Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

DISPÕE SOBRE A APROVAÇÃO E INSTITUIÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE NO ÂMBITO DO FUNDO DE PREVIDÊNCIA SOCIAL DO MUNICÍPIO DE MACIEIRA(SC), FUPEM, EM CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD (LEI Nº 13.709/2018) E AS EXIGÊNCIAS DO PRÓ-GESTÃO RPPS.

O PRESIDENTE DO FUNDO DE PREVIDÊNCIA SOCIAL DO MUNICÍPIO DE MACIEIRA(SC), no uso de suas atribuições legais e considerando as disposições da Lei Federal nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural bem como em observância aos princípios da administração pública, à Lei Complementar nº 101/2000, às diretrizes do Pró-Gestão RPPS e às boas práticas de governança e segurança da informação.

CONSIDERANDO que a informação é um ativo que deve ser protegido e cuidado por meio de regras e procedimentos das políticas de segurança, do mesmo modo que protegemos nossos recursos financeiros e patrimoniais;

CONSIDERANDO que a política de segurança da informação é um documento oficial que inclui informações e regras sobre a gestão de senhas, acesso a dados, backup de dados, gerenciamento de dispositivos móveis e outras questões correlatas;

CONSIDERANDO que a política de segurança é um instrumento importante para proteger a sua organização contra ameaças à segurança da informação que ela pertence ou que está sob sua responsabilidade. Uma ameaça à segurança é compreendida neste contexto como a quebra de uma ou mais propriedades fundamentais (confidencialidade, integridade e disponibilidade);

CONSIDERANDO que o conjunto de padrões, normas e diretrizes que estabelece princípios, compromissos, valores, requisitos e orientações a fim de mitigar riscos para os dados armazenados se chama Política de Segurança da Informação — PSI;

CONSIDERANDO que o FUPEM detém informações cadastrais, funcionais e financeiras dos servidores segurados obrigatórios do RPPS do Município de MACIEIRA(SC) e seus dependentes, bem como os funcionários da Unidade Gestora.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

RESOLVE:

Art. 1°. DISPOR e **DAR** conhecimento a todos os servidores do Fundo de Previdência dos Servidores Públicos Municipais de Macieira(SC) e prestadores de serviço acerca das regras que se seguem que compõe a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI.**

Parágrafo único: Esta Política aplica-se a todos os dados pessoais, dados pessoais sensíveis, informações institucionais e ativos de informação, independentemente do meio ou suporte em que se encontrem.

CAPÍTULO I - DOS FUNDAMENTOS

Art. 2°. Um sistema de segurança da informação baseia-se em três princípios básicos:

- **a.** Confidencialidade;
- **b.** Integridade;
- **c.** Disponibilidade.

§1º. Se falar em segurança da informação, deve-se levar em consideração estes três princípios básicos, **pois toda ação que venha a comprometer qualquer um desses princípios, atentará contra a sua segurança.**

§2º. Confidencialidade: A confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso. Caso a informação seja acessada por uma pessoa não autorizada, intencionalmente ou não, ocorre a quebra da confidencialidade. A quebra desse sigilo pode acarretar danos inestimáveis para a empresa ou até mesmo para uma pessoa física.

§3º. Integridade: A integridade é a garantia da exatidão e completeza da informação e dos métodos de processamento. Garantir a integridade é não permitir que a informação seja modificada, alterada ou destruída sem autorização; que ela seja legítima e permaneça consistente. Quando a informação é alterada, falsificada ou furtada, ocorre à quebra da integridade. A integridade é garantida quando se mantém a informação no seu formato original.

§4º. Disponibilidade: A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. Quando a informação está indisponível para o acesso, ou seja, quando os servidores estão inoperantes por conta de ataques e invasões, considera-se um incidente de segurança da informação por quebra de disponibilidade. Mesmo as interrupções involuntárias de sistemas, ou seja, não intencionais, configuram quebra de disponibilidade.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

Art. 3º. Sobre o SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI) devem-se obedecer às seguintes normas de Política de Segurança da Informação:

a. Organização da segurança da informação;
b. Gestão de ativos;
c. Segurança em recursos humanos;
d. Segurança física e do ambiente;
e. Gestão das operações e comunicações;
f. Controle de Acesso;
g. Aquisição, desenvolvimento e manutenção de sistemas de informação;
h. Gestão de incidentes de segurança da informação;
i. Gestão da continuidade do negócio e conformidade;
j. Sigilo sobre as informações acessadas pelos integrantes do FUPEM;
k. Sigilo e proteção dos dados pessoais e sensíveis, nos termos da Lei nº 13.709/2018.

