POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVOS

Este documento descreve diretrizes fundamentais para o uso aceitável dos ativos de informação, no que se refere a recursos, dados e informações geradas, armazenadas, processadas ou transmitidas pela Requestia, baseadas nos princípios de confidencialidade, integridade e disponibilidade.

2. ABRANGÊNCIA (PÚBLICO ALVO)

Esta Política de Segurança da Informação é um documento com valor jurídico e aplicabilidade imediata e indistinta a todas as áreas de negócio, os colaboradores, estagiários, consultores, prestadores de serviços, parceiros e sócios (referidos neste documento como apenas "Colaboradores") que venham acessar ou utilizar as informações da Requestia e demais ativos tangíveis ou intangíveis da empresa.

3. RESPONSABILIDADES

A Política de Segurança da Informação tem a responsabilidade de direcionar a Requestia, seus colaboradores, parceiros e alta administração em tudo que diz respeito a Segurança da Informação. É dever de todos entender e seguir as diretrizes descritas nesta política.

4. PROPRIEDADE INTELECTUAL

É um conceito que visa positivar e/ou reconhecer direitos legais a respeito de um produto, processo ou obra de produção intelectual, como por exemplo, produtos, invenções, patentes, marcas, desenhos, códigos de software, programas de computadores, sistemas, base de dados, projetos, textos, etc., sejam eles tangíveis ou intangíveis.

Os colaboradores devem ser conscientizados em relação a proteção da propriedade intelectual da Requestia onde a criação, material, produto e/ou códigos fontes produzidos por qualquer colaborador é de propriedade exclusiva da Requestia.

5. GESTÃO DE ATIVOS

A Requestia está comprometida em gerenciar o ciclo de vida de todos os ativos que são relevantes para o negócio, sejam eles tangíveis ou intangíveis, desta forma, as seguintes diretrizes são estabelecidas:

i. Deve haver um processo que permita gerenciar todo o ciclo de vida de um ativo, desde a aquisição, identificação, utilização, alteração até o descarte seguro, de modo que estejam protegidos contra acessos indevidos;
ii. Devem haver controles que permitam identificar o responsável do ativo, como está sendo utilizado, quem está utilizando e para quais finalidades;
iii. Todos os colaboradores devem ter acesso aos ativos necessários para realizar as suas atividades corporativas, cientes da responsabilidade de preservação, bom uso e a preocupação com a segurança da informação;
iv. Todo ativo utilizado para realizar qualquer função dentro da empresa deve ser de propriedade da Requestia;

6. GESTÃO DE TERCEIROS

A Requestia aplica as diretrizes de segurança da informação também para a gestão de terceiros (clientes, fornecedores e parceiros), principalmente em atividades relevantes que envolvem o acesso, manuseio, processamento, armazenamento, transferência e descarte de dados em estruturas tecnológicas para a prestação de serviços, seja no acesso ao ambiente da própria Requestia ou no acesso a ambientes de terceiros.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação processada pela Requestia possui um grau de sigilo, desta forma a informação é classificada conforme indicado abaixo:

Confidencial

Informação confidencial possui alta criticidade e impacto ao negócio da Requestia e/ou de seus clientes, na qual poderá ser acessada apenas por pessoas autorizadas, sendo vedada a transmissão ou divulgação de seu conteúdo. Por exemplo: dados estratégicos de produtos como novidades ou lançamentos de funcionalidades, senhas, planilhas de cargos e salários, código fonte, etc.

Interna

Informação interna deve ser utilizada dentro da Requestia onde o acesso é limitado aos Colaboradores e sua divulgação deve ser realizada apenas para o público interno. Entretanto, se esses dados se tornarem públicos, as consequências não serão críticas.

Pública

Informação que pode ser divulgada ao público em geral, isto é, colaboradores, clientes, fornecedores, parceiros, sem que isso provoque impactos no negócio. Por exemplo: informações sobre congressos, webinar, etc.

Vale ressaltar que nem toda informação processada pela Requestia é considerada confidencial, salvo se estiver expressamente classificada como interna ou pública.

8. PROTEÇÃO E TRATAMENTO DE DADOS

A Requestia protege e trata os seus dados através da gestão do ciclo de vida da informação que contempla as fases de Geração, Manuseio, Divulgação, Armazenamento, Transferência e Descarte. Esta gestão se estende a dados pessoais, fundamentada na LGPD - Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018) e dados de terceiros, ao qual a Requestia de alguma maneira, trabalha com estes dados.

9. CRIPTOGRAFIA

O uso de criptografia em ativos de informação da empresa deve sempre ser avaliado a aplicado quando necessário, afim de garantir a proteção em todo o ciclo de vida da informação, atendendo padrões de segurança dos órgãos reguladores.

