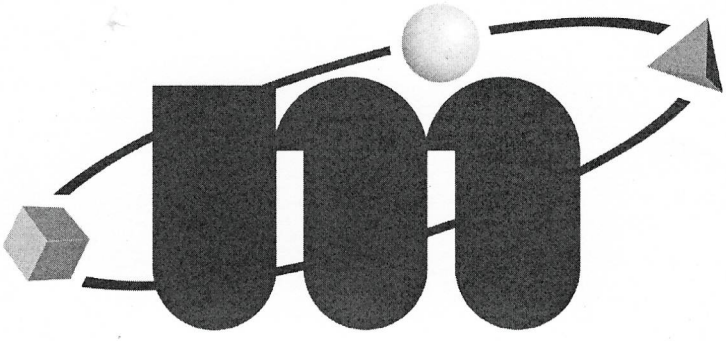

manager
SYSTEMS

Política Segurança da Informação

Rua Patrício Farias, 55 – Sala 307 à 311
88034-132 - Florianópolis - SC - Brasil
Fone: +55 (48) 2108 4000

Home Page: www.mngs.com.br

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO MANAGER SYSTEMS

A política de Segurança da Informação é constituída por regras e procedimentos estabelecidos pela Manager Systems para proteger as informações de ameaças, acessos não autorizados, perda, roubos, dentre outros. Estes procedimentos devem ser seguidos por todos para garantir a confidencialidade, integridade da empresa.

1. OBJETIVO

As informações da Manager Systems são tratadas de forma ética e sigilosa, de acordo com as leis vigentes e as normas internas, evitando-se o mau uso e a exposição indevida.

A presente Política visa estabelecer diretrizes gerais que possibilitem aos profissionais seguirem padrões de comportamento capazes de garantir a observância dos princípios inerentes à segurança da informação, que sejam:

Integridade: garantir de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

Confidencialidade: garantir que o acesso à informação seja obtido somente por pessoas autorizadas.

Disponibilidade: garantir de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2. NORMAS DE REFERÊNCIA

ABNT NBR ISO/IEC 27001:2022 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação -Requisitos.

ABNT NBR ISO/IEC 27002:2022 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.

3. ÂMBITO DE APLICAÇÃO

Esta Política se aplica a todos os profissionais, cientificando-os de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados, em qualquer tempo e circunstância.

É obrigação de cada profissional se manter atualizado em relação a esta Política e aos Procedimentos e Normas a ela relacionadas.

4. DEFINIÇÕES

a) Ambiente Tecnológico: Compreende todos os sistemas, computadores e redes da empresa.
b) Aplicativos de comunicação: Programas de computador, geralmente instalados em dispositivos móveis, usados para troca rápida de mensagens, conteúdos e informações multimídia, a exemplo de WhatsApp, Telegram, Skype, Slack, etc.
c) Ativo: Qualquer coisa que tenha valor para a empresa e precisa ser adequadamente protegida.
d) Antivírus: Programa de proteção do computador que detecta e elimina os vírus (programas danosos) nele existentes, como impede sua instalação e propagação.
e) Profissionais: Empregados, estagiários e empregados terceirizados.
f) TI: Tecnologia da Informação.

g) VPN (Virtual Private Network): Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna.

5. RESPONSABILIDADES

A correta utilização dos recursos disponibilizados é dever dos profissionais, sendo que o uso indevido, negligente ou imprudente será responsabilizado, conforme normativos internos e legais. A Manager Systems reserva-se o direito de analisar dados e evidências, a fim de obter provas, que possam ser utilizadas nos processos investigatórios, bem como, de adotar as medidas legais cabíveis.

5.1 DOS PROFISSIONAIS EM GERAL

a) Conhecer e cumprir a presente Política.
b) Buscar orientação em caso de dúvidas relacionadas à Segurança da Informação.
c) Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados.
d) Garantir a confidencialidade e o sigilo das informações, fornecendo aos terceiros apenas os dados estritamente necessários à realização da sua atividade.
e) Assegurar que os recursos tecnológicos à sua disposição sejam utilizados para atividades profissionais.
f) Comunicar imediatamente quando do descumprimento ou violação desta política via sistema de chamado para o Consultor Técnico de TI.

