[logotipo da organização]

[nome da organização]

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

POLÍTICA DE DISPOSITIVO MÓVEL, TELETRABALHO E TRABALHO EM HOME OFFICE

Commented [AES2]: Esta Política não precisa constar em um documento separado se as mesmas regras forem descritas pela Política de segurança de TI.

Commented [AES3]: Para saber mais sobre o assunto, leia este artigo:

How to Use ISO 27001 To Secure Data When Working Remotely https://advisera.com/27001academy/blog/2021/10/27/how-to-use-iso-27001-to-secure-data-when-working-remotely/

Commented [AES4]: 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.

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

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 impedir o acesso não autorizado aos dispositivos móveis localizados fora das instalações da organização.

Este documento aplica-se a todo o escopo do Sistema de Gestão da Segurança da Informação (SGSI), isto é, a todas as pessoas, todos os dados e todos os equipamentos no escopo do SGSI.

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

Commented [AES5]: Inclua o nome da sua organização.

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas A.6.7, A.7.9 e A.8.1
- Política da segurança da informação
- [Política de classificação da informação]
- [Política de segurança de TI]

Commented [AES6]: Você pode encontrar um modelo para este documento na pasta "05_Politicas_gerais" do Kit de documentação ISO 27001.

Commented [AES7]: Você pode encontrar um modelo para este documento na pasta "09_Anexo_A_Controles_de_seguranca" do Kit de documentação ISO 27001.

Commented [AES8]: Você pode encontrar um modelo para este documento na pasta "09_Anexo_A_Controles_de_seguranca" do Kit de documentação ISO 27001.

3. Computação móvel

3.1. Introdução

Os equipamentos de computação móvel incluem todos os tipos de computadores portáteis, celulares, smartphones, cartões de memória e outros equipamentos móveis usados para armazenar e processar dados, não importa onde o equipamento seja usado.

[redacted]

Commented [AES9]: Exclua este parágrafo se o controle A.7.10 [redacted]

3.2. Regras básicas

Deve tomar-se cuidados especiais quando i equipamento de computação móvel estiver em veículos [redacted]

A pessoa que levar equipamentos de computação móvel para fora das instalações deve seguir essas regras:

- os equipamentos de computação móvel que contiverem informações importantes, confidenciais ou críticas não devem ser deixados sem supervisão e, se possível, devem ser trancados fisicamente. Também é possível usar travas espaciais para garantir a segurança do equipamento
- [redacted]

Commented [AES10]: Trecho a ser excluído se o o controle [redacted]

- as atualizações de patches e outras configurações do sistema são realizadas [especifique como é feita a implementação técnica ou faça referência a um documento que define o processo]
- a proteção contra códigos maliciosos é instalada e atualizada [especifique como é feita a implementação técnica ou faça referência a um documento que define o processo]
- [redacted]
- [redacted]
- [as informações] em computadores portáteis devem ser criptografadas [especifique como isso é implementado tecnicamente ou faça referência a um documento que defina o processo]
- a proteção de dados confidenciais deve ser implementada de acordo com a [Política de classificação da informação]
- [redacted]
- [redacted]

O [cargo] é responsável pelo treinamento e pela conscientização de pessoas que usam equipamentos de computação móveis fora das instalações da organização.

4. Teletrabalho e trabalho em home office

4.1. Introdução

Teletrabalho significa que equipamentos de informação e comunicação são usados para permitir que os usuários trabalhem fora da organização, incluindo a trabalho em home office. O teletrabalho não inclui o uso de celulares fora das instalações da organização.

[redacted]

4.2. Regras adicionais para teletrabalho

Todas as pessoas que realizam teletrabalho devem seguir as regras para computação móvel definidas na seção 3.17 deste documento e as regras definidas abaixo:

- o local físico onde é realizado o teletrabalho deve ser protegido por [especifique como é feita a implementação técnica ou faça referência a um documento que define o processo]
- no mínimo, as pessoas que realizam teletrabalho devem ter [liste aqui as configurações mínimas necessárias para o teletrabalho]
- [redacted]

Commented [AES11]: Por exemplo, acesso semanal ao [redacted]

Commented [AES12]: Por exemplo, forçando a instalação da [redacted]

Commented [AES13]: Ex.: acessando a rede da organização e [redacted]

Commented [AES14]: Por exemplo, estabelecendo um canal [redacted]

Commented [AES15]: Especifique o tipo de informação armazenada em computadores portáteis que deve ser criptografada de acordo com as práticas da sua organização. [redacted]

Commented [AES16]: Por exemplo, por meio de criptografia [redacted]

Commented [AES17]: Caso sua organização não possua uma [redacted]

Commented [AES18]: A ser excluído caso o uso de dispositivos [redacted]

Commented [AES19]: Você pode usar o seguinte treinamento de conscientização de segurança para treinar seus funcionários: [redacted]

Commented [AES20]: A autorização pode ser concedida [redacted]

Commented [AES21]: Exemplos de elementos a serem usados são:
- prevenção do acesso não autorizado de residentes, transeuntes, etc., pela utilização de salas e gabinetes com fechaduras, não funcionamento em espaços partilhados, layouts que impeçam a visualização ou audição de informação por terceiros, etc. [redacted]

Commented [AES22]: Por exemplo, fonte de alimentação [redacted]

Commented [AES23]: Caso a Política de mesa limpa e tela [redacted]

- [illegible]
- a devolução de dados e equipamentos em caso de rescisão do contrato de trabalho deve ser implementada de acordo com a [Política de Segurança de TI]
- as atividades especificamente proibidas para funcionários que realizam teletrabalho são: [enumerar aqui as atividades expressamente proibidas aos colaboradores no exercício do teletrabalho]
- [illegible]

Commented [AES24]: Caso sua organização não possua uma [illegible]

Commented [AES25]: Por exemplo, participar de reuniões com [illegible]

Commented [AES26]: Você pode excluir este texto se não [illegible]

Commented [AES27]: Você pode excluir este texto se não [illegible]

Commented [AES28]: Por exemplo, alterar configurações em [illegible]

5. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*	[illegible]	[illegible]	[illegible]
[Autorização para teletrabalho]	[especifique considerando o formato da autorização concedida]	[cargo]	[illegible]	[illegible]

Commented [AES29]: Ajuste conforme adequado.

Somente o [cargo] pode conceder aos demais funcionários o acesso a qualquer um dos documentos mencionados acima.

6. Validade e gestão de documentos

Este documento é válido a partir de [data].

[illegible]

Commented [AES30]: Isso é apenas uma recomendação; [illegible]

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

- quantidade de incidentes relacionados à retirada de equipamentos de computação móvel das instalações da organização sem autorização
- [illegible]

[cargo]

[nome]

_____

[assinatura]

Commented [AES31]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.