

# POLÍTICA DE SEGURANÇA

## DA

# INFORMAÇÃO

## SUMÁRIO:

1 – INTRODUÇÃO	4
2 – NORMA ABNT NBRISO/IEC 27002:2005 E DEFINIÇÕES	5
3 – OBJETIVO	7
4 - INSTRUMENTOS NORMATIVOS	7
5 - DO ACESSO A INFORMAÇÃO E DA SUA DIVULGAÇÃO	9
6 - DA APROVAÇÃO E REVISÃO DA POLITICA DE SEGURANÇA DA INFORMAÇÃO.	10
7 - DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO	10
8 - CLASSIFICAÇÃO DA INFORMAÇÃO	10
9 - PROTEÇÃO DA INFORMAÇÃO	12
10 - PRIVACIDADE DA INFORMAÇÃO	13
11 - TRANSFERÊNCIAS DE SERVIDORES	13
12 - CÓPIAS DE SEGURANÇA – BACKUP	14
13 - USO DO AMBIENTE WEB (Internet)	15
14 - USO DO CORREIO ELETRÔNICO – (E-mail)	15
15 - SISTEMAS, APLICATIVOS E EQUIPAMENTOS DO IPREMISA.	17
16 - USO DE COMPUTADORES E EQUIPAMENTOS DO IPREMISA	17
17 - PAPÉIS E RESPONSABILIDADES	18
17.1. SERVIDORES, CONSELHEIROS, SEGURADOS, ESTAGIÁRIOS E PRESTADORES DE SERVIÇOS.	18
18 – DIRETOR SUPERINTENDENTE DO IPREMISA	19
21 - JURÍDICO	21
22 - GESTOR DA INFORMAÇÃO	21
23 – AUDITORIA	22
24 - VIOLAÇÕES E SANÇÕES	22
24.1 - VIOLAÇÕES	22
24.2 - SANÇÕES	23
25 - LEGISLAÇÃO APLICÁVEL	23



## 1 – INTRODUÇÃO

O presente documento constitui uma declaração formal do **IPREMISA** – Instituto de Previdência Municipal de Ilha Solteira do seu compromisso com a proteção dos dados e das informações de sua propriedade ou sob sua custódia, a fim de reduzir exposições aos riscos (incertezas) com o objetivo de assegurar as conformidades com a segurança da informação. Portanto, esta PSI - Política de Segurança da Informação devem ser seguidos por todos os seus dirigentes, conselheiros, servidores, segurados, e os prestadores de serviços deste Regime Próprio de Previdência Social.

Visando assegurar que as informações do **IPREMISA** não estejam com pessoas desautorizadas, não sejam corrompidas ou mesmo inacessíveis, faz-se necessário a implementação da Política de Segurança da Informação - P.S.I para garantir a confidencialidade, integridade e disponibilidade, que são os pilares da segurança da informação.

O propósito é formalizar o direcionamento estratégico da gestão de segurança da informação, estabelecendo as diretrizes a serem seguidas para a implantação e manutenção de uma política de segurança da informação, guiando-se, pelos conceitos e orientações das normas ABNT ISO/IEC da família 27000.

O gerenciamento dos riscos é um dos principais processos da gestão da segurança, pois visa identificar, analisar, avaliar e mitigar os riscos inerentes à segurança da informação. Para isso, a conscientização de todos é imprescindível para a prevenção de incidentes e, esta política de segurança da informação devem ser seguidas por todos nas instalações do **IPREMISA** como uma ferramenta de trabalho que serve para ajudá-los em suas rotinas operacionais.

É dever de todos do **IPREMISA** – INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE ILHA SOLTEIRA, seguir as normas e as diretrizes estabelecidas nesta Política de Segurança da Informação - P.S.I.

## 2 – NORMA ABNT NBRISO/IEC 27002:2005 E DEFINIÇÕES

A **ABNT NBR ISO/IEC 27002:2005**, define a segurança da informação como sendo a “preservação da confidencialidade, da integridade e da disponibilidade da informação”. Nesse contexto, a segurança da informação é a garantia de que as informações da organização serão protegidas de acordo com estes três pilares:

**Confidencialidade:** pode ser definida como a garantia de que as informações serão acessadas apenas pelas pessoas que tem autorização para acessá-las;

**Integridade:** é a garantia de que as informações são corretas e completas e;

**Disponibilidade:** é a garantia de que as informações estarão disponíveis para serem acessadas pelas pessoas que tem autorização para vê-las quando forem necessárias.

**Destaca ainda que a “Segurança da informação”** é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.”

**Ainda de acordo com a norma ABNT BR ISO/IEC27002:2005**, “A *segurança da informação* é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.”

