POLÍTICA DE SEGURANÇA CIBERNÉTICA

DA

ALPHA KEY CAPITAL MANAGEMENT INVESTIMENTOS LTDA.

Esta Política de Segurança Cibernética ("Política") estabelece diretrizes aplicáveis a todos os Colaboradores Internos da **ALPHA KEY CAPITAL MANAGEMENT INVESTIMENTOS LTDA.** ("Alpha Key").

Os Colaboradores devem cumprir as exigências desta Política e, além disso, assumem a responsabilidade profissional de agir de maneira ética em todos os atos que pratiquem.

Para fins da presente Política, serão aplicadas as definições listadas no Item I do Código de Ética e de Políticas Internas da Alpha Key, salvo se outro significado lhes for expressamente atribuído neste documento.

Adicionalmente ao disposto no presente documento, serão aplicadas as políticas do prestador de serviços de TI (Norma de Utilização de Recursos da Rede Corporativa e Diretrizes de Segurança da Informação da Tecnoqualify) desenvolvidos para a Alpha Key.

1. Objetivos

Esta Política visa proteger os equipamentos, sistemas e dados de propriedade, uso ou sob responsabilidade da Alpha Key ("Recursos ou Infraestrutura de TI") contra fraudes, uso indevido, ataque de cibercriminosos, perda ou sequestro de dados.

O acesso, o uso indevido ou não autorizado aos referidos ativos da Alpha Key são tratados na Política de Segurança da Informação, parte integrante do Código de Ética.

2. Responsabilidades

2.1. Da Administração

(i) Direcionar os esforços e recursos para a segurança da informação, de acordo com a estratégia de negócios da empresa;

(ii) Aprovar as normas de segurança da informação e suas atualizações;

(iii) Aprovar os controles a serem utilizados para garantir a segurança das informações, bem como a implementação e aplicação efetiva dos princípios e direitos previstos na Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018 - LGPD), na condição de Encarregado;

(iv) Acompanhar os indicadores de segurança e os incidentes reportados pela empresa prestadora de serviços de TI e pela Diretoria de *Compliance*;

(v) Comunicar a Diretoria de *Compliance* os casos de violações ou indícios de violação das Políticas Internas relativas à informação;

(vi) Apoiar as iniciativas para melhoria contínua de medidas de proteção da informação da empresa, com vistas a reduzir os riscos identificados, inclusive no que diz respeito à capacitação dos Colaboradores sobre o tema;

(vii) Aprovar o planejamento, alocação de verbas, os recursos humanos e de tecnologia, no que tange a segurança da informação;

(viii) Delegar as funções de segurança da informação aos profissionais responsáveis;

(ix) Coordenar a elaboração do relatório de impacto à proteção de dados pessoais, sempre que exigido pelas autoridades competentes.

2.2. Da Empresa Prestadora de Serviços de TI

(i) Monitorar as violações de segurança e tomar ações corretivas visando saná-las e cuidando para que não haja recorrência;

(ii) Orientar os testes da infra-estrutura de tecnologia e de sistemas para avaliar os pontos fracos e detectar possíveis ameaças;

(iii) Assessorar as demais áreas da empresa no processo de classificação das informações;

(iv) Auxiliar as áreas de negócio na elaboração do Plano de Continuidade dos Negócios específico de cada uma;

(v) Assegurar que exista um processo apropriado para a comunicação dos incidentes e violações de segurança detectados pelos usuários da informação, independentemente dos recursos tecnológicos utilizados;

(vi) Identificar recursos e fornecer orientação para a tomada de ações rápidas caso sejam detectados incidentes de segurança;

(vii) Manter a infraestrutura que suporta o ambiente controlado;

(viii) Manter a infraestrutura e sistemas atualizados;

(ix) Garantir a implementação e operação dos indicadores de segurança;

(x) Notificar imediatamente os incidentes de segurança à diretoria;

(xi) Garantir a rápida tomada de ações em caso de incidentes de segurança.

2.3. Da Diretoria de *Compliance*

(i) Desenvolver, manter e implementar programas de treinamento e de conscientização aos Colaboradores Internos e Externos sobre as normas de segurança da informação, a forma como ela está estruturada e os principais conceitos de segurança da informação;

(ii) Decidir o tratamento que será dispensado aos dados de terceiros coletados e/ou armazenados nos diretórios da Alpha Key, na condição de Controlador a que se refere a LGPD, bem como realizá-lo, na qualidade de Operador previsto naquela legislação;

(iii) Obter o consentimento dos titulares para uso de dados pessoais não decorrentes de obrigação legal;

(iv) Gerenciar os problemas disciplinares resultantes de violações dos controles de segurança da informação, juntamente com os gestores dos envolvidos;

(v) Em conjunto com a Administração, determinar as sanções cabíveis;

(vi) Revisar periodicamente as políticas internas relacionadas à Segurança da Informação e sugerir as alterações necessárias.

