ANEXO II
DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO **Câmara Municipal de Pato Branco**	Versão: **1.0**
	Nível de confidencialidade: ( ) Público (X) Restrito ( ) Confidencial	Atualização: **12/11/24**

SUMÁRIO

HISTÓRICO DE VERSÕES			
Data	**Versão**	**Descrição**	**Autoria**
11/09/2024	1.0	Política de Segurança da Informação	Luana Varaschim Perin

1. DOS OBJETIVOS

1.1 A Política de Segurança da Informação (POSIN) institui diretrizes, responsabilidades e competências visando a assegurar a confidencialidade, disponibilidade, integridade e autenticidade das informações e comunicações, bem como a conformidade, padronização e normatização das atividades de gestão de segurança da informação e comunicações no âmbito da Câmara Municipal de Pato Branco.

2. DA ABRANGÊNCIA

2.1 Ficam submetidos a esta Política de Segurança da Informação todos os servidores, colaboradores, estagiários, prestadores de serviços e demais agentes públicos ou privados que tenha qualquer tipo de acesso aos dados ou informações oriundas da Câmara Municipal de Pato Branco, sob pena de responsabilidade, conforme previsto na legislação brasileira.

3. DOS TERMOS E DEFINIÇÕES

I. Agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública e equipara-se a agente público quem trabalha para empresa prestadora de serviços contratada ou conveniada para a execução de atividade, de qualquer natureza, desenvolvida na Câmara Municipal de Pato Branco;

II. Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

III. Áreas restritas: são locais dentro da Câmara Municipal de Pato Branco onde o acesso é controlado e limitado a pessoas autorizadas, devido à natureza sensível ou crítica das atividades ou informações ali presentes. Essas áreas incluem: sala de servidores, arquivos, salas de segurança, áreas com equipamentos críticos, centros de processamento de dados, etc.

IV. Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

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

VI. Backup: é a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados;

VII. Confidencialidade: é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;

VIII. Integridade: é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

IX. Disponibilidade: garante que as informações e recursos estejam disponíveis quando necessários.

X. Firewall: É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede;

XI. Incidente de segurança da informação: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação, de computação ou das redes de computadores;

XII. Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros;

XIII. Modem 3G: É um dispositivo sem fio, com saída USB para conexão em outro dispositivo tais como Tablets (com suporte 3G), notebooks, netbooks, desktops, etc. objetivando conexão com a internet. O modem 3G recebe e decodifica o sinal digital de alta velocidade transmitido pelas operadoras de celulares para aparelhos portáteis (celulares, smartphones e notebooks) compatíveis com a tecnologia 3G;

XIV. Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares;

XV. TI: Tecnologia da Informação.

4. NÍVEIS DE CONFIDENCIALIDADE DE INFORMAÇÕES E DOCUMENTOS

4.1 As informações e documentos existentes são classificadas de acordo com os seguintes níveis de confidencialidade:

I. Público: É uma informação ou documento da Câmara Municipal de Pato Branco com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter legal, informativo, educativo ou promocional. É destinada ao público externo

ou cidadãos ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

II. Restrito: É uma informação ou documento da Câmara Municipal de Pato Branco que o órgão não tem obrigação legal de divulgar, onde o acesso por parte de indivíduos externos à organização 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 agentes públicos da Câmara Municipal de Pato Branco.

III. Confidencial: É uma informação crítica que está acessível apenas a servidores ou agentes públicos previamente definidos, sempre associados aos interesses estratégicos da Câmara Municipal de Pato Branco. É sempre restrita a um grupo específico de pessoas. Dados Pessoais, ou seja, toda informação relacionada a pessoa natural identificada ou identificável, neste contexto aplicável também à dados pessoais sensíveis, isto é, toda informação sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, são informações confidenciais.

5. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

5.1 Cabe a todos os agentes públicos:

I. Cumprir fielmente esta Política;

II. Buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação;

III. Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados;

IV. Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo órgão;

V. Comunicar imediatamente o órgão quando do descumprimento ou violação desta política, através da Ouvidoria.

5.2 Cabe às Diretorias, Gerências e Coordenações:

I. Cumprir, disponibilizar os recursos e orçamento necessários e fazer cumprir esta

Política;

II. Assegurar que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação;

III. Comunicar imediatamente eventuais casos de violação de segurança da informação à Ouvidoria.

5.3 Cabe ao Comitê de Privacidade e Proteção de Dados:

I. Propor ajustes, melhorias, aprimoramentos e modificações desta Política;

II. Convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política;

III. Prover todas as informações de gestão de segurança da informação solicitadas por Gestores;

IV. Observar o Plano de Resposta à Incidentes e Remediação e servir como equipe para execução do mesmo.

6. PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

6.1 As normas e procedimentos que complementam esta Política de Segurança da Informação abordam a segurança física e lógica, conforme os aspectos a seguir:

I. Segurança do Ambiente Físico;

II. Segurança do Ambiente Lógico:

a) Acesso à Rede;
b) Estação de Trabalho;
c) Uso da Internet;
d) Controles de Acesso;
e) Credenciais de Acesso e Senhas;
f) Backups (Cópias de Segurança)
g) Programas
h) Equipamentos Particulares e Dispositivos Móveis;
i) Dos Usos de Computação em Nuvem;
j) E-mail Corporativo;
k) Mídias Removíveis e Portas USB.

6.2 O órgão deverá assegurar que todas as transferências internacionais de dados pessoais sejam realizadas em conformidade com Procedimento para Transferência

Internacional de Dados.

7. DA SEGURANÇA DO AMBIENTE FÍSICO

7.1 Disposições Gerais

7.1.1 A segurança física se baseia no acesso físico das pessoas aos ambientes que possuam equipamentos de tecnologia da informação e/ou tratem ou armazenem informações e tem como escopo garantir a proteção da informação contra violações e acessos não autorizados, permitindo a circulação apenas de pessoas treinadas, capacitadas e autorizadas.

7.2 Controle de Acesso Físico

7.2.1 Toda e qualquer pessoa que necessitar ingressar na Câmara Municipal de Pato Branco, além do Plenário e das áreas destinadas ao atendimento ao público, deverá ser devidamente identificada nas áreas de recepção. O acesso deve ser concedido apenas para finalidades específicas e autorizadas.

7.2.2 Todo e qualquer acesso de terceiros às dependências internas da Câmara Municipal de Pato Branco deverá ser acompanhado durante toda sua permanência por um servidor do órgão.

7.2.3 É vedada a entrada de qualquer pessoa não autorizada nas dependências internas da Câmara Municipal de Pato Branco.

7.2.4 O acesso às dependências da Câmara Municipal de Pato Branco com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar fora do ambiente da Plenária e saguão só pode ser feito a partir de autorização expressa da Diretoria Geral ou Presidência e mediante supervisão, exceto para eventos e treinamentos organizados pelo próprio órgão.

7.2.5 O acesso às áreas restritas é franqueado apenas aos agentes públicos autorizados da Câmara Municipal de Pato Branco, devendo ser protegido a evitar acesso não autorizado.

7.2.6 Deve ser mantido registro detalhado de todos os acessos físicos às áreas restritas, incluindo data, hora e identidade do indivíduo que acessou as instalações.

7.3 Ameaças Ambientais

7.3.1 Compete ao Departamento de Administração assegurar o funcionamento adequado do suprimento de energia elétrica, telecomunicações e ar-condicionado, protegidos

contra incêndios e alagamentos.

7.3.2 Os locais que armazenem informações restritas devem estar equipados com sistemas de detecção e combate a incêndios adequados, incluindo alarmes, extintores de incêndio e, quando necessário, sistemas de supressão de incêndios que não danifiquem equipamentos eletrônicos.

7.3.3 As salas de servidores e outros locais críticos devem ter sistemas de controle ambiental para manter níveis adequados de temperatura e umidade, prevenindo danos aos equipamentos e dados.

7.3.4 Áreas de armazenamento de dados e equipamentos essenciais devem ser protegidas contra inundações, com medidas como instalação de barreiras físicas e sistemas de drenagem adequados.

7.3.5 Todos os sistemas de proteção ambiental devem ser sujeitos a manutenção preventiva regular, garantindo que estejam sempre operacionais e eficientes.

7.4 Gestão de Ativos Físicos

7.4.1 Deverá ser mantido e atualizado regularmente inventário completo de todos os ativos físicos que armazenam ou processam informações restritas.

7.4.2 Equipamentos que armazenem informações restritas devem ser descartados de maneira segura, utilizando métodos de destruição que garantam que os dados não possam ser recuperados.

7.4.3 Os documentos impressos e anotações que precisem estar em um papel devem permanecer nas mesas em caráter temporário devendo ser recolhidos em compartimentos fechados disponíveis em seu departamento ou qualquer dependência da organização que forneça segurança e proteção a esses materiais.

7.4.3.1 Toda informação que permanecer nas mesas poderá e deverá ser destruída pelo agente público responsável ou por qualquer outro agente público que assim o quiser fazê-lo exercitando as boas práticas de proteção de informações da organização.

7.4.4 Os documentos órfãos notoriamente importantes (que possuem assinaturas, por exemplo) deverão ser depositados em um armário ou gaveta designada pelo Departamento de Administração para que possam ser revisados posteriormente antes de sua destruição segura.

8. DA SEGURANÇA DO AMBIENTE LÓGICO

8.1 Disposições Gerais

8.1.1 Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado. Os dados, as informações e os sistemas de informação da entidade devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, confidencialidade e disponibilidade desses bens.

8.2 Estações de Trabalho

8.2.1 Constituem estações de trabalho os computadores e notebooks registrados como patrimônio do órgão e utilizados pelos servidores no desempenho de suas atividades funcionais. As seguintes medidas de segurança que devem ser adotadas quanto à utilização das estações de trabalho:

I. Tudo que for executado na estação de trabalho é de responsabilidade do agente público a quem pertence;

II. Fica proibida a instalação, modificação ou desinstalação de hardwares e softwares sem a autorização do Setor de Tecnologia da Informação. Qualquer software que, por necessidade do serviço, necessitar ser instalado deverá ser comunicado ao Setor de Tecnologia da Informação, para que o mesmo possa ser homologado e disponibilizado para a área requerente;

III. Somente devem ser utilizados softwares devidamente licenciados;

IV. Ao se ausentar da estação de trabalho, o agente público deve efetuar o bloqueio ou “logoff” da mesma, evitando assim o acesso indevido de outra pessoa à estação de trabalho através do seu usuário (login);

V. O acesso à estação de trabalho deverá ser encerrado no final do expediente, desligando-se o equipamento;

VI. As estações de trabalho devem sofrer bloqueio automático depois de 10 minutos de inatividade;

VII. As configurações de segurança de estações de trabalho não devem ser alteradas, desativadas ou ignoradas pelo agente público;

VIII. Informações restritas, confidenciais ou cuja divulgação possa causar ao órgão só devem ser manipuladas em equipamentos com controles adequados;

IX. A liberação do dispositivo móvel (notebook, tablets ou celulares) será permitida após os solicitantes assinarem o acordo de conhecimento das suas responsabilidades;

X. Em caso de furto/roubo ou perda do dispositivo móvel, o servidor deverá comunicar imediatamente à Diretoria Geral, bem como deverá ser tal fato registrado em boletim de ocorrência junto às autoridades policiais;

XI. As estações de trabalho devem ser utilizadas somente para o exercício funcional;

XII. A proteção antivírus das estações de trabalho devem ser atualizadas regularmente;

XIII. A varredura por vírus é dever do agente público e deverá ser constantemente executada nas estações e nos servidores.

8.3 Equipamentos Particulares e Dispositivos Móveis

8.3.1 Ficam estabelecidas as seguintes regras para o uso de equipamentos particulares e de dispositivos moveis:

I. A liberação para utilização de notebooks e para acesso à internet do órgão se dará mediante solicitação justificada e assinatura do termo de compromisso, vide anexo I;

II. É proibida a inclusão de smartphones na rede corporativa, a inclusão desses equipamentos se dará conforme disposto nesta Política.