Parágrafo único — O sistema de gestão de segurança da informação é o resultado da sua aplicação planejada, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para a segurança da informação.

Art. 4º. As informações podem ser classificadas em:

a. informações públicas, quando não necessita de sigilo algum;
b. informações internas, quando o acesso externo as informações deve, ser negado;
c. informações confidenciais, quando essas devem ser confidenciais tanto dentro da empresa quanto fora dela e protegidas contra tentativas de acesso interno elou externo.

§1º. A principal razão em classificar as informações, é de que elas não possuem o mesmo grau de confidencialidade, ou então as pessoas podem ter interpretações diferentes sobre o nível de confidencialidade da informação;

§2º. Antes de se iniciar o processo de classificação é necessário conhecer o processo de negócio da organização, compreender as atividades realizadas e, a partir disso, iniciar as respectivas classificações.

Art. 5º. Para fins da Lei Geral de Proteção de Dados Pessoais:

I – O FUPEM é o CONTROLADOR dos dados pessoais tratados no âmbito de suas atividades institucionais;

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

II – Os prestadores de serviços que realizarem tratamento de dados serão considerados OPERADORES;

III – O Encarregado pelo Tratamento de Dados Pessoais será formalmente designado por ato da Presidência.

Art. 6º. A definição clássica é que o ativo compreende ao conjunto de bens e direitos de uma entidade. Entretanto, atualmente, um conceito mais amplo tem sido adotado para se referir ao ativo como tudo aquilo que possui valor para a empresa.

Parágrafo único — A informação ocupa um papel de destaque no ambiente das organizações empresariais, e também adquire um potencial de valorização para as empresas e para as pessoas, passando a ser considerado o seu principal ativo.

Art. 7º. A ameaça pode ser considerada um agente externo ao ativo de informação, pois se aproveita de suas vulnerabilidades para quebrar um ou mais dos princípios básicos da segurança da informação — a confidencialidade, integridade e/ou disponibilidade.

Parágrafo único — As ameaças podem ser divididas nos seguintes tipos básicos:

a. As naturais — são aquelas que se originam de fenômenos da natureza;
b. As involuntárias — são as que resultam de ações desprovidas de intenção para causar algum dano;
c. As intencionais — são aquelas deliberadas, que objetivam causar danos, tais como às realizadas pelos hackers ou crackers.

Art. 8º. A vulnerabilidade é definida como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Vulnerabilidade são as fraquezas presentes nos ativos, que podem ser exploradas, seja ela intencionalmente ou não, resultando assim na quebra de um ou mais princípios da segurança da informação.

§1º. Após terem sido identificadas as vulnerabilidades ou os pontos fracos, é possível dimensionar os riscos ao qual o ambiente está exposto e assim definir medidas de segurança apropriadas para sua correção.

§2º. As vulnerabilidades podem advir de vários aspectos: instalações físicas desprotegidas contra incêndios, inundações, desastres naturais; material inadequado empregado nas construções; ausência de política de segurança para RH; funcionários sem treinamento elou locais de trabalho insatisfatórios; ausência ou não utilização de procedimento de controle de acesso elou utilização de equipamentos por pessoal contratado sem a observância dos requisitos citados anteriormente ou desautorizados; equipamentos obsoletos, sem manutenção e sem restrições para sua utilização; além de softwares sem patch de atualização elou sem licença de funcionamento.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

Art. 9º. Com relação à segurança, os riscos são compreendidos como condições que criam ou aumentam os potenciais de danos e perdas, sendo medido pela possibilidade de um evento vir a acontecer e produzir perdas.

Art. 10º. Para evitar possíveis perdas de informações, que dependendo do seu grau de sigilo, poderá levar o ente a problemas graves, é necessária a elaboração de uma gestão de riscos, onde os riscos são determinados e classificados, sendo depois realizado um conjunto equilibrado de medidas de segurança que permitirá reduzir ou eliminá-los a que o órgão possa estar sujeito além de garantir melhor eficiência nas ações preventivas.

Art. 11º. O backup dos sistemas deve ser armazenado periodicamente em outra mídia, e guardado o mais longe possível do ambiente atual, como em outro setor (cofre da instituição, por exemplo). O procedimento de backup é um dos recursos mais efetivos para assegurar a continuidade das operações em caso de paralisação por conta da ocorrência de algum sinistro.

