PORTARIA 003/2019

CRIA A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO PREVIDÊNCIA DO MUNICÍPIO DE TRÊS MARIAS - IPREM E DEFINE SUAS DIRETRIZES.

A Superintendente do Instituto de Previdência Municipal de Três Marias/MG - IPREM no uso de suas atribuições legais e de conformidade com o art. 22 da Lei Municipal n.º1.945 de 20 de dezembro de 2005 e do artigo 11 da lei 2.668/17 que dispõe sobre a Estrutura Organizacional do Instituto de Previdência Municipal de Três Marias – IPREM pela presente Portaria, com atribuições e responsabilidades da função:

CONSIDERANDO a necessidade de implantação de modelo de governança de Tecnologia da Informação (TI);

CONSIDERANDO a necessidade de estabelecer papéis e responsabilidades que permitam garantir aos Segurados, Beneficiários e Processos Administrativos Previdenciários deste Instituto dentro de um perfil de Confidencialidade, Integridade e Disponibilidade;

CONSIDERANDO que a área de Tecnologia da Informação caminha rumo à Governança de TI, visando se adequar às boas práticas do mercado, especialmente no campo previdenciário municipal próprio;

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações previdenciárias necessárias aos segurados, beneficiários e aos Processos Administrativos deste Instituto com integridade, confidencialidade e disponibilidade;

CONSIDERANDO a constante preocupação com a qualidade e celeridade na prestação de serviços previdenciários aos segurados e beneficiários deste Instituto;

R E S O L V E:

Criar a Política de Segurança da Informação do Instituto de Previdência do Município de Três Marias e suas diretrizes.

CAPÍTULO I
DAS DEFINIÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 1° Para fins deste ato considera-se:

I. **Confidencialidade:** garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;

II. **Integridade:** salvaguarda de exatidão da informação previdenciária e dos métodos de processamento;

III. **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação previdenciária e aos recursos correspondentes sempre que necessários;

IV. **Recursos de Tecnologia de Informação:** qualquer equipamento eletrônico, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, ou as instalações físicas que os abriguem;

V. **Usuários de Tecnologia de Informação:** servidores autárquicos e servidores municipais ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, bem como, estagiários, empresas terceirizadas ou outros que se encontrem a serviço do Instituto, utilizando, em caráter temporário, os recursos tecnológicos no âmbito da autarquia previdenciária municipal;

VI. **Ativos de Tecnologia de Informação**: qualquer mecanismo de software ou dispositivo de hardware que compõem a infraestrutura da tecnologia de informação do Instituto, utilizado como ferramenta de trabalho para o desempenho funcional dos seus servidores;

VII. **Segurança da Informação**: conjunto de medidas que tem como objetivo o estabelecimento dos controles necessários à proteção das informações durante sua criação, aquisição, uso, transporte, guarda e descarte, contra destruição, modificação, comercialização ou divulgação indevidas e acessos não autorizados, acidentais ou

intencionais, garantindo a continuidade dos serviços e a preservação de seus aspectos básicos de confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

CAPÍTULO II
DAS DIRETRIZES GERAIS

Art. 2º A Política de Segurança da Informação do IPREM obedecerá às seguintes diretrizes:

I. Estabelecer e promover ações para garantir a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações previdenciárias em meio computacional;

II. Mitigar os riscos associados à dependência da organização em relação ao uso massivo da TI previdenciária;

III. Definir as atribuições e responsabilidades relativas ao processo de estabelecer e promover a aplicação da Política de Segurança da Informação do IPREM.

IV. Os recursos de tecnologia da informação adquiridos pelo Instituto e disponibilizados na sua área de abrangência previdenciária, bem como as informações geradas, integram o patrimônio e destinam-se, exclusivamente, ao atendimento das necessidades do serviço autárquico municipal, cabendo ao seu usuário zelar pela conservação, dispensando-lhe, no uso diário, os cuidados que exigirem.

