Sumário

1. OBJETIVO

A política de Segurança da Informação da Fesp tem como objetivo estabelecer os princípios, diretrizes e responsabilidades em relação aos ativos da informação e informações clínicas, visando proteger suas propriedades de confidencialidade, disponibilidade e integridade.

2. ÂMBITO DE APLICAÇÃO

Todas as pessoas físicas e jurídicas, inclusive administradores (sejam sócios, diretores, estatuários ou não, membros do Conselho de Administração e demais gestores), colaborador s, colaboradores, prestadores de serviços, parceiros e/ou quaisquer outros terceiros que mantenham um relacionamento com a UNIMED FESP e que, no âmbito dessa relação, possam vir a ter acesso às áreas, equipamentos, informações, arquivos, redes e dados de titularidade do Sistema e de seus beneficiários, cujo acesso seja controlado.

3. DEFINIÇÕES

Acordo de Confidencialidade: É o documento formal, juridicamente respaldado, contendo a descrição de uso permitido da informação, tempo de duração, responsabilidades, utilização da informação e consequências por violação do acordo.

Ambientes Internos: áreas comuns, áreas internas que envolvem departamentos, datacenter, salas de reunião, auditório, dentre outros ambientes que explicitam informações e pessoas atuantes na UNIMED FESP.

Aplicativos de Mensagens: WhatsApp, Telegram, face time, Skype, Facebook, messenger, Instagram, Twitter e outros que tenham finalidade igual ou similar.

Ativos de Tecnologia de Informação: equipamentos fixos (computador, impressoras etc.), equipamentos móveis (smartphone, notebooks, tablets etc.), demais equipamentos de propriedade da UNIMED FESP, e-mails e os softwares utilizados dentro de seu ambiente. Denominados nesta política somente como ativos de TI.

Gestor: Supervisor, Coordenador, Gerente ou Diretor.

Incidente de Segurança: É toda a ação que viole as políticas internas, tais como: quaisquer ações ou situações que possam expor a UNIMED FESP a perdas financeiras ou de imagem, direta ou indiretamente, potenciais ou reais, uso indevido de dados corporativos ou institucionais, divulgação não autorizada de informações ou de segredos comerciais e

industriais sem a autorização expressa dos proprietários ou área competente, uso de dados, informações, equipamentos, softwares, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, a não comunicação imediata de quaisquer violações ou atitudes anormais de que porventura um usuário da informação venha a tomar conhecimento ou presencie ou ainda, a não aderência às políticas de Segurança da Informação.

Malwares: Programas indesejados, instalado sem o devido consentimento.

Risco de Segurança da Informação: Ameaças possam explorar vulnerabilidades em um ou mais ativos de informação e causar dano a organização (ISO 27005:2011).

Segurança da Informação: Conjunto de conceitos, técnicas e estratégias, as quais visam proteger os ativos de informação da UNIMED FESP a fim de preservá-las de ações não autorizadas relativas à manipulação, transferência ou destruição.

Spam: Qualquer tipo de comunicação online não desejada. A forma mais comum de spam é o e-mail não desejado.

Spywares: Programas que espionam os hábitos de navegação dos usuários, a fim de instanciar janelas (do tipo pop-up) que exibem conteúdos de interesse dos usuários.

Vírus: Pequenos programas desenvolvidos para se espalhar de computador a outro, e interferir no funcionamento do computador.

Worms: Programas similares ao vírus, com a capacidade de fazer cópias deles mesmos, sem a necessidade de outros programas para se multiplicarem.

4. DIRETRIZES

A formulação desta Política deu-se com base na missão, nos princípios e valores da UNIMED FESP e em conformidade com as legislações vigentes e melhores práticas com relação a segurança da informação.

Para garantir o objetivo referente a segurança da informação, 3 (três) pilares devem ser estabelecidos em linha com o praticado pelo mercado:

a) Confidencialidade: Garantia de que a informação estará disponível ou será divulgada somente para indivíduos, entidades, pessoas ou processos devidamente autorizados.
b) Integridade: Garantia de que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não;
c) Disponibilidade: Garantia de que a informação estará disponível sempre que for necessário.