Art. 12º. Convém que sejam utilizados perímetros de segurança para proteger as áreas que contenham informações e instalações de processamento da informação.

Art. 13º. Apesar de todos os cuidados em se definir os perímetros de segurança, essa ação não produzirá resultados positivos se os colaboradores não estiverem sintonizados com a cultura de segurança da informação. Essa cultura deve estar pulverizada em todo o órgão e especialmente consolidada dentro das áreas críticas de segurança. A informação pertinente ao trabalho dentro dessas áreas deve estar restrita a própria área e somente durante a execução das atividades em que ela se torna necessária.

Parágrafo único - Os locais escolhidos para a instalação dos equipamentos devem estar em boas condições de uso, com boas instalações elétricas, devem conter extintores de incêndios, bem como preferencialmente saídas de emergência, alarme contra incêndio, entre outros aspectos que devem ser levados em consideração.

CAPÍTULO II - DOS ATOS NORMATIVOS

Art. 14º. A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI pode ser definida como um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades sobre o que deve ser feito para alcançar um padrão desejável de proteção para as informações.

§1º.Ela é basicamente um manual de procedimentos que descreve como os recursos de TI da empresa devem ser protegidos e utilizados e é o pilar da eficácia da segurança da informação. Sem regras preestabelecidas, ela torna-se inconsistentes e vulnerabilidades podem surgir.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

§2º. A política tende a estabelecer regras e normas de conduta com o objetivo de diminuir a probabilidade da ocorrência de incidentes que provoquem, por exemplo, a indisponibilidade do serviço, furto ou até mesmo a perda de informações.

§3º. As políticas de segurança geralmente são construídas a partir das necessidades do negócio e eventualmente aperfeiçoadas pela experiência do gestor.

§4º. O intervalo médio utilizado para a revisão da política é de seis meses ou um ano, porém, deve ser realizada uma revisão sempre que forem identificados fatos novos, não previstos na versão atual que possam ter impacto na segurança das informações da organização.

§5º. É recomendado que a política de segurança da informação seja revisada periodicamente e de forma planejada ou quando ocorrerem mudanças significativas, para assegurar a sua continua pertinência, adequação e eficácia.

§6º.A política de segurança não define só procedimentos específicos de manipulação e prote#o da informação, mas atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários e prestadores de serviços) que lidam com essa informação.

Art. 15º. A política de segurança da informação deve estabelecer:

a. Como será efetuado o acesso às informações de todas as formas possíveis, seja ela internamente ou externamente;
b. Quais os tipos de mídias poderão transportar e ter acesso a esta informação;
c. Os mecanismos através dos quais estes requisitos podem ser alocados.

CAPÍTULO III - DA ORGANIZAÇÃO E DO CUMPRIMENTO

Art. 16º. A política de segurança da informação do FUPEM comporá de um gestor de área afins do Município/Unidade Gestora que tenha responsabilidade de gestão.

§1º. A responsabilidade das informações do FUPEM está sob a responsabilidade da proteção dos dados é dos Dirigentes, ressaltando que as informações deverão ser armazenadas em servidores de redes exclusivos do FUPEM.

§2º. Os servidores de redes do FUPEM atualmente são feitos por computadores/desktops que executam essa função e deverão encontrar-se na sede do fundo para condicionamento das informações exclusivas do mesmo.

§3º. Deverão ser digitalizados todos os processos, com o devido armazenamento em Drive na nuvem e a manutenção de backups nos computadores do fundo.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

§4º. No cenário atual, em que as empresas dependem cada vez mais da tecnologia e da informação TI, é vital garantir a segurança adequada deste. ativo, considerado estratégico em sua missão de prestar serviços de qualidade.

§5º. O conjunto de normas e regras que regulem a utilização dos sistemas das empresas, assim como o acesso a redes sociais e e-mails pessoais.

§6º. Os servidores deverão estar cientes do monitoramento.

Art. 17º. A política de segurança da informação do FUPEM estende também à empresa terceirizada onde mantêm o site https://www.macieira.sc.gov.br, serviços on-line, aplicativos administrativos e os e-mails institucionais, onde tem regras específicas, porém que atendem a política de segurança de informação da contratada.

Art. 18º. Quando necessário será contratada empresa especializada para estudo das vulnerabilidades e se existir será realizado ações para saná-las.

