SUMÁRIO

1. DECLARAÇÃO

"A Mannesoft está comprometida em implementar e monitorar seus controles de segurança da informação e privacidade para garantir a confidencialidade, integridade, disponibilidade de todo ativo de informação atendendo a legislação, regulamentações e requisitos contratuais de seus clientes, colaboradores, e partes externas interessadas sempre buscando a melhoria contínua de seus produtos, processos e serviços."

2. INTRODUÇÃO

A informação utilizada pela MANNESOFT são bens que têm valor. Eles devem ser gerenciados adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade e privacidade independentemente do meio de coleta, garantindo a segurança em todo o ciclo de vida da informação, desde a coleta até o descarte seguro das informações.

Para garantir a implementação adequada do SGPI, foram utilizadas políticas e procedimentos separados para cada área de segurança da informação e privacidade e, quando aplicável, consta a referência a essas políticas externas neste documento.

Todas as políticas e procedimentos de segurança da informação e privacidade devem ser lidos e referidos em conjunto entre si, pois seus significados, controles e medidas são complementares. As políticas e documentos que fazem parte do SGPI da MANNESOFT serão descritos no neste documento.

Dessa forma, a MANNESOFT estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

3. PROPÓSITO

Este documento é um conjunto de normas que tem como finalidade orientar o gerenciamento das informações, protegendo e garantindo os pilares de confidencialidade, integridade, disponibilidade e privacidade em observância das normas NBR ISO/IEC 27001:2022, NBR ISO/IEC 27701:2019, NBR ISO/IEC 27017:2016 e NBR ISO/IEC 27018:2021 e leis aplicáveis.

- **Disponibilidade:** Que os ativos e as informações estejam disponíveis e acessíveis aos usuários autorizados quando necessário;
- **Integridade:** Que as informações estejam protegidas de modificações, destruição deliberada ou acidental por usuários autorizados e não autorizados, garantindo a exatidão das informações da organização;
- **Confidencialidade:** Que as informações só possam ser acessadas e visualizadas por pessoas autorizadas evitando sua divulgação deliberada ou acidental;

- **Privacidade:** dispõe sobre o tratamento de dados pessoais, em qualquer meio, realizado por pessoas ou organizações, e que visa a proteger os direitos dos titulares de dados e determinar as responsabilidades dos agentes de tratamento em consonância com a regulamentação legal e normativa as boas práticas de governança corporativa, a boa-fé dos agentes e o interesse das partes interessadas.

4. ESCOPO

Esta política de Segurança da Informação se aplica a:

- Quaisquer softwares fornecidos ou sob o controle da Mannesoft;
- Quaisquer comunicações enviadas ou recebidas;
- Quaisquer dados pertencentes, controlados ou processados, incluindo dados mantidos em sistemas externos;
- Locais a partir dos quais os dados são acessados, incluindo uso doméstico e externo;
- Ativos de informação mantidos, processados ou armazenados nas instalações ou locais externos;
- Informações em trânsito pelas redes de voz ou dados.

Todos os colaboradores da MANNESOFT (empregados, prestadores de serviço, representantes ou subcontratados de terceiros, estagiários e aprendizes) devem conhecer esta política. A adesão a esta política é obrigatória e o não cumprimento pode levar a sanções disciplinares.

5. PAPÉIS E RESPONSABILIDADES

Todos os usuários: É responsabilidade de qualquer indivíduo ou organização que tenha acesso aos sistemas e informações da MANNESOFT cumprir esta política de segurança da informação e as diretrizes, medidas e procedimentos associados a ela.

Analista da qualidade: Tem a responsabilidade global pela manutenção deste documento e seus procedimentos associados.

Gerente de Macroprocessos (Infraestrutura): Tem a responsabilidade pela coordenação das atividades operacionais associadas à segurança da informação. Cabe ao mesmo, recepcionar os relatos de qualquer suspeita ou real falha, ameaças, eventos ou incidentes de segurança da informação.