5.2 DAS DIRETORIAS E GESTORES

Além dos itens citados para todos os colaboradores, as diretorias e gestores devem:

a) Fazer cumprir as normas aqui presentes;
b) Assegurar que as equipes possuam acesso e conhecimento desta Política;
c) Apoiar, incentivar e acompanhar a participação ativa de todos os colaboradores no Plano de Divulgação e Treinamento;
d) Promover juntamente com o responsável da TI a segregação de acessos necessários aos sistemas da Manager Systems, evitando conflitos de interesse e adotando perfis de acesso.

5.3 ÁREA DE TI / SEGURANÇA DA INFORMAÇÃO

a) Executar as ações necessárias para tratar violações de segurança no âmbito tecnológico;
b) Configurar os equipamentos, instalar softwares e implementar os controles necessários, bem como, definir regras para a instalação de software e hardware nos equipamentos da empresa;
c) Coordenar as atividades de tratamento e resposta a incidentes de TI;
d) Promover a recuperação de sistemas, se necessário;
e) Orientar e informar aos profissionais as práticas necessárias à segurança da informação dos dados digitais;
f) Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos operacionais considerados críticos;
g) Planejar e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida e a disponibilidade da rede interna;

h) Assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades na rede e nos equipamentos;
i) Promover guarda de logs de auditoria dos sistemas da Manager Systems sempre que os mesmos fornecerem a referida possibilidade.

5.4 ÁREA DE RISCOS E CONTROLES INTERNOS

a) Avaliar os riscos do processo juntamente com os responsáveis;
b) Elaborar e executar planos de testes e realizar auditoria nos controles relacionados à Segurança da Informação.

6. DIRETRIZES

A fim de garantir que as informações da Manager Systems sejam adequadamente gerenciadas e protegidas contra roubo, fraude, espionagem, perda não intencional, acidentes e outras ameaças, bem como, de que os princípios inerentes à Segurança da Informação sejam preservados, faz-se necessária a observância das seguintes diretrizes:

6.1 PROPRIEDADE INTELECTUAL

Toda informação produzida, acessada, recebida, manuseada ou armazenada pelos profissionais, como resultado da atividade profissional, bem como, a reputação, a marca e demais ativos são de propriedade e direito de uso exclusivos da Manager Systems, sendo, portanto, proibido cópias, reproduções ou distribuições sem a devida autorização.

A utilização da marca, id visual e demais sinais distintivos da Manager Systems, em qualquer veículo de comunicação, inclusive na internet e nas mídias sociais, só poderão ser feitos para atender a atividades profissionais.

6.2 CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade de cada gestor estabelecer critérios relativos ao nível de confidencialidade da informação gerada ou recebido por sua área, de acordo com os critérios a seguir:

a) **Pública**: Informações da empresa com linguagem e formato dedicado à divulgação ao público em geral, sendo de caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação.
b) **Restrita**: Informações de conhecimento exclusivo dos profissionais da empresa e deve ser divulgada apenas para o público interno.
c) **Confidencial**: É uma informação crítica para os negócios da empresa ou de parceiros, devendo haver indicação do nome ou cargo dos profissionais. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda ações administrativas, civis e/ou criminais.

6.3 GUARDA E DESCARTE DE DOCUMENTOS

As áreas devem observar a exigência e o prazo legal definido em tabela vigente à época, para manutenção dos documentos produzidos em razão de suas atividades. Decorrido o prazo para armazenamento os documentos devem ser destruídos antes de descartados, mediante autorização prévia da Diretoria.

Os descartes dos documentos mantidos na empresa deverão seguir o mesmo procedimento dado aos documentos de guarda externa.

6.4 CONTROLES DE ACESSO / LOGINS

Para cada profissional é fornecido dispositivos de identificação pessoal, como crachá, códigos de acesso e senhas, os quais, não poderão ser compartilhados, divulgados ou transferidos a outra pessoa.

É de responsabilidade de cada profissional a guarda dos dispositivos de identificação que lhe forem designados (crachá), bem como, a memorização de sua própria senha, não devendo anotar ou armazená-las em arquivos eletrônicos (Word, Excel, etc.).

Se existir login de uso compartilhado por mais de um profissional, a responsabilidade perante a empresa e a legislação (cível e criminal) será dos profissionais que se utilizarem.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum profissional for demitido ou solicitar demissão, licenças ou outro tipo de afastamento, o Coordenador de RH deverá imediatamente comunicar o departamento de TI.

No caso de profissionais cujo contrato ou prestação de serviços tenham se encerrado, o responsável pelo contrato deverá comunicar imediatamente tal fato à área de TI.

