POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CONSIDERANDO a Portaria MPS nº 185, de 14 de maio de 2015, que instituiu o 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";
CONSIDERANDO a necessidade de estabelecer diretrizes para proteção das informações geradas, processadas e armazenadas,
"INSTITUI A Política de Segurança da Informação DO INSTITUTO DE PREVIDÊNCIA E ASSISTENCIA DOS SERVIDORES MUNICIPAIS DE NOVO HAMBURGO – IPASEM-NH".

Esta Política de Segurança da Informação é uma declaração formal de compromisso do IPASEM-NH com a proteção das informações sob sua guarda e a formalização das normas para segurança, devendo ser observado por todos os seus servidores, segurados e prestadores de serviços.

DEFINIÇÕES E TERMOS

- **Autenticidade de Informação** é a garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.
- **Confidencialidade de Informação** é a garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento.
- **Disponibilidade de Informação** é a garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito.
- **Integridade de Informação** é a fidelidade das informações. Indica a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Indica, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital.
- **Serviço de backup** compreende a realização de cópias de segurança dos arquivos com o objetivo de restaurá-los no menor tempo possível caso haja necessidade.

DAS DISPOSIÇÕES INTRODUTÓRIAS:

a) Fica instituída a Política de Segurança da Informação – Política de Segurança da Informação do Instituto de Previdência e Assistência dos Servidores Municipais de Novo Hamburgo – IPASEM-NH.
b) A Política de Segurança da Informação é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico, gerencial e pelos usuários internos e externos. A Política de Segurança da Informação tem por objetivo preservar a disponibilidade, integridade, confidencialidade, autenticidade e salvaguarda das informações geradas, processadas e armazenadas no âmbito do Instituto, mediante o estabelecimento e difusão de diretrizes e princípios para o IPASEM-NH orientando quanto ao uso adequado da informação de sua propriedade ou em custódia.
c) A segurança da informação e comunicação busca reduzir o risco de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações e roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação, os recursos de processamento da informação, ou os equipamentos do IPASEM-NH, fundamentada nos princípios da confiabilidade, responsabilidade, disponibilidade, integridade, confidencialidade, autenticidade, legalidade e ética.
d) O cumprimento da Política de Segurança da Informação e de suas normas complementares deverá ser avaliado periodicamente pela Diretoria do Instituto.
e) Toda informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada pelos agentes públicos ou privados vinculados ao IPASEM-NH, no exercício de suas atividades, é de propriedade do IPASEM-NH e será protegida.

1. REGRAS GERAIS PARA PROTEÇÃO DA INFORMAÇÃO

1.1. Define-se como necessária a proteção das informações da instituição ou sob sua custódia como fator primordial nas atividades profissionais de cada servidor, segurado ou prestador de serviços do IPASEM-NH,
1.2. Os servidores devem assumir uma postura proativa no que diz respeito à proteção das informações e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido a sistemas de informação sob sua responsabilidade;
1.3. Assuntos confidenciais não devem ser expostos publicamente;
1.4. Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados, divulgados e/ou revelados a outras pessoas, nem serem digitadas em máquinas de terceiros, especialmente fora do IPASEM-NH;
1.5. Somente softwares homologados pelo setor de Tecnologia da Informação podem ser utilizados no ambiente computacional;
1.6. Arquivos digitais e/ou documentos impressos (incluindo papéis para "rascunho") contendo dados pessoais de terceiros ou informações confidenciais devem ser armazenados e protegidos de acesso por

pessoal não autorizado, sendo o seu descarte realizado na forma da legislação pertinente.

1.7. Deve ser adotado o conceito de “mesa limpa”, ou seja, ao terminar o trabalho o usuário não deve deixar nenhum documento e/ou mídias com informações confidenciais e/ou restritas sobre as mesas, impressoras e/ou demais locais de fácil acesso.

1.8. Todo usuário cadastrado pode acessar dados das redes de computadores do IPASEM-NH de acordo com as suas permissões relativas à atividade executada e o setor onde está alocado;

1.9. Não é permitido o compartilhamento de pastas e/ou arquivos salvos nos computadores do Instituto. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis.

