1. OBJETIVO

Estabelecer diretrizes para o tratamento e a segurança das informações da Unimed Limeira seguindo os princípios da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais em consonância com a RN 452 e RN 443.
Sob os aspectos de confidencialidade, integridade, disponibilidade e legalidade.

2. DEFINIÇÕES:

Malwares: Temo usuado para descrever programas malicioso que causam danos nos sistemas computacionais.

VPN: Sigla em inglês para "Virtual Private Network" ou Rede Virtual Privada

WIRELESS: Tecnologia de conexão entre dipositivos computacionais por meio de ondas de radio ou infravermelho, sem a necessidade de utilizar cabos de conexão.

Spam: Mensagens enviadas em massa sem uma solicitação previa, a fim de divulgar e distribuir propagandas por e-mail.

Hardwares: É a parte fisica de um dispositivo computacional (componentes eletronicos)

Softwares: É o conjunto dos programas e dos meios não materiais que possibilitam o funcionamento do computador, na execução das diversas tarefas.

Ativos: É o termo utilizado para expressar bens patrimoniais como equipamentos de tecnologia em geral

Acesso Remoto: É a capacidade de acesso a um dispositivo computacional de qualquer outro local remoto.

Usuário: Um usuário ou utilizador é um agente, tanto um agente humano (usuário final) como um agente de software, que usa um computador ou serviço de rede.

3. APLICAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:

A Política de Segurança da Informação se aplica a todos os públicos (colaborador em regime CLT, Diretores Executivos, Conselhos, Cooperados, Prestadores de Serviços Médicos e Rede Prestadora de Serviços) que trabalham com as informações e recursos da Cooperativa.

4. CONTRATAÇÃO, CONSCIENTIZAÇÃO E TREINAMENTO:

Na contratação dos novos funcionários é entregue a **PSI-01 Política de Segurança da Informação** para que todos tenham conhecimento.

Periodicamente podem ser enviadas informações referentes à Segurança da Informação através do Boletim de Segurança da Informação a fim de conscientizar os funcionários, cooperados e rede prestadora.

5. PROTEÇÃO DA INFORMAÇÃO:

Todas as informações pertencentes à Cooperativa, em formato físico ou eletrônico, devem ser protegidas de divulgação, modificação ou roubo através da aplicação de controles pertinentes.

As informações críticas ou sensíveis devem ser mantidas em áreas seguras, protegidas por barreiras de segurança apropriadas e ter acesso controlado, registrado e monitorado.

6. CONTROLE DE ACESSO:

As redes são separadas por áreas, sendo que nestas terão acesso somente os funcionários pertencentes ao referido setor e os perfis não se diferem em privilégio de acesso.

No Sistemas de ERP como Solus, MKSaude e MV os acessos são restritos de acordo com a atividade de cada usuário. Exemplo: Médico, Secretária, Enfermeiros, Usuário Setor Financeiro e Usuário Setor Comercial.

Para os funcionários, todos os acessos às informações (rede, pastas, sistema) assim como acesso a internet e e-mails devem ser autorizados previamente pelo Gestor do solicitante. As solicitações de acesso são realizadas através de chamado para o setor de Tecnologia da Informação, anexando no mesmo o e-mail de autorização do Gestor.

7. RECURSOS

Os recursos disponibilizados pela Unimed Limeira aos usuários dos sistemas de tecnologia internos (Rede, Internet, Sistemas ERP, E-mail, Equipamentos) devem ser utilizados exclusivamente para uso profissional, ético, seguro e legal. A detecção de uso impróprio, ou seja, utilização dos recursos disponibilizados sem autorização ou para fins não profissionais relacionados à atividade exercida, estando o usuário sujeito a punições estipuladas pela Cooperativa Unimed Limeira.
Os recursos da Cooperativa não devem ser utilizados para recebimento, divulgação, exibição, transmissão ou execução de conteúdo:

a. Ilícitos;
b. Contrário aos bons costumes;
c. Pornográfico, obsceno ou pedófilo;
d. Que gerem calúnia, difamação, ofensas ou ameaças;
e. Práticas de atos discriminatórios (sexo, raça, cor, crenças ou qualquer outro);
f. Propaganda política;

g. Que gerem violação de direitos de propriedade intelectual de terceiros;
h. De caráter ofensivo ao sistema Unimed.
i. Que contenham malwares, spam ou outros elementos físicos e eletrônicos que possam danificar ou impedir o funcionamento dos hardwares e softwares da Unimed Limeira.

