequados. Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer

recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

Dever de informar. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao CTO e ela, se julgar necessário, deverá encaminhar posteriormente à DC para análise.

4.4 Termo de confidencialidade

Todo Colaborador assina termo de confidencialidade de informações conforme o Anexo ao presente Manual.

V CYBER SEGURANÇA

5.1 Estrutura básica de TI

A Vórtx adotou integralmente a tecnologia “cloud computing”. A capacidade de processamento da empresa foi ampliada em mais de 200% com a transferência de todos os servidores físicos para a nuvem. A estrutura adotada inclui servidores escaláveis segregados em duas nuvens: uma nuvem pública (para serviços ao público) e uma nuvem, privada (para serviços legado internos). Além disso, manteve-se um servidor local para desenvolvimento.

5.2 Acesso da equipe de TI

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

5.3 Trilhas de auditoria

Os sistemas geram e mantêm trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

5.4 Logins e usuários

Cada usuário deverá ter uma única conta para acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física.

Nenhum usuário poderá usar a conta de outro.

5.5 Senhas

A configuração dos parâmetros de senha dos sistemas prevê:

Descrição	Configuração
Número mínimo de caracteres da senha	6 caracteres
Composição da senha	Contendo, no mínimo: 1 número; 1 letra minúscula; 1 letra maiúscula; e 1 caractere especial
Prazo máximo para a troca de senhas	30 dias
Mantém histórico de senha	6 últimas senhas
Bloqueio da conta	Após 3 tentativas inválidas de acesso
Desbloqueio da conta	Até o desbloqueio do administrador
Bloqueio automático das contas inativas	Após 60 dias sem uso

5.5 Gateway

Foi adquirido um gateway de APIs para aumentar a segurança contra ameaças externas, com certificações CommonCriteria, FIPS e PCI-DSS.

5.6 Acessos proibidos

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

5.7 Link dedicado

A empresa também adquiriu um link dedicado para acesso à internet de 100MB/s, e uma redundância de 50MB/s para contingências. A estrutura de switchers e hubs de última geração foi adquirida da CISCO. Além disso, foi adotado o sistema de telefonia Voice over IP (VoIP) com recursos de gravação e mensageria digitais.

5.8 Software não-autorizado

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela área de Tecnologia de Informação. Os Colaboradores com acesso à internet não poderão fazer o download (baixar) de programas, mesmo que ligados diretamente às suas atividades na Vórtx e deverão solicitar a área de Tecnologia da Informação a instalação e licenciamento desses programas, desde que autorizados pela diretoria.

5.9 Conteúdo proibido

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente à área de Tecnologia de Informação.

5.10 Vírus

Os Colaboradores não poderão utilizar os recursos da Vórtx para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

5.11 Revisão periódica

O processo de alteração e revogação de acesso a Sistemas de Informação é de responsabilidade do gestor do usuário, o qual deverá revisar periodicamente (bimestralmente), revalidando ou solicitando a revogação de acessos indevidos, sendo que para alterações ocorridas no quadro de colaboradores, seja por desligamento ou alteração de área/setor, a área administrativa comunica às áreas responsáveis pelo controle de acesso, para que adotem as ações pertinentes para revalidação ou revogação da concessão de acessos, caso necessário.
Assim como na concessão de acesso, nas alterações deverá ser informado se o acesso manterá o seu perfil atual ou se deverão ocorrer alterações no mesmo, garantindo a segregação de papéis.

5.12 Acesso por VPN

O acesso via computadores remotos pode ser realizado remotamente, por meio de autorização prévia, mediante conexão VPN (Virtual Private Network – Rede Privada Virtual) e processo de login neste ambiente remoto. Toda a segurança física e lógica é fornecida pelo contratado (fornecedor do serviço), além da sua construção e controle ambientais.

5.13 Emails

A Vórtx monitora as comunicações via email dos Colaboradores. O monitoramento é automatizado e os padrões de busca são decididos pela equipe de compliance em conjunto com o CTO.

VI BACKUP, GRAVAÇÕES E REDUNDÂNCIAS

6.1 Backup e recuperação

O sistema na nuvem da Vórtx grava diariamente imagem dos servidores, bases de dados e sistemas críticos. As imagens diárias são guardadas por 30 dias, quando então são descartadas.

Para recuperar arquivos danificados ou perdidos, um Colaborador poderá solicitar à equipe de TI, que realizará o processo de restore.

