INSTITUTO DE PREVIDÊNCIA DO MUNICÍPIO DE MIRANDÓPOLIS
IPEM
CNPJ– 02.365.145/0001-11
PRAÇA MANOEL ALVES DE ATAÍDE, 160 – CENTRO, MIRANDÓPOLIS/SP

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Introdução

Este programa de conscientização sobre Segurança da Informação tem como objetivo principal definir os princípios e diretrizes gerais que visam a preservação da segurança da informação, primando pela confidencialidade, integridade, disponibilidade, autenticidade, bem como legalidade dos processos que amparam a operacionalização e gestão das atividades desta Instituição e estabelecer as responsabilidades e limites de atuação dos Dirigentes, Servidores e Prestadores de Serviços do IPEM em relação à segurança da informação e comunicação, reforçando uma cultura interna baseada em integridade.

Com isso se pretende influenciaros servidores a mudarem seus hábitos, bem como criar a consciência de que todos são corresponsáveis pela Segurança da Informação. Esse processo de conscientização deve ser contínuo, para manter os usuários alertas e para prepará-los para os novos riscos e ameaças que surgem a cada dia.

2. Para que serve?

A Política de Segurança da Informação é necessária para garantir a proteção das informações do IPEM, assegurando que nenhuma informação seja alterada ou utilizada indevidamente.

A Segurança da Informação é garantida por meio da preservação de dos cinco pilares básicos:

- **Confidencialidade:** É a garantia de que somente pessoas autorizadas terão acesso à informação;
- **Integridade**: É a garantia de que a informação mantém as características originais estabelecidas por seu proprietário, ou seja, de que não foi modificada ou alterada de forma indevida;
- **Disponibilidade**: É a garantia de que a informação estará pronta para o uso (por pessoas autorizadas) quando for necessária;
- **Autenticidade:** É a garantia de que a informação vem da fonte anunciada, ou seja, de que o autor da informação é realmente quem diz ser e,
- **Não repúdio:** É a garantia de que a pessoa não negue ter assinado ou criado a informação.

3. Fundamentos e Conceitos

A Política de Segurança da Informação tem por finalidade estabelecer as diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações de conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio pelos sistemas de informação.

O objetivo da Política de Segurança da Informação é estabelecer diretrizes que permitam aos usuários do IPEM seguirem padrões de comportamento relacionados à segurança adequados as necessidades de negócio da informação, bem como a implementação de controle e processos para seus atendimentos.

A Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos do IPEM, com vista à garantia de integridade, disponibilidade, conformidade e confiabilidade.

Todos os mecanismos utilizados para a segurança da informação devem ser mantidos para preservar a continuidade das funções institucionais.

O gerenciamento dos ativos de informações, deverão observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua.
O acesso às informações, sistemas e instalações depende da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento.
Comete a Diretoria Executiva do IPEM promover a cultura de segurança da informação e comunicação e o acompanhamento de investigações e avaliações de danos decorrentes de quebras de segurança.

4. DEFINIÇÕES BÁSICAS

Para os fins dessa Política de Segurança da Informação, considera-se:
Acesso lógico: acesso a rede de computadores, sistemas e estações de trabalho por meio de autenticação;
Acesso remoto: ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;
Agente responsável: servidor público ocupante de cargo efetivo ou em comissão no IPEM, direta ou indiretamente incumbido de chefiar e gerenciar os funcionários que sejam usuários das informações no âmbito da autarquia;
Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
Análise/avaliação de riscos: processo completo de análise e avaliação de riscos;
Ativo: qualquer bem que o IPEM possua e que tenha valor para a organização;
Ativo da informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas a eles tem acesso;
Ativo sigiloso: qualquer bem que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos ao IPEM e seus segurados;
Banco de dados: é um sistema de armazenamento de dados que tem como objetivo organizar e guardar as informações;
Auditoria: verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir ou eliminar fraudes, erros, práticas ineficientes ou ineficazes;
Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
Bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso;
Chefe de mais alto nível: está envolvido com toda a responsabilidade da segurança da informação. Pode delegar a função de segurança, mas é visto como o principal ponto quando são consideradas as responsabilizações por eventos relacionados com a segurança;
Cópia de Segurança (Backup): copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;
Classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;
Confidencialidade: propriedade de que a inflação não esteja disponível ou revelada a pessoa física ou jurídica, sistema, órgão ou entidade não autorizada;
Correio Eletrônico: é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;
Download: baixar copiar arquivos de um servidor/site na internet para um computador pessoal;
Internet: rede mundial de computadores;
Log: é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado.

