FCL CAPITAL

POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES E SEGURANÇA CIBERNÉTICA

Agosto de 2022

ÍNDICE

Introdução

A presente Política de Segurança das Informações ("Política") reflete o compromisso da FCL Capital Gestão de Recursos de Terceiros Ltda. ("FCL" ou "Gestora") com a proteção de informações sigilosas provenientes do exercício da atividade de administração de carteiras e valores mobiliários, visando evitar os danos e prejuízos que seu mau uso pode causar para a FCL, seus clientes, funcionários e fundos de investimentos geridos pela Gestora.

A presente Política tem como objetivo estabelecer as diretrizes a serem seguidas em relação à adoção de procedimentos e mecanismos relativos à segurança de informações sigilosas, a testes periódicos de segurança para os sistemas de informações e ao treinamento daqueles que tenham acesso a informações confidenciais ou participem de processo de decisão de investimento. Com isso, os riscos de ocorrência de danos e prejuízos capazes de comprometer os objetivos e os interesses da Gestora e de seus clientes são minimizados.

A aplicação da presente Política se estende a todos os sócios, funcionários, estagiários, integrantes de cargos de administração da FCL e terceiros contratados que tenham acesso a informações confidenciais ("Colaboradores").

Aplicabilidade e Responsabilidades

O rigoroso cumprimento desta Política deve ser prioridade constante de todos os Colaboradores da FCL que utilizam os recursos tecnológicos disponibilizados pela Gestora.

Nesse sentido, todos os Colaboradores deverão:

a) proteger as informações sigilosas contra acesso, modificação, destruição ou divulgação não autorizados pela Gestora;

b) assegurar que os recursos de tecnologia à sua disposição sejam utilizados apenas ara as finalidades aprovadas ou não proibidas expressamente pela FCL;

c) cumprir fielmente as leis e normas aplicáveis aos aspectos relativos a direito autoral e propriedade intelectual das informações sigilosas;

d) assinar, de forma manual ou eletrônica, documento de confidencialidade sobre as informações reservadas ou privilegiadas às quais tenham acesso em virtude do exercício de suas atividades profissionais, excetuadas as hipóteses permitidas em lei;

e) comunicar imediatamente o Diretor de Compliance e Gestão de Riscos sobre qualquer descumprimento ou violação à presente Política; e

f) buscar orientação de seu superior hierárquico imediato em caso de dúvidas quanto à segurança das informações sigilosas.

Os terceiros contratados que tiverem acesso às informações reservadas ou privilegiadas que lhes tenham sido confiadas no âmbito de suas atividades deverão assinar documento de confidencialidade, cabendo ao Diretor de Compliance e Gestão de Riscos garantir o cumprimento do disposto neste item.

Princípios Gerais

A fim de garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações sigilosas provenientes do exercício das atividades da FCL, sua guarda e segurança, os seguintes princípios serão sempre observados pela Gestora e seus Colaboradores:

a) o acesso a informações sigilosas será concedido somente a pessoas devidamente autorizadas pela FCL;

b) as informações sigilosas manterão sua integridade e serão protegidas contra adulterações, sendo certo que alterações, supressões e adições a tais informações somente poderão ser realizadas se autorizadas pela FCL; e

c) as informações sigilosas serão disponibilizadas aos Colaboradores autorizados sempre que necessário ao bom exercício de suas atividades.

Nenhuma informação sigilosa deverá ser divulgada a qualquer pessoa que não necessite ou não deva ter acesso a tais informações para o exercício de suas atividades profissionais, seja dentro ou fora da FCL.

Qualquer informação sobre a FCL, suas atividades, seus sócios, clientes ou fundos de investimento e carteiras por ela geridas, sigilosa ou não, obtida em decorrência do exercício das atividades dos Colaboradores, somente poderá ser revelada ou fornecida ao público, à mídia ou a terceiros se em conformidade com as regras previstas nos documentos internos da Gestora.