V. A área de Tecnologia da Informação já fornece identificação e senha de acesso inicial à rede corporativa, de uso pessoal e intransferível, cabendo ao usuário mantê-la em sigilo, sendo vedada a sua cessão ou empréstimo sob qualquer pretexto a terceira pessoa.

VI. A solicitação de identificação e senha de acesso inicial deverá ser feita pelo Superintendente, para onde o usuário está desempenhando suas atividades funcionais, por meio de formulário específico ou por e-mail.

VII. A senha de acesso inicial deverá ser alterada pelo usuário, quando este acessar pela primeira vez a rede corporativa municipal. Os atos decorrentes da utilização dos sistemas de informática, por meio de conta de acesso com identificação e senha, são de responsabilidade do usuário ao qual a conta está formalmente vinculada.

VIII. Após o término das atividades funcionais realizadas na estação de trabalho, o usuário deverá efetuar o encerramento da seção (logoff), evitando o acesso indevido por outro usuário e desligar os equipamentos que estavam em uso.

IX. Deverão ser implantadas políticas para criação, renovação, bloqueio e expiração de senhas, com o intuito de aumentar o nível de segurança da rede corporativa.

X. O privilégio de administrador na estação de trabalho somente será concedido ao técnico de informática do IPREM, que necessita de acesso privilegiado à estação somente para casos excepcionais. Nos demais casos fará o acesso via login no sistema.

XI. Os direitos de acesso serão concedidos de maneira seletiva, de acordo com a necessidade de cada unidade administrativa e com a atribuição referente ao cargo do usuário, mediante deferimento de perfis e níveis de acesso elaborados pela área de Tecnologia da Informação.

XII. Os direitos de acesso a cada recurso serão configurados pela área de Tecnologia da Informação, devendo ser observadas as necessidades do serviço, e poderão ser retirados ou restringidos por solicitação do Superintendente. A solicitação de acesso ao sistema de informação de uso da Autarquia Municipal somente poderá ser feita por escrito e deferida somente pelo Superintendente.

XIII. O acesso à internet dar-se-á, exclusivamente, por intermédio dos meios autorizados e configurados pela área de Tecnologia da Informação. Excetuando-se os casos previstos neste ato, o acesso à internet provido pela rede do Instituto deve restringir-se às páginas com conteúdo estritamente relacionado com as atividades desempenhadas pelo órgão.

XIV. Possuem acesso à internet os servidores contratados, cedidos e servidores de cargo em comissão em exercício e com identificação de acesso à rede do IPREM. Em casos excepcionais de serviços necessários, estagiários poderão ter acesso à internet durante o período de estágio, observando as disposições aqui enumeradas, desde que seja formalmente solicitado e justificado pelo responsável da unidade onde está sendo prestado o estágio, autorizado pela Superintendente.

CAPÍTULO III
DAS ATRIBUIÇÕES AOS USUÁRIOS DE TI

Art. 3º Constitui atribuições comuns aos usuários de TI do IPREM:

I. Cabe a todos os usuários de TI do IPREM observar e adotar as ações de Política de Segurança da Informação previdenciária municipal.

II. Os usuários de TI devem utilizar os recursos de Tecnologia da Informação, de propriedade do IPREM, somente para fins corporativos, no interesse da administração e para as tarefas a que se destinam.

III. É considerada imprópria a utilização destes recursos para propósitos particulares ou não autorizados.

IV. A capacitação deverá basear-se nas responsabilidades e papéis previstos na Política de Segurança da Informação, sem prejuízo de conteúdos que estejam fora do escopo da norma, mas podem contribuir para sua melhoria.

V. Adotar a Política de Segurança da Informação, seus normativos, alterações, atualizações e quaisquer ações decorrentes da aplicação das normas previstas serão comunicados aos usuários de TI através das ferramentas de correio eletrônico e site do IPREM.

VI. O usuário deve manter, sempre que possível cópia dos arquivos de trabalho nas unidades lógicas de armazenamentos de rede disponibilizadas pela área de Tecnologia da Informação.

