POLÍTICA DE SEGURANÇA CIBERNÉTICA DA SPARTAX CAPITAL & CO LTDA

1. Objetivo

O objetivo desta política é estabelecer as diretrizes necessárias para assegurar a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados pela **SpartaX Capital & CO LTDA** ("SpartaX Bank").

2. Público-Alvo

As disposições desta política aplicam-se:

(i) A todas as instituições pertencentes à SpartaX Bank, bem como aos respectivos funcionários, estagiários e aprendizes, doravante denominados "colaboradores";

(ii) Às entidades e órgãos que possuam acesso às informações da SpartaX Bank;

(iii) Aos prestadores de serviços, pessoas físicas ou jurídicas, que manuseiam dados ou informações sensíveis à condução das atividades operacionais da organização.

3. Princípios de Segurança Cibernética

O processo de Segurança Cibernética da SpartaX Bank é pautado pelos seguintes princípios fundamentais:

- **Confidencialidade:** acesso à informação apenas para entidades ou pessoas devidamente autorizadas;
- **Integridade:** garantir que a informação armazenada e trafegada mantenha suas características originais ao longo do seu ciclo de vida;
- **Disponibilidade:** assegurar que a informação esteja acessível sempre que necessário para entidades ou pessoas autorizadas.

4. Diretrizes

As diretrizes desta política estabelecem um programa de prevenção, detecção e redução de vulnerabilidades e impactos relacionados a incidentes cibernéticos.

4.1 Informação: Importância e Proteção

- A informação é um ativo estratégico da SpartaX Bank e deve ser preservada conforme normas internas e legislações aplicáveis.
- A SpartaX Bank se compromete com a conformidade às leis de privacidade e proteção de dados de seus clientes e parceiros.

4.2 Gestão de Identidades e de Acessos

- Os acessos aos recursos computacionais serão revisados periodicamente, garantindo que apenas usuários autorizados possuam permissões necessárias.

4.3 Controles dos Dispositivos de Tecnologia

- Todos os dispositivos de tecnologia disponibilizados serão protegidos por medidas de segurança para prevenir ataques e vazamento de dados.

4.4 Desenvolvimento de Sistemas e Garantia de Qualidade

- A segurança deve ser integrada ao desenvolvimento de sistemas, desde sua concepção até sua implementação e manutenção.

4.5 Segurança e Monitoramento da Infraestrutura, Redes e Sistemas

- Redes e sistemas relevantes devem ser monitorados e protegidos contra acessos não autorizados por meio de tecnologias atualizadas e testadas periodicamente.

4.6 Registro e Respostas a Incidentes de Segurança

- Todos os incidentes cibernéticos devem ser documentados, investigados e tratados conforme plano de resposta a incidentes.

4.7 Continuidade do Negócio e Recuperação de Incidentes

- A SpartaX Bank mantém um plano de continuidade de negócio para lidar com incidentes relevantes e minimizar impactos operacionais.

4.8 Gestão dos Prestadores de Serviços Relevantes

- Prestadores de serviços que lidam com informações da SpartaX Bank devem estar sujeitos a auditorias e controles de segurança.

4.9 Avaliação de Riscos Cibernéticos de Produtos ou Serviços

- Riscos cibernéticos devem ser identificados, documentados e tratados conforme protocolos definidos.

4.10 Backup de Dados

- A SpartaX Bank deve garantir processos de backup eficientes para recuperação de dados em caso de falhas ou incidentes.

4.11 Conscientização de Colaboradores, Clientes e Fornecedores

- Manutenção de programas de conscientização para desenvolvimento de boas práticas de segurança.

5. Violações de Segurança

As violações das regras definidas nesta política poderão ensejar sanções disciplinares, conforme o Código de Ética da SpartaX Bank.

6. Canal de Comunicação

No caso de alertas de segurança e/ou incidentes, as notificações devem ser enviadas para o canal de comunicação oficial:

 E-mail: sac@spartaXcapital.com.