3. Equipamentos

Os equipamentos objeto desta Política são os de propriedade da Alpha Key, tais como *desktops*, monitores, teclados, *mouses*, telefone, impressoras, desfragmentador de papéis e outros destinados ao uso pessoal ou comum dos Colaboradores da Alpha Key.

Eles deverão ser utilizados exclusivamente para fins profissionais, estão sujeitos ao monitoramento pela Diretoria de *Compliance* e o uso indevido está sujeito às penalidades previstas no Código de Ética.

Em caso de quebra ou indisponibilidade de equipamento (*desktop*, teclado, *mouse*, monitor, telefone), estarão disponíveis para uso imediato os equipamentos de contingência.

Nas hipóteses em que for necessário acionar uma infraestrutura replicada - física ou virtualizada - que garanta a substituição de um servidor, roteador, *nobreak* e/ou outro equipamento de TI que falhe ou esteja inacessível (Redundância de TI) entrará em operação a Política de Continuidade dos Negócios da Alpha Key.

4. Controle de acesso ao escritório

Os Colaboradores terão acesso identificado às dependências da Alpha Key por meio de controle biométrico. O acesso às áreas poderá ser restringido de acordo com as atividades desenvolvidas por cada Colaborador, cabendo à Diretoria de *Compliance* identificá-las, bem como definir a lista de pessoas autorizadas.

O acesso de pessoas estranhas às instalações físicas da Alpha Key e as áreas restritas somente é permitida com a autorização expressa da Administração e/ou da Diretoria de *Compliance*.

Quaisquer trabalhos que envolvam informações confidenciais deverão ocorrer em áreas seguras.

Os computadores, telefones, acesso à internet, *e-mail* e demais facilidades disponíveis no espaço físico da Alpha Key são de propriedade desta e se destinam exclusivamente para fins profissionais.

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

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar à Diretoria de Compliance.

5. Instalações elétricas e o sistema de refrigeração

A fim de assegurar as condições ideais de funcionamento da Infraestrutura de TI, evitando perda de dados por falta ou sobrecarga de energia ou superaquecimento; e danos aos equipamentos de informática, é imprescindível instalações elétricas e sistema de refrigeração adequados.

Ambos foram dimensionados de acordo com a estrutura instalada sob orientação de profissionais especializados.

6. Funcionamento contínuo dos Recursos de TI

Os Recursos de TI em sistema *no-stop* será feito por *nobreak,* que garante o funcionamento da infraestrutura por tempo suficiente para que nenhuma informação seja perdida quando ocorre falta de energia elétrica por até 6 horas. Os critérios de funcionamento e o procedimento para realização dos testes de verificação estão descritos na Política de Continuidade dos Negócios.

Adicionalmente, vale ressaltar que o prédio em que o escritório da Alpha Key está localizada possui gerador, que em caso de interrupção no fornecimento de energia, passa a funcionar imediatamente de maneira ininterrupta, até o fornecimento de energia voltar a funcionar. O gerador abastece tanto as áreas comuns do prédio, como o escritório da gestora.

7. *Firewall*

As intrusões ou invasões são praticadas por pessoas que pretendem acessar, roubar ou sequestrar dados confidenciais e/ou informações privilegiadas, capturar dados para realização de fraudes, causar danos a sistemas e aplicativos.

A fim de evitar esses riscos, a Alpha Key conta com um mecanismo de controle do tráfego de dados entre os computadores de uma rede interna e desses com redes externas ("*Firewall*"). Ele trabalha segundo protocolos de segurança que garantem o correto funcionamento da comunicação entre as duas pontas, visando impedir intrusões.

Seu funcionamento é contínuo, as atualizações são programadas e realizadas automaticamente pelo sistema.

8. Senhas

A Alpha Key adota uma estrutura e configuração que induz a criação de senhas fortes, a fim de dificultar o acesso de pessoas mal intencionadas em seus sistemas. Há, ainda, um mecanismo automático que obriga a troca periódica de senhas pelos usuários ativos e cancela as senhas de usuários inativos/desligados da organização.

A senha e o *login* para acesso aos dados contidos em todos os computadores, bem como nos *e-mails*, são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. Assim, o Colaborador pode ser penalizado caso os compartilhe com terceiros para quaisquer fins.

9. *Softwares*

A Alpha Key possui as licenças de uso de todos os *softwares* que utiliza. A Administração é responsável pelas renovações nos prazos e termos definidos em cada contrato.