VII. Cada usuário é responsável pela Segurança da Informação no Órgão e deve conhecer, entender e cumprir as diretrizes, normas, procedimentos e instruções integrantes da política de segurança da informação, zelando pela correta aplicação das medidas de proteção.

VIII. O usuário que apagar, destruir, modificar ou, de qualquer forma, inutilizar, total ou parcialmente, arquivo ou programa de computador, fizer uso, de forma indevida ou não autorizada, dos equipamentos de informática, bem como agir em desacordo com os termos deste ato, fica sujeito à aplicação das penalidades administrativas, civis e penais, se for o caso.

IX. O acesso ao ambiente físico da rede – servidores, cabos de rede, racks, switches, entre outros – é limitado aos técnicos da área de Tecnologia da Informação. Os casos omissos e as dúvidas surgidas na aplicação deste ato serão dirimidos pela Superintendente do IPREM.

CAPÍTULO IV
DAS VEDAÇÕES AOS USUÁRIOS DE TI

Art. 4º Constitui como vedação ao usuário da tecnologia da informação:

I. Utilizar mecanismos com o objetivo de descaracterizar o acesso indevido às páginas ou serviços proibidos neste documento;

II. Instalar em qualquer computador programas ou softwares que não tenham sido adquiridos pelo Instituto e homologados pela área de Tecnologia da Informação, com exceção daqueles que solicitados formalmente e homologados, bem como a adição ou a execução de qualquer documento, planilha ou arquivo alheios às atividades do IPREM;

III. Copiar programas de computador, licenças de software e sistemas implantados nas estações de trabalho, quer seja para uso externo, quer seja para uso em outra estação de trabalho na unidade do IPREM;

IV. Instalar quaisquer periféricos, componentes, placas de hardware que não tenham sido adquiridos pelo IPREM, exceto nos casos de comprovada necessidade e com acompanhamento de técnico qualificado da área de Tecnologia da Informação;

V. Utilizar microcomputadores particulares, portáteis ou não, na rede do IPREM, exceto em casos de comprovada necessidade, e mediante anuência da área de Tecnologia da Informação, que acompanhará para que sejam, obrigatoriamente, adotados os padrões de segurança estabelecidos pelo IPREM;

VI. Conectar equipamentos de rede sem fio, exceto os que forem homologados pela área de Tecnologia da Informação;

VII. Utilizar correios eletrônicos que não sejam homologados pela área de Tecnologia da Informação, ou utilizar mecanismos com o objetivo de descaracterizar o uso indevido do correio eletrônico;

VIII. Armazenar arquivos não relacionados com as atividades institucionais nas unidades de rede, tais como: músicas, vídeos e fotos e arquivos que não sejam correlacionados as atividades desenvolvidas;

IX. Compartilhar de recursos ou ativação de serviços de rede nas estações de trabalho, ou de qualquer outra ação que possa comprometer a segurança da rede corporativa.

CAPÍTULO V

DO USO DE SITES E E-MAIL CORPORATIVO

Art. 5º Constitui regras quanto a utilização de softwares e sites de navegação:

I. O acesso aos sítios e serviços que estejam enquadrados como uso indevido, mas que sejam necessários ao desempenho das atribuições funcionais do usuário, será liberado mediante autorização por escrito do Superintendente do IPREM;

II. Não constitui utilização indevida o acesso a sítios que possam ser úteis ao desenvolvimento das atividades funcionais do usuário, ou sítios bancários, sítios de notícias, sítios de pesquisa e busca;

III. A área de Tecnologia da Informação, sempre que possível, poderá registrar os endereços das páginas acessadas pelos usuários, e sendo comprovada a utilização indevida, o acesso à internet do usuário será bloqueado, e a chefia imediata será comunicada para as providências cabíveis.

IV. Os parâmetros de configuração dos computadores serão definidos pela área de Tecnologia da Informação, que levará em conta os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional do IPREM. Assim não será autorizada modificação efetuada em parâmetros diferentes das definições estabelecidas.