Comitê do SGPI: Tem a responsabilidade pela governança das disposições deste documento, bem como a revisão desta política anualmente, ou quando mudanças que afetem o SGPI sejam identificadas para garantir que ela esteja em conformidade com todos os requisitos e regras legais, estatutárias e regulamentares. É de inteira responsabilidade do comitê do SGPI garantir que essas revisões ocorram e que o conjunto de políticas esteja e permaneça internamente consistente.

6. POLÍTICAS E DIRETRIZES

As políticas e diretrizes de segurança da informação e privacidade são aplicáveis tanto aos sistemas computadorizados quanto aos meios convencionais de processamento, comunicação e armazenamento de informações. Devem ser seguidas por todos os colaboradores, cabendo a cada um a responsabilidade pelo seu cumprimento.

O objetivo da gestão de Segurança da Informação e Privacidade da MANNESOFT é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação e privacidade, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos na organização.

6.1. USO ACEITÁVEL DOS ATIVOS

Todos os colaboradores têm a responsabilidade de proteger as informações e os ativos de informação sob sua responsabilidade que devem ser usados de maneira aceitável e de acordo com esta e outras políticas e processos relacionados ao SGPI.

6.2. MESA LIMPA TELA LIMPA

Os dispositivos de computação desacompanhados ou não sendo utilizados são protegidos com uma tela ou mecanismo de bloqueio controlado por senha ou mecanismo de autenticação semelhante (isso inclui laptops, tablets, smartphones e estações de trabalho).

Ao ausentar-se de sua estação de trabalho ou laptop, é obrigatório bloqueá-lo imediatamente, como medida básica de proteção à informação. Isso impede o acesso não autorizado a dados e sistemas enquanto o dispositivo estiver desacompanhado.

- Para computadores Windows: use Ctrl + Alt + Del e selecione "Bloquear", ou pressione Windows + L;
- Para computadores macOS (MacBook): use Control + Command (⌘) + Q.

O bloqueio deve ser realizado sempre que o colaborador se afastar do equipamento, mesmo que por breves períodos.

Ao visualizar informações confidenciais ou que contenham dados pessoais em uma tela, os usuários devem estar cientes de seus arredores e devem garantir que pessoas não autorizadas não consigam visualizar tais informações. As telas dos computadores nas quais informações confidenciais ou pessoais são processadas ou visualizadas devem ser posicionadas de tal forma que não possam ser visualizadas por pessoas não autorizadas.

Informações confidenciais ou de acesso restrito, por exemplo, em papel ou em meio de armazenamento eletrônico, devem ser protegidas quando não exigidas, especialmente quando o escritório é desocupado no final do expediente. Deve-se também tomar cuidado ao imprimir documentos confidenciais ou de acesso restrito para evitar a divulgação não autorizada.

6.3. USO DA INTERNET

O uso da Internet deve ser realizado de modo consciente, segundo a necessidade para execução das atividades laborais e, eventualmente, pessoais. O uso abusivo, que possa comprometer o bom desempenho laboral, ou conscientemente colocar em risco ativos da informação da empresa, pode resultar em advertências verbais ou formais, de acordo com a gravidade. O acesso à Internet em ativos da empresa é monitorado e controlado por meio de um sistema de filtro de conteúdo (Antivírus e Firewall), salvo se houver necessidade explícita de acesso irrestrito para a execução da atividade laboral relacionada à função. O acesso irrestrito é autorizado por gestor ou diretor.

6.4. USO DO E-MAIL

O uso do e-mail corporativo para fins pessoais é impróprio e não é permitido em nenhum momento. Você só deve usar os sistemas de e-mail fornecidos pela Mannesoft para enviar e receber informações da Mannesoft.

