LINHAS GERAIS DA
POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. OBJETIVO

Este documento tem por finalidade,divulgar à público as diretrizes da Política da Segurança Cibernética (“Política”) da Issuer Instituição de Pagamento Ltda. (“Issuer”), visando a proteção dos ativos de informação de modo seguro e transparente, através da prevenção, detecção e redução dos riscos associados, de forma alinhada ao negócio, complexidade e porte da, assim como aos requisitos legais e exigências dos órgãos regulatórios de acordo com o negócio.

2. BASE LEGAL E REGULATÓRIA

Esta Política cumpre fielmente a legislação concernente e as disposições do Banco Central do Brasil (“BCB”) e Conselho Monetário Nacional (“CMN”), em especial:

- Resolução BCB nº 85, de 8 de abril de 2021 que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.

3. DESTINATÁRIOS

Esta Política se aplica a todos os sócios, diretores, gestores, administradores, funcionários, prestadores de serviços, prepostos, terceirizados e quaisquer demais pessoas físicas ou jurídicas contratadas ou outras entidades que participem, de forma direta ou indireta, das atividades diárias e negócios da Issuer (“Destinatários”).

Os Destinatários devem atender a todas às diretrizes e procedimentos estabelecidos nesta Política, desde o momento de início do relacionamento, em que tomem ciência do mesmo, e, naquilo o que se prolongar no tempo, pelo prazo de 10 (dez) anos contados do término do vínculo do Destinatário com a Issuer.

4. DEFINIÇÕES

Para os fins desta Política, consideram-se:

- **Confidencialidade:** somente o usuário da informação, que esteja devidamente autorizado pelo gestor da informação, deve ter acesso às Informações respeitando os critérios de segregação de funções;

- **Adequação:** garantir que informações não sejam alteradas desde a sua criação até seu uso. Eventuais alterações, supressões e/ou adições devem ser autorizadas pelo gestor da informação;

- **Disponibilidade:** garantir que as informações estejam sempre disponíveis para o usuário da informação;

- **Autenticidade:** garantir a identidade de quem está enviando a Informação, ou seja, gera o não-repúdio que se dá quando há garantia de que o emissor não pode se esquivar da autoria da mensagem (irretratabilidade);

- **Riscos Cibernéticos:** riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

- **Negação de serviço:** um ataque de negação de serviço (também conhecido como DoS Attack, um acrônimo em inglês para Denial of Service), é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis na rede. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

- **Fraudes Externas e invasões:** realização de operações por fraudadores, utilizando-se de ataques em contas de pagamento, com o uso de conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

5. DIRETRIZES

O cumprimento da Política é de responsabilidade de todos os Destinatários, os quais devem seguir as diretrizes abaixo:

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;

- Prover a adequada classificação da informação, considerando os critérios de confidencialidade, integridade e disponibilidade;

- Assegurar que os recursos utilizados para o desempenho da sua função sejam utilizados apenas para as finalidades desempenhadas a sua atividade;

- Garantir que os sistemas e as informações que estão sob a sua responsabilidade sejam adequadamente protegidos;

- Atender às leis e resoluções que regulamentam as atividades da Issuer e seu mercado de atuação;

- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;
- Garantir a continuidade do processamento das informações críticas de negócios;
- Comunicar imediatamente aos responsáveis quaisquer descumprimentos desta Política.

Visando o fortalecimento da cultura de Segurança da Informação e Cibernética através da disseminação dos princípios e diretrizes descritos nesta Política, a Issuer possui processo de capacitação e conscientização, de todos os níveis, ao que se refere à segurança da informação, contemplando segurança de dados, segurança cibernética, inclusive com relação aos terceiros e demais contrapartes.

A Issuer conta com ferramentas, mecanismos e controles adequados para garantir a efetividade do objetivo, diretrizes, princípios, regras, papéis, responsabilidades e demais conteúdos abordados em sua Política.

6. PRINCÍPIOS E REGRAS

A estratégia de Segurança da Informação da Issuer é baseada em arquitetura com os seguintes domínios:

- Governança de Segurança da Informação;
- Segurança Cibernética Ofensiva;
- Segurança Cibernética Defensiva e Treinamento; e,
- Conscientização e Cultura.

Todos os princípios adotados pela Issuer visam atingir as diretrizes e objetivos desta Política, reduzindo a sua vulnerabilidade quanto aos riscos de segurança cibernética. Os procedimentos e os controles da segurança cibernética são implementados de modo a abranger a autenticação, criptografia, prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes de invasão e de outras metodologias de operações ofensivas para detecção e correção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores, a manutenção de cópias de segurança dos dados e das informações, e a prevenção e reposta de incidentes de segurança da informação.

A Política da Issuer possui um item específico para tratar e detalha cada um dos processos abaixo:

6.1. Acesso, classificação, manuseio e rotulagem da informação

6.2 Proteção de Dados Pessoais

6.3 Desenvolvimento de Aplicações e Sistemas

6.4 Processamento, Armazenamento de Dados e Computação em Nuvem

6.5 Cópias de Segurança (Backup)

6.6 Gestão de Riscos e Incidentes de Segurança

6.7 Plano de Continuidade de Negócios

7. PAPÉIS E RESPONSABILIDADES

Todos os Destinatários e a Issuer são responsáveis por adotar e cumprir as diretrizes, deveres, controles e práticas a eles aplicáveis contidas desta Política, zelando para que todas as normas éticas e legais sejam cumpridas por todos aqueles com quem são mantidas relações de cunho profissional, e comunicando imediatamente qualquer violação ao Responsável, para adoção das respectivas providências, de acordo com sua gravidade.

A Política interna atribui ainda, de modo detalhado aos procedimentos internos, os papéis e responsabilidades específicas que devem ser seguidas por todos os Destinatários, pelos Gestores da Informação e pelo Diretor Responsável.

8. VIOLAÇÃO

Todo Destinatário é responsável por garantir a segurança cibernética, com o objetivo de evitar que ela possa ser acessada por pessoa não autorizada. Sendo assim, é vedado:

- Expor a Issuer à uma perda monetária efetiva ou perda potencial por meio do comprometimento da segurança de dados ou de informações ou, ainda, por meio da perda de equipamento;
- Revelar dados confidenciais e negociações;
- Usar indevidamente e sem autorização direitos autorais, patentes e dados corporativos;
- Utilizar dados para propósitos ilícitos que violem qualquer lei, regulamento ou seja qual for outro dispositivo governamental.

Em caso de violação desta Política, será avaliada a severidade, a amplitude e o tipo de infração cometida. A punição para tal pode resultar desde advertência verbal ou escrita até em uma ação judicial.

9. VIGÊNCIA E CONTROLE DE VERSÕES

Esta Política entra em vigor a partir da data de disponibilização e divulgação aos Destinatários e será periodicamente revisada e atualizada pelo Diretor Responsável, com a frequência mínima de uma vez a cada 12 (doze) meses.

ELABORADO POR:	REVISADO POR:	ALTERAÇÕES:	DATA:
COMPLIANCE	T.I	CRIAÇÃO DA POLÍTICA REDUZIDA COM ESCOPOS GERAIS PARA DIVULGAÇÃO PÚBLICA	15/05/2023

10. APROVAÇÃO

A Diretoria da Issuer, ao aprovar esta Política de Segurança Cibernética, institui um compromisso para com a melhoria contínua dos procedimentos relacionados com a segurança cibernética, buscando sempre manter a Issuer em conformidade com normas legais e regulamentares sobre os referidos temas, guiada pelos princípios, conceitos, valores e práticas aqui adotados, com o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados da Issuer ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à Issuer prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.