SUMÁRIO

DAS ATUALIZAÇÕES

Atualizações feitas nesta versão:

- Retirada a necessidade da nomeação do Gestor de Segurança da Informação e Comunicações e do Comitê de Segurança da Informação e Comunicações do artigo 10;
- Acrescentado as informações (servidores efetivos e comissionados) informações ao artigo 36;
- Alterada a informação sobre contratados no artigo 38;
- Acrescentado as informações sobre bloqueio de websites no item V do artigo 47;
- Retirada a indicação de necessidade sobre atualização a cada 12(doze) meses desta POSIC.

Atualizações feitas na versão de 2022:

- Adicionado o Sumário do documento;
- Adicionado artigo referente ao tratamento de dados segundo a LGPD;
- Alterado artigo referente a nomeação de Gestor de Segurança da Informação;
- Adicionado artigo referente ao uso de backups;
- Adicionado artigo referente ao uso de antivírus;
- Adicionado artigo referente a senhas de administrador;
- Adicionado artigo referente ao acesso ao Data Center;
- Adicionado artigo referente a criação de senhas individuais;
- Adicionado artigo referente ao uso de crachás pelos funcionários;
- Adicionado artigo referente a perda ou furtos de equipamentos do Instituto;
- Adicionado artigo referente ao acompanhamento de visitantes ao Instituto;
- Adicionado o Link de acesso a POSIC;
- Adicionado ANEXO com o TERMO DE CONFIDENCIALIDADE.

Instrução Normativa nº 01/2024

Dispõe sobre a revisão da Política de Segurança da Informação e das Comunicações - POSIC do IPREM.

O Diretor-Presidente do IPREM, Daniel Ribeiro Vieira, usando das atribuições que lhe são conferidas pela Lei 4.643/2007,

Considerando o art. 41 da Instrução Normativa nº 02/2019, de 11 de janeiro de 2020, que prevê que a Política de Segurança da Informação e das Comunicações – POSIC, do Instituto de Previdência Municipal de Pouso Alegre, será revisada e atualizada quando identificada necessidade,

RESOLVE:

Art. 1º Instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a integridade, confidencialidade, disponibilidade e autenticidade das informações custodiadas e de propriedade do Instituto, de modo a preservar seus ativos e sua imagem institucional.

Art. 2º Trata-se do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito do Instituto, em todo o seu ciclo de vida - criação, manuseio, divulgação, armazenamento, transporte e destinação final, visando à continuidade de seus processos críticos, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 3º Aplica-se a todas as unidades da estrutura regimental do Instituto, podendo ser estendida às demais unidades eventualmente por ele atendidas.

Política de Segurança da Informação e das Comunicações – POSIC

CAPÍTULO I
DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para efeitos desta POSIC, entende-se por:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - agente público: todo aquele que exerce cargo, emprego ou função no Instituto, ainda que transitoriamente, com ou sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de vínculo (servidores públicos, militares, servidores temporários regidos pela Lei nº 8.745, de 9 de dezembro de 1993 e colaboradores);

III - ameaça: conjunto de fatores externos, internos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

IV - assinatura eletrônica: geração, por computador, de qualquer símbolo ou série de símbolos executados, adotados ou autorizados legalmente equivalentes à assinatura manual do indivíduo;

V - ativo classificado: ativo de informação com informação classificada como sigilosa;

VI - 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. Inclui meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VII - ativo sob restrição de acesso: ativo de informação com informação institucional não pública ou com informação de acesso transitoriamente restrito;

VIII - auditabilidade: atributo que garante a rastreabilidade dos diversos passos de um processo informatizado, identificando os participantes, ações e horários de cada etapa;

IX - auditoria: atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais, com o intuito de verificar sua conformidade com os objetivos e políticas institucionais, orçamentos, regras, normas e padrões;

X - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

XI - classificação: grau de sigilo atribuído por autoridade competente a dados, informações, documentos, materiais, áreas ou instalações;

XII - colaborador: pessoa jurídica ou pessoa física que desempenhe atividade de interesse do Instituto, realize estágio ou preste serviço, em caráter permanente ou eventual;