1.10. Todo dispositivo, para poder obter acesso a rede de computadores utilizadas pelo IPASEM-NH, deverá ser previamente autorizado pelo gestor do respectivo setor, e cadastrado pelo departamento de Tecnologia da Informação, afim de obter o devido acesso com segurança;

1.11. Todos os dados considerados como imprescindíveis aos objetivos do IPASEM-NH devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança (backup), devendo ser submetidos à testes periódicos de recuperação;

1.12. O acesso lógico aos sistemas computacionais disponibilizados pelo IPASEM-NH deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade da informação, garantindo a rastreabilidade e a efetividade do acesso autorizado;

1.13. O acesso às dependências do IPASEM-NH ou à ambientes sob controle do IPASEM-NH devem ser acompanhado de um colaborador do Instituto, e controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade da informação ali armazenada ou manipulada, garantindo a rastreabilidade e a efetividade do acesso autorizado;

1.14. É vedado aos usuários de sistemas e informações do IPASEM-NH aceitar ajuda técnica de pessoas estranhas e/ou não autorizadas, seja de forma presencial, por e-mail, telefone, entre outros. A ajuda técnica deve ser provida pelo quadro de funcionários do IPASEM-NH ou da equipe técnica contratada responsável pelo equipamento, devendo em ambos os casos a pessoa ser devidamente identificada.

2. CLASSIFICAÇÃO DA INFORMAÇÃO

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

2.1. **Confidencial:** É uma informação crítica para IPASEM-NH. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais ao IPASEM-NH. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por

servidores, empregados, beneficiados ou segurados vinculados e/ou fornecedores.

2.2. **Pública:** É uma informação do IPASEM-NH 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 que exija publicidade da mesma.

2.3. **Interna:** É uma informação do IPASEM-NH que ela não tem interesse em divulgar, mas cujo acesso por parte de indivíduos externos à autarquia deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à Imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os servidores, empregados e prestadores de serviços do IPASEM-NH.

2.4. **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

3. CONTAS DE USUÁRIO E AUTENTICAÇÃO NOS SISTEMAS DE INFORMÁTICA

3.1. A autenticação nas estações de trabalho e/ou demais sistemas de informática ocorrerá por meio de senha alfanumérica, individual e intransferível, composta por, no mínimo, 8 (oito) caracteres.

3.2. Deve-se evitar a utilização de senhas consideradas “fracas”, “comuns”, ou de fácil dedução, como por exemplo datas de aniversários, “123456”, entre outras, de modo a se reduzir o risco de incidentes de segurança relacionados às contas de usuário.

3.3. Todas as ações executadas enquanto autenticado (seja na estação de trabalho ou nos sistemas de informática) serão de inteira responsabilidade do usuário.

3.4. A criação/atualização das contas de usuário deve ser realizado pelo setor de Tecnologia da Informação com as permissões de acesso designadas e autorizadas via e-mail, pelo superior imediato do respectivo setor, devendo possuir somente o privilégio necessário para desempenhar suas funções;

3.5. É de responsabilidade do usuário, logar os sistemas e contas de e-mail, em cada acesso, sendo vedado manter senhas salvos automaticamente;

3.6. As senhas de acesso às estações de trabalho serão atualizadas trimestralmente ou sempre que necessário, devendo o usuário cadastrar novas senhas alfanuméricas, com nível de complexidade e diferente das 2 (duas) últimas senhas criadas anteriormente.

4. DO CORREIO ELETRÔNICO E ACESSO À INTERNET

4.1. Os recursos de internet, e-mail ou qualquer outro existente ou que venham a ser adotados deverão ser utilizados em consonância com os interesses do Instituto.