A Unimed Limeira exonera-se de qualquer responsabilidade do uso indevido dos recursos disponibilizados, tendo o direito de analisar os dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios e adotar as medidas legais cabíveis. Tornando-se públicos no caso de exigência judicial.

8. MONITORAMENTO DE AMBIENTES FÍSICOS E ELETRÔNICOS

Serão aplicados os controles apropriados em todos os recursos necessários para reduzir o risco aos ativos da Cooperativa Unimed Limeira, com o objetivo de prevenir e detectar ameaças, vulnerabilidade e violações a esta Política de Segurança da Informação e demais procedimentos da Cooperativa.

Para proteção dos ativos internos da Cooperativa, a Unimed Limeira reserva-se no direito de:

a. Monitorar as estações de trabalho, servidores, correio eletrônico (e-mail), acesso à internet e todos os demais recursos disponibilizados;
b. Instalar sistemas de proteção preventivos e de detecção para garantir a segurança das informações;
c. Inspecionar sistemas de proteção preventivos e de detecção para garantir a segurança das informações.
d. Inspecionar todos os arquivos que estejam na rede ou qualquer outro ambiente conectado a ela.
e. Inspecionar equipamentos de sua propriedade ou de terceiros que estejam em suas instalações físicas ou em contato com os seus ambientes eletrônicos, quando necessário;
f. Instalar câmeras de vigilância que julgar necessárias.
g. As ligações gravadas são propriedades da Unimed Limeira, podendo ser disponibilizadas apenas para fins de processos jurídicos, mediante solicitação judicial.

9. PROPRIEDADE INTELECTUAL

Todas as informações produzidas pelos funcionários no exercício de suas atividades são de propriedade da Cooperativa Unimed Limeira e estão protegidas por sigilo profissional.

10. DESCUMPRIMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O descumprimento das regras estabelecidas nesta Política de Segurança da Informação, mesmo que não tenham sido gerados prejuízos para a Unimed Limeira, poderá

acarretar a aplicação de punição. Sendo que em primeira instância será enviado comunicado ao Gestor responsável. E as demais serão analisadas pontualmente.
Para os demais públicos (cooperados e rede prestadora) serão analisados pontualmente pela Diretoria Executiva.

11. INCIDENTES

Todos os colaboradores em regime CLT, Diretores Executivos, Conselhos, Cooperados, Rede Prestadora, devem reportar os incidentes e situações que possam causar prejuízos à Cooperativa por meio do canal: dpo@unimedlimeira.com.br.

12. RESPONSABILIDADES:

Todos os envolvidos nesta Política de Segurança da Informação deverão:

a. Cumprir e zelar pelas regras de Segurança da Informação;
b. Responsabilizar-se por qualquer ato que causarem prejuízos à Cooperativa em decorrência do não cumprimento desta Política;
c. Zelar pela confidencialidade de qualquer login/senha que lhe tenha sido concedido;
d. Utilizar os recursos disponibilizados pela Unimed Limeira para fins exclusivamente do exercício de sua atividade.
e. Buscar orientação com a área de Tecnologia da Informação sempre que estiver inseguro quanto ao manuseio e descarte de informações.
f. Não divulgar informações da Cooperativa em locais públicos e em ambientes virtuais, tais como redes sociais, salas de bate-papo, fóruns de discussão, ente outros.
g. Reportar formalmente todos os incidentes que tenham tomado conhecimento, os quais possam afetar ou afetaram a Confidencialidade, Integridade e Disponibilidade das Informações.

Os gestores devem:

a. Cumprir, fazer cumprir e zelar pelas regras de Segurança da Informação;
b. Ter postura exemplar em relação à Segurança da Informação, servindo como modelo de conduta para os colaboradores sob a sua gestão;
c. Adaptar processos sob sua responsabilidade para atender a esta Política de Segurança da Informação;
d. Informar no ato da demissão do colaborador, à área de Tecnologia da Informação para retirada imediata dos acessos.

O departamento de Recursos Humanos deverá:

a. Fornecer a todos os novos funcionários a Política de Segurança da Informação.
b. Fornecer a todos os novos funcionários o Termo de Sigilo para assinatura.

Os Médicos Cooperados, Prestadores de Serviços Médicos e Rede Prestadora deverão:

a. Informar ao setor de Tecnologia da Informação da Unimed Limeira, sempre que houver a troca do usuário do sistema WebSolus, ou seja, secretárias, recepcionistas e demais usuários.

13. CONTROLE E USO DOS RECURSOS INTERNOS:

A utilização dos ativos desta Cooperativa somente será disponibilizada aos funcionários mediante a aceitação formal pelo funcionário, através da assinatura no Termo de Sigilo e autorização prévia e formal do gestor da área do colaborador, por meio de abertura de chamado no sistema GLPI.

