

MAA – DSM – Segurança no Desenvolvimento de Aplicações (DAS)

Equipe de Trabalho: MoveSmart	
Participante	Função
Nilton Dionisio Guerra	Desenvolvedor

Trabalho da Equipe
ELABORAÇÃO DE UM MODELO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
Empresa MoveSmart

SUMÁRIO

1	Revisão e atualização da política.....	4
1	Controle de versões	4
2	Introdução	4
2.1	Objetivo do documento.....	4
2.2	Escopo de aplicação.....	4
3	Responsabilidades	4
3.1	Diretoria.....	5
3.2	Equipe de TI	5
3.3	Funcionários/parceiros/usuários	5
3.4	Responsabilidades da função de provisionamento	5
3.5	Responsabilidades dos proprietários de ativos.....	6

3.6	Responsabilidades do usuário	6
4	Princípios gerais	7
4.1	Princípios orientadores	7
5	Definições e termos	7
6	Educação e conscientização	7
6.1	Treinamento	7
6.2	Conscientização	8
7	Conformidade	8
7.1	Legislação e regulamentos	8
7.2	Políticas e regras internas	8
7.3	Referências bibliográficas	8
8	Controle de Acesso	8
8.1	Autenticação	8
8.2	Controles de medidas de segurança	9
	Autorização	9
9.1	Cadastro de usuário	9
9.2	Cancelamento do registro de usuário	9
9.3	Provisionamento de acesso de usuário	10
9.4	Remoção ou ajuste de direito de acesso	10
9.5	Gestão de direitos de acesso privilegiado	10
9.7	Autenticação de usuários, senhas e credenciais	11
9.8	Utilização de senhas e credenciais	11
9.9	Procedimentos de criação de conta	12
	Proteção de Dados	Erro! Indicador não definido.
10	Rede	12
11	Criptografia	12
12	Backup	12
	Gerenciamento de Vulnerabilidades	12
13	Atualizações e Patches	12
14	Testes de Penetração	13
14.2	Controles de medidas de segurança	13
15	Monitoramento e Auditoria	14
15.1	Monitoramento Contínuo	14
15.2	Auditoria	14

16 Resposta a Incidentes..... 15

16.1 Plano de Resposta a Incidentes 15

16.2 Comunicação de Incidentes 15

17 CONFORMIDADE 15

Aprovações..... 16

Anexos:..... 17

Anexo A: Contatos de Segurança..... 18

Anexo B: Glossário de termos..... 19

Anexo C: Referências Bibliográficas 20

1 Revisão e atualização da política

A fim de assegurar a contínua relevância e eficácia da presente política, será realizada uma revisão sistemática a cada seis meses. Ademais, qualquer alteração significativa no código de proteção de dados do país em que o sistema estiver operando acarretará uma revisão imediata e abrangente desta política. Esta prática assegura que a política permaneça em conformidade com as regulamentações vigentes e que permaneça adequadamente alinhada com as melhores práticas de segurança da informação.

Controle de versões

Versão	Data	Autor	Notas da Revisão
0	06/06/2024	nilton	
1	20/06/2024	Nome do grupo	

2 Introdução


2.1 Objetivo do documento

O propósito desta política é definir diretrizes e procedimentos para resguardar os ativos de informação da Empresa MoveSmart, assim como também de todos os seus parceiros e clientes contra ameaças, assegurando a confidencialidade, integridade e disponibilidade das informações.

2.2 Escopo de aplicação

Esta política é válida para todos os funcionários, contratados, parceiros e clientes e fornecedores e outras partes que possuam acesso aos sistemas e informações da Empresa MoveSmart.

3 Responsabilidades

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

A lista de contatos com os responsáveis pela segurança encontra-se no Anexo A: Contatos de Segurança.

3.1 Diretoria

A diretoria será responsável por aprovar e apoiar a política de segurança da informação, assegurando recursos adequados para sua implementação e manutenção, incluindo a revisão periódica da política.

3.2 Equipe de TI

À equipe de TI cabe implementar e manter medidas de segurança técnica, incluindo a instalação e atualização de softwares em todos os computadores, além de monitorar e responder a incidentes de segurança, bem como também a verificação de possíveis faltas de cumprimento das medidas de segurança por conta dos usuários nesta política de segurança.

3.3 Funcionários/parceiros/usuários

É obrigatório cumprir todas as diretrizes e procedimentos de segurança, bem como relatar imediatamente quaisquer incidentes ou suspeitas de violação de segurança ou corrupção. A omissão de falhas de segurança pode resultar em punições legais de acordo com a lei.

3.4 Responsabilidades da função de provisionamento


Designação da Função de Provisionamento: A equipe de Segurança da Informação é responsável por designar uma “Função de Provisionamento” encarregada das atividades de controle de acesso, de acordo com suas responsabilidades.

Mecanismos de Confirmação de Identidade: Implementar e gerenciar mecanismos de desafio e/ou resposta para confirmar as identidades dos usuários antes de realizar qualquer alteração em suas credenciais.

Manutenção de Lista de Acesso Autorizado: Manter uma lista centralizada de aplicativos, funções e usuários autorizados para acesso, garantindo a conformidade com as políticas de segurança da informação.

Suspensão Oportuna de Acessos: Colaborar com os gerentes de linha para suspender os direitos de acesso aos ativos de forma oportuna, quando necessário, em casos de término de contrato ou outras circunstâncias relevantes.

Procedimento para Concessão de Autorizações: Definir e seguir um procedimento formal para verificar e conceder autorizações de registro de usuário, assegurando a integridade do processo de atribuição de privilégios.

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

Atualização e Encerramento de Conexões de Fornecedores: Atualizar ou encerrar as conexões de fornecedores mediante notificação do proprietário do contrato ou da parte responsável pelo serviço, garantindo a conformidade com os termos acordados.

3.5 Responsabilidades dos proprietários de ativos

Estabelecimento de Regras de Controle de Acesso: Definir, em colaboração com a equipe de "Provisionamento", regras de controle de acesso, direitos específicos e restrições apropriadas para as funções de usuário em seus ativos.

Revisão e Autorização de Solicitações de Acesso: Revisar e formalmente autorizar, em conjunto com a equipe de "Provisionamento", solicitações de acesso aos ativos de informação, assegurando que a autorização seja concedida por uma parte independente do solicitante.

Gerenciamento de Credenciais de Acesso: Trabalhar com a equipe de "Provisionamento" para identificar, remover ou desabilitar regularmente credenciais de acesso redundantes ou desnecessárias.

Estabelecimento de Controles Físicos e Lógicos: Determinar, em colaboração com o departamento de Segurança da Informação, controles físicos e lógicos para seus ativos.

Definição de Controles de Acesso Considerando a Criticidade: Estabelecer controles de acesso considerando a criticidade e o impacto nos negócios, mantendo consistência entre os direitos de acesso e os requisitos de segurança da informação.

Garantia de Conformidade Legal e Contratual: Colaborar com as áreas jurídica, de continuidade de negócios e de conformidade para assegurar que os controles de acesso estejam em conformidade com a legislação e os contratos pertinentes.

Autoridade para Concessão e Revisão de Acessos: Assegurar que a autoridade para conceder, revisar e revogar acessos seja exclusiva do proprietário do ativo ou de uma função designada e autorizada por ele.


Capacitação de Usuários com Contas Privilegiadas: Garantir que os usuários com contas privilegiadas possuam conhecimento técnico suficiente para compreender as implicações do uso de suas contas.

3.6 Responsabilidades do usuário

Compromisso com a Política de Segurança: É fundamental compreender e aderir às declarações estabelecidas nesta política.

Responsabilidade na Proteção de Acesso: Os usuários têm a responsabilidade de desempenhar seu papel na proteção do acesso concedido, garantindo sua integridade e segurança.

Uso Adequado de Contas de Acesso: Certifique-se de que sua conta seja utilizada de forma apropriada e não seja utilizada para fins indevidos ou abusivos em relação à organização.

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

Respeito aos Privilégios e Controles de Acesso: Os usuários não devem modificar ou remover os controles de acesso concedidos, nem tentar elevar seus privilégios, a menos que seja aprovado por canais apropriados.

Reporte de Desvios de Controle: É importante relatar imediatamente qualquer desvio dos controles de segurança descritos neste documento para garantir a pronta correção e a manutenção da conformidade.

4 Princípios gerais

4.1 Princípios orientadores

A. Confidencialidade

Assegurar que as informações sejam acessíveis apenas por pessoas autorizadas.

B. Integridade

Garantir que as informações sejam precisas e completas, protegendo-as contra alterações não autorizadas.

C. Disponibilidade

Assegurar que as informações estejam disponíveis para uso sempre que necessário.


5 Definições e termos

A lista de siglas, definições e termos técnicos específicos utilizados neste documento está disponível no Anexo B: Glossário de Termos.

6. Educação e conscientização

6.1 Treinamento

Será oferecido treinamento regular sobre segurança da informação para todos os funcionários, abrangendo tópicos como phishing, engenharia social e boas práticas de segurança. Além disso, anualmente, os funcionários deverão ler as políticas de segurança da empresa e completar um questionário para comprovar a compreensão do conteúdo. A pontuação mínima para aprovação será de 6 pontos de 10, e caso não seja atingida, será avaliada a continuidade do profissional na empresa.

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

6.2 Conscientização

A empresa disponibilizará esta política para os novos funcionários, garantindo que no primeiro dia de trabalho recebam uma palestra sobre este documento e uma cópia física para leitura, assegurando que estejam cientes e compreendam a política de segurança da informação desde o início de sua jornada na empresa.

7 Conformidade

7.1 Legislação e regulamentos

É obrigatório cumprir todas as leis e regulamentos aplicáveis à segurança da informação, incluindo a LGPD (Lei Geral de Proteção de Dados), regulamentos de compliance, leis anti-corrupção e demais leis pertinentes aos países em que a empresa opera. A política de segurança será revisada e atualizada conforme necessário para garantir a conformidade com essas leis.

7.2 Políticas e regras internas

Será assegurado que todas as políticas internas estejam alinhadas com a política de segurança da informação. As políticas internas serão revisadas e atualizadas periodicamente para garantir esse alinhamento. Entre as principais políticas internas a serem adotadas, destacam-se a proibição de contratação de parentes diretos pelo chefe, como filhos ou cônjuges, e a exigência de que pessoas com acesso a dados sensíveis não tenham histórico criminal.

7.3 Referências bibliográficas


A lista das referências bibliográfica encontra-se no Anexo C: Referência Bibliográficas.

8 Controle de Acesso

8.1 Autenticação

As senhas serão obrigatoriamente formadas por:

- Mínimo 8 caracteres
- Máximo de 16 caracteres
- 2 letras maiúsculas
- 2 letras minúsculas
- 3 caracteres números.

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

Sem a permissão de colocar símbolos.
Permitido repetir caracteres.

Além de que será necessário que a senha seja trocada uma vez a cada 6 meses, sendo que a senha não poderá ser igual a última senha criada.

8.2 Controles de medidas de segurança

A fim de garantir o cumprimento dos requisitos estabelecidos para a criação ou atualização de senhas, será implementada uma máscara de caracteres utilizando REGEX. Essa medida tem como objetivo impedir que o usuário crie uma senha que não esteja em conformidade com os padrões definidos durante o processo de criação ou atualização de senha na tela correspondente; essa máscara em REGEX irá permitir apenas senhas com no mínimo 8 caracteres, 2 letras maiúsculas, 2 minúsculas e 3 números.

9 Autorização

9.1 Cadastro de usuário

Configuração de Senhas Fortes: Todas as contas devem ser configuradas com senhas fortes, conforme definido na política de senhas estabelecida anteriormente.
Identificadores Únicos para Contas de Usuário: Cada conta de usuário será associada a um email de usuário exclusivo, que não é compartilhado com outros usuários e está vinculado a um indivíduo específico.