4.2. Cada usuário que necessite utilizar os serviços de e-mail corporativo receberá uma conta para login no mesmo, com uma senha única, pessoal e intransferível e de responsabilidade exclusiva do titular, que deverá ser providenciada pelo setor de Tecnologia da Informação com base na solicitação, via e-mail, do superior imediato do respectivo setor;

4.3. O uso do e-mail corporativo deve ser apenas para assuntos profissionais, sendo todas as mensagens de propriedade do IPASEM-NH

4.4. É terminantemente proibido enviar ou encaminhar qualquer mensagem, seja entre usuários do Instituto ou externos, com conteúdo difamatório, ofensivo, racista, especulativo, obsceno, bullying, spams, correntes ou de qualquer natureza similar, indução religiosa, comércio, propaganda e incentivo a atos de terrorismo, ou que visem instigar, ameaças, invadir a privacidade ou prejudicar pessoas e/ou organizações;

4.5. É terminantemente proibido utilizar o e-mail corporativo e demais recursos de informática para executar quaisquer tipos de fraudes;

4.6. No caso de utilização de e-mail não institucional, através das estações de trabalho, o usuário fica ciente que tais acessos podem comprometer a segurança da informação, ficando o usuário única e exclusivamente responsável por eventuais danos gerados à instituição;

4.7. É vedado o abuso no uso do e-mail corporativo, considerando-se abuso a utilização que comprometa o desempenho do servidor em horário de trabalho, a boa imagem do IPASEM-NH e a segurança dos dados do Instituto, bem como qualquer outra forma de utilização que fuja à Legalidade, à Moralidade ou a qualquer outro princípio constitucional a que a Administração Pública esteja sujeita.

4.8. **E-mails com assuntos ou conteúdos suspeitos, de origem desconhecida, ou mesmo e-mails de origem conhecida, mas recebidos de forma inesperada ou com conteúdo suspeito, deverão ser reportados à equipe de Tecnologia da Informação antes que qualquer ação seja feita para abrir a mensagem**;

4.9. O acesso à internet pela rede interna será disponibilizado em todas as estações de trabalho em que o mesmo seja necessário para o atendimento dos objetivos institucionais do IPASEM-NH

4.10. Os casos específicos que exigirem outros acessos, diferentes dos especificados para as atividades do setor, deverão ser solicitados previamente pelo coordenador do setor solicitante, via e-mail, ao coordenador(a) do setor de Tecnologia de Informação do Instituto.

4.11. O uso da Internet para fins particulares deverá especialmente observar, além dos princípios constitucionais da Legalidade, Moralidade e demais aplicáveis, as seguintes restrições:

4.11.1. Proibição do acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados;

4.11.2. Proibição do uso de ferramentas P2P;

4.11.3. Proibição do uso de Instant Messengers não homologados/ autorizados pela equipe de Tecnologia da Informação.

4.11.4. Proibição do uso e instalação de jogos ou do download de arquivos que comprometam o tráfego da rede (vídeos, imagens, músicas, etc.), para fins particulares;

4.11.5. Proibição de uso excessivo ou abusivo, que não interfiram no cumprimento das funções do agente público, durante seu horário de expediente e/ou que comprometa o desempenho e segurança da rede de dados interna e/ou seus sistemas.

4.11.6. Será permitido o acesso à internet para o uso com fins particulares pelos agentes públicos para a utilização de Internet Bank e a sites cujo conteúdo proporcionem desenvolvimento pessoal aos agentes públicos.

4.11.7. O uso da Internet para fins particulares não deverá ser contabilizado para justificar a necessidade de aumento da capacidade de acesso do usuário, substituição de sua estação de trabalho por outra mais potente, entre outros.

4.12. O acesso poderá ser bloqueado a qualquer momento devido a critérios técnicos ou requerimento da Diretoria, sem que seja responsabilizado o Instituto por qualquer perda ou dano decorrente do bloqueio do acesso;

4.13. O IPASEM-NH não será responsabilizado por qualquer perda ou dano decorrente de alguma falha na segurança durante o acesso para fins particulares;

4.14. As conexões e conteúdos transmitidos (inclusive as de caráter recreativo e/ou para fins particulares) poderão ser monitoradas e registradas pelo setor de Tecnologia da Informação do Instituto, a qualquer momento, sem aviso prévio, independente de autorização superior, para fins de detecção de uso indevido, invasão ou malwares;

4.15. O uso da internet em desconformidade com as normas desta política, poderá ensejar responsabilidade administrativa.

5. DO USO DA INTERNET PELA REDE WI-FI

5.1. A internet pela rede Wi-Fi do Ipasem-NH, é provida pela Prefeitura de Novo Hamburgo, através do Anel Digital, disponibilizada de forma gratuita e pública em todos os Locais Públicos e Autarquias do Município.