Na ausência de previsão específica para o tratamento das informações acima referidas, a sua revelação ou o seu fornecimento somente poderão ocorrer mediante prévia autorização do Diretor de Compliance e Gestão de Riscos da FCL.

Medidas de Prevenção e Proteção

Para a devida proteção das informações sigilosas, além de adotar condutas pró-ativas e engajadas no que diz respeito à proteção das informações, os seguintes procedimentos devem ser observados por todos os Colaboradores no exercício de suas atividades:

a) os Colaboradores devem conhecer e evitar as ameaças externas capazes de afetar a segurança das informações sigilosas, como, por exemplo, vírus de computador, interceptação de mensagens eletrônicas e grampos telefônicos, além de fraudes e tentativas de roubo de senhas de acesso a sistemas de tecnologia da informação e a servidores;

b) todo e qualquer acesso a dados e informações da FCL que não for expressamente autorizado é vedado;

c) assuntos relativos ao desempenho de atividades e funções na FCL somente podem ser discutidos no espaço interno da Gestora ou em ambientes reservados que garantam a segurança das informações tratadas, e não em ambientes públicos ou em áreas expostas;

d) as senhas conferidas aos Colaboradores para o exercício de suas atribuições na FCL são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive a outros Colaboradores) nem anotadas em papéis ou em sistemas visíveis ou de acesso desprotegido;

e) os Colaboradores devem bloquear seus computadores sempre que se ausentarem de suas estações de trabalho;

f) somente softwares e equipamentos homologados e previamente aprovados pela FCL podem ser instalados e utilizados nas estações de trabalho, o que deve ser feito com exclusividade por pessoas indicadas pelo Diretor de Compliance e Gestão de Riscos;

g) a utilização de equipamentos pessoais nas instalações da FCL e a sua conexão à rede interna e à internet, bem como a conexão de dispositivos móveis de armazenamento, requer autorização prévia e expressa do Diretor de Compliance e Gestão de Riscos;

h) os Colaboradores não devem abrir e/ou executar, em seus computadores, arquivos eletrônicos de origem desconhecida;

i) a utilização do endereço de e-mail corporativo deve ser direcionada exclusivamente aos negócios conduzidos pela FCL, sendo permitido o uso residual de tal endereço para assuntos particulares, desde que de forma não abusiva;

j) não é permitido o envio de mensagens e arquivos que possam constranger terceiros, que tenham conteúdo político ou que possam colocar a Gestora em risco;

l) toda e qualquer mensagem eletrônica e seus anexos são para uso exclusivo do seu remetente e destinatário, não podendo ser parcial ou totalmente divulgadas, utilizadas ou reproduzidas sem o consentimento prévio do remetente ou do autor, dependendo do caso;

m) o uso da internet deve ser estritamente relacionado às atividades exercidas pela FCL; e

n) documentos impressos e arquivos contendo informações sigilosas devem ser adequadamente armazenados e protegidos.

Monitoramento e Testes

A FCL realizará testes periódicos de segurança para os sistemas de informações, em especial aqueles mantidos em meio eletrônico, e implantará programa de treinamento para seus Colaboradores de modo a mantê-los sempre cientes e em linha com as regras desta Política.

A revelação de informações sigilosas a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas deverá ser prévia e tempestivamente comunicada ao Diretor de Compliance e Gestão de Riscos, que decidirá sobre a forma mais adequada para a referida revelação.

Controle de Fluxo das Informações Sigilosas

A Gestora, por meio de equipe definida pelo Diretor de Compliance e Gestão de Riscos e/ou por meio de prestador de serviço externo, monitora continuamente o uso das informações sigilosas, dos recursos de tecnologia, dos sistemas e dos dados por ela disponibilizados e poderá usar os registros advindos desse monitoramento para atestar a observância e a adequação das regras presentes nesta Política.