Art. 19º. Quando da necessidade de cadastramento de um novo usuário para utilização de sistemas ou equipamentos de informática no FUPEM, o setor de origem do novo usuário deverá comunicar esta necessidade aos Dirigentes por meio de memorando, e-mail ou correio interno, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

Art. 20º. É terminantemente proibido o uso de programas ilegais (PIRATAS) elou desautorizados pela UG Previdenciária. Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos/computadores e afins. Periodicamente, o Setor de Informática (TI) fará verificações nos dados dos servidores elou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

Art. 21º. O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva dos Dirigentes, assim como a manutenção, alteração e atualização de equipamentos e programas.

Art. 22º. Os Dirigentes deverão informar ao administrador do site/sistemas, toda e qualquer movimentação de temporários e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema do órgão. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo Setor Responsável.

Art. 23º. É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios do FUPEM.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

Art. 24º. É de propriedade do FUPEM, todos os "designs", criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício.

CAPÍTULO IV - DO ACESSO E DAS PROIBIÇÕES

Art. 25º. O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais. Sites que não contenham informações que agreguem conhecimento profissional elou para o desenvolvimento do trabalho não devem ser acessados.

§1º. O uso da Internet será monitorado a luz das normas vigentes, inclusive através de "logs" (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

§2º. A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição da unidade gestora do FUPEM ou responsável definido pela mesma, com base, também, em recomendação.

§3º. Não é permitido instalar programas provenientes da Internet nos microcomputadores do órgão, sem expressa anuência, exceto os programas oferecidos por órgãos públicos federais, estaduais elou municipais, todos previamente informados aos Dirigentes.

§4º. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

§5º. Quando navegando na Internet, é proibido a visualização, transferência (downloads/uploads), cópia ou qualquer outro tipo de acesso a sites:

a. De estações de rádio;
b. De conteúdos pornográficos ou relacionados a sexo;
c. Que defendam atividades ilegais;
d. Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
e. Que promovam a participação em salas de discussão de assuntos não relacionados aos serviços;
f. Que promovam discussão pública sobre os assuntos do órgão, a menos que autorizado pela Diretoria;
g. Que possibilitem a distribuição de informações de níveis "Confidenciais";
h. Que permitam a transferência (downloads ou uploads) de arquivos elou programas ilegais;

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

i. Que permitem a transferência (downloads ou uploads) de arquivos elou programas que promovam o acesso remoto a qualquer dispositivo do FUPEM, sem a anuência do Setor Responsável;
j. Que permitam a transferência (downloads ou uploads) de arquivos elou programas que busquem na rede interna elou externa vulnerabilidades em dispositivos elou serviços de qualquer natureza, salvo em casos de anuência da gestora elou Setor de Informática (TI);
k. Que permitam o uso elou armazenamento de programas elou serviços relacionados a entretenimento tais como jogos, karaokê e desafios (ou similares);

§6º. Será disponibilizado um servidor de arquivos, contendo diretórios para cada setor do FUPEM onde os funcionários lotados no setor específico terão acesso, e ainda será disponibilizado acesso comum a setores distintos elou a todos os setores quando os dados constantes nos diretórios subsidiar o desenvolvimento do trabalho da Instituição em mais de um setor, assim será cognominado o diretório de "PublicoNet".

§7º. A Diretoria do FUPEM na pessoa do gestor terá acesso a todos os diretórios da Instituição.

Art. 26º. O correio eletrônico fornecido pelo FUPEM é um instrumento de comunicação interna e externa para a realização do negócio do Órgão.

§1º. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem do FUPEM, não podem ser contrárias à legislação vigente e nem aos princípios éticos do FUPEM.

§2º. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

§3º. Para incluir um novo usuário no correio eletrônico, a Diretoria deverá fazer um pedido formal ao Setor de Informática, que providenciará a inclusão do mesmo.

§4º. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado. Eril caso de congestionamento no Sistema de correio eletrônico o Setor de Informática fará auditorias no servidor de correio elou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

Art. 27º. É terminantemente proibido o envio de mensagens que:

a. Contenham declarações difamatórias e linguagem ofensiva;
b. Possam trazer prejuízos a outras pessoas;
c. Sejam hostis e inúteis;
d. Sejam relativas a "correntes", de conteúdos inúteis, pornográficos ou equivalentes;
e. Possam prejudicar a imagem da organização;
f. Possam prejudicar a imagem de outras empresas;
g. Sejam incoerentes com as políticas do FUPEM.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

Art. 28º. O Setor de Informática é responsável pela aplicação da Política do órgão em relação à compra e substituição de "software" e "hardware".

Parágrafo único - Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de Informática.