5.2. O uso da Internet pela rede Wi-fi (Wireless Fidelity), no âmbito do IPASEM-NH, é permitido aos servidores efetivos, cedidos, comissionados, temporários, estagiários, conselheiros, segurados do Instituto, pessoal terceirizado e fornecedores;

5.3. A Política de Uso da rede Wi-fi (Wireless Fidelity), no âmbito do IPASEM-NH, especificamente para os servidores efetivos, cedidos, comissionados, temporários ou estagiários é constituída pelas seguintes regras:

5.3.1. Não usar a rede para trafegar informações confidenciais e/ou sigilosas;

5.3.2. Não infringir qualquer lei ou regulamento local, estadual, nacional ou internacional aplicável;

5.3.3. Acessar, mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos;
5.3.4. Utilizar o recurso para constranger, assediar, ameaçar ou perseguir qualquer pessoa;
5.3.5. Fazer uso ou divulgar conteúdos impróprios como: pornografia, erotismo, racista, sexista, difamatório, falsos perfis em sites pessoais ou quaisquer outros tipos de ataques dessa categoria;
5.3.6. O tempo de acesso e conteúdo acessado não interfiram no cumprimento das funções do agente público;

6. DAS ESTAÇÕES DE TRABALHO E EQUIPAMENTOS DE INFORMÁTICA

O uso das estações de trabalho do IPASEM-NH deverá observar, além dos princípios constitucionais da legalidade, moralidade, razoabilidade e demais aplicáveis, as seguintes restrições:

6.1. Cada usuário deverá utilizar uma estação de trabalho determinada, com recursos disponibilizados de acordo com a necessidade das suas atribuições;
6.2. Somente poderão ser mantidos na estação de trabalho arquivos supérfluos ou pessoais, sendo que todos os dados de produção referentes ao IPASEM-NH deverão ser mantidos no servidor central, que possui acesso com segurança e sistema de backup diário.
6.3. É proibida a instalação de softwares ou hardwares sem autorização do setor de Tecnologia da Informação, o qual poderá submeter o pedido à aprovação da Diretoria. Fica vedado também a utilização ou armazenagem de MP3, filmes, fotos e softwares com direitos autorais, ou qualquer outro tipo de pirataria.
6.4. O anti-vírus deverá estar sempre atualizado, cabendo à equipe de Tecnologia da Informação a atualização constante do mesmo.
6.5. Os usuários deverão reportar as atitudes suspeitas em sua estação de trabalho para o setor de Tecnologia da Informação, de forma que possíveis vírus sejam identificados no menor espaço de tempo possível.
6.6. Todo arquivo em mídia e/ou armazenamento móvel proveniente de entidade externa (cd, hd, pendrive), ou recebido/obtido através da rede mundial de computadores (internet), deve ser verificado por programa antivírus, executado pelo próprio usuário.
6.7. Os usuários deverão ponderar e avaliar cada ação executada, pois serão de inteira responsabilidade de cada usuário. Na dúvida sempre deverá requisitar ajuda do setor de Tecnologia da Informação.
6.8. Cada usuário deverá **bloquear** sua estação de trabalho sempre que se ausentar do ambiente de trabalho. Para Bloquear o computador o usuário pode utilizar os botões ‘CTRL + ALT + DEL’ e a opção "bloquear" ou a combinação das teclas ‘Windows’ + ” L"
6.9. As estações de trabalho e demais equipamentos de informática devem ser manuseados com cuidado, considerando que os mesmos e seus acessórios são patrimônio público. Em caso de o usuário notar alguma anormalidade ou a ausências desses, deve avisar imediatamente a

setor de Tecnologia da Informação para que sejam tomadas as devidas providências;

