QUARTER

POLÍTICA DE CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

QUARTER INVESTIMENTOS ASSET MANAGEMENT LTDA.

Porto Alegre, 15 de setembro de 2021.

Capítulo I – Política de Confidencialidade e Segurança da Informação e Segurança Cibernética

1.1. A presente Política de Confidencialidade e Segurança da Informação e Segurança Cibernética (“Política de Confidencialidade e Segurança”) tem como objetivo estabelecer princípios e diretrizes de proteção das informações no âmbito da QUARTER INVESTIMENTOS, aplicando-se a todos os seus Integrantes.

1.2. Os Integrantes devem atender às diretrizes e procedimentos estabelecidos nesta Política de Confidencialidade e Segurança, informando quaisquer irregularidades ao Diretor de Compliance, a quem caberá avaliá-las e submetê- las ao Comitê de Compliance, Controles Internos e Ética, o qual decidirá sobre eventuais medidas cabíveis.

1.2.1. O Diretor de Compliance deve garantir o atendimento a esta Política de Confidencialidade e Segurança, sendo o responsável por temas de segurança da informação e cibernética.

1.3. Esta Política de Confidencialidade e Segurança deverá ser revisada e atualizada a cada 12 (doze) meses, ou em prazo inferior, caso necessário, em função de mudanças legais, regulatórias, autorregulatória ou complementações.

Capítulo II – Definições

2.1. São consideradas “Informações Confidenciais” aquelas não disponíveis ao público, que:

- Identifiquem dados pessoais, patrimoniais ou estratégicos;
- Sejam objeto de acordo de confidencialidade celebrado com terceiros;
- Identifiquem ações estratégicas – dos negócios da empresa, seus clientes ou dos portfólios sob gestão – cuja divulgação possa prejudicar a gestão

dos negócios, clientes e fundos de investimentos geridos pela QUARTER INVESTIMENTOS, ou reduzir sua vantagem competitiva;

- Todas as informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente que digam respeito às atividades da QUARTER INVESTIMENTOS e que sejam devidamente identificadas como sendo confidenciais, constituam propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral;
- Sejam assim consideradas face a determinação legal, previsão legal e/ou regulamentar; e que
- O Integrante utiliza para autenticação de sua identidade (senhas de acesso ou crachás) de uso pessoal e intransferível.

2.2. Na atividade de gestão, a QUARTER INVESTIMENTOS considera que o controle do fluxo de informações é o risco mais relevante em termos de controle estratégico para o negócio. A mitigação de tal risco se dá através de procedimentos operacionais de segurança, ligados ao uso de equipamentos internos (mitigado através dos contratos/sistemas fornecidos pelos prestadores de serviço), e, através de procedimentos internos que parametrizam o comportamento dos Integrantes, descritos neste documento.

2.3. Não caracteriza descumprimento desta Política de Confidencialidade e Segurança a divulgação de Informações Confidenciais mediante prévia autorização do Diretor de Compliance, em atendimento a ordens do Poder Judiciário ou autoridade regulatória, administrativa ou legislativa competente, seja em âmbito municipal, estadual ou federal, bem como, quando a divulgação se justificar, por força da natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

2.4. Em caso de dúvida, o Integrante deverá consultar previamente o Diretor de Compliance acerca da possibilidade de compartilhamento da Informação Confidencial, a qual deverá se manifestar formalmente sobre o caso.

Capítulo III – Disposições Gerais

3.1. Os seguintes princípios norteiam a segurança da informação na QUARTER INVESTIMENTOS:

- Confidencialidade: o acesso à informação deve ser obtido somente por pessoas autorizadas, e quando ele for de fato necessário;
- Disponibilidade: as pessoas autorizadas devem ter acesso à informação sempre que necessário;
- Integridade: a informação deve ser mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

3.2. As seguintes diretrizes devem ser seguidas por todos os Integrantes da QUARTER INVESTIMENTOS:

- As informações confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida;
- A informação deve ser utilizada de forma transparente, e apenas para a finalidade para a qual foi coletada;

- A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades. Desta forma, há a segregação lógica das informações, de modo que somente os Integrantes autorizados têm acesso às pastas virtuais respectivas às suas atividades desenvolvidas na QUARTER INVESTIMENTOS;
- A identificação de qualquer Integrante deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- Segregação de instalações, equipamentos e informações comuns, quando aplicável;

- A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

3.3. Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação devem ser reportados ao Diretor de Compliance.