XIII - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, jurídica, sistema, órgão ou entidade não autorizado e credenciado, observada a disposição do inciso X do art. 5º da Constituição Federal e as disposições da Lei 12.527/2011;

XIV - continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos de informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

XV - custodiante do ativo de informação: aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

XVI - desastre: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

XVII - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

XVIII - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

XIX - documento classificado: documento com informação classificada como sigilosa;

XX - Gestão da Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, prevenção, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto à tecnologia da informação e comunicações;

XXI - Gestor de Segurança da Informação e Comunicações: servidor responsável pelas ações de segurança da informação e comunicações;

XXII - Gestor do Ativo de Informação: autoridade legal responsável pela concessão de acesso a terceiros (pode ser a autoridade marcadora, a autoridade classificadora ou a autoridade instituidora do processo);

XXIII - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXIV - informações institucionais públicas: informações geradas ou custodiadas pelo Instituto ou por seus colaboradores, no exercício de suas funções, às quais o acesso será permitido, observando-se eventual restrição temporária. Dividem-se em:

a) **de acesso ostensivo:** aquelas que não estão sujeitas a nenhuma restrição de acesso;

b) **de acesso transitoriamente restrito:** aquelas referentes a documentos utilizados como fundamento de decisões e atos administrativos, às quais o acesso será franqueado após a edição do correspondente ato decisório, conforme previsto no parágrafo 3º do art. 7º da Lei nº 12.527, de 18 de novembro de 2011, salvo se forem, posteriormente, objeto de classificação como sigilosas.

XXV - informações institucionais não públicas: informações geradas ou custodiadas pelo ou por seus colaboradores, no exercício de suas funções, sujeitas a restrição de acesso. Dividem-se em:

a) **informações pessoais:** aquelas relacionadas à pessoa natural identificada ou identificável e que diga respeito à sua intimidade, vida privada, honra e imagem, cujo tratamento é regulado pelo art. 31 da Lei nº 12.527, de 18 de novembro de 2011;

b) **informações sujeitas a outros tipos de sigilo:** aquelas sob segredo de justiça ou protegidas por sigilo comercial, bancário, fiscal, industrial ou outros, na forma da legislação vigente, conforme o disposto no art. 22 da Lei nº 12.527, de 18 de novembro de 2011;

c) **informação classificada:** informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada;

d) **registros:** informações contidas em anotações, levantamentos e análises preliminares, ou seja, aquelas de produção e guarda dos agentes públicos no exercício de suas funções, e que não integrem processo ou expediente que subsidie decisão administrativa editada.

XXVI - informação sob restrição de acesso: informação institucional não pública ou informação de acesso transitoriamente restrito;

XXVII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

XXVIII - legalidade: atributo que garante a legalidade jurídica da informação, assegurando que todos os seus dados estão de acordo com as cláusulas contratuais pactuadas ou com a legislação vigente;

XXIX - não repúdio: propriedade da informação que não possa ter seu envio ou conteúdo contestados, rejeitados ou repudiados por seu emissor ou por seu receptor;

XXX - Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável pelo órgão com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

XXXI - princípios: são idéias centrais que estabelecem diretrizes a um dado sistema, conferindo-lhe um sentido lógico, harmonioso e racional;

XXXII - privacidade: propriedade da informação privada que só possa ser acessada por terceiros com conhecimento e autorização prévios das pessoas de que ela trata;

XXXIII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXXIV - recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XXXV - recursos de tecnologia da informação: servidores de rede, estações de trabalho, equipamentos de conectividade, todo e qualquer hardware e software que compõem soluções e aplicações de Tecnologia da Informação;

XXXVI - segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXXVII - tratamento da informação: conjunto de ações referentes à produção, classificação, utilização, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

XXXVIII - usuário: agente público, auditores e quaisquer outros entes que podem acessar ativos de informação do Instituto, mediante autorização de um gestor de ativo de informação;

XXXIX - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO II
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 5º Esta POSIC observa a legislação vigente e normas específicas, destacando-se:

I - Leis Federais, Estaduais e Municipais;

II - Acórdãos do TCU;

III - Instruções Normativas e Normas Complementares aprovadas pelo CGSI/PR;

IV - Normas ABNT;

