TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

1. INTRODUÇÃO

Este termo é aplicável a todos os colaboradores, estagiários, consultores, prestadores de serviços, parceiros e sócios (referidos neste documento como apenas “Colaboradores”) que venham acessar ou utilizar equipamentos e ter acesso às informações da Requestia e demais ativos tangíveis ou intangíveis da empresa. É de responsabilidade de todos os Colaboradores cumprir rigorosamente os controles descritos neste termo.

2. PROPRIEDADE INTELECTUAL

Qualquer informação e propriedade intelectual pertencente à Requestia, ou por ela disponibilizada, não deve ser utilizada para fins particulares, nem repassada a outrem, ainda que tenha sido obtida, inferida ou desenvolvida pelo próprio Colaborador em seu ambiente de trabalho, em acordo ao que está estabelecido nos contratos de trabalho.

Produtos

Para todos aqueles que possuem contato com as informações sobre os produtos desenvolvidos pela Requestia, fica claro que é expressamente proibido divulgar informações sobre futuras versões e/ou atualizações dos produtos antes do seu anuncio público oficial.

Código Fonte

Todos que possuem acesso a qualquer código fonte da empresa, deverão seguir as regras de uso e armazenamento destas informações:

i. Somente é permitido o armazenamento destas informações nos servidores de desenvolvimento, portanto, é proibido qualquer outro tipo de armazenamento;
ii. O código fonte é categorizado como informação confidencial, ou seja, é expressamente proibido divulgar para qualquer outra pessoa que não esteja autorizada a acessar tal informação.

3. RECURSOS

Quaisquer recursos disponibilizados, seja físico ou lógico, para realização de atividades profissionais são de propriedade da Requestia e/ou de seus Clientes e devem ser utilizados exclusivamente para desempenhar as funções de trabalho.

4. USO DE HARDWARE E SOFTWARE

Estações de Trabalho e Acessórios

Cada Colaborador recebe um computador e um conjunto de acessórios (monitor, mouse, teclado, etc.) para realizar as suas atividades diárias. Não é permitida a alteração da configuração de hardware como a troca de peças, upgrade de memória e/ou disco. Qualquer manutenção ou upgrade é responsabilidade da equipe de suporte da Requestia, que deverá ser acionada conforme necessidade.

Softwares

Todo computador já vem com um conjunto de softwares instalados para realizar as atividades diárias. Não é permitida a instalação de softwares não homologados pela Requestia bem como a desinstalação de softwares padrão. É terminantemente proibido o uso de softwares não licenciados. Qualquer software que precise ser instalado deverá ser solicitado a área de Suporte Técnico.

Redes Sociais

Está vedado o uso de aplicações de mensagens instantâneas e redes sociais usando os computadores e as redes corporativas da Requestia. É expressamente proibida troca de qualquer informação da Requestia, de seus colaboradores ou clientes pelas redes sociais ou outros meios de comunicação não oficiais da empresa. Estes assuntos deverão ser tratados por e-mail, chat corporativo, telefone ou pessoalmente.

5. ACESSOS ÀS REDES E SERVIÇOS

Todo usuário tem uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O acesso a rede de computadores, sistemas e outros recursos de tecnologia da Requestia, é concedido mediante apresentação de uma identificação, geralmente um nome de usuário e senha. Esse método é utilizado para controlar os direitos de acesso às informações, como também identificar cada Colaborador e uso dos recursos.

Senhas

A distribuição das senhas aos usuários, inicial ou de recuperação, devem ser feitas de forma segura, ou seja, não devem ser anotadas em agendas, *post-its*, cadernos, folhas, entre outros. As senhas só podem ser armazenadas no cofre de senha corporativo.

A troca de senha expirada só deverá ser liberada por solicitação do próprio usuário, preferencialmente usando um mecanismo de autosserviço. As senhas devem ser alteradas em qualquer caso de suspeita do comprometimento de seu sigilo.

O usuário deverá evitar colocar na senha dados óbvios, como por exemplo nome da empresa, de familiares, datas de aniversários, nome de animais de estimação, entre outros.

O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.

Acesso à Rede Corporativa

À Rede Corporativa só deverão se conectar Colaboradores da Requestia com dispositivos homologados para uso profissional, devidamente autorizados e configurados conforme os padrões definidos.

Acesso à Rede Convidados

Nesta rede poderão se conectar convidados, clientes, fornecedores e Colaboradores com seus dispositivos pessoais. É apenas nesta rede que deverão ser conectados celulares ou equipamentos pessoais.

Acesso à Rede via VPN

O serviço de conexão VPN deve ser utilizado para conexão à rede da Requestia a partir de um local externo (Ex. Home Office). Este tipo de conexão pode ser realizado somente em período comercial durante a realização de atividades corporativas, salvo em casos especiais em que esteja alinhado com seu superior imediato.