4.1. Regras Gerais

I. Todas as informações geradas ou desenvolvidas para o negócio ou atividades operacionais e de apoio são consideradas ativos de informação da UNIMED FESP;
II. Os colaboradores desde a geração, manutenção, distribuição até o descarte serão responsáveis pela confidencialidade, integridade e disponibilidade da informação;
III. Todo o material desenvolvido utilizando recursos, tanto físicos como lógicos, da Unimed Fesp e atendendo as demandas de negócio serão de sua propriedade;
IV. Os ativos de informação podem estar presentes em diversas formas, tais como: arquivos digitais, equipamentos, mídias externas, documentos impressos, sistemas, dispositivos móveis, bancos de dados e conversas;
V. A responsabilidade do colaborador pelas suas ações ou incidentes de segurança estará refletida no contrato de trabalho ou no contrato de prestação de serviços, quando for o caso;
VI. Os recursos tecnológicos serão homologados e controlados pelas áreas de Tecnologia da Informação e Segurança da Informação não sendo permitidos recursos que não tenham sido formalmente homologados por essas áreas. Maiores informações estão disponíveis na política PL 1044-01 Política de Utilização de Recursos de TI;

VII. Os usuários dos recursos tecnológicos da UNIMED FESP serão responsáveis pela proteção física e lógica contra danos e prejuízos materiais, morais e intelectuais, assim como pela manutenção do sigilo profissional e confidencialidade das informações de seu conhecimento em função do cumprimento de suas atividades na empresa;

VIII. Independentemente da forma apresentada, compartilhada ou armazenada, a informação deve ser utilizada apenas para a sua finalidade devidamente autorizada, sendo sujeita a monitoração e auditoria;

IX. Deve ser assegurado que todo o ativo de informação de propriedade da UNIMED FESP tenha um responsável, seja devidamente classificado e adequadamente protegido de quaisquer riscos e ameaças que possam comprometer o negócio;

X. Nenhuma informação confidencial, ou ainda, sem autorizada pela área de Marketing/Comunicação e GRC sobre o sistema UNIMED FESP deve ser divulgada em sites da Internet, salas de bate-papo, correio eletrônico ou qualquer outro meio eletrônico de troca de informações;

XI. Divulgar informações confidenciais é passível de ações de natureza jurídica ao colaborador que desrespeitar esta Política;

XII. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

XIII. Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

XIV. O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pela Governança de TI;

XV. Todas as gravações das reuniões virtuais devem ser acompanhadas de um aviso aos participantes. O alerta também é vinculado ao aviso de privacidade dos participantes online, e o organizador da reunião controla quais deles têm a capacidade de gravar. No entanto, está proibida a gravação de reuniões de trabalho. As mesmas somente serão permitidas sob demanda da Diretoria Executiva e/ou da

Presidência da UNIMED FESP, sendo ainda necessário o conhecimento da estrutura de GRC;

XVI. O acesso às dependências da UNIMED FESP 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 Área de Marketing, Eventos e/ou GRC e mediante supervisão;

XVII. Não é permitido aos colaboradores, parceiros, clientes, fornecedores, associadas e terceiros em geral, tirar fotos, gravar, filmar, publicar elou compartilhar imagens dos ambientes internos da UNIMED FESP que possam:

a) Comprometer a segurança dos demais colaboradores e Diretoria Executiva;
b) Comprometer o sigilo das informações;
c) Impactar negativamente a imagem da Unimed FESP, outros colaboradores, clientes, parceiros e/ou visitantes.

4.2. Classificação da Informação

A informação é um importante ativo para a operação das atividades institucionais da UNIMED FESP, para manter a confiabilidade e demonstrar a veracidade das informações as suas associadas. Tal como os ativos da UNIMED FESP, a informação deve ser adequadamente manuseada e protegida.

Toda e qualquer informação, incluindo o proprietário da informação deve ser classificada num nível de restrição de acesso (grau ou nível de confidencialidade) os ativos (informações e recursos de informação), conforme a importância para os negócios da UNIMED FESP e conforme os padrões de classificação de ativos da informação descritos a seguir.

CLASSIFICAÇÃO	CRITÉRIO(S)	PÚBLICO	EXEMPLO(S)
CONFIDENCIAL	Informações de caráter estratégico de negócios. A informação confidencial é restringida dentro da organização e protegida de acesso externo. Qualquer perda de confidencialidade causará eventual comprometimento das operações, resultando em perdas financeiras, de competitividade, de imagem, risco de ações judiciais à UNIMED FESP e a seus executivos.	Pessoas elegíveis pelo Presidente e Diretores da UNIMED FESP, como também, do Conselho Diretor.	Reuniões do Conselho Diretor.
RESTRITA	Informações de caráter restrito e circulação controlada. Este tipo de informação é de uso restrito a um grupo de pessoas, departamentos específicos, equipes de um projeto etc., divulgada de forma seletiva e mediante o conhecimento e a autorização expressa do proprietário da informação (ex.: informações de projetos, processos etc.).	Somente pessoas elegíveis para tomar conhecimento e uso destas informações.	Fórmulas e ativos protegidos por direito autoral; Assuntos de Comitês e Grupos de trabalho; Notas fiscais; Informações pessoais de colaborador s e integrantes.
INTERNA	Informações de conhecimento e circulação interna. A informação de uso interno é tratada como importante e mantida dentro do domínio UNIMED FESP, divulgada de forma seletiva e mediante o conhecimento e a	Integrantes e parceiros de negócios para conhecimento e uso destas informações.	Comunicações internas; Procedimentos internos.