Art. 29º. Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade do FUPEM, devem estar cientes de que:

a. Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo realização de atividades profissionais.
b. A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
c. É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
d. O usuário não deve alterar a configuração do equipamento recebido.

Art. 30º. Alguns cuidados que devem ser observados:

§1° Fora do trabalho:

a. Mantenha o equipamento sempre com você;
b. Atenção em hall de hotéis, aeroportos, aviões, táxi, etc.,
c. Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;
d. Atenção ao transportar o equipamento na rua.

§2º. Em caso de furto:

a. Registre a ocorrência em uma delegacia de polícia;
b. Comunique ao seu superior imediato e ao Setor de Informática;
c. Envie uma cópia da ocorrência para o Setor de Informática.

Art. 31º. Os responsáveis pelos setores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

§1º.O Setor verificará se houve acesso dos usuários às informações, verificando:

a. Que tipo de informação o usuário pode acessar;
b. Quem está autorizado a acessar determinada rotina elou informação;
c. Quem acessou determinada rotina e informação;
d. Quem autorizou o usuário a ter permissão de acesso determinada rotina ou informação;
e. Que informação ou rotina determinadas usuário acessou;
f. Quem tentou acessar qualquer rotina ou informação sem estar autorizado.
g. Se algum usuário teve acesso de forma indevida a senhas de sistemas do CADPREV, BANCOS, E-MAIL elou tipos de sistemas.

§2º.0 exercício fiscalizatório acima previsto deverá ser exercido com moderação e estrita observância da necessidade de forma a não implicar em violação de intimidade de qualquer servidor ou de seus dados eletrônicos por parte do servidor, implicara em cometimento de crime previsto em Lei sobre a matéria.

§3º.Todas as informações e dados colhidos no âmbito do FUPEM, no exercício do poder fiscalizatório enumerado no parágrafo 1 º, é integralmente sigilosa, não podendo ser exposta a terceiro, devendo constar unicamente em relatório técnico que deve ser entregue diretamente à Gestão do FUPEM, para adoção das medidas cabíveis.

§4º. Todos os funcionários que tenham acesso às informações de qualquer natureza, seja de processos eletrônicos ou físicos, dados eletrônicos e pessoais de segurados e funcionários do FUPEM, encontra-se vinculado a dever de sigilo profissional art. 154 do Código Penal e abrangido por obrigação civil de não fazer, sujeitando-se às penalidades previstas no art. 251 do Código Civil.

§5º. Todos os dados que o setor de Tecnologia da Informação armazenar em dispositivos como pendrive, HD externo ou similar, por motivo de transferência de dados das máquinas, entre outros, deverão ser posteriormente excluídos de tais dispositivos com total segurança.

§6º. Deverá o setor de TI ter uma rotina de verificação de máquinas e equipamentos de informática nos setores, recebendo a demanda dos usuários e realizando o atendimento.

Art. 32º. Todo arquivo em mídia proveniente de entidade externa ao órgão deve ser verificado por programa antivírus.

§1º. Todo arquivo recebido/obtido através do ambiente Internet deve ser verificado por programa antivírus.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

§2º. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede.

§3º. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

Art. 33º. Quanto aos equipamentos e informações contidas nos mesmos:

a. É proibida a execução de programas externos nos computadores e/ou equipamentos do FUPEM sem o devido consentimento da gestora elou setor de informática;

b. É proibido abrir quaisquer equipamentos relacionados à área de informática (ou similares) com o intuito de realizar reparos, troca de peças, instalação de novos dispositivos ou complementos (físicos elou virtuais), sem o devido consentimento da gestora elou setor de informática;

c. Tornar ciente de que o FUPEMnão é responsável por informações pessoais que não se referem à natureza de sua operação, definindo essas informações como sendo indevidas para uso interno à instituição;

d. É terminantemente proibido disseminar, intencional ou não, vírus ou qualquer programa que gere ameaça à continuidade do serviço.

e. É proibido o compartilhamento de senhas elou similares, sendo o usuário responsabilizado pelo seu uso indevido.

Art. 34º. É proibido o uso de notebook ou similares, de propriedade privada dos funcionários do FUPEM, para uso no desenvolvimento de trabalhos da instituição e também de arquivamento de dados, sejam imagens, textos ou quaisquer dados exclusivos da Instituição.

Art. 35º. A presente Política de Segurança da Informação aplica-se a todos os servidores, diretores, conselheiros, estagiários, prestadores de serviços e demais colaboradores que, de forma direta ou indireta, executem atividades relacionadas ao Fundo de Previdência do Município de MACIEIRA(SC), FUPEM, bem como aos convênios, acordos, termos e instrumentos congêneres celebrados pelo fundo.

