POL-IS-001
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Código	Política de Segurança da Informação	Emissão	Classificação
POL-IS-001		28/01/2025	Uso Público
Versão		**Validade**	**Aprovado por:**
6.0		27/01/2026	Comitê de Riscos

1. OBJETIVO

Estabelecer diretrizes de Segurança da Informação aos colaboradores, terceiros e prestadores de serviços visando assegurar a confidencialidade, integridade e disponibilidade das informações da Monkey ou sob sua responsabilidade. A segurança eficaz é um esforço de equipe que envolve a participação e o apoio de cada funcionário ou contratado da Monkey que lida com informações e/ou sistemas de informação. É responsabilidade de cada membro da equipe ler e compreender esta política e conduzir suas atividades de acordo.

2. ABRANGÊNCIA

Aplica-se a todos os colaboradores, dentro ou fora das dependências da empresa. Inclui terceiros que se relacionam com a Monkey, sejam eles fornecedores, representantes comerciais, prestadores de serviços, coligadas, subsidiárias, entre outros, representados tanto na figura de pessoa jurídica, quanto física. A “Política de Segurança da Informação” da Monkey é composta por esta política e por todas as políticas referenciadas e/ou vinculadas neste documento.

3. RESPONSÁVEL

3.1. Alta Administração

a) Alinhar a Política de Segurança da Informação aos objetivos estratégicos da organização;
b) Patrocinar e demonstrar compromisso com o Sistema de Gestão de Segurança da Informação (SGSI), atuando como líder e exemplo no cumprimento da Política de Segurança da Informação;
c) Prover a alocação de recursos necessários para a execução das atividades de segurança da informação.

3.2. Segurança da Informação

d) Revisar e implementar a Política de Segurança da Informação e Normas complementares;
e) Gerenciar a classificação da informação e assegurar o tratamento adequado conforme seu nível de confidencialidade;
f) Realizar a gestão de acessos, monitorar atividades e tratar irregularidades identificadas;
g) Prover Treinamento e Conscientização de Segurança da Informação;
h) Apoiar os gestores em novos projetos, orientando nos quesitos de segurança da informação;
i) Identificar, tratar e monitorar os riscos de segurança da informação;
j) Conduzir o plano de resposta a incidentes de segurança da informação;
k) Assegurar a melhoria contínua do processo de segurança da informação.

3.3. Todos os Colaboradores, Terceiros e Prestadores de Serviços

a) Tomar conhecimento da Política de Segurança da Informação e exercê-la em sua integridade; e
b) Assinar e cumprir o Termo de Confidencialidade, protegendo informações sensíveis e evitando divulgações não autorizadas;
c) Reportar imediatamente quaisquer incidentes ou situações de risco de segurança da informação;
d) Utilizar os recursos tecnológicos e sistemas de informação exclusivamente para fins autorizados.

3.4. Todos os Gestores

a) Encorajar suas equipes no cumprimento da Política de Segurança da Informação e participação em Treinamento de Segurança da Informação;
b) Identificar e comunicar possíveis riscos ou situações de não conformidade em suas áreas de atuação;

c) Apoiar a implementação de controles de segurança específicos em seus processos operacionais;
d) Atuar como ponto focal para questões de segurança da informação em sua área, proporcionando alinhamento com a equipe de Segurança da Informação.

3.5. Comitê de Gestão de Riscos

a) Aprovar formalmente a Política de Segurança da Informação e revisar alterações propostas;
b) Avaliar periodicamente os riscos identificados e acompanhar a eficácia das ações mitigadoras;
c) Analisar situações adversas, incluindo incidentes ou descumprimentos desta política, recomendando ações corretivas ou preventivas;
d) Monitorar a eficácia da gestão de segurança da informação através de relatórios regulares;
e) Fornecer suporte estratégico para decisões relacionadas a riscos de segurança da informação.

4. TERMOS E DEFINIÇÕES

INTEGRIDADE - assegurar que a Informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

CONFIDENCIALIDADE - assegurar que o acesso à Informação seja obtido somente por pessoas autorizadas.

DISPONIBILIDADE - assegurar que os usuários autorizados obtenham acesso à Informação e aos ativos correspondentes sempre que necessário.

