POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão 3.0

Vigência e Aprovação
Esta Política tem vigência a partir da data de sua aprovação e divulgação. Podendo ser revisada sempre que necessário.

Data aprovação: 03/04/2023

Data divulgação: 17/04/2023
A divulgação ocorrerá por meio dos canais de comunicação interno da Instituição e pelo site https://www.vilevepay.com.br

SUMÁRIO Folha

1. OBJETIVO

Esta Política de Segurança da Informação ("Política") visa orientar as ações, procedimentos e diretrizes para o uso dos ativos de Informação da VILEVE PAY, ou a elas confiados, a fim de garantir a confidencialidade, integridade, disponibilidade e privacidade (quando aplicável) das informações, sendo aplicável a todos os colaboradores da VILEVE PAY.

2. ABRANGÊNCIA

Para a presente Política, deverão ser seguidos por todos os colaboradores da VILEVE PAY, independentemente de sua relação contratual e nível hierárquico e são aplicáveis a toda Informação da empresa, seus clientes e usuários, em qualquer fase de seu ciclo de vida e meio ou suporte que os mesmos se encontrem, tais como, mas não se limitando a: mídias físicas, mídias eletrônicas, transmissão de dados ou mesmo pela transmissão verbal.

3. DEFINIÇÕES

- Informação: Conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão, além de toda a base de conhecimento, conteúdo, dado, conceito, envio ou recebimento de mensagem, processo ou fato existente, em meio físico ou eletrônico, que compõe documentos e Informações de propriedade, interesse ou posse da VILEVE PAY e inclui, mas não se limita a, qualquer dado, material, procedimento, processo, especificações, inovações e aperfeiçoamentos técnicos e comerciais que agreguem valor para o negócio da empresa, assim como todas as informações confidenciais dos nossos clientes sob nossa custódia.

- Segurança da informação: Segurança da Informação é a proteção da Informação contra vários tipos de ameaças, para garantir a continuidade do negócio, minimizando os riscos para VILEVE PAY e seus clientes. A Segurança da Informação é obtida a partir da implementação de um conjunto de controles, incluindo tecnologia, políticas, processos, procedimentos e a própria estrutura organizacional da empresa. Estes controles precisam ser estabelecidos,

implementados, monitorados, analisados criticamente, sempre que necessários, e melhorados continuamente para garantir que os objetivos e a segurança sejam atendidos.

- Confidencialidade: É um dos fundamentos da base de referência que compõe o objetivo de controle estabelecido pela política, não permitindo disponibilização ou exposição da Informação a indivíduos, entidades ou processos não autorizados expressamente, seja por contratos ou outros instrumentos formais.

- Integridade: É um dos fundamentos da base de referência que compõe do objetivo de controle estabelecido pela política, salvaguardando exatidão e completeza das informações, tal como foram criadas ou recebidas utilizando tecnologias, controles e processos que garantam esse requerimento.

- Disponibilidade: É um dos fundamentos da base de referência que compõe do objetivo de controle estabelecido pela política, que os sistemas e informações pertencentes ao ecossistema tecnológico da VILEVE PAY deverão estar disponíveis para seus clientes, associados e colaboradores, atendendo também a confidencialidade das Informações e integridade de seu conteúdo, formando, assim, uma tríade de Segurança de qualidade superior.

- Privacidade e Proteção de Dados Pessoais: É um dos fundamentos da base de referência que compõe do objetivo de controle estabelecido pela política, que os dados pessoais contidos nas Informações devem ser protegidos com a adoção de medidas técnicas e organizacionais de Segurança da Informação, nos termos impostos pela Lei nº 13.709/2018, conhecida por LGPD ou Lei Geral de Proteção de Dados e que estará disciplinada em conjunto com o Procedimento de Tratamento de Dados Pessoais e o Código de Conduta Ética.

- Software: Programa de computador que executa determinada tarefa.

- TI (Tecnologia da Informação): Conjunto de todas as atividades e soluções providas por recursos de computação. A Gerência de TI da VILEVE PAY tem a responsabilidade de

implantar e administrar os recursos de informática (estações de trabalho, servidores, redes, programas aplicativos, sistemas, etc.) que possibilitam o acesso e uso das informações corporativas pelos usuários que delas necessitam, além de implementar e monitorar as determinações de caráter tecnológico do comitê de segurança da informação.

- Recursos de Informática: Equipamentos como microcomputadores, servidores, redes, programas aplicativos, sistemas, etc., que possibilitam o acesso e a utilização das informações corporativas pelos usuários que delas necessitam.

- Download: Ação de salvar um programa, aplicativo ou arquivo da Internet.

- Internet: Rede mundial de computadores interligados de diversas plataformas, compartilhando informações de diferentes formas, conteúdos e mídias (textos, imagens, vídeo e som).

4. GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

4.1. Organização e Estrutura organizacional aplicadas à política de Segurança de Informação.

São atribuições específicas da Diretoria:

● Definir a estratégia de Segurança da Informação, alinhando a mesma às demais estratégias do negócio;
● Convocar e coordenar, a seu critério, reuniões periódicas e emergenciais do Comitê;
● Aprovar os documentos estratégicos.

O Comitê de Segurança da Informação será composto pelos membros dos departamentos de RH, TI, Jurídico e Controles Internos.

São atribuições do Comitê de Segurança da Informação:

- Elaboração e revisões da Política de Segurança da Informação, o qual servirá como guia para as ações de educação e difusão cultural do tema de Segurança da Informação e os controles técnicos aplicáveis;
- Revisão das ações educacionais já existentes, como treinamento específico para novos colaboradores além de iniciativas recorrentes de atualização para os demais

colaboradores, objetivando uma reciclagem total em até 12 meses para todos os colaboradores e associados
- Revisão dos procedimentos para continuidade dos negócios (Plano de Continuidade de Negócios), bem como a produção e implantação de novos procedimentos que garantam a operação contínua dos negócios frente aos riscos;

Todos os sócios, empregados, colaboradores, associados, incluindo terceiros ou quaisquer prestadores de serviços, independentemente da relação contratual estabelecida e do nível hierárquico, são responsáveis por:

- Conhecer e cumprir rigorosamente a Política de Segurança da Informação, bem como toda a documentação correlata;
- Pela ótica da responsabilidade pela segurança, todos são colaboradores e devem se atentar e reportar ao se deparar com práticas em não conformidade com a Política de Segurança, ajudando, inclusive, na reeducação dos hábitos em não conformidade;
- Reportar ao Comitê de Segurança da Informação, a suspeita ou confirmação de descumprimentos da documentação da política de Segurança da Informação e seus objetivos de Controle, bem como de tentativas de burla de recursos e ferramentas e quaisquer incidentes, tais como:

⇒ Acesso não autorizado a recursos de TI, sistemas e banco de dados da VILEVE PAY ou de terceiros.
⇒ Vírus.
⇒ Ataques de navegação de serviços.
⇒ Violação a esta Política ou procedimentos de Segurança da informação correlatos.
⇒ Acesso não autorizado ou vazamento de dados, inclusive de dados pessoais que estejam sob custódia da VILEVE PAY.
⇒ Uso impróprio de Informações.
⇒ Pirataria.
⇒ Falha do equipamento da VILEVE PAY.