Adicionalmente, todo acesso a informações sigilosas, aos ambientes estratégicos e à sede da FCL é controlado para permitir acesso apenas às pessoas expressamente autorizadas pelo Diretor de Compliance e Gestão de Riscos. O controle de acesso é documentado e formalizado e contempla as seguintes metodologias:

a) necessidade de pedido formal para concessão e cancelamento de autorização de acesso do usuário aos sistemas;

b) utilização de identificador para cada Colaborador, de forma a assegurar a individualização da responsabilidade de cada um por suas ações e omissões;

c) verificação da adequação do nível de acesso concedido ao perfil do Colaborador;

d) remoção imediata de autorizações concedidas aos Colaboradores afastados ou desligados da FCL;

e) adaptação das autorizações concedidas aos Colaboradores que tenham mudado de função internamente na FCL, se for o caso; e

f) revisão periódica das autorizações concedidas.

Os ramais telefônicos utilizados pelos Colaboradores que exercerem funções comerciais e de gestão de carteiras de títulos e valores mobiliários terão suas ligações gravadas, sendo o respectivo conteúdo armazenado em arquivos nos servidores da Gestora. O Diretor de Compliance e Gestão de Riscos possui livre acesso às gravações.

Ao término de cada verificação, a Diretoria de Compliance e Gestão de Riscos indicará e documentará, por escrito, o arquivo acessado, a data de acesso e a eventual identificação de indícios que possam indicar eventual infração a esta Política ou a outras regras aplicáveis à Gestora.

Todas as ordens de compra e venda da FCL se dão (i) por meios eletrônicos, via Terminal Bloomberg, direto à mesa de operações; ou (ii) via ordem no terminal do Saxo Bank, a corretora utilizada pela FCL para ordens internacionais. Ambos os métodos geram arquivos com histórico de ordens e minimizam possíveis erros.

Todas as informações vitais da FCL Capital, como e-mails, ordens, teses e planos estratégicos ficam armazenados em servidores na nuvem, no provedor Google Enterprise e Dropbox (no caso de mensagens, documentos e arquivos) e na Bloomberg LP (no caso de ordens de compra e venda de ativos).

Os arquivos em nuvem são verificados e alterados diariamente. Arquivos mais antigos são acessados com bastante frequência, graças à computação em nuvem.

A utilização de telefones celulares e a comunicação por mensagens instantâneas de texto e voz pela internet nas instalações internas da FCL durante o expediente devem ser evitadas pelos Colaboradores.

Segregação de Atividades

O Diretor de Compliance e Gestão de Riscos não pode e não será responsável, direta ou indiretamente, por nenhuma atividade relacionada à gestão de fundos de investimento e de carteiras de títulos e valores mobiliários.

Caso a FCL tenha interesse de desenvolver qualquer outra atividade além da gestão de fundos de investimento e carteiras de títulos e valores mobiliários, tal atividade será devidamente segregada das atividades atualmente exercidas pela Gestora, com preservação das informações confidenciais e a identificação das pessoas que tenham acesso à área, inclusive por meio de controles de acesso digitais, em atenção às normas previstas pela Instrução CVM nº 558, de 26 de março de 2015.

Política de Segurança Cibernética

As regras de Segurança Cibernética aqui previstas tem como objetivo assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela FCL, bem como estabelecer as metodologias e os procedimentos utilizados pela FCL na identificação, na proteção, no monitoramento e no controle de riscos cibernéticos.

As diretrizes aqui estabelecidas deverão ser seguidas pelos Colaboradores, independentemente do nível hierárquico ou função desempenhada, e pelos prestadores de serviço contratados pela FCL. Os ambientes, sistemas, computadores e redes da Gestora poderão ser monitorados e gravados, devendo ser utilizados para a realização de suas atividades profissionais. O uso pessoal desses recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

Para melhor atender aos interesses dos clientes da FCL, os riscos cibernéticos são monitorados e controlados por meio de procedimentos avançados de criptografia e backup diário de dados, arquivos e sistemas, implementados pela Gestora e por terceiro contratado, que atuará no direcionamento tecnológico quanto à infraestrutura de TI da FCL, para a instalação, configuração e implementação dos recursos computacionais e tecnológicos necessários ao exercício das atividades (servidores, racks, switches, wireless, firewall, equipamentos de videoconferência, telefones, nobreaks, desktops e impressoras), de acordo com planejamento já realizado em conjunto com a FCL.