Correio Eletrônico

Os servidores poderão utilizar o correio eletrônico desde que essa ferramenta não seja utilizada de modo indevido, ilegal ou antiético.

Os servidores NÃO poderão utilizar o serviço de correio eletrônico para:

- Modificar arquivos ou assumir, sem autorização, a identidade de outro usuário;
- Prejudicar intencionalmente usuários da internet, através do envio de programas e de acesso não autorizados a computadores, ou de alterações de arquivos de programas;
- Utilizar-se do serviço de propriedade do IPEM, desvirtuando sua finalidade com o intuito de cometer fraude;
- Utilizar o serviço de correio eletrônico de qualquer forma a participar em atividades de pesquisa comercial correntes, lixo eletrônico ou quaisquer mensagens periódicas ou não solicitadas (SPAM);
- Difamar, ofender, perseguir ou ameaçar ou de qualquer outra forma violar os direitos de terceiros;
- Enviar arquivos que contenham vírus, arquivos corrompidos ou quaisquer outros softwares ou programas semelhantes que possam danificar a operação de outros computadores ou a propriedade de terceiros;
- Vedado o acesso não autorizado às caixas postais de terceiros e as tentativas de acesso deverão ser registradas em log, inclusive acessos feitos indevidamente por administradores de sistemas;
- Vedado o envio de informações críticas para pessoas ou organizações não autorizadas observando quando for o caso, orientações para o tratamento de informações classificadas;
- Vedado o envio de material obsceno, ilegal ou não ético, envio de propaganda, mensagem do tipo corrente e de entretenimento, relacionadas com nacionalidade, raça, orientação sexual, religiosa, convicção política ou qualquer outro assunto que possa vir a difamar o usuário como cidadão e que não tenha relação com o serviço a que o usuário é destinado no ambiente do TI do IPEM;
- O Correio Eletrônico do IPEM deve ser utilizado sempre baseado no bom senso e de acordo com os preceitos legais.

Acesso à Rede

O servidor do IPEM deve ser utilizado seguindo as seguintes normas:

- Os usuários devem receber acesso somente aos serviços que tenham sido especificamente autorizados a usar.
- É obrigatório armazenar os arquivos inerentes ao IPEM no servidor de arquivos para garantir a cópia de segurança do mesmo;
- É proibido o uso do servidor de arquivos para armazenar informações de cunho pessoal;
- Os arquivos gravados em diretórios temporários e públicos do servidor e das estações de trabalho podem ser acessados por todos os usuários que utilizarem a rede, portanto não se pode garantir sua integridade e disponibilidade;
- Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento da estrutura tecnológica;
- O usuário deve fazer manutenções periódicas no diretório pessoal, evitando acumulo de arquivos desnecessários;
- São de responsabilidade do usuário as informações em seu diretório pessoal, sendo que o mesmo deve evitar o acumulo de arquivos desnecessários e,
- As contas podem ser monitoradas pela Diretoria responsável, com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais.

Regras Gerais

- Não são permitidas alterações das configurações da rede de inicialização das maquinas bem como as modificações que possam trazer algum problema futuro;
- A utilização de equipamentos de informática particulares na rede, só será liberada mediante autorização e vistoria no equipamento para saber se o mesmo atende aos requisitos mínimos de segurança exigidos;

- Quando ocorrer a nomeação/contratação/exoneração/ demissão do servidor, a Diretoria Administrativa deverá providenciar a ativação ou desativação dos acessos do usuário a qualquer recurso da rede do IPEM;
- É proibida a instalação ou remoção de softwares que não forem devidamente acompanhados pelo Diretor Administrativo e/ou responsável pelo setor de informática;
- O uso e manuseio, alteração, reposição de equipamento defeituoso será executado unicamente pelo responsável pelo setor da informática;
- É proibida a manutenção de equipamentos de informática particulares dentro das dependências do IPEM, e
- Todo arquivo em mídia proveniente de entidade externa ao IPEM deve ser verificado por programas antivírus. Todo arquivo recebido/obtido através do ambiente da internet deve ser verificado por programa antivírus. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

Usuários

- Todo servidor do IPEM terá direito a uma senha de acesso a rede corporativa e uma conta de e-mail do IPEM;
- O acesso a quaisquer outros serviços ou sistemas providos pelo IPEM ou por outros órgãos da administração direta deverá ser solicitado a chefia imediata;
- O usuário é o único responsável pelo uso da sua identificação (login e senha), quaisquer ações praticadas durante a utilização desta identificação será de sua inteira responsabilidade;
- O usuário não deverá compartilhar sua senha com outros usuários. Caso, o usuário perceba que outro usuário possa estar utilizando seu login de acesso, o mesmo deverá informar imediatamente a chefia imediata, para efetuar a troca da senha e auditoria das atividades executadas com este login e,
- Antes de ausentar-se do local de trabalho, o usuário deverá fechar todos os programas em uso, efetuar o logoff da rede ou fazer o bloqueio do computador, evitando o uso dos recursos de TI por pessoas não autorizadas.

Recomendações para o uso seguro dos recursos de TI

O envolvimento do usuário é importante no processo da segurança dos recursos de TI, pois é na adequada utilização destes recursos, como instrumento de trabalho, que se inicia a formação de uma cultura de segurança da informação. Desta forma, recomenda-se aos usuários a adoção das seguintes práticas:

- Fazer regularmente cópias de segurança de seus dados;
- Manter registro das cópias de segurança;
- Guardar as cópias de segurança em local seguro e distinto daquele onde se encontra a informação original;
- Alterar periodicamente suas senhas;
- Certificar que o endereço apresentado no navegador corresponde ao sítio que realmente se quer acessar, antes de realizar qualquer ação ou transação;
- Digitar no navegador o endereço desejado e não utilizar links como recurso para acessar um outro endereço destino;
- Não abrir arquivos ou executar programas anexados a e-mails, sem antes verificá-los com um antivírus.

Recomendações sobre atividades permitidas

Utilizar programas de computador licenciados para uso pelo IPEM, de acordo com as disposiçõesespecíficas previstas em contrato.

- A instalação de programas e sistemas homologados é atribuição da administração desistemas e TI;

- Criar, transmitir, distribuir, disponibilizar e armazenar documentos, desde que respeite às leis e regulamentações, notadamente aquelas referentes aos crimes informáticos, ética, decência, pornografia envolvendo crianças, honra e imagem de pessoas ou empresas, vida privada e intimidade;
- Fazer cópia de documentos e ou programas de computador a fim de salvaguardá-los, respeitada a legislação que rege a salvaguarda de dados, informações, documentos e materiais sigilosos do IPEM, exigindo-se autorização para aqueles protegidos pelosdireitos autorais, inclusive músicas, textos, documentos digitalizados e qualquer conteúdoencontrado em revistas, livros ou quaisquer outras fontes protegidas por direitos autorais.

Recomendações sobre atividades NÃO permitidas

- Introduzir códigos maliciosos nos sistemas de TI;
- Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;
- Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas de TI;
- Alterar registro de evento dos sistemas de TI;
- Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de TI;
- Monitorar ou interceptar o tráfego de dados nos sistemas de TI, sem a autorização de autoridade competente;
- Violar medida de segurança ou de autenticação, sem autorização de autoridade competente;
- Fornecer informações a terceiros, sobre usuários ou serviços disponibilizados nos sistemas de TI, exceto os de natureza pública ou mediante autorização de autoridade competente;
- Fornecer dados classificados de acordo com a legislação vigente, sem autorização de autoridade competente.

Recomendação para a Utilização de Aplicações Corporativas e Software de Terceiros

- Deve ser vedado aos usuários que fazem uso de sistemas de informação o acesso não autorizado a qualquer outro sistema que não possua permissão de uso, assim como a danificação, a alteração a interrupção da operação de qualquer sistema do ambiente de TI. Da mesma maneira deve ser vedado aos usuários a obtenção indevida de senhas de acesso, chaves criptográficas ou qualquer outro mecanismo de controle de acesso que possa possibilitar o acesso não autorizado a recursos informacionais;
- A classificação ou reclassificação da informação deve seguir as orientações da legislação vigente;
- Deve ser vedado aos usuários o acesso, modificação, a remoção ou a cópia de arquivos que pertençam a outro usuário sem a permissão expressa do mesmo;
- As configurações e atribuição de parâmetros em todos os computadores conectados à rede do IPEM devem estar de acordo com as políticas e normas de gerenciamento internas.
- Quando do desligamento do usuário, seus arquivos armazenados em estação de trabalho ou em qualquer servidor de rede do IPEM e, também, seus documentos em papel devem ser imediatamente revisados pela chefia imediata para determinar quem tornar-se-á curador das informações relacionadas, assim como nos casos devidos, identificar o método mais adequado para a eliminação das mesmas, levando-se em conta as orientações sobre a eliminação de informações classificadas contidas na legislação vigente.
- Todas as atividades dos usuários que podem afetar os sistemas de informação do IPEM devem ser possíveis de reconstituição a partir dos logs de maneira a evitar ou dissuadir o comportamento incorreto. Estes procedimentos devem contar inclusive com mecanismos de responsabilização claros e amplamente divulgados nos meios de comunicação internos.