5. CLASSIFICAÇÕES

5.1. Classificação da Informação

A Informação é tida como um ativo e possui valor diferente dependendo do seu conteúdo. Os controles de proteção desses ativos podem aumentar de acordo com seu valor. A classificação das Informações também pode definir quais controles de proteção precisam ser implementados.

Podemos entender a classificação da Informação também como uma escala de proteção a ser aplicada na mesma. São cinco os níveis de classificação da Informação em ordem crescente de importância e sigilo:

PÚBLICAS: são todas as Informações que já sejam de conhecimento público e estejam disponibilizadas para Clientes, Colaboradores e Público em Geral através da Internet,

ou veiculadas em documentos publicados em jornais, revistas, folders, redes sociais, panfletos, avisos ou palestras autorizadas.

INTERNAS: são Informações que estão disponíveis aos colaboradores por meio das ferramentas aprovadas, com armazenamento interno, em servidores da VILEVE PAY ou terceiros autorizados. Qualquer Informação classificada como "INTERNA" não poderá ser encaminhada, divulgada ou publicada em quaisquer meios para terceiros não autorizados, devendo a sua disponibilização ser restrita ao ambiente de trabalho e uso limitado aos Colaboradores ou terceiros (mediante assinatura de termo de "não divulgação" - NDA), que realmente necessitem ter acesso a tais Informações.

RESTRITAS: os documentos classificados como "INFORMAÇÃO RESTRITA" somente poderão ser acessados pela área, departamento, setor ou função dentro da VILEVE PAY que classificou a Informação. Normalmente são Informações de uma determinada área que não devem ser acessadas por outros setores da empresa, por exemplo, os documentos do setor de RH ou departamento financeiro da empresa.

CONFIDENCIAL: todas as Informações classificadas como confidenciais deverão ser mantidas em arquivos físicos ou eletrônicos com níveis de segurança compatíveis com a relevância da Informação, tais como cofres, armários com chaves, diretórios criptografados ou envio dos arquivos somente após a inclusão de mecanismos de segurança (senha ou criptografia). A transmissão de arquivos confidenciais só deverá ser feita utilizando meios de transmissão seguras, para as partes previamente autorizadas, com contrato de sigilo claro e dentro da validade, sejam as partes: funcionários, colaboradores, associados, fornecedores ou qualquer tipo de parceiro de negócios que precisam: criar, armazenar ou processar qualquer tipo de Informação CONFIDENCIAL.

ARMAZENAMENTO E TRANSMISSÃO DE INFORMAÇÕES CONFIDENCIAIS:

Atendendo aos requisitos contratuais de sigilo, os meios de armazenamento previamente aprovados são: discos criptografados, transmissão por rede ou internet utilizando SSL (com certificado de origem e destino da transmissão pertencentes às partes acordadas em contrato), SSH ou SFTP (FTP via SSH). Para transmissão de Informações confidenciais por e-mail em servidores e domínios diferentes, é necessário adicionar criptografia adicional em nível de arquivo (senha no arquivo utilizando criptografia forte de no mínimo AES 1024 bits ou equivalente). A proteção por senha deve ser aplicada INCLUSIVE para proteção de certificados privados de uso geral (por exemplo, ao se gerar pares de chaves SSH, é necessário aplicar senha FORTE nas chaves privadas).

Deverão ser classificadas como CONFIDENCIAIS as Informações que por sua origem, natureza ou importância não devam ser compartilhadas ou colocadas à disposição de pessoas não autorizadas. Consideram-se Informações confidenciais todas as que assim forem classificadas, bem como – indistintamente – dados recebidos ou

compilados de/sobre clientes, senhas, informações financeiras ou de salários, código fonte, informações sensíveis de usuários entre outras.

SECRETAS: as Informações classificadas como SECRETAS possuem o mais alto nível de sensibilidade e criticidade para o negócio. Chaves de criptografia (certificados SSL ou chaves SSH) e credenciais de acesso em geral são exemplos de Informações SECRETAS. Outras Informações estratégicas com alto nível de confidencialidade também pode ser classificadas como SECRETAS a critério do proprietário da Informação.

Informações em que seu possível vazamento implica em impacto financeiro direto ao negócio ou ponha em risco a continuidade dos negócios é um indício para que ela receba a classificação máxima de proteção: SECRETA.

As Informações SECRETAS normalmente possuem os seguintes controles e proteções:

- São armazenadas em volumes criptográficos acrescidos de criptografia de arquivo: criptografia multinível com chaves e algoritmos distintos.
- As Informações SECRETAS não podem ser copiadas, fotografadas, filmadas (incluindo sistemas de CFTV) ou testemunhadas, pessoalmente ou por meio de telepresença de qualquer forma.
- Algumas Informações SECRETAS podem simplesmente não ser armazenadas (brain storage only), processadas ou transmitidas no ambiente computacional, sempre que isso for possível.
- O armazenamento das Informações SECRETAS só pode ocorrer em regime de exceção em sistemas offline ou sistemas online aprovados nesta Política:

a. Senhas e Credenciais corporativas de acesso: só poderão ser armazenadas na sua memória ou por meio de software de gestão de senhas.

b. Quaisquer senhas armazenadas nos sistemas internos aprovados, para colaboradores e clientes só deverão ser armazenadas utilizando conversão em HASH (SHA256 ou superior) adicionada de técnicas de SALT, técnicas conhecidas como boas práticas de segurança mínima para armazenamento de senhas. Deste modo, TODAS AS SENHAS dentro dos sistemas de.

informações da VILEVE PAY, para acesso interno ou externo, somente são conhecidas pelo seu proprietário.

c. Tamanho de senha mínimo recomendável: mínimo de 9 caracteres e obrigação do uso de 4 opções (maiúsculo, minúsculo, character especial e numeral).

HASH: função criptográfica de via única em que uma sequência de dados gera uma saída única de tamanho fixo que não pode ser revertida. Ou seja, conhecendo o HASH não é possível conhecer a informação que o gerou.

SALT: trata-se de uma técnica para aumentar a segurança do HASH e evitar ataques do tipo dicionário, onde de posse de um banco de dados de palavras e seus respectivos HASH, se possa chegar à sequência, neste caso a senha em formato aberto.

A classificação dos documentos deverá ocorrer em campo visível, preferencialmente na primeira página e próximo ao cabeçalho do Documento.

Quando um Documento contiver mais de um tipo de Informação com classificação original distintas, por exemplo, dois documentos unidos em um único arquivo, a classificação mais restritiva passa a valer para todo o documento.