V - Lei 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD) e

VI - Código de Ética do IPREM

CAPÍTULO III
DOS PRINCÍPIOS

Art. 6º As ações de Segurança da Informação e Comunicações são norteadas pelos seguintes princípios:

I - Alinhamento Estratégico: deve haver um alinhamento entre a POSIC e a missão institucional e seu planejamento estratégico;

II - Propriedade da informação: toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IPREM é considerada seu patrimônio e deve ser protegida conforme normas em vigor;

III - Responsabilidade: os agentes públicos devem conhecer e respeitar a POSIC;

IV - Ética: os direitos dos agentes públicos devem ser preservados, sem o comprometimento da segurança da informação e comunicações;

V - Celeridade: as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas de segurança;

VI - Clareza: as regras de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;

VII - Privacidade: informação que fira o respeito à intimidade e à honra dos cidadãos não pode ser divulgada;

VIII - Publicidade: dar transparência no trato da informação, observados os critérios legais;

IX - Domínio: É vedado o domínio exclusivo, por apenas um colaborador, de um processo de negócio ou recurso; e

X - Serão observados ainda, sem prejuízo das demais, outros princípios constitucionais que regem a Administração Pública Municipal.

CAPÍTULO IV
DA CONFIDENCIALIDADE DAS INFORMAÇÕES

Art. 7º A confidencialidade deve-se restringir às hipóteses constitucionais em que resguardam a intimidade da pessoa e segurança institucional.

Art. 8º A confidencialidade de informações dispostas nesta POSIC não poderá comprometer a transparência contemplada no Plano de Ações vigente e deverá seguir os conceitos de dados pessoais, sensíveis e anonimizados da LGPD.

CAPÍTULO V
DAS DIRETRIZES GERAIS

Seção I

Da Gestão da Segurança da Informação e Comunicações

Art. 9º A gestão da segurança da informação e comunicações compreende a preservação dos ativos do Instituto, quanto aos aspectos de confidencialidade, integridade, disponibilidade e autenticidade, independentemente do meio que se encontrem.

Art. 10 De forma a promover a gestão e fomentar os aspectos de segurança da informação, o Instituto deve:

I - Instituir uma estrutura para a gestão de segurança da informação e comunicações;

II - Nomear o **Encarregado pelo Tratamento de Dados Pessoais**;

III - Instituir normas e procedimentos que garantam a segurança da informação em ambientes de computação móvel, computação na nuvem e de trabalho remoto;

IV - Instituir normas e procedimentos que estabeleçam critérios de acesso e uso de internet, redes sociais, sistemas corporativos, banco de dados, rede de comunicações, uso de dispositivos de armazenamento (pendrive, cartões de memória, discos rígidos externos e dispositivos similares);

V - Instituir normas e procedimentos que estabeleçam a Gestão de Continuidade do Negócio para minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre os serviços sob responsabilidade do Instituto; e

VI - Resguardar todo ativo de informação contra acesso e manipulação indevidos.

Seção II

Do Tratamento da Informação

Art. 11 Toda informação criada, adquirida ou custodiada pelo agente público, no exercício de suas atividades para o Instituto, é considerada um bem e deve estar protegida de acordo com as regulamentações de segurança existentes.

Art. 12 As informações devem ser protegidas de acordo com as diretrizes descritas nesta POSIC e demais regulamentações em vigor.

Art. 13 As informações do Instituto produzidas ou custodiadas pelo Setor de Comunicações e Tecnologia devem ter destinação final, conforme o seu nível de classificação.

Art. 14 Backups: É de responsabilidade do setor de Suporte da área de T.I, realizar backups (cópias) das áreas de armazenamento dos Servidores da empresa, em rotinas diárias, mensais e eventuais, de acordo com o Plano de Backups documentado no T.I, bem como manter atualizado o documento de teste de restore localizado no departamento.

Art. 15 Antivírus: Todas as máquinas devem possuir o Windows Defender e Antimalware ativos no Windows 10/11.

Art.16 As senhas de administrador dos sistemas e equipamentos devem ser de acesso restrito ao setor de T.I do Instituto, devendo uma cópia em envelope selado e rubricado ser entregue à Diretor-Presidente para que fique em posse e tenha acesso em caso de perda ou requerida judicialmente.