Você não deve usar o sistema de e-mail de forma insultuosa ou ofensiva. Todos os e-mails enviados interna ou externamente possuem um aviso de confidencialidade. Para alterar a classificação deve-se considerar POL-SG-0002 - POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

Se você receber um e-mail impróprio ou abusivo, deve relatá-lo imediatamente ao seu superior, que tomará as medidas cabíveis. Se o remetente for conhecido por você, informe-o de que ele deve interromper o envio do material. E-mails que parecem suspeitos, podem ser tentativas de "phishing" ou malware, devem ser relatados imediatamente como um incidente de segurança.

6.5. USO DE MÍDIAS REMOVÍVEIS

Entende-se por mídia removível qualquer tipo de memória que pode ser removida conferindo portabilidade para os dados que foram armazenados nela. Alguns exemplos de mídias removíveis são: PEN DRIVE, HD EXTERNO, memória USB, entre outros.

A Mannesoft possui diretrizes para o uso de mídias removíveis que estão documentadas na POL-SG-0007 - POLÍTICA DE MÍDIAS REMOVÍVEIS.

6.6. DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

Qualquer pessoa que armazena ou transporta dados e informações relacionadas com a Mannesoft, usando dispositivos móveis é considerada pela empresa como responsável pela segurança e privacidade dos dados e deve tomar as medidas adequadas e apropriadas para protegê-los. Dados restritos ou confidenciais não devem ser copiados, replicados ou baixados para celular ou dispositivos remotos sem a permissão do proprietário das informações. Onde a permissão for concedida, medidas adequadas devem ser tomadas pelo usuário para proteger os dados enquanto eles existem no dispositivo móvel ou remoto.

Perda ou furto de equipamento (corporativo ou não) que foi usado para acessar os ativos de informação da Mannesoft ou que possam ter uma cópia ou parte de informação devem ser comunicados à Gerência de Macroprocessos (Infraestrutura), área de infraestrutura e ao Gerente Administrativo. Se houver perda ou divulgação não autorizada de dados confidenciais, sensíveis ou pessoais da Mannesoft devido a práticas inadequadas ou negligência de sua parte, uma ação disciplinar pode ser tomada contra o infrator.

Os colaboradores da Mannesoft que exercem trabalho remoto devem seguir as medidas de segurança e proteção de dados para garantir uma comunicação com segurança e que seus dispositivos estejam protegidos contra ameaças. Boas práticas de segurança para dispositivos móveis e trabalho remoto:

- Quando em deslocamentos de carro, coloque o notebook no porta-malas ou em local não visível;
- Ao movimentar-se com o notebook, se possível, não utilize malas convencionais para notebook e sim mochilas ou malas discretas;
- Em locais públicos (recepção de hotéis, restaurantes e aeroportos dentre outros), mantenha o notebook próximo e sempre à vista, não se distanciando do equipamento;
- Evite utilizar o notebook em locais públicos;
- Nos hotéis, sempre que possível, guarde o notebook no cofre do seu apartamento;

- Para tablets e celulares sempre utilize o bloqueio de tela com senha;
- Não conecte em redes Wi-Fi desconhecidas, essas redes podem conter mecanismos para captura de dados do seu dispositivo;

A utilização do Whatsapp na empresa estará condicionada a utilização de autenticação de dois fatores, evitando assim clonagem no número e a divulgação de informações da empresa e somente em smartphones habilitados pela empresa.

6.7. RESTRIÇÕES SOBRE O USO E INSTALAÇÕES DE SOFTWARE

Os softwares são gerenciados e controlados de acordo com as políticas da empresa em relação ao gerenciamento de ativos e contratos de licença. Todos os softwares usados em dispositivos gerenciados pela empresa devem ser instalados de acordo com as diretrizes internas de licenciamento de software atuais.
A instalação, atualização e desinstalação de software somente é executada pelos profissionais da área de infraestrutura.
Violar os direitos de qualquer pessoa ou empresa protegida por direitos autorais, segredo comercial, patente ou outra propriedade intelectual, ou leis ou regulamentos semelhantes, incluindo, mas não se limitando a, instalação ou distribuição de produtos "pirateados" ou outros produtos de software que não sejam apropriadamente licenciados pode deixar o colaborador sujeito a ação disciplinar.