PRIVACIDADE - assegurar o manuseio adequado dos dados referentes ao acesso, consentimento, aviso, sensibilidade e em atendimento a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) e outras leis aplicáveis.

DISPOSITIVO MÓVEL - Todo dispositivo que permita o acesso remoto a qualquer dado da Monkey, incluindo, mas não se limitando à smartphone, tablet, pen drive, HD externo e notebook.

COLABORADOR – Refere-se a todo e qualquer conselheiro, administrador, diretor e funcionário que compõe o quadro da Monkey.

GESTOR – Colaborador que exerce cargo de gestão e liderança na Monkey.

GESTOR DE CONTA DE USUÁRIO - É aquele que é o responsável por gerenciar as Informações ou Informações Confidenciais, bem como sua distribuição e autorizações de acesso para dada Conta de Usuário, sendo que no caso de uma Conta de Colaborador será o seu gestor imediato e no caso de uma Conta de Terceiro será o Gestor do Contrato.

INFORMAÇÃO – É todo e qualquer dado, informação, elemento, notícia, comunicação, material, instrução ou direção que sejam disponibilizados por escrito, oralmente ou de qualquer outra forma, gravados ou não, com a expressão "confidencial" ou não pelo Usuário final, em decorrência do desenvolvimento das atividades profissionais da Monkey.

INFORMAÇÃO CONFIDENCIAL - Dados ou informações da Monkey, informações de natureza técnica, comercial, financeira, jurídica, estratégica, tecnológica, know-how, desenhos, modelos, dados, cadastros, especificações, relatórios, compilações, análises, previsões, estudos, reproduções, sumários, comunicados, fórmulas, patentes, dados financeiros e econômicos, informações relacionadas a clientes, fornecedores atuais ou potenciais, operações financeiras, planos comerciais, demonstrações ou planos financeiros, estratégias de marketing e outros negócios, contratos, produtos existentes ou futuros e quaisquer outras informações de propriedade da Monkey reveladas em confiança para o Colaborador.

RECURSOS DE TECNOLOGIA DA INFORMAÇÃO - São ferramentas de tecnologia da informação disponibilizadas ao Colaborador ou Terceiro para utilização a serviço da Monkey, tais como, mas não se limitando a: internet, intranet, rede corporativa com seus respectivos diretórios, correio eletrônico (e-mail), notebooks, computadores, impressoras, scanners, softwares e sistemas aplicativos.

TERCEIRO - Refere-se, mas não está limitado, a toda e qualquer pessoa física ou jurídica, que a Monkey se relacione ou venha a se relacionar, como, por exemplo, prestador de serviços, fornecedor, consultor, cliente, parceiro de negócio, terceiro contratado ou subcontratado, locatário, cessionário de espaço comercial, independentemente de contrato formal ou não, incluindo aquele que age em nome da Monkey direta ou indiretamente para qualquer fim ou que presta serviços, fornece materiais, interage com Funcionário Público, com o Governo ou com outros Terceiros em nome da Monkey.

UPLOAD - Envio de dados de um computador local para um computador remoto através da Internet.

USUÁRIO - Qualquer Colaborador, Terceiro Relacionado ou qualquer outra pessoa que venha a ter acesso à Informação ou Informação Confidencial que transitam no âmbito dos Recursos de Tecnologia da Informação da Monkey, seja através de uma Conta de Usuário ou de uma Conta de Terceiro.

5. DIRETRIZES

5.1. Segurança da Informação

Toda informação gerada, armazenada, processada, administrada ou confiada à Monkey é considerada de sua propriedade, estando regulamentada por esta Política de Segurança da Informação e suas Normas complementares, e sujeita à auditoria e monitoramento, visando assegurar que ela seja utilizada por usuários devidamente autorizados, para fins profissionais, no estrito interesse da Monkey.

5.2. Uso de Dispositivos Móveis

Todos os dispositivos usados para acessar sistemas da Monkey (como laptops e celulares) devem seguir a política de segurança, incluindo registro no portal, uso de senhas fortes e bloqueio de tela. É proibido compartilhar dispositivos ou acessos, e qualquer uso indevido ou roubo deve ser reportado ao TI imediatamente. Após o desligamento, dispositivos e dados corporativos devem ser devolvidos ou excluídos.