O uso do recurso de VPN deverá ser realizado para fins estritamente profissionais, de forma a cumprir os controles descritos **neste termo e na Política de Segurança da Informação da Requestia**, ficando sob responsabilidade do Colaborador a utilização adequada dos recursos de VPN.

Acesso à Internet

O uso da internet deve ser permitido 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.

Acesso à E-mail Corporativo

O serviço de correio eletrônico (e-mail) é um instrumento de comunicação interna e externa para a realização das atividades funcionais do colaborador com fins corporativos.

Não deve ser usado para enviar grande quantidade de mensagens (spam). Não devem ser enviados e-mails do tipo corrente, mensagens com notícias falsas, entre outros.

A escrita deve ser realizada usando 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. Mensagens fora destas características não devem ser enviadas.

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

O Colaborador não deve manter qualquer expectativa de privacidade sobre as mensagens criadas, armazenadas, enviadas ou recebidas através do sistema de e-mail corporativo.

Autenticação Multifator

Sempre que disponível, deve-se usar autenticação multifator para acessar as aplicações corporativas como e-mail e a própria plataforma Requestia Service Management usada para atendimento aos clientes da Requestia.

6. CRIPTOGRAFIA DOS DADOS LOCAIS E UNIDADES EXTERNAS

Os dados armazenados em notebooks e desktops devem estar em unidades lógicas separadas dos sistemas operacionais e aplicações. As unidades lógicas, onde são armazenados os dados e qualquer unidade externa que contenha informações confidenciais, devem estar protegidas por criptografia de dispositivo (Bitlocker).

7. SISTEMAS DE GESTÃO DE CÓDIGO FONTE

Qualquer código fonte desenvolvido por Colaboradores da Requestia deverá ser armazenado no sistema de gestão de código fonte corporativo. Sempre que possível, ou quando devidamente solicitado, o processo de *check-in* deverá ser efetuado para que os códigos sejam devidamente armazenados.

8. ACESSO A AMBIENTES DE TERCEIROS

Nenhum acesso a ambiente de terceiros será feito sem a expressa autorização do seu proprietário ou responsável. Sempre que possível, o Colaborador da Requestia deverá fazê-lo mediante o uso de gravação de sessões.

O Colaborador, ao receber credenciais e senhas de acesso aos ambientes de terceiros, deverá adotar os mesmos cuidados aplicados aos acessos da Requestia e solicitar sua revogação assim que terminar suas atividades, ainda que possa ser necessário novo acesso no futuro. A solicitação de revogação deve ser solicitada a área de Gestão de Acessos da Requestia e/ou do terceiro.

É expressamente proibido o uso de dados pessoais, informações da Requestia ou de seus Clientes em ambientes de testes e/ou homologação.

9. ANTIVÍRUS E OUTROS MECANISMOS DE PROTEÇÃO

As estações de trabalho e servidores são protegidos por mecanismos de detecção de vírus ou outras ameaças. É vedada qualquer tentativa de desabilitar, desativar, remover ou desinstalar qualquer mecanismo de proteção que esteja instalado em qualquer dispositivo da Requestia.

Todas as atualizações automáticas de sistemas operacionais e aplicações deverão ser aplicadas assim que disponível. Após a atualização, efetue a reinicialização da máquina.

10. PROTEÇÃO E TRATAMENTO DOS DADOS

Armazenamento e Transferência

Não é permitido realizar o upload (transmitir arquivos) ou compartilhamento de informação da Requestia ou de seus clientes para serviços e aplicativos de comunicação instantânea, de armazenamento na nuvem ou repositórios digitais, a exemplo, mas não se limitando a WhatsApp, Facebook Messenger, Telegram, WeTransfer, Google Drive, OneDrive, Dropbox, iCloud, Box, Slideshare, Trello e Scribd.

É proibida a utilização de dispositivos móveis removíveis, como pen drive e HD Externo, para armazenar ou copiar informações classificadas como confidencial e/ou interna.

Para toda informação classificada como confidencial fica proibido o uso de ferramentas online para conversão de formatos (e.g. PDF para Word, PDF para Excel, XML para JSON) ou validador de códigos e/ou textos (e.g. validador de XML, formatação de JSON). Nestes casos, todos deverão optar por processar e manipular os dados com ferramentas instaladas localmente.

Diretório Temporário de Rede

Não use diretórios temporários para armazenamento de documentos classificados como confidencial. O diretório temporário de rede da Requestia é uma área comum entre todos da empresa, destinada exclusivamente para transferências entre os usuários de arquivos que não sejam considerados confidenciais.