6.8. SENHAS

Senhas e outras formas de autenticação secreta, tais como chaves criptográficas e padrões de desenho, utilizadas para acessos a dispositivos, redes e sistemas, são de uso exclusivo do usuário, portanto não devem ser compartilhadas. Da mesma forma, o usuário não deve utilizar a senha de outra pessoa.

As senhas e outras formas de autenticação secreta são de complexidade suficiente para serem difíceis de serem adivinhadas. Para atender a este requisito, o cofre de senhas indicado de pela Mannesoft deve ser utilizado, pois com a sua devida utilização as senhas são compostas de números, caracteres especiais, letras maiusculas e minúsculas. Nos sistemas onde for possível, o responsável pelo sistema deve configurá-lo para que a complexidade de senha seja obrigatória.

O colaborador é responsável por todas as transações atribuídas ao seu identificador de usuário, confirmado por senha ou outra forma de autenticação secreta.

Ao suspeitar de que uma senha ou outra forma de autenticação secreta possa ter sido comprometida, o colaborador deve alterá-la imediatamente em todos os dispositivos, redes e sistemas em que ela esteja sendo utilizada e comunicar, também imediatamente, à área responsável pela gestão de incidentes de segurança da informação.

Consultar a POL-SG-0009 - POLÍTICA DE SENHAS para regras sobre o cumprimento de senhas e o uso de frases secretas.

6.9. CONTRATOS DE TRABALHO

Os requisitos de segurança são tratados na fase de recrutamento e todos os contratos de trabalho contém cláusulas de confidencialidade e privacidade. Os requisitos de segurança, proteção de dados e privacidade estão incluídos nas definições de trabalho.

6.10. PROTEÇÃO CONTRA MALWARE

Todas as estações de trabalho da empresa possuem software antivírus instalado e configurado para atualizar as assinaturas antivírus automaticamente. As estações de trabalho são verificadas periodicamente em busca de malware, programas maliciosos ou indesejados.

Todos os sistemas serão protegidos por várias camadas de segurança envolvendo firewall, segmentação de rede, AntiSpam e proteção contra malware em todas as estações de trabalho na rede da empresa.

O tráfego de entrada e saída da rede é monitorado para identificar qualquer atividade anômala que possa ser uma ameaça à segurança da rede.

6.11. CONTROLE DE ACESSOS

O acesso às informações é restrito a usuários autorizados que tenham uma necessidade de acessar as informações. Todos os ativos de informação são protegidos de forma a garantir sua confidencialidade, integridade, disponibilidade e privacidade.

O acesso às informações está de acordo com a POL-SG-0006 - POLÍTICA DE CONTROLE DE ACESSO e ser restrito ao mínimo necessário para realizar atividades de negócios autorizada. A Mannesoft adota o princípio de que "o acesso é proibido a menos que tenha sido especificamente e formalmente autorizado".

Procedimentos para o registro e cancelamento de registro de usuários para o acesso a todos sistemas de informação são estabelecidos para garantir que todos os direitos de acesso do usuário correspondem à sua autorização. Esses procedimentos são implementados pela área de Infraestrutura.

6.12. CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÕES

As informações são classificadas em diferentes níveis de sensibilidade considerando seu valor para a Mannesoft, requisitos legais e impacto devido à perda de confidencialidade, disponibilidade, integridade e privacidade são ser protegidas de acordo com o seu nível de sensibilidade.

Os critérios de classificação estão documentados na POL-SG-0002 - POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO.

6.13. SEGURANÇA FÍSICA E DO AMBIENTE

Todas as instalações de processamento de informações são protegidas por controles físicos apropriados de acordo com requisitos relativos à criticidade, sensibilidade e conformidade regulamentar e riscos para os sistemas ou serviços operados nestes locais.

O acesso de visitantes e prestadores de serviços é acompanhado de um colaborador com acesso autorizado ao ambiente. É proibido o acesso de visitantes e prestadores de serviço, em áreas restritas, sem o devido registro de entrada realizado na portaria.