- É vedada a utilização de software da Internet ou de qualquer outro sistema externo ao IPEM. Esta proibição é necessária porque tal software pode conter vírus que podem comprometer o ambiente de TI.
- É vedada a utilização de dispositivos de armazenamento de origem externa, nas estações de trabalho do IPEM ou nos servidores de rede antes de serem submetidos a um software antivírus.
- Todos os softwares e arquivos transferidos de fontes que não sejam do próprio IPEM via Internet (ou qualquer outra rede Pública) devem ser examinados com o software de detecção de vírus utilizado pelo IPEM. Este exame deve acontecer antes que o seja executado ou aberto por um outro programa, como por exemplo, por um processador de texto e também, antes e depois que o material tenha sido descompactado.
- O usuário do ambiente de TI do IPEM não deve executar ou desenvolver qualquer tipo de programa ou processo externo às suas atividades.
- Os usuários não devem desenvolver, gerar, compilar, copiar, coletar, propagar, executar ou tentar introduzir qualquer código projetado para se auto-replicar, danificar ou de outra maneira obstruir o acesso ou afetar o desempenho de qualquer computador, rede ou sistema de TI do IPEM.

Responsabilidade:

Os atuais e futuros **Dirigentes, Servidores, Conselheiros e Prestadores de Serviços** do **IPEM**, deverão assinar o **Termo de Compromisso para Dirigentes e Colaboradores** ou **Termo de Compromisso de Segurança da Informação para Terceiros – Pessoa Jurídica,** tomando ciência do conteúdo dessa Política de Segurança da Informação e responsabilizando-se pelo seu fiel cumprimento.

Penalidades:

O não cumprimento pelos servidores neste documento, seja isolada ou cumulativamente, poderá ensejar, de acordo com a infração cometida, as seguintes punições:

- Comunicação de Descumprimento: será encaminhado ao funcionário, por email, notificação informando o descumprimento da norma, com a indicação precisa da violação praticada e, em caso de reincidência, será enviada também, uma cópia para a respectiva chefia.
- Advertência ou Suspensão: a pena de advertência ou suspensão será aplicada nos casos legais e após regular apreciação através de processo administrativo disciplinar.

6. DAS DISPOSIÇÕES FINAIS

Esta Política de Segurança da Informação deve ser revisada e atualizada periodicamente no mínimo a cada 3 (tês) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.
Os casos omissos e as dúvidas com relação a essa Política de Segurança da Informação serão submetidos ao Conselho de Administração do IPU.

Mirandópolis, 09 de janeiro de 2025.

Edilene da Costa da Silva
Presidente do Instituto de Previdência
Municipal de Mirandópolis

ANEXO A - TERMO DE COMPROMISSO E RESPONSABILIDADE PARA DIRIGENTES E COLABORADORES

Eu [NOME COMPLETO] pelo presente instrumento afirmo cumprir e estar ciente de que:

1. Sou responsável por manter e zelar pela confidencialidade, integridade, disponibilidade, autenticidade e legalidade de toda e qualquer informação de propriedade ou sob a responsabilidade do **IPEM** a mim confiada e/ou por mim acessada em razão de atividades profissionais;

2. Todas as informações disponibilizadas, acessadas e/ou criadas por mim em razão de atividades profissionais são de propriedade e/ou direito de uso exclusivo aos interesses do **IPEM**;

3. Devo agir de forma profissional, cautelosa, ética e legal em relação às informações e recursos de Tecnologia da Informação (Recursos de TI) de propriedade ou sob a responsabilidade do **IPEM**, além de utilizá-los apenas para fins profissionais, limitados aos interesses do **IPEM** e às atividades contratadas, de acordo com as funções e cargos estabelecidos;