Divulgação

É proibida a divulgação, fornecimento ou tampouco facilitar o acesso a informações da Requestia e/ou de seus Clientes a terceiros, afiliados, parceiros, familiares, funcionários ou quaisquer outras pessoas que não estejam expressamente autorizadas.

Descarte Adequado

Quando necessário fazer o descarte de mídias, documentos, entre outros, todos deverão seguir as regras abaixo:

i. Ao descartar objetos como HD, Pen Drive, CDs, DVDs, computadores, notebooks, celulares, entre outras mídias, toda informação contida deverá ser totalmente removida pelo responsável, de preferência usando métodos como: desmagnetização, destruição física, sobrescrever;
ii. Os documentos físicos deverão ser triturados na fragmentadora de papel;
iii. Não é permitido em lixo comum o descarte de documentos confidenciais, como crachás, notas fiscais, currículos, planilhas, entre outros.

Dados de Terceiros

Os Colaboradores da Requestia têm acesso a dados de terceiros, clientes, fornecedores ou parceiros, durante a configuração da aplicação ou para a execução de suas atividades de suporte à aplicação. A manutenção destes dados nos computadores (sejam eles notebooks ou servidores da Requestia) após a execução de tais atividades é expressamente proibida, devendo tais dados serem descartados assim que não forem mais necessários.

Dados Pessoais

A Requestia possui duas políticas de privacidade para o tratamento de dados pessoais que estão fundamentadas na LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018). Todo colaborador tem a responsabilidade de ler e devem estar cientes de como cada política é aplicada.

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

11. HOME OFFICE

O Colaborador que estiver trabalhando em um regime de home-office, teletrabalho ou qualquer outra forma de trabalho remoto (referenciado neste documento como Trabalho Remoto), deverá seguir as seguintes regras:

i. Deverá cuidar que o lugar elegido para o Trabalho Remoto tenha privacidade no que refere à confidencialidade e segurança das informações da Requestia, assim como baixo ruído ambiental;
ii. Não é autorizado realizar o Trabalho Remoto em restaurantes, cafeterias, parques, ou qualquer outro lugar público;
iii. Não é autorizado realizar a conexão para o Trabalho Remoto através de redes de internet não confiáveis, como redes WiFi públicas, sejam elas de lojas, shoppings ou mesmo uma rede compartilhada com vizinhos;
iv. Os Colaboradores que praticarem o Trabalho Remoto deverão portar os devidos equipamentos: notebook corporativo com acesso à internet e VPN proporcionado pela companhia, seguindo os critérios vigentes estabelecidos pela área de Suporte e Segurança da Informação;
v. A prática de Mesa Limpa e Tela Limpa descrita neste documento também se aplica ao Trabalho Remoto;
vi. Deverá retornar ao local de trabalho quando houver impossibilidade de realizar seus afazeres remotamente devido a imprevistos como a falta de energia elétrica, conexão à internet, entre outros.

12. MESA LIMPA E TELA LIMPA

A prática de mesa limpa e tela limpa é destinada 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.

São práticas de **Mesa Limpa**:

i. Não escreva em agendas, post-its, cadernos, folhas, quaisquer informações caracterizadas como confidenciais ou internas. Por exemplo: senhas, logins, dados de clientes, fornecedores ou colaboradores, etc.;
ii. Ao terminar uma reunião, não deixe informações descritas nos quadros brancos ou flip-chart;
iii. Não deixe recados nas mesas de outras pessoas através de post-its ou papeis;
iv. Não deixe papeis impressos nas impressoras. Ao imprimir, pegue imediatamente.

São práticas de **Tela Limpa**:

i. Não deixe a tela do computador desbloqueada ao se afastar dele, evitando o acesso não autorizado;
ii. Não salve informações categorizadas como confidenciais ou internas no armazenamento local do computador ou área de trabalho, opte por salvar no diretório de rede;
iii. Ao final do expediente, ou no caso de ausência prolongada do local de trabalho, guardar os documentos, trancar as gavetas, armários e desligar o computador.

Os arquivos contidos na “lixeira” do computador deverão ser excluídos periodicamente.

13. ENGENHARIA SOCIAL E PHISHING

A Engenharia Social corresponde a exploração de confiança das pessoas para roubo de informações pessoais ou de empresas. Este tipo de golpe é devido principalmente à falta de conscientização do usuário em 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.

São boas práticas de prevenção à Engenharia Social

i. Nunca considere que uma mensagem é confiável com base na confiança depositada em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada. Portanto, ligue para confirmar com o remetente daquela informação se realmente o assunto tratado é verídico;
ii. Para manter as informações da empresa seguras, é vedada qualquer tipo de troca de informações relacionadas à empresa fora do ambiente de trabalho, principalmente com pessoas desconhecidas ou não relacionadas com o processo organizacional.

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.