Dentre os principais recursos tecnológicos disponibilizados exclusivamente para fins profissionais estão:

a. Acesso à Internet;
b. Rede Interna;
c. Correio Eletrônico;
d. Sistemas ERP.

13.1. As configurações dos recursos tecnológicos, somente poderão ser alteradas pela Equipe de Tecnologia da Informação.

13.2. Toda manutenção, instalação e desinstalação deverão ser realizadas somente pela Equipe de Tecnologia da Informação ou com o acompanhamento da mesma.

13.3. É proibida a abertura ou manuseio dos recursos tecnológicos para qualquer tipo de reparo que não seja realizado pela Equipe de Tecnologia da Informação.

13.4. Nos períodos em que o colaborador estiver afastado por motivos diversos, como medidas disciplinares, dispensas, férias e etc. automaticamente suas credenciais devem ser suspensas, cabendo ao gestor da área ou o setor de Gestão de Pessoas registrar a solicitação através de chamado no sistema GLPI ou E-mail.

13.5. O funcionário é responsável por tomar as medidas cabíveis de salvaguarda das informações classificadas como confidenciais para o negócio.

13.6. Sempre que necessário a recuperação de cópias de segurança (backup) de tais informações, o colaborador deve buscar o auxílio da Equipe de Tecnologia da Informação.

13.7. É proibida a utilização das unidades de CDs, Pen Drives e outros dispositivos de armazenamento. Caso haja real necessidade de transferência de arquivos externos para internos ou vice-versa, as alternativas serão:

Arquivos até 10MB: pode ser enviado pelo e-mail corporativo (@unimedlimeira.com.br);
Arquivos acima de 10MB: levar o dispositivo de armazenamento para uma das áreas de TI (Sede ou Hospital) onde será escaneado com antivírus e o arquivo em questão será disponibilizado pela TI na área solicitada;
Para transferência de arquivos entre áreas internas: pode ser utilizada a área Transferência (X:).

NOTA 1: São disponibilizados pen drives para uso exclusivo da Diretoria e Centro Cirúrgico.

14. GERENCIAMENTO DE SENHAS DO USUÁRIO PARA USO DA REDE INTERNA:

A senha de acesso inicial ao computador deve ser temporária e gerada com data de expiração, para que o colaborador altere-a logo após o primeiro acesso.

É recomendado que as senhas contenham caracteres conforme as categorias abaixo:
Maiúsculos (A-Z)
Minúsculos (a-z)
Dígitos de base 10 (0 a 9)
A senhas expiram a cada 30 dias e não pode ser reutilização as 20 últimas senhas.

O colaborador será bloqueado após 5 tentativas frustradas de autenticação e será liberado para tentar novamente após 30 minutos ou o colaborador deverá entrar em contato com a Equipe de TI para geração de uma nova senha de acesso inicial.

Caso haja esquecimento da senha, deve-se entrar em contato com a Equipe de TI para criação de uma nova senha inicial que deverá ser alterada posteriormente.
É de responsabilidade de cada usuário, guardar e manter o seu login/senha, sendo PROIBIDO o compartilhamento da mesma.

O usuário que utilizar da autenticação de outra pessoa estará sujeito à medidas disciplinares cabíveis.

O usuário que fornecer sua autenticação a outros estará sujeito à medidas disciplinares cabíveis

Cada usuário é responsável por tomar as medidas de proteção das informações da Cooperativa.

Ao se ausentar do computador/notebook, o mesmo deve ser bloqueado pelo usuário.

15. GERENCIAMENTO DE SENHAS DOS MÉDICOS NO SISTEMA WEBSOLUS:

A senha de acesso ao sistema WebSolus devem conter no mínimo 8 caracteres, sendo 1 letra maiúscula e 1 caractere especial.

16. ACESSO À INTERNET

16.1. LIBERAÇÃO DE ACESSO:

A solicitação de acesso à internet aos funcionários deverá ser realizada com o consentimento formal do gestor do funcionário através de abertura de chamado no sistema GLPI. Para os médicos que atendem no Hospital Unimed Limeira, a solicitação deverá ser realizada pela TI do Hospital Unimed Limeira.