§1° Todos os usuários abrangidos por esta Política deverão proteger os ativos de informação do fundo, observando os princípios da confidencialidade, integridade, disponibilidade e autenticidade, e utilizar tais informações exclusivamente para fins institucionais, em conformidade com as normas internas e a legislação vigente.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

§2° O descumprimento das obrigações previstas nesta Política sujeitará o infrator, servidor, diretor, conselheiro, estagiário ou prestador de serviço às sanções cabíveis, inclusive responsabilidade administrativa, civil e penal, sem prejuízo de outras medidas disciplinares previstas em lei, regulamentos ou contratos.

Art. 36º. Os prestadores de serviço e contratados deverão tratar os dados pessoais e institucionais aos quais tenham acesso exclusivamente para a execução dos serviços contratados, comprometendo-se a:

I. manter sigilo e confidencialidade sobre as informações;

II. adotar medidas técnicas e administrativas adequadas à proteção contra acessos não autorizados, vazamentos, alterações indevidas ou qualquer forma de tratamento ilícito;

III. observar as disposições da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e demais normas aplicáveis.

§1º. Deverá constar, nos contratos de prestação de serviços firmados com o FUPEM, Cláusula de Confidencialidade, como condição indispensável para a concessão de acesso aos sistemas e ativos de informação do fundo.

§2º.Qualquer solicitação de arquivos, banco de dados ou similares por parte de prestadores de serviço somente poderá ser atendida mediante autorização formal do gestor responsável, comunicada ao setor de Tecnologia da Informação.

Art. 37º. Todos os usuários abrangidos por esta Política, servidores, conselheiros, estagiários, diretores e prestadores deverão assinar o Termo de Responsabilidade e Confidencialidade, como condição prévia ao recebimento de credenciais de acesso ou ao início das atividades que envolvam informações do fundo.

§1º.A assinatura dos Termos ocorrerá durante as ações de divulgação e sensibilização da Política de Segurança da Informação, promovidas pelo fundo.

§2º. Com a assinatura, o usuário assume formalmente:

I. a responsabilidade pelo uso adequado dos ativos e sistemas de informação;

II. o compromisso de cumprir integralmente as disposições desta Política;

III. a obrigação de manter o sigilo das informações às quais teve acesso, inclusive após o desligamento ou término da prestação de serviços, pelo prazo legal aplicável.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

CAPÍTULO V - DO CUMPRIMENTO DAS ORIENTAÇÕES

Art. 38º. O não cumprimento da Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações:

a. advertência formal;
b. suspensão;
c. exoneração do cargo.

d. outras sanções administrativas previstas em legislação específica e normas internas, observados o contraditório e a ampla defesa.

§1º. Respeitar-se-á o Estatuto dos Servidores Públicos de MACIEIRA(SC) no que se refere ao Regime Disciplinar ou outra Lei específica que a determine.

§2º. No que couber, outra ação disciplinar ou processo civil ou criminal poderá ser aplicado, a depender da gravidade da conduta.

Art. 39º. A presente Política de Segurança da Informação aplica-se a todos os servidores, diretores, conselheiros, estagiários, prestadores de serviços e demais colaboradores que, de forma direta ou indireta, executem atividades relacionadas ao Fundo de Previdência Social do Município de MACIEIRA(SC) – FUPEM, bem como aos convênios, acordos, termos e instrumentos congêneres celebrados pelo Fundo.

§1º. Todos os usuários abrangidos por esta Política deverão **proteger os ativos de informação do Fundo**, observando os princípios da **confidencialidade, integridade, disponibilidade e autenticidade**, e utilizar tais informações **exclusivamente para fins institucionais**, em conformidade com as normas internas e a legislação vigente.

§2º. O **descumprimento** das obrigações previstas nesta Política sujeitará o infrator, servidor, diretor, conselheiro, estagiário ou prestador de serviço às **sanções cabíveis**, inclusive **responsabilidade administrativa, civil e penal**, sem prejuízo de outras medidas disciplinares previstas em lei, regulamentos ou contratos.

