Resumo da Política de Segurança da Informação

A Política de Segurança da Informação da PAY4FUN foi criada com o objetivo de definir diretrizes e princípios gerais para a proteção de informações, tanto internas quanto externas. Ela se aplica a todos os colaboradores e terceiros que possuem acesso aos sistemas e dados da empresa.

Objetivo: A política busca preservar os princípios básicos da política de segurança que envolve a confidencialidade, disponibilidade, integridade, sigilo e autenticidade das informações da PAY4FUN. Além disso, foca em estabelecer medidas técnicas e administrativas para proteger as informações contra acessos não autorizados e situações acidentais ou ilícitas.

Público-Alvo: Esta política é aplicável a todos os membros da PAY4FUN, incluindo funcionários, estagiários, temporários, terceiros e parceiros de negócios. É dever de cada colaborador cumprir as disposições desta política.

Estrutura de Governança: A PAY4FUN mantém uma estrutura de governança responsável pela segurança da informação. Essa estrutura assegura a conformidade com as leis e regulamentos aplicáveis, além de realizar análises e revisões regulares dos riscos e da política de segurança da informação.

A PAY4FUN está comprometida em seguir os mais altos padrões de segurança da informação, alinhando as práticas de negócios às necessidades de segurança e legislação atual.

Diretrizes Gerais

Os princípios estabelecidos na Política têm relacionamento direto ou indireto com aspectos de segurança da informação, controle e gestão dessas informações utilizadas e/ou geradas pela PAY4FUN em seu desempenho corporativo.

As diretrizes gerais da Política expressam as estratégias, valores e o nível de comprometimento que a PAY4FUN estabelece em relação à segurança da informação corporativa, assim como as respectivas instruções orientam o quadro de colaboradores quanto ao cumprimento de atividades e rotinas relacionadas à segurança da informação.

Privacidade e Proteção de Dados: Esta Política abrange todos os dados, incluindo pessoais, coletados pela PAY4FUN. O uso desses dados é restrito e deve cumprir com os termos da política de segurança da informação, com acordos contratuais e medidas de proteção, conforme a legislação aplicável. Os colaboradores são instruídos a seguir as melhores práticas de segurança em todo o ciclo de vida dos dados.

Monitoramento e Auditoria do Ambiente: Todo o ambiente físico e digital da PAY4FUN é monitorado, respeitando a legislação, para garantir a conformidade com as normas de segurança. Isso inclui servidores, redes, conexões de internet, softwares e dispositivos, além de inspeções físicas.

Conscientização dos Colaboradores: Os colaboradores devem estar cientes das práticas de monitoramento, que têm como objetivo proteger não só os sistemas da PAY4FUN mas também o próprio colaborador. As informações coletadas podem ser usadas para auditoria,

investigações e conforme exigido por lei. O acesso a esses dados é restrito a departamentos competentes e usados apenas para finalidades legítimas.

Diretrizes Gerais

A Política define diretrizes específicas de segurança da informação, a saber:

Gestão de Identidades e Acessos:

- A PAY4FUN garante identificação única e intransferível para usuários.
- Os usuários são responsáveis pela proteção das informações de autenticação e devem seguir práticas de segurança.
- A empresa gerencia o ciclo de vida dos acessos, garantindo concessão, manutenção e revogação, e monitora acessos privilegiados.
- O acesso é baseado no princípio "Need-to-know", e a PAY4FUN reserva-se o direito de revisar privilégios.

Acesso Remoto e Teletrabalho

- O acesso remoto é autorizado para suporte e monitoramento e é feito através de perfis pré-estabelecidos.
- Todos os acessos remotos devem utilizar métodos seguros e o uso de dispositivos privados, como regra, é proibido.

Uso de Senhas

- A senha é confidencial e intransferível, com requisitos mínimos de segurança.
- A criação e uso de senhas devem seguir diretrizes específicas, como ter no mínimo de caracteres, variação de maiúsculas e minúsculas, autenticação de dois fatores para serviços críticos, entre outros.

Concessão de Acesso Privilegiado

- Os ativos da PAY4FUN são classificados para gestão de acessos privilegiados.
- A concessão e uso devem ser feitos conforme diretrizes, como vinculação à conta do indivíduo, uso distinto da conta geral, inventário de contas privilegiadas e aprovação pela diretoria de tecnologia.

Ambiente e Recursos de Trabalho

Mesa Limpa

- As mesas devem ser mantidas limpas.
- Documentos e Informações Protegidas devem ser armazenados com segurança.
- Mídias de armazenamento eletrônico devem ser trancadas.
- Gavetas das mesas devem ser trancadas.
- Documentos impressos devem ser retirados das impressoras imediatamente.
- Salas de reuniões devem ser mantidas limpas.
- Documentos protegidos devem ser distribuídos ao serem descartar.

Estações de Trabalho

- Colaboradores são responsáveis pela integridade do equipamento.
- Utilização deve ser feita conforme o Código de Conduta Ética.
- Armazenamento de informações devem ser feitas em servidores corporativos.
- Configurações padronizadas conforme boas práticas de segurança, incluindo antivírus e atualizações críticas.

Acesso à Internet

- Uso restrito para trabalho e pesquisa.
- Monitoramento do uso e conteúdo.
- Proibição de acesso a conteúdo inapropriado, uso comercial não autorizado e violação de direitos autorais.

E-mail

- Fornecido para fins corporativos.
- Monitorado e sujeito a acesso pelas Áreas de Segurança da Informação.
- Uso proibido para conteúdo abusivo, não profissional, campanhas humanitárias, ou tráfego de anexos não autorizados.

