

Política de Segurança BYOD - Aggrandize

Políticas corporativas

AGGRANDIZE TECNOLOGIA DA INFORMAÇÃO LTDA

VERSÃO 1.0

25 de outubro de 2021

Criação: Dartagnan Farias

Política de Segurança BYOD - Aggrandize

Políticas corporativas

1. Introdução

Colaboradores que utilizam Dispositivos de Propriedade Pessoal (DPP) para fins de trabalho necessitam de autorização para tal, precisam garantir a segurança de dados corporativos e não podem expor as redes que estão conectados a riscos de segurança (malwares) através de vulnerabilidades nos seus equipamentos.

Esta política é complementar a Política de Segurança da Informação da Aggrandize. O aceite dos termos desta política subentende-se a conformidade com a Política de Segurança da Informação da Aggrandize.

2. Aplicabilidade

Colaboradores que utilizam Dispositivos de Propriedade Pessoal (DPP) para fins de trabalho necessitam de autorização para tal, precisam garantir a segurança de dados corporativos e não podem expor as redes que estão conectados a riscos de segurança (malwares) através de vulnerabilidades nos seus equipamentos.

Esta política é complementar a Política de Segurança da Informação da Aggrandize. O aceite dos termos desta política subentende-se a conformidade com a Política de Segurança da Informação da Aggrandize.

A Política de Segurança BYOD (Bring Your Own Device) da Aggrandize define diretrizes e atribuições para colaboradores que utilizam Dispositivos de Propriedade Pessoal (DPP) para fins de trabalho.

Para os fins desta política, são considerados Colaboradores da Aggrandize todos os funcionários integrantes do quadro de pessoal, os estagiários, os sócios, os diretores e demais prestadores de serviço. Também são considerados colaboradores, aqueles que estejam em licença, férias ou por outro motivo afastado. Entende-se por recursos computacionais todos e quaisquer recursos de software ou hardware utilizados para acesso a dados, informações e sistemas de informações.

3. Riscos de Segurança

Colaboradores autorizados a utilizar DPP para fins de trabalho atuam na modalidade BYOD. BYOD é associada a riscos de segurança da informação tais como:

- I. Perda, exposição ou corrompimento de dados corporativos salvos no DPP;
- II. Incidentes de segurança envolvendo ameaças, ou comprometimento da infraestrutura de rede corporativa e outros recursos computacionais;
- III. Não conformidade com leis, regulamentações e obrigações (ex.: privacidade ou pirataria);
- IV. Direitos de propriedade intelectual para informações corporativas criadas, armazenadas, processadas ou comunicadas em DPP no decorrer do trabalho para a Aggrandize.

Os colaboradores que irão aderir ao BYOD necessitam, obrigatoriamente, de autorização e também necessitam aceitar explicitamente os requisitos desta política de antemão.

A Aggrandize reserva-se ao direito de não autorizar a adesão ao BYOD se considerar que não é apropriado, de acordo com a atividade do colaborador. Nestes casos, a Aggrandize disponibiliza recursos computacionais para a realização do trabalho de forma profissional.

4. Objetivos

Objetivo desta política:

- I. Orientar os Colaboradores da Aggrandize quanto às práticas de segurança da informação na modalidade BYOD.

5. Diretrizes de uso de DPP na modalidade BYOD

- I. A utilização de dispositivos móveis BYOD deve ser solicitada e formalizada pelo gestor da área ou superior;
- II. Dados corporativos só podem ser criados, processados e armazenados em DPP que estiverem inseridos no MDM (Mobile Device Management) da Aggrandize;
- III. Não é permitida a instalação de licenças corporativas em dispositivos móveis BYOD;

- IV. O DPP deve possuir método apropriado de autenticação de usuário aprovado pelo Departamento de Tecnologia da Informação da Aggrandize e não deve ser compartilhado. (Senha, certificados, biometria, etc.);
- V. O DPP deve possuir método de criptografia para transferir dados na rede, (SSL ou VPN) e também em dados armazenados em disco local ou qualquer outra tecnologia de armazenamento externo ligado ao DPP. (Ex.: bitlocker);
- VI. Não infringir a privacidade dos outros colaboradores, como por exemplo utilizar recursos de gravação de tela não autorizada;
- VII. A Aggrandize não se responsabilizará pelo reembolso ou percentagem dos DPP nos casos de roubo, furto, uso indevido, defeito e condutas assemelhadas;

6. Disposições finais

Esta política deve ser objeto de atualização periódica, no mínimo a cada 2 anos, objetivando refletir as alterações ocorridas nos ambientes interno e externo da Aggrandize.

7. Termo de compromisso para usuários de recursos computacionais

Nome do Colaborador:

CPF/CNPJ: _____

Entendo que a Política de Segurança BYOD tem o objetivo principal de assegurar a segurança dos dados, informações e sistemas de informações da Aggrandize.

Comprometo-me a preservar a integridade, a disponibilidade e a confidencialidade das informações obtidas junto a AGGRANDIZE, mesmo após o término da prestação de serviço permanente ou temporária.

Declaro estar ciente de que o descumprimento do conteúdo da Política de Segurança BYOD poderá resultar em medidas preventivas e punitivas.

A assinatura do Termo de compromisso é expressão de que recebi, li e compreendi todas as normas constantes na Política de Segurança da Informação da Aggrandize.

Local/Data: _____, ____/____/____

Assinatura do colaborador

Observação: Este termo pode ser enviado por e-mail ao Colaborador, juntamente com o conjunto de políticas corporativas. Após leitura e análise do código e das políticas o Colaborador deve sinalizar, por e-mail, o de acordo com o constante nos mesmos.