DECRETO Nº 2.411, DE 19 DE ABRIL DE 2021.

"Institui a Política de Segurança da Informação no âmbito da administração direta no Município e cria a Comissão Gestora da Tecnologia da Informação e Comunicação da Prefeitura Municipal de Santo Antônio do Pinhal"

ANDERSON JOSÉ MENDONÇA, Prefeito do Município de Santo Antônio do Pinhal, Estado de São Paulo, no uso de suas atribuições legais que lhe são conferidas no disposto na Lei Orgânica Municipal, e

CONSIDERANDO a necessidade de garantir a segurança das informações geradas, adquiridas, processadas, armazenadas e transmitidas no âmbito da administração municipal, de forma a atender aos princípios da confidencialidade, integridade, disponibilidade, autenticidade e legalidade;

CONSIDERANDO que os agentes públicos devem zelar pelas informações que lhes são confiadas no exercício de suas funções e

CONSIDERANDO que as ações de Segurança da Informação reduzem custos e riscos e aumentam os benefícios prestados aos cidadãos, ao permitir a oferta de processos, produtos e serviços suportados por sistemas de informações mais seguros;

DECRETA:

Art. 1º - Por este Decreto fica estabelecida a Política de Segurança da Informação, conforme disposições contidas no Anexo Único.

Art. 2º - Este Decreto entra em vigor na data de sua publicação.

Art. 3º - Ficam revogadas as disposições em contrário.

Prefeitura Municipal da Estância Climática de Santo Antônio do Pinhal, em 19 de abril de 2021.

ANDERSON JOSÉ MENDONÇA
Prefeito Municipal

Publicado e registrado na Secretaria Municipal de Administração da Prefeitura Municipal, em 19 de abril de 2.021.

LUCAS DIEGO E SILVA SANTOS
Secretário Municipal de Administração

ANEXO ÚNICO

Sumário

CAPÍTIULO I - OBJETIVOS

Estabelecer diretrizes que permitam aos servidores e demais usuários da Prefeitura do Município de Santo Antônio do Pinhal seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da Prefeitura e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações desta Prefeitura quanto à:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário

CAPÍTULO II - COMISSÃO GESTORA DE SEGURANÇA DA INFORMAÇÃO (C.G.S.I.)

O Comissão Gestora de Segurança da Informação (C.G.S.I.) é um grupo multidisciplinar que reúne servidores de diversas áreas da Prefeitura, indicados pelos seus respectivos Chefes, com o intuito de definir e apoiar estratégias necessárias à implantação e manutenção do PSI (Política de Segurança da Informação).

Compete ao C.G.S.I.:

- Propor ajustes, aprimoramentos e modificações na estrutura normativa da PSI submetendo à aprovação do Executivo;
- Redigir o texto das normas e procedimentos de segurança da informação, submetendo à aprovação do Executivo;
- Requisitar informações das demais áreas, através dos (as) Secretários (as), Chefias e Coordenadorias, com o intuito de verificar o cumprimento da política, das normas e procedimentos de segurança da informação;
- Receber, documentar e analisar casos de violação da política de segurança da informação;
- Estabelecer mecanismos de registro e controle de eventos e incidentes de segurança da informação, bem como, de não conformidades com a política, as normas ou os procedimentos de segurança da informação;
- Notificar as Secretarias e chefias quanto a casos de violação da política e das normas e procedimentos de segurança da informação;
- Receber sugestões dos gestores da informação para implantação de normas e procedimentos de segurança da informação;
- Propor projetos e iniciativas relacionadas à melhoria da segurança da informação;

- Acompanhar o andamento dos projetos e iniciativas relacionados à segurança da informação;
- Propor a relação de gestores da informação;
- Realizar, sistematicamente, a gestão dos ativos da informação;
- Gerir a continuidade dos negócios, demandando junto às diversas áreas da Prefeitura, planos de continuidade dos negócios, validando-os periodicamente.
- Realizar, sistematicamente, a gestão de riscos relacionados à segurança da informação.

CAPÍTULO III - CORREIO ELETRÔNICO

O objetivo desta norma é informar aos servidores quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico. O uso do correio eletrônico do PMSAP.SP.GOV.BR é para fins corporativos e relacionado às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais não é permitida, todas as solicitações, divulgações devem ser realizadas com e-mail oficial da Prefeitura.