4. Não devo copiar, transferir, compartilhar, alterar, adulterar ou utilizar indevidamente ou para propósitos particulares quaisquer informações de propriedade ou sob a responsabilidade do **IPEM**, além de não praticar quaisquer atos que possam causar prejuízo à Instituição;

5. Devo devolver as informações e recursos de TI de propriedade ou sob a responsabilidade do **IPEM** imediatamente quando solicitado ou em caso de encerramento das atividades profissionais, além de realizar o descarte seguro das informações do **IPEM**;

6. Estou ciente que o **IPEM** monitora seus ambientes físicos e lógicos visando a eficácia dos controles implantados e a proteção de seu patrimônio e reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes ligados à segurança da informação;

7. Devo comunicar imediatamente ao meu superior imediato qualquer falha, suspeita ou ameaça por mim detectada aos recursos do **IPEM**, como informações, recursos de TI, ambientes físicos, imagem e reputação;

8. Devo ler, cumprir e manter-me atualizado com a Política de Segurança da Informação (PSI) do **IPEM**;

9. O presente Termo vigorará até o término do contrato ou vínculo relacional com o **IPEM**, contudo as obrigações e responsabilidades em relação ao sigilo, preservação de informações e de direitos de propriedade aqui tratados, permanecem mesmo após o término do contrato ou vínculo relacional estabelecido;

10. Quaisquer atitudes ou ações contrárias ao estabelecido por este Termo, ainda que por mera tentativa de burla, enseja a aplicação das medidas disciplinares ou legais cabíveis;

Por fim, manifesto nesse ato minha ciência expressa com todas as cláusulas acima, assinando o presente Termo de Compromisso e Responsabilidade.

_____, [DIA] de [MÊS] de [ANO].

_____

[NOME COMPLETO]

N.º da Matrícula:

N.º do CPF:

ANEXO B - TERMO DE COMPROMSSO DE SEGURANÇA DA INFORMAÇÃO PARA TERCEIROS – PESSOA JURÍDICA

INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE MIRANDÓPOLIS – doravante denominado **IPEM**, e **[NOME COMPLETO DA PESSOA JURÍDICA], já qualificados pelo Contrato** [***] **celebrado entre as partes em** [***] **de** [***] **de** [***], firmam o presente **Termo de Compromisso de Segurança da Informação para Terceiros – Pessoa Jurídica**, passando a serintegrante do referido **Contrato.**

Pelo presente **Instrumento**, as partes têm entre si acordado cláusulas específicas e necessárias para adequada consecução dos serviços contratados, a fim de reger as responsabilidades com relação à **Segurança da Informação** em razão do acesso às **INFORMAÇÕES** de propriedade ou sob a responsabilidade do **INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE MIRANDÓPOLIS** – doravante denominado **IPEM**, aos seus ambientes lógicos e/ou **recursos de Tecnologia da Informaçãoe Comunicação.**

O/A **[NOME COMPLETO DA PESSOA JURÍDICA]**, pelo presente **Instrumento** afirma cumprir, bem como garantir o cumprimento por seus profissionais, sejam eles funcionários, colaboradores, prepostos, empregados e prestadores de serviços (**Profissionais**), de todas as orientações e determinações especificadas e outras que vierem a ser editadas estando ciente e compreendendo que é responsável por:

1. Prestar os serviços acordados com estrita observância dos preceitos éticos e legais, envidando todos os esforços para atender aos padrões e condições técnicas exigidos, as regras relacionadas ao tratamento de **INFORMAÇÕES** do **IPEM** e as melhores práticas de mercado concernentes a Segurança da Informação;

2. Garantir que os **Profissionais** alocados para execução do presente **Contrato** estejam cientes e cumpram as regras de **Segurança da Informação** estabelecidas por este **Instrumento, especialmente a Política de Segurança da Informação (PSI)** e pelos demais documentos normativos do **IPEM**, além daqueles entregues no momento da contratação ou disponíveis para acesso em razão dos serviços contratados;

3. Possuir ou elaborar uma **Política de Segurança da Informação** e acordos de confidencialidade com todos os **Profissionais**, que tiverem acesso ou manusearem as **INFORMAÇÕES** do **IPEM** em razão da prestação dos serviços contratados;

4. Assegurar a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das **INFORMAÇÕES** do **IPEM** no desenvolvimento dos serviços prestados;