6.10. Não é permitida a abertura física ou a desmontagem de equipamentos de informática, exceto se realizada pelo setor de Tecnologia da Informação ou empresa autorizada;

6.11. As mudanças de local dos equipamentos de informática devem ser realizadas/supervisionadas pelo setor de Tecnologia Da Informação, com prévio aviso do supervisor do respectivo setor via e-mail, com o objetivo de evitar danos ao patrimônio;

6.12. Não é permitida a retirada de todo e qualquer equipamento que componha o parque computacional do IPASEM-NH, salvo autorização da Diretoria, ou com conhecimento do setor de Tecnologia da informação.

6.12.1. O mesmo vale para os casos de manutenção por empresa contratada/autorizada e '*Home Office'*, que somente poderão realizar a retirada do equipamento mediante preenchimento de formulário específico com assinatura de um colaborador do setor de Tecnologia da Informação e do responsável pela retirada;

6.13. Não é permitido o uso de impressoras para fins particulares;

6.14. Não é permitida a retirada de arquivos físicos ou digitais da sede do IPASEM-NH, salvo com autorização da Diretoria;

7. DO ACESSO REMOTO

7.1. Em casos excepcionais, com autorização da Diretoria e prévio aviso por e-mail ao Supervisor do setor de Tecnologia da Informação, é permitido o TeleTrabalho ou '*home office*', onde poderá ser disponibilizado equipamento do Instituto para tal atividade. O acesso deverá ser protegido no mínimo por senha, e disponibilizado através de ferramenta(s) gratuita(s) e/ou licenciada(s), devendo a(s) mesma(s) serem homologadas pelo setor de Tecnologia da Informação do Instituto~~,~~

7.2. O acesso remoto de terceiros à rede do IPASEM-NH será permitido somente para atender aos interesses do Instituto, mediante autorização e acompanhamento de um técnico do setor de Tecnologia da Informação do IPASEM-NH, com a anuência do supervisor do setor de Tecnologia da Informação ou hierarquia superior.

7.3. A(s) ferramenta(s) de conexão remota utilizada(s) por terceiros deverão ser homologadas pelo setor de Tecnologia da Informação do Instituto. Caso não sejam de uso gratuito, estas devem possuir licença de uso pelos detentores da licença.

7.4. Os terceiros que tenham acesso remoto à rede do IPASEM-NH deverão observar os seguintes requisitos, sob pena de aplicação das penalidades cabíveis:

7.4.1. Ter o seu acesso acompanhado de um técnico do setor de Tecnologia da Informação durante a execução das atividades por acesso remoto;

7.4.2. Manter sigilo das informações às quais tiverem acesso, sendo de sua total e exclusiva responsabilidade qualquer operação realizada sob suas credenciais de uso;

7.4.3. Relatar ao final da atividade remota as alterações realizadas e os possíveis impactos no funcionamento dos sistemas informatizados ou na rede de dados interna.

8. ACESSO E ARMAZENAMENTO DE ARQUIVOS NA REDE CORPORATIVA

8.1. Será disponibilizado na rede interna de dados do IPASEM-NH, um drive para cada setor do IPASEM-NH, dentro do qual serão disponibilizados diretórios/pastas, contendo as permissões necessárias para os usuários dos respectivos departamentos desempenharem suas atividades.

8.2. É de responsabilidade exclusiva dos usuários de cada setor manter, neste diretório, as informações produzidas a fim de facilitar as consultas pelos demais colegas do setor e/ou demais setores, bem como para que essas informações sejam preservadas através das rotinas de segurança e backup;

8.3. Será disponibilizado em rede, o diretório "público" para transferência e armazenamento de arquivos entre usuários com caráter temporário, **sujeitos à exclusão mensal;**

8.4. As definições das permissões de acesso dos diretórios da Rede Corporativa são definidas pela Diretoria em conjunto com o respectivo gestor de cada setor do IPASEM-NH e a configuração e implementação das permissões nos diretórios é de responsabilidade do setor de Tecnologia da Informação.