Encontra- se protegida com uma edificação robusta, possui alarme com detecção de movimento em seu interior bem como nas janelas e câmeras monitorando 24 hs por dia. As medidas de segurança contemplam:

- Alarme com detecção de movimento operante por 24 horas
- Câmeras posicionadas em locais estratégicos tanto na parte interior e exterior do edifício onde está localizada a empresa;
- O disparo do alarme aciona gestores e colaboradores responsáveis
- O alarme contra incêndio conta com monitoramento de detecção de fumaça;
- O acesso a áreas seguradas, como a recepção, almoxarifado, produção e sala de equipamentos de TI, mas não se limitando a elas, conta com uma porta com dispositivo de leitura, ou seja, utilizando cartão magnético, biometria ou uso de senha;
- Locais onde há servidores, permanecem com as portas fechadas na ausência dos colaboradores destes setores e não devem conter identificação.

6.14. BACKUP

A Mannesoft realiza backup e testa regularmente as informações essenciais, estejam elas armazenadas em servidores locais ou nuvem. A periodicidade, retenção, abrangência e tipo de backup são definidos de acordo com a criticidade da informação ou sistema para a organização. Os colaboradores devem armazenar as informações no servidor de arquivos que é salvaguardado por backup. As definições relacionadas a backup estão documentadas na POL-SG-0005 - POLÍTICA DE BACKUPS.

6.15. GERENCIAMENTO DE VULNERABILIDADES TÉCNICAS

A gestão das vulnerabilidades é realizada através de um comitê composto por um membro da equipe de infraestrutura, um membro de cada um dos sistemas disponíveis (Winner, Prime, +Lojas e Backoffice Mannesoft, tendo ainda um Sistema Saas que faz o monitoramento em tempo real das vulnerabilidades encontradas.

Acompanhamento e tratativas que são realizados podem ser evidenciados detalhadamente no Procedimento PO-SG-0008 - GESTÃO DE VULNERABILIDADES.

6.16. CONTROLES CRIPTOGRÁFICOS

A Mannesoft assegura a utilização efetiva e adequada de criptografia para proteger a confidencialidade, autenticidade e a integridade das informações. As diretrizes para o gerenciamento de chaves e algoritmos criptográficos estão documentadas na POL-SG- 0008 - POLÍTICA DE CONTROLE CRIPTOGRÁFICO.

6.17. SEGURANÇA NAS COMUNICAÇÕES

As redes da empresa são segmentadas por departamento e todo tráfego e acesso é monitorado. A segregação da rede é baseada nos princípios de segurança da “segregação de funções” e “menor privilégio”.

Todos os colaboradores possuem um ID e senha único, que não deve ser compartilhado, para acessar sua estação de trabalho.

A Mannesoft possui um firewall que monitora e bloqueia ataques, vírus e atua como filtro de conteúdo. O analista de redes monitora rotineiramente o tráfego da rede, incluindo o tráfego da Internet, para utilização da largura de banda e para fins de segurança. Se o analista de segurança da informação se deparar com o uso inadequado de recursos de rede, essa ocorrência será levada ao conhecimento do Gerente de Macroprocessos (Infraestrutura) para a ação corretiva necessária.

6.18. RELACIONAMENTO NA CADEIA DE SUPRIMENTOS

Qualquer fornecedor que colete, armazene, manuseie, transmita, processe, comunique, gerencie ou descarte as informações da Mannesoft deve estabelecer, implementar e manter políticas razoáveis e um programa de medidas de segurança organizacional, operacional, administrativa, física e técnica e organizacional adequadas para impedir qualquer acesso às informações da Mannesoft de uma maneira não autorizada.

O fornecedor garante que sua equipe de segurança da informação tenha experiência necessária em segurança da informação e rede.