Parágrafo único. Sempre que o envelope for aberto as senhas devem ser trocadas e feito novo envelope.

Seção III

Da Relação com Terceiros

Art. 17 As particularidades das relações com terceiros deverão ser definidas em norma interna específica.

Seção IV

Da Classificação da Informação

Art. 18 As informações custodiadas ou de propriedade do Instituto devem ser classificadas quanto aos aspectos de sigilo, disponibilidade e integridade de forma implícita ou explícita e receber o nível de proteção condizente com sua classificação, conforme normas e legislação específica em vigor.

Art. 19 O gestor da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade.

Art. 20 A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte.

Art. 21 Todo agente público deve ser capaz de identificar a classificação atribuída a uma informação custodiada ou de propriedade do Instituto e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

Seção V

Da Sensibilização, Conscientização e Capacitação

Art. 22 Deve ser adotado processo permanente de divulgação, sensibilização, conscientização e capacitação dos agentes públicos sobre os cuidados e deveres relacionados à segurança da informação e comunicações.

Seção VI

Da Gestão de Riscos

Art. 23 Deve ser adotado processo contínuo de gestão de riscos, o qual será aplicado na implantação e operação da gestão de segurança da informação e comunicações.

Seção VII

Da Gestão de Continuidade

Art. 24 Deve ser adotado processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

Art. 25 As ações de continuidade devem ser observadas por todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional.

Art. 26 As informações de propriedade ou custodiadas pelo Instituto, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança de forma a garantir a continuidade das atividades do Instituto.

Parágrafo único. As informações armazenadas em outros meios devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

Seção VIII

Do Tratamento de Incidentes de Rede Computacional

Art. 27 O setor de T.I tem a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

Parágrafo único. Os acidentes considerados graves pelo setor de T.I deverão ser reportados à Diretoria de Administração que decidirá as devidas providências.

Seção IX

Do Uso de Recursos Computacionais e de Comunicações

Art. 28 O uso de recursos computacionais e de comunicações do Instituto, pelos agentes públicos, deve ser direcionado prioritariamente para realização das atividades profissionais desempenhadas para o Instituto nos limites dos princípios da ética, razoabilidade e legalidade.

§ 1º A área de tecnologia do Instituto poderá monitorar o acesso à internet e restringir acesso aos sítios que possam oferecer riscos à segurança da rede ou ao ambiente computacional.

§ 2º Só poderão ser utilizados no ambiente computacional softwares homologados ou autorizados pela área de tecnologia do Instituto.

§ 3º Não devem ser permitidos usuários com privilégios de administrador de sistema operacional nos computadores do Instituto, exceto os do setor de T.I.

§ 4º O uso do Internet banking tanto pelo navegador web quanto pelo aplicativo para celular deve seguir as normas de segurança instituídas pelas instituições financeiras.

Seção X

Da Auditoria e Conformidade

Art. 29 Devem ser criados e mantidos registros e procedimentos, como trilhas de auditoria que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos e rede interna do Instituto.

Art. 30 Periodicamente deve-se promover verificação de conformidade às regulamentações de segurança e legislações em vigor.

Seção XI

Dos Controles de Acesso

Art. 31 Devem ser sistematizados procedimentos para a concessão de acesso como forma de evitar a quebra de segurança da informação e comunicações.

Art. 32 Devem ser implementados mecanismos de controle de acesso como consequência do processo de gestão de riscos de segurança da informação e comunicações.

Art. 33 O acesso às informações custodiadas ou de propriedade do Instituto pelos agentes públicos deve ser restrito ao necessário para desempenho de suas funções.

Art. 34 O acesso à sala do Data Center deverá ser controlado e restrito aos servidores do T.I ou em acompanhamento dos mesmos.

Art. 35 As senhas de acesso aos sistemas e equipamentos do Instituto deverão ser pessoais e intransferíveis e deverão ser bloqueadas em caso de desligamento do servidor ou agente público.

Art. 36 Os funcionários(servidores efetivos e comissionados) deverão utilizar crachá de identificação em todo o período que se encontrarem nas dependências do Instituto.