Os Colaboradores possuem à sua disposição, além dos recursos computacionais acima descritos, sistemas internos para o uso de internet, e-mail e telefonia, bem como sistemas externos, necessários ao desempenho de diversas atividades da FCL, como a negociação e cotação de ativos, o acesso a notícias e o desenvolvimento de bancos de dados ("Processos e Ativos Relevantes"). Os Processos e Ativos Relevantes estão sujeitos a ataques cibernéticos, que poderão ser realizados por meio de softwares desenvolvidos para corromper computadores e redes internas e

outros métodos de manipulação eletrônica cujos objetivos são a obtenção de informações confidenciais e a identificação de fragilidades tecnológicas dos sistemas implementados pela FCL.

A FCL, por meio de terceiro contratado, supervisionado pela Diretor de Compliance e Gestão de Risco, deverá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas. Referidos arquivos poderão ser acessados pelo Diretor de Compliance e Gestão de Risco 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.

As senhas de acesso a dispositivos corporativos, sistemas e rede da FCL serão atualizadas trimestralmente e os Colaboradores contarão com um gerenciador de senhas, que limitará o acesso dos Colaboradores aos recursos relevantes para o desempenho de suas atividades específicas. Além disso, eventos de login, alteração de senhas, criptografia e backup de dados serão auditáveis, rastreáveis e monitorados diariamente, por meio das estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. Os Colaboradores que não possuem perfil de administrador ou acesso privilegiado deverão ter senhas deverão ter tamanhos variáveis, possuindo no mínimo 8 caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempreque possível. Os Colaboradores que, por sua vez, possuírem perfil de administradorou acesso privilegiado deverão utilizar uma senha de no mínimo 9 (nove) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúscula e minúsculo) obrigatoriamente.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos não criptografados, não devem ser constituídas de combinações óbvias de teclado e não devem ser baseadas em informações pessoais do Colaborador. Após 3 tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o Diretor de Compliance e Gestão de Riscos.

Todo e qualquer dispositivo de identificação pessoal, como senhas, logins, crachás, certificados e assinaturas digitais ou dados biométricos não poderão ser compartilhados por mais de um Colaborador em nenhuma hipótese.

Os sistemas e computadores devem ter versões de software antivírus devidamente instaladas, ativadas e atualizadas permanentemente. Eventos de suspeita de vírus, demissão de Colaboradores, perdas de senha ou de acessos indevidos aos logins/senhas deverão ser informados imediatamente ao Diretor de Compliance e Gestão de Riscos.

A FCL poderá, nos casos de exigência judicial ou por solicitação do Diretor de Compliance e Gestão de Riscos, tornar públicas as informações obtidas pelos sistemas de monitoramento.

A FCL exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos Processos e Ativos Relevantes, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

A verificação, mensuração, monitoramento de riscos cibernéticos relevantes e inspeção física nas máquinas da FCL serão realizados pelo Diretor de Compliance e Gestão de Riscos e equipe a ser por ele indicada, que também deverá revisar a Política de Segurança Cibernética periodicamente (anualmente) e sempre que algum fato relevante ou evento motive sua revisão antecipada.