8.3.2 Os dispositivos de usuário final utilizados pelo órgão deverão ter criptografia implementada para proteger os dados armazenados contra acessos não autorizados. A criptografia deverá seguir as melhores práticas do mercado e estar em conformidade com as normativas de segurança vigentes.

8.3.3 Os dispositivos móveis adquiridos pelo órgão deverão ser configurados para ocorrer o bloqueio automático após 2 minutos de inatividade.

8.4 Mídias Removíveis e Portas USB

8.4.1 O uso de mídias removíveis não órgão não é estimulado, devendo ser tratado como exceção à regra.

8.4.2 É vedada a transferência de informações das estações de trabalho para

dispositivos de armazenamento externo, como pendrives e discos rígidos externos, sem a autorização da Diretoria Geral.

8.4.3 Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos que podem danificar e corromper dados, além de serem passíveis de extravio.

8.4.4 É vedado aos agentes públicos utilizarem as mídias removíveis como meio preferencial de armazenamento de informações corporativas.

8.5 Acesso à Rede

8.5.1 Os agentes públicos terão acesso única e exclusivamente àqueles recursos da rede corporativa que lhe forem indispensáveis à realização de suas atividades.

8.5.2 Os serviços e sistemas autenticados serão disponibilizados para os usuários registrados e identificados pelo seu login e senha.

8.5.3 Cada unidade de lotação terá uma unidade de armazenamento em rede para os usuários lotados na respectiva área de atuação, com acesso de leitura e gravação.

8.5.4 O órgão disponibilizará o acesso à rede de internet sem fio (Wi-Fi) a seus visitantes e agentes públicos, o ingresso a rede se dará mediante cadastro quando solicitado o acesso. A rede de internet sem fio (Wi-Fi) será segregada, garantido assim o isolamento da rede interna do órgão.

8.5.5 Material sexualmente explícito não pode ser acessado, exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa.

8.5.6 Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc..) nos drivers de rede.

8.6 Uso da Internet

8.6.1 A concessão de acesso à internet em ambiente laboral na Câmara Municipal de Pato Branco será disponibilizada como ferramenta de trabalho destinada ao atendimento das finalidades institucionais do órgão.

8.6.1.1 O uso da internet no órgão poderá ser monitorado e os acessos serão registrados em dispositivo ou sistema computacional que assegure a possibilidade de rastreio e apuração de responsabilidades em caso de incidentes cibernéticos, incidentes de segurança e outras violações à esta Política.

8.6.1.2Para apuração das quebras de segurança de que trata o *caput*, os ativos de informação fornecidos pelo órgão poderão ser analisados, a qualquer tempo, pelo Departamento de Tecnologia da Informação.

8.6.2 O uso de Internet deve ocorrer apenas através da arquitetura segura definida pelo Setor de Tecnologia da Informação, devendo ser acessada por meio da rede local da organização com a infraestrutura adequada e proteção do firewall.

8.6.3 Deverão ser utilizadas conexões cifradas (TLS/HTTPS) ou aplicativos com criptografia ponta-a-pronta para serviços de comunicação.

8.6.4 Fica proibido ao agente público alterar as configurações do navegador da sua estação de trabalho no que diz respeito aos parâmetros de segurança. Havendo necessidade, o Setor de Tecnologia da Informação deve ser acionado para informar o procedimento a ser seguido.

8.6.5 O acesso às páginas e websites é de responsabilidade de cada usuário ficando vedado o acesso a sites com conteúdos impróprios e de relacionamentos.

8.6.6 O agente público deve se certificar da procedência do site e a utilização de conexões seguras (criptografadas) ao realizar transações via internet.

8.6.7 O agente público deve verificar se o certificado do site ao qual se deseja acessar é íntegro e corresponde realmente aquele site, observando ainda, se o mesmo está dentro do prazo de validade.

8.6.8 O agente público deve certificar que o endereço apresentado no navegador corresponde ao sítio que realmente quer acessar, antes de realizar qualquer ação ou transação.

8.6.9 O agente público deve digitar no navegador o endereço desejado e não utilizar links como recurso para acessar um outro endereço destino.