5.3. Política de Tela Limpa e Mesa Limpa

Os usuários não deverão deixar materiais confidenciais desprotegidos em suas mesas ou áreas de trabalho e garantirão que as telas estejam bloqueadas quando não estiverem em uso.

5.4. Classificação da Informação

Toda informação gerada, armazenada, processada, administrada ou confiada à Monkey deve ser classificada e tratada de modo adequado durante todo seu ciclo de vida, ou seja, manuseio, transmissão, transporte e descarte, seguindo níveis adequados de proteção, de acordo com seu grau de confidencialidade e relevância.

5.5. Treinamento e Conscientização

Todos os colaboradores, terceiros e prestadores de serviços devem receber o treinamento adequado quanto à manipulação da informação e ao uso dos recursos de tecnologia da informação, a fim de assegurar a proteção contra modificação não autorizada, uso indevido, destruição, desvio, acesso ou divulgação não autorizada, preservando a integridade, confidencialidade, disponibilidade da informação.

5.6. Acesso às Informações

O acesso às informações deve ser controlado e o ambiente monitorado com a finalidade de identificar e mitigar vulnerabilidades que possam intensificar riscos e gerar impactos decorrentes de incidentes ou ações má intencionadas.

5.7. Gerenciamento de Projetos

A área de Segurança da Informação deverá ser considerada pelos gestores no gerenciamento de projetos, sob demanda dada a identificação de potenciais riscos ou impactos significativos relacionados à segurança da informação. Os gestores dos projetos são responsáveis por avaliar, no início de cada iniciativa, a necessidade de envolvimento da área de Segurança da Informação, garantindo que as potenciais questões relacionadas à segurança sejam devidamente tratadas, alinhadas às boas práticas e exigências do Sistema de Gestão de Segurança da Informação (SGSI).

5.8. Desenvolvimento Seguro

Os softwares devem seguir codificação segura e passarem por teste de vulnerabilidade antes de migrar do ambiente de desenvolvimento e homologação para o de produção. Esses ambientes devem ser ambientes apartados e a migração para o ambiente de produção deve seguir um processo de gestão de mudanças pré-definido com a finalidade de mitigar riscos.

5.9. Gerenciamento de Riscos

Os riscos de segurança da informação devem ser mapeados, classificados e tratados (mitigados / terceirizados / formalmente aceitos) e monitorados, para assegurar a Confidencialidade, Integridade e a Disponibilidade.

5.10. Gerenciamento de Vulnerabilidades

Periodicamente deve ser efetuada análise de vulnerabilidade para possibilitar a identificação, priorização e correção antes que sejam exploradas.

5.11. Resposta à Incidentes de Segurança da Informação

Incidentes de segurança da informação devem ser tratados integralmente, de forma que sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicado às autoridades apropriadas.

5.12. Melhoria Contínua

A gestão de Segurança da Informação deve objetivar sempre a melhoraria continua através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

5.13. Cumprimento de Leis e Regulamentações

A organização deve buscar atender aos requisitos de segurança da informação definidos por regulamentações, legislações e normas aplicáveis às suas atividades, como a ISO 27001, a Lei Geral de Proteção de Dados (LGPD) e outras regulamentações relevantes ao setor. As mudanças legais e regulatórias devem ser acompanhadas com o

objetivo de alinhar processos e práticas às exigências vigentes, promovendo um ambiente de segurança e conformidade.

6. MEDIDAS DISCIPLINARES

O descumprimento das diretrizes estipuladas nesta Política caracteriza uma situação de não conformidade e para tanto, deverá ser apontada através da comunicação ao Compliance ou ao Comitê de Riscos. Tal fato será objeto de avaliação e poderá levar à aplicação de medidas disciplinares e administrativas pela Monkey.

Aquele que adotar ações de retaliação contra qualquer pessoa que tenha, em boa-fé, suscitado questões ou preocupações de conformidade com esta política estará sujeito às mesmas sanções disciplinares.

7. CONFIDENCIALIDADE

Este documento é público para conhecimento das partes interessadas com referência ao comprometimento da Monkey com a Segurança da Informação, no entanto não pode ser reproduzido parcial ou integralmente sem autorização prévia.