São boas práticas de prevenção à phishing:

i. Todos os Colaboradores devem ficar atentos às mensagens recebidas em nome de alguma instituição, que tentem induzi-los a fornecer informações, instalar/executar programas ou clicar em links;
ii. Não deve considerar que uma mensagem é confiável com base na confiança depositada em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada;
iii. Todos devem ser cuidadosos ao acessar links, executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .msi, .vbs, .ps1, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela equipe de Segurança da Informação da Requestia;

iv. É recomendado que todos excluam os e-mails ou arquivos recebidos que sejam suspeitos e reportem aos supervisores e à equipe de Segurança da Informação;
v. Não é permitido acessar via rede e nem instalar aplicativos de Internet/Home Banking pessoais nos equipamentos da empresa.

14. NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA

Incidentes ou Dúvidas relacionadas à Segurança da Informação devem ser reportados imediatamente à área responsável através do e-mail **seginfo@requestia.com**.

Um incidente de segurança deve ser reportado nas seguintes situações:

i. Roubo ou extravio de equipamentos corporativos (notebooks, celulares, etc.);
ii. Perda de informações, dados considerados críticos para o negócio;
iii. Seja percebido acesso indevido a informações e/ou equipamentos;
iv. Identificação de comportamento estranho relacionado à infecção por vírus, antivírus desatualizado, softwares e/ou programas suspeitos;
v. Identificação da possibilidade de uso de senhas fracas em qualquer sistema corporativo, ou ainda que ele não esteja solicitando a alteração de senha de forma periódica;
vi. Situações identificadas e contraditórias ao que está descrito na Política de Segurança da Informação, nas Políticas de Privacidade, no Termo de Responsabilidade e Confidencialidade e em documentos relacionados.

Uma dúvida de segurança deve ser reportada quando necessitar esclarecimento sobre interpretação e aplicação da Política de Segurança da Informação, Políticas de Privacidade, Termo de Responsabilidade e Confidencialidade ou em documentos relacionados.

15. DECLARAÇÃO DE RESPONSABILIDADE

i. TODOS OS COLABORADORES SÃO CIENTES DE QUE OS RECURSOS ELETRÔNICOS SÃO DE PROPRIEDADE E LICENCIADOS À REQUESTIA, E, PORTANTO, PODERÃO SER MONITORADOS. A RASTREABILIDADE E MONITORAMENTO DE INFORMAÇÕES NÃO CONFIGURA LESÃO, INVASÃO DE PRIVACIDADE OU QUALQUER CONSTRANGIMENTO PASSÍVEL DE DANOS MORAIS;
ii. Todo colaborador deve zelar pela segurança e utilizar corretamente todos os recursos e informações sob sua responsabilidade;
iii. Qualquer atividade realizada com recursos tais como identificação de usuários em sistemas, autenticação de usuário em sistemas, senhas, crachás, cartões de acesso e chaves, disponibilizados ao Colaborador, são de sua responsabilidade;
iv. O Colaborador não deve explorar em benefício próprio ou para fins não éticos informações e documentos de propriedade da Requestia e/ou de seus Clientes;
v. O Colaborador não deve reproduzir ou alterar documentos, arquivos ou informações de propriedade da Requestia e/ou de seus Clientes a não ser que a atividade faça parte de suas obrigações profissionais e esteja formalmente autorizado;
vi. O Colaborador não deve levar documentos ou arquivos contendo informações da Requestia e/ou de seus Clientes para fora das dependências da empresa sem autorização prévia;
vii. Em relação as informações que o Colaborador tem ou teve acesso em função das suas atribuições profissionais na Requestia, não está permitido divulgá-las a pessoas não autorizadas.

16. PENALIDADES

Constitui infração funcional inserir ou facilitar a inserção de dados falsos, alterar, excluir, ler ou copiar indevidamente dados dos sistemas informatizados da Requestia e/ou de seus Clientes, ou tentar acessar informações às quais não esteja autorizado.

O Colaborador responderá por suas ações e omissões que causem infrações aos regulamentos de segurança da informação, às políticas e as normas da Requestia e à legislação em vigor, sabendo que sua conduta será analisada, estando sujeita às ações disciplinares aplicáveis, sem prejuízo das penalidades trabalhistas, civis e criminais cabíveis.

Descumprindo os compromissos assumidos neste termo, o Colaborador estará sujeito às penalidades internas previstas no processo disciplinar da Requestia e/ou ações penais/cíveis previstas em lei.

17. VIGÊNCIA

O Colaborador deve estar ciente de que as regras e responsabilidades contidas neste termo se estendem por tempo indeterminado, independente da quebra do vínculo profissional com a Requestia.

18. HISTÓRICO DE VERSÕES DESTE DOCUMENTO

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