É proibido o *download* de aplicativos de qualquer natureza ou procedência sem o consentimento da Diretoria de *Compliance*.

10. Correspondências eletrônicas ("*e-mails*" e *chats*)

Apenas os Colaboradores Internos e sócios da Alpha Key possuirão contas de *e-mail* corporativo, que serão criadas pela empresa responsável pela Infraestrutura de TI no momento da contratação ou integralização de cotas sociais.

O responsável pela conta de *e-mail* individual ou da área deverá lhe atribuir uma senha de acesso pessoal, sigilosa e intransferível.

Essas correspondências poderão ser acessadas para fins de monitoramento pela Diretoria de *Compliance.*

Em caso de desligamento do Colaborador ou retirada do sócio, o acesso ao respectivo *e-mail* será imediatamente bloqueado pelo profissional de TI por orientação da Diretoria de *Compliance*.

Os *e-mails* serão armazenados pela Microsoft, que proverá também os serviços de anti *spam,* anti vírus, recuperação de informação, *site* de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas.

As ordens de negociação de ativos e demais comunicações realizadas pela equipe de gestão por meio do *chat* do Bloomberg são automaticamente gravadas pelo sistema.

11. Armazenamento duplo de dados *(back up)*

Com vistas a evitar a perda de informações proprietárias, confidenciais e/ou privilegiadas, a Alpha Key adota a armazenagem duplicada de dados em HD externo e, ainda, em *cloud*. O *backup* de dados em HD externo é realizado automaticamente, abrange todos os dados do servidor local e é mantido por período mínimo de 180 dias. O *back up* em *cloud* é mantido por tempo indeterminado sendo limitado apenas ao espaço disponível.

12. Telefone

A Alpha Key definirá os Colaboradores que terão acesso à linha telefônica corporativa, conforme a atividade que desempenhem.

O uso do telefone deverá se restringir às atividades profissionais em prol da Alpha key e estará sujeita à gravação automática que será mantida por até 90 dias, para fins de monitoramento e confirmação de operações.

O monitoramento será feito periodicamente à critério da Diretoria de *Compliance,* mediante acesso ao portal do provedor de telefonia contratado, a fim de fazer cumprir o Código de Ética.

A Alpha Key conta com 7 linhas VOIP e 1 linha analógica, que serve como backup e que só será utilizada e ligada em caso de contingência. Em caso de falhas nas linhas telefônicas VOIP, poderão ser utilizadas as linhas analógicas.

13. Internet

O acesso à internet é disponibilizado por 2 links de velocidade: um link dedicado (Mundivox) e 1 link ADSL de 100 mbps (VIVO). Os sistemas estão permanentemente disponíveis e são ativados automaticamente em caso de perda de sinal do outro provedor.

14. Dados de terceiros

A Alpha Key trata dados pessoais primordialmente para o cumprimento de obrigação legal. Nos demais casos, será obtido consentimento do titular.

Os dados de terceiros, quer sejam Colaboradores ou Clientes, que venham a ser compartilhados com a Alpha Key, deverão ser tratados como confidenciais, nos termos da Política descrita no item 12 do Código de Ética, e de acordo com as especificidades da LGPD.

15. Erros de procedimentos internos

Procedimentos de gestão da segurança da informação mal-estruturados ou desatualizados podem acarretar vulnerabilidades e perdas de dados. Essas vulnerabilidades se manifestam por falhas no desenvolvimento, na implementação ou na configuração de mecanismos de segurança em *softwares,* no funcionamento dos *hardwares* ou em exposição a ameaças previsíveis.

A Alpha Key conta com equipe especializada para a execução dos protocolos de manutenção e segurança de seus Recursos de TI, como apontado acima.

16. Crises ou situações críticas

Na hipótese de situações não rotineiras em que os mecanismos descritos nesta Política se tornarem insuficientes ou ficarem indisponíveis, será acionada a Política de Continuidade dos Negócios, no que couber.

Alteração inserida	Ano	Responsável	Aprovação
Atualização da forma de back up (HD externo)	2020	Simone de Grandis	Diretor-Presidente
Menção aos canais de comunicação	2020	Simone de Grandis	Diretor-Presidente
Explicitação do sistema de gravação de ramais, monitoramento de emails e gravação do chat Bloomberg	2020	Simone de Grandis	Diretor-Presidente
Fornecedor do link dedicado	2021	Simone de Grandis	Diretor-Presidente
Revisão Anual	2022	Simone de Grandis	Diretor-Presidente
Revisão Anual	2024	Daniela Sessa	Comitê de Compliance