Processamento de Solicitações com Procedimentos Formais: Todas as solicitações serão processadas de acordo com um procedimento formal, garantindo verificações de segurança apropriadas e obtenção de autorização antes da criação da conta de usuário.


Criação de Contas com Adesão a Princípios de Segurança: A criação de contas de usuário seguirá os procedimentos formais definidos e aderirá aos princípios de "segregação de funções", "necessidade de saber" e "privilegio mínimo".

9.2 Cancelamento do registro de usuário

Suspensão Inicial de Contas de Usuário: As contas de usuário devem ser inicialmente suspensas ou desativadas e não excluídas, a fim de preservar informações de trabalho de ex-colaboradores, se necessário.

Não Reutilização de Email de Conta de Usuário: Os email de conta de usuário não devem ser reutilizados para evitar confusão em investigações posteriores.

Procedimentos de Desativação de Contas: A solicitação para desativação de uma conta deve ser feita pelo próprio usuário, seja ele consumidor ou prestador de

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

serviços. No entanto, caso o usuário seja um colaborador, é dever e responsabilidade da equipe informar sobre o desligamento da empresa.

Suspensão de Acesso ao Deixar a Organização: Quando um funcionário deixa a organização sob circunstâncias normais, seu acesso a sistemas e dados de computador deve ser suspenso no encerramento do expediente no último dia útil do funcionário.

9.3 Provisionamento de acesso de usuário

Atribuição de Direitos de Acesso: Cada usuário receberá direitos de acesso e permissões aos sistemas e dados de computador, alinhados com os requisitos comerciais e os princípios de "privilegio mínimo" e "necessidade de saber".

Gerenciamento de Perfis Baseados em Função: Os perfis baseados em função serão criados, atribuídos e mantidos, com qualquer exceção de particularidade devidamente documentada.

Manutenção Periódica de Funções de Grupo: As funções de grupo serão periodicamente revisadas de acordo com os requisitos de negócios. Todas as alterações serão formalmente autorizadas, documentadas e controladas por meio de um processo de gerenciamento de mudanças.

9.4 Remoção ou ajuste de direito de acesso

Atualizações de Acesso Sob Solicitação: As atualizações de direitos de acesso ou permissões serão realizadas conforme necessário e solicitadas por meio de um processo válido de gerenciamento de mudanças, como em casos de mudança de papel individual.


Remoção de Acessos Desnecessários: É garantido que acessos não mais necessários sejam removidos prontamente das contas de usuário.

9.5 Gestão de direitos de acesso privilegiado

Identificação de Acessos Privilegiados: Os direitos de acesso privilegiado, como aqueles associados a contas de nível de administrador, devem ser claramente identificados para cada ativo.

Restrição do Uso de Contas Privilegiadas: Os usuários técnicos não devem fazer uso diário de contas de usuário com acesso privilegiado.

Atribuição de Acesso Administrativo Qualificado: Acesso a permissões de nível de administrador deve ser atribuído apenas a indivíduos qualificados, cujas funções exijam tal acesso e que tenham recebido treinamento relevante para entender as implicações de seu uso, seja técnico ou não.

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

Mitigação de Riscos em Rotinas Automatizadas: O uso de contas de usuário com acesso privilegiado em rotinas automatizadas, como trabalhos em lote ou de interface, deve ser evitado sempre que possível. Quando necessário, as credenciais de autenticação devem ser protegidas (por exemplo, por meio de criptografia, sem armazenamento de texto não criptografado, e com rotação regular de senhas).

9.6 Revisão de direitos de acesso do usuário

Regularmente, uma pessoa designada conduzirá revisões das contas de usuário com acesso privilegiado para garantir a conformidade com esta política.

Análise Conjunta de Acesso a Ativos e Sistemas: Os proprietários de ativos e sistemas, juntamente com a equipe de Provisionamento, realizarão revisões periódicas para analisar o acesso às suas áreas de responsabilidade e identificar:

- i. Pessoas que não devem ter acesso (por exemplo, abandonando)
- ii. Contas de usuário com excesso de acesso para suas funções
- iii. Alocações de função incorretas em contas de usuário
- iv. Contas de usuário com identificação inadequada, como contas genéricas ou compartilhadas.
- v. Quaisquer outras discrepâncias não conformes com esta política.