Mediante tal embasamento e considerando o disposto na adesão ao Pró Gestão - Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social, o **IPREMISA – INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE ILHA SOLTEIRA** resolve implantar a Política de Segurança da Informação (P.S.I.), cuja estrutura e diretrizes são expressas neste documento. Para os efeitos desta Política, aplicam-se os seguintes termos e definições:

**Colaborador:** Todos os servidores de quaisquer cargo, conselheiros, segurados e estagiários;



**Confidencialidade:** Informação acessível ou divulgada somente às pessoas autorizadas;

**Disponibilidade:** Pessoas autorizadas com acesso à informação sempre que necessário;

**Integridade:** Informações mantidas integras em seu formato original;

**Normas de Segurança da Informação:** Especificam os processos e controles que devem ser implementados para o alcance dos objetivos de segurança da informação definidos nesta política;

**Prestadores de serviços:** Pessoa jurídica ou física que mantenha contrato de prestação de serviço com o **IPREMISA**.

**Segurança da Informação:** É o conjunto de controles que visam garantir a preservação dos aspectos de confidencialidade, integridade e disponibilidade das informações;

**Termos de ciência de Segurança:** Declaração onde o colaborador atesta a ciência sobre todos os termos tratados nessa PSI, normas a ela vinculadas e a sua estrutura de funcionamento;

**Visitante:** Todo indivíduo que não mantenha qualquer vínculo formal com o **IPREMISA**, ou seja, aqueles que não se enquadram na definição de colaborador, conforme acima.

**Ativo:** É tudo aquilo que tenha valor para a organização. [ISO/IEC 13335- 1:2004]

**Ativo de Informação:** qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio.

**Ameaça:** Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou a instituição. [ISO/IEC 13335-1:2004].

**Controle:** forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. [ABNT NBR ISO/IEC 27002:2005].

**Evento de segurança da informação:** ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação. [ISO/IEC TR 18044:2004].

**Incidente de segurança da informação:** indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. [ISO/IEC TR 18044:2004].

**Informação:** agrupamento de dados que contenham algum significado.

**Risco:** combinação da probabilidade de um evento e de suas consequências. [ABNT ISO/IEC Guia 73:2005].

**Vulnerabilidade:** fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. [ABNT NBR ISO/IEC 27002:2005].

### 3 – OBJETIVO

Esta PSI - Política de Segurança da Informação foi elaborada para orientar na criação de normas mais específicas e procedimentos para o tratamento seguro das informações e de outros ativos organizacionais que processam ou armazenam dados e informações, além de auxiliar também na identificação e classificação das informações e dos demais ativos quanto à sua importância para este Regime Próprio de Previdência Social do Município de Ilha Solteira - IPREMISA.

Esta norma a ser implementada define uma série de controles para proteção desses ativos e informações, como a análise crítica e manutenção da própria Política de Segurança da Informação, a atribuição de responsabilidades relativas à segurança da informação, a elaboração de contratos e acordos de confidencialidade entre instituições prevendo a preservação da segurança da informação, a execução de inventários de ativos, a contratação de mão de obra, termo de responsabilidade e sigilo da informação, termo de uso dos sistemas de informação e os controles de acesso físico às dependências do IPREMISA.

O objetivo da PSI – Política da Segurança da Informação é garantir a segurança dos ativos desta autarquia previdenciária municipal que busca prevenir e mitigar os riscos e incidentes



na operacionalização das suas atribuições institucional. Por definição, um ativo é tudo aquilo que pode ser transformado em valor para a empresa. Assim, quando falamos em informação, ela só tem valor se os três pilares da segurança que são: Confidencialidade, Integridade e Disponibilidade também conhecida pela sigla CID forem alcançados.

## 4 - INSTRUMENTOS NORMATIVOS

A preocupação com segurança da informação na Administração Pública Federal vem sendo demonstrada através de diferentes instrumentos normativos. Podemos destacar os seguintes ordenamentos jurídicos:

Código Penal (Decreto-lei nº 2.848, de 07 de dezembro de 1940), prevê estabelece, no art. 153 e art. 325 que se deve guardar o sigilo necessário da informação. O mesmo código prevê ainda, as penalidades nos termos da legislação para a divulgação de segredo; invasão de dispositivo informático; falsidade ideológica; inserção de dados falsos em sistema de informações; modificação ou alteração não autorizada de sistema de informações e violação de sigilo funcional.

Lei nº 8.159/1991 diz que é *“dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação”*.

A Lei nº 9.983/2000 altera o Código Penal, incluindo uma preocupação com a integridade e confiabilidade das informações armazenadas em sistemas computacionais ao tipificar a alteração desses dados.

O Decreto nº 9.637/2018 que revogou o Decreto nº 3.505/2000 institui a Política de Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação, destacando que um dos pressupostos básicos é a conscientização dos órgãos e entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco de suas vulnerabilidades.

Já o Decreto nº 7.845/2012, regulamenta procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo no âmbito do Poder Executivo Federal, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Por último, temos em vigor desde o último dia 18 de setembro de 2020, a Lei Nº 13.709/2018, de 14 de agosto de 2018, que é a 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 tem como objetivo regulamentar a política de proteção de dados pessoais e, modifica alguns dos artigos do Marco Civil da Internet e impacta outras normas como as alterações no cadastro positivo, transformando drasticamente a maneira como empresas e órgãos públicos tratam a privacidade e a segurança das informações de usuários e clientes.

A LGPD prevê a utilização de medidas técnicas e administrativas aptas a proteger os dados, tornando necessária haver a Governança dos Dados, identificando o seu armazenamento, qual seu fluxo, classificando seu nível (dados pessoais, sensíveis ou não), gerenciando seu uso e ciclo de vida, protegendo de possíveis vazamentos ou deleções indevidas e monitorando sua utilização.

