POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA FORNECEDORES

SECURITYBOX SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO LTDA.
CNPJ: 11.928.104/0001-87
End: R. Emanuel Kant, 60 Sala 609
Curitiba – PR Telefone: 41 2170-0770

Controle de Versão

Data	Ação	Autor	Empresa	Versão
15/05/2024	Criação	Wellington Rosset	SECURITYBOX	1.0

Classificação de Confidencialidade

Classificação	Nível	Características
PÚBLICO	0	Documento que pode ser compartilhado com qualquer pessoa ou empresa.
INTERNO	1	Documento restrito, não se recomenda compartilhar com pessoas físicas ou outras empresas.
RESTRITO	2	Documento deve ser compartilhado apenas entre as empresas que foram endereçadas no cabeçalho do documento.
CONFIDENCIAL	3	Documento não deve ser compartilhado com outras pessoas além das pessoas permitidas e listadas no quadro abaixo.

1. OBJETIVO

A informação é um patrimônio de grande valor para a SecurityBox e zelamos por ela protegendo-a de forma a garantir a sua confidencialidade e integridade, conforme o Código de Ética e Conduta (PL-029). Esta política tem como objetivo:

1.1 Definir diretrizes sobre o comportamento dos fornecedores em relação às informações da SecurityBox.
1.2 Conscientizar os fornecedores sobre o correto uso das informações da SecurityBox.
1.3 Definir responsabilidades e penalidades sobre a Segurança da Informação.

2. DEFINIÇÕES

2.1 Segurança da Informação: Está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.
2.2 Fornecedores: Toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.
2.3 Propriedade Intelectual: – Área do Direito que, por meio de leis, garante a inventores ou responsáveis por qualquer produção do intelecto – seja nos domínios industrial, científico, literário ou artístico – o direito de obter, por um determinado período de tempo, recompensa pela própria criação.
2.4 Incidente de Segurança da Informação: Evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade

ou a autenticidade de um ativo de informação, assim como qualquer violação da Política de Segurança da Informação.

3. ORIENTAÇÕES

ASPECTOS GERAIS

a) Autores e Revisão

A Política de Segurança da Informação para Fornecedores da SecurityBox é de autoria da equipe de Segurança da Informação Corporativa. A aplicação desta política, sua revisão e manutenção é de responsabilidade do Gerente de TIC. Dúvidas sobre a aplicação desta política ou sugestões de alteração e melhoria podem ser encaminhadas para **csirt@securitybox.net.br**.

b) Divulgação e Distribuição

Esta Política de Segurança da Informação para Fornecedores deve ser parte integrante do Contrato do Fornecedor da SecurityBox. No ato da assinatura dos contratos, o fornecedor deve assumir total conhecimento e concordância com as diretrizes expostas nesta Política de Segurança da Informação para Fornecedores.

4. CONCIENTIZAÇÃO E TREINAMENTO DE SEGURANÇA DA INFORMAÇÃO

A SecurityBox define diretrizes de educação contínua para o aculturamento de boas práticas de segurança e disseminação para utilização no dia a dia dos Fornecedores, seja

para fins profissionais quanto para fins pessoais. A Política aborda procedimentos utilizados no programa de conscientização da instituição, tais como treinamentos e informativos internos. Os Fornecedores que acessarem ou processarem dados pessoais e/ou informações sensíveis devem ter ciência desta Política e do que diz respeito a treinamento de segurança da informação proveniente pela SecurityBox.

5. SENHA

Os Fornecedores devem utilizar senhas qualificadas de acordo com os critérios da SecurityBox que utiliza de meios de autenticação seguros, exigindo o uso de senhas complexas para acesso ao ambiente de tecnologia. Os critérios de criação de senhas para acesso ao ambiente tecnológico da SecurityBox serão repassados ao Fornecedor no momento da criação do perfil. As senhas devem seguir as melhores práticas do mercado, com tamanho mínimo de caracteres definidos, bloqueio por tentativas sem sucesso e periodicidade de alteração.

6. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

A gestão de riscos cibernéticos é de responsabilidade do Fornecedor, bem como da área de Segurança da Informação da SecurityBox. Este processo identifica os requisitos de segurança da informação relacionado com a cadeia de suprimentos. A gestão de riscos cibernéticos é contínua e define contextos internos e externos para avaliação, além de tratar riscos identificados de modo que sejam reduzidos a níveis aceitáveis.

7. GESTÃO DE ATIVOS

Os Fornecedores devem contar com um registro de ativos atualizado, no qual seja possível conferir os ativos empregados para a prestação do serviço. Sempre que um ativo contiver informações consideradas sigilosas, o Fornecedor deve dar baixa nos ativos garantindo que essas informações foram eliminadas de maneira segura aplicando medidas de eliminação segura ou destruindo o ativo fisicamente de tal forma que as informações que continha não possam ser recuperadas.

8. PROTEÇÃO E CLASSIFICAÇÃO DA INFORMAÇÃO

A SecurityBox estabelece diretrizes para a classificação, manuseio e rotulagem dos ativos de informação da empresa. Desta forma todos os fornecedores deverão considerar a classificação de informação contida na tabela abaixo, sempre que estiver em tratativas de qualquer cunho com a SECURITYBOX.