9. DAS PENALIDADES

9.1. A não observância dos preceitos da Política De Segurança Da Informação implicará aplicação de sanções administrativas, previstas na legislação em vigor. Todos os servidores, estagiários, temporários e terceirizados, que tenham acesso às informações digitais ou físicas deste Instituto, assinarão um Termo de Compromisso onde demonstram a ciência desta Política De Segurança Da Informação e de suas sanções.

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

9.2.1. Quaisquer ação ou situação que possa expor o IPASEM-NH ou seus segurados à danos à imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;

9.2.2. Utilização indevida de dados da Instituição, divulgação não autorizada de informações, sem a permissão expressa do Gestor do seu setor ou da Diretoria;

9.2.3. 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 IPASEM-NH ou de seus segurados;

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

10. DISPOSIÇÕES FINAIS

10.1. Os usuários de sistemas e serviços de informação serão instruídos a registrarem e relatarem à equipe de Tecnologia da informação, por intermédio do Gestor de cada setor, qualquer observação ou suspeita de fragilidade de segurança em sistemas ou serviços.

10.2. As evidências dos incidentes de segurança deverão ser coletadas, se possível, e enviadas para a equipe de Tecnologia da Informação preferencialmente através de e-mail corporativo.

10.3. Caberá aos terceiros e fornecedores, tomar conhecimento da Política De Segurança Da Informação do IPASEM-NH;

10.4. Fica vedada a divulgação ou reprodução de informações produzidas ou recebidas como resultado de atividade com o IPASEM-NH, sem a autorização da autoridade competente.

10.5. Os usuários deverão ser cientificados da existência da Política de Segurança da Informação e sobre o uso correto dos ativos disponibilizados ao estabelecerem vínculo com o IPASEM-NH, de forma a minimizar os possíveis riscos de segurança, bem como garantir o conhecimento de suas responsabilidades.

10.6. Todos os servidores em exercício no IPASEM-NH deverão ler esta Política de Segurança da Informação assim como receber o termo de compromisso com a Política de Segurança da Informação, mediante a assinatura e ciência do mesmo.

10.7. Todos os usuários ficam cientes de que os ambientes, sistemas, computadores e redes do IPASEM-NH poderão ser monitorados, auditados e gravados.

10.8. O IPASEM-NH exime-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos, serviços e informações, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas em processos investigatórios, bem como adotar as medidas legais cabíveis.

Parágrafo Único. O usuário que tomar conhecimento de qualquer irregularidade sobre essa Política de Segurança da Informação deverá comunicar, imediatamente, a autoridade competente do IPASEM-NH.

10.9. A Política De Segurança Da Informação e todos os atos normativos dela decorrentes deverão ser revisados, sempre que necessário, não excedendo o período máximo de 1 (um) ano.

10.10. Os casos não previstos nesta Política De Segurança Da Informação deverão ser tratados diretamente pelo setor de Tecnologia da Informação e homologados pela Diretoria.

11. PAPÉIS E RESPONSABILIDADES

11.1. **Usuários Internos e Externos**

11.1.1. Cabe aos servidores, empregados, estagiários, aprendizes, parceiros, colaboradores, prestadores de serviços, fornecedores, entre outros, do IPASEM-NH cumprir com as seguintes obrigações:

11.1.1.1. Zelar continuamente pela proteção das informações do IPASEM-NH contra acesso, modificação, destruição ou divulgação não autorizada;

11.1.1.2. Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades estatutárias do IPASEM-NH;

11.1.1.3. Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;

11.1.1.4. Zelar para que os sistemas e informações sejam utilizados de acordo com as normas estabelecidas nesta Política;

11.1.1.5. Ter ciência do conteúdo do objetivo desta Política de Segurança da Informação;

11.1.1.6. Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação.

11.1.1.7. Comunicar imediatamente ao setor de Tecnologia Da Informação qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação para devidas providências cabíveis;

11.2. **Diretoria**

11.2.1. Conscientizar, orientar e divulgar aos servidores, empregados, estagiários, aprendizes, parceiros, colaboradores, prestadores de serviços, fornecedores, entre outros, o uso seguro dos ativos do Instituto, nos termos constantes da Política de Segurança da Informação;

11.2.2. Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação entre seus colaboradores;

11.2.3. Assegurar que suas equipes possuam acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação;

11.2.4. Comunicar imediatamente ao setor de Tecnologia da Informação eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação.