Este documento que compõem a estrutura normativa está dividido em três categorias:

**a) Política** (nível estratégico): constituída do presente documento, define as regras de alto nível que representam os princípios básicos que o **IPREMISA** decidiu incorporar à sua gestão de acordo com a visão estratégica e serve como base para que as normas e os procedimentos sejam criados e detalhados;

**b) Normas** (nível tático): especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes da política de segurança da informação;

**c) Procedimentos** (nível operacional): instrumentalizam o disposto nas normas e na política, permitindo a direta aplicação nas atividades do **IPREMISA**.

## 5 - DO ACESSO A INFORMAÇÃO E DA SUA DIVULGAÇÃO

Caberá ser observadas as normas e procedimentos específicos aplicáveis, visando assegurar a:

- I - Gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;
- II - Proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade e;
- III- Proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.



Os documentos integrantes da estrutura desta P.S.I. devem ser divulgados a todos os servidores, conselheiros, segurados, estagiários e prestadores de serviços do **IPREMISA**, através dos meios oficiais de divulgação interna do **IPREMISA** e, publicadas no site da instituição, de maneira que seu conteúdo possa ser consultado a qualquer momento.

## 6 - DA APROVAÇÃO E REVISÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

Os documentos integrantes da estrutura normativa da Segurança da Informação do IPREMISA deverão ser aprovados e revisados conforme critérios descritos abaixo:

**a) Política**

Nível de aprovação: Superintendencia  
Periodicidade da revisão: anual

**b) Normas**

Nível de aprovação: Assessoria Jurídica  
Periodicidade da revisão: semestral

**c) Procedimentos**

Nível de aprovação: Responsável da área. (administrativo / tecnologia).  
Periodicidade da revisão: semestral.

Durante o primeiro ano de vigência de cada documento, considerado a partir da data de sua publicação, a periodicidade das revisões poderá ser igual à metade dos períodos acima definidos.

## 7 - DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A seguir, apresentamos as diretrizes da política de segurança da informação do IPREMISA que constituem os principais pilares do sistema de segurança da informação da instituição, norteando a elaboração das normas e procedimentos.

## 8 - CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação das informações é o processo de identificar e definir níveis e critérios de proteção adequada para as informações, objetivando garantir a segurança das mesmas. Uma organização precisa ser capaz de identificar os valores de suas informações para garantir sua confidencialidade, integridade e disponibilidades. O objetivo principal desta classificação está em priorizar recursos, focando os investimentos nas informações mais importantes para a

organização. São exemplos de informações:

- a) **Dados:** Base de dados e arquivos, documentação de sistemas, informações armazenadas, procedimentos de suportes ou operação;
- b) **Software:** Aplicativos, sistemas ferramentas de desenvolvimento e utilitários;
- c) **Ativos físicos:** equipamentos computacionais (processadores, monitores e impressoras), equipamentos de comunicação (roteadores, hub), token, pen drive e mídias magnéticas (fitas, discos), estações de trabalho (mesas e cadeiras);
- d) **Serviços:** serviço de operadora de telecomunicação, dados e internet, serviço de energia elétrica, água e etc..

Define-se como necessária a classificação de toda a informação de propriedade do **IPREMISA** de maneira proporcional ao seu valor para a instituição, para possibilitar o controle adequado da mesma, devendo ser utilizados os seguintes níveis de classificação:

- a) **Pública:** É uma informação do **IPREMISA** ou de seus segurados com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente.
- b) **Interna:** É uma informação do **IPREMISA** na qual não tem interesse em divulgar, mas cujo acesso por parte de indivíduos externos ao **IPREMISA** deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da instituição, porém, não com a mesma magnitude de uma informação confidencial ou restrita. Pode ser acessada sem restrições por todos os segurados do **IPREMISA**.
- c) **Confidencial:** É uma informação crítica para o **IPREMISA** ou de seus segurados. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem institucional, operacional ou, ainda, sanções administrativas, civis e criminais aos seus servidores e segurados. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por servidores, conselheiros, segurados e/ou prestadores de serviços.
- d) **Informação Restrita:** É toda informação que pode ser acessada somente por



usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos à organização e/ou comprometer a estratégia da organização.

É importante manter a vigilância para que não circulem informações e/ou mídias consideradas confidenciais e/ou restritas, bem como não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, usando o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas que possam ficar expostos indevidamente.

## 9 - PROTEÇÃO DA INFORMAÇÃO

Define-se como necessária a proteção das informações da instituição ou sob sua custódia como fator primordial nas atividades profissionais de cada servidor, conselheiro, segurado, estagiário ou prestador de serviços do IPREMISA, sendo que:

- a) Os servidores devem assumir uma postura proativa no que diz respeito à proteção das informações do **IPREMISA** e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido a sistemas de informação sob responsabilidade do **IPREMISA**;
- b) As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções;
- c) Assuntos confidenciais não devem ser expostos publicamente;
- d) Senhas, chaves, token e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;
- e) Somente softwares homologados podem ser utilizados no ambiente computacional do **IPREMISA**;
- f) Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;

- g)** Todo usuário, para poder acessar dados da rede de computadores do IPREMISA, deverá possuir um código de acesso atrelado à uma senha previamente cadastrada, sendo este pessoal e intransferível, ficando vedada a utilização de códigos de acesso genéricos ou comunitários;
- h)** Não é permitido o compartilhamento de pastas nos computadores de servidores da instituição. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;
- i)** Todos os dados considerados como imprescindíveis aos objetivos do IPREMISA devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo estas cópias serem submetidos à testes periódicos de recuperação;

## 10 - PRIVACIDADE DA INFORMAÇÃO

Define-se como necessária a proteção da privacidade das informações, aquelas que pertencem aos seus segurados e que são manipuladas ou armazenadas nos meios às quais o IPREMISA detém total controle administrativo, físico, lógico e legal.

