FUTURUM CAPITAL GESTÃO DE ATIVOS LTDA.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

(abril de 2024)

1. A **FUTURUM CAPITAL GESTÃO DE ATIVOS LTDA.** ("**Futurum**") reconhece a importância de seus sócios, diretores, empregados, colaboradores, administradores e pessoas ligadas a esses ("**Membros**") conseguirem administrar, desenvolver e manter medidas de segurança da informação.

Referidas medidas têm por finalidade minimizar as ameaças aos negócios da Futurum e às disposições de suas políticas, buscando, principal, mas não exclusivamente, a proteção de informações confidenciais e privilegiadas, quais sejam, informações relacionadas às atividades, investimentos, ativos e toda e qualquer informação não pública ou restrita sobre a Futurum e seus Membros, levando em consideração o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Futurum.

2. As instalações da Futurum são protegidas por controles de entrada apropriados para assegurar a segurança dos Membros e proteger o sigilo, a integridade e a disponibilidade de informação.

3. O Diretor de Compliance (ou pessoa por ele incumbida) adotará as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, sempre que houver indícios de alguma irregularidade ou descumprimentos:

(i) Monitoramento, por amostragem, do acesso dos Membros a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos;

(ii) Monitoramento, por amostragem, das ligações telefônicas dos seus colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela Futurum para a atividade profissional de cada Membro; e

(iii) Verificação, por amostragem, das informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

4. O Diretor de Compliance poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

5. Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Futurum (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer informações confidenciais, reservadas e/ou privilegiadas,

mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance prontamente. O Diretor de Compliance determinará quais membros da administração da Futurum e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

6. Ademais, o Diretor de Compliance determinará quais clientes ou investidores, se houver, deverão ser contatados com relação a eventual violação.

7. O Diretor de Compliance responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos Futurum de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;

(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);

(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo informações confidenciais de fundo de investimento sob gestão da Futurum, a fim de garantir a ampla disseminação e tratamento equânime da informação confidencial);

(vii) Determinação do responsável (ou seja, a gestora ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Diretor de Compliance após a condução de investigação e uma avaliação completa das circunstâncias do incidente

8. O acompanhamento das políticas e procedimentos de segurança e a aplicação de sanções adequadas na hipótese de qualquer infração de tais políticas ou procedimentos serão realizados pelo Departamento de Compliance. Os usuários receberão acesso restrito aos sistemas de informação/tecnologias da Futurum com um perfil específico, dependendo de suas respectivas tarefas. Uma vez ao ano, os administradores de domínio (usuários seniores de seus sistemas) deverão, sistema por sistema: (i) conciliar todas as identidades de usuários com os registros do departamento de recursos humanos; (ii) solicitar uma recertificação da lista de usuários; e (iii) manter registros de cada recertificação e das ações de controle realizadas.

9. Independentemente dos mecanismos de controle, sempre que receberem qualquer informação privilegiada, os Membros acordarão, de forma vinculante, em informar imediatamente o Departamento de Compliance (i) caso tal Membro ocupe qualquer cargo no departamento técnico da Futurum e obteve informação privilegiada de qualquer fonte, inclusive no curso normal de suas atividades; ou (ii) caso esteja trabalhando em uma possível função interna, que recebe regularmente informações privilegiadas, e tenha recebido informações privilegiadas de fontes externas à Sociedade, porém não no curso normal de suas atividades.

10. Com base nas informações recebidas conforme descrito acima, o Departamento de Compliance deverá, uma vez ao mês, criar uma lista contendo as situações de informações privilegiadas que ocorreram no curso do respectivo período. A Futurum pretende manter permanentemente arquivadas, para consulta futura, todas e quaisquer ocasiões em que seus profissionais a informaram sobre possíveis conflitos.

11. De acordo com os dados registrados e de identificação de clientes, para evitar facilitar os Crimes de Lavagem de Dinheiro, e em todos os regulamentos aplicáveis emitidos pela CVM – a Futurum realizará sessões de treinamento anuais com todos os sócios e colaboradores de forma a prevenir a entrada de recursos ilícitos. Ainda no que diz respeito aos dados registrados e de identificação de clientes ("know your client"), a Futurum implementará sessões de treinamento anuais para seus sócios e colaboradores a respeito dos procedimentos de registro consistente com as leis aplicáveis. Dentro do escopo da Futurum, é essencial que todos os Membros estejam cientes dos riscos legais e de imagem na hipótese de qualquer envolvimento direito ou indireto com atividades relacionadas à lavagem de dinheiro. Em caso de dúvidas ou necessidade de orientação, o Departamento de Compliance deverá ser procurado.

12. Adicionalmente, a fim de proteger informações valiosas da Futurum e evitar sua remoção das instalações desta, os Membros estão expressamente proibidos de utilizar mídias removíveis (por exemplo, CDs, DVDs, unidades USB e similares).

13. A coordenação direta das atividades relacionadas à esta política ficará a cargo do Diretor de Compliance, que será o responsável inclusive por sua revisão, realização de testes e treinamento dos Membros, conforme aqui descrito.

DocuSigned by:
Heloísa Lourenço Ishii
11302C56DDF6473...

Heloísa Lourenço Ishii
Cargo: Administradora

DocuSign

Certificado de Conclusão

Identificação de envelope: C260A470E3EE42CB8245E17F6CDCB9EC
Status: Concluído
Assunto: Complete com a DocuSign: Política de Seg. da Informação e Seg. Cibernética.docx
Envelope fonte:
Documentar páginas: 3
Assinaturas: 1
Remetente do envelope:
Certificar páginas: 1
Rubrica: 0
Docusign Futurum
Assinatura guiada: Ativado
Rua Girassol
Selo com EnvelopeId (ID do envelope): Ativado
1033
Fuso horário: (UTC-03:00) Brasília
São Paulo, 05433-002
docusign@futurum.capital
Endereço IP: 200.232.114.215

Rastreamento de registros

Status: Original
Portador: Docusign Futurum
Local: DocuSign
26/04/2024 14:29:20
docusign@futurum.capital

Eventos do signatário	Assinatura	Registro de hora e data
Heloísa Lourenço Ishii heloisa.ishii@futurum.capital Nível de segurança: E-mail, Autenticação da conta (Nenhuma)	DocuSigned by: Heloísa Lourenço Ishii 11302C56DDF6473... Adoção de assinatura: Estilo pré-selecionado Usando endereço IP: 200.146.7.21	Enviado: 26/04/2024 14:32:49 Visualizado: 29/04/2024 08:26:17 Assinado: 29/04/2024 08:27:16

Termos de Assinatura e Registro Eletrônico:
Não oferecido através do DocuSign

Eventos do signatário presencial	Assinatura	Registro de hora e data

Eventos de entrega do editor	Status	Registro de hora e data

Evento de entrega do agente	Status	Registro de hora e data

Eventos de entrega intermediários	Status	Registro de hora e data

Eventos de entrega certificados	Status	Registro de hora e data

Eventos de cópia	Status	Registro de hora e data

Eventos com testemunhas	Assinatura	Registro de hora e data

Eventos do tabelião	Assinatura	Registro de hora e data

Eventos de resumo do envelope	Status	Carimbo de data/hora
Envelope enviado	Com hash/criptografado	26/04/2024 14:32:49
Entrega certificada	Segurança verificada	29/04/2024 08:26:17
Assinatura concluída	Segurança verificada	29/04/2024 08:27:16
Concluído	Segurança verificada	29/04/2024 08:27:16

Eventos de pagamento	Status	Carimbo de data/hora