V. Os programas e sistemas utilizados pelo IPREM somente podem ser instalados nas estações de trabalho por pessoas autorizadas pela área de Tecnologia da Informação, podendo ser feita, inclusive, por meio de programas de gerenciamento remoto.

VI. O usuário deverá utilizar o correio eletrônico institucional para os objetivos e funções próprios e inerentes às suas atribuições funcionais. O usuário deverá manter a capacidade de armazenamento de sua caixa postal, eliminando as mensagens desnecessárias. Caso o usuário venha a receber mensagens externas de conteúdo não apropriado, deverá excluí-las no primeiro acesso à caixa postal após o recebimento das mesmas.

VII. Caracteriza-se uso inapropriado do serviço de Correio Eletrônico enviar mensagens contendo:

a. Texto obsceno, ilegal, antiético, preconceituoso ou discriminatório;
b. Conteúdo calunioso ou difamatório;
c. Vírus ou qualquer programa danoso;
d. Material de natureza político-partidária ou sindical ou material protegido por leis de propriedade intelectual;
e. Entretenimentos e correntes;
f. Assuntos ofensivos;
g. Imagens, áudio ou vídeo que não estejam relacionados ao desempenho das atividades funcionais;
h. Arquivos executáveis de qualquer tipo;
i. Mensagens comerciais não solicitadas, também conhecidas como spam;
j. Outros conteúdos notadamente fora do contexto do trabalho desenvolvido.

VIII. As mensagens ou arquivos eletrônicos com assinaturas digitais e cujos certificados forem emitidos por entidades certificadoras que façam parte da ICP-Brasil são considerados documentos oficiais no âmbito deste Instituto.

CAPÍTULO VI

DAS PROIBIÇÕES DE USO

Art. 6º Constituem abaixo o uso indevido e inadequado do serviço de acesso à internet as seguintes ações previstas:

I. Acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como: pornografia, pedofilia, racismo, comunidades de relacionamento pessoal, jogos de azar, dentre outros semelhantes;

II. Utilizar programas de troca de mensagens em tempo real (bate-papo), exceto os definidos como ferramenta de trabalho e homologados pela área de Tecnologia da Informação;

III. Acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto nos casos de comprovada necessidade, mediante solicitação à área de Tecnologia da Informação;

IV. Obter na Internet arquivos (download) que não estejam relacionados com suas atividades funcionais, a saber: imagens, áudio, vídeo, jogos e programas de qualquer tipo;

V. Acessar endereços (sites) que apresentem vulnerabilidade de segurança ou possam comprometer de alguma forma a segurança e integridade da rede de computadores deste Instituto.

CAPÍTULO VII
DA SEÇÃO DE SEGURANÇA DA INFORMAÇÃO

Art.7º Cabe à área de Segurança da Informação:

I. Promover as ações necessárias para a disponibilização da infraestrutura técnica de segurança e aplicação das normas de segurança;

II. Promover continuamente iniciativas de capacitação para servidores nos procedimentos de segurança que envolva o uso da Tecnologia da Informação, de forma a minimizar ocorrência de problemas de segurança, sem prejuízo das normas internas específicas sobre capacitação;

III. Promover a comunicação e dar publicidade das normas e ações previstas na Política de Segurança da Informação.

CAPÍTULO VIII
DO ÂMBITO E DA APLICAÇÃO

Art.8º A Política de Segurança da Informação aplica-se a todos aqueles autorizados a fazerem uso dos ativos de TI, no âmbito da rede de computadores do IPREM.

Parágrafo único. Aplica-se ainda esta política, no que couber, ao relacionamento do IPREM com outros órgãos públicos ou entidades públicas ou privadas.

CAPÍTULO IX
DA CAPACITAÇÃO

Art.9º A proposta de capacitação dos servidores envolvidos nos procedimentos de segurança deverá ser anualmente encaminhada ao Superintendente.

Parágrafo único. A capacitação deverá basear-se nas responsabilidades e papéis previstos na Política de Segurança da Informação, sem prejuízo de conteúdos que estejam fora do escopo da norma, mas podem contribuir para sua melhoria.