5. Utilizarem as **INFORMAÇÕES** e os **recursos de TI** do **IPEM**. além do acesso aos ambientes físicos e lógicos, **somente para prestação dos serviços contratados**, de acordo

com a legislação nacional vigente e a ética;

6. Reconhecer que todas as **INFORMAÇÕES** recebidas, criadas ou acessadas por seus **Profissionais** em razão dos serviços contratados são de propriedade exclusiva do **IPEM**;

7. Preservar e proteger as **INFORMAÇÕES** a que tiverem acesso, em razão dos serviços contratados, por si e pelos seus **Profissionais,** assim como os recursos de TI dos diversostipos de ameaça e em todo o seu ciclo de vida, contida em qualquer suporte ou formato;

8. Utilizar os meios físicos de suporte das cópias das **INFORMAÇÕES** a serem assinalados, quer legíveis humanamente, por equipamentos ou dispositivos (dados eletrônicos), com rótulo de informação **"CONFIDENCIAL";**

9. Tratar todas as **INFORMAÇÕES** a que tiverem acesso, por si e seus **Profissionais**,como confidenciais, inclusive aquelas que não estejam explicitamente rotuladas;

10. Manter as **INFORMAÇÕES** do **IPEM** em segurança e sob sigilo, obrigando-se a tomar todas as medidas necessárias para impedir que sejam transferidas, reveladas, divulgadas ou utilizadas, sem autorização, a qualquer terceiro estranho a este **Instrumento** por si e por parte de seus **Profissionais,** ou utilizar de forma contrária ao aqui estabelecido;

11. Não é permitido, por si e pelos seus Profissionais:

11.1. Utilizar, reter ou duplicar as **INFORMAÇÕES** que lhe forem fornecidas para criação de qualquer arquivo, lista ou banco de dados de sua utilização particular ou de quaisquer terceiros, exceto quando autorizada expressamente por escrito pelo **IPEM**;

11.2. Copiar, reproduzir, transferir ou usar indevidamente quaisquer **INFORMAÇÕES** para qualquer outra finalidade que não seja a promoção dos serviços contratados;

11.3. Utilizar as **INFORMAÇÕES** de forma que possa configurar concorrência desleal com o **IPEM** tampouco explorá-las em outros negócios ou oportunidades comerciais, assim como promover ou participar no seu desenvolvimento, sem prévia e expressa autorização do **IPEM**;

11.4. Modificar ou adulterar as **INFORMAÇÕES** fornecidas pelo **IPEM**, bem como subtrairou adicionar qualquer elemento indevidamente;

11.5. Comentar, compartilhar ou publicar na Internet ou em mídias sociais, ou qualquer plataforma de armazenagem aberta de dados, como repositórios digitais, quaisquer **INFORMAÇÕES** relacionadas à prestação de serviços que tem junto o **IPEM**, a não ser que tenha havido prévia e expressa autorização;

11.6. Realizar qualquer atividade relacionada a captura de áudio, vídeo ou imagens dentro das dependências do **IPEM**, exceto quando relacionada a atividade contratada.

12. Respeitar os controles estabelecidos pelo **IPEM**, além de garantir o controle automatizado de acessos físicos e lógicos aos ambientes que contiverem **INFORMAÇÕES** do **IPEM**, por meio de:

12.1. Controle de acessos a ambientes físicos por dispositivos automatizados com o uso de biometria, senhas, cartão de proximidade ou qualquer outro dispositivo de controle de acesso único;

12.2. Identificação de usuários individuais com o uso de senhas para acesso a sistemas, redes ou qualquer ambiente tecnológico, além de duplo grau de autenticação para acessos críticos;

12.3. Monitoramento, gravação de histórico e auditoria dos acessos relacionados à prestaçãodos serviços contratados;

12.4. Gravação de acessos de usuários privilegiados.

13. Armazenar as **INFORMAÇÕES** físicas e os dispositivos que as armazenam em ambientecom acesso físico controlado e restrito, por exemplo: gavetas ou armários com chaves;

14. De acordo com a criticidade da informação, armazenar e transmitir as **INFORMAÇÕES** digitais em ambiente seguro, com controle de acesso e mediante o uso de criptografia;

15. Utilizar mecanismo de identificação e autenticação individual, sendo responsável pelo uso, proteção e sigilo de sua identidade digital, não sendo permitido compartilhar, revelar, salvar, replicar, publicar ou fazer uso não autorizado de suas credenciais, tal qual de terceiros;

