FLEETCOR®

Política de Segurança da Informação e Cibernética

GIS – Global Information Security

Agosto/2022

Sumário

1. OBJETIVO

A Política de Segurança da Informação e Cibernética da Fleetcor tem como objetivo estabelecer as diretrizes e responsabilidades sobre os principais temas de segurança da informação e cibernética, bem como definir os princípios fundamentais que formam a base para as Normas de Segurança da Informação tais como a elaboração de processos, padrões e procedimentos.

A segurança da informação na Fleetcor visa a proteção das informações contra diversos tipos de ameaças e vulnerabilidades, garantindo confidencialidade, integridade, disponibilidade, privacidade, conformidade dos dados e informações.

2. ABRANGÊNCIA

Esta política se aplica a todos os Colaboradores e unidades de negócios da Fleetcor no Brasil.

As informações cobertas por esta política incluem todas aquelas Tratadas pela Fleetcor, ou seja, informações que são criadas, armazenadas, processadas ou compartilhadas por quaisquer meios.

3. PRINCIPAIS DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

- Todo e qualquer Colaborador, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações e deve cumprir as determinações deste documento, de leis, normas e demais padrões de segurança da informação definidos pela Fleetcor e documentados por meio das Política de segurança da Informação

- Informações na Fleetcor devem ser classificadas de acordo com seu valor, requisitos legais, sensibilidade e criticidade. Para estas recebem o nível adequado de proteção afim de evitar a modificação ou a divulgação não autorizada. As informações podem ser classificadas como: confidenciais, restritas, internas ou públicas.

- Todos os Colaboradores devem tratar as informações da Fleetcor de acordo com seu nível de classificação de forma a protegê-las contra acessos indevidos ou divulgação não autorizada, mantendo sua confidencialidade, integridade e disponibilidade.

- Independente dos meios onde a Informação esteja armazenada ou transmitida, cada Colaborador é responsável por assumir um comportamento seguro e proativo impedindo a divulgação indevida ou vazamento desta informação para pessoas ou entidades externas.

- O acesso a qualquer sistema tecnológico deve ser autenticado, ou seja, protegido por credenciais de acesso, certificados, tokens ou qualquer outro método seguro de identificação e autenticação.

- As credenciais de acesso a sistemas e informações, compostas por usuário e senha, são concedidas pela Fleetcor aos Colaboradores e o seu compartilhamento ou empréstimo não é permitido.

- O acesso as informações ou sistemas devem ser revisados periodicamente, seguindo os critérios de segregação da função e observando os princípios de real necessidade de acesso e concessão do menor nível de privilégios.

- O uso da marca, nome ou citação de qualquer empresa da Fleetcor deve cumprir os requisitos de autorização por direito de imagem e propriedade.

- O desenvolvimento de software deve seguir as recomendações e boas práticas de mercado para o desenvolvimento seguro.

- Para garantir a segurança física dos ambientes, devem ser implementados medidas de segurança que evitem o acesso não autorizado e qualquer tipo de ameaça que possa ocasionar a indisponibilidade dos ativos de informação.

- A Política de Segurança da Informação e Cibernética da Fleetcor é revisada anualmente ou quando houver mudanças significativas que justifiquem alterações pontuais.

3.1. Resposta a Incidentes de Segurança da Informação

A resposta a incidentes de segurança da informação é governada pelo departamento de Segurança da Informação de acordo com as boas práticas de SI e detalhado na Norma específica para o tema.

A Fleetcor considera fundamental que os Colaboradores informem imediatamente ao departamento de Segurança da Informação caso tenham conhecimento de violações de políticas, anomalias ou outros sinais que possam indicar a ocorrência de um incidente de segurança. Esta comunicação e principalmente a velocidade em que ela é feita pode minimizar drasticamente impactos decorrentes e incidentes de segurança.

3.2. Continuidade de Negócios

Em acordo com as necessidades do negócio, a Fleetcor possui planos de continuidade de negócios, planos de recuperação de desastres e planos de gestão de crises, todos pautados e priorizados por análises de impactos nos negócios.

4. CONSIDERAÇÕES FINAIS

Os Colaboradores são legalmente responsáveis por todas as atividades realizadas com as credenciais de acesso (usuário e senha) concedidas para seu uso, portanto devem garantir a segurança destas credenciais e que não sejam usadas por outros.

Os Colaboradores não podem alegar desconhecimento das políticas, normas e padrões que compõem a Política de Segurança da Informação, pois seu conteúdo é publicado em locais de fácil acesso, divulgado pelos canais oficiais da Fleetcor e reforçado por campanhas de conscientização em segurança da informação.

É da responsabilidade de cada Colaborador conhecer esta política, as demais políticas de segurança e as políticas do programa de privacidade da Fleetcor, assim como realizar suas atividades em conformidade com elas.

A Fleetcor reserva-se o direito de notificar as autoridades competentes, responsáveis pela aplicação da lei, sobre qualquer atividade ilegal e cooperar em qualquer investigação de tal atividade.

5. CONTROLE DE VERSÃO

Este documento deve ser revisado anualmente ou quando houver mudanças significativas que justifiquem alterações pontuais.

VERSÃO	DATA	ALTERAÇÕES	REVISORES	APROVADORES
1.0	**08/2022**	Criação do documento	Andre Nogueira Rodrigues / Fernanda Cordeiro Genu	Alain Deberdt