As diretivas abaixo refletem os valores institucionais do IPREMISA e reafirmam o seu compromisso com a melhoria contínua desse processo, em consonância com a Lei Geral de Proteção de Dados (LGPD):

- a)** As informações são coletadas de forma ética e legal, com o conhecimento do segurado, para propósitos específicos e devidamente informados;
- b)** As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado e específico;
- c)** As informações podem para fins específicos na prestação de serviços serem disponibilizadas as empresas contratadas, sendo exigido de tais organizações o cumprimento de nossa política e diretivas de segurança e privacidade de dados; Tais informações fornecidas por força de elaboração de trabalhos técnicos ou contida em banco de dados de sistemas de fornecedores são permanentemente proibidas de



serem repassadas a terceiros.

d) As informações somente são fornecidas a terceiros, mediante autorização prévia da superintendência para atendimento de exigência contratual;

e) As informações e dados constantes dos cadastros, bem como outras solicitações que venham garantir direitos legais só poderão ser fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos vigentes.

## 11 - TRANSFERÊNCIAS DE SERVIDORES

Quando houver na gestão de pessoal a movimentação de transferência de seção ou de setor de servidores, o responsável pelo setor na qual o servidor está lotado deverá comunicar o fato ao setor de Tecnologia da Informação, para que sejam realizadas as adequações necessárias para o acesso do referido servidor ao sistema informatizado do IPREMISA.

## 12 - CÓPIAS DE SEGURANÇA – BACKUP

Todas as cópias de segurança serão gerenciadas e executadas por sistemas de agendamento automatizado, para que sejam executadas diariamente após o horário de expediente.

O setor de Tecnologia da Informação será responsável pela gestão dos sistemas de backup e deverá realizar rotineiramente testes de restauração das cópias sejam elas físicas ou nas nuvens para certificar a integridade dos dados, proceder com pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, estatística de crescimento do uso dos dados entre outros.

As cópias (backup's) de segurança devem ser devidamente identificadas e datadas para o efetivo controle das mídias. O tempo de vida e uso das mídias de backup deve ser monitorado e controlado, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante. Recomenda que os testes de restauração (restore) de backup devem ser executados, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que

assim não sobreponha os arquivos válidos.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup. Recomenda-se que as mídias de backups históricos ou especiais deverão ser armazenadas sejam elas nas nuvens e ou fisicamente em instalações seguras.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios do IPREMISA, o setor de Tecnologia da Informação disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações salvas. Tais informações serão incluídas na rotina diária de backup.

### 13 - USO DO AMBIENTE WEB (Internet)

O acesso à Internet será autorizado para os usuários que necessitem da mesma para o desempenho das suas funções e atividades profissionais vinculadas ao IPREMISA. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o instituto não devem ser acessados. Não é permitido instalar programas provenientes da Internet nos microcomputadores do IPREMISA, sem expressa anuência do setor da área administrativa / tecnologia, mesmo os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais devem ser solicitados ao setor.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Não baixar e executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços. Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites tais como:

- De conteúdo pornográfico;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito;
- Que promovam a participação em salas de discussão de assuntos não relacionados institucionalmente ao IPREMISA;



- Que possibilitem a distribuição de informações de nível "Confidencial".
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

## 14 - USO DO CORREIO ELETRÔNICO – (E-mail)

O correio eletrônico fornecido pelo IPREMISA é um instrumento de comunicação interna e externa do instituto. As mensagens devem ser escrita com zelo profissional, não devem comprometer a imagem do IPREMISA, não podem ser contrárias à legislação vigente e nem aos princípios éticos e morais. O uso do correio eletrônico é pessoal e o usuário é responsável por todas as mensagens enviadas pelo seu endereço. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas e ao IPREMISA;
- Sejam hostis;
- Sejam relativas a "correntes", de conteúdos diversos;
- Possam prejudicar a imagem e a reputação do IPREMISA;
- Possam prejudicar a imagem de outras empresas ou órgãos públicos do município;
- Sejam incoerentes com as políticas do IPREMISA.

Para incluir um novo usuário no correio eletrônico, deverá fazer um pedido formal ao setor de Tecnologia da informação ou para o Gestor da Informação, que providenciará a inclusão do mesmo.

É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem do IPREMISA perante seus servidores e a comunidade em geral e que possam causar prejuízos à imagem institucional e financeira ao IPREMISA.

Evitar a utilização do e-mail institucional para assuntos pessoais.

Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para as atividades de negócio e podendo ser monitorado por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria.

Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de Tecnologia da Informação. Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/Symantec, solicitação de atualização de dados bancários, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, fakenews etc.