6.5 UTILIZAÇÃO DA REDE

Todos os arquivos devem ser gravados na rede ou, se possível, na nuvem, pois arquivos gravados no computador não possuem cópias de segurança (backup) e podem ser perdidos.

O espaço na rede é controlado pelo Consultor de TI, assim, os usuários devem administrar suas pastas, excluindo arquivos desnecessários.

Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc..) nos drivers de rede, pois ocupam espaço comum limitado ao departamento. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente, sem prévia comunicação.

6.6 USO DOS EQUIPAMENTOS DE INFORMÁTICA E COMUNICAÇÃO

As estações de trabalho possuem códigos internos (IP), que permitem a rastreabilidade das atividades executadas, assim como, é possível o responsável de TI monitorar acessos realizados através da rede, sendo de responsabilidade de cada profissional zelar pelos seus respectivos acessos.

6.7 USO DAS MÍDIAS REMOVÍVEIS

O uso de mídias removíveis deve ser tratado como exceção à regra, pois a porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais, sendo assim, as mesmas estão bloqueadas e podem ser liberadas com devida solicitação e autorizações em casos extremos.

6.8 USO DA INTERNET

A internet, via cabo ou Wi-fi, deverá ser utilizada para fins profissionais, como ferramenta de busca de informações, que contribuam para o desenvolvimento das atividades da Manager Systems, sendo vedado o acesso a sites com conteúdo impróprio ou de relacionamentos.

O uso pessoal é permitido de forma eventual e desde que não comprometa as atividades operacionais, sendo responsabilidade de cada profissional o acesso às páginas e web sites.

Os equipamentos fornecidos para o acesso à internet são de propriedade da empresa, que poderá analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede ou internet, estejam eles em disco local ou na rede.

Assim, a empresa, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos.

6.9 USO DO E-MAIL

O uso do e-mail é disponibilizado para fins corporativos e relacionado às atividades do profissional, devendo sempre ser usada uma linguagem profissional.

É expressamente proibidas as ações abaixo:

a) Enviar mensagens não solicitadas para múltiplos destinatários (ex. correntes), exceto se relacionadas ao uso legítimo da empresa;
b) Enviar qualquer mensagem que torne a empresa vulnerável a ações civis ou criminais;
c) Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal;
d) Apagar mensagens relacionadas às atividades profissionais, quando a empresa ou pessoas a ela relacionadas estiver sujeita a algum tipo de investigação.
e) Produzir, transmitir ou divulgar mensagem que:
    I. Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da empresa;
    II. Contenha ameaças eletrônicas, como: spam, vírus de computador;

III. Contenha arquivos com código executável (.exe, .com, .bat, .pif,.js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
IV. Vise obter acesso não autorizado a outro computador, servidor ou rede;
V. Vise interromper um serviço, servidores ou de rede por meio de qualquer método ilícito ou não autorizado;
VI. Vise assediar outro usuário;
VII. Vise acessar informações confidenciais sem explícita autorização do proprietário ou informações que possam causar prejuízos a qualquer pessoa;
VIII. Inclua imagens criptografadas ou de qualquer forma mascaradas;
IX. Tenha conteúdo considerado impróprio, obsceno ou ilegal;
X. Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
XI. Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
XII. Tenha fins políticos;
XIII. Inclua material protegido por direitos autorais, sem a permissão do detentor dos direitos.

6.10 SOFTWARE DE MENSAGENS INSTANTÂNEAS / REDES SOCIAIS

Os serviços de comunicação instantânea instalados na máquina poderão ser inicialmente disponibilizados aos profissionais que necessitem dessa ferramenta e poderão ser bloqueados, caso o gestor requisite formalmente à área de TI.

O uso de aplicativos de comunicação pelos profissionais, a partir de recursos da Manager Systems, para compartilhar informações profissionais, deverá ser feito de forma responsável para evitar riscos desnecessários, que possam comprometer as atividades, os projetos ou a própria empresa.

Ainda, deve o profissional sempre preservar o sigilo e a confidencialidade das informações, atender aos requisitos de segurança previstos nesta Política e respeitar as leis nacionais.

6.11 SEGURANÇA DOS EQUIPAMENTOS

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento da área de TI ou de quem este determinar.

Os sistemas e computadores tem versões do software e antivírus instalados, ativados e atualizados permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a área de TI, abrindo chamado no sistema de chamados.