A relação com fornecedores que envolve coleta, armazenamento, manuseio, transmissão, processamento, comunicação, gerenciamento ou descarte das informações, sistemas de informação ou recursos de processamento de informações da Mannesoft são baseadas em um contrato formal contendo cláusula de confidencialidade e penalidades. O Código de Conduta e Relacionamento com Fornecedores rege os critérios para contratação, monitoramento e avaliação dos fornecedores.

6.19. INVENTÁRIO DE ATIVOS

Um inventário de ativos é mantido e classificado com base no impacto à organização, devido à perda de sua confidencialidade, integridade, disponibilidade e privacidade. O inventário de ativos atribuiu um proprietário nomeado para cada ativo, que compreenderá totalmente suas responsabilidades para a proteção do ativo. Os ativos inventariados estão registrados RG-SG-0004 Inventário de ativos.

6.20. DESENVOLVIMENTO SEGURO

Os colaboradores da MANNESOFT, membros da equipe de desenvolvimento de software, seguem as diretrizes e procedimentos estabelecidos na POL-SG-0004 - POLÍTICA DE DESENVOLVIMENTO SEGURO e PO-SG-0003 - PROCEDIMENTO DE DESENVOLVIMENTO SEGURO.

7. GERENCIAMENTO DE FALHAS DE SEGURANÇA

A definição da Mannesoft de violação de segurança da informação e privacidade para fins deste, e de outros documentos relacionados, é uma divergência de qualquer procedimento operacional estabelecido pela empresa, que causa uma falha no cumprimento das normas de conformidade exigidas, conforme estabelecido pelos objetivos do próprio sistema de conformidade e ou os de qualquer órgão regulador.

A Mannesoft tem objetivos e controles robustos para prevenir falhas de segurança e para gerenciá-las se ocorrerem. Devido à natureza do negócio, a Mannesoft processa e armazena informações pessoais e dados confidenciais de clientes e, portanto, requer um sistema estruturado e documentado de incidentes de violação para mitigar o impacto de quaisquer violações. Embora tome todos os cuidados com sistemas, segurança da informação e privacidade, os riscos ainda existem ao usar a tecnologia e depender da intervenção humana, necessitando de medidas e protocolos definidos para lidar com quaisquer violações.

A empresa realiza avaliações de riscos e auditoria uma vez ao ano para garantir que processos, funções e procedimentos estejam em conformidade e que as ações para reduzir os riscos estejam em vigor quando necessário. No entanto, caso haja alguma violação, está totalmente preparada para identificar, investigar e mitigar imediatamente e assim reduzir os impactos. Os detalhes podem ser encontrados na POL-SG-0003 - POLÍTICA DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO.

8. SANÇÕES

A falha de contratados, funcionários temporários, públicos, parceiros ou organizações terceirizadas em cumprir a política de segurança da informação da MANNESOFT pode resultar na rescisão dos contratos e relações, suspensão de serviços e ou instauração de processo judicial.

Aos colaboradores que desrespeitarem as normas estabelecidas neste documento, serão aplicadas as seguintes sanções, imediatamente à ocorrência do ato faltoso:

- 2 advertências verbais;
- 2 advertências por escrito;
- 1 suspensão de 3 dias;
- 1 suspensão de 5 dias;
- Dispensa por justa causa.

Objetiva-se que o referido rol de penalidades seja aplicado de forma gradativa, porém, e conforme permite a legislação vigente, quando a gravidade do ato assim demandar, a penalidade será mensurada e aplicada proporcionalmente ao ato faltoso cometido, ainda que a medida anterior não tenha sido levada a efeito.

8.1 ADVERTÊNCIA ESCRITA E SUSPENSÕES

- A suspensão do direito de uso de serviços oferecidos pela rede da empresa por tempo indeterminado poderá ser aplicada além da suspensão do comparecimento ao trabalho;
- No caso de falta considerada leve, penas de advertência e suspensão serão aplicadas nos casos legais e imediatamente após a regular apreciação do ato faltoso, sendo que no caso da suspensão, o funcionário sofrerá o desconto salarial correspondente ao número de dias em que perdurar a penalidade e, conforme legislação vigente (art. 130, CLT), referido período será considerado como falta injustificada para o cômputo das férias.