	autorização expressa do proprietário da informação (ex.: informações publicadas na intranet da UNIMED FESP).		
PÚBLICA	Informações de circulação geral, de conhecimento público. Toda informação que não necessite de sigilo terá livre acesso e não causará qualquer prejuízo para os negócios caso seja divulgada fora da UNIMED FESP (ex.: informações publicadas no site da UNIMED FESP, na Internet).	Público geral	Notícias Press releases Campanhas sociais

4.3. Acordos de Confidencialidade

A disponibilização de informações confidenciais, seja para execução de projetos ou para elaboração de propostas de consultorias, auditorias e/ou fornecedores, deverá ser precedida da assinatura de um Acordo de Confidencialidade que, em sua contratação o colaborador já a realiza. No caso de identificar a não assinatura deste, o termo deve ser aplicado sob responsabilidade da Gerência e/ou Diretoria solicitante das informações, mediante suporte do departamento Jurídico.

Todos os contratos com prestadores de serviços ou demais entidades que irão se relacionar com a UNIMED FESP e que venham a acessar informações privilegiadas deverão conter, obrigatoriamente, a cláusula de confidencialidade, responsabilidade e consequências, caso as exigências previstas não sejam adequadamente cumpridas.

4.4. Encerramento ou mudança da contratação

Caberá ao Gestor da área responsável pela contratação do terceiro ou prestador de serviços, solicitar o cancelamento dos acessos aos recursos tecnológicos ao término de cada contrato. Será necessária também a solicitação de exclusão do usuário nos sistemas da empresa.

Caberá ao Gestor responsável pelo colaborador ou pelo terceiro garantir a devolução dos recursos de computação móvel da UNIMED FESP (notebooks, telefones celulares, tablets, smartphones e similares) pelo usuário, no encerramento das atividades, contrato ou acordo, assim como a notificação de alteração de atividades e/ou unidade/departamento/setor.

4.5. Gestão de Incidentes de Segurança da Informação

O usuário da informação deverá comunicar imediatamente o seu gestor e a área de Segurança da Informação qualquer incidente que possa trazer impactos na segurança dos ativos organizacionais (informação ou recursos de processamento).
A comunicação com a área de Segurança de Informação deverá ser feita por e-mail para o endereço eletrônico segurança.fesp@unimedfesp.coop.br.

4.5.1. Infrações e Tentativas de Burla

Os usuários da informação não deverão testar fragilidades de segurança, pois tais eventos serão interpretados como uso impróprio do sistema/exploração de vulnerabilidades.

4.6. Controle de Acesso Físico

I. O acesso ao ambiente de Tecnologia – Data Center deve ser controlado pela área e registrado em caso de anormalidade, assim como o controle de acesso à área de Produção deve ser acompanhado de registro.
II. O acesso às dependências dos Data Centers com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da equipe de Governança de TI e mediante supervisão;
III. O acesso às instalações internas será permitido somente a colaborador e temporários contratados, prestadores de serviços ou visitantes autorizados mediante alinhamento com Serviços Administrativos e Gestão de Pessoas.
IV. Para o acesso fora do expediente normal da empresa será necessária autorização da gerência responsável.
V. Dentro das dependências da empresa, cada pessoa, independentemente de seu cargo ou função, deverá usar um crachá de identificação de forma visível.
VI. Em nenhuma circunstância, uma pessoa poderá adentrar ou permanecer, sozinha, nas dependências da empresa em horário distinto daquele contratualmente

acordado, mesmo que seja para trabalho urgente e inadiável, independentemente de seu cargo ou função. Exceções a essa regra deverão ser aprovadas, caso a caso, por um Diretor e sob a ciência de Governança.