9.7 Autenticação de usuários, senhas e credenciais

A autenticação do usuário será feita via senha, como está definido na política de senhas fortes e através de token enviado para o email do usuário, isso se aplicará tanto para o consumidor de serviços, prestador de serviços como também para os colaboradores do sistema.

9.8 Utilização de senhas e credenciais


As credenciais de usuário só podem ser utilizadas pelas pessoas para as quais foram emitidas, não sendo permitido seu uso por terceiros.

Todas as credenciais de sistemas são consideradas informações confidenciais e não devem ser anotadas ou transmitidas sem criptografia. Isso inclui senhas, autenticadores e outras chaves privadas.

A identidade de um usuário deve ser verificada por mecanismos adequados de desafio e resposta antes de qualquer alteração em suas credenciais.

Senhas, chaves SSH e outros autenticadores criptográficos devem ser alterados caso sejam perdidos ou considerados comprometidos.

Quando possível, todas as senhas de sistemas e aplicativos devem seguir uma política de senhas fortes desenvolvida.

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

As senhas não devem ser codificadas ou armazenadas em formato de texto sem formatação em aplicativos de software.

O token criado e enviado para o email do usuário terá validade de 5 minutos. Após esse período, o sistema gerará outro token para acesso à conta.

9.9 Procedimentos de criação de conta

Para criar uma conta, o usuário deverá fornecer seu email. Antes de concluir o processo de registro, será enviado um token via email para o usuário. Este token deverá ser inserido durante o registro para confirmar a veracidade do email fornecido, que será utilizado para enviar futuros tokens. Para acessar o sistema, o usuário deverá sempre fornecer uma senha e utilizar o token enviado via email.

10 Rede

1. Os sistemas e/ou dispositivos não devem ser conectados à rede da MoveSmart sem a autorização prévia do proprietário do ativo da MoveSmart correspondente.
2. A Função de Provisionamento deve ser responsável por manter o controle de acesso à rede e impedir que dispositivos não autorizados acessem a rede.

11 Criptografia

Iremos implementar a criptografia bcrypt para proteger dados em repouso, pois é uma tecnologia amplamente reconhecida e utilizada, com uma comunidade ativa que facilita a correção de possíveis falhas de forma rápida, simples e eficaz. As chaves de criptografia serão gerenciadas de forma segura para garantir a integridade do sistema.


12 Backup

Vamos agendar backups diários para as 4 da manhã, garantindo assim a segurança dos dados críticos e evitando perdas significativas. Essa prática reforça a importância de preservar a integridade e a disponibilidade dos dados.

Gerenciamento de Vulnerabilidades

13 Atualizações e Patches

Vamos disponibilizar patches de segurança obrigatórios para todos os membros da empresa, garantindo a segurança contínua do sistema e evitando possíveis pontos de vulnerabilidade que possam ser explorados por ataques cibernéticos. Essa

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

medida reforça o compromisso com a proteção dos dados e a integridade do sistema.

14 Testes de Penetração

Serão realizados testes de segurança na empresa em um ambiente de Qualidade Assegurada (QA), simulando ataques controlados ao sistema para identificar e corrigir vulnerabilidades. Essa prática permitirá a constante melhoria da segurança da empresa.

Além disso, a cada 6 meses, serão realizados testes internos na empresa para garantir a integridade e a comunicação segura entre as aplicações do sistema. Essas medidas visam fortalecer as defesas da empresa contra possíveis ameaças e garantir a proteção dos dados.

14.1 Mitigação e controle de riscos

Se ocorrerem mais de sete tentativas incorretas de senha ou token, o acesso ao sistema será temporariamente bloqueado por um período de 24 horas. Em caso de recorrência deste bloqueio por mais de 10 vezes, a conta será permanentemente bloqueada como medida de segurança. Para recuperar o acesso à conta após o bloqueio permanente, será necessário entrar em contato com o suporte técnico da empresa para realizar o procedimento de desbloqueio.

