	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		
	Tipo: Política Institucional		Versão: 6
Área: Compliance Office	Autor: Silvio Freitas	Aprovador e/ou Revisor: Gustavo Duani	Data da Versão: 06/Nov/2023

1. Escopo

Este documento define as diretrizes para a **segurança da informação** na Sencinet.

Protegemos a confidencialidade, integridade e disponibilidade de nossas informações e ativos.

Nós os protegemos de ataques maliciosos, vazamentos deliberados, perda acidental e tudo o que se encaixa nesse meio. As ameaças são reais e podem vir de dentro e de fora da organização, então, todos nós temos que estar atentos ao papel que desempenhamos na proteção de nossos negócios.

Esta diretriz é publicada e comunicada a todos. É de propriedade do fórum de Segurança e revisado pelo menos a cada ano para garantir que ela continue a atender aos requisitos, bem como aos nossos objetivos de negócios, conforme descrito no Sistema de Gestão de Segurança da Informação (ISMS).

É aplicável a todos que trabalham para a Sencinet.

2. Declaração do CISO

No que acreditamos

Lidamos com uma grande quantidade de informações sobre nossos clientes, nossos funcionários e nossa empresa todos os dias. Somos responsáveis por mantê-los seguros, pois além da regulação, da legislação somos uma empresa de serviços de cibersegurança e devemos prezar pelos pilares de integridade, confidencialidade e disponibilidade.

Por que é importante

A Segurança da Informação deve permear por todas as áreas da empresa, as ações que tomamos executamos no nosso dia a dia corporativo devem estar alinhadas com políticas e processos definidos. Estar atento aos sinais e as possíveis ameaças é responsabilidade de cada um.

Nossa abordagem é simples:


A política de segurança da informação deve ser entendida, aceita e executada por todos.

A área de Governança que estabelece deveres e responsabilidade perante a segurança da informação.

A segurança dos dados também é uma exigência legal e há penalidades graves para indivíduos e empresas que violam esses requisitos.

Gustavo Duani – CISO Sencinet

PÚBLICA		
Próxima revisão: Nov/2024		1
Cópia NÃO controlada se impressa ou baixada. Considere o meio ambiente antes de imprimir este documento.		

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		
	Tipo: Política Institucional		Versão: 6
Área: Compliance Office	Autor: Silvio Freitas	Aprovador e/ou Revisor: Gustavo Duani	Data da Versão: 06/Nov/2023

3. Quem é responsável

Esta política se aplica a qualquer um que trabalhe para, ou em nome da empresa, que lide com informações para a Sencinet.

Você deve ler e entender os requisitos desta política, incluindo as outras políticas e normas associadas, e seguir a mesma e o Código de Ética e Conduta da Sencinet. Violar esta política pode levar a ações disciplinares e, em casos graves, demissão. Você também pode ter problemas com a lei. Existem penas graves para qualquer pessoa, ou qualquer empresa, que infrinja a lei, incluindo multas ilimitadas e prisão.

Os gestores são responsáveis por garantir que seu pessoal esteja familiarizado e cumpra com os requisitos desta política e das políticas e normas associadas.

Podemos alterar esta política de tempos em tempos, quando seja requerido, estando sujeita a quaisquer processos de consulta acordados.

Protegemos as informações e mantemos os ativos da Empresa seguros.

Valorizamos a confidencialidade de todas as informações detidas pela Empresa, seja de clientes, fornecedores, parceiros de negócios ou nossos próprios.

Proibimos o uso de informações privilegiadas obtidas em serviço pela empresa para ganho pessoal indevido.

Informações confidenciais não devem ser deliberadamente divulgadas ou discutidas. Devem ser reservadas para casos de requisitos comerciais e/ou legais.

4. Nossos Princípios

A estratégia geral de gestão da Sencinet em relação ao programa de segurança da informação está detalhada no Sistema de Gestão de Segurança da Informação (ISMS), incluindo responsabilidades e deveres.


O ISMS e o quadro de apoio serão revisados regularmente com o objetivo de melhoria contínua.

