POLITICA DE SEGURANÇA DA INFORMAÇAO

1. INTRODUÇAO

1.1. A SECURITY tem como missão levar tranquilidade aos clientes, através de soluções integradas e especializadas em segurança e serviços.

1.2. A SECURITY entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos produtos ofertados a seus clientes.

1.3. A SECURITY compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

1.4. Dessa forma, a SECURITY estabelece sua Política Geral de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

2. PROPOSITO

2.1. Esta política tem por proposito estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores da SECURITY adotar padrões de comportamento seguro, adequados às metas e necessidades;

2.2. Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

2.3. Resguardar as informações da SECURITY, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

2.4. Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros;

2.5. Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da SECURITY como resultado de falhas de segurança.

3. ESCOPO

3.1. Esta política se aplica a todos os usuários da informação da SECURITY, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com a SECURITY, tais como empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores, que

possuíram, possuem ou virão a possuir acesso às informações da SECURITY e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura SECURITY.

4. POLITICA DE PRIVACIDADE

4.1. As políticas de privacidade e proteção de dados da SECURITY estão disponíveis no endereço (https://www.sousecurity.com.br/pt-br/lgpd) e estão vinculadas a esta Política.

5. DOCUMENTOS COMPLEMENTARES

Código do Documento	Descrição	Propósito
T-SI-001	Termo de uso dos sistemas internos	O Termo de uso de sistemas internos complementa a Política Geral de Segurança da Informação, definindo as regras de utilização dos sistemas disponibilizados pela SECURITY e coletando o consentimento do usuário em relação as regras.
N-SI-001	Norma para acesso remoto	A Norma de segurança da informação N-SI-001 complementa Política Geral de Segurança da Informação, definindo as diretrizes para o acesso remoto a ativos/serviços de informação e recursos computacionais, garantindo níveis adequados de proteção aos mesmos
N-SI-003	Norma para uso de serviços de e-mail e comunicadores instantâneos	A Norma de segurança da informação N-SI-003 complementa Política Geral de Segurança da Informação, definindo as diretrizes para utilização segura dos serviços de e-mail e comunicadores instantâneos

N-SI-004	Norma para gestão da identidade	A Norma de segurança da informação N-SI-004 complementa Política Geral de Segurança da Informação, definindo as diretrizes para gestão de identidade e acesso aos ativos e sistemas de informação

6. DIRETRIZES

6.1. O objetivo da gestão de Segurança da Informação da SECURITY é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a instituição.

6.2. A Alta Direção está comprometida com uma gestão efetiva de Segurança da Informação na SECURITY. Desta forma, as medidas cabíveis para garantir que esta política seja adequadamente comunicada são adotadas, entendidas e seguidas em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades da SECURITY.

6.3. E política da SECURITY:

6.3.1. Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;

6.3.2. Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: Empregados, terceiros contratados e, onde pertinente, clientes.

6.3.3. Garantir a educação e conscientização sobre as práticas adotadas de segurança da informação para Empregados, terceiros contratados e, onde pertinente, clientes.

6.3.4. Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

6.3.5. Tratar integralmente incidentes de segurança da informação, garantindo que eles sejam adequadamente registrados, classificados, investigados,

corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;

6.3.6. Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;

6.3.7. Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

7. PAPEIS E RESPONSABILIDADES

7.1. Comitê Diretivo – Foco em Segurança da Informação e Privacidade

7.1.1. A SECURITY possui um Comitê Diretivo formado, com foco em Segurança da Informação.

7.1.2. E responsabilidade do Comitê Diretivo:

7.1.2.1. Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;

7.1.2.2. Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;

7.1.2.3. Garantir que as atividades de segurança da informação sejam executadas em conformidade com a PGSI;

7.1.2.4. Promover a divulgação da PGSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da SECURITY.

7.2. GESTAO DA SEGURANÇA DA INFORMAÇAO

7.2.1. E responsabilidade da Gestão da Segurança da Informação:

7.2.1.1. Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do Comitê Diretivo;

7.2.1.2. Apoiar o Comitê Diretivo em suas deliberações;

7.2.1.3. Elaborar e propor ao Comitê Diretivo as normas e procedimentos de segurança da informação, necessários para se fazer cumprir esta Política de Segurança da Informação;

7.2.1.4. Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

7.2.1.5. Tomar as ações cabíveis para se fazer cumprir os termos desta política;

7.2.1.6. Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

7.3. GESTORES

7.3.1. E responsabilidade dos Gestores:

7.3.1.1. Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela SECURITY;

7.3.1.2. Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela SECURITY;

7.3.1.3. Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem delas conforme necessário;

7.3.1.4. Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

7.3.1.5. Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela SECURITY.

