Resumo da Política de Segurança Cibernética

Política de Segurança Cibernética da WP Instituição de Pagamento Ltda (“WisePay”)

1. Objetivo:

A Política de Segurança Cibernética da WisePay estabelece os princípios e diretrizes para a prevenção, detecção e resposta a ameaças digitais, garantindo a confidencialidade, integridade e disponibilidade dos dados e sistemas sob nossa responsabilidade. Também busca assegurar o cumprimento dos requisitos legais e das exigências dos órgãos reguladores, de acordo com a natureza, complexidade e porte das nossas operações.

2. Abrangência:

A Política de Segurança Cibernética da WisePay 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 WisePay.

3. Escopo:

A Wise Pay está comprometida com a proteção das informações e com a manutenção de um ambiente digital seguro para clientes, colaboradores e parceiros. Para isso, adota ferramentas, mecanismos e controles eficazes para garantir a aplicação das diretrizes, princípios, regras, papéis e responsabilidades definidos nesta Política. Entre esses recursos, destacam-se: processos, métricas, indicadores, trilhas de auditoria e testes de conformidade.

Essa Política integra o plano de auditoria interna da empresa, e eventuais deficiências identificadas são tratadas de forma tempestiva, com foco na melhoria contínua.

4. Diretrizes:

Adotamos controles técnicos e administrativos robustos, alinhados às melhores práticas do mercado e à legislação vigente, como a Resolução BCB nº 85/2021 e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD). Entre as principais medidas adotadas, destacamos:

- Monitoramento contínuo dos sistemas e acessos;
- Controles de autenticação, classificação e restrição de permissões;
- Armazenamento de logs por, no mínimo, 12 meses;

- Avaliação rigorosa de prestadores de serviços de tecnologia e nuvem;
- Treinamentos periódicos de segurança para colaboradores;
- Análises de vulnerabilidades, incluindo testes de invasão (pentests);
- Gestão ativa de riscos e plano de resposta a incidentes cibernéticos;
- Procedimentos de backup, descarte seguro e continuidade de negócios;
- Conformidade com a LGPD e respeito aos direitos dos titulares de dados.

Todas as ações são conduzidas com transparência, visando proteger você e suas transações no ambiente digital.

Nossa Política é revisada periodicamente para garantir sua efetividade diante das constantes mudanças no cenário tecnológico. A segurança da informação é parte essencial da nossa cultura organizacional e do nosso compromisso com a confiança nas relações.