A Gestora possui um plano de resposta a incidentes, considerando os cenários de ameaças previstos durante a avaliação de riscos, que permitirá a continuidade dos negócios ou a recuperação adequada das informações em casos mais graves. O plano inclui:

a) os arquivos relativos às atividades da Gestora são armazenados também em servidores virtuais na internet, com criptografia avançada e backup diário de dados;

b) a Gestora contratou terceiro especializado para implementar, supervisionar e acompanhar continuamente os serviços de internet, e-mail, telefonia e demais recursos computacionais e tecnológicos utilizados nas atividades da FCL;

c) manutenção dos sistemas em funcionamento, apesar da falta de energia temporária, por meio de equipamentos de no break instalados para suprir o fornecimento de energia nos equipamentos principais para a manutenção das comunicações e atividades mínimas da FCL; a FCL conta também com CPD interno e prédio comercial com gerador próprio.

d) manutenção de local alternativo em endereço externo e distante de sua sede e instalações físicas, com infraestrutura necessária e suficiente para a continuidade de suas atividades chaves, de modo a evitar a interrupção das atividades e eventuais contingências;

e) a Gestora terá servidores adequados e provedores dedicados como medidas de proteção;

f) todos os aplicativos e sistemas essenciais à Gestora poderão ser acessados de lugares remoto em que haja acesso à internet por meio de VPN (Virtual Private Network);

Para que se aprimore a infraestrutura da FCL e a continuação de suas atividades, testes de contingência serão realizados com periodicidade mínima, compreendendo pelo menos os seguintes eventos:

a) testes dos no-breaks, verificando o status de funcionamento e do tempo de suporte das baterias com carga;

b) acesso aos sistemas e aos e-mails remotamente, do endereço externo;

c) acesso aos dados armazenados externamente; e

d) outros necessários à continuidade das atividades da FCL, relativos ao plano de resposta descrito no item anterior.

Incluem-se, ainda, entre as obrigações do Diretor de Compliance e Gestão de Riscos:

a) administrar, proteger e promover testes das cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a FCL;

b) implantar controles que gerem registros auditáveis para a retirada e transporte de mídias das informações;

c) garantir que as informações de um usuário não sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário;

d) planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;

e) definir as regras formais para instalação de software e hardware no ambiente de produção corporativo, exigindo o seu cumprimento dentro da FCL;

f) realizar auditorias periódicas de configurações técnicas e análise de riscos;

g) responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais;

h) garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da FCL;

i) monitorar o ambiente de TI, gerando indicadores e históricos de: (i) uso da capacidade instalada da rede e dos equipamentos; (ii) tempo de resposta no acesso à internet e aos sistemas críticos da FCL; (iii) períodos de indisponibilidade no acesso à internet e aos sistemas críticos da FCL; (iv) incidentes de segurança (vírus, trojans, furtos, acessos indevidos e outros); (v) atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros); e

j) promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da FCL, mediante campanhas, palestras, treinamentos e outros meios.

É vedado ao Colaborador e ao prestador de serviços contratado pela FCL utilizar os serviços de correio eletrônico e internet providenciados pela Gestora no âmbito das seguintes atividades:

a) enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da FCL;

b) enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

c) enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a FCL vulnerável a ações civis ou criminais;

d) 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 quando a FCL estiver sujeita a algum tipo de investigação;

f) produzir, transmitir ou divulgar mensagem que: (i) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da FCL; (ii) contenha ameaças eletrônicas, como spam, mail bombing, vírus de computador, etc.; (iii) contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança; (iv) vise obter acesso não autorizado a outro computador, servidor ou rede; (v) vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado; (vi) vise burlar qualquer sistema de segurança; (vii) vise vigiar secretamente ou assediar outro usuário; (viii) vise acessar informações confidenciais sem explícita autorização do proprietário; (ix) vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa; (x) inclua imagens criptografadas ou de qualquer forma mascaradas; (xi) contenha anexo(s) superior(es) a 15 MB para envio (internet e internet) e 15 MB para recebimento (internet); (xii) tenha conteúdo considerado impróprio, discriminatório, obsceno, ofensivo ou ilegal; (xiii) seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, entre outros; (xiv) contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas; (xv) tenha fins políticos locais ou do país (propaganda política); e (xvi) inclua material protegido por direitos autoriais sem a permissão do detentor dos direitos. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato: nome do Integrante, departamento, nome da empresa, telefone(s) e correio eletrônico;

g) divulgar ou compartilhar indevidamente informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha a surgir na internet; e

h) usar, instalar, copiar ou distribuir softwares sem autorização que tenham direitos autorais, marca registrada ou patente na internet.