CAPÍTULO X
DO DESCUMPRIMENTO DA POLÍTICA DE SEGURANÇA

Art.10º O descumprimento das normas referentes à política de segurança da informação deste Instituto poderá acarretar, isolada ou cumulativamente, nos termos da legislação vigente, sanções administrativas, civis e penais, assegurada aos envolvidos a ampla defesa.

Parágrafo único. Os modelos de declaração de compromisso e de ciência das normas de Segurança da Informação vigentes no IPREM estão presentes no ANEXO I.

Art. 11 Esta Portaria entra em vigor na data de sua publicação.

Três Marias, 17 de dezembro de 2019.

JOANA DARC SILVEIRA MACEDO
Superintendente do IPREM

SILVIO APARECIDO SOBRINHO
Presidente do Conselho Administrativo do IPREM.

ANEXO I

TERMO DE COMPROMISSO CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO	
IDENTIFICAÇÃO DO CONTRATO:	
Nº DO CONTRATO	
NOME DA EMPRESA CONTRATADA	
CNPJ DA CONTRATADA	
OBJETO RESUMIDO	
VIGÊNCIA CONTRATUAL	

TERMO:

O <Contratante>, sediado em <Endereço Contratante>, CNPJ n.º <CNPJ Contratante>, doravante denominado CONTRATANTE, e, de outro lado, a <Contratada>, sediada em <Endereço Contratada>, CNPJ n.º <CNPJ Contratada>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º <n° contrato / ano> doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;
CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO E CONFIDENCIALIDADE DAS INFORMAÇÕES, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE - por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes - segundo Portaria nº 003/2019, de 17 de dezembro de 2019, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe

sobre o Núcleo de Segurança e Credenciamento.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

I. Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

II. Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestritas, obtidas por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

III. Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiro.

IV. Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

V. Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO DE COMPROMISSO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O termo INFORMAÇÃO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, publicações, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, projetos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominado INFORMAÇÕES, a que, diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

§1° – Comprometem-se as partes a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

§2° – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

§3°– As obrigações constantes deste TERMO DE COMPROMISSO não serão aplicadas àquelas informações que:

I. Sejam comprovadamente de domínio público no momento da revelação;

II. Tenham sido comprovada e legitimamente recebidas de terceiros, estranhos ao presente TERMO DE COMPROMISSO;

III. Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO DE COMPROMISSO.

§1° – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

§2° – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO DE COMPROMISSO bem como da natureza sigilosa das informações.

I. A CONTRATADA deverá firmar acordos por escrito com seus empregados visando a garantir o cumprimento de todas as disposições do presente TERMO DE COMPORMISSO e dará ciência à CONTRATANTE dos documentos comprobatórios.
§3° – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

§4° – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO DE COMPROMISSO.
I. Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

§5° – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, prepostos, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

§6° – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I. Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II. Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III. Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV. Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta – DA VIGÊNCIA

O presente TERMO DE COMPROMISSO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislação em vigor que trata desse assunto, podendo culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima – DISPOSIÇÕES GERAIS

Este TERMO DE COMPROMISSO é parte integrante e inseparável do CONTRATO PRINCIPAL.

§1° – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

§2° – O disposto no presente TERMO DE COMPROMISSO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tais como aqui definidas.

§3° – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I. A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II. A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL;

III. A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV. Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V. O presente TERMO DE COMPROMISSO somente poderá ser alterado mediante TERMO ADITIVO firmado pelas partes;

VI. Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO DE COMPROMISSO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII. O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO ADITIVO ao CONTRATO PRINCIPAL;

VIII. Este TERMO DE COMPROMISSO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

A CONTRATANTE elege o foro da cidade de CIDADE (UF), onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

DE ACORDO

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE

COMPROMISSO é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.	
CONTRATANTE	**CONTRATADA**
Local, dia/mês/ano. Nome do Responsável pelo Contratante Cargo	Local, dia/mês/ano. Nome do Responsável pela Contratada Cargo/ CPF