## 15 - SISTEMAS, APLICATIVOS E EQUIPAMENTOS DO IPREM.

O setor de Tecnologia da informação, por força de suas atribuições é responsável pela aplicação da Política de Segurança da Informação do IPREMISA e pela definição de configuração visando a aquisição e atualização de "software", "hardware" e dispositivos eletrônicos. Quando da necessidade de novas aquisições de programas ("softwares") ou de equipamentos de informática (hardware) deverá ser discutida com o responsável técnico pelo setor de Tecnologia da informação.

## 16 - USO DE COMPUTADORES E EQUIPAMENTOS DO IPREM

Os servidores que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade do IPREMISA, devem estar cientes de que:

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

### Os cuidados a serem observados:

#### **Ambiente Externo ao IPREMISA:**

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



### **Em caso de furto ou roubo**

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e ao setor de Tecnologia da informação;
- Envie uma cópia da ocorrência para ao setor da área (administrativa / tecnologia) do IPREMISA.

## **17 - PAPÉIS E RESPONSABILIDADES**

### **17.1. SERVIDORES, CONSELHEIROS, SEGURADOS, ESTAGIÁRIOS E PRESTADORES DE SERVIÇOS.**

Todo arquivo em mídia proveniente de entidade externa ao IPREMISA deve ser verificado por programa antivírus, bem como todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Tecnologia da informação, via rede. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

#### **Cabe a todos os servidores, estagiários e prestadores de serviços do IPREMISA cumprir com as seguintes obrigações:**

- a) Assinar o Termo de Responsabilidade e Sigilo da Informação;
- b) Assinar o Termo de Uso dos Sistemas de Informação;
- c) Zelar continuamente pela proteção das informações da instituição ou de seus segurados contra acesso, modificação, destruição ou divulgação não autorizada;
- d) Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades da Instituição;
- e) Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
- f) Comunicar imediatamente ao setor de Tecnologia da informação qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação; e
- g) A pessoa física ou entidade privada que, em razão de qualquer vínculo com o

IPREMISA, executar atividades de tratamento de informações sigilosas adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta Política de Segurança da Informação.

## 18 – DIRETOR SUPERINTENDENTE DO IPREMISA

### 18.1 - Cabe ao Diretor Superintendente:

- a) Aprovar a política e as normas de segurança da informação e suas revisões;
- b) Nomear o gestor da informação;
- c) Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação;
- d) Assegurar que todos possuam acesso e que tenham o entendimento desta política, das normas e dos procedimentos de Segurança da Informação;
- e) Controlar, zelar e manter o patrimônio do IPREMISA;
- f) Controlar e coordenar os atos administrativos e manter sob guarda e zelo o acervo documental e legal do IPREMISA, zelando pelos atos administrativos, previdenciários, contábeis e financeiros, garantindo o acesso às informações sobre funcionamento do IPREMISA, procedimentos e normas de direitos e obrigações aos conselheiros e demais interessados;
- g) Fazer a gestão dos documentos, bancos de dados e informações que deram suporte às avaliações atuariais do RPPS e aos demais estudos técnicos previstos na Portaria nº 464 de 19/11/18, visando atender a exigência para que deverão permanecer arquivados na unidade gestora do RPPS todo conjunto de informações à sua disposição pelo prazo de 10 (dez) anos;
- h) Manter a guarda e o controle de todos os arquivos gerados para o preenchimento de todos os demonstrativos que são exigidos para a alimentação dos sistemas gerenciais da SPREV, tais como: o Sistema de Informações Gerenciais dos



Regimes Próprios de Previdência Social (SIG- RPPS), o Cadastro Nacional de Informações Sociais (CNIS); Siprev Gestão; CADPREV WEB e CADPREV LOCAL e GESCON. Tais arquivos estão nos diversos formatos para atender as finalidades institucionais desta autarquia previdenciária;

i) Receber, por intermédio do responsável da área administrativa / tecnologia, relatórios de violações da política e das normas de segurança da informação, quando aplicáveis;

j) Tomar decisões referentes aos casos de descumprimento da política e das normas de segurança da informação, mediante a apresentação de propostas do setor de Tecnologia da informação; e

k) Garantir a manutenção e funcionamento dos equipamentos e instrumentos necessários ao funcionamento eficiente do IPREMISA;

## 19 - JURÍDICO

### 19.1 - Cabe, adicionalmente, ao setor Jurídico:

a) Incluir na análise e elaboração de contratos, obrigatoriamente, cláusulas específicas relacionadas à segurança da informação e a LGPD, com o objetivo de proteger os interesses do IPREMISA, em especial a devolução das informações e do banco de dados que povoam o sistema de gestão quando da finalização de contrato com prestadoras de serviços;

b) Manter o Diretor Superintendente do IPREMISA informado sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo a gestão de segurança da informação;

c) Avaliar, quando solicitado, a política, as normas e procedimentos de segurança da informação;

d) Redigir e detalhar, técnica e operacionalmente, as normas e procedimentos de segurança da informação relacionados à sua área, quando solicitado pela superintendência.

## 20 - GESTOR DA INFORMAÇÃO

O Gestor da Informação, designado pelo Diretor Superintendente como responsável por determinado ativo de informação. Este gestor deve dominar todas as regras de negócio necessárias à criação, manutenção e atualização de medidas de segurança relacionadas ao ativo de informação sob sua responsabilidade, seja este de propriedade do IPREMISA.