VII. Todas as áreas de trabalho devem permanecer limpas e arrumadas, evitando o acúmulo de material combustível.

VIII. Todo colaborador, independentemente de seu cargo ou função, deverá zelar para que qualquer material, contendo informações sobre clientes ou que seja de natureza sensível, como políticas e procedimentos internos, planos estratégicos e de marketing, informações pessoais, propostas comerciais, descrições de sistemas, produtos ou programas automatizados, entre outros, que esteja sob sua guarda, seja mantido inacessível a pessoas não autorizadas, principalmente durante sua ausência do posto de trabalho.

IX. Ao final do expediente, todos os documentos deverão ser trancados e retirados das mesas.

Maiores informações estão estabelecidas em Normativas internas específicas para cada assunto.

4.7. Cópias de Segurança

Cópias de segurança dos dados e de software essenciais ao negócio devem ser feitas regularmente.

Os recursos e instalações alternativos devem ser disponibilizados de forma a garantir que todos os dados e sistemas aplicativos essenciais ao negócio possam ser recuperados após um desastre ou problemas em mídias.

Os backups de sistemas individuais devem ser testados regularmente, de maneira a garantir que satisfaçam os requisitos dos planos de continuidade de negócios. Abaixo controles que devem ser considerados:

- Deve ser mantido um nível mínimo de cópias de segurança, juntamente com o controle consistente e atualizado dessas cópias e com a documentação dos procedimentos de recuperação em local remoto a uma distância suficiente para livrá-los de qualquer dano que possa ocorrer na instalação principal. Convém também que no mínimo três gerações ou ciclos de cópias de segurança das aplicações críticas sejam mantidos;

- Deve ser dado às cópias de segurança um nível adequado de proteção física e ambiental, compatível com os padrões utilizados no ambiente principal. Todos os controles adotados para as mídias no ambiente principal devem ser estendidos para o ambiente de backup;
- As mídias utilizadas para cópias devem ser periodicamente testadas, de modo a garantir sua confiabilidade;
- Os procedimentos de recuperação devem ser verificados e testados periodicamente para assegurar que sejam efetivos e que possam ser aplicados dentro dos prazos estabelecidos para os procedimentos operacionais de recuperação.

4.8. Senhas

A senha é instrumento de trabalho, por isso, todo usuário deve fazer uso correto desta.

Cada usuário deve ser responsável por manter sua senha confidencial, pois se utilizada por terceiros, todas as operações efetuadas com a senha concedida, serão de exclusiva responsabilidade do usuário.

A senha inicial fornecida pelo setor de TI-Service Desk deve ser imediatamente alterada para uma de conhecimento apenas do usuário responsável pela custódia dela.

Quando o usuário estiver em período de férias, o gestor da área deve informar a área de Segurança da Informação para que retirem os acessos no período que o usuário estiver fora da empresa indicando um substituto para exercer a função do colaborador de férias, no entanto, será criado um novo usuário, e em caso de correio eletrônico redirecionem seus e-mails em período de férias para outro usuário que o esteja substituindo, se necessário.

Alterações de senha devido a bloqueio após 3 tentativas ou casos onde o colaborador tenha esquecido a mesma, devem ser solicitadas pelo superior imediato do usuário, nenhuma solicitação de alteração será aceita se realizada pelo próprio usuário do Sistema e/ou Rede.

4.9. Internet

Os serviços da Internet serão cedidos a todos os colaboradores que tiverem necessidade de utilizá-los em seu trabalho, desde que seja autorizado pelo gestor da área solicitante, que deverá acompanhar o bom uso deste serviço.

Acessos inapropriados, sites não relacionados com os negócios do sistema UNIMED FESP são proibidos para os horários comerciais. Os membros da empresa devem ter bom senso ao selecionar um site para visitar.

Fica terminantemente proibido o acesso a sites de pornografia, pedofilia, racismo, violência etc., sendo considerada falta grave, e se comprovado serão tomadas às medidas previstas em Lei.

Os recursos do sistema UNIMED FESP não devem ser usados para transmitir ou receber informação classificada como "Confidencial", "Restrita" ou "Interna", pois a Internet não é um ambiente seguro, podendo a mensagem ser interceptada e aberta por qualquer pessoa.