10. BACKUP E RESTAURAÇÃO

Os backups devem ser realizados de forma periódica e automática, com período de retenção definido e armazenamento seguro. O objetivo é diminuir os riscos de perda de informações que gerem impactos ao negócio. Devem ser desenvolvidos e mantidos os procedimentos de backup e restauração devidamente atualizados, através de processos de revisão periódica e melhoria contínua.

11. CONTROLES DE ACESSO E LOGINS

O processo de gestão de acessos a sistemas e serviços da Requestia considera a seguinte premissa, "Tudo deve ser proibido a menos que expressamente permitido". Desta forma, as seguintes diretrizes para controle dos acessos e logins são estabelecidas:

i. Todo e qualquer acesso deve possuir um processo de autenticação com o objetivo de identificar o usuário;
ii. Todo colaborador deve possuir um usuário e senha para acesso aos serviços e sistemas da empresa e deve ser proibido o compartilhamento de uso com outros colaboradores;
iii. A identificação de qualquer colaborador deve ser única, intransferível e pessoal, onde é responsabilizado por qualquer ação realizada;
iv. Somente usuários autorizados devem possuir acesso aos recursos sistêmicos da Requestia;
v. O acesso de usuários deve seguir o critério de menor privilégio, restrito somente ao que é necessário, devidamente alinhado com as atribuições e atividades de sua função;
vi. O acesso a rede interna realizado de forma remota somente deve ser permitido e estabelecido mediante a utilização de software do tipo "VPN Client To Site" devidamente homologado pela Requestia;
vii. O acesso internet deve ser disponibilizado somente para usuários autorizados com o propósito profissional, como recurso de apoio complementar as atividades diárias realizadas;
viii. A Concessão, Revogação ou Alteração de Acesso a sistemas e serviços da empresa deve ser gerenciado através do sistema de Gestão de Identidades, devidamente aprovado pelos níveis requeridos;
ix. Contas de usuários que estão de férias ou afastados, independentemente do motivo, devem ser bloqueadas durante o período de ausência. A comunicação destas situações deve ser realizada pelo departamento pessoal (RH), através do sistema de chamados, ou em casos de exceção, via e-mail, para a equipe de TI responsável. Em caso de "Demissão", deverá ser reportado imediatamente;

12. REDE CORPORATIVA E CONVIDADOS

A Rede Corporativa e de Convidados devem ser separadas logicamente para garantir maior segurança e controle do acesso de colaboradores, visitantes, consultores, temporários, parceiros, entre outros. Desta forma, as seguintes diretrizes são estabelecidas:

i. A Rede Corporativa deve ser de uso exclusivo de colaboradores da empresa explicitamente para fins profissionais. Os meios de conexão a esta rede devem estar disponíveis por cabo ou através da rede sem fio (Wi-Fi);

ii. A Rede de Convidados deve ser de uso exclusivo de visitantes, consultores, temporários, parceiros, entre outros, quando justificada a necessidade de conectar-se à rede para acesso à Internet. O meio de conexão a esta rede deve estar disponível somente através da rede sem fio (Wi-Fi);
iii. A utilização da Rede de Convidados por colaboradores para fins profissional não é permitida. Neste caso, devem usar a Rede Corporativa através dos meios de conexão disponíveis;

13. SEGURANÇA DO AMBIENTE FÍSICO

O acesso às dependências internas da empresa devem ser gerenciados e controlados de modo a evitar acesso não autorizado, desta forma, as seguintes diretrizes são estabelecidas:

i. É proibido o acesso de pessoas não autorizadas as áreas internas da Requestia.
ii. O acesso de visitantes as áreas internas da empresa somente é permitido, se o visitante estiver identificado e acompanhado de um colaborador da empresa.
iii. O acesso às dependências da empresa com qualquer tipo de equipamento com propósito de gravar o ambiente de trabalho, tirar fotos, publicar e/ou compartilhar imagens somente pode ser realizado com autorização prévia desde que não comprometa a segurança dos colaboradores, privacidade, sigilo de informações e/ou impacte negativamente a imagem da Requestia.

14. DESENVOLVIMENTO DE SOFTWARE

A Requestia desenvolve seu sistema seguindo práticas de desenvolvimento ágil, respeitando padrões de segurança da informação, de acordo com suas necessidades e seguindo procedimentos fundamentados na política de segurança da informação. Desta forma, as seguintes diretrizes são estabelecidas:

i. Os códigos desenvolvidos são controlados e armazenados de forma segura em sistema específico, com controle de versionamento, onde somente pessoas autorizadas possuem acesso.
ii. Os ambientes de desenvolvimento são segregados, ou seja, divididos em ambiente de desenvolvimento, ambiente de teste (QA) e ambiente de produção.