5. Declarações de Diretrizes de Política

5.1. Todas as políticas de segurança, normas, horários, processos e diretrizes serão documentadas, mantidas e publicadas e irão:

- a. Abordar todos os requisitos legais, regulatórios, comerciais e contratuais aplicáveis.
- b. Para as Políticas de Segurança que se derivam da presente política ([Ver seção 6](#)) deve-se realizar como mínimo, revisões e atualizações a cada 2 (dois) anos ou quando há mudanças no ambiente. Para esta Política de Segurança, que inclui um compromisso de conformidade com os requisitos do PCI-DSS, esta revisão deve ser realizada pelo menos 1 (uma) vez por ano.


PÚBLICA		
Próxima revisão: Nov/2024		2
Cópia NÃO controlada se impressa ou baixada. Considere o meio ambiente antes de imprimir este documento.		

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		
	Tipo: Política Institucional		Versão: 6
Área: Compliance Office	Autor: Silvio Freitas	Aprovador e/ou Revisor: Gustavo Duani	Data da Versão: 06/Nov/2023

c. Definir claramente as responsabilidades envolvendo a segurança da informação para todos que trabalham para a Sencinet.

- 5.2. O sigilo das informações será garantido.
- 5.3. A integridade das informações será preservada.
- 5.4. A disponibilidade de informações para os processos de negócios será preservada.
- 5.5. Todos os controles apropriados estarão em vigor para proteger nossas instalações de processamento de informações.
- 5.6. Todos os ativos de informação detidos pela Sencinet terão um proprietário nomeado pela empresa.
- 5.7. Será definida uma política relativa ao uso aceitável de informações e dos sistemas de informação.
- 5.8. As informações serão protegidas contra acesso ou uso não autorizados.
- 5.9. As informações serão classificadas de acordo com seu valor e sensibilidade ao negócio e a perda ou exposição potencial.
- 5.10. Todas as informações serão tratadas com base em sua classificação durante seu ciclo de vida (como ela é criada, armazenada, acessada, processada, compartilhada, transmitida e descartada).
- 5.11. O treinamento de conscientização sobre segurança da informação será obrigatório para todos os funcionários.
- 5.12. As informações serão distribuídas a funcionários, contratados e terceiros em uma base de "necessidade comercial".
- 5.13. Todos os controles apropriados estarão em vigor ao processar informações com terceiros.
- 5.14. Procedimentos de segurança operacional serão desenvolvidos para controlar a entrega de nossas políticas de segurança da informação, normas, obrigações legais e regulatórias.
- 5.15. Todas as violações, reais ou suspeitas, de segurança da informação serão denunciadas, investigadas e remediadas.
- 5.16. A segurança de nossos negócios, incluindo todos os nossos serviços e processos, será avaliada e endereçada para garantir que os riscos sejam identificados e os controles apropriados sejam documentados, implementados e monitorados para eficácia nas três Linhas de Defesa (3LoD).
- 5.17. Planos de continuidade de negócios serão desenvolvidos, mantidos e testados.
- 5.18. Revisaremos e faremos melhorias contínuas no nosso ISMS e estrutura de suporte.
- 5.19. Atenderemos a regulamentação e as normas externas, desde que não comprometam nossas políticas e controles de Segurança. Nota: Se houver risco de isso acontecer, entre em contato com askcompliance@sencinet.com.
- 5.20. A segurança da informação deverá ser abordada na gestão de projetos, independentemente do tipo de projeto.

PÚBLICA		
Próxima revisão: Nov/2024		3
Cópia NÃO controlada se impressa ou baixada. Considere o meio ambiente antes de imprimir este documento.		

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		
	Tipo: Política Institucional		Versão: 6
Área: Compliance Office	Autor: Silvio Freitas	Aprovador e/ou Revisor: Gustavo Duani	Data da Versão: 06/Nov/2023


5.21. Ao abordar a segurança da informação sob a norma PCI-DSS, por uma exigência contratual estabelecida por um de nossos clientes, os requisitos aplicáveis a cada uma das partes deverão ser claramente delimitados e em consenso com o mesmo, dependendo do escopo e objeto do contrato. Sempre que você tiver um tipo de solicitação PCI-DSS de um cliente, entre em contato com askcompliance@sencinet.com.

6. Políticas Complementares

Essa política de Segurança da Informação é uma consolidação das políticas de segurança abaixo, onde você encontrará detalhes e especificidades de cada área da segurança da informação. Elas devem ser consultadas e aplicadas em conjunto sempre que necessário.