Art. 40º.Os prestadores de serviço e contratados deverão tratar os dados pessoais e institucionais aos quais tenham acesso exclusivamente para a execução dos serviços contratados, comprometendo-se a:

I. manter sigilo e confidencialidade sobre as informações;

II. adotar medidas técnicas e administrativas adequadas à proteção contra acessos não autorizados, vazamentos, alterações indevidas ou qualquer forma de tratamento ilícito;

III. observar as disposições da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e demais normas aplicáveis.

§1º Deverá constar, nos contratos de prestação de serviços firmados com o FUPEM**, Cláusula de Confidencialidade**, como **condição indispensável** para a concessão de acesso aos sistemas e ativos de informação do Fundo.

§2º Qualquer solicitação de **arquivos, banco de dados ou similares** por parte de prestadores de serviço somente poderá ser atendida mediante **autorização formal do gestor responsável**, comunicada ao setor de Tecnologia da Informação.

Art. 41º. Todos os usuários abrangidos por esta Política, servidores, conselheiros, estagiários, diretores e prestadores deverão assinar o Termo de Responsabilidade e Confidencialidade, como condição prévia ao recebimento de credenciais de acesso ou ao início das atividades que envolvam informações do Fundo.

§1º A assinatura dos Termos ocorrerá durante as **ações de divulgação e sensibilização da Política de Segurança da Informação**, promovidas pelo Fundo.

§3º Com a assinatura, o usuário assume formalmente:

I. a **responsabilidade pelo uso adequado** dos ativos e sistemas de informação;
II. o **compromisso de cumprir integralmente** as disposições desta Política;
III. a **obrigação de manter o sigilo** das informações às quais teve acesso, inclusive **após o desligamento ou término da prestação de serviços**, pelo prazo legal aplicável.

MACIEIRA(SC), 06 de Julho de 2026.

EDUARDO MIGUEL ZILIO:03418619959

Assinado digitalmente por EDUARDO MIGUEL ZILIO:03418619959
ND: C=BR, O=ICP-Brasil, OU=Certificado Digital PF A1, OU=Videoconferencia, OU=15074920000202, OU=AC SyngularID Multipla, CN=EDUARDO MIGUEL ZILIO:03418619959
Razão: Eu sou o autor deste documento
Localização:
Data: 2026.07.10 08:10:33-03'00'
Foxit PDF Reader Versão: 2025.2.1

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

ANEXO I

TERMO DE RESPONSABILIDADE E SIGILO DA INFORMAÇÃO

Eu, _____, RG nº _____, CPF nº _____, Cargo/Função/Prestador de Serviço: _____, Matrícula funcional ou Contrato nº _____, nos termos da Política de Segurança da Informação do Fundo de Previdência Social dos Servidores do Município de Macieira(SC|)- FUPEM, declaro que:

Tenho pleno conhecimento das minhas responsabilidades quanto ao sigilo, confidencialidade e proteção das informações e ativos de informação aos quais tenha acesso, venha a ter acesso ou obtenha conhecimento em razão das atividades exercidas no âmbito do Fundo, ou fora dele.

Comprometo-me a:

a. Utilizar as informações institucionais exclusivamente para o desempenho das minhas atividades funcionais ou contratuais, vedada qualquer outra finalidade;
b. Manter o sigilo e a confidencialidade sobre todas as informações sigilosas, ainda que após o desligamento ou término da prestação de serviço;
c. Adotar medidas de segurança adequadas, conforme orientações da Política de Segurança da Informação;
d. Comunicar imediatamente ao gestor ou setor competente qualquer ocorrência de violação, perda, acesso indevido ou uso indevido de informações do Fundo.

Estou ciente das penalidades legais aplicáveis em caso de violação do dever de sigilo,

especialmente as previstas nos artigos 153 e 325 do Código Penal (Decreto-Lei nº 2.848/1940), além das sanções administrativas, civis e contratuais decorrentes do descumprimento das normas internas e legais.

A obrigação de sigilo aqui assumida permanece válida enquanto a informação não for tornada pública por autoridade competente ou mediante autorização formal e expressa do Fundo.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

Para os fins deste Termo, entende-se por Informação Sigilosa toda informação, em formato físico, eletrônico, verbal ou de qualquer outro meio, que possua restrição de acesso público em razão de sua relevância para a segurança institucional, patrimonial ou administrativa, incluindo, mas não se limitando a:

I. dados pessoais e sensíveis de servidores, aposentados e pensionistas;
II. informações sobre operações, processos, planos, intenções, projetos, sistemas, metodologias, fluxogramas, relatórios e documentos internos;
III. quaisquer outros dados cuja divulgação não autorizada possa comprometer a imagem, a segurança, os ativos ou as atividades do Fundo .