Todos os terminais (computadores) devem ser protegidos por senha e bloqueados, quando não estiverem sendo utilizados. Ao final do expediente, o computador deverá ser desligado.

6.12 SEGURANÇA DOS DADOS EM MEIO FÍSICO

Documentos que contenham informações sensíveis, críticas ou classificadas como corporativa, confidencial ou restrita, não devem ficar expostos na estação de trabalho, em impressoras, fax, scanner, telas de computadores, áreas comuns, locais de trânsito de pessoas, refeitório e nas salas de reuniões, devendo ser armazenados em local seguro, de preferência, com acesso restrito.

6.13 USO DOS DISPOSITIVOS MÓVEIS CORPORATIVOS

Todo profissional deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel corporativo. Não é permitida a alteração da configuração dos sistemas operacionais dos equipamentos, em especial, os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um profissional da área de TI. O profissional deverá responsabilizar-se em não utilizar quaisquer programas e/ou aplicativos, inclusive gratuitos, que não tenham sido instalados ou autorizados por um profissional da área de TI.

É responsabilidade do profissional, no caso de furto ou roubo de um dispositivo móvel fornecido pela empresa, notificar imediatamente seu coordenador e a área de TI. Também deverá, assim que possível, registrar um Boletim de Ocorrência na Delegacia de Furtos de Roubos (BO).

O profissional deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à empresa e/ou a terceiros.

6.14 ACESSO REMOTO - VPN

O acesso remoto implica em riscos para a rede corporativa, uma vez que com ele é possível acessá-la a partir de qualquer ponto de internet, por isso não é recomendado acessar a rede via VPN em locais com a internet pública (cafés, aeroporto, lan house, shoppings, etc).

O responsável de TI instala um certificado individual da VPN na máquina do profissional. O acesso a VPN pelo profissional é feita com autenticação de dois fatores. A autenticação em dois fatores é um processo de segurança que aumenta a probabilidade de uma pessoa ser quem ela diz ser, exigindo que o usuário forneça dois fatores de autenticação diferentes para acessar um sistema ou aplicativo. No primeiro acesso é inserido uma segunda senha que somente a TI possui acesso, evitando assim que o profissional possa instalar a VPN em outra máquina, essa senha é inserida pela TI somente no primeiro acesso.

É vedado aos profissionais compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a outro colaborador.

Sempre que o profissional estiver conectado remotamente e precisar se afastar do equipamento deve executar logoff ou bloquear seu equipamento.

6.15 INSTALAÇÕES DE SOFTWARE

Não é permitida a instalação/uso de softwares ilegais (sem licenciamento), sendo que a área de TI poderá valer-se desta Política para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

É proibido executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa.

6.16 COMUNICAÇÃO VERBAL DENTRO E FORA DA EMPRESA

Somente os profissionais que estão devidamente autorizados a falar em nome da Manager Systems, para os meios de comunicação, podem fazê-lo. A fim de evitar exposição desnecessária da Manager Systems, os profissionais não devem tratar de assuntos internos em locais públicos ou dentro das instalações físicas da empresa, quando próximos a visitantes ou terceiros.

6.17 SEGURANÇA DO AMBIENTE FÍSICO

O acesso às dependências da empresa com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, para fins de gravação dos ambientes de trabalho, somente poderá ser realizado a partir de autorização da Diretoria.

Não é permitido aos profissionais tirar fotos, gravar, filmar, publicar e/ou compartilhar imagens dos ambientes internos da Manager Systems que possam:

a) Comprometer a segurança dos demais profissionais;
b) Comprometer o sigilo das informações;
c) Impactar negativamente a imagem da Manager Systems e outros profissionais.

7. PLANO DE CONTINGÊNCIA

A Manager Systems manterá uma Política de Continuidade de Negócios, cuja operacionalização estará descrita no processo MNGS -20 – Gestão da Continuidade.

8. COMUNICAÇÃO DE VIOLAÇÕES

As violações à esta Política estão sujeitas às sanções disciplinares previstas no processo MNGS-61 Política de Medidas Disciplinares da Manager Systems, e na legislação vigente no Brasil. Os casos de violação das normas presentes nesta Política poderão ser comunicados, conforme disposto abaixo:

a) Para o e-mail sgq@mngs.com.br;

b) À área de TI, se no âmbito tecnológico.

Luiz Fernando Dantas
Presidente