Capítulo IV – Processos e Controles

4.1. Para assegurar que as informações sejam adequadamente protegidas, a QUARTER INVESTIMENTO definiu os seguintes processos/controles:

a. Identificação da Informação: o Integrante que recebe ou prepara uma informação deve identificar a natureza desta, conforme o item a seguir.

b. Classificação da Informação: algumas informações podem ser classificadas como confidenciais. Para tal, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

c. Controles para Informações Classificadas como “Confidencial”: o acesso às informações confidenciais deve ser controlado. Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros, sob supervisão do Diretor de Compliance, e, se reputado necessário, da assessoria jurídica da QUARTER INVESTIMENTOS.

d. Salvaguarda da Informação: a informação deve receber proteção adequada em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento e descarte.

e. Descarte de Informação Confidencial: armazenada em meio físico deve ser efetuado utilizando máquina fragmentadora de papéis ou incineradora.

f. Mesa Limpa: nenhuma Informação Confidencial deve ser deixada à vista nos locais de trabalho dos Integrantes. Ademais, ao usar uma impressora coletiva, o documento impresso deve ser imediatamente recolhido.

g. Gestão de Acessos: os serviços de rede, internet e correio eletrônico disponíveis na QUARTER INVESTIMENTOS são de sua propriedade exclusiva, sendo permitido o uso moderado para fins particulares, mediante autorização prévia do Diretor de Compliance.

4.2. A QUARTER INVESTIMENTOS poderá, a qualquer momento mediante prévia aprovação do Diretor de Compliance:

- Inspecionar conteúdo e registrar o tipo de uso dos e-mails feitos pelos usuários;
- Disponibilizar esses recursos a terceiros, caso entenda necessário;
- Solicitar aos usuários justificativas pelo uso efetuado.

4.3. No caso de mudança de área ou desligamento do Integrante, a respectiva senha de acesso é imediatamente adaptada para compatibilizar/adequar o acesso, ou cancelada em definitivo, visando ao impedimento de acesso não autorizado pelo ex-Integrante.

4.4. A utilização da rede, internet, e-mail e dispositivos móveis na QUARTER INVESTIMENTOS e/ou pelos seus Integrantes em comunicações de trabalho devem se dar pelas seguintes regras:

- Somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos;
- Somente imprimir as mensagens quando realmente necessário;
- Ao identificar mensagem com título ou anexo suspeito, certificar-se sobre a segurança em abri-la, para evitar vírus ou códigos maliciosos;

- No caso de recebimento de mensagens que contrariem as regras estabelecidas pela QUARTER INVESTIMENTOS, nunca as repassar, alertando o responsável da sua área e o Diretor de Compliance, se for o caso;
- Ao se ausentar do seu local de trabalho, mesmo que temporariamente, bloquear a estação de trabalho;
- Quando sair de férias ou se ausentar por períodos prolongados, o Integrante deve utilizar o recurso de ausência temporária de e-mail.

4.5. Vedações: é vedado ao usuário:

- Enviar e-mail ou acessar sites que promovam a veiculação de mensagens, produtos, imagens ou informações que interfiram na execução das atividades profissionais, sendo proibido, sobretudo, conteúdo pornográfico, racista, subversivo ou ofensivo à moral e aos princípios éticos;
- Divulgar informações ou trocar arquivos com configurações dos equipamentos e de negócios da QUARTER INVESTIEMNTOS, ou qualquer outra informação sobre a QUARTER INVESTIMENTOS, seus negócios, produtos, equipamentos ou Integrantes, sem prévia aprovação para isso. Em caso de exigência de alguma autoridade ou entidade autorreguladora, solicitar orientação ao Diretor de Compliance;
- Trocar informações que causem quebra de sigilo bancário e/ou possuam caráter confidencial ou estratégico;
- Prejudicar intencionalmente usuários da internet, mediante desenvolvimento de programas, acessos não autorizados a computadores e alteração de arquivos, programas e dados residentes na rede da QUARTER INVESTIMENTOS;
- Divulgar propaganda ou anunciar produtos ou serviços particulares pelo correio eletrônico da QUARTER INVESTIMENTOS;
- Alterar qualquer configuração técnica dos softwares que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pela Diretor de Compliance;