Local e data: _____, ___ de _____ de _____

Assinatura do(a) Usuário(a)

( ) Servidor ( ) Conselheiro ( ) Diretor ( ) Estagiário ( ) Prestador de Serviço

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

ANEXO II

COMPROMISSO LEGAL CÓDIGO PENAL BRASILEIRO

DIVULGAÇÃO DE SEGREDO - **Art. 153 § 1º**-A - Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em Lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção de 1(um) a 4(quatro) anos e multa.

INVASÃO DE DISPOSITIVO INFORMÁTICO – Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)

INSERÇÃO DE DADOS FALSOS EM SISTEMA DE INFORMAÇÕES – Art. 313-A Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou banco de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão de 2(dois) a 12(doze) anos e multa.

MODIFICAÇÃO OU ALTERAÇÃO NÃO AUTORIZADA DE SISTEMA DE INFORMAÇÕES – Art. 313-B. Modificar ou alterar, o funcionário, sistema de informação ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção de 3(três) meses a 2(dois) anos e multa. Parágrafo único: As penas são aumentadas de um terço até a metade se a modificação ou alteração resulta em dano para a Administração Pública ou para o administrado.

FALSIDADE IDEOLÓGICA – **Art. 299** – Omitir, em documento público ou particular, declaração que dele deva constituir, ou nele inserir, fazer inserir declaração falsa ou diversa da que deva ser escrita, com fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante.

Pena – Reclusão de 01 (um) a 05 (cinco) anos e multa se o documento é público, e reclusão de 01 (um) a 03 (três) anos e multa se o documento é particular.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

Parágrafo único – Se o agente é funcionário público e comete o crime prevalecendo-se do cargo ou se a falsificação ou alteração e de assentamento de registro civil, aumenta-se a pena da sexta parte.

VIOLAÇÃO DE SIGILO FUNCIONAL – Art. 325 – Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena: detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.

Art. 325 § 1º-Nas mesmas penas deste artigo incorre quem: I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistema de informações ou banco de dados da Administração Pública, II – se utiliza, indevidamente, do acesso restrito.

§2º - Se da ação ou omissão resulta dano à Administração Pública ou a outrem: Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.

FUNCIONÁRIO PÚBLICO – Art. 327 – Considera-se funcionário público para os efeitos penais, quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública.

Art. 327 § 1º – Equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal e quem trabalha para empresa prestadora de serviço contratada ou conveniada para execução de atividade típica da Administração Pública.

Art. 327 § 2º – A pena será aumentada da terça parte quando os autores dos crimes previstos neste capítulo, forem ocupantes de cargos em comissão ou de função de direção ou assessoramento de órgão da administração direta, sociedade de economia mista, empresa pública ou fundação instituída pelo poder público.

Rua José Augusto Royer, 133, Centro, Macieira - SC | Cep: 89.518-000
macieira.sc.gov.br | prefeitura@macieira.sc.gov.br
(49) 3574-2000

ANEXO III

TERMO DE USO DOS SISTEMAS DE INFORMAÇÃO

Eu, _____, RG nº _____, CPF nº _____, Função/cargo/Prestador de Serviços: _____, Sob a matrícula funcional/Contrato nº _____,

CONSIDERANDO que o FUPEM:

a. disponibiliza a infraestrutura tecnológica, como ferramenta de trabalho, para o pleno desenvolvimento das atividades profissionais;

b. detém a exclusiva propriedade da infraestrutura tecnológica disponibilizada;

c. torna explícito que não há expectativa de privacidade sobre os ativos, informações e recursos institucionais, tendo em vista que os mesmos são destinados para fins profissionais;

d. pode haver prejuízos pela má utilização dos recursos disponibilizados;

DECLARO, estar ciente e ter pleno conhecimento:

a. da Política de Segurança da Informação do Fundo de Previdência Social dos Servidores do Município de Macieira (SC) - FUPEM, apresentada na entrevista de admissão e disponibilizada de inteiro teor na Intranet;

b. da realização do monitoramento dos recursos tecnológicos disponibilizados, indispensável para a manutenção do nível de segurança adequado da organização;

c. de que o FUPEM pode realizar auditoria interna sobre os recursos de hardware e software disponibilizados para as atividades profissionais e;

d. que o descumprimento da PSI está sujeito às sanções previstas em Lei Municipal, cláusulas contratuais e demais legislações vigentes, sem prejuízo das ações penal, civil e administrativa, previstas em legislação específica, respeitados os princípios constitucionais do contraditório e da ampla defesa.

_____, _____, de ___ de ____

_____ (Assinatura)