6. DEVERES E RESPONSABILIDADES

6.1. ATRIBUIÇÃO INICIAL DA CLASSIFICAÇÃO À INFORMAÇÃO

Caberá ao colaborador AUTOR da Informação definir os acessos, níveis de permissão e formas de proteção quando se tratar de uma Informação RESTRITA, CONFIDENCIAL ou SECRETA.

Será considerado como AUTOR da Informação o colaborador que primeiro produzir ou manipular a informação dentro do ambiente da VILEVE PAY.

Todo colaborador será responsável pela sua classificação e armazenamento, seguindo as recomendações contidas neste documento.

Caberá ao departamento de RH, juntamente com departamento de TI e Controles Internos, prover o suporte técnico aos autores das informações geradas e realizar os devidos treinamentos sobre proteção e armazenamento seguro de dados.

O departamento de Tecnologia da informação é a provedora dos recursos e meios de armazenamentos seguro dessas informações, assim como as ferramentas de controle de acesso, proteção e criptografia.

Caberá ao colaborador armazenar os arquivos digitais da empresa obrigatoriamente no servidor de arquivos por meio dos compartilhamentos carregados em sua estação de trabalho. A área de Tecnologia da informação não realiza nenhum tipo de backup de dados

armazenados de forma local nos equipamentos e não se responsabiliza por arquivos salvos nos mesmos.

6.2. PUBLICAÇÃO DE INFORMAÇÕES ABERTAS

Somente os gestores da VILEVE PAY, com assessoria devida da área de comunicação, poderão classificar Informações para divulgar externamente ou as definir como Informação Pública.

6.3. DESCARTE DE INFORMAÇÃO CLASSIFICADA

As Informações classificadas como RESTRITA, CONFIDENCIAL ou SECRETA devem sofrer tratamento especial no seu descarte.

O descarte de Informações, armazenadas em meio físico ou eletrônico, deverá ser realizado segundo o procedimento de descarte aplicável para garantir que a Informação descartada não possa ser recuperada de qualquer forma, sendo utilizados os procedimentos:

- ⇒ Todas as Informações impressas deverão ser trituradas antes de seu descarte.
- ⇒ Aparelhos eletrônicos devem ser "resetados" antes de seu descarte.
- ⇒ Informações eletrônicas deverão ser deletadas mediante o uso de ferramentas apropriadas ao descarte de dados, a ser disponibilizada pela área de Tecnologia da Informação.

6.4. EXTRAVIO DE INFORMAÇÃO

Qualquer evento de perda, extravio ou roubo de Informações, devem ser reportados IMEDIATAMENTE ao Comitê de Segurança da Informação.

7. UTILIZAÇÃO DOS RECURSOS DE TI

7.1 Hardware e Software

A VILEVE PAY poderá fornecer ao colaborador conta de correio eletrônico, acesso à internet e outras ferramentas de comunicação e produtividade para a dinamização do trabalho ou utensílios como aparelho e linha celular, gavetas, armários e quaisquer dispositivo, físico ou lógico, para a execução do trabalho.

O uso destas ferramentas estará sujeito a esta Política e restrições de acesso, de acordo com o nível de acesso outorgado ao usuário e deliberações do Comitê de Segurança da Informação.

Como política de nível de acesso à Informação, utilizamos a premissa de "menor privilégio possível". O colaborador somente terá acesso aos aplicativos e Informações que forem estritamente necessários para a realização do seu trabalho.

A reputação da VILEVE PAY, quanto à integridade ao tratar com a propriedade intelectual de seus clientes e de terceiros é vital para a continuidade do sucesso de seus negócios, salientando-se que os atos ilícitos e criminosos que infringem os direitos de propriedade de software têm cada vez mais sofrido sanções legais.

Devido ao software computacional não ser uma propriedade tangível na sua forma, torna-se fácil a sua duplicação não autorizada, o que constitui uma forma de roubo de propriedade.

Esta norma e os termos anexos procuram proteger a VILEVE PAY e o usuário de consequências legais devido a infrações dos direitos de propriedade, e apresentar as restrições e regras para o uso de equipamentos e outros recursos computacionais.

É expressamente proibido o uso de qualquer recurso corporativo, computadores, redes, acessos bem como quaisquer meios de comunicação corporativas para uso pessoal e/ou prática de qualquer ato ilícito, sob pena de responsabilização civil ou até criminal.

O colaborador é responsável pelos ativos de TI, bem como pelas informações que inserir em tais ativos

A utilização deverá estar em conformidade com as diretrizes apresentadas no formulário PLGTIANX01 / TERMO DE RESPONSABILIDADE PARA UTILIZAÇÃO DOS RECURSOS DE TI. apresentado no Anexo 01, devendo o mesmo ser assinado.

7.2 Empréstimo e Concessão de Equipamentos

O empréstimo de equipamento de TI da VILEVE PAY deverá ser conforme as diretrizes apresentadas no formulário PLGTIANX03 / TERMO DE RESPONSABILIDADE PARA EMPRÉSTIMO DE EQUIPAMENTO DE TI apresentado no Anexo 03, devendo o mesmo ser assinado como termo de responsabilidade.

A concessão de equipamento de TI da VILEVE PAY deverá ser conforme as diretrizes apresentadas no formulário PLGTIANX04 / TERMO DE RESPONSABILIDADE PARA CONCESSÃO RECURSO TI apresentado no Anexo 04, devendo o mesmo ser assinado como termo de responsabilidade.

7.3 Internet, e-mail e correio eletrônico

7.2.1 Internet

Para atender às necessidades dos trabalhos, os usuários previamente autorizados poderão ter acesso à Internet e a navegação em sites de conteúdo, sempre de acordo com a sua política de Segurança da Informação e bloqueios de sites classificados como inseguros ou não confiáveis. que deverá ser utilizada como uma ferramenta de trabalho, no auxílio à realização das tarefas.

As conversas virtuais, grupos de notícias e o correio eletrônico possibilitam que seus usuários tenham um alcance considerável para difundir as informações da VILEVE PAY. Desta forma, deve haver um cuidado especial em manter a transparência, coerência, integridade da imagem da empresa e sua posição corporativa. Assim, qualquer acesso ou informação transmitida através da Internet, mesmo que de forma particular, pode se tomar uma expressão ou posição corporativa.

Não será permitido o download de materiais protegidos por direitos autorais ou a instalação de softwares não homologados pela área de Segurança da Informação. O colaborador deve consultar o departamento de TI antes de fazer o download de qualquer software de terceiro.

7.2.2 E-mail e Correios Eletrônicos

O correio eletrônico da VILEVE PAY, assim como todas as plataformas de comunicação utilizadas na empresa, são ferramentas de trabalho, não devendo ser utilizado para outros fins.