6.2 Gravacão

A Vórtx utiliza sistema de voz sobre IP (VoIP). As gravações são realizadas diretamente no sistema de gestão de telefones, e são executadas pela área de Tecnologia da Informação da Vórtx. O sistema está configurado para gravar as ligações originadas e recebidas pelas áreas da Vórtx automaticamente, registrando, além da própria conversa, a data, horário de início e de término de cada ligação.

Ramais-chave relacionados às atividades reguladas pela ANBIMA nos termos do Código de Serviços qualificados foram selecionados para gravação e manutenção por 5 anos. Além disso, outros terminais serão gravados para serem posteriormente auditados. Após um mês, as gravações de terminais comuns que não forem auditadas serão destruídas.

6.3 Redundância e disponibilidade

O provedor de serviços de nuvem da Vórtx garante um mínimo de disponibilidade de sistemas de 99.9%. Perdas de capacidade de processamento são compensadas pela própria fornecedora. Por essa razão, considera-se que a redundância é responsabilidade do provedor.

VII SEGREGAÇÃO DE OPERAÇÕES

A Vórtx mantem a devida segregação entre as suas diversas áreas e implementará controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

7.1 Segregação de atividades e funções

O primeiro nível de segregação refere-se às diferenças funcionais de atuação e autoridades definidas para as posições de Fund Trust, Corporate Trust, Custódia, Escrituração, Compliance/Risco, e Administrativo/Financeiro. Perfis de acesso físico e eletrônico, e o controle são realizados com base nessas divisões.

Apesar dessa segregação, para permitir que as atividades internas ocorram de modo eficiente, certas informações serão compartilhadas na base da necessidade ("*as-needed basis*"), sendo que os Colaboradores responsabilizam-se pelo sigilo das informações recebidas.

7.2 Segregação física

Existe segregação física das equipes das Áreas de Administração Fiduciária, Custódia e Escrituração. O controle de acesso é efetuado por meio de identificação funcional (biometria) que delimita o acesso ao local físico, pois cada área possui espaços fechado definidos onde é permitido apenas para as pessoas autorizadas. A definição de perfis de acesso e configuração é realizada pelo DdC, restringindo o acesso a cada área a que cada Colaborador tem perfil específico de permissões de acordo com sua função. É feito reset desses acessos e reconfiguração das permissões semestralmente.

O acesso de pessoas que não fazem parte do quadro de Colaboradores será restrito à recepção e às salas de reunião ou atendimento, exceto mediante prévio conhecimento e autorização da administração, e desde que acompanhadas de Colaboradores. Em caso de antigos colaboradores, não será permitida a sua permanência nas dependências da empresa, com exceção dos casos em que tenha sido chamado pela área de recursos humanos para conclusão do processo de desligamento, de aposentadoria ou outros. O atendimento a clientes nas dependências da empresa devem ocorrer, obrigatoriamente, nas salas destinadas para reuniões e visitas.

7.3 Segregação eletrônica

7.3.1 Acesso a sistemas

Cada Colaborador possui acesso a rede com senha com troca obrigatória definido pela Intranet limitados a sua área de atuação.

7.3.2 Controle de Acesso de Diretórios

O controle de Acesso aos diretórios é configurado por grupos de segurança do *Active Directory*:

A revisão e manutenção aos acessos aos sistemas e diretórios são efetuados anualmente pela empresa terceirizada (Intranet).

VIII ASPECTOS FINAIS

8.1 Treinamento

A área de Compliance, em conjunto com a área de tecnologia da informação, promoverá, a cada 12 (doze) meses, treinamentos adequados para capacitação de todos os Colaboradores com relação aos procedimentos previstos neste PCN e na legislação ou regulamentação aplicáveis, sendo tal treinamento obrigatório a todos os Colaboradores.

Quando do ingresso de um novo Colaborador, o departamento de serviços qualificados aplicará o devido treinamento de forma individual para o novo Colaborador.

O treinamento acima descrito será realizado conjuntamente com o treinamento contínuo, descrito na política de treinamento contínuo da empresa.