Em caso de perda ou esquecimento da senha por parte do usuário, será disponibilizada a opção de recuperação por meio de confirmação do e-mail cadastrado durante a criação da conta. Esta medida visa garantir que os usuários tenham um meio seguro e confiável de restabelecer o acesso à sua conta em situações de perda de senha.

14.2 Controles de medidas de segurança


Com relação ao controle de medidas de segurança irá ser implementado:

Verificação de Identidade durante o Cadastro:

Antes de concluir o processo de registro, será implementada a verificação de identidade por meio do envio de um token via email para o endereço de email fornecido pelo usuário.

O usuário será obrigado a inserir este token durante o processo de cadastramento para confirmar a veracidade do email, fortalecendo assim a autenticidade das informações fornecidas.

Uso de Tokens para Acesso ao Sistema:

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

Para acessar o sistema, os usuários serão obrigados a fornecer uma senha e utilizar um token enviado via email.

O uso de dois fatores de autenticação (senha e token) aumentará a segurança do acesso, mitigando o risco de acesso não autorizado.

Monitoramento e Auditoria:

Será implementado um sistema de monitoramento e auditoria para registrar todas as tentativas de acesso ao sistema, incluindo o uso de tokens.

Os registros de acesso serão revisados regularmente para detectar e investigar atividades suspeitas ou não autorizadas.

Treinamento de Usuários:

Serão fornecidos treinamentos regulares aos usuários sobre a importância da segurança da informação e as melhores práticas para proteger suas credenciais de acesso e informações pessoais.

Atualizações e Revisões:

Esta política será revisada periodicamente para garantir sua conformidade contínua com as melhores práticas de segurança e os requisitos regulamentares aplicáveis.

Alterações significativas no ambiente de ameaças ou na infraestrutura de TI exigirão uma revisão imediata desta política para garantir sua eficácia contínua na proteção dos recursos de informação da organização.


15 Monitoramento e Auditoria

15.1 Monitoramento Contínuo

Para garantir a eficácia das operações, adotaremos o sistema da Kaspersky para controlar os sites e plataformas acessíveis aos funcionários. Além disso, implementaremos sistemas de monitoramento que registram em um banco de dados as informações sobre quem acessou determinado conteúdo. Essas medidas permitirão o monitoramento em tempo real para detectar atividades suspeitas e fortalecer a segurança da empresa.

15.2 Auditoria

A empresa realizará auditorias externas regularmente para garantir o bom funcionamento e a integridade de todo o sistema, visando assegurar que os sistemas operem da melhor forma possível. Os resultados das auditorias serão documentados e revisados para garantir a conformidade com os padrões de segurança estabelecidos.

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

16 Resposta a Incidentes

16.1 Plano de Resposta a Incidentes

Vamos designar uma equipe de correção de bugs para lidar com os incidentes de segurança, priorizando-os de acordo com os critérios de gravidade estabelecidos: muito crítico, crítico e atualizações de segurança para aprimorar o desempenho, definidos pelo próprio time de correção de bugs. Essa abordagem garantirá uma resposta eficiente e organizada a incidentes de segurança.


16.2 Comunicação de Incidentes

Vamos estabelecer um processo para comunicar incidentes de segurança, enviando um e-mail para todos os funcionários envolvidos, a fim de informá-los sobre os problemas de segurança e permitir que se planejem adequadamente para continuar suas atividades diárias. Além disso, notificaremos as partes afetadas e as autoridades relevantes conforme necessário para garantir uma resposta completa e transparente aos incidentes de segurança.

17 Conformidades

Todos os funcionários, prestadores de serviço ou consumidores de serviço devem aderir aos requisitos descritos neste documento, a menos que uma exceção seja identificada e exigida pelos órgãos reguladores aos quais a MoveSmart está sujeita. Qualquer exceção ou desvio à Política de Segurança da Informação e suas diretrizes de suporte deve ser fundamentado em requisitos legislativos ou exclusivos do negócio. Solicitações de exceção à política podem ser encaminhadas ao Diretor de Segurança da Informação para avaliação. Tais solicitações devem ser devidamente documentadas, com uma avaliação de risco relacionada e submetidas ao Líder de Risco de Segurança da Informação ou seu delegado antes da implementação da exceção.