As Informações contidas nas mensagens eletrônicas são de propriedade da VILEVE PAY, podendo ser monitoradas a qualquer tempo sem aviso ou notificação prévia para fins de auditoria de conformidade às normas internas, regulamentações ou boas práticas aplicadas ao negócio.

É expressamente proibido o envio de Informações classificadas como “INTERNAS” e “CONFIDENCIAIS” para endereços de e-mail de outros domínios além da vilevepay.com.br,

exceto para terceiros (clientes ou fornecedores) diretamente envolvidos no respectivo assunto da mensagem.

As Informações classificadas, como “SECRETAS” não devem ser armazenadas ou transmitidas por e-mail simples. Para isso, é obrigatório o uso de criptografia forte adicional para proteção do conteúdo da mensagem e seus anexos, através de solicitação à área de Tecnologia de Informação e autorização do superior imediato.

Quando um colaborador for desligado, deverão ser observados os seguintes procedimentos em relação ao seu e-mail corporativo:

- ⇒ O colaborador, independente de seu cargo, deverá ser informado de que seu e-mail corporativo foi suspenso.
- ⇒ O e-mail corporativo do colaborador desligado deve emitir mensagem resposta ao receber e-mails informando que o e-mail está suspenso e que o remetente poderá entrar em contato por meio de outro canal de comunicação (por exemplo, e-mail de eventual gestor do colaborador desligado)
- ⇒ O e-mail corporativo deve ficar ativo somente por um prazo razoável de até 3 meses e após esse período deve ser excluído juntamente com todas as Informações.

A utilização dos recursos de internet deverá ser conforme as diretrizes apresentadas no formulário PLGTIANX02 / TERMO DE RESPONSABILIDADE PARA UTILIZAÇÃO DOS RECURSOS DE INTERNET E E-MAIL, apresentadas no Anexo 02, devendo o mesmo ser assinado.

8. SENHAS DE ACESSO

A senha de acesso aos recursos computacionais da VILEVE PAY é de inteira responsabilidade do colaborador, que não deverá, em hipótese alguma, compartilhar ou emprestar a outros colaboradores e terceiros.

Os usuários deverão utilizar senhas “fortes”, misturando letras e números, em todos os sistemas corporativos e o tamanho mínimo recomendado para as senhas é de 9 (nove) caracteres.

Informações classificadas como SECRETAS deverão obrigatoriamente utilizar uma sequência longa de pelo menos 16 caracteres, ou optar pela utilização de uma chave criptográfica de pelo menos 1024 bits (utilizando-se sempre uma senha adicional para a proteção da chave criptográfica).

Toda ação feita, dentro ou fora do ambiente computacional da VILEVE PAY, será de responsabilidade do colaborador associado às credenciais de acesso associadas às ações.

9. CONTAS INATIVAS

Toda e qualquer credencial de acesso que não tiver atividade em até 30 dias serão bloqueadas em TODOS os sistemas corporativos.

10. AUTENTICAÇÃO DE MULTI FATOR (DOIS FATORES)

É obrigatório o uso de autenticação multi-fator (2FA ou MFA; Two factor Authentication ou MultiFactor Authentication) para TODOS os serviços onde a opção estiver disponível.

11. ACESSO REMOTO

Colaboradores previamente cadastrados, mediante aprovação explícita dos seus gestores diretos, poderão obter acesso remoto ao ambiente computacional da VILEVE PAY para trabalho fora de seu ambiente normal. Para isso, é necessário a abertura de chamado com aprovação da gestão.

Esse processo deve utilizar apenas equipamentos corporativos fornecidos pela VILEVE PAY com a aplicação dos controles de segurança vigentes. A conexão será estabelecida por meio de VPN privada corporativa.

12. MESA LIMPA

Todos os colaboradores deverão obedecer às regras de limpeza e organização do ambiente de trabalho a fim de não expor desnecessariamente Informações classificadas.

Os documentos impressos e anotações que precisem estar em um papel, devem permanecer nas mesas em caráter temporário devendo ser recolhidos em compartimentos fechados

disponíveis em seu departamento ou qualquer dependência da empresa que forneça segurança e proteção a esses materiais.

13. BLOQUEIO DE DISPOSITIVO POR INATIVIDADE

Todo dispositivo corporativo de acesso aos sistemas corporativos deve sofrer bloqueio automático depois de 60 minutos de inatividade (computadores, smartphones, tablets ou qualquer outro dispositivo, móvel ou não).

14. CAPTURA DE TRÁFEGO NA REDE

É expressamente proibido a captura de tráfego de rede dentro da rede corporativa da VILEVE PAY salvo eventos devidamente autorizados pelo Comitê de Segurança ou pelo gestor de segurança para fins exclusivos de diagnóstico, auditoria e monitoração previamente autorizados.

15. DISPOSITIVOS PESSOAIS

O uso de dispositivos pessoais fica restrito a rede de convidados da VILEVE PAY. Não é permitido a conexão de dispositivos não corporativos as redes internas, cabeadas ou sem fio.

Aos colaboradores que precisem fazer uso de dispositivos móveis para o desempenho de funções e tarefas específicas, o farão utilizando equipamentos fornecidos pela empresa, com os devidos controles e proteções técnicas aplicadas.

16. REDES SOCIAIS

É expressamente proibido que qualquer colaborador emita qualquer comunicado, opinião ou comentário EM NOME da VILEVE PAY sem a expressa aprovação e alinhamento com as áreas de marketing e comunicação.

As interações de resposta, réplica aos comentários feitos por terceiros sobre a empresa e afins, só podem ser feitas pelas áreas específicas de comunicação e gestão de mídias sociais, mesmo sendo postadas em redes pessoais.

A publicação de fotos em área internas também deve ser evitada, para evitar que Informações restritas contidas nas áreas internas da empresa sejam publicadas inadvertidamente, a não ser que seja previamente autorizada pela área de comunicação.

17. SOFTWARE, APPS E PLUGINS

Não é permitido a instalação de softwares não aprovados pela área de TI em quaisquer dispositivos que acessam os sistemas de Informação da VILEVE PAY que inclui: computadores, notebooks e dispositivos portáteis como tablets e celulares. Inclusive software, aplicativos, plugins pagos ou gratuitos.

A área de TI deve possuir um portfólio de ferramentas e aplicativos para atender as demandas do negócio incluindo ferramentas de produtividade e afins. A maioria dessas ferramentas já são previamente instaladas em todos os dispositivos corporativos.

18. POSTURA GERAL DE PRIVACIDADE

Todos os acessos aos sistemas internos devem ter como justificativa um propósito real de negócio. É expressamente proibido o acesso a quaisquer Informações de clientes, colaboradores ou qualquer registro nos sistemas de Informação da VILEVE PAY sem um propósito claro de negócio, e ligado diretamente ao exercício das funções atribuídas na relação de trabalho entre o colaborador e a empresa.

