[logotipo da organização]

[nome da organização]

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

POLÍTICA DE TRAGA SEU PRÓPRIO DISPOSITIVO (BYOD)

Commented [AES2]: Para saber mais sobre o assunto, leia este artigo:

What is a BYOD policy, and how can you easily write one using ISO 27001 controls?
https://advisera.com/27001academy/blog/2015/09/07/how-to-write-an-easy-to-use-byod-policy-compliant-with-iso-27001/

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 definir como a [nome da organização] irá reter o controle sobre suas informações, quando estas informações estiverem sendo acessadas através de dispositivos que não são de propriedade da organização.

Este documento se aplica a todos os dispositivos de propriedade pessoas que têm a habilidade para armazenar, transferir ou processar quaisquer informações sensíveis no escopo do Sistema de Gestão de Informação (SGSI). Estes dispositivos incluem laptops, smartphone, tablets, pendrives, câmeras digitais, etc. Tais dispositivos serão referidos como BYOD nesta Política.

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

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

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

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas A.5.14, A.6.7 e A.8.1

3. Regras de segurança para uso de BYOD

As regras desta Política se aplicam a todos os BYODs, sejam eles usados para trabalho ou para uso privado,

3.1. Política da empresa

A [nome da organização] suporta o uso disseminado de BYOD para uso no trabalho – ou seja, uso destes dispositivos para executar o trabalho para a empresa.

Commented [AES6]: Inclua o nome da sua organização.

Commented [AES7]: Alternativamente, é possível dizer algo

3.2. Quem tem permissão de usar o BYOD e para quais fins

O [cargo] irá criar uma lista de cargos e/ou pessoas que têm a permissão de usar o BYOD, junto com os aplicativos e bancos de dados aos quais eles têm permissão de acesso em seus próprios dispositivos.

3.3. Quais dispositivos são permitidos

O [cargo] irá criar uma Lista de dispositivos aceitáveis que podem ser usados como BYOD,

Commented [AES8]: Por exemplo, firewall, backup, bloqueio

3.4. Uso aceitável

Para cada BYOD, o seguinte é obrigatório:

- [descreva como deve ser feito o backup de informações da organização]
- [descreva qual software de segurança deve ser instalado – por exemplo, software antivírus, prevenção contra intrusão, software de gestão de dispositivo móvel, etc.]
- [descreva o método seguro de conexão á rede da organização]
- Ao usar o BYOD fora das instalações da organização, ele não deve ser deixado de lado e, se possível, deveria estar fisicamente trancado.
- Informações classificadas precisam ter proteção adicional de acordo com a [Política de classificação da informação].

Não é permitido fazer o seguinte com o BYOD:

- Permitir o acesso a nenhuma pessoa exceto pelo funcionário que seja proprietários do dispositivo.
- Instalar aplicativos que estão listados como aplicativos BYOD proibidos.
- Conectar através de Bluetooth com qualquer tipo de dispositivo.
- Conectar-se com redes sem fio desconhecidas.
- Transferir dados da organização para outros dispositivos que não são permitidos.

3.5. Direitos especiais

A [nome da organização] tem o direito de visualizar, editar e excluir todos os dados da organização que estejam armazenados, transferidos ou processados no BYOD.

O [cargo] está autorizado a configurar qualquer BYOD de acordo com esta Política a e monitorar seu uso através de [especifique o nome do software de gestão de dispositivo móvel].

3.6. Reembolso

Commented [AES9]: Por exemplo, senhas, códigos de acesso,

Commented [AES10]: Por exemplo, VPN.

Commented [AES11]: Trecho a ser excluído se essa Política

Commented [AES12]: Inclua o nome da sua organização.

Commented [AES13]: Exclua isso se você não usar nenhum

Commented [AES14]: Inclua o nome da sua organização.

Commented [AES15]: Se for tecnicamente viável, você pode

A [nome da organização] não irá pagar para os funcionários (os proprietários do BYOD) quaisquer

A [nome da organização] irá pagar o seguinte:

- Qualquer novo software que precisa ser instalado para uso da organização.
-

3.7. Violações de segurança

Todas as violações de segurança relativas ao BYOD precisam ser reportadas imediatamente para o [cargo].

3.8. Treinamento e conscientização

O [cargo] está a cargo de treinar funcionários novos e existentes sobre o uso apropriado do BYOD,

4. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*			
[Lista de usuários permitidos para o BYOD e o que eles podem acessar]	[intranet da organização]			
[Lista de dispositivos BYOD aceitáveis e suas configurações]	[intranet da organização]			
[Lista dos aplicativos BYOD proibidos]	[intranet da organização]			

Commented [AES16]: Inclua o nome da sua organização.

Commented [AES17]: Alternativamente, você pode definir que

Commented [AES18]: Inclua o nome da sua organização.

Commented [AES19]: Ajuste-os de acordo com as práticas da

Commented [AES20]: Isso é geralmente o diretor de

Commented [AES21]: Este treinamento ajudará você a treinar

Commented [AES22]: Ajuste conforme adequado.

5. Validade e gestão de documentos

O documento é válido a partir de [data].

[redacted]

Commented [AES23]: Isso é apenas uma recomendação; [redacted]

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

- quantidade de incidentes relativos ao uso do BYOD
- [redacted]

[cargo]
[nome]

_____

[assinatura]

Commented [AES24]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.