Classificação	Nível	Características
Público	**0**	Documento que pode ser compartilhado com qualquer pessoa ou empresa.
Interno	**1**	Documento interno, não é permitido compartilhar com pessoas físicas ou outras empresas.
Restrito	**2**	Documento restrito que deve ser compartilhado apenas entre as pessoas e empresas que foram endereçadas no cabeçalho do documento.
Confidencial	**3**	Documento não deve ser compartilhado com outras pessoas além das pessoas permitidas e listadas na capa do documento

SECURITYBOX SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO LTDA.
CNPJ: 11.928.104/0001-87
End: R. Emanuel Kant, 60 Sala 609
Curitiba – PR Telefone: 41 2170-0770

Todas as informações produzidas, individualmente ou em conjunto, pelo Fornecedor, originadas ou derivadas de suas atividades de trabalho são consideradas de propriedade da SecurityBox, aplicando-se isso também para qualquer informação provida ou licenciada para a SecurityBox. Os Fornecedores devem ter acesso somente às informações e recursos que são necessários para a execução do seu trabalho.

9. USO ACEITÁVEL DE RECURSOS DE TECNOLOGIA

Os Fornecedores que utilizarem recursos de tecnologia da SecurityBox, devem fazê-lo de forma profissional, ética e legal, conforme definido no termo de responsabilidade aplicável.

10. GESTÃO DE IDENTIFICAÇÃO DE ACESSO

A SecurityBox estabelece diretrizes gerais para acesso a ativos e sistemas de informação. Toda gestão de acessos é de responsabilidade da área de Tecnologia da Informação e é baseada no princípio da necessidade de acesso à informação para a execução das atividades laborais do Fornecedor. A Política define diretrizes, tais como:

- Acesso de Fornecedores;
- Acesso a Banco de Dados;
- Acesso Remoto;
- Acesso Físico;
- Revisão de Acessos;
- Parametrização de Senhas; e
- Múltiplo Fator de Autenticação.

11. PROPRIEDADE INTELECTUAL

A SecurityBox preza e resguarda a propriedade intelectual por ela produzida, bem como a dos Fornecedores. Não é permitida a reprodução ou manutenção de cópias ilegais de propriedade intelectual de qualquer natureza de serviços. A SecurityBox preserva os direitos autorais e de propriedade intelectual das informações e dos recursos por ela manuseados.

12. GESTÃO DE VULNERABILIDADE E CONFORMIDADE

O Fornecedor deve possuir processo de gestão de vulnerabilidade e conformidade, de modo que as seguintes diretrizes estejam estabelecidas:

- Gestão de Vulnerabilidade;
- Gestão de Conformidade;
- Testes Periódicos de Segurança;
- Diretrizes para a proteção contra ameaças de códigos maliciosos (Malwares); e
- Correções de Segurança (Gestão de Patch).

13. GESTÃO DE INCIDENTES DE SEGURANÇA DE INFORMAÇÃO

Os Fornecedores devem possuir um processo estruturado de resposta a incidentes. A SecurityBox pode solicitar informações relacionadas a quantidade de incidentes ocorridos em determinado período (máximo 12 meses), classificando pela sua relevância. Ameaças ou incidentes de segurança da informação que sejam de conhecimento do Fornecedor e que podem comprometer a segurança da informação da SecurityBox, devem ser imediatamente relatados ao responsável da SecurityBox, através do canal **csirt@securitybox.net.br.**

14. SEGURANÇA EM DISPOSITIVOS MÓVEIS

Os Fornecedores devem seguir as diretrizes, que serão repassadas pontualmente, definidas pela SecurityBox para utilização segura de dispositivos móveis, bem como as atribuições das áreas responsáveis pelo monitoramento.

15. SEGURANÇA EM REDES

A SecurityBox possui ferramentas de segurança capazes de detectar e responder tentativas de intrusão e seu ambiente de rede. No presente tópico, a Política aborda, também, regras sobre a rede sem fio corporativa e pública. Os equipamentos dos Fornecedores não podem ser conectados na rede interna da SecurityBox sem a aprovação prévia da área de Tecnologia da Informação. Computadores que serão conectados na rede deverão estar protegidos por software antivírus/anti-malware e demais softwares devidamente licenciados.

16. TRANSFERÊNCIA DE DADOS

Todas as transferências de dados devem ser realizadas por ferramentas validadas pela SecurityBox e o Fornecedor, responsáveis pela Segurança da Informação. A transferência de dados através de plataformas públicas (Dropbox, Wetransfer, entre outros) não é recomendada. Todos os sistemas de transferência de dados (e-mail, compartilhamento de arquivos, transferência de dados entre aplicativos, etc.) devem incluir os devidos meios de proteção de transmissão e armazenamento de dados, com a garantia da confidencialidade, integridade, disponibilidade e responsabilidade com base nos níveis de classificação das informações.

17. CONFIDENCIALIDADE DAS INFORMAÇÕES

O Fornecedor deve proteger as informações da SecurityBox contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade.

18. PLANO DE CONTINUIDADE

A SecurityBox exige que os Fornecedores de Cloud possuam um plano de continuidade e/ou um plano de recuperação de TI que permitam prestar o serviço em casos de incidentes ou desastres. Para os demais Fornecedores é recomendado que tenham um plano de continuidade e/ou um plano de recuperação de TI que permitam prestar o serviço

Controle de Aprovação

Data	Ação	Versão	Aprovador	Assinatura
31/05/2024	Aprovação	1.0	GEORGE SILVERIO DA SILVA	gov.br Documento assinado digitalmente GEORGE SILVERIO DA SILVA Data: 31/05/2024 21:41:27-0300 Verifique em https://validar.iti.gov.br