[logotipo da organização]

[nome da organização]

Commented [AES1]: Todos os campos desde documento que aparecem entre colchetes devem ser preenchidos.

POLÍTICA DE SENHAS

Commented [AES2]: Não há necessidade de escrever um documento separado para a Política de senhas se as mesmas regras forem descritas na Política de segurança de TI e na Política de controle de acesso.

Código:	
Versão:	
Data da versão:	
Criado por:	
Aprovado por:	
Nível de confidencialidade:	

Commented [AES3]: O sistema de codificação do documento deve estar de acordo com o atual sistema de codificação de documentos da organização. Caso não haja um sistema desse tipo na organização, esta linha pode ser excluída.

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
	0.1	Advisera	Esboço básico do documento

Sumário

1. Finalidade, escopo e usuários

A finalidade deste documento é descrever as regras para garantir o gerenciamento e uso seguros de senhas.

Este documento aplica-se a todo o escopo do Sistema de Gestão da Segurança da Informação (SGSI), isto é, a todos os locais de trabalho e todos os sistemas do escopo do SGSI.

Os usuários deste documento são todos os funcionários da [nome da organização].

Commented [AES4]: Inclua o nome da sua organização.

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas A.5.16, A.5.17 e A.5.18
- Política de segurança da informação
- [Declaração de aceitação de documentos do SGSI]

Commented [AES5]: Você pode encontrar um modelo para este documento na pasta "05_Politicas_gerais" do Kit de documentação ISO 27001.

3. Obrigações do usuários

Commented [AES6]: Exclua esta seção se as regras já forem

Os usuários devem aplicar as seguintes boas práticas de segurança ao selecionar e usar senhas:

Commented [AES7]: Estes são apenas exemplos de melhores

- as senhas não devem ser divulgadas a outras pessoas, incluindo a gestão e os administradores do sistema
- as senhas não devem ser escritas a menos quê um método de segurança tenha sido aplicado por [cargo]
- [redacted]
- [redacted]
- senhas fortes devem ser selecionadas da seguinte forma:
  - use pelo menos 16 caracteres
  - use pelo menos um caractere numérico
  - [redacted]
  - [redacted]
  - uma senha não deve ser uma palavra registrada em dicionário ou que faça parte de um dialeto ou jargão de qualquer idioma, nem qualquer uma dessas palavras escrita ao contrário
  - as senhas não devem ser baseadas em dados pessoais (por exemplo, data de nascimento, endereço, nome de um membro da família, etc.)
  - [redacted]
- as senhas devem ser alteradas a cada três meses
- a senha deve ser alterada no ato da primeira entrada no sistema
- [redacted]

- as senhas usadas para fins particulares não devem ser usadas para fins comerciais

Quando algumas dessas regras escritas acima não puderem ser aplicadas (por exemplo, devido a limitações de sistemas), as práticas mais fortes disponíveis devem ser usadas.

4. Gestão de senhas de usuário

Commented [AES8]: Exclua esta seção se as regras já forem

Ao alocar e usar senhas de usuário, as seguintes regras devem ser seguidas:

Commented [AES9]: Adapte essas regras de acordo com os

Commented [AES10]: Regras em separado devem ser

- assinando a Declaração de aceitação de documentos do SGSI, os usuários também aceitam a obrigação de manter as senhas como confidenciais, conforme indicado neste documento
- os usuários só devem usar seus próprios nomes de usuários exclusivos
- todos os usuários devem ter a opção de escolher sua senha quando aplicável
- a senha temporária usada para a primeira entrada no sistema deve ser exclusiva e forte conforme descrito acima
- as senhas temporárias devem ser comunicadas ao usuário de forma segura e a identidade do usuário devem ser verificadas anteriormente

Commented [AES11]: É possível fornecer mais detalhes aqui.

- o sistema de gestão de senhas deve solicitar que o usuário altere a senha temporária na primeira entrada no sistema
- o sistema de gestão de senhas deve solicitar que o usuário selecione senhas fortes
- o sistema de gestão de senhas deve solicitar que os usuários alterem suas senhas a cada [x] meses

Commented [AES12]: Isso é apenas uma recomendação;

- se o usuário solicitar uma nova senha, o sistema de gestão de senhas deve determinar a identidade do usuário [especifique como]

Commented [AES13]: Por exemplo, com o envio de e-mails

- o sistema de gestão de senhas deve impedir a reutilização das últimas [especifique quantas] senhas anteriores

Commented [AES14]: Por exemplo, três senhas anteriores.

- o usuário deve confirmar o recebimento de senha [especifique como]
- a senha não deve ficar visível na tela durante a entrada

Commented [AES15]: Por exemplo, entrando no sistema

- se um usuário inserir uma senha incorreta três vezes consecutivas, o sistema deve bloquear a conta do usuário em questão
- as senhas criadas pelo fabricante do software ou hardware devem ser alteradas durante a instalação inicial
- os arquivos que contêm senhas devem ser armazenados separadamente dos dados do sistema de aplicativos

5. Validade e gestão de documentos

Este documento é válido a partir de [data].

O proprietário do documento é o [cargo], que deve verificar e, se necessário, atualizar o documento pelo menos [uma vez por ano].

Commented [AES16]: Isso é apenas uma recomendação;

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- [illegible]
- quantidade de incidentes relacionados ao gerenciamento inadequado de senhas

[cargo]
[nome]

_____
[assinatura]

Commented [AES17]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.