Política de Segurança da Informação

1. INTRODUÇÃO

Este documento descreve procedimentos e práticas para uma rotina de trabalho mais segura, define o tratamento que deve ser dado às informações geradas, armazenadas, processadas ou transmitidas pela Requestia, tanto nos ambientes convencionais quanto de tecnologia.

2. ABRANGÊNCIA

Esta Política de Segurança da Informação é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta a todos 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. DIRETRIZES

Qualquer informação gerada, armazenada, processada, recebida ou transmitida é referenciada apenas como "processada" para fins desta política. A informação processada pela Requestia é um bem que tem valor e deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a integridade, disponibilidade, confidencialidade, legalidade e auditabilidade, independente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

4. 4. RESPONSABILIDADES

É de responsabilidade do todos prezar e manter as informações, ambientes e aplicações da Requestia seguros e em conformidade com esta política. Enquadra-se a todos a responsabilidade das ações feitas através de seus logins de acesso

5. CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação processada pela Requestia é classificada segundo sua confidencialidade da seguinte forma:

Confidencial

Informação classificada como confidencial é aquela que 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

A informação classificada como interna é aquela que deverá ser utilizada dentro da Requestia e poderá ser acessada por todos os colaboradores, mas, caso haja algum vazamento da mesma, ela não venha causar danos ou impactos a companhia. Por exemplo: políticas, procedimentos, etc.

Pública

A informação classificada como pública é aquela que pode ser divulgada a todos, isto é, colaboradores, clientes, fornecedores e público em geral, sem que isso provoque impactos no negócio. Por exemplo: informações sobre congressos, webinar, etc.

VALE LEMBRAR QUE NA TODA INFORMAÇÃO PROCESSADA PELA REQUESTIA É CONSIDERADA CONFIDENCIAL, SALVO SE ESTIVER EXPRESSAMENTE CLASSIFICADA COMO INTERNA OU PÚBLICA.

6. LEGISLAÇÃO DE PROTEÇÃO DE DADOS

A Requestia cumpre toda legislação de proteção de dados e proteção de dados pessoais da legislação brasileira. Todo Colaborador compromete-se a seguir rigorosamente as seguintes políticas de privacidade e seus respectivos endereços eletrônicos:

Política de Privacidade de Dados para Aplicações, Sites e Portais da Requestia

Descreve a politica 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/docs/politica-de-privacidade-sites-e-portais.pdf**

Política de Privacidade de Dados para a Plataforma Requestia

Descreve a política de privacidade adotadas pela Requestia para tratamento de dados armazenados em sua plataforma, por seus licenciados. Disponível em: **https://requestia.com/docs/politica-de-privacidade-plataforma.pdf**

7. USO DE HARDWARE E SOFTWARE

Todo software instalado nos equipamentos deve ser utilizado para fins corporativos. Qualquer software que, por necessidade do serviço, precisar ser instalado deverá ser comunicado a área de Suporte Técnico, para que o mesmo possa ser homologado e verificado o licenciamento, pois é terminantemente proibido o uso de softwares ilegais (sem licenciamento) na empresa.

Todos ficam responsáveis por zelar pelos equipamentos de trabalho, bem como seguir as normas descritas conforme nos documentos de **Normas e Procedimentos da Requestia** e o **Termo de Responsabilidade sobre Equipamentos**.

8. REDE CORPORATIVA E WI-FI

A Rede Corporativa existe para com que somente colaboradores da empresa a utilizem para fins profissionais. Portanto, visitantes, consultores, temporários, parceiros, entre outros, quando necessário conectar-se à rede, deverá usar a Rede Convidados. Ambas as redes deverão seguir a política de troca de senha disponível no documento de **Normas e Procedimentos da Requestia**.

9. USO DA INTERNET

Fica permitido o uso da internet apenas para atividades com fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações e tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa. Desta forma, está proibido acessar qualquer conteúdo pornográfico, erótico, censurado, racista, difamatório, evasivos, com o intuito de cometer fraude, crime, violação de direitos e da lei, entre outros. Portanto, todo acesso é proibido, salvo se estiver expressamente permitido.

Está vedada qualquer troca de informações como senhas, informações de clientes, entre outros assuntos classificados como confidenciais, por meios de comunicações não oficiais da empresa, ou seja, WhatsApp, e-mail pessoal, Skype, entre outros. Estes assuntos deverão ser tratados por meio do e-mail corporativo, por telefone ou pessoalmente (mas sempre se atentando quanto à Engenharia Social).

10. USO DO CORREIO ELETRÔNICO

As mensagens de correio eletrônico (e-mail) são instrumentos de comunicação interna e externa para a realização das atividades funcionais do usuário com fins corporativos. Elas devem ser escritas em linguagem profissional e que não comprometa a imagem da Requestia perante seus clientes e a sociedade em geral, que possam causar prejuízo moral e/ou financeiro, bem como

utilizar o e-mail da empresa para assuntos pessoais. Mensagens fora destas características não devem ser enviadas.

Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, mensagens com notícias falsas, entre outros.

Não é permitido o uso de correios eletrônicos particulares, a exemplo de Hotmail, Yahoo e Gmail, para o envio, recebimento e encaminhamento de informações corporativas da/sobre a Requestia e seus clientes, bem como encaminhar os e-mails da conta corporativa para o e-mail particular.

11. MESA LIMPA E TELA LIMPA

A prática 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 o comprometimento de documentos classificados como internos e confidenciais. Todo Colaborador deverá seguir as boas práticas indicadas documento de **Normas e Procedimentos da Requestia**

12. HOME OFFICE

O colaborador que necessitar usufruir do benefício de Home Office deverá seguir as boas práticas indicadas documento de **Normas e Procedimentos da Requestia**, sendo aplicáveis para o trabalho fora das instalações da Requestia todas as mesmas políticas, normas e procedimentos existentes para o trabalho nos escritórios da Requestia.

13. ENGENHARIA SOCIAL E PHISHING

Engenharia Social é exploração de confiança das pessoas para roubo de informações pessoais ou de empresas. Este tipo de golpe é dado principalmente devido à falta de conscientização do usuário com relação à Segurança da Informação para a obtenção de informações sigilosas e importantes. Ela pode ser feita diretamente, ou seja, pelo contato direto entre o engenheiro social e a vítima através de telefonemas, e-mails, mensagens de texto, mensagens via WhatsApp e até mesmo pessoalmente.

Phishing é um tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário ou organização através da utilização combinada de meios técnicos e engenharia social. O Phishing ocorre principalmente através de envio de e-mails com links, aplicativos e sites que são projetados especificamente para roubar dados e informações.

Todos os profissionais da Requestia devem seguir as orientações de prevenção de golpes por Engenharia Social e por Phishing que constam no documento de **Normas e Procedimentos da Requestia**

14. DISPOSIÇÕES GERAIS

O não cumprimento dessa política acarretará ao usuário punições administrativas e/ou contratuais, poderão ser adotadas sem prévio aviso, podendo culminar com o desligamento e eventuais processos legais, se aplicáveis.

Esta Política encontra-se disponível no endereço:
https://requestia.com/docs/politica-de-seguranca-informacao.pdf.

Se você acredita que qualquer comunicação complementar é inconsistente com esta Política, por favor, entre em contato com Encarregado pelo Tratamento de Dados Pessoais da Requestia.

15. HISTÓRICO DE VERSÕES DESTE DOCUMENTO

Versão 1 de 01 de Dezembro de 2020: Versão inicial do documento (*sob revisão*)