

	<b>Política de segurança da informação para Ong de proteção animal</b>  Classificação Interna	PSI-001-2024
		Versão 1.0
		Revisão: 2024

## Sumário

1. INTRODUÇÃO	2
2. OBJETIVOS	2
3. ABRANGÊNCIA	2
4. DIRETRIZES GERAIS	2
4.1 CONTROLE DE ACESSO	3
4.2 CLASSIFICAÇÃO DA INFORMAÇÃO	3
4.3 USO DE RECURSOS DIGITAIS	3
4.4 MESA LIMPA E TELA LIMPA	3
4.5 MONITORAMENTO	3
4.6 PROTEÇÃO DE DADOS (LGPD)	3
4.7 MÍDIAS SOCIAIS	3
4.8 RECURSOS DE TI	3

4.9 ÁUDIOS, VÍDEOS E FOTOS	
.....	3
4.10 DISPOSITIVOS MÓVEIS	
.....	3
4.11 INTERNET	
.....	3
4.12 CORREIO ELETRÔNICO	
.....	3
 5. PAPÉIS E RESPONSABILIDADES	
.....	4
5.1 COLABORADORES E VOLUNTÁRIOS	
.....	5
5.2 GESTORES	
.....	5
6. DISPOSIÇÕES FINAIS	
.....	2

# Política de Segurança da Informação para a ONG de Proteção Animal

## 1. Introdução

Esta Política de Segurança da Informação (PSI) foi elaborada para proteger os ativos tangíveis e intangíveis da nossa ONG de proteção animal. Isso inclui dados de doadores, informações sobre animais, imagens e outros recursos essenciais para o funcionamento da organização.

A aplicação desta política visa garantir a confidencialidade, integridade e disponibilidade das informações e recursos tecnológicos.

## 2. Objetivos

- Estabelecer diretrizes para proteger informações confidenciais e sensíveis relacionadas à ONG.
- Orientar colaboradores e voluntários sobre boas práticas de segurança.
- Prevenir acessos não autorizados e incidentes de segurança.
- Promover uma cultura de uso consciente e seguro de recursos digitais.

## 3. Abrangência

Esta política se aplica a todos os colaboradores, voluntários e parceiros que acessam e utilizam os recursos da ONG, incluindo sistemas de dados, documentos, redes internas e dispositivos.

## 4. Diretrizes Gerais

#### 4.1 Controle de Acesso

- Cada colaborador ou voluntário terá uma identidade digital intransferível para acesso aos sistemas e áreas da ONG.
- O compartilhamento de credenciais é estritamente proibido.
- Devem ser usados mecanismos de autenticação fortes, como senhas seguras e, quando possível, autenticação em duas etapas.

#### 4.2 Classificação da Informação

- Informação Pública: Dados que podem ser divulgados livremente (e.g., campanhas de adoção).
- Informação Interna: Informativos restritos aos colaboradores e voluntários (e.g., relatórios internos).
- Informação Confidencial: Dados sensíveis como informações de doadores e registros de animais resgatados.

#### 4.3 Uso de Recursos Digitais

- Os dispositivos da ONG devem ser usados apenas para atividades relacionadas à proteção animal.
- O armazenamento de arquivos deve ocorrer em repositórios seguros e controlados.
- O uso de mídias sociais deve seguir diretrizes claras que protejam a imagem e a missão da ONG.

#### 4.4 Mesa Limpa e Tela Limpa

- Documentos contendo informações confidenciais não devem ser deixados em áreas comuns ou visíveis em estações de trabalho.
- Monitores devem ser bloqueados ao se afastar da estação de trabalho.

#### 4.5 Monitoramento

- A ONG pode monitorar o uso de recursos digitais para proteger ativos e assegurar o cumprimento desta política.