Proteção contra Malware

- Todas as estações de trabalho, servidores e ativos compatíveis conectados na rede corporativa ou que utilizem informações da PAY4FUN devem estar protegidos com a solução de antivírus especificada.
- O usuário está proibido de remover, desabilitar ou alterar as configurações do antivírus, ou instalar outro programa de antivírus em computadores pertencentes à PAY4FUN.

Gestão de Ativos

Segurança em Manuseio de Mídias

- Uso de mídias removíveis (pen drives etc.) é limitado a Administradores, Gestores e autorizados pela Diretoria de Tecnologia.

Informações Protegidas

- Propriedade exclusiva da PAY4FUN, exceto disposição contrária.
- Proibição de reprodução, divulgação etc., a terceiros sem autorização.
- Deve ser restituída ou eliminada no término da relação com o colaborador.
- Divulgação exigida por Lei após análise da área Jurídica.

Classificação das Informações Protegidas

- Pública: Informações liberadas para o público geral.
- Interna: Acessíveis por usuários autorizados.
- Confidencial: Uso restrito.
- Secreta: Acesso controlado.

Segurança na Operação e Padrões de Configuração

Aplicação de Hardening

- Implementação de padrões de segurança em todos os sistemas, administrado pelo time de tecnologia e aprovado pelo time de segurança da informação.

Desenvolvimento Seguro de Software

- Segregação em camadas: apresentação, aplicação e banco de dados.
- Adoção de boas práticas como OWASP.
- Adesão a padrões tecnológicos e mitigação de riscos de propriedade intelectual.
- Aprovação de exceções pela área de Segurança da Informação.

Segurança de Rede e Perímetro

- Estrutura para garantir disponibilidade, integridade, confidencialidade e autenticidade.
- Mecanismos e controles: prevenção de intrusão, vazamento, segregação de ambientes.
- Acesso somente por usuários autenticados e métodos autorizados.

Gestão de Mudanças

- Processo rigoroso para manter integridade, performance e disponibilidade.
- Segregação em Desenvolvimento, Homologação, Pré-produção e Produção.
- Tratamento de informações sensíveis nos ambientes de desenvolvimento.

Criptografia

- Utilização efetiva para assegurar confidencialidade, autenticidade e integridade.
- Aprovação e revisão pela área de Segurança da Informação.
- Documentação da arquitetura criptográfica, incluindo detalhes e inventário de dispositivos.

Testes de Segurança

- Realização de testes de penetração periódicos.
- Validação, identificação de vulnerabilidades e definição de planos de ação.

Gestão de Incidentes de Segurança

- Comunicação imediata em caso de violação ou risco.
- Gestão de vulnerabilidades e incidentes reais.
- Reporte imediato de incidentes.
- Resposta em casos de dados pessoais.
- Relatório de registros para Diretoria ou Conselho.

Cloud Computing

- **Requisitos para Fornecedores**: Segregação de dados, cumprimento de legislação, acordos com autoridades, continuidade operacional.
- **Itens Contratuais**: Inclui garantias de integridade, confidencialidade, disponibilidade, planos de contingência, acordos de nível de serviço e operacional, gestão de acessos, registros de logs, transferência e exclusão de dados, acesso do Banco Central, e notificação de interrupção de serviços.

Segurança Física

Identificação

- Obrigatório uso visível de crachás para colaboradores, estagiários e prestadores de serviço.

Áreas Seguras

- Definição e proteção dos perímetros de segurança.
- Proteção contra acessos físicos não autorizados, danos e interferências.
- Consideração de ameaças externas e ambientais.

Equipamentos

- Proteção com controles físicos para reduzir riscos de ameaças, perigos ambientais e acesso não autorizado.

Gestão da Continuidade de Negócios

- Plano de Continuidade de Negócios documentado, testado e revisado.

  Requisitos mínimos:

  - Análise de impacto.
  - Estratégia de recuperação.
  - Gerenciamento de crise.
  - Planejamento de continuidade e recuperação.
  - Procedimentos de retorno à normalidade.
  - Metodologia para planos de continuidade.
  - Normas e padrões de continuidade, incluindo prestadoras de serviço.

Segurança para Recursos Humanos

- Programa de conscientização, avaliação, educação e treinamento.
- Treinamento obrigatório em Segurança da Informação.
- Divulgação de normas e padrões no processo de admissão e integração.
- Gestão de Terceiros, Parceiros e Fornecedores.
- Inclusão de cláusulas de segurança nos contratos.
- Conformidade dos colaboradores externos com as normas da PAY4FUN.
- Permissão de segurança para prestação de serviço, renovada periodicamente.

Em atendimento à Resolução 4.893 do BACEN, anualmente a PAY4FUN deverá emitir um relatório sobre em conformidade das ações tomadas para alinhar suas estruturas com os princípios e diretrizes da política em questão, um resumo dos resultados alcançados na implementação de rotinas, procedimentos, controles e tecnologias para prevenção e resposta a incidentes, a descrição dos incidentes relevantes que ocorreram durante o período, e os resultados dos testes de continuidade de negócios

Sanções

Em Caso de Violação

- Medidas disciplinares, como dispensa, advertência, suspensão, justa causa.
- Processo civil e/ou criminal.
- Término ou cessão de contrato de prestação de serviço/relação comercial
- Ressarcimento dos prejuízos e danos

- Sanções estipuladas pela PAY4FUN
- Sanções conforme legislação e códigos de ética, civis e comerciais.