As seguintes regras abaixo devem ser respeitadas por todos da UNIMED FESP:

- É proibido utilizar recursos do sistema UNIMED FESP para fazer downloads (mp3, vídeos, programas diversos, conteúdo não autorizado etc.), distribuição de software, ou, dados não legalizados, bem como distribuição destes;
- É proibido a divulgação de informações confidenciais do sistema UNIMED FESP em grupos de discussão, listas ou bate-papo;
- Pode ser utilizada a internet para atividades não profissionais fora do expediente, desde que dentro das regras de uso definidas nesta política;
- Os integrantes com acesso à internet podem fazer o download de programas ligados diretamente às atividades do sistema UNIMED FESP, e devem solicitar ao departamento de Tecnologia da Informação, por intermédio de chamado aberto na ferramenta oficial do sistema UNIMED FESP, a instalação e a regularização de licenças, se aplicável, desses programas;
- Colaboradores com acesso à Internet não podem efetuar upload de quaisquer dados e/ou softwares de propriedade, e licenciados à UNIMED FESP, sem expressa autorização da Administração;
- Caso o departamento de Tecnologia da Informação julgue necessário, haverá bloqueios de acesso a arquivos, domínios e serviços de Internet que comprometam o uso de banda, da segurança da rede corporativa, ou, o bom andamento dos trabalhos;
- É proibida a utilização de softwares de P2P (peer-to-peer) como Kazaa, Morpheus, eMule, µTorrent e afins;

- É proibida a utilização de serviços de streaming, tais como rádios on-line e afins, a não ser que o acesso seja inerente a trabalhos, pesquisas ou negócios do sistema UNIMED FESP;
- É proibido o uso de IM (Instant Messenger) não homologados/autorizados pelo sistema UNIMED FESP.

<u>É extremamente proibido:</u>

- O uso da Internet para ganhos pessoais ou lucros, enquanto estiverem sendo utilizados os recursos do sistema UNIMED FESP;
- A utilização de qualquer sistema de bate-papo e demais sistemas e aplicativos não permitidos pelo sistema UNIMED FESP;
- O uso de qualquer software de troca de arquivos na Internet;
- Qualquer transferência de arquivos que violem as Leis de Direitos Autorais;
- O sistema UNIMED FESP não assumirá nenhuma responsabilidade sobre as transações pessoais em sites de comércio eletrônico, Internet Banking, entre outros sites de transações.

4.10. Correio Eletrônico

I. As mensagens de correio eletrônico são instrumentos de comunicação interna e externa para realização do negócio do sistema UNIMED FESP. Estas mensagens devem ser escritas em linguagem profissional e não devem comprometer a imagem da empresa e/ou de outras entidades;

II. Os recursos eletrônicos, incluindo e-mail, são de propriedade do sistema UNIMED FESP, que se reserva no direito de monitorar, ler, inspecionar e arquivar qualquer informação transmitida ou armazenada em qualquer sistema eletrônico;

III. O e-mail é um serviço e um recurso provido pelo sistema UNIMED FESP aos seus colaboradores para fins de negócio. Qualquer uso pessoal deve ser ocasional e não deve interferir nas atividades do sistema UNIMED FESP;

IV. O acesso ao correio eletrônico com equipamento que não seja de propriedade do sistema UNIMED FESP deve ter aprovação da Diretoria responsável e da área de Tecnologia da Informação, quando solicitado acesso a rede de dados interna;

V. O acesso a e-mails particulares por meio dos equipamentos de propriedade do sistema UNIMED FESP e a utilização deles para tratamento de assuntos

corporativos é autorizado desde que utilizado de forma consciente e não concorram com as atividades dentro do período contratual do colaborador, terceiro ou prestador de serviço contratado;

VI. As mensagens de correio eletrônico devem permitir a correta identificação do(s) seu(s) emissor(es) e receptor(es);

VII. Os e-mails devem ser padronizados, deve existir um único e-mail e login para todos os sistemas operacionais;

VIII. A monitoração de e-mails deve ser realizada sempre que solicitado pelo Gestor de alguma área ou sempre que a estrutura de Governança Corporativa ou a Auditoria acharem necessário;

IX. As mensagens deverão ser armazenadas em pasta particular;

X. Cada usuário deve eliminar quaisquer mensagens desnecessárias da sua caixa de correio eletrônico, visando disponibilizar espaço para recebimento de novas mensagens;

XI. A área de Infraestrutura de Tecnologia é responsável pela padronização de assinatura nos e-mails e deve verificar os sistemas que não estão de acordo com o definido;

XII. Não é permitido acrescentar quaisquer outras informações além das acima citadas;

XIII. É vetado também o emprego de figuras, desenhos, frases de efeito, citações e mensagens;

XIV. O sistema UNIMED FESP não será responsável pelas mensagens alteradas ou falsificadas.

4.10.1 Anexos Não Permitidos

Os anexos inseridos em mensagens eletrônicas, somente devem ser enviados quando for imprescindível. Alguns cuidados devem ser tomados ao repassar uma mensagem recebida (Encaminhar) para evitar repassar desnecessariamente arquivos anexados.

