[logotipo da organização]

[nome da organização]

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

POLÍTICA DE SEGURANÇA DO FORNECEDOR

Commented [AES2]: Para saber como selecionar as cláusulas de segurança, leia estes artigos:

- Processo em 6 etapas para tratar a segurança em fornecedores de acordo com a ISO 27001 https://advisera.com/27001academy/pt-br/blog/2014/07/03/processo-em-6-etapas-para-tratar-a-seguranca-em-fornecedores-de-acordo-com-a-iso-27001/
- Which security clauses to use for supplier agreements? https://advisera.com/27001academy/blog/2017/06/19/which-security-clauses-to-use-for-supplier-agreements/

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 o de definir as regras para o relacionamento com fornecedores e parceiros, incluindo provedores de serviços em nuvem.

Este documento é aplicável para todos os fornecedores e parceiros que têm a habilidade de influenciar a confidencialidade, integridade e disponibilidade de informações sensíveis da [nome da organização].

Os usuários deste documento são a direção e as pessoas responsáveis por fornecedores e parceiros na [nome da organização].

Commented [AES4]: Esta Política de alto nível está escrita de acordo com o controle A.5.19 do Anexo A da ISO 27001, definindo requisitos para mitigar os riscos associados ao acesso do fornecedor aos ativos da organização e não descreve práticas detalhadas a serem seguidas.

Se sua organização deseja definir práticas detalhadas a serem seguidas pelos fornecedores, veja como exemplo o documento Política de segurança de TI. Você pode encontrar um modelo para este documento na pasta "09_Anexo_A_Controles_de_seguranca" do Kit de documentação ISO 27001.

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

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

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas A.5.7, A.5.11, A.5.19, A.5.20, A.5.21, A.5.22, A.5.23, A.6.1, A.6.2, A.6.3 e A.8.30
- Metodologia de avaliação e tratamento de riscos
- Relatório de avaliação e tratamento de riscos
- Política de controle de acesso
- Declaração de confidencialidade

Commented [AES7]: Você pode encontrar um modelo para este documento na pasta "06_Avaliacao_e_tratamento_de_riscos" do Kit de documentação ISO 27001.

Commented [AES8]: Você pode encontrar um modelo para este documento na pasta "06_Avaliacao_e_tratamento_de_riscos" do Kit de documentação ISO 27001.

3. Relacionamento com fornecedores e parceiros

3.1. Identificação dos riscos

Commented [AES9]: Exclua este seção se o controle A.5.19

Os riscos de segurança relativos aos fornecedores e parceiros, incluindo provedores de serviços em nuvem são identificados durante o processo de avaliação de riscos, como definido na Metodologia de avaliação e tratamento de riscos. Durante a avaliação de riscos, deve ser tomado cuidado especial para identificar os riscos relativos à tecnologia da informação e comunicação, assim como os riscos relativos a cadeia de suprimento de produtos.

3.2. Seleção

O [cargo] decide se é necessário executar verificações cadastrais para fornecedores e parceiros

Commented [AES10]: Por exemplo, experiência de seus outros

3.3. Contratos

Commented [AES11]: Exclua este seção se o controle A.5.20

O [cargo] é responsável por decidir quais cláusulas de segurança serão incluídas no contrato com o fornecedor ou parceiro.

As seguintes cláusulas são mandatórias em acordos com fornecedores:

- Manter a confidencialidade da informação;
- Devolução dos ativos após o término do contrato;
- [illegible]
- [illegible]

Uma lista de cláusulas sugeridas é fornecida no Cláusulas de segurança para fornecedores e parceiros.

[illegible]

O [cargo] decide quem será o proprietário para cada contrato – por exemplo, quem será responsável por um determinado fornecedor ou parceiro.

3.4. Treinamento e conscientização

O proprietário do contrato decide quais funcionários dos fornecedores e parceiros precisam de conscientização e treinamento em segurança.

[illegible]

3.5. Monitoramento e revisão

O proprietário do contrato precisa verificar e monitorar com regularidade o nível do serviço e o atendimento as cláusulas de segurança por fornecedores e parceiros, relatórios e registros e registros criados pelo fornecedor/parceiro, assim como auditar o fornecedor ou parceiro ao menos uma vez por ano.

[illegible]

3.6. Mudanças ou término de serviços do fornecedor

O proprietário propõe mudanças ou a rescisão do contrato e, o [cargo] toma a decisão final. [illegible]

3.7. Remoção de direitos de acesso/devolução de ativos

Quando o contrato é modificado ou rescindido, os direitos de acesso para os funcionários dos parceiros/fornecedores devem ser removidos de acordo com a Política de controle de acesso.

[illegible]

4. Gestão de registros mantidos de acordo com este documento

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

Commented [AES13]: Exclua este seção se o controle A.6.3 [illegible]

Commented [AES14]: Você pode sugerir este treinamento ao fornecedor para conscientizar seus colaboradores e acompanhar seus conhecimentos: [illegible]

Commented [AES15]: Exclua este seção se o controle A.5.22 [illegible]

Commented [AES16]: Se necessário, as tabelas podem ser [illegible]

Commented [AES17]: Auditorias no local devem ser [illegible]

Commented [AES18]: Adapte como necessário, ou seja, com [illegible]

Commented [AES19]: Este é geralmente o gerente de segurança.

Commented [AES20]: Exclua este seção se o controle A.5.22 [illegible]

Commented [AES21]: Exclua este parágrafo se o controle [illegible]

Commented [AES22]: Exclua este parágrafo se o controle [illegible]

Nome do registro	***Local de armazenamento***	[illegible]	[illegible]	[illegible]
Contratos com fornecedores e parceiros	[gabinete, cofre ou similar]	[illegible]	[illegible]	[illegible]
Registros de monitoramento e revisão	Computador do proprietário do contrato	[illegible]	[illegible]	[illegible]

Commented [AES23]: Adapte este período de acordo com [illegible]

5. Validade de gestão de documentos

Este documento é válido a partir de [data].

[illegible]

Commented [AES24]: Isso é apenas uma recomendação; [illegible]

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

- quantidade e significância de incidentes resultantes de atividades de fornecedores e parceiros
- [illegible]

[cargo]
[nome]

_____
[assinatura]

Commented [AES25]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.