- Contratar provedores de acesso sem autorização prévia do Diretor de Compliance;
- Redirecionar caixa postal pessoal (e-mail de outros provedores) para a sua caixa postal de correio eletrônico na QUARTER INVESTIMENTO e vice-versa.

4.6. Bloqueio de Acesso a Sites: o Diretor de Compliance, juntamente com os responsáveis pelo departamento de tecnologia da informação, são responsáveis por monitorar os acessos feitos a sites através de computadores de propriedade da QUARTER INVESTIMENTOS, para reporte de eventual mau uso ao Comitê de Compliance, Controles Internos e Ética e bloqueio de acesso a sites proibidos.

4.7. Sites de Armazenamentos de Arquivos: o acesso a sites de armazenamento de arquivos em “nuvem” é permitido. Os equipamentos, ferramentas e sistemas concedidos aos Integrantes devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à QUARTER INVESTIMENTOS.

4.8. Apenas os Integrantes devidamente autorizados terão acesso às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede da QUARTER INVESTIMENTOS, mediante segregação física e lógica. Quaisquer exceções deverão ser previamente solicitadas ao Diretor de Compliance, que poderá ou não conceder a exceção.

4.9. Gestão de Riscos, Tratamento de Incidentes de Segurança da Informação, Continuidade de Negócio e Backups: os riscos e incidentes de segurança da informação devem ser reportados ao Diretor de Risco, que adotará as medidas cabíveis.

4.10. O plano de contingência e de continuidade dos principais sistemas e serviços deve ser objeto de testes, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

4.11. No caso de vazamento de informação, ou acesso indevido a informação, o Diretor de Compliance deverá ser imediatamente comunicado para a tomada das medidas cabíveis, variando de simples repreensão pelo acesso, ou mensagem ao destinatário errôneo da mensagem enviada para que apague em definitivo o seu conteúdo (se for o caso), até o estudo e implementação efetiva de providências judiciais, quando e se for o caso, tudo isso sem prejuízo da investigação e eventual punição dos Integrantes envolvidos, mediante apresentação do caso pelo Diretor de Compliance no Comitê de Compliance, Controles Internos e Ética da QUARTER INVESTIMENTOS.

4.12. O backup de todos os dados e informações da QUARTER INVESTIMENTOS é realizado na nuvem diariamente.

Capítulo V – Procedimentos de Segurança Cibernética

5.1. A QUARTER INVESTIMENTOS deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Guia ANBIMA de Segurança Cibernética definiu que os ataques mais comuns de cybercriminals são os seguintes:

- Malware (vírus, cavalo de troia, spyware e ransomware);
- Engenharia Social;
- Pharming;
- Phishing scam;
- Vishing;
- Smishing;
- Acesso pessoal;
- Ataques de DDoS e botnets;
- Invasões (advanced persistent threats).

5.2. Com a finalidade de se manter resguardada contra estes e outros potenciais ataques, a QUARTER INVESTIMENTOS definiu todos os ativos

relevantes da instituição, fundamentais a seu funcionamento, criou regras para classificação

das informações geradas e avalia continuamente a vulnerabilidade de cada um desses ativos.

5.3. Uma regra importante de prevenção consiste na segregação de acessos a sistemas e dados que a QUARTER INVESTIMENTOS adota, conforme já detalhado nas regras internas que tratam de Segurança da Informação.