Art. 37 Os visitantes deverão estar sempre acompanhados por um servidor do Instituto, que será o responsável por guiá-los durante todo o período que se encontrarem nas dependências do Instituto.

Art. 38 Os contratados deverão estar devidamente uniformizados e identificados com crachá contendo nome, função e horário de trabalho. Os mesmos não poderão permanecer nas dependências do Instituto sem a presença do encarregado que deverá preencher termo de responsabilidade.

Parágrafo único. Não será permitida a circulação de pessoas não autorizadas nas dependências do Instituto, salvo na recepção para obter informações presencialmente.

CAPÍTULO VI
DAS PENALIDADES

Art. 39 Ações que violem a política de segurança da informação e comunicação poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

CAPÍTULO VII
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 40 É dever do agente público do Instituto conhecer e zelar pelo cumprimento desta norma.

Art. 41 Os agentes públicos são responsáveis pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações, tais como: crachá, login, senha eletrônica, certificado digital, cópia de segurança dos arquivos pessoais e endereço de correio eletrônico.

Parágrafo único. A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o seu reconhecimento.

Art. 42 Independentemente da adoção de outras medidas, o titular da unidade administrativa deverá, de imediato, comunicar todo incidente de segurança que ocorra no âmbito de suas atividades ao gestor de segurança da informação e comunicações.

Art. 43 No caso de incidente na rede do Instituto, o setor de T.I. deve ser comunicado.

Art. 44 No caso de perda ou furto de equipamentos, o responsável deve registrar o Boletim de Ocorrência junto à Autoridade Policial e comunicar de imediato a Diretoria do IPREM.

Art. 45 Sempre que necessário, o gestor da informação providenciará autorização relativa à cessão de direitos sobre as informações de terceiros, antes de utilizá-las.

Art. 46 A cessão de informações do Instituto a terceiros deverá ser submetida previamente à autorização do gestor da informação.

Art. 47º - O gestor de segurança da informação, com apoio da área de tecnologia, tem total autonomia para atuar sobre os recursos de TI do instituto, sem prévio aviso, para:

I - realizar auditoria (local ou remota);

II - redefinir perfis de usuários cujos privilégios possam levar à prática de atividades tidas como nocivas à rede ou ao ambiente computacional;

III - instalar softwares de monitoramento;

IV - desinstalar quaisquer softwares não homologados ou considerados nocivos à integridade da rede ou ao ambiente computacional;

V - bloquear websites que estejam em desacordo com a legislação vigente ou que o gestor considere impróprio ao ambiente de trabalho.

VI - credenciar/descredenciar usuários.

CAPÍTULO VIII
DA DIVULGAÇÃO

Art. 48 Após a publicação desta POSIC, ela deverá ser divulgada amplamente a todos os agentes públicos do Instituto, inclusive de forma permanente na página da intranet do Instituto através do link https://iprem.mg.gov.br/documents/POSIC.pdf

Parágrafo único. Todos os agentes públicos do Instituto deverão ler e assinar o Termo de Confidencialidade em anexo a esta POSIC.

CAPÍTULO IX
DA ATUALIZAÇÃO E VIGÊNCIA

Art. 49 Esta POSIC deverá ser revisada e atualizada quando identificada necessidade.

Art. 50 Revogadas as disposições em contrário.

Pouso Alegre, 11 de dezembro de 2024

Assinado por DANIEL RIBEIRO VIEIRA:***535496** Diretor Presidente ***.535.496-**

Daniel Ribeiro Vieira

DIRETOR-PRESIDENTE

ANEXO I
TERMO DE CONFIDENCIALIDADE

Declaro estar ciente e de acordo com a Política de Segurança de Informação e Comunicações (POSIC) do IPREM, disponível no endereço eletrônico https://iprem.mg.gov.br/documents/POSIC.pdf .

Comprometo-me a verificar futuras alterações da POSIC e comunicar o setor de T.I. do IPREM sobre qualquer ato que esteja em desacordo com esta norma e suas atualizações.

Declaro que as informações abaixo preenchidas por mim, são verdadeiras

[ ] Autorizo que atualizações da política sejam enviadas para o seguinte

e-mail: _____

ou número de whatsapp:_____

Pouso Alegre ____ de _____ de 202__

Nome:_____

CPF:_____