CARTILHA DE SEGURANÇA DA INFORMAÇÃO

ONG AMBIENTAL 2024

6. CONTROLE DE ACESSO

- Senhas Seguras: Use senhas fortes e únicas, alterando-as regularmente.
- Autenticação Multifator (MFA): Ative MFA para aumentar a segurança das contas.
- Privilégios de Acesso: Acesso aos sistemas e dados deve ser concedido com base na necessidade de conhecer.

7. PROTEÇÃO DE DADOS

- Criptografia: Utilize criptografia para proteger dados sensíveis durante armazenamento e transmissão.
- Backups: Realize backups regulares de dados críticos.

8. SEGURANÇA DA REDE

- Firewalls e Antivírus: Mantenha os sistemas protegidos com firewalls e software antivírus atualizados.
- Monitoramento de Rede: Monitore o tráfego de rede para identificar e responder a atividades suspeitas.

9. GESTÃO DE INCIDENTES

- Relato de Incidentes: Relate imediatamente quaisquer incidentes de segurança ou violações à equipe de TI.
- Resposta a Incidentes: Siga os procedimentos estabelecidos para responder rapidamente a incidentes.

10. REVISÃO E AUDITORIA

- Avaliações Periódicas: Realize auditorias regulares para garantir a conformidade com a política.
- Atualizações: Atualize a política conforme necessário para abordar novas ameaças e regulamentações.

11. PENALIDADES POR VIOLAÇÃO

- Ações Disciplinares: Violações da política podem resultar em advertências, suspensão ou rescisão do contrato de trabalho.

12. CONSIDERAÇÕES FINAIS

- A segurança da informação é uma responsabilidade compartilhada. Siga estas diretrizes para proteger os dados e recursos da ONG. Em caso de dúvidas, entre em contato com a equipe de TI.

OBRIGADO PELA SUA COLABORAÇÃO!

ELABORADO PELO DEPARTAMENTO DE TI

CARTILHA DE SEGURANÇA DA INFORMAÇÃO

ONG AMBIENTAL 2024

OLÁ!

Esta cartilha foi elaborada para ajudá-lo a entender e seguir a Política de Segurança da Informação da ONG. Manter a segurança da informação é responsabilidade de todos. Leia atentamente e siga as diretrizes para proteger nossos dados e recursos.

1. INTRODUÇÃO

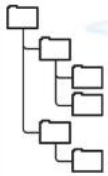
A Política de Segurança da Informação da ONG estabelece as diretrizes e responsabilidades para proteger os ativos de informação da organização contra ameaças internas e externas. Esta política abrange todas as áreas da organização e se aplica a todos os funcionários, voluntários, contratados e parceiros que tenham acesso a sistemas, dados e informações da ONG.

2. OBJETIVOS

- Proteger informações sensíveis: Assegurar que dados confidenciais estejam seguros contra acessos não autorizados.
- Cumprir com leis e regulamentos: Adotar práticas de segurança que atendam às exigências legais.
- Promover a conscientização: Informar e educar todos os usuários sobre a importância da segurança da informação.

3. RESPONSABILIDADES

- Todos os usuários: Devem seguir as diretrizes da política e relatar incidentes de segurança.
- Equipe de TI: Responsável pela implementação e manutenção das medidas de segurança.
- Gestores: Devem assegurar que suas equipes compreendam e sigam a política.



4. CLASSIFICAÇÃO DA INFORMAÇÃO

- Confidencial: Dados altamente sensíveis, como informações pessoais e financeiras.
- Interna: Informações relacionadas às operações da ONG, acessíveis apenas a funcionários autorizados.
- Pública: Informações que podem ser divulgadas sem causar prejuízo à organização.

5. DISPOSIÇÕES GERAIS

a. Uso da Internet

- Utilize a internet apenas para fins profissionais.
- Evite acessar sites não seguros ou de conteúdo inadequado.

b. Uso do Email

- Utilize o email corporativo apenas para comunicações relacionadas ao trabalho.
- Não abra anexos ou links de remetentes desconhecidos.

c. Redes Sem Fio (WiFi)

- Conecte-se apenas a redes WiFi seguras.
- Utilize VPN para acessar recursos internos remotamente.

d. Uso de Recursos de TI

- Use os equipamentos e softwares da ONG apenas para fins profissionais.
- Não instale softwares não autorizados.

e. Uso de Mídias Sociais

- Não compartilhe informações confidenciais ou sensíveis em mídias sociais.
- Representar a ONG de maneira profissional e responsável.

f. Áudio, Vídeos e Fotos

- Utilize mídias apenas para fins autorizados e relacionados ao trabalho

g. Limpeza e Organização do Ambiente de Trabalho

- Mantenha a mesa de trabalho limpa e organizada.
- Bloqueie a tela do computador sempre que se afastar da mesa e armazene documentos físicos de maneira segura.
- Descarte documentos confidenciais, utilizando serviços de destruição apropriados.

ELABORADO PELO DEPARTAMENTO DE TI