8.2 JUSTA CAUSA

- Nos casos de falta gravíssima a pena de demissão por justa causa será aplicada nos casos legais e, imediatamente, após regular apreciação através de processo administrativo disciplinar;

- Aos funcionários enquadrados no regime de trabalho CLT, ditos “empregados”, a pena de demissão por justa causa será aplicada nas hipóteses previstas no artigo 482 e parágrafo único da Consolidação das Leis do Trabalho - DECRETO-LEI N.º 5.452, de 1º de maio de 1943 e recente alteração promovida pela Lei nº 13.467/17;

- Aos funcionários terceirizados, será solicitado à empresa prestadora da respectiva mão-de-obra, o afastamento temporário ou definitivo do funcionário, conforme a falta cometida, podendo em último caso a organização solicitar a rescisão do contrato de prestação de serviço.

De acordo com a gravidade analisada e de posse dos registros comprobatórios, o assunto será encaminhado à direção para tomar as medidas cabíveis para o caso em questão.

Conforme a legislação trabalhista vigente, além da aplicação das penalidades disciplinares, o funcionário estará sujeito a desconto salarial para pagamento do prejuízo a que tiver dado causa à organização, o qual será incluído na próxima folha de pagamento a ser gerada após a ocorrência e apuração do ato faltoso, consoante permite o art. 462, § 1º da CLT.

A aplicação destas sanções não isenta o colaborador de sofrer outras penalidades previstas em regulamentos internos (contratos) ou mesmo de sofrer processos penais por crimes de peculato, de extravio, sonegação e inutilização de livro ou documento, de condescendência criminosa, de violação de sigilo funcional entre outros, estabelecidos no código penal, sem prejuízo, ainda da responsabilização civil, também aplicada aos colaboradores que não se enquadrem como funcionários, inclusive a título de indenização por danos morais, quando cabível, nos termos dos arts. 186 c/c 927 do Código Civil.

9. DISTRIBUIÇÃO E IMPLEMENTAÇÃO

9.1. DISTRIBUIÇÃO

Este documento é disponibilizado a todos os colaboradores por meio dos canais de comunicação internos da Mannesoft. Um aviso global é enviado a todos os colaboradores notificando-os sobre a liberação deste documento e sempre que uma revisão significativa for realizada. Um link para este documento é fornecido no site da intranet da Mannesoft.

10. CONSIDERAÇÕES FINAIS

A utilização das informações pelos colaboradores da Mannesoft deve estar de acordo com as políticas da empresa. Todos os usuários devem conhecer e entender esses documentos. A segurança e proteção da informação é uma responsabilidade contínua de cada colaborador da entidade em relação às informações que acessa e gerência. Todos os colaboradores devem utilizar a informação da entidade, de acordo com as determinações desta política de segurança da informação.

O não cumprimento desta política e ou dos demais instrumentos normativos que complementarão o processo de segurança e privacidade constitui em falta grave e o colaborador está sujeito a penalidades administrativas e ou contratuais. Situações não previstas, dúvidas, informações adicionais e sugestões devem ser encaminhadas para o e-mail dpo@mannesoft.com.br, de acordo com o grau de relevância e urgência da questão.

11. NATUREZA DAS ALTERAÇÕES

Tabela – Histórico de revisões

Data	Revisão	Descrição	Alterado por	Aprovado por
5 de set. de 2023	00	Emissão inicial	Fernando Henriqu…	Luis Armando Dias
10 de jan. de 2025	01	Alteração no item 6.8 sobre a utilização de um cofre de senhas; Inclusão do modo de bloqueio para macOS no item 6.2; Alteração no item 6.15 mencionando o processo atualizado da gestão de vulnerabilidades e suas referências.	Fernando Henriqu…	Luis Armando Dias