5.4. A QUARTER INVESTIMENTOS adota, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância do ativo acesso. A QUARTER INVESTIMENTOS trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

5.5. Os eventos de login e alteração de senhas são auditáveis e rastreáveis.

5.6. O acesso remoto a arquivos e sistemas internos tem controles adequados. O acesso ao acervo digital conta com dupla verificação. Quando o Integrante acessa para logar no e-mail, é enviado um código de segurança no seu celular, garantindo a autenticidade.

5.7. Outro ponto importante é que, ao concluir novos equipamentos e sistemas em produção, a QUARTER INVESTIMENTOS deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção. A QUARTER INVESTIMENTOS conta com recursos anti-malware em estações e servidores de rede, como anti-virus e firewalls pessoais. A QUARTER INVESTIMENTOS deve, adicionalmente, proibir o acesso a determinados websites e a execução de softwares e/ou aplicações não autorizadas.

5.8. É terminantemente proibido que os Integrantes façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da QUARTER INVESTIMENTOS e circulem em ambientes externos à QUARTER INVESTIMENTOS com estes arquivos, uma vez que tais arquivos

contêm informações que são consideradas como informações confidenciais. Qualquer exceção à presente regra deverá ser previamente autorizada por escrito pelo Diretor de Compliance.

5.9. A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do

desenvolvimento dos negócios e dos interesses da QUARTER INVESTIMENTOS. Nestes casos, o Integrante que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

5.10. Em consonância com as normas internas acima, os Integrantes devem se abster de utilizar pen-drivers, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na QUARTER INVESTIMENTOS.

5.11. Para segurança dos perfis de acesso dos Integrantes, as senhas de acesso dos Integrantes são parametrizadas conforme regras estabelecidas globalmente. Dessa forma, o Integrante pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

5.12. Cada Integrante é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

5.13. A QUARTER INVESTIMENTOS adota também backup das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do plano de continuidade dos negócios da QUARTER INVESTIMENTOS.

5.14. Os Integrantes deverão manter arquivada toda e qualquer informação, incluindo informações confidenciais, privilegiadas ou reservadas bem como

documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com o inciso IV do Artigo 16 da Instrução CVM nº 558/15, em locais seguros, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.

5.15. Deve-se, ademais, realizar trimestralmente testes de invasão externa, phishing, bem como análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura. Os logs e trilhas de auditoria criados devem ser analisados regularmente pela área responsável, de forma a permitir rápida identificação de ataques, sejam internos ou externos.

Capítulo VI – Plano de Resposta

6.1. A área de compliance deve, conjuntamente com o departamento de tecnologia da informação, elaborar um plano formal de resposta a ataques

virtuais. A QUARTER INVESTIMENTOS deverá estabelecer os papeis de cada área em tal plano, prevendo o acionamento de Integrantes-chave e contatos externos relevantes.

6.2. O plano de resposta deverá levar em conta os cenários de ameaças previstos no risk assessment. Deve haver critérios para a classificação dos incidentes, por severidade. O plano deve prever, conforme o caso, o processo de retorno às instalações originais após o final do incidente, na hipótese em que as instalações de contingência ou acessos remotos tenham de ser utilizados.

6.3. A QUARTER INVESTIMENTOS desenvolveu planos de contingência para efeito de gerenciamento de situações de crise, de forma a garantir a continuidade de seus negócios, até a sua completa superação. Nesse sentido, caso ocorra algum evento extraordinário que impossibilite a utilização de suas instalações e estrutura físicas, a QUARTER INVESTIMENTOS continuará as suas atividades

em um escritório remoto, situado próximo a sua sede e que poderá ser utilizado em caso de contingências. Para tanto, a QUARTER INVESTIMENTOS manterá telefones, computadores e impressoras adicionais para fins de substituição.

Capítulo VII – Reciclagem e Revisão

7.1. O programa de segurança cibernética, que contempla os procedimentos aqui descritos, o plano formal de resposta e demais políticas internas da QUARTER INVETIMENTOS sobre a matéria, deverá ser revisto e atualizado anualmente.

7.3. Os grupos de trabalho diretamente envolvidos com qualquer parte do programa devem se manter atualizados, buscando fornecedores especializados, se necessário.