19. MONITORAMENTO

A VILEVE PAY se reserva ao direito de monitorar todas as atividades feitas pelos seus colaboradores em seus sistemas de informação para garantir o cumprimento desta e outras políticas da empresa.

Os ambientes internos também podem sofrer gravação audiovisual com o propósito principal de gerenciar a segurança do perímetro interno da empresa contra incidentes de segurança de qualquer natureza.

20. MODIFICAÇÃO / ROOT / JAILBREAKING

Com o propósito de proteger os dados da VILEVE PAY e seus clientes, não é permitido acessar qualquer ferramenta corporativa utilizando dispositivos que sofreram alterações nos sistemas nativos de segurança, como:

⇒ Acesso utilizando celular ou tablet Android com alterações e desbloqueios, conhecidos também como "Root de Android";
⇒ Acesso utilizando um iPhone ou iPad com "Jailbreak".

Devido a criticidade e o entendimento de que essas modificações afetam seriamente a segurança desses dispositivos, acessos feitos a partir de dispositivos pessoais com essas modificações é expressamente proibido.

21. ACESSO AO ESCRITÓRIO E ESCOLTA DE VISITANTES

O acesso aos nossos escritórios NÃO pode ser feito por pessoas DESACOMPANHADAS. O anfitrião do visitante deverá acompanhá-lo, DESDE a chegada na recepção da VILEVE PAY, até a entrada no escritório. Quem não possui senha de acesso cadastrada ou crachá de acesso, sempre terá que ser acompanhado pelo seu anfitrião ou por um colaborador. Para colaboradores ou consultores externos que trabalhem mais de dois dias por semana no escritório, iremos cadastrar sua senha de acesso ou crachá e liberar o acesso sem escolta.

A porta principal DEVE PERMANECER SEMPRE FECHADA, mesmo para saídas rápidas do escritório. Antes de abrir a porta, sempre OBSERVE com cuidado QUEM está no hall dos elevadores, na parte externa do escritório. Se houver presença de estranhos NÃO abram a porta, retornem para a recepção e aguarde alguns minutos.

22. CRIAÇÃO DE USUÁRIOS

22.1 Etapas de Criação de Usuário

22.1.1 Identificar a necessidade de criar um usuário com privilégios mínimos: É importante identificar a necessidade de criar um usuário com privilégios mínimos e garantir que

a pessoa selecionada tenha as habilidades e conhecimentos necessários para executar as tarefas com o nível de acesso atribuído.

22.1.2 Definir as responsabilidades do usuário: Antes de criar o usuário, é importante definir suas responsabilidades e privilégios mínimos necessários para executar as tarefas designadas.

22.1.3 Criar o usuário: Depois de identificar a necessidade e definir as responsabilidades do usuário, a conta do usuário deve ser criada no sistema. Isso deve ser feito seguindo as políticas de segurança da empresa e garantindo que a senha seja forte e complexa.

22.1.4 Configurar as permissões mínimas: Uma vez que a conta do usuário tenha sido criada, é importante configurar as permissões mínimas do usuário para garantir que ele tenha acesso apenas aos recursos necessários para executar suas tarefas.

22.1.5 Realizar treinamento de segurança: É importante que o usuário seja treinado em práticas de segurança para garantir que ele possa proteger os dados da empresa e evitar qualquer acesso não autorizado.

22.1.6 Monitorar a atividade do usuário: A atividade do usuário deve ser monitorada regularmente para garantir que ele esteja executando suas tarefas de forma apropriada e que não haja nenhum acesso não autorizado.

22.1.7 Revisar as permissões do usuário: As permissões do usuário devem ser revisadas regularmente para garantir que ele tenha apenas os privilégios mínimos necessários para executar suas tarefas.

22.1.8 Desativar a conta do usuário: Quando a conta do usuário não for mais necessária, ela deve ser desativada no sistema e as permissões do usuário devem ser removidas para evitar qualquer acesso não autorizado.

22.2 **Usuários Administradores**

22.2.1 **Etapas de Criação de Usuário Administrador**

22.2.2 Identificar a necessidade de criar um usuário administrador: É importante identificar a necessidade de criar um usuário administrador e garantir que a pessoa selecionada tenha as habilidades e conhecimentos necessários para executar as tarefas de administração de sistema.

22.2.3 Definir as responsabilidades do usuário administrador: Antes de criar o usuário administrador, é importante definir suas responsabilidades e privilégios. As

responsabilidades devem ser claramente definidas para evitar qualquer confusão ou sobreposição de funções.

22.2.4 Criar o usuário administrador: Depois de identificar a necessidade e definir as responsabilidades do usuário administrador, a conta do usuário deve ser criada no sistema. Isso deve ser feito seguindo as políticas de segurança da empresa e garantindo que a senha seja forte e complexa.

22.2.5 Configurar as permissões do usuário administrador: Uma vez que a conta do usuário administrador tenha sido criada, é importante configurar as permissões do usuário para garantir que ele tenha acesso apenas aos recursos necessários para executar suas tarefas de administração.

22.2.6 Realizar treinamento de segurança: É importante que o usuário administrador seja treinado em práticas de segurança para garantir que ele possa proteger os dados da empresa e evitar qualquer acesso não autorizado.

22.2.7 Monitorar a atividade do usuário administrador: A atividade do usuário administrador deve ser monitorada regularmente para garantir que ele esteja executando suas tarefas de administração de forma apropriada e que não haja nenhum acesso não autorizado.

22.2.8 Revisar as permissões do usuário administrador: As permissões do usuário administrador devem ser revisadas regularmente para garantir que ele tenha apenas os privilégios necessários para executar suas tarefas de administração.

22.2.9 Desativar a conta do usuário administrador: Quando a conta do usuário administrador não for mais necessária, ela deve ser desativada no sistema e as permissões do usuário devem ser removidas para evitar qualquer acesso não autorizado.

23. GESTÃO DE MUDANÇAS

23.1.1 As alterações no código fonte das aplicações ou nos próprios sistemas base podem impactar negativamente os Sistemas de Informação, motivo pelo qual é necessário controlar todas as alterações realizadas em aplicações e sistemas. A VILEVE PAY deve definir os mecanismos pertinentes de Gestão de Mudanças para poder controlar os processos de alterações de aplicações e sistemas instalados no ambiente de Produção.

23.1.2 Tais mecanismos devem estabelecer que toda documentação relacionada com as aplicações sujeitas a alterações deverá ser atualizada. Todas as alterações realizadas nas aplicações devem estar adequadamente identificadas, registradas e autorizadas, de forma a assegurar o controle de todas as modificações realizadas no ambiente de Produção.

23.1.3 Antes de implantar as mudanças no ambiente de Produção, é necessário testar tais mudanças nos ambientes de Testes e Desenvolvimento. Toda documentação dos

sistemas e aplicações deverão ser atualizadas após a implantação de alterações significativas.