#### 4.6 Proteção de Dados Pessoais (LGPD)

- Coleta de Dados: Coletar apenas os dados pessoais necessários para as atividades da ONG, garantindo que os titulares dos dados sejam informados sobre a finalidade da coleta.
- Armazenamento de Dados: Armazenar os dados pessoais em ambientes seguros, protegidos contra acessos não autorizados e perdas acidentais.

#### 4.7 Mídias sociais

- Os colaboradores e voluntários devem adotar um comportamento seguro e respeitoso no acesso e utilização das mídias sociais, em conformidade com todos os direitos e deveres estabelecidos pela ONG de adoção de animais.
- A participação institucional do colaborador ou voluntário, por meio de acesso e/ou conexão a mídias sociais a partir do ambiente da ONG e durante o horário de trabalho, deve ser diretamente relacionada à sua função profissional e aos objetivos da ONG. O colaborador ou voluntário é responsável por qualquer ação ou omissão resultante de sua postura e comportamento.

#### 4.8 Recursos de TI

- Acesso aos sistemas de TI da ONG deve ser controlado e restrito a colaboradores e voluntários autorizados, com base em suas funções e responsabilidades.
- Os recursos de TI da ONG, incluindo computadores, redes e dispositivos móveis, devem ser utilizados exclusivamente para atividades relacionadas à missão e objetivos da ONG.

#### 4.9 Áudios, vídeos e Fotos

- Não é permitido tirar fotos, gravar áudio, filmar, publicar e/ou compartilhar imagens das instalações da ONG, incluindo áreas internas e externas, tais como salas de atendimento, áreas de convivência, canis, gatis, e demais espaços

pertencentes ao perímetro físico da ONG, bem como dos animais, adotantes, visitantes, voluntários e colaboradores, sem prévia autorização.

- Toda e qualquer captura de imagens ou gravações deve ser previamente autorizada pela administração da ONG. Esta autorização deve ser obtida por escrito, especificando o propósito e o uso pretendido das mídias.

#### 4.10 Dispositivos Móveis

- O uso de dispositivos móveis no ambiente da ONG é permitido apenas para colaboradores e voluntários autorizados. O uso deve estar diretamente relacionado às atividades e objetivos da ONG.

- O uso de dispositivos móveis para fins pessoais deve ser minimizado durante o horário de trabalho e não deve interferir nas atividades da ONG.

- Tutores autorizados podem usar dispositivos móveis para documentar o processo de adoção, compartilhar atualizações e interagir com a ONG de acordo com as diretrizes estabelecidas. Qualquer captação de imagens ou gravações deve seguir as regras estabelecidas na seção 4.9

#### 4.11 Internet

- Os recursos de conectividade são fornecidos para atender ao propósito administrativo e operacional da ONG, visto que o acesso à internet é essencial para a condução das atividades da organização. No entanto, todos os colaboradores, voluntários e tutores devem fazer uso da internet em estrita observância das leis em vigor, respondendo por qualquer descumprimento.

#### 4.12 - Correio eletrônico

- A utilização do correio eletrônico corporativo da ONG deve se ater à execução das atividades profissionais e operacionais, respeitando as regras de direitos autorais, licenciamento de software, direitos de propriedade e privacidade.

- O correio eletrônico corporativo pode ser utilizado em dispositivos móveis particulares, porém o acesso às mensagens e informações institucionais fora do horário normal de expediente não configura sobrejornada, sobreaviso ou plantão

do colaborador, visto que pode ocorrer por ato de liberalidade e/ou conveniência sem a expressa e prévia requisição da ONG.

## 5. Papéis e Responsabilidades

### 5.1 Colaboradores e Voluntários

- Conhecer e seguir a política de segurança da informação.
- Preservar a confidencialidade das informações.
- Reportar incidentes de segurança imediatamente.

### 5.2 Gestores

- Assegurar que as diretrizes sejam seguidas.
- Orientar e treinar novos colaboradores e voluntários sobre as boas práticas de segurança.

## 6. Disposições Finais

Esta política deve ser revisada periodicamente e estar em conformidade com as leis e melhores práticas de proteção de dados.