Todas as exceções ou desvios aprovados devem ser registrados e gerenciados no registro de risco e revisados anualmente. A MoveSmart reserva-se o direito de aplicar medidas disciplinares, incluindo demissão, em relação a qualquer desvio da Política de Segurança da Informação ou outras políticas relacionadas. Dependendo da gravidade da violação, pode ser iniciado um processo de acordo com a lei local.


FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

Aprovações

Cargo	Nome/Assinatura	Data
Gerente de segurança	Nilton Dionisio Guerra	

FACULDADE DE TECNOLOGIA DE MAUÁ	Fatec Mauá
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

Anexos:

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	


Anexo A: Contatos de Segurança

Equipe de TI:

1. [Nilton Dionisio Guerra, nilton.guerra@MoveSmart.com, Tel:932313383]

Responsável pela Segurança da Informação:

2. [Nilton Dionisio Guerra, [@MoveSmart.com](mailto:nilton.guerra@MoveSmart.com), Tel: 932313383]

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

Anexo B: Glossário de termos


Bcrypt: biblioteca muito usada para encriptografar senhas em sistemas web

Backend: Refere-se à parte do sistema que opera nos servidores, sendo responsável pelo processamento e armazenamento de dados, bem como pela lógica de negócios e pela interação com o banco de dados. O backend é essencial para a funcionalidade do sistema, porém não é acessível diretamente pelos usuários finais.

Frontend: Corresponde à parte do sistema com a qual o usuário interage diretamente. É responsável pela apresentação dos dados e pela interface com o usuário, incluindo elementos visuais e interativos. O frontend é projetado para oferecer uma experiência de usuário intuitiva e amigável.

Regex (Expressões Regulares): Trata-se de uma anotação criada na programação para inclusão ou exclusão de caracteres, com o objetivo de criar uma máscara de dados ou identificar uma string por meio de características específicas. As expressões regulares são utilizadas para realizar operações de busca, validação e substituição em strings de texto, oferecendo um método poderoso e flexível para manipulação de dados.

Token: Consiste em um objeto digital que contém informações sobre a identidade do principal que faz a solicitação e para que tipo de acesso ele está autorizado. Os tokens são frequentemente utilizados em sistemas de autenticação e autorização para validar e controlar o acesso dos usuários a recursos específicos. Eles fornecem uma forma segura e eficiente de gerenciar a segurança e o controle de acesso em sistemas distribuídos e na web.

FACULDADE DE TECNOLOGIA DE MAUÁ	
POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	

Anexo C: Referências Bibliográficas

PMI, Project Management Institute. Guia PMBOK 7: Conhecimento em Gerenciamento de Projetos. 7ª Ed. PMI, 2022.

- **Legislação e Regulamentações:**
- Legislação de Proteção de Dados: GDPR (Regulamento Geral de Proteção de Dados), LGPD (Lei Geral de Proteção de Dados)
- Regulamentações específicas da indústria: PCI DSS (Padrão de Segurança de Dados para a Indústria de Cartões de Pagamento)
- Políticas Internas: a. Política de Senhas b. Política de Proteção de Dados c. Política de Segurança da Informação
- **Normas e Procedimentos: a. Normas técnicas de segurança da informação:**
- ISO/IEC 27001:2013 - Sistemas de gestão de segurança da informação b. Procedimentos de recuperação de senha:
- Procedimento para recuperação de senha por e-mail: Descrever o processo passo a passo para os usuários recuperarem suas senhas por meio de um e-mail de confirmação. c. Procedimentos de monitoramento de atividade suspeita:
- Procedimento de monitoramento de logs de acesso: Especificar como os logs de acesso são monitorados regularmente para identificar atividades suspeitas. d. Procedimentos de bloqueio de conta:
- Procedimento de bloqueio de conta por tentativas de login malsucedidas: Descrever quando e como uma conta é bloqueada após um número específico de tentativas de login malsucedidas.