8.6.10 O acesso à internet poderá ser monitorado pelo Setor de Tecnologia da Informação.

8.6.11 É vedada a transferência ou cópia de arquivos de vídeo, som, ou quaisquer outros tipos de arquivos que não sejam relacionados aos interesses do órgão.

8.7 Controle de Acesso

8.7.1 Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados, concedendo-se permissão apenas aos recursos necessários e indispensáveis ao desempenho de suas funções, definidas pela chefia imediata aplicando-se o princípio do menor privilégio (*need to know*). O responsável pela autorização deve ser claramente definido e ter registrado a

aprovação concedida.

8.7.2 Todo usuário deverá possuir identificação pessoal e intransferível, qualificando-o, inequivocamente, como responsável por qualquer atividade desenvolvida sob essa identificação.

8.8 Credenciais de Acesso e Senhas

8.8.1 Todo agente público deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação.

8.8.2 É dever do agente público manter sigilo e trocar periodicamente a senha pessoal de acesso aos sistemas do órgão, bem como não divulgar a terceiros suas credenciais, além de não utilizar a identificação de acesso e senha de terceiros.

8.8.3 É dever do agente público utilizar senha de qualidade, com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos). Não deverão ser utilizadas informações pessoais fáceis de serem obtidas como o nome, o número de telefone ou data de nascimento como senha.

8.8.4 A senha inicial, quando gerada pelo sistema, deve ser trocada pelo agente público no primeiro acesso.

8.8.5 As credenciais de acesso não podem ser deixadas em notas postadas sobre ou sob as estações de trabalho, nem escritas em locais acessíveis a terceiros.

8.8.6 É obrigatório o uso de autenticação multifator (2FA ou MFA; Two factor Authentication ou MultiFactor Authentication) para todos os serviços onde a opção estiver disponível.

8.9 E-mail Corporativo

8.9.1 O serviço de correio eletrônico (e-mail corporativo) é permitido somente para as atividades profissionais de seus usuários, não sendo permitido enviar ou arquivar mensagens que não estejam relacionadas ao atendimento das finalidades institucionais do órgão ou que:

I. Contenham assuntos que provoquem assédio, perturbação a outras pessoas ou que prejudiquem a imagem do Iprev/DF;

II. Contenham temas difamatórios, discriminatórios, calunioso, degradante, ofensivo, violento, ameaçador, material obsceno, material pornográfico, ilegal ou antiético;

III. Contenham fotos, imagens, sons ou vídeos que não tenham relação com as finalidades institucionais do órgão;

IV. Compartilhem arquivos com códigos executáveis (.exe, .cmd, .pif, .js, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que possa apresentar risco a segurança da informação do órgão.

8.9.2 É vedada a instalação ou utilização de outras soluções de e-mail que não as oficialmente disponibilizadas pelo Setor de Tecnologia da Informação.

8.10 Aplicativos de Mensageria

8.10.1 É vedado o envio de documentos com informações restritas e/ou confidenciais através de aplicativos de mensageria não autorizados ou sem criptografia adequada (como WhatsApp, por exemplo). Em vez disso, deve-se utilizar canais de comunicação seguros, aprovados pelo Setor de Tecnologia da Informação, que garantam a proteção dos dados em trânsito e estejam em conformidade tanto com a Política de Privacidade quando esta Política.

8.11 Backups (Cópias de Segurança)

8.11.1 Os procedimentos de backup deverão ser fixados por norma interna de segurança da informação do órgão.

8.11.2 O serviço de backup deverá ser automatizado por sistemas informacionais próprios, considerando, inclusive, a execução agendada fora do horário de expediente.

8.11.3 A solução de backup deverá ser testada regularmente e mantida sempre atualizada, considerando suas diversas características, tais como atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros.

8.11.4 O órgão deve possuir pelo menos 3 cópias dos dados, armazená-las em pelo menos 2 tipos de mídia diferentes e manter pelo menos 1 das cópias em um local fora das dependências da Câmara Municipal de Pato Branco.

8.12 Gestão de Ativos Digitais

8.12.1 Não poderão ser executados softwares que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

8.12.2 Não poderão ser executados programas, instalados equipamentos, armazenados arquivos ou promovidas ações que possam facilitar o acesso de usuários não autorizados à rede corporativa do órgão.

8.12.3 Deverá ser realizada a desinstalação ou desativação periódica de serviços desnecessários nos ativos e softwares do órgão, garantindo que apenas os serviços essenciais para o funcionamento das atividades permaneçam ativos. Esta prática deve ser revisada regularmente para assegurar a otimização da segurança dos sistemas.

8.12.4 O órgão deverá garantir a implementação de mecanismos de coleta de logs do provedor de serviços, incluindo a captura de eventos de autenticação e autorização. Esses logs deverão ser armazenados de forma segura e analisados regularmente para detecção de atividades suspeitas ou não autorizadas.

8.12.5 O órgão deverá implementar um processo semanal para a identificação e tratamento de ativos não autorizados, garantindo a remoção ou regularização desses ativos conforme as políticas internas estabelecidas. Este processo incluirá a atualização contínua do inventário de ativos e a validação de suas autorizações. Qualquer exceção deverá ser formalmente documentada e aprovada pela equipe responsável pela segurança da informação.

8.13 Dos Uso de Computação em Nuvem

8.13.1 A implementação ou contratação de computação em nuvem deverá estar em conformidade com as diretrizes desta Política e com a legislação sobre contratação vigente no órgão.

8.13.2 O uso de recursos de computação em nuvem para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação será regido por norma interna de segurança da informação que deverá ser instituída pela unidade responsável pelos ativos de tecnologia e atenderá às determinações desta Política.

8.13.3 Fica vedado o uso de recurso de computação em nuvem não disponibilizado pelo órgão para o armazenamento de ativo de informação institucional.

8.13.4 O uso da computação em nuvem deverá promover:

I. melhorias no ambiente computacional do órgão;

II. facilidade e agilidade na implementação;

III. diminuição de vulnerabilidades pela atualização constante de aplicações defasadas;

IV. possibilidade de integração à outras soluções;
V. melhoria da gestão da segurança da informação; e
VI. redução de custos.

9. DA CONSERVAÇÃO E ELIMINAÇÃO

9.1.9. Os prazos de guarda da documentação contendo Informações Restritas e Confidenciais devem seguir estritamente a Tabela de Temporalidade do órgão.

9.1.10. Após o término do prazo de guarda estabelecido na Tabela de Temporalidade, as Informações Restritas e Confidenciais devem ser descartadas de forma segura e irreversível, garantindo que não possam ser recuperadas ou identificadas.

9.1.11. O descarte de Informações Restritas e Confidenciais contidas em documentos físicos deve ser realizado por meio de trituração ou incineração, de forma que os dados não possam ser reconstruídos.

9.1.12. Para documentos eletrônicos, deve-se utilizar técnicas de exclusão segura que garantam a impossibilidade de recuperação dos dados, tais como a sobrescrita de dados ou a destruição física dos dispositivos de armazenamento.

9.1.13. Todos os processos de descarte de Informações Restritas e Confidenciais devem ser devidamente documentados, incluindo a data, o método de descarte e o responsável pela execução.

9.1.14. É responsabilidade de todos os agentes públicos garantirem que o descarte de Informações Restritas e Confidenciais seja realizado de acordo com esta Política e com a Tabela de Temporalidade.

9.1.15. Qualquer incidente ou não conformidade relacionada ao descarte de Informações Confidenciais envolvendo Dados Pessoais deve ser reportado imediatamente ao Encarregado pelo Tratamento de Dados Pessoais para a devida investigação e correção.

10. DA GESTÃO DE INCIDENTES

10.1 O órgão deverá estabelecer e manter um Plano de Respostas a Incidentes que inclua a designação de uma equipe de gestão de incidentes, composta por agentes públicos designados. O plano deverá abranger funções e responsabilidades, requisitos de conformidade e estratégias de comunicação. Além disso, deverá ser implementado um processo contínuo para atualizar as informações de contato relevantes para a

comunicação durante incidentes de segurança, bem como a realização de exercícios regulares de resposta a incidentes para testar a eficácia dos canais de comunicação e dos recursos técnicos. Após a resolução de cada incidente, deverá ser realizada uma análise pós-incidente para identificar lições aprendidas e definir ações de acompanhamento necessárias.

11. DAS CONDUTAS VEDADAS

11.1 Além das demais condutas não permitidas insertas nesta Política, é proibido:

I. Introduzir códigos maliciosos nas redes e sistemas do órgão;

II. Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas etc.) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;

III. Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas do órgão;

IV. Tentar interferir sem autorização em um serviço, sobrecarregá-lo ou, ainda, desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos;

V. Alterar registro de evento dos sistemas, informações ou dados;

VI. Modificar qualquer dado, configuração, protocolos de comunicação, sem a expressa autorização da Diretoria Geral ou Presidência;

VII. Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas do órgão;

VIII. Monitorar ou interceptar o tráfego de dados nos sistemas sem as devidas autorizações;

IX. Violar medida de segurança ou de autenticação, sem as devidas autorizações;

X. Fornecer informações a terceiros sobre usuários ou serviços disponibilizados nos sistemas do órgão, exceto os de natureza pública ou mediante autorização de autoridade competente;

XI. Compartilhar ou viabilizar o compartilhamento, sem autorização da Presidência ou Diretoria Geral, de informações classificadas como restritas ou confidenciais, bem como dados pessoais;

XII. Enviar informações do órgão para endereços particulares de e-mail;

XIII. Utilizar uma impressora coletiva para gerar informações confidenciais e não recolher o documento impresso imediatamente;

XIV. Discutir ou comentar assuntos confidenciais em locais públicos;

XV. Discutir ou comentar assuntos confidencias com pessoas não autorizadas;

XVI. Utilizar as informações do órgão para obter ganhos pessoais;

XVII. Armazenamento ou uso de jogos em computador ou sistema informacional do órgão.

12. DAS PENALIDADES

12.1.1. A violação das regras estabelecidas nesta Política ou suas normas internas de segurança, por qualquer pessoa física ou jurídica, acarretará as penalidades civis, penais e administrativas previstas na legislação, conforme o caso.

12.1.2. Para os agentes públicos, pode acarretar na aplicação de advertência, suspensão, desligamento formal ou rescisão contratual sem prejuízo das penalidades civis, penais e administrativas previstas na legislação, conforme o caso.

13. VIGÊNCIA E VALIDADE

13.1.1. Esta Política, suas normas internas de segurança e suas atualizações deverão ser divulgadas amplamente aos agentes públicos do órgão.

13.1.2. Esta Política, bem como todas as normas dela decorrentes, deverão ser revisadas e atualizadas sempre que se fizer necessário, não excedendo o período máximo de dois anos.

13.1.3. Os integrantes do Comitê de Privacidade e Proteção de Dados (CPPD) poderão expedir instruções complementares, no âmbito de suas competências, que detalharão suas particularidades e procedimentos relativos à Segurança da Informação alinhados às diretrizes emanadas pelo CPPD e aos respectivos Planos Estratégicos Institucionais da Câmara Municipal de Pato Branco.

13.1.4. Casos omissos serão resolvidos pelo Comitê de Privacidade e Proteção de Dados (CPPD), ao qual também serão submetidas eventuais dúvidas sobre esta Política e seus documentos.

13.1.5. Esta Política entra em vigor na data de sua publicação.

ANEXO III
TERMO DE CIÊNCIA E RESPONSABILIDADE

Eu, nome, nacionalidade, estado civil, profissão, inscrito no CPF nº XXX.XXX.XXX-XX, declaro ciência de que, durante o exercício do mandato parlamentar de vereador na _____ª Legislatura da Câmara Municipal de Pato Branco, quando realizar atividades de tratamento de dados pessoais relacionadas ao desempenho do mandato por vereadores, lideranças, bancadas, blocos e frentes parlamentares, em que não forem utilizados sistemas institucionais da Câmara Municipal de Pato Branco, exercerei as atribuições de controlador de dados pessoais, nos termos da Lei Federal nº 13.709/2018 (LGPD).

Pato Branco, _____ de _____ de 20___.

_____
Nome
Vereador