Todo incidente que afete a segurança da informação deverá ser comunicado imediatamente ao Diretor de Compliance e Gestão de Risco.

Caberá ao Diretor de Compliance e Gestão de Riscos da FCL tratar e responder questões de segurança cibernética, bem como promover e disseminar a política interna de segurança cibernética, tendo em vista a conscientização dos Colaboradores acerca dos riscos, das práticas de segurança e de treinamentos de uso adequado da estrutura tecnológica da FCL.

Terceiros Contratados

A área de tecnologia da informação é composta pelos seguintes provedores de serviços de notícias, análises macroeconômicas e armazenamento de dados:

(i) Google Enterprises (armazenamento de dados em nuvem);
(ii) Dropbox (armazenamento de dados em nuvem);
(iii) GoDaddy (registro de domínio e servidor de e-mail);
(iv) Wix.com (serviço de *host* do *website* da Gestora);
(v) Bloomberg LP (terminal financeiro); e
(vi) RGE Monitor (consultoria macroeconômica especializada).

Disposições Gerais

Quaisquer dúvidas dela decorrentes poderão ser submetidas ao Diretor de Compliance e Gestão de Riscos da FCL.

Vigência e Atualização

Esta Política, incluindo as regras relativas à segurança cibernética, será revisada anualmente (no mês de fevereiro de cada ano) e sempre que necessário, devendo ser alterada a qualquer tempo caso seu conteúdo deva ser atualizado ou em razão de circunstâncias especiais.

Anexo 1

Termo de Confidencialidade

Por meio deste instrumento ("Termo"), [nome e qualificação] ("Colaborador"), compromete-se a utilizar as Informações Confidenciais, conforme abaixo definido, estrita e exclusivamente para o desempenho de suas atividades na FCL Capital Gestão de Recursos de Terceiros Ltda. ("FCL Capital") e a não divulgar a terceiros (incluindo cônjuges, parentes, pessoas de relacionamento próximo, mídia) tais Informações Confidenciais para quaisquer fins.

São consideradas Informações Confidenciais para os fins deste Termo quaisquer informações sobre as atividades da FCL Capital, seus sócios, cliente e colaboradores, incluindo:

(i) know-how, técnicas, cópias, modelos, amostras, programas de computador;
(ii) informações técnicas, financeiras ou relacionadas a estratégias de investimento e desinvestimento ou comerciais, incluindo extratos e posições de clientes;
(iii) operações analisadas pelos fundos de investimento e carteiras geridos pela FCL;
(iv) relatórios, estudos, opiniões sobre ativos financeiros;
(v) troca de correspondências internas;
(vi) relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
(vii) informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da FCL, seus sócios, clientes, colaboradores ou projetos e negócios investidos;
(viii) informações a respeito de resultados financeiros, salvo se publicadas pela FCL; e
(ix) outras informações obtidas junto a sócios, diretores, funcionários, estagiários da FCL ou, ainda, junto a seus consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

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 período em que trabalhou para a FCL.

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.

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

O descumprimento do previsto neste Termo ensejará, inclusive, motivo de justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos da legislação trabalhista aplicável.

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

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 FCL são e permanecerão sendo propriedade exclusiva da FCL, 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 FCL,

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

c) A base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da FCL, 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 em lei.

Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a FCL, permitindo que a FCL procure a medida judicial cabível para atender ou evitar a revelação.

Caso a FCL 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 à parcela que o Colaborador esteja obrigado a divulgar.

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

Rio de Janeiro, [data]

_____

[Colaborador]