8.2 Dúvidas e aconselhamento

Em caso de dúvidas ou necessidade de aconselhamento, o Colaborador deve buscar auxílio junto ao DR ou CTO. Tais dúvidas poderão ser enviadas por escrito a compliance@vortx.com.br

8.3 Formulário de ocorrências operacionais

A Vórtx mantêm um formulário de ocorrências operacionais no link https://forms.office.com/Pages/ResponsePage.aspx?id=9r2BMzu7xk2ZUoupkGwd1JXL7ej4coBMigEDaxKlKFFUQzVFV0ZTWFZZTFNJMU1DRlc1TDNHTE5aTy4u.

Este formulário deve ser utilizado para registrar toda e qualquer ocorrência, seja ela positiva (que gere ganhos financeiros ou de horas de trabalho) ou negativa (que gere perdas financeiras ou de horas de trabalho). Os Colaboradores são incentivados a preencher o formulário para gerar dados e informações.

8.4 Atualizações periódicas

Esta PCI é revisto periodicamente. Ao menos anualmente, no bojo do processo de revisão anual de compliance, as obrigações e processos aqui descritos deverão ser revistos.

ANEXO – TERMO DE CONFIDENCIALIDADE

Através deste instrumento, _____, inscrito no CPF sob o no _____, doravante denominado Colaborador, e Vórtx Distribuidora de Títulos e Valores Mobiliários Ltda. ("Vórtx"), inscrita no CNPJ/MF sob o nº. [completar], resolvem, para fim de preservação de informações pessoais e profissionais dos clientes e da Vórtx, celebrar o presente termo de confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais ("Informações Confidenciais"), para os fins deste Termo:

a) Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, podendo incluir: know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela Vórtx, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela Vórtx, 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 Vórtx e a seus sócios ou clientes, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos.

b) Informações acessadas pelo Colaborador em virtude do desempenho de suas atividades na Vórtx, bem como informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da Vórtx ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

2. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Vórtx, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, colaboradores não autorizados, mídia, ou pessoas estranhas à Vórtx, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1 O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Vórtx, se comprometendo, ainda a não utilizar, praticar ou divulgar informações privilegiadas, *insider trading*, Divulgação Privilegiada e front running, seja atuando em benefício próprio, da Vórtx ou de terceiros.

2.2 A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.

3 O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis e sem remédio jurídico para a Vórtx e terceiros, ficando deste já o Colaborador obrigado a indenizar a Vórtx, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1 O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho, ou desligamento ou exclusão por justa causa, conforme a função do Colaborador à época do fato, obrigando-lhe a indenizar a Vórtx e/ou terceiros pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, independente da adoção das medidas legais cabíveis.

3.2 O Colaborador expressamente autoriza a Vórtx a deduzir de seus rendimentos, sejam eles remuneração, participação nos lucros ou dividendos, observados, caso aplicáveis, eventuais limites máximos mensais previstos na legislação em vigor, quaisquer quantias necessárias para indenizar danos por ele dolosamente causados, no ato da não observância da confidencialidade das Informações Confidenciais, nos termos do parágrafo primeiro do artigo 462 da Consolidação das Leis do Trabalho, sem prejuízos do direito do Vórtx de exigir do Colaborador o restante da indenização, porventura não coberta pela dedução ora autorizada.

3.3 A obrigação de indenização pelo Colaborador em caso de revelação de Informações Confidenciais subsistirá pelo prazo durante o qual o Colaborador for obrigado a manter as Informações Confidenciais, mencionados nos itens 2 e 2.1 acima.

3.4 O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Colaborador reconhece e toma ciência que:

a) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Vórtx são e permanecerão sendo propriedade exclusiva da Vórtx e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Vórtx, devendo todos os documentos permanecer em poder e sob a custódia da Vórtx, salvo se em virtude de interesses da Vórtx for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Vórtx;

b) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Vórtx todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

c) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos (“Informação Protegida”), são de propriedade exclusiva da Vórtx, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

d) Nos termos da Lei 9.279/95, é proibida a divulgação, exploração ou utilização sem autorização, de Informação Protegida a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

5. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Vórtx, permitindo que a Vórtx procure a medida judicial cabível para atender ou evitar a revelação.

5.1 Caso a Vórtx não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela a que o Colaborador esteja obrigado a divulgar.

5.2 A obrigação de notificar a Vórtx subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Este Termo é parte integrante das regras que regem a relação de trabalho e/ou societária do Colaborador com a Vórtx, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

6.1 A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da Vórtx.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

[Cidade], [data]

_____

[COLABORADOR]