16.2. MONITORAMENTO E CONTROLE DOS ACESSOS INTERNOS:

Todos os conteúdos recebidos ou enviados e sites acessados pelos funcionários são monitorados pelo setor de Tecnologia da Informação, a fim de prevenir e detectar o não cumprimento das regras de Segurança da Informação.
Os softwares para acesso à internet são:

a. Internet Explorer
b. Google Chrome
c. Mozila Firefox

17. CORREIO ELETRÔNICO (E-MAIL) (USO INTERNO)

17.1. LIBERAÇÃO DE ACESSO

A liberação de acesso ao e-mail corporativo será liberada mediante consentimento formal do gestor do funcionário por meio da abertura de chamado no sistema GLPI ou e-mail.

17.2. FORMATO DE ENDEREÇO DE E-MAIL

Os endereços eletrônicos são do seguinte formato:
<nome.sobrenome do funcionário@unimedlimeira.com.br>
Exemplo: maria.santos@unimedlimeira.com.br

Caso exista um endereço de e-mail que já contenha o nome e sobrenome do funcionário, deve ser definido um novo endereço conforme recomendações da equipe de Tecnologia da Informação.

17.3. USO SEGURO DO CORREIO ELETRÔNICO

O Sistema de correio eletrônico (e-mail) é de propriedade da Unimed Limeira, e seu uso é destinado exclusivamente para atender aos interesses relativos a ela, sendo proibido para fins particulares. É recomendável que as mensagens tenham assinatura padrão, conforme abaixo:

Nome Completo do Funcionário (a)

Nome da área

www.unimedlimeira.com.br

(Nome da Rua), (Número)
(CEP), (cidade) - SP
T. (DDD) (Nº do Telefone) Ramal: (Nº do Ramal)

17.4. DEVERES

São deveres dos funcionários:

a. Zelar pela segurança e senha de acesso à sua caixa de correio eletrônico, que é de caráter pessoal e intransferível.
b. Redigir as mensagens de forma clara, objetiva e formal.
c. Excluir imediatamente quaisquer mensagens caracterizadas como spam e notificar a equipe de Tecnologia da Informação em caso de recebimento constante destas mensagens.

17.5. MONITORAMENTO

Todos os conteúdos recebidos ou enviados via correio eletrônico são monitorados para prevenção de violações às regras de Segurança da Informação.

17.6. PROIBIÇÕES

É **proibido**:

a. Enviar e-mail a partir de endereço diferente do seu próprio, ou se fazendo passar por outra pessoa.
b. Acessar a caixa de correio eletrônico de outro funcionário sem a devida permissão.

c. Compartilhar conteúdos que comprometam a confidencialidade de informações relacionadas à Cooperativa Unimed Limeira, bem como enviar arquivos contendo informações sobre os negócios da empresa a pessoas não autorizadas.

d. Divulgar o endereço eletrônico fornecido pela Unimed Limeira, para o recebimento de mensagens pessoais ou de entidades alheias aos interesses às atividades prestadas à essa cooperativa.

e. Enviar mensagens utilizando termos que possam caracterizar intimidade ou que não sejam apropriados em ambiente de trabalho, bem como dar continuidade a e-mail em forma de corrente.

f. Transmitir mensagens cujo anexo seja superior ao limite de 10 megabytes. Caso seja necessário deverá ser feito o compartilhamento através da rede "Transferência" (X:\).

17.7. BLOQUEIO / CANCELAMENTO / DESVIOS

a. Na demissão de um funcionário, antes do mesmo ser comunicado o Gestão de Pessoas deverá solicitar para a TI o bloqueio do acesso ao Computador.

b. Quando houver desligamento de funcionários a conta de correio eletrônico deverá ser excluída. Podem ocorrer situações em que seja necessário transferir as informações do e-mail para um determinado computador onde ficará disponível para consulta e o redirecionamento dos e-mails enviados deste endereço para outro determinado e-mail escolhido pelo superior imediato, dependendo das informações contidas no e-mail, necessárias para o andamento da Cooperativa.
As contas de acesso aos sistemas por ele utilizado nas suas atividades serão bloqueadas/desativadas mantendo os históricos de utilização por ele realizado, mediante o recebimento pela TI do comunicado de desligamento enviado através do Gestão de Pessoas.

c. Quando o funcionário se ausentar (férias, licença, entre outros) as mensagens podem ser redirecionadas a outro funcionário.

18. USO DE CONEXÃO REMOTA (USO INTERNO)

O acesso via conexão remota será permitido mediante a solicitação realizada pelo diretor/gerente da área, em casos de necessidade para execução das atividades do setor.

A conexão remota para execução de trabalho de suporte técnico de TI e para auditorias médicas serão permitidas, mediante ao uso de antivírus confiável no computador de origem, após analisado e comprovado pelo Departamento de TI.

O acesso remoto se faz através de uma conexão de área de trabalho remoto através de dois links de endereços distintos até o servidor de Terminal Service e é necessário o login de rede do usuário ter autorização a conectar a esse servidor.