Arquivos anexados em e-mails que representem riscos de segurança ou que não sejam de interesse do sistema UNIMED FESP serão bloqueados para envio e recebimento, e nenhum tipo de aviso será enviado.

Não se devem abrir arquivos anexados de remetentes desconhecidos. Remova esses arquivos do seu ambiente de correio eletrônico ou envie para área de Tecnologia da Informação verificar, caso seja pertinente.

4.10.2 Lista de Distribuição

Para toda mensagem que for enviada para alguma lista de distribuição deve ser observado se todas as pessoas dessa lista possuem interesse ou necessidade de receber tais informações.

Caso seja necessário criar listas que sejam utilizadas por diversos usuários (por exemplo: “Diretoria”), deve ser solicitado junto a área de Tecnologia da Informação do sistema UNIMED FESP com o nome da lista, pessoas que farão parte dessa lista e quem será o responsável pela manutenção desta lista.

5. AUDITORIA E MONITORAMENTO

Os recursos disponibilizados pelo sistema UNIMED FESP são para uso dos colaboradores no desempenho das atividades profissionais.

Todas as informações produzidas, acessadas, armazenadas ou distribuídas pelos recursos disponibilizados pela UNIMED FESP poderão ser monitoradas e controladas.

O acesso e uso das informações corporativas e pessoais para o desempenho de atividades de monitoramento e auditoria na UNIMED FESP são restritas às áreas de Tecnologia da Informação e Segurança da Informação.

O processo de monitoramento e auditoria é autorizado exclusivamente para atender o objetivo de averiguar o cumprimento das diretrizes corporativas, identificar conteúdo e/ou acessos indevidos, detectar fraudes ou coletar evidências para suportar a companhia em processos judiciais ou em atendimento às auditorias internas e externas, órgãos reguladores e fiscalizadores.

Os acessos às informações com finalidade diversa das acima citadas serão interpretados como uso impróprio.

Em caso de ocorrência de incidente de segurança ou fraude as áreas competentes deverão ser imediatamente notificadas pelo gestor responsável para, em conjunto com a área jurídica estabelecer critérios de guarda de provas eletrônicas.

A UNIMED FESP reserva o direito de registrar e examinar todos os eventos relacionados ao acesso à Internet, a fim de garantir que os recursos não estejam sendo utilizados de forma indevida, ou, para fins não autorizados. Relatórios regulares são emitidos, constando os comportamentos de acesso que podem vir a interferir no tráfego de dados, e tentativas de acessos a sites de conteúdos considerados impróprios para o ambiente corporativo. A navegação e o conteúdo exibido nos recursos computacionais da Organização são controlados e armazenados para auditoria, sendo possível, gerar relatórios de acesso por usuário.

6. PAPÉIS E RESPONSABILIDADES

A. Conselho de Administração e Diretoria Executiva

- Fazer cumprir as regras constantes nesta política.

B. Gestores/Líderes de Áreas

- Assegurar que os colaboradores estejam conscientes da importância da prática da boa segurança nas atividades diárias, e solicitar/providenciar educação e treinamento adequados e apropriados às suas responsabilidades, incluindo aspectos relevantes da legislação, regulamentos, direitos autorais e contratos;
- Segregar as funções de aprovação de operações, execução e controle das mesmas, de modo que nenhuma pessoa possa ter completa autoridade sobre uma parcela significativa de qualquer processo;
- Assegurar que as permissões de acesso aos sistemas dos seus colaboradores estejam sempre atualizadas, contendo as devidas solicitações e aprovações de acesso, revendo-as também em caso de transferências e/ou desligamentos;
- Acompanhar o cumprimento dessa política e assegurar que os riscos de Segurança em suas áreas de atuação estejam avaliados e controlados adequadamente;
- Orientar suas equipes sobre o uso adequado das informações e recursos de informações disponibilizados pela empresa;

- Sempre que necessário, devem documentar orientações específicas, regulamentando os níveis de confidencialidade das informações que geram e processam, bem como os direitos de acesso a essas informações;
- Comunicar à área de Governança Corporativa - Compliance os casos de descumprimento de Políticas, Normas ou Procedimentos internos, e os casos de falhas na execução de atividades operacionais;
- Prover informações necessárias para a identificação e tratamento de riscos e incidentes de Segurança da Informação.

