Normas de Segurança da Informação

AgaTrend Indústria e Comércio Ltda.

Políticas e diretrizes para proteção de ativos de informação, sistemas e dados

1. Propósito

A AgaTrend Indústria e Comércio Ltda. estabelece estas Normas de Segurança da Informação para proteger ativos de informação, sistemas, pessoas e processos contra acessos não autorizados, danos, uso indevido ou perda de dados. A segurança da informação é essencial para a continuidade dos negócios, para o cumprimento de requisitos legais e regulatórios (incluindo a LGPD – Lei Geral de Proteção de Dados Pessoais) e para a confiança de clientes, colaboradores e parceiros.

2. Âmbito de Aplicação

Estas normas se aplicam a todos os colaboradores, prestadores de serviço, terceirizados, parceiros, fornecedores e quaisquer pessoas que tenham acesso direto ou indireto aos sistemas, informações ou infraestrutura da empresa, independentemente do local físico ou tecnológico de atuação.

O diagrama ilustra o amplo alcance das Normas de Segurança da Informação, abrangendo todas as partes interessadas que interagem com os ativos da AgaTrend Indústria e Comércio Ltda.

3. Ativos de Informação

Ativos de informação incluem dados, documentos, sistemas, equipamentos, redes, aplicações e qualquer recurso que contenha ou processe informações relevantes à operação da empresa. Todos os ativos devem ser classificados conforme sua criticidade, sensibilidade e necessidade de proteção.

- Dados
- Documentos
- Sistemas
- Equipamentos
- Redes
- Aplicações

4. Princípios de Segurança

A proteção das informações na AgaTrend é orientada pelos pilares da segurança da informação:

Confidencialidade

garantir que a informação esteja acessível apenas a pessoas autorizadas

Integridade

assegurar que a informação seja precisa, completa e não seja alterada indevidamente

Disponibilidade

assegurar que a informação esteja acessível quando necessária para as atividades da empresa

5. Gestão de Acesso

O acesso aos sistemas e informações da AgaTrend será concedido com base no princípio do mínimo privilégio, ou seja, cada pessoa terá acesso apenas ao que necessitar para cumprir sua função. Senhas, autenticação multifatorial e controles de acesso deverão ser utilizados para reforçar a proteção.

- Mínimo Privilégio
- Senhas Fortes
- Autenticação Multifatorial
- Controles de Acesso

AGA TREND

6. Proteção de Dados Pessoais

Dados pessoais e sensíveis tratados no contexto das atividades da empresa devem ser protegidos conforme as exigências da LGPD (Lei nº 13.709/2018), adotando práticas que evitem vazamentos, uso indevido, alteração ou divulgação sem autorização, e garantindo consentimento e transparência quando aplicáveis.

- Consentimento
- Transparência
- Segurança
- Privacidade

7. Segurança em Infraestrutura e Redes

A infraestrutura de TI da AgaTrend deverá ser mantida com mecanismos de segurança que minimizem ameaças externas e internas, incluindo:

- Firewalls e segmentação de rede
- Antivírus e proteção contra malwares
- Monitoramento de eventos anômalos
- Atualizações regulares de sistemas e aplicações

AGA TREND

8. Uso de Dispositivos e Recursos da Empresa

Equipamentos corporativos (computadores, dispositivos móveis, storage, etc.) e sistemas internos só podem ser utilizados para finalidades autorizadas pela empresa. O armazenamento de dados pessoais ou corporativos em plataformas não autorizadas é proibido.

- Computadores
- Dispositivos Móveis
- Storage
- Sistemas Internos

9. Resposta a Incidentes

AgaTrend adotará processos estruturados para identificar, registrar, responder e corrigir incidentes de segurança da informação, mitigando impactos e reportando os fatos conforme exigido pelo compliance interno e, quando necessário, às autoridades competentes.

Identificar

Detectar e reconhecer a ocorrência de um incidente de segurança.

Registrar

Documentar todos os detalhes do incidente para análise e auditoria.

Responder

Tomar ações imediatas para conter e erradicar o incidente.

Corrigir

Implementar medidas para prevenir a recorrência do incidente.

10. Treinamento e Conscientização

Todos os colaboradores e partes autorizadas que utilizem ativos de informação da empresa deverão ser periodicamente treinados em práticas de segurança, políticas internas e comportamentos que reduzam riscos.

- Práticas de Segurança
- Políticas Internas
- Comportamentos Seguros
- Conscientização Contínua

11. Conformidade e Penalidades

O não cumprimento destas normas pode expor a empresa e seus colaboradores a riscos legais, operacionais ou financeiros. Violações podem resultar em medidas disciplinares, incluindo advertências, restrições de acesso, ou outras ações compatíveis com a legislação e a política interna.

- Riscos Legais
- Riscos Operacionais
- Riscos Financeiros

Possíveis medidas disciplinares em caso de violação:

Advertências
Notificações formais sobre o descumprimento das normas.

Restrições de Acesso
Limitação ou suspensão do acesso a sistemas e informações.

Outras Ações
Medidas compatíveis com a legislação vigente e a política interna da empresa.

12. Atualizações e Governança

Estas normas serão revisadas periodicamente, considerando mudanças tecnológicas, legais ou organizacionais, para garantir que os mecanismos de proteção acompanhem as melhores práticas do campo de segurança da informação e a evolução normativa internacional.

- Revisão Periódica
- Mudanças Tecnológicas
- Conformidade Legal
- Melhores Práticas

Seu Compromisso com a Segurança

A segurança da informação é responsabilidade de todos. Cada colaborador da AgaTrend tem o dever de conhecer, compreender e cumprir estas normas, contribuindo para a proteção dos ativos da empresa, dos dados de clientes e parceiros, e da reputação organizacional.

Dúvidas ou relatos de incidentes devem ser comunicados imediatamente ao departamento de TI ou à área de Compliance.

- Responsabilidade Compartilhada
- Proteção de Ativos
- Reputação Corporativa

AGA TREND