23.1.4 Antes da realização de mudanças nos Sistemas Operacionais, Banco de Dados, e demais Sistemas dos Servidores, é necessário verificar que as aplicações não são impactadas com nenhuma falta de funcionalidade ou mau funcionamento.

24. BACKUPS

24.1.1 Todas as informações da Vileve Pay, ou informações sob nossa guarda estão sujeitas às políticas de backup da Vileve Pay. A seguir listamos as principais definições dessa política:

24.1.2 A informação mantida nos servidores centrais, servidores de rede, roteadores, sistemas de e-mail, etc. está sujeita a cópias periódicas de segurança que permitam sua recuperação ante uma perda imprevista, causada por erros, falhas do sistema, desastre naturais, sabotagem, roubo, etc.;

24.1.3 Deve-se realizar uma cópia de segurança completa antes e depois da instalação de um novo sistema e antes de qualquer atualização relevante, com o objetivo de manter uma cópia total da configuração das instalações homologadas;

24.1.4 As cópias periódicas totais devem complementar-se com as cópias incrementais as quais concentram as mudanças introduzidas nos dados a partir das cópias totais. No mínimo devem-se realizar cópias mensais totais e semanais incrementais. A periodicidade das cópias de segurança deve ser diretamente proporcional à relevância ou sensibilidade da informação armazenada, à frequência de modificações ou atualizações e ao risco de que o sistema falhe ou se corrompa;

24.1.5 As cópias são retidas durante um período suficiente para restaurar os dados e serviços críticos. As cópias diárias devem ser mantidas, ao menos, por uma semana, as semanais, no mínimo, um mês e as mensais devem ser guardadas ao menos 6 meses;

25. DESENVOLVIMENTO SEGURO

25.1 Segurança no Ciclo de Vida do Desenvolvimento

25.1.1 Os riscos de segurança serão identificados, avaliados e gerenciados em todas as fases do ciclo de vida do desenvolvimento de software.

25.1.2 As vulnerabilidades serão mitigadas em todas as fases do ciclo de vida do desenvolvimento de software, com especial atenção às fases de projeto e codificação.

25.2 Segurança em Requisitos

25.2.1 Os requisitos de segurança serão identificados e documentados em conjunto com os requisitos funcionais e não-funcionais.

25.2.2 A segurança será incluída nos testes de aceitação de requisitos.

25.3 **Segurança em Design**
25.3.1 As ameaças de segurança serão identificadas e avaliadas no processo de design do sistema.
25.3.2 As contramedidas de segurança serão incluídas no design do sistema.
25.3.3 Os padrões de segurança serão seguidos para o design do sistema.

25.4 **Segurança em Codificação**
25.4.1 Os desenvolvedores seguirão as melhores práticas de codificação segura.
25.4.2 As ferramentas de verificação de segurança serão utilizadas durante o processo de desenvolvimento para identificar vulnerabilidades de segurança.
25.4.3 As vulnerabilidades identificadas durante a fase de codificação serão corrigidas antes da liberação do software.

25.5 **Segurança em Testes**
25.5.1 A segurança será incluída nos casos de teste e nos testes de aceitação.
25.5.2 Os testes de penetração serão realizados para identificar vulnerabilidades no software.
25.5.3 Os testes de segurança serão realizados antes do lançamento do software.

25.6 **Segurança em Implantação**
25.6.1 A segurança será incluída na configuração do ambiente de produção.
25.6.2 Os procedimentos de implantação seguros serão documentados e seguidos.

25.7 **Segurança em Manutenção**
25.7.1 As vulnerabilidades serão corrigidas assim que forem identificadas.
25.7.2 As atualizações de segurança serão aplicadas regularmente.

25.8 **Gerenciamento de Vulnerabilidades**
25.8.1 As vulnerabilidades serão documentadas, avaliadas e gerenciadas de acordo com o processo de gerenciamento de vulnerabilidades.
25.8.2 As contramedidas de segurança serão implementadas para lidar com as vulnerabilidades identificadas.

25.9 **Conscientização sobre Segurança**
25.9.1 A conscientização sobre segurança será promovida entre os desenvolvedores.
25.9.2 A conscientização sobre segurança será promovida entre os usuários finais.

26. VIOLAÇÃO DAS POLÍTICAS

A violação desta Política poderá acarretar sanções administrativas e/ou legais, sem prejuízo da rescisão do contrato de trabalho e/ou qualquer outro contrato de relacionamento de prestação de serviço entre o colaborador, associado, consultor e/ou sócio, assim como qualquer entidade com relação contratual direta ou indireta com a VILEVE PAY.

A observação do descumprimento desta política deve ser imediatamente reportada ao comitê de segurança da informação.

27. DOCUMENTOS DE REFERÊNCIA

⇒ Contrato de Trabalho
⇒ Manual de Normas e Condutas Éticas
⇒ Lei Geral de Proteção de Dados (Lei nº 13.709)

ANEXO 01 – PLGTIANX01 / TERMO DE RESPONSABILIDADE PARA UTILIZAÇÃO DOS RECURSOS DE TI.

Termo de Responsabilidade para Utilização dos Recursos.

A utilização dos recursos de TI deverá estar em conformidade com o presente termo, devendo este documento ser assinado pelo usuário como termo de responsabilidade no ato de sua contratação ou a partir da data de divulgação da Política Geral de T.I.

Equipamentos computacionais

Estão disponibilizados de acordo com as normas de segurança do fabricante do produto.

Devem ser utilizados para uso restrito no desenvolvimento de atividades profissionais.

São de responsabilidade individual, não sendo permitido o acesso a terceiros não autorizados.

São lacrados por motivo de segurança, sendo que em caso de rompimento do lacre, por quaisquer motivos, o usuário deverá informar imediatamente a Gerência de TI, bem como qualquer eventual dano ou extravio.

Não é permitido:

- Remover recursos computacionais de software ou hardware;
- Remover ou transferir para outros equipamentos, documentos de propriedade da VILEVE PAY, ou por ela administrados, salvo autorização expressa;
- A entrada de equipamentos computacionais que não sejam de propriedade da VILEVE PAY, tais como notebook, sem a autorização prévia da Gerência de TI. Em casos de necessidade de entrada de visitantes, clientes e fornecedores com seus próprios equipamentos deverão ser imediatamente informados a Gerência de TI;
- Utilizar os recursos computacionais da VILEVE PAY para efetuar trabalho de natureza particular, sem prévia autorização;
- O uso de modens para conexões externas dentro das dependências da VILEVE PAY sem prévia autorização da Gerência de TI.

NOTA: A Gerência de TI tem acesso irrestrito aos arquivos de dados dos equipamentos computacionais, sempre que se fizer necessário, como para execução de backup, diagnóstico de problemas, suspeita de violação, etc.