16. Utilizar hardware e software licenciados, de acordo com a legislação aplicável, respeitando tratados e convenções internacionais, bem como que estes sejam sempre homologados e autorizados previamente pelo(a) **[NOME COMPLETO DA PESSOA JURÍDICA]**;

17. Respeitar os direitos de propriedade intelectual do **IPEM** e de terceiros durante a realização das atividades contratadas;

18. Quando houver uso de dispositivos móveis por parte de **Profissionais**, tais como notebooks, smartphones, tablets, celulares e pendrives, sempre aplicar as medidas de **Segurança da Informação** relacionadas a cada equipamento, que envolvam desde a implementação e/ou ativação de recursos como uso de senha de bloqueio, bloqueio automático por inatividade, antivírus, antispyware, apagamento remoto até uso de recursos de backupseguro;

19. No caso de haver necessidade de se fazer uso de Repositórios Digitais, a exemplo, mas não se limitando a Google Drive, Dropbox, OneDrive e iCloud, para transmissão de **INFORMAÇÕES**

entre as partes, que seja feito o uso de criptografia ou outro método similar que possa garantir a integridade e confidencialidade da informação;

20. Sempre que houver destruição de **INFORMAÇÕES**, inclusive, de cópias, reproduções, reimpressões, traduções ou de materiais que contenham ou relacionem **INFORMAÇÕES,** adotar o "descarte seguro de **INFORMAÇÕES**", ou seja, papéis e demais **INFORMAÇÕES** impressas deverão ser processadas no picotador de papéis e mídias deverão ser apropriadamente destruídas ou sanitizadas;

21. Devolver ao **IPEM**, ou a exclusivo critério deste, descartar todas as **INFORMAÇÕES** que estejam em seu poder, em até 48h (quarenta e oito horas), contados da data da solicitação;

22. Estabelecer procedimentos e processos para treinamento e conscientização das normas e políticas de **Segurança da Informação** para todos os **Profissionais**;

23. Informar imediatamente ao **IPEM** todos os incidentes de **Segurança da Informação** que ocorrerem ou puderem ocorrer relacionados à **INFORMAÇÕES** do **IPEM**;

24. Reconhecer que o **IPEM** realiza o monitoramento de seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes ligados à **Segurança da Informação**;

25. Estar ciente que o **IPEM** pode auditar ou inspecionar os recursos de TIC que estiverem em suas dependências ou que interajam com seus ambientes lógicos sempre que considerar necessário, sempre atendendo aos princípios da proporcionalidade, razoabilidadee privacidade de seus proprietários ou portadores;

26. Observar e garantir o cumprimento das recomendações acima durante a prestação dos serviços, sendo responsável pelas perdas e danos de qualquer natureza decorrentes de infrações a que houver dado causa pela sua inobservância.

27. Quaisquer atitudes ou ações contrárias ao estabelecido por este Termo, ainda que por mera tentativa de burla, enseja a aplicação das medidas disciplinares ou legais cabíveis.

Este **Instrumento** obriga as Partes e seus sucessores, a qualquer título.

A omissão ou tolerância do **IPEM**, em exigir o estrito cumprimento dos termos e condições deste **Instrumento**, não constituirá novação ou renúncia, nem afetará os seus direitos, que poderão ser exercidos a qualquer tempo.

Este **Instrumento** permanecerá em vigor por prazo indeterminado e, mesmo depois de encerrado o Contrato, o (a) **[NOME COMPLETO DA PESSOA JURÍDICA]** continuará obrigada e responsável com relação às disposições sobre sigilo e preservação dos direitos de propriedade aqui tratados. É vedada a cessão e/ou transferência a terceiros, parcial ou total, dos direitos e obrigações deste **Instrumento**, sem a prévia anuência, escrita, da outra Parte.

As Partes declaram, sob as penas da Lei, que os signatários do presente Instrumento são seus procuradores / representantes legais, devidamente constituídos na forma dos respectivos Estatutos / Contratos Sociais, com poderes para assumir as obrigações ora contraídas.

E por estarem assim, justas e contratadas, as **Partes** celebram o presente **Instrumento**, em 2 (duas) vias, de igual forma e teor, na presença de 2(duas) testemunhas que igualmente o subscrevem.

Mirandópolis/SP, ____ de _____ de_____.

_____

IPEM

C.N.P.J. sob o nº 02.365.145/0001-11

_____

[NOME COMPLETO DA PESSOA JURÍDICA]

C.N.P.J sob o nº [***]