7.4. A QUARTER INVESTIMENTOS deverá divulgar o programa de segurança cibernética internamente e disseminar a cultura de segurança, alertando sobre os riscos principais e as práticas de segurança.

Capítulo VIII – Testes e Controles

8.1. A efetividade desta Política de Confidencialidade e Segurança é verificada por meio de testes periódicos dos controles existentes, com intervalos não superiores a 1 (um) ano, sob responsabilidade do Diretor de Compliance e reportados ao Comitê de Compliance, Controles Internos e Ética. Os testes devem verificar se:

- Os recursos humanos e computacionais são adequados ao porte e às áreas de atuação;

- Há adequado nível de confidencialidade e acessos às informações confidenciais, com identificação de pessoas que tem acesso a estas informações;
- Há segregação física e lógica;

- Os recursos computacionais, de controle de acesso físico e lógico, estão protegidos;
- A manutenção de registros permite a realização de auditorias e inspeções.

Capítulo IX – Propriedade Intelectual

9.1. Tecnologias, marcas, metodologias e quaisquer informações que pertençam à QUARTER INVESTIMENTOS não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Integrante em seu ambiente de trabalho.

Capítulo X – Rastreamento

10.1. É permitido o uso pessoal dos equipamentos de informática e de comunicação de propriedade da QUARTER INVESTIMENTOS utilizados pelos Integrantes para a realização das atividades profissionais. Lembrando que, como tais recursos (e-mails, sistemas, computadores, telefones etc.) pertencem à QUARTER INVESTIMENTOS, estes são rastreáveis e sujeitos a monitoramento, bem como podem se tornar públicos em caso de auditoria, exigência judicial ou regulatória.

Capítulo XI – Termo de Conhecimento

11.1. Os Integrantes devem aderir formalmente a um termo (anexo I), comprometendo-se a agir de acordo com esta Política de Confidencialidade e Segurança.

11.2. Os Integrantes que tenham acesso a Informações Confidenciais ou participem de processo de decisão de investimento devem solicitar ao Diretor de Compliance eventuais esclarecimentos sobre o tema de segurança de informação e segurança cibernética.

Capítulo XII – Disposições Finais

12.1. Dúvidas devem ser esclarecidas junto ao Diretor de Compliance.

12.2. A área de compliance informará oportunamente aos Integrantes sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da QUARTER INVESTIMENTOS na rede mundial de computadores.

12.3. Este documento revoga todas as versões anteriores e passa a vigorar na data de sua aprovação.

Porto Alegre, 15 de setembro de 2021.
Diretor de Compliance

ANEXO I

TERMO DE CONHECIMENTO DA POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICOS

NOME		
ÁREA	*CARGO*	
DOC. IDENTIDADE No	*TIPO*	*CPF*

Declaro que tenho conhecimento da Política de Confidencialidade e Segurança da Informação e Segurança Cibernética da QUARTER INVESTIMENTOS (“Política de Confidencialidade e Segurança”), e que estou ciente do seu teor, o qual está diretamente ligado ao exercício de minhas funções.

De acordo com este termo, comprometo-me a:

a) adotar e cumprir as diretrizes indicadas na Política de Confidencialidade e Segurança durante a vigência deste Termo e por prazo indeterminado após sua rescisão;
b) comunicar imediatamente ao Diretor de Compliance e Diretor de Risco qualquer violação desta Política de Confidencialidade e Segurança de que eu venha a ter conhecimento, independentemente de qualquer juízo individual, materialidade ou relevância da violação.

Estou ciente e concordo que meus acessos físicos, lógicos, de voz e de imagem podem ser objeto de monitoramento.

Desde já, aceito incondicionalmente atender e cumprir quaisquer novos itens e condições que possam vir a ser considerados partes integrantes desta Política de Confidencialidade e Segurança, sem a necessidade de apor assinatura em

novo Termo, bem como, em caso de negligência ou imprudência na aplicação desta Política, tenho total ciência da responsabilidade disciplinar que recairá sobre tal inobservância.

_____, _____de _____de 20_____(local)

_____Assinatura do Colaborador