7.4. USUARIOS

7.4.1. E responsabilidade dos Usuários:

7.4.1.1. Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

7.4.1.2. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos a Gestão da Segurança da Informação ou, quando pertinente, ao Comitê Diretivo;

7.4.1.3. Comunicar à Gestão da Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da SECURITY;

7.4.1.4. Assinar o Termo de Uso da Informação da SECURITY, formalizando a ciência e o aceite integral das disposições da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

7.4.1.5. Responder pela inobservância da Política Geral de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

8. PRINCIPIOS DA SEGURANÇA DA INFORMAÇAO

8.1. Confidencialidade

Toda informação deverá ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.

8.2. Integridade

Toda informação deverá ser mantida na condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.

8.3. Disponibilidade

Garantia de que os colaboradores autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

8.4. Autenticidade

Garantir que as informações não sejam passíveis de alteração e ou capturada quando ela é trafegada do seu ponto de origem até o seu ponto de destino.

9. TRATAMENTO DA INFORMAÇAO

9.1. Perfis de acessos por Função

Os sistemas de informação que geram dados tipo Confidencial e tipo Uso Interno deverão estabelecer segregação de funções, com objetivo de minimizar riscos de uso indevido acidental ou deliberado dos sistemas de

informação da SECURITY. Os Perfis por Função deverão estabelecer os seguintes controles:

9.1.1. Convêm que sejam tomados os cuidados para impedir que uma pessoa possa acessar, modificar ou usar ativos sem a devida autorização ou detecção.

9.1.2. Convêm que, o início de um evento seja separado de sua autorização. Quem gera o evento não pode aprovar.

9.1.3. Convêm que, a possibilidade de existência de conluio seja mitigada antes da criação dos perfis.

9.1.4. Convêm que, caso haja dificuldades de segregação por características do próprio negócio seja estabelecido controles específicos como, monitoração de atividades, auditorias específicas e acompanhamento gerencial.

9.2. As ferramentas de segregação da informação deverão ser parametrizadas de forma que garantam o acesso as informações conforme sua classificação. Estas ferramentas deverão ter:

9.2.1. Planejamento dos Perfis por Função em conjunto com RH;

9.2.2. Processo de revisão de acesso periódicos;

9.2.3. Matriz de responsabilidade dos Perfis;

9.2.4. Processo de criação de novos Perfis por Função;

9.2.5. Desenvolver transações específicas para que sejam utilizadas pelos diversos perfis.

10. SANÇOES E PUNIÇOES

10.1. As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

10.2. A aplicação de sanções e punições será realizada conforme a análise do Comitê Diretivo, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o Comitê Diretivo, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

10.3. No caso de terceiros contratados ou prestadores de serviço, o Comitê Diretivo deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

10.4. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a SECURITY, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens 6.1, 6.2 e 6.3 desta política.

11. CASOS OMISSOS

11.1. Os casos omissos serão avaliados pelo Comitê Diretivo para posterior deliberação.

11.2. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da SECURITY adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção das informações.

12. GLOSSARIO

12.1. **Ameaça**: Causa potencial de um incidente, que pode vir a prejudicar a Organização;

12.2. **Ativo:** Tudo aquilo que possui valor para a Organização;

12.3. **Ativo de informação:** Patrimônio intangível da SECURITY, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas à Organização por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da Organização ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

12.4. **Comitê Diretivo – Foco em Segurança da Informação:** Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da Organização, que tem por finalidade tratar questões ligadas à Segurança da Informação.

12.5. **Confidencialidade:** Propriedade dos ativos da informação da Organização, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

12.6. **Controle:** Medida de segurança adotada pela Organização para o tratamento de um risco específico.

12.7. **Disponibilidade:** Propriedade dos ativos da informação da Organização, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

12.8. **Gestor:** Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

12.9. **Incidente de segurança da informação:** Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da Organização.

12.10. **Integridade:** Propriedade dos ativos da informação da Organização, de serem exatos e completos.

12.11. **Risco de segurança da informação:** Efeito da incerteza sobre os objetivos de segurança da informação da Organização.

12.12. **Segurança da informação:** A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da Organização.

12.13. **Usuário:** Empregados (Colaboradores) com vínculo empregatício de qualquer área da Organização ou terceiros alocados na prestação de serviços, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar ou manipular qualquer ativo de informação da Organização para o desempenho de suas atividades profissionais.

12.14. **Vulnerabilidade:** Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da Organização.

13. REVISOES

13.1. Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê Diretivo – Foco em Segurança da Informação.

13.2. Controle de Revisões:

DATA DA REVISAO	AUTOR	O QUE FOI MODIFICADO

14. GESTAO DA POLITICA

14.1. A Política Geral de Segurança da Informação é aprovada pelo Comitê Diretivo, em conjunto com a Diretoria da SECURITY.

14.2. A presente política foi aprovada no dia 17/06/2021.