A conexão utiliza o protocolo TLS 1.0 (Transport Layer Security). O TLS 1.0 verifica a identidade do servidor Host de Sessão de Área de Trabalho Remota e criptografa toda a comunicação entre o servidor Host de Sessão de Área de Trabalho Remota e o computador cliente

Quando houver a necessidade de acesso remoto pelos prestadores ou médicos cooperados deverão solicitar ao setor de Tecnologia da Informação, que irá solicitar autorização da Diretoria.

19. ACESSO À REDE WIRELESS (VISITANTES E FORNECEDORES)

A Unimed Limeira disponibilizará acessos à internet por meio de sua rede wireless, gratuitamente, a pedido do visitante, com a autorização da área que está recebendo a visita, sendo que é expressamente proibido que o visitante compartilhe informações da Cooperativa.

20. IMPRESSÃO (USO INTERNO)

a. A configuração e manutenção das impressoras só podem ser realizadas pela equipe de TI ou terceiros autorizados quando necessário.
b. É de responsabilidade de cada departamento o controle e estoque de toner e cartuchos de tintas por meio da empresa parceira contratada para essa finalidade.
c. É configurado uma senha de liberação as impressões para cada usuário conforme disponibilidade do serviço para cada impressora. A Senha é formada por 4 dígitos numéricos escolhida pelo usuário e configurada pela equipe de TI. A essa senha é intrasferível e de responsabilidade de cada usuário.

É proibida:

a. Utilização da impressora para fins pessoais.
b. Reaproveitar folhas impressas com informações confidenciais, devendo as mesmas serem descartadas.
c. Não recolher material impresso, expondo seu conteúdo e comprometendo o sigilo das informações.

21. USO DO COMUNICADOR INSTANTÂNEO

a. O software de comunicação instantânea utilizado por todos usuários da rede Unimed Limeira é o Spark. Áreas/Funcionários previamente autorizados poderão utilizar também, quando necessário, o Skype, Teams e Zoom para chats e videoconferências.

b. O uso do comunicador instantâneo é destinado exclusivamente para atender os interesses da cooperativa.
c. Toda a comunicação efetuada por meio do comunicador instantâneo (Spark) é monitorada para prevenir e detectar violações as normas de procedimentos em vigor, sendo disponível, para que seu superior imediato, o pedido a qualquer momento dessa comunicação.

É proibido:

a. Acessar o comunicador instantâneo através da conta de outro colaborador, bem como informar a senha de acesso para outros colaboradores.
b. Transmitir conteúdo que represente uma quebra de confidencialidade de informações relacionado a cooperativa ou terceiros que mantenham relação com ela.
c. Enviar mensagens usando termos que possam caracterizar intimidade ou que não sejam apropriados em ambiente de trabalho.
d. Por se tratar de uma ferramenta disponível para uso profissional fica proibido aos colaboradores o uso do comunicador instantâneo para fins particulares.

22. USO DO APLICATIVO WHATSAPP WEB (USO INTERNO)

a. O Aplicativo Whatsapp Web deve ser de uso exclusivo sobre assuntos pertinentes aos processos de trabalho.
b. É proibida a sua utilização para fins pessoais.
c. O compartilhamento de arquivos **deve ser restrito** ao que é necessário para realização dos processos.
d. O uso indevido desta ferramenta é passível de aplicação de penalidade ao colaborador nos termos da Lei.

É proibido:

e. Acessar o whatsapp web através da conta de outro colaborador.
f. Transmitir conteúdo que represente uma quebra de confidencialidade de informações relacionado a cooperativa ou terceiros que mantenham relação com ela.
g. Enviar mensagens usando termos que possam caracterizar intimidade ou que não sejam apropriados em ambiente de trabalho.
h. Por se tratar de uma ferramenta disponível para uso profissional fica proibido aos colaboradores o uso do whatsapp web para fins particulares.

23. CIÊNCIA DA POLITICA DE SEGURANÇA DA INFORMAÇÃO

A ciência do colaborador com as disposições contidas nesta Politica de Segurança da Informação é requisito essencial para seu acesso às informações e aos recursos disponibilizados pela Unimed Limeira Cooperativa de Trabalho Médicos.

O colaborador manifesta sua ciência com as disposições contidas nesta Política de Segurança da Informação e compromete-se ao cumprimento de todas suas disposições por meio da assinatura no Termo de Sigilo Profissional.

A Política de Segurança da Informação encontra-se disponível no site da Unimed Limeira: unimedlimeira.com.br.