Softwares

São adotados controles pela Gerência de TI da VILEVE PAY para impedir a cópia ou uso de softwares não autorizados. Qualquer software não autorizado será retirado imediatamente.

Os usuários não poderão modificar os arquivos de configuração ou registro. As mudanças de configuração, que se fizerem necessárias, serão realizadas somente pela Gerência de TI.

Não é permitido:

- Fazer uso de software de jogos;
- Transmitir, difundir ou disponibilizar, informações, dados, conteúdos, mensagens, gráficos, desenhos, arquivos, sons e /ou imagens, fotografias, gravações, softwares ou quaisquer classes de materiais que não estejam relacionados às atividades profissionais da VILEVE PAY;
- A exibição de quaisquer tipos de imagens ou documentos sexualmente explícitos, não devendo estes serem arquivados, armazenados, distribuídos, editados ou gravados usando os recursos e infraestrutura de TI da VILEVE PAY, sendo vetado o acesso a sites de conteúdo pornográfico, ofensivo ou relacionados a atividades ilegais;
- O acesso não autorizado aos dados computacionais da VILEVE PAY, bem como, tentativa de alteração, destruição e divulgação indevida dos mesmos;
- O acesso a mensagens pessoais de terceiros, bem como a arquivos confidenciais.

Disposições Gerais

O *login* e senha do usuário da rede da VILEVE PAY constituem a identidade do usuário, devendo os mesmos ser mantidos confidenciais, sendo expressamente proibido o seu compartilhamento.

Em caso de violação a este termo cabe à Gerência de TI analisar e sugerir as devidas penalidades, junto a diretoria.

ANEXO 02 - PLGTIANX02 / TERMO DE RESPONSABILIDADE PARA UTILIZAÇÃO DOS RECURSOS DE INTERNET E E-MAIL

Termo de Responsabilidade para Utilização dos Recursos de Rede WiFi Internet e e-mail

REDE WIFI

É disponibilizado na infraestrutura de rede da VILVE PAY a modalidade de rede **Wi-Fi** (***Wireless Fidelity***) que é um tipo de rede local que utiliza sinais de rádio para comunicação.

A finalidade deste recurso é permitir a comunicação, dos colaboradores autorizados pela TI da VILEVE PAY, por meio de sinais de rádio, em ambientes onde há limitação do acesso à rede física, a um ambiente restrito, ou onde não há as redes cabeadas.

A utilização deste recurso está disponível, estritamente, para fins corporativos, sendo vetado a utilização para outros fins.

Considera-se violação das regras o seguinte:

- Divulgar as credenciais de acesso à rede *WiFi* da **VILEVE PAY** para qualquer pessoa. Estas informações são de caráter sigiloso e de responsabilidade da TI **VILEVE PAY**.
- Utilizar os recursos da rede ***WIFI*** para fins ilícitos e proibidos.
- Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais da **VILEVE PAY**.

Monitoramento / Auditoria Rede *Wifi*

A **VILEVE PAY**, através da Gerencia de TI, se reserva o direito, a qualquer tempo e sem aviso prévio, de examinar os registros de tráfego da rede ***Wifi*** para verificação de atendimento à Política de Segurança.

Tais registros podem referir-se a websites visitados, arquivos copiados da Internet, tempo gasto nos acessos e outras informações necessárias para a otimização dos recursos de acesso e realização de auditoria.

Esta política tem a finalidade de estabelecer as regras e orientar as ações e procedimentos na utilização da rede sem fio, além de garantir a continuidade dos serviços na VILEVE PAY.

Os Colabores que tiverem interesse em utilizar a rede sem fio, para realização dos seus trabalhos, deverão solicitar à Gerencia de TI.

INTERNET

A utilização dos recursos de Internet da VILEVE PAY é restrita aos profissionais autorizados pela Gerência de Área ou Diretoria. Estes recursos devem ser usados estritamente para atender as necessidades das atividades de trabalho, devendo estar em conformidade com as diretrizes deste termo, devendo o mesmo ser assinado pelo usuário como termo de responsabilidade.

O sistema de segurança instalado na rede da VILEVE PAY é capaz de monitorar e gravar todo o uso da Internet, ou seja, acessos a *websites*, conversações virtuais, acessos a grupos de notícias, envio ou recebimento de mensagens de correio eletrônico, bem todas as transferências de arquivos. Assim nenhum usuário deve esperar qualquer tipo de privacidade quanto ao uso de Internet e correio eletrônico, pois é reservado à Gerência de TI o direito de verificar os dados monitorados e gravados a qualquer momento.

Ao participar de conversações virtuais ou grupos de notícias, e/ou ao estabelecer contas em sistemas computacionais externos em atendimento a necessidades de trabalho, o usuário das conexões de Internet da VILEVE PAY deverá se identificar de maneira honesta, exata e completa (incluindo a afiliação a VILEVE PAY e sua função, se solicitado).

A VILEVE PAY retém o direito de autoria sobre quaisquer dados publicados através de sua rede em quaisquer foros, grupos de notícias, conversações virtuais ou páginas de internet (***www***). Como estes foros são públicos, não é apropriado revelar informações confidenciais da VILEVE PAY, de clientes ou de quaisquer dados desta natureza.

É expressamente proibida a utilização do Logotipo da VILEVE PAY e/ou quaisquer informações de propriedade da VILEVE PAY em páginas pessoais.

Não é permitido usar as conexões de Internet da VILEVE PAY para:

- Acessar, armazenar, imprimir ou distribuir qualquer dado que não estejam diretamente relacionados com as atividades de trabalho da VILEVE PAY, valendo ressaltar que a Internet permite o acesso a inúmeros dados que podem ser considerados ofensivos, devendo os mesmos ser evitados qualquer acesso;
- Fazer download ou distribuir intencionalmente softwares ou dados pirateados;
- Fazer download de jogos, músicas ou softwares de entretenimento;
- Participar de jogos em rede através da Internet;
- Publicar informações da VILEVE PAY sem prévia autorização;
- Utilizar inadequadamente os bens ou recursos de TI da VILEVE PAY, como por exemplo, roubo de propriedade intelectual, assédio sexual, etc.
- Constitui uma violação gravíssima, a exibição de quaisquer tipos de imagens ou documentos sexualmente explícitos, não devendo estes ser arquivados, armazenados, distribuídos, editados ou gravados usando os recursos e infraestrutura de TI da VILEVE PAY.
- É vetado o acesso a sites de conteúdo pornográfico, ofensivo ou relacionados a atividades ilegais. Caso o usuário conecte acidentalmente a um endereço desta natureza deverá desconectar-se imediatamente.
- A rede de computadores da VILEVE PAY possui Firewall instalado, que garante a segurança e privacidade, não sendo permitido ao usuário usar as conexões de Internet da VILEVE PAY para:
- Propagar deliberadamente qualquer *Vírus, Worm*, Cavalo de Tróia, *Spyware* ou código de programas que constituam uma armadilha e/ou ameaça;
- Tentar desabilitar, ultrapassar ou evitar qualquer software ou equipamento de segurança da VILEVE PAY relativos a TI.
- Desabilitar ou sobrecarregar qualquer sistema ou rede computacional, ou passar sobre qualquer sistema cujo propósito seja proteger a privacidade/segurança dos usuários.
- Utilizar o serviço para transmitir ou divulgar material ilícito, proibido ou difamatório que viole a privacidade de terceiros, ou que seja abusivo, ameaçador, discriminatório, injurioso ou calunioso.
- Utilizar o serviço para transmitir/divulgar material que incentive discriminação ou violência.

