TERMO DE COMPROMISSO PARA UTILIZAÇÃO DO SISTEMA SENTRY

1. IDENTIFICADOR DO OPERADOR DO SISTEMA

1- NOME COMPLETO:	**2- DATA:**
3- E-MAIL:	**4- MATRÍCULA:**
5- DEPARTAMENTO/SETOR:	**6- TELEFONE:**

2. NOTIFICAÇÃO DE CREDENCIAMENTO

INFORMO QUE NESTA DATA V. Sª FOI CADASTRADO(A) COMO OPERADOR(A) DO SISTEMA ACIMA IDENTIFICADO, FICANDO-LHE ATRIBUÍDA SENHA INDIVIDUAL E PROVISÓRIA PARA SER IMEDIATAMENTE MODIFICADA EM SEU PRIMEIRO ACESSO ATRAVÉS DO MENU: CONFIGURAÇÃO > ALTERAR SENHA.

3. SOLICITAÇÃO DE ACESSO:

PERFIL	MENU

Observações:
_____
_____
_____
_____

4. IDENTIFICAÇÃO DA CHEFIA IMEDIATA:

1- NOME COMPLETO:	**2- DATA:**
2- EMAIL:	**4- MATRÍCULA:**
5- DEPARTAMENTO/SETOR:	**6- TELEFONE:**

5. TERMO DE RESPONSABILIDADE

a) Acessar o (s) sistema (s) informatizado (s) somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na instrução normativa que rege os acessos e sistemas e a rede de dados propriamente dita;

b) Não revelar fora do âmbito profissional fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como autoridade superior;

c) Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

d) Não me ausentar da estação de trabalho sem encerrar a sessão de uso do sistema e da rede, garantindo assim a impossibilidade de acesso indevido por terceiros;

e) Não revelar minha senha de acesso ao (s) sistema (s) e a rede de dados a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

f) Responder em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Declaro ainda, estar plenamente esclarecido e consciente que:

1. É minha responsabilidade cuidar da integridade, confidencialidade e disponibilidade dos dados, informações contidas nos sistemas, devendo comunicar por escrito à chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas nos sistemas, sendo proibida a exploração de falhas ou vulnerabilidade porventura existentes;

2. O acesso a informação não me garante direito sobre ela, nem me confere autoridade para liberar o acesso a outras pessoas;

3. Constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional, divulgar dados obtidos dos sistemas ou da rede de dados aos quais tenho acesso para outros servidores não envolvidos nos trabalhos executados;

4. Devo alterar minha senha, sempre que solicitado ou que tenha suposição descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas;

5. Respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na instituição (tais como direitos de acesso a arquivos, diretórios e recursos disponíveis no ambiente da instituição)

6. Cumprir e fazer cumprir os dispositivos da Política Corporativa de Segurança da Informação, de suas diretrizes, bem como deste Termo de Responsabilidade. Ressalvadas as hipóteses de requisições legalmente autorizadas, constitui infração funcional e penal a revelação de segredo do qual me apropriei em razão do cargo. Sendo crime contra a administração. pública, a divulgação a quem não seja servidor da prefeitura, das informações do (s) sistema (s) ou da rede de dados ao (s) qual (is) tenho acesso, estando sujeito às penalidades previstas em lei.

Sem prejuízo da responsabilidade penal e civil, e de outras infrações disciplinares, constitui falta de zelo e dedicação as atribuições do cargo e descumprimento de normas legais e regulamentares, não proceder com cuidado na guarda e utilização de senha ou emprestá-la a outro servidor, ainda que habilitado.

Constitui infração funcional e penal inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos dos sistemas ou bancos de dados da administração pública, a fim de obter vantagem indevida para si, para outrem ou para causar dano; bem como modificar ou alterar o sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente; ficando assim o infrator sujeito as punições previstas no Código Penal Brasileiro, conforme responsabilização por crime contra a administração pública, tipificado no art. 313-A e 313-B do Código Penal.

Declaro, nesta data, ter ciência e estar de acordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente.

Maricá, _____ de _____ de 20____.

_____ _____

Assinatura e matrícula do servidor | Assinatura e matrícula do Superior Imediato

Política de Uso Aceitável

As informações a seguir apresentam integram a Política de Uso Aceitável (PUA), tratando de todos os detalhes da forma mais genérica possível. Os usuários devem conhecer e respeitar a política, colaborando assim pela segurança na instituição e evitando o desperdício de recursos públicos.

Objetivos

A PUA tem como objetivos:

● Oficializar o uso aceitável e não aceitável dos recursos de TI da PMM;
● Instruir os usuários sobre as boas práticas relacionadas ao uso dos recursos de TI;
● Embasar os trabalhos da TI quanto à disponibilidade, integridade e confidencialidade dos recursos de TI.

Definições

Para fins desta política, entende-se por:

I. Autenticidade – Propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.
II. Backup – É a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.
III. Confidencialidade – Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.
IV. Conta de Usuário – Identificação de um usuário para acesso a algum recurso ou serviço da rede.
V. