Política de Segurança da Informação

A Política de Segurança da Informação (PSI) é o documento que orienta e estabelece as diretrizes corporativas do Regime Próprio de Previdencia Social (RPPS) para a proteção dos ativos de informação e a responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da Autarquia e por todos os servidores e prestadores de serviço que tenham acesso às informações de propriedade do RPPS.

Aplica-se à esta Política de Segurança da Informação as normas gerais e princípios relativos à razoabilidade, eficiência, ética e bons costumes, aplicando-se, no que couber, os dispositivos constantes no Código de Ética desta Autarquia.

Objetivos da PSI:

I - estabelecer diretrizes que permitam aos servidores e fornecedores do RPPS seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da Autarquia e do indivíduo;

II - nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento; e

III - preservar as informações do RPPS quanto à:
a) Confidencialidade: Proteção e garantia de que determinadas informações só são disponíveis a pessoas autorizadas.
b) Integridade: Garantia da exatidão das informações e dos métodos de processamento.
c) Disponibilidade: Garantia de que os usuários autorizados e os interessados tenham acesso às informações.

Aplicações da PSI:

As diretrizes aqui estabelecidas deverão ser seguidas por todos os servidores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

É obrigação de cada servidor se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Responsabilidades Específicas:

Entende-se por servidor toda e qualquer pessoa física, contratada no regime estatutário, CLT ou temporário, e os prestadores de serviço, contratados por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora do RPPS.

Os servidores deverão:

I - manter sigilo das informações do RPPS;

II - zelar pelos ativos de informação do RPPS, sejam eles físicos (processos, documentos, etc) ou digitais (arquivos, sistemas, etc); e

III - seguir as diretrizes e recomendações do IPREMU quanto ao uso, divulgação e descarte de dados e informações.

Será de inteira responsabilidade de cada servidor, todo prejuízo ou dano que vier a sofrer ou causar ao RPPS e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

O acompanhamento dos procedimentos de backups e de contigência será desempenhado por servidor do quadro do IPREMU, designado por ato da diretoria.

Monitoramento e da auditoria do ambiente:

Para garantir as regras mencionadas nesta PSI, o IPREMU poderá:

I - implantar sistemas de monitoramento nas estações de trabalho, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede - a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

II - tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação do superior hierárquico;

III - realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade; e

IV - instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

Correio Eletrônico (e-mail):

O uso do correio eletrônico do RPPS é para fins corporativos e relacionados às atividades do servidor usuário da Autarquia, sendo terminantemente proibido:

I - enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Autarquia;

II - enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

III - enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o RPPS vulneráveis a ações civis ou criminais;

IV - divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

V - falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

VI - apagar mensagens pertinentes de correio eletrônico quando o RPPS estiver sujeito a algum tipo de investigação;

VII - produzir, transmitir ou divulgar mensagem que:
a) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do RPPS;
b) contenha ameaças eletrônicas, como: spam, vírus de computador;
c) contenha arquivos com código executável ou qualquer outra extensão que represente um risco à segurança;
d) vise obter acesso não autorizado a outro computador ou rede;
e) vise interromper um serviço ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
f) vise burlar qualquer sistema de segurança;
g) vise vigiar secretamente ou assediar outro usuário;

h) vise acessar informações confidenciais sem explícita autorização do proprietário;
i) vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
j) inclua imagens criptografadas ou de qualquer forma mascaradas;
k) tenha conteúdo considerado impróprio, obsceno ou ilegal;
l) seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
m) contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
n) tenha fins políticos locais ou do país (propaganda política);
o) inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com os seguintes dados:

I - Nome do servidor;
II - Cargo/Departamento;
III - Nome da Autarquia;
IV - Telefone(s); e
V - Site do RPPS na internet.

O Diretor-geral ou outro servidor designado poderá definir o formato da assinatura de que trata este artigo, obrigando sua utilização por todos os usuários do correio eletrônico.

Internet:

Exige-se dos servidores usuários comportamento eminentemente ético e profissional no uso da internet.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do IPREMU, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Qualquer informação acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria, tendo o RPPS, em total conformidade legal, o direito de monitorar e registrar todos os acessos a ela.

Qualquer alteração dos parâmetros de segurança, por qualquer servidor, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao servidor e ao respectivo superior hierárquico.

O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a Autarquia cooperará ativamente com as autoridades competentes.

O uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os servidores que estão devidamente autorizados a falar em nome do RPPS para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os servidores autorizados pela Autarquia poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os servidores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no RPPS e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pelo seu respectivo diretor.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

Os servidores não poderão em hipótese alguma utilizar os recursos do RPPS para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

É proibido o acesso, exposição, armazenamento, distribuição, edição, impressão ou

gravação por meio de qualquer recurso, de materiais de cunho sexual.

Os servidores não poderão utilizar os recursos do RPPS para deliberadamente propagar qualquer tipo de vírus, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

As regras expostas aqui se aplicam ao uso de computadores e outros dispositivos de propriedade do RPPS, bem como a dispositivos particulares dos usuários que estiverem conectados à internet do RPPS (cabeada ou semfio).

Computadores e outros dispositivos:

Os computadores disponibilizados pelo IPREMU aos servidores, constituem instrumento de trabalho para execução das atividades do RPPS.

Cada servidor deve zelar para segurança e bom uso dos equipamentos, reportando à área competente qualquer incidente que tenha conhecimento.

Em caso de mau uso, ou uso em desacordo com as instruções desta norma, o servidor poderá ser responsabilizado.

Identificação e controle de acesso:

Para o acesso aos recursos tecnológicos do IPREMU será exigido, sempre que possível, identificação e senha exclusiva de cada servidor, permitindo assim o controle de acesso. É proibido o compartilhamento de login entre os servidores. Recomenda-se como boa prática de segurança que, ao realizar o primeiro acesso ao ambiente de rede local, o usuário seja direcionado a trocar imediatamente a sua senha.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Backup e contingência

Todas as cópias de segurança (backups) serão gerenciadas e executadas por sistemas de agendamento automatizado, executados preferencialmente fora do horário comercial, nas

chamadas “janelas de backup” - períodos em que não há nenhum ou pouco acesso de usuários. Quando a instalação for realizada em ambiente sob responsabilidade do IPREMU, deverão ser realizadas cópias de segurança do banco de dados diariamente, e pelo menos 1 (uma) vez por semana dos arquivos de execução do sistema informatizado. Quando a instalação do sistema for realizada em ambiente terceirado, por exemplo, em data center ou na “nuvem”, deverão ser garantidos, em contrato, os mesmos requisitos previstos para o ambiente IPREMU.