- **3rd Party Security Responsibilities Policy:** Contém controles e medidas de segurança que devem ser implementados, como o gerenciamento, monitoramento e mitigação de riscos em relação à nossa cadeia de suprimentos.
- **Acceptable Use Policy:** Contém controles e medidas de segurança que devem ser implementados para proteger sistemas e ativos que usamos no trabalho.
- **Access Control Standard:** Contém os princípios-chave para garantir o controle de acesso às aplicações, sistemas, redes e dispositivos da Sencinet.
- **Cryptographic Control Standard:** Define como os controles criptográficos devem ser implantados e configurados para atender aos requisitos da legislação e diretrizes internacionais.
- **Data Sanitization and Disposal Policy:** Contém informações sobre como gerenciar o descarte seguro de dados e ativos.
- **Information Classification Data Handling Standard:** Contém informações sobre classificação das informações, a rotulagem, o manuseamento/processamento, a retenção e a eliminação.
- **Information Retention Policy:** Contém diretrizes de como estipular períodos de retenção de informação para diversas categorias e localizações.
- **People Manager Security Requirements:** Contém requerimentos específicos para que os gerentes garantam que sua equipe atenda às expectativas e necessidades da empresa.
- **Physical Security Policy:** Contém diretrizes de como manter nossa infraestrutura segura.
- **Technical Security Policy:** Contém um resumo de alto nível dos controles técnicos de segurança que devem ser implementados para proteger nossos sistemas e as informações que eles manipulam ou armazenam.
- **Data Privacy and Protection:** Contém diretrizes para proteção dos dados pessoais e resguardo da privacidade dos indivíduos, garantindo que os dados pessoais em posse da Sencinet sejam tratados com responsabilidade, ética e em linha com os princípios, políticas e legislações aplicáveis.

PÚBLICA		
Próxima revisão: Nov/2024		4
Cópia NÃO controlada se impressa ou baixada. Considere o meio ambiente antes de imprimir este documento.		

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO		
	Tipo: Política Institucional		Versão: 6
Área: Compliance Office	Autor: Silvio Freitas	Aprovador e/ou Revisor: Gustavo Duani	Data da Versão: 06/Nov/2023

7. Links e informações úteis

Link Intranet para Políticas Complementares de Segurança da Informação:
[Complementary Security Policies](#)

Para relatar um 'Incidente de Segurança da Informação' envie um e-mail:
security.incidents@sencinet.com

Se você precisar de mais informações ou orientações sobre esta política ou qualquer outra política de segurança ou padrão, entre em contato: askcompliance@sencinet.com.

8. Glossário

Prazo	Explicação
ISMS	Sistema de Gestão de Segurança da Informação
3LoD	Three Lines of Defence (Três Linhas de Defesa) Exemplo de segurança física no Datacenter: Primeira Linha de Defesa: Controles de acesso físico e lógico, Manutenção de Infraestrutura, Gestão de Ativos. Segunda Linha de Defesa: Gestão de Riscos, Acompanhamento do Escritório de Compliance. Terceira Linha de Defesa: Auditoria Internas.

9. Histórico de Revisão

Versão	Dados	Autor(es)	Conteúdo revisado
1	18/02/2021	Silvio Freitas	Criação de documentos
2	14/04/2021	Silvio Freitas	O e-mail do incidente mudou. Exemplo de 3LoD alterado.
3	05/05/2021	Silvio Freitas	A periodicidade da revisão desta política é ajustada para 1 ano e de qualquer política que inclua compromissos PCI-DSS. O numeral 5.21 está incluído na delimitação dos requisitos do PCI-DSS quando eles são uma exigência contratual do cliente.
4	09/05/2022	Silvio Freitas	Vigência da Política revisada
5	13/09/2022	Julia Limas Rolim	Troca da declaração de CEO para CISO e troca de aprovador
6	06/11/2023	Silvio Freitas	Informações sobre políticas complementares adicionadas (seção 6) e esclarecimento sobre validade das políticas (5.1)

PÚBLICA		5
Próxima revisão: Nov/2024		
Cópia NÃO controlada se impressa ou baixada. Considere o meio ambiente antes de imprimir este documento.		