O Gestor da Informação mesmo delegando a sua autoridade sobre o ativo de informação, continua sendo dele a responsabilidade final pela sua proteção.

### 20.1 - Compete ao Gestor da Informação:

a) Classificar a informação sob sua responsabilidade, inclusive aquela gerada por servidores, fornecedores ou outras entidades externas, que devem participar do processo de definição do nível de sigilo da informação;

b) Inventariar todos os ativos de informação sob sua responsabilidade;

c) Enviar ao Diretor Superintendente, quando solicitado, relatórios sobre as informações e ativos de informação sob sua responsabilidade. Os modelos de relatórios serão definidos pelo responsável da área (administrativa / tecnologia) e aprovados pela Superintendencia;

d) Sugerir procedimentos para proteger os ativos de informação, conforme a classificação realizada, além da estabelecida pela Política de Segurança da Informação e pelas Normas de Segurança da Informação;

e) Manter um controle efetivo do acesso à informação, estabelecendo, documentando e fiscalizando a política de acesso à mesma. Tal política deve definir quais usuários ou grupos de usuários têm real necessidade de acesso à informação, identificando os perfis de acesso;

f) Reavaliar, periodicamente, as autorizações dos usuários que acessam as



informações sob sua responsabilidade, solicitando o cancelamento do acesso dos usuários que não tenham mais necessidade de acessar a informação;

g) Participar da investigação dos incidentes de segurança relacionados às informações sob sua responsabilidade.

## 21 – AUDITORIA

Todo ativo de informação sob responsabilidade do setor de Tecnologia da Informação é passível de auditoria em data e horários determinados pelo Diretor Superintendente, podendo esta, também, ocorrer sem aviso prévio.

A realização de uma auditoria deverá ser obrigatoriamente aprovada pela Superintendência e, durante a sua execução, deverão ser resguardados os direitos quanto a privacidade de informações pessoais, desde que estas não estejam dispostas em ambiente físico ou lógico de propriedade do IPREMISA.

Com o objetivo de detectar atividades anômalas de processamento da informação e violações da política, das normas ou dos procedimentos de segurança da informação, o setor de Tecnologia da Informação ou o Gestor da Informação poderá realizar monitoramento e controle proativos, mantendo a confidencialidade do processo e das informações obtidas.

Em ambos os casos, as informações obtidas poderão servir como indício ou evidência em processo administrativo e/ou legal.

## 22 - VIOLAÇÕES E SANÇÕES

### 22.1 - VIOLAÇÕES

São consideradas violações à política, às normas ou aos procedimentos de segurança da informação as seguintes situações, não se limitando às mesmas:

a) Quaisquer ações ou situações que possam expor o IPREMISA ou seus segurados

à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;

b) Utilização indevida de dados da Instituição, divulgação não autorizada de informações, sem a permissão expressa do Gestor da Informação;

c) Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação do IPREMISA ou de seus segurados;

d) A não comunicação imediata à área de Gerência da Informação de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação, que porventura um servidor, segurado, estagiário ou prestador de serviços venha a tomar conhecimento ou chegue a presenciar.

## 22.2 – SANÇÕES

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à política de segurança da informação do IPREMISA são consideradas faltas graves, podendo ser aplicadas penalidades previstas em lei.

## 23 - LEGISLAÇÃO APLICÁVEL

- Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);
- Lei Federal nº 8.159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);
- Lei Federal 10.406, de 10 de janeiro de 2002 (Institui o Código Civil);
- Lei Federal 9.983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências);
- Lei Federal nº 12.527, de 18 de novembro de 2011. (Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37



e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências);

- Lei nº 9.717, de 27 de novembro de 1998, que dispõe sobre regras gerais para a organização e o funcionamento dos regimes próprios de previdência social dos servidores públicos da União, dos Estados, do Distrito Federal e dos Municípios, dos militares dos Estados e do Distrito Federal e dá outras providências;
- Portaria SPREV Nº 3.030, de 15 de Março de 2021, Altera disposições da Portaria SPREV nº 03, de 31 de janeiro de 2018 e Aprova a Versão 3.2 do Manual do Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios - Pró-Gestão RPPS (Processo nº 10133.101343/2019-57).
- Lei Nº 13.709/2018, de 14 de agosto de 2018, já está em vigor desde 18 de setembro é a 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;
- LEI COMPLEMENTAR Nº 1/1993 - "Dispõe sobre o "Regime Jurídico Único" dos Servidores Públicos do Município, das Autarquias e das Funções Municipais;"
- LEI COMPLEMENTAR Nº 7/1993 - Estabelece o Regime de Concessão de Benefícios Previdenciários aos Servidores Públicos Municipais e dá outras providências;
- LEI COMPLEMENTAR Nº 043, DE 7 DE NOVEMBRO DE 2001 - Dispõe sobre o Sistema de Previdência Municipal, do Município de Ilha Solteira, do Estado de São Paulo, reformula o Instituto de Previdência e Benefícios dos Servidores Públicos do Município de Ilha Solteira, adequando-o à Legislação Federal e adota outras providências;

- RESOLUÇÃO N° 01, DE 28 DE JUNHO DE 2019 - Dispõe sobre o sistema de registro eletrônico de ponto com identificação biométrica nas dependências do IPREMISA; e
- PORTARIA N° 01, DE 13 DE SETEMBRO 2021 - Dispõe sobre normas de funcionamento no âmbito do Instituto de Previdência Municipal de Ilha Solteira - IPREMISA, e dá outras providências.



## ANEXO I

### Termo de Responsabilidade e Sigilo da Informação

Nos termos da Política de Segurança da Informação do **IPREMISA – INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE ILHA SOLTEIRA**, declaro que tenho pleno conhecimento de minhas responsabilidades no que concerne ao sigilo que deve ser mantido em relação aos ativos e informações sigilosas das quais eu tenha tido acesso ou possa vir a acessar ou ter conhecimento, em decorrência das atividades funcionais desempenhadas no exercício do cargo, função ou da prestação de serviço no âmbito do IPREMISA, ou fora do ambiente do mesmo.

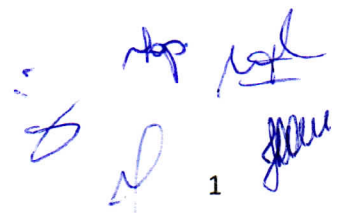
Comprometo-me a guardar o sigilo necessário a que sou obrigado, estando ciente das penalidades nos termos da legislação vigente, especialmente dos art. 153 e art. 325 do Código Penal (Decreto-lei nº 2.848, de 07 de dezembro de 1940) e demais legislações constantes do verso deste anexo I, bem como de quaisquer sanções administrativas que poderão advir.

A vigência da obrigação de sigilo, assumida pela minha pessoa por meio deste termo, terá validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa ou entidade, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste termo.

#### **Neste Termo, as seguintes expressões serão assim definidas:**

**Informação Sigilosa** significará toda informação, apresentada sob forma escrita, verbal ou por quaisquer outros meios, que possui restrição de acesso público em razão de sua criticidade para a segurança do IPREMISA, da sociedade e do município de Ilha Solteira.

**Informação sigilosa inclui**, mas não se limita à informação relativa às operações, processos, planos ou intenções, informações sobre produção, instalações, equipamentos, sistemas, dados, habilidades especializadas, projetos, métodos e metodologia, fluxogramas, especializações, componentes, fórmulas, produtos e questões relativas ao desempenho das atividades laborais.



## COMPROMISSO LEGAL

### CÓDIGO PENAL BRASILEIRO ESTATUTO DOS SERVIDORES PÚBLICOS MUNICIPAIS

#### 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 - detenção, de 3 (três) meses a 1 (um) ano, e multa (Lei 12.737/2012).*

**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.*

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



## **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.*

**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.*

**§ 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 à 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.

*Handwritten marks: a stylized 'S' and a '4'.*

*Handwritten signatures and initials in blue ink.*

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

*§ 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.*

*§ 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.*

## **ESTATUTO DOS SERVIDORES PÚBLICOS MUNICIPAL DO MUNICÍPIO DA ILHA SOLTEIRA**

(...)

**“Art. 148. São deveres do servidor:**

*I - I - exercer com zelo e dedicação as atribuições de cargo;*

*II - ser leal às atribuições a que servir;*

*III - observar as normas legais e regulamentares;*

*IV - cumprir as ordens superiores, exceto quando manifestamente ilegais;*

*V - atender com presteza:*

*a) ao público em geral, prestado as informações requeridas, ressalvadas as protegidas por sigilo;*

*b) à expedição de certidões requeridas para defesa de direito ou esclarecimento de situação de interesse pessoal;*

*c) às requisições para a defesa da Fazenda Pública.*

*VI - levar ao conhecimento da autoridade as irregularidades de que tiver ciência em razão do cargo;*

*VII - zelar pela economia do material e a conservação do Patrimônio Público.*

*[Handwritten signatures and initials]*



VIII - guardar sigilo sobre assunto de repartição;

IX - manter conduta compatível com a moralidade administrativa;

X - ser assíduo e pontual ao serviço;

XI - representar contra ilegalidade, omissão ou abuso do poder;

XII - tratar com urbanidade as pessoas.

Parágrafo único. A representação de que trata o Inciso XII será encaminhada pela via hierárquica e apreciada pela autoridade superior àquela contra a qual é formulada, assegurando-se representado o direito de defesa."

(...)

## **"Capítulo II DAS PROIBIÇÕES**

### **Art. 149 Ao servidor é proibido:**

I - ausentar-se do serviço durante o expediente, sem prévia autorização do chefe imediato;

II - retirar, sem prévia anuência da autoridade competente, qualquer documento ou objeto da repartição;

III - recusar fé a documento públicos;

IV - opor resistência injustificada ao andamento do documentos e processos ou execução de serviço;

V - promover manifestação de apreço ou desapreço no recinto da repartição;

VI - cometer a pessoa estranha à repartição, fora dos casos previstos em lei, o desempenho de atribuição que seja de sua responsabilidade ou de seu subordinado;

4

5

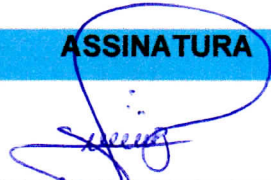
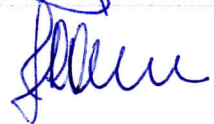