15. USO DE HARDWARE E SOFTWARE

A Requestia possui um conjunto de hardware e softwares que são homologados para serem utilizados por seus colaboradores. Todo hardware e software instalado nos equipamentos deve ser utilizado para fins corporativos. Desta forma, as seguintes diretrizes são estabelecidas:

i. Todo Hardware e Softwares fornecidos pela Requestia são de propriedade da Requestia.
ii. Toda Estação de Trabalho e Servidor devem possuir por padrão, software de antivírus, firewall ativado e atualizações de segurança devidamente atualizados para remover vulnerabilidades e garantir um maior nível de segurança dos equipamentos e das informações contidas nos mesmos.
iii. Todos ficam responsáveis por zelar pelos equipamentos de trabalho e utilização de softwares, desta forma, devem assinar o Termo de Responsabilidade de Uso de Hardware e Software.

16. USO DO SERVIÇO DE CORREIO ELETRÔNICO

A Requestia oferece aos seus colaboradores um sistema seguro para a troca de mensagens com clientes, parceiros e fornecedores. O serviço de e-mail corporativo tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais. Todo Colaborador da Requestia deve possuir um endereço de e-mail para troca de mensagens e ser orientado quanto ao uso adequado respeitando as práticas recomentadas para garantir a segurança das informações.

17. MESA LIMPA E TELA LIMPA

As práticas de mesa limpa e tela limpa são destinadas a todos os colaboradores com o objetivo de manter as informações da empresa seguras, evitando exposições desnecessárias e consequentemente o comprometimento de informações importantes para o negócio.

18. HOME OFFICE

A Requestia permite em situações específicas o trabalho Home Office levando em consideração a preocupação com a segurança da informação. O Trabalho Home Office somente é permitido se devidamente autorizado e se for utilizado equipamento homologado e que possui o serviço de VPN (Virtual Private Network) para se conectar à rede da empresa. Todo colaborador é orientado quanto as práticas de segurança da informação para o Trabalho Home Office.

19. PROGRAMA DE CONSCIENTIZAÇÃO

A Requestia implementa e mantem um programa contínuo de conscientização de todos os colaboradores em relação a aplicabilidade da Política de Segurança da Informação e documentos relacionados, principalmente, no que se refere à prevenção de golpes por engenharia social, phishing, fraudes, roubo de Senhas, privacidade e tratamento de dados, uso correto dos ativos de informação, etc.

20. PRIVACIDADE DE DADOS PESSOAIS

A Requestia cumpre com a legislação de proteção de dados com base na LGPD - Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018). Os detalhes de cumprimento podem ser consultados nas políticas de privacidades indicadas a seguir:

Política de Privacidade de Dados para Aplicações, Sites e Portais da Requestia
Descreve a política de privacidade adotadas pela Requestia para tratamento de dados pessoais de seus funcionários, sócios, clientes, fornecedores e qualquer outra pessoa física que tenha algum relacionamento com a Requestia através de seus sites e portais ou qualquer outro meio digital, ou não. Disponível em:

https://requestia.com/privacidade-e-seguranca/politica-de-privacidade-sites-e-portais

Política de Privacidade de Dados para a Plataforma Requestia
Descreve a política de privacidade adotada pela Requestia para tratamento de dados armazenados em sua plataforma SaaS, por seus licenciados. Disponível em:

https://requestia.com/privacidade-e-seguranca/politica-de-privacidade-plataforma

21. TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A Requestia realiza a gestão do tratamento de incidentes de segurança da informação considerando as diretrizes de sua política de segurança da informação e com o suporte de documentos internos que descrevem o processo para responder e tratar adequadamente incidentes de segurança de maneira proativa e reativa, permitindo a avaliação de risco e impacto nos serviços e ativos de informação da empresa.

22. DECLARAÇÃO DE RESPONSABILIDADE

Todo colaborador da Requestia deve assinar formalmente um Termo de Responsabilidade e Confidencialidade, comprometendo-se em agir de acordo com as regras e orientações descritas no mesmo, que estão alinhadas com a política de segurança da informação.

23. DISPOSIÇÕES GERAIS

As violações a esta política estão sujeitas a punições administrativas e/ou contratuais, que poderão ser adotadas sem prévio aviso, podendo culminar em eventuais demissões, cancelamento de contrato de prestação de serviços, processos legais, se aplicável. Esta Política encontra-se publicada no endereço:
https://requestia.com/privacidade-e-seguranca/politica-de-seguranca-informacao

Se você entende que as disciplinas e diretrizes especificadas neste documento são inconsistentes, estão incorretas ou incompletas, por favor, entre em contato com o Departamento de Segurança da Informação através do e-mail seginfo@requestia.com.

24. HISTÓRICO DE VERSÕES DESTE DOCUMENTO

Versão 1: Criado por Adalton Narezzi e Aprovado por Márcio Vinholes em Fevereiro de 2023.