Acrescentamos que é proibido aos servidores o uso do correio eletrônico da Prefeitura:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- 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;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Prefeitura ou suas unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da Prefeitura estiver sujeita a algum tipo de investigação.
- Sistema de mala direta, ou qualquer ato de direcionamento e encaminhamento para e-mail particular ou de terceiros.
- Produzir, transmitir ou divulgar mensagem que:

I. Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Prefeitura;
II. Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
III. Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
IV. Vise obter acesso não autorizado a outro computador, servidor ou rede;
V. Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
VI. Vise burlar qualquer sistema de segurança;
VII. Vise vigiar secretamente ou assediar outro usuário;
VIII. Vise acessar informações confidenciais sem explícita autorização do proprietário;

IX. Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
X. Inclua imagens criptografadas ou de qualquer forma mascaradas;
XI. Contenha anexo (s) superior (es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)
XII. Tenha conteúdo considerado impróprio, obsceno ou ilegal;
XIII. Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
XIV. Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
XV. Tenha fins políticos locais ou do país (propaganda política);
XVI. Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

CAPÍTULO IV - INTERNET

Todas as regras atuais visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, esta Prefeitura, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, 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 privados da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação. A Prefeitura, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas.

Toda tentativa de 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 à respectiva chefia. 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 instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus servidores, independentemente de sua relação contratual, poderá ser utilizada nas dependências da prefeitura, desde que não prejudique o andamento dos trabalhos nas unidades.

Como é do interesse desta Prefeitura que seus servidores estejam bem informados, 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 da Prefeitura 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 instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens sendo ela a 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 ou que venha surgir na internet.

Os servidores com acesso à internet não poderão fazer download de programas ligados diretamente ou indiretamente às suas atividades nesta Prefeitura, caso necessário a solicitação deverá ser encaminhada à Secretaria Municipal de Administração, devidamente justificada e assinado pelo solicitante, a liberação ocorrerá mediante análise de riscos e licenciamento do serviço pelo STI, em casos de negativa a resposta seguirá com o motivo pelo qual a solicitação não poderá ser atendida.

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. Qualquer software não autorizado baixado será excluído pelo Suporte de Tecnologia da Informação (STI).

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

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários, autorizados, que tenham atividades profissionais relacionadas a essas categorias mediante solicitação com justificativa e assinatura conforme citação anterior.

Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de cursos relacionados ao desenvolvimento de jogos.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelas respectivas chefias.

Servidores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado à Prefeitura ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

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

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, afins), serviços de comunicação instantânea e redes sociais (MSN, Skype, Facebook, Twitter, Youtube e afins) serão permitidos a grupos específicos, via solicitação formal com justificativa e assinatura do requerente à área responsável.

Não é permitido acesso a sites de proxy.

CAPÍTULO V - ACESSO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante esta Prefeitura e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os servidores.

Todos os dispositivos de identificação utilizados na Prefeitura, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a Prefeitura e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

O STI (Suporte de Tecnologia da Informação) desta Prefeitura é o responsável pela emissão e pelo controle de requisitos de identidade dos servidores. Ele responde pela criação da identidade lógica dos servidores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %...) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente. 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. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras. Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o STI. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

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.

A periodicidade máxima para troca das senhas é 45 (quarenta e cinco) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao STI, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca à área técnica responsável para cadastrar uma nova.

CAPÍTULO VI - COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos servidores são de propriedade desta Prefeitura, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas chefias responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do STI da Prefeitura, ou de quem este determinar, caso seja realizado independente sem o prévio consentimento a unidade ou área fica responsável jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a área técnica responsável mediante registro de chamado no *site* do STI.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada pelo STI, se analisada e validada positivamente e estiver de acordo com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da Prefeitura (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos servidores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os servidores da Prefeitura e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização do STI.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

• Os servidores devem informar à área técnica qualquer identificação de dispositivo estranho conectado ao seu computador.

• É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico do STI ou por terceiros devidamente contratados para o serviço.

Todos os modems internos ou externos (Aparelhos 3G ou 4G) devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização das chefias das áreas e STI.

O servidor deverá manter a configuração do equipamento disponibilizado pela Prefeitura, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custo diante de informações.

- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.
- Todos os recursos tecnológicos adquiridos pela Prefeitura devem ter imediatamente suas senhas padrões (default) alteradas.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos servidores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos desta Prefeitura:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

CAPÍTULO VII - DISPOSITIVOS MÓVEIS

A Prefeitura deseja facilitar a mobilidade e o fluxo de informação entre seus servidores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por seu STI, como: notebooks, smartphones, tablets e pendrives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os servidores que utilizem tais equipamentos.
A Prefeitura, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O servidor, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na Prefeitura, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo servidor deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.

O suporte técnico aos dispositivos móveis de propriedade desta Prefeitura e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo servidor deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico do Suporte TI.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do servidor, no caso de furto ou roubo de um dispositivo móvel fornecido pela Prefeitura, notificar imediatamente seu chefe imediato e o Suporte da Tecnologia da Informação. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O servidor deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à Prefeitura e/ou a terceiros.

O servidor que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da Prefeitura deverá submeter previamente tais equipamentos ao processo de autorização do STI.

Equipamentos portáteis, como smartphones, tablets, pendrives e players de qualquer espécie, quando não fornecidos ao servidor pela instituição, não serão validados para uso e conexão em sua rede corporativa.