11.2.5. Assegurar-se de que os servidores, empregados, estagiários, aprendizes, parceiros, colaboradores, prestadores de serviços, fornecedores, entre outros, estejam cientes da implementação da Política de Segurança da Informação;

11.2.6. Exigir dos Prestadores de Serviço contratados ou que venham a ser contratados, clausulas ou políticas de segurança da informação (LGPD) específicas nos contratos firmados, onde exista contato com informações privadas do Instituto e seus segurados. devendo se responsabilizar pelo sigilo absoluto de toda e qualquer informação que venha a ter acesso, inclusive dados que estejam contidos nos equipamentos, tratando as informações de forma confidencial, sob qualquer condição, orientando seus funcionários sobre esta conduta, sendo vedada a divulgação ou disponibilização de tais informações em qualquer meio - exceto mediante autorização prévia por parte do IPASEM/NH - estando, a CONTRATADA, sujeita a penalidades.

11.2.7. Comunicar o desligamento ou realocação de servidores, empregados e/ou estagiários para que sejam feitas as

adequações necessárias de acordo com as permissões concedidas em razão das atividades realizadas.

11.2.8. Avaliar, quando solicitado, a política, as normas e procedimentos de segurança da informação.

11.2.9. Aprovar a política e as normas de segurança da informação e suas revisões;

11.2.10. Deliberar sobre os casos de descumprimento e violação desta política de segurança da informação.

11.3. **Assessoria Jurídica**

11.3.1. Manter as áreas do IPASEM-NH informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo a gestão de segurança da informação;

11.3.2. Incluir na análise e elaboração de contratos, sempre que necessárias, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses do IPASEM-NH;

11.4. **Coordenadoria de Tecnologia da Informação**

11.4.1. Cadastrar usuários, disponibilizando acesso necessário para o desenvolvimento de suas atribuições;

11.4.2. Emitir Termo de Responsabilidade e Sigilo, colher assinatura do usuário responsável e manter arquivo em processo administrativo de Política de Segurança da Informação, para consulta a qualquer tempo;

11.4.3. Assessorar os usuários sobre dúvidas pertinentes a esta Política;

11.4.4. Monitorar a utilização das ferramentas tecnológicas, inclusive acesso à internet e rede corporativa;

11.4.5. Eliminar arquivos e programas que estejam em desacordo com as normas desta política.

11.4.6. Definir procedimentos de contingência, que determinem a existência de cópias de segurança dos sistemas informatizados e dos bancos de dados, o controle de acesso (físico e lógico) e a área responsável por elas, estando estes procedimentos mapeados e manualizados.

11.4.7. Compete ao Coordenado do setor de Tecnologia da Informação:

11.4.7.1. Propor ajustes, aprimoramentos e modificações na estrutura normativa da Política de Segurança da Informação à Diretoria;

11.4.7.2. Redigir o texto das normas e procedimentos de segurança da informação, submetendo à aprovação da Diretoria;

11.4.7.3. Requisitar informações das demais áreas do IPASEM-NH, com o intuito de verificar o cumprimento da política, das normas e procedimentos de segurança da informação;

11.4.7.4. Receber e analisar casos de violação da política e das normas e procedimentos de segurança da informação;

11.4.7.5. Notificar à Diretoria quanto a casos de violação da política e das normas e procedimentos de segurança da informação;
11.4.7.6. Receber sugestões dos usuários para implantação de normas e procedimentos de segurança da informação;
11.4.7.7. Propor projetos e iniciativas relacionadas à melhoria da segurança da informação;
11.4.7.8. Supervisionar o andamento dos projetos e iniciativas relacionados à segurança da informação;
11.4.7.9. Coordenar a gestão dos ativos da informação, bem como a gestão dos riscos relacionados à segurança da informação.