- Transmitir e/ou divulgar qualquer material que viole direitos de terceiros, incluindo direitos de propriedade intelectual.
- Obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores da VILEVE PAY.
- Interferir ou interromper o serviço, as redes ou os servidores conectados ao parque tecnológico da VILEVE PAY.
- Usar de falsa identidade ou utilizar dados de terceiros para obter acesso aos recursos computacional da VILEVE PAY.
- Tentar enganar ou subverter as medidas de segurança dos sistemas e da rede de comunicação da VILEVE PAY.
- Utilizar serviço de proxy *(Proxy Tunnel)* para burlar sites com acesso não autorizado.
- Efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais da VILEVE PAY.
- Utilizar os recursos da Internet da VILEVE PAY para intimidar, assediar, difamar ou aborrecer qualquer pessoa.
- Consumir inutilmente os recursos da Internet da VILEVE PAY de forma intencional.
- Desenvolver qualquer outra atividade que desobedeça às normas apresentadas acima.

Os computadores com modens próprios para criar conexões independentes de dados esquivam os mecanismos de segurança da rede VILEVE PAY, assim a conexão privada de computador individual a qualquer computador externo pode ser usada por um atacante para pôr em perigo a rede da VILEVE PAY.

Caso seja necessário o *download* de softwares para realização das atividades de trabalho, deverá ser solicitada a autorização da Gerência de TI, que procederá ao devido registro após verificar as condições de licença e direitos do autor, passando o software em questão ser propriedade da VILEVE PAY, da mesma forma, o *download* de quaisquer arquivos deverá ser autorizado.

Em caso de necessidades profissionais, os usuários deverão programar, junto a Gerência de TI, suas operações de comunicações consideradas pesadas, como transferências de arquivos de grande tamanho, *download* de vídeos, envio de mensagens eletrônicas em massa, ou operações similares para as horas que sejam de menor tráfego, ressaltando que as tecnologias para baixar

e pôr em serviço vídeos e áudios representam um tráfego significativo de dados que pode causar um congestionamento, devendo os mesmos serem evitados.

Disposições Gerais

A Gerência de TI ao verificar os dados relativos ao uso da Internet e julgar haver alguma irregularidade poderá divulgar a mesma à Gerência de Área, solicitando as devidas providências junto ao usuário, visando assegurar os mais altos níveis de produtividade na VILEVE PAY.

É reservada a Gerência de TI o direito de inspecionar todos os arquivos armazenados nos computadores e áreas privadas da rede VILEVE PAY.

As conexões da Internet e os recursos computacionais da VILEVE PAY não deverão ser usadas quando houver ciência de que estão sendo violadas as diretrizes estabelecidas neste documento.

Declaro expressamente estar de acordo com as diretrizes citadas neste documento e que é minha responsabilidade cumpri-las. Por ser verdade firmo o presente.

Colaborador:_____

Data:____/_____/_____

Assinatura:_____

ANEXO 03 - PLGTIANX03 / TERMO DE RESPONSABILIDADE PARA EMPRÉSTIMO DE EQUIPAMENTO DE TI

Termo de Responsabilidade para Empréstimo de Equipamento de TI

O empréstimo do equipamento, de propriedade da **VILEVE PAY**, deverá estar em conformidade com as seguintes diretrizes, devendo este documento ser assinado pelo solicitante como termo de responsabilidade.

A **VILEVE PAY** está disponibilizando o equipamento citado no descritivo abaixo, para o solicitante, sendo que seu uso deve ser exclusivo para o desempenho das atividades de trabalho, ficando expressamente vetado a utilização para outros fins.

O solicitante é responsável pelo correto manuseio e utilização do equipamento recebido, consoante com as normas de segurança da **VILEVE PAY** e cuidados estabelecidos pelo fabricante do produto.

O solicitante declara que o cumprimento deste termo é sua responsabilidade, e que caso ocorra quaisquer danos ou perdas, oriundos de dolo ou culpa, autoriza os descontos referentes aos mesmos em sua remuneração.

Desta forma, declaro expressamente estar de acordo com as diretrizes citadas neste documento e que é minha responsabilidade cumpri-las.

Data:___/___/____

Nº. Patrimônio/Equipamento:_____

Colaborador:_____

Assinatura:_____

ANEXO 03 - PLGTIANX03 / TERMO DE RESPONSABILIDADE PARA EMPRÉSTIMO DE EQUIPAMENTO DE TI

Devolução

Recebido por: _____

Assinatura:_____

Data:____/_____/____

Observações:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

ANEXO 04 - PLGTIANX04 / TERMO DE RESPONSABILIDADE PARA CONCESSÃO RECURSO TI

Termo de Responsabilidade para Concessão de Recurso de TI

A concessão da utilização de recursos de TI nos equipamentos de propriedade da *VILEVE PAY* será feita de forma restrita e deverá estar em conformidade com as diretrizes de segurança da empresa, devendo este documento ser assinado pelo solicitante como termo de responsabilidade.

A VILEVE PAY está disponibilizando o(s) recurso(s) citado no descritivo abaixo, ao solicitante, sendo que seu uso deve ser exclusivo para o desempenho das atividades de trabalho, ficando expressamente vetado a utilização para outros fins.

O solicitante é responsável pela correta utilização do(s) recurso(s) disponibilizado(s).

O solicitante declara que o cumprimento deste termo é sua responsabilidade e que caso ocorra quaisquer danos ou perdas ocasionadas pela utilização indevida destes recursos, sofrerá as devidas penalidades.

Este termo também se aplica à situações relacionadas ao distanciamento social e o home office quando necessários em razão da Pandemia causada pela Covid-19, para fins de execução dos processos vinculados à função do colaborador.

Desta forma, declaro expressamente estar de acordo com as diretrizes citadas neste

Colaborador: _____

NºPatrimônio/Equipamento:_____

Data Concessão:____/____/_____

Assinatura:_____

02-03/04/23	Revisão	GP	GP	Diretoria
01-02/06/22	Revisão	GP	GP	Diretoria
00-27/04/21	Emissão Inicial	Gestão de TI	Gestão de Pessoas	Diretoria
Revisão/Data	Descrição	Elaboração	Verificação	Aprovação