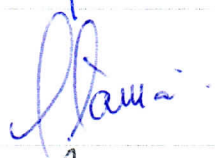
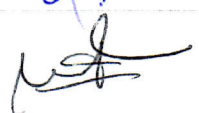
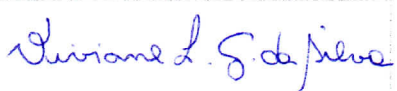
- VII - coagir ou aliciar subordinados no sentido de filiarem-se a associação profissional ou sindical ou a partido político;
- VIII - manter sob sua chefia imediata, em cargo ou função de confiança, cônjuge, companheiro ou parente até o segundo grau civil;
- IX - valer-se do cargo para lograr proveito pessoal ou de outrem, em detrimento da dignidade da função pública;
- X - participar de gerência ou administração de empresa privada, de sociedade civil, ou exercer o comércio, exceto na qualidade de acionista, ou comanditário;
- XI - atuar, como procurador ou intermediário, junto as repartições públicas, salvo quando se tratar de benefícios previdenciários ou assistenciais de parentes até o segundo grau, e de cônjuge ou companheiro;
- XII - receber propina, comissão, presente ou vantagem de qualquer espécie, em razão de suas atribuições;
- XIII - aceitar comissão, emprego ou pensão de estado estrangeiro;
- XIV - praticar usura sob qualquer de suas formas;
- XV - proceder de forma desidiosa;
- XVI - utilizar pessoal ou recursos materiais de repartição em serviços ou atividades particulares;
- XVII - cometer a outro servidor atribuições estranhas ao cargo que ocupa, exceto em situações de emergência e transitórias;
- XVIII - exercer quaisquer atividades que sejam incompatíveis com o exercício do cargo ou função e com o horário de trabalho;
- XIX - residir fora do município, se servidor efetivo, após o período probatório."

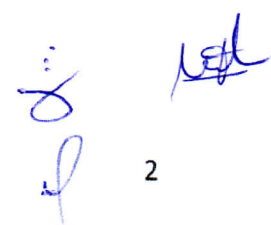
2  
4

6



### RELAÇÃO DE SERVIDORES DO IPREMISA:

MATRÍCULA	NOME COPLETO	DATA	ASSINATURA
100052	LUIZ FRANCISCO ZOGHEIB FERNANDES	25/10/2021	
3391	JACKELINE ROCHA DE OLIVEIRA	25/10/2021	
100021	ANA PAULA DE AVILA	25/10/2021	
100001	WOLFGANG VELOZO WAESSMAN	25/10/2021	
100011	FLAVIA LEATI PELAES DE ALMEIDA	25/10/2021	
100031	JOAO MANUEL DE QUEIROZ	25/10/2021	
100041	VIVIANE LUCIZANO GARCIA DA SILVA	25/10/2021	



## ANEXO II

### TERMO DE USO DOS SISTEMAS DE INFORMAÇÃO DO IPREMISA

**CONSIDERANDO** que o IPREMISA – INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE ILHA SOLTEIRA:

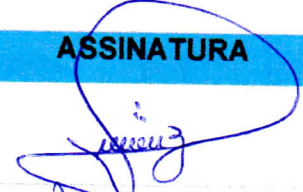
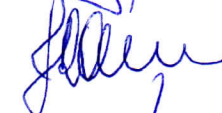


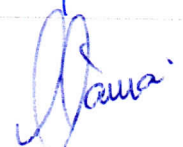

- a) Disponibiliza a infraestrutura tecnológica, como ferramenta de trabalho para o pleno desenvolvimento das atividades profissionais;
- b) Detém a exclusiva propriedade da infraestrutura tecnológica disponibilizada;
- c) Torna explícito que não há expectativa de privacidade sobre os ativos, informações e recursos institucionais, tendo em vista que os mesmos são destinados para fins profissionais e;
- d) Podendo haver prejuízos pela má utilização dos recursos disponibilizados;

**DECLARO** estar ciente e ter pleno conhecimento:

- a) Da Política de Segurança da Informação – PSI apresentada e disponibilizada de inteiro teor no pelo IPREMISA seja no sitio institucional e ou impressa;
- b) Da realização do monitoramento dos recursos tecnológicos disponibilizados, indispensável para a manutenção do nível de segurança adequado desta Autarquia Previdenciária;
- c) Que o IPREMISA – INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE ILHA SOLTEIRA pode realizar auditoria interna sobre os recursos de hardware e software disponibilizados para as atividades profissionais e;
- d) Que o descumprimento desta Política de Segurança da Informação está sujeito às sanções previstas no Estatuto dos Servidores Públicos do Município de Ilha Solteira, 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.



## RELAÇÃO DE SERVIDORES DO IPREMISA:

MATRÍCULA	NOME COPLETO	DATA	ASSINATURA
100052	LUIZ FRANCISCO ZOGHEIB FERNANDES	25/10/2021	
3391	JACKELINE ROCHA DE OLIVEIRA	25/10/2021	
100021	ANA PAULA DE AVILA	25/10/2021	
100001	WOLFGANG VELOZO WAESSMAN	25/10/2021	
100011	FLAVIA LEATI PELAES DE ALMEIDA	25/10/2021	
100031	JOAO MANUEL DE QUEIROZ	25/10/2021	
100041	VIVIANE LUCIZANO GARCIA DA SILVA	25/10/2021	