C. Área Tecnologia da Informação

- Adequar e configurar equipamentos e aplicativos para correta utilização dos recursos de Tecnologia da Informação, atentando inclusive para que os requisitos de segurança para os negócios da UNIMED FESP sejam identificados e que os controles de segurança estejam adequadamente implementados, operados e mantidos de acordo com esses padrões;
- Viabilizar condições tecnológicas para monitoração da utilização dos recursos de Tecnologia da Informação disponíveis aos usuários, informando a ocorrência de incidentes de segurança e a percepção de violações desta política, visando a aplicação das penalidades e/ou providências cabíveis.

D. Área Segurança da Informação

- Desenvolver e manter atualizada a política de Segurança da Informação;
- Monitorar o seu cumprimento, de forma proativa e sob demanda, sempre que solicitado por alguma área de negócio da UNIMED FESP;
- Definir e executar e/ou coordenar o programa de conscientização de usuários em Segurança da Informação;
- Identificar, planejar e coordenar programas para melhoria da segurança das informações, implementando e aprimorando os controles em todos os recursos tecnológicos e em projetos e processos de negócio;
- Prover consultoria e suporte às áreas de Gerência, sob quaisquer requerimentos de segurança para as áreas de negócios, análises técnicas e seleção de controles apropriados, e verificar/auditar a implementação, manutenção e operação destes controles;

- Homologar em conjunto com as demais áreas de tecnologia todos os recursos de Tecnologia da Informação, com foco em segurança, atentando sempre para Disponibilidade, Integridade e Confidencialidade das Informações;
- Revisar os impactos na segurança do ambiente tecnológico quando da alteração dos atuais recursos, inclusão de novos recursos, ou devido à aquisição de serviços e ativos da informação, emitindo parecer sobre as necessidades de adequação dos mesmos antes de iniciarem suas operações;
- Comunicar às áreas responsáveis a identificação de ocorrências de incidentes de segurança, para que medidas disciplinares cabíveis sejam adotadas;
- Manter registros e documentação de segurança em nível corporativo, incluindo um banco de dados de riscos e assuntos de segurança;
- Avaliar o risco de assuntos relacionados à segurança e comunicar os eventuais problemas às áreas competentes, provendo suporte nas eventuais ações preventivas e/ou corretivas;
- Registrar formalmente todos os incidentes de segurança da informação identificados e/ou reportados;
- Detectar, identificar e registrar violações, ou, tentativas de acessos relevantes e significativas não autorizadas, para tomada de providências corretivas, legal e de auditoria;
- Monitorar os acessos visando verificar: vazamento de informações; acessos ou tentativas de acessos a sites com conteúdo inadequado, repasse de conteúdo inadequado, tentativa de quebra de controles de segurança da informação e armazenamento de arquivos multimídia que não façam parte do negócio da UNIMED FESP;
- Revisar anualmente as regras de proteção estabelecidas;
- Restringir e controlar os acessos e os privilégios de usuários, incluindo os daqueles com privilégios de acesso remoto e externo;
- Em qualquer tempo ou momento, solicitar a restrição, bloqueio, suspensão e/ou cancelamento de acessos e/ou tecnologias (hardware e/ou software) que estejam infringindo as políticas de segurança ou nos casos em que sejam verificados incidentes de segurança, ou em que haja identificação de vulnerabilidades que necessitem de tempo para serem analisadas e se possível, corrigidas.

E. Área Gestão de Pessoas

- Obter a ciência do colaborador no termo de compromisso e responsabilidade sobre a política de Segurança da Informação no ato da admissão, e mantê-lo arquivado no prontuário dele;
- Orientar a Gerência das áreas na aplicação das medidas disciplinares quando cabíveis;
- Desenvolver e implementar, em conjunto com a área de Segurança da Informação, programas de capacitação e conscientização dos usuários sobre o uso adequado dos recursos disponibilizados pela empresa e sobre Segurança da Informação;
- Comprometer-se com o suporte estratégico no desenvolvimento de ações de divulgação desta política;
- Divulgar no processo de integração (treinamento) para todos os usuários (colaborador s, prestadores de serviços e terceiros) que tiverem acesso aos ativos da informação, as principais diretrizes definidas por esta política.

F. Usuários dos recursos de TI

Entende-se por usuário todos que obtiverem acesso aos recursos e ativos de informação da UNIMED FESP.

- Manter-se atualizado com relação às políticas da UNIMED FESP, devendo periodicamente consultar os documentos normativos, disponíveis na intranet;
- Obedecer a legislação e os regulamentos vigentes, padrões de conduta da UNIMED FESP e determinações existentes nesta política;
- Fazer uso adequado das informações e dos recursos tecnológicos disponibilizados pela empresa em suas atividades diárias;
- Utilizar somente softwares e hardwares disponibilizados pela UNIMED FESP, devidamente homologados e com autorização de uso;
- Assegurar que não haverá má utilização dos recursos tecnológicos sob sua guarda e protegê-los de mau uso por terceiros;
- Zelar por ter uma postura ética e segura na utilização dos recursos e informações da UNIMED FESP;
- Ter postura zelosa, diligente e evitar excesso de exposição;

- Reportar à sua gerência e à área de Segurança da Informação quaisquer suspeitas de falha de segurança, em quaisquer de seus controles.

G. Área Jurídica

- Assegurar, também, que nos contratos celebrados pelo sistema UNIMED FESP, estejam presentes cláusulas de sigilo e confidencialidade que reflitam os princípios e normatizações aqui dispostas, quando cabível.

H. Governança Corporativa - Compliance

- Monitorar o cumprimento de Políticas, Normas e Procedimentos internos;
- Avaliar os riscos e suficiência dos controles envolvidos nas falhas operacionais e, quando aplicável, registrar ocorrência de risco.

I. Auditoria Interna

A Auditoria Interna é uma unidade de caráter executiva e de assessoramento, vinculada organizacionalmente ao Conselho de Administração, com subordinação hierárquica a estrutura de Governança da Unimed FESP, que por sua vez se reporta ao presidente da Unimed Fesp. Compete à Auditoria Interna, no âmbito das Políticas Institucionais de Controles Internos e de Gestão de Riscos e de Capital:

- Supervisionar e monitorar a qualidade e integridade dos mecanismos de controles internos, gestão de riscos e Compliance da empresa, apresentando as recomendações de aprimoramento de políticas, práticas e procedimentos que entender necessárias, manifestando-se ao Conselho de Administração;
- Prestar apoio ao Conselho Fiscal, quando solicitado;
- Recomendar, à Diretoria, a correção ou o aprimoramento de políticas, práticas e procedimentos identificados no âmbito de suas atribuições;
- Outras atividades específicas e correlatas de serviços de auditoria.

7. GESTÃO DE CONSEQUÊNCIA

Colaboradores, fornecedores ou outros que observarem quaisquer desvios às diretrizes desta Política, poderão relatar o fato ao Canal de Ética (https://www.contatoseguro.com.br/unimedfesp), podendo ou não se identificar.

O descumprimento das diretrizes desta Política acarretará aplicação de medidas cabíveis conforme o respectivo grau de importância e de acordo com normativos internos.

Situações excepcionais serão encaminhadas para a Diretoria Executiva e/ou demais órgãos de Governança.

8. REFERÊNCIAS

- Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 Tecnologia da informação. Técnicas de segurança. Código de prática para a gestão da segurança da informação, incluindo sua versão original e posteriores atualizações
- Lei do Marco Civil da Internet e suas respectivas alterações
- Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais, “LGPD”.
- Norma Derivada nº 015/19 - Sobre a Política Nacional de Proteção de Dados Pessoais do Sistema Unimed.
- Lei federal 11.846 – Anticorrupção e Política de Relacionamento com Órgãos Públicos.
- Resolução Normativa 443 da ANS, que dispõe sobre adoção de práticas mínimas de governança corporativa, com ênfase em controles internos e gestão de riscos, para fins de solvência das operadoras de planos de assistência à saúde.

9. DOCUMENTAÇÃO COMPLEMENTAR

- Código de Conduta
- PL 1044-01 Política de Utilização de Recursos de TI

10. DISPOSIÇÕES GERAIS

Nenhum código de conduta ou política pode abranger todas as situações possíveis que envolvam condutas éticas, de falta de transparência e de integridade. Portanto, todos os colaboradores, parceiros, prestadores de serviços e demais deverão exercer vigilância e julgamento cuidadosos em todos os momentos no decorrer de suas atividades profissionais.

Em caso de dúvida, devem buscar orientação do Núcleo de Ética da Unimed FESP.
As disposições desta Política têm validade pelo prazo de 2 (dois) anos, quando deverá ser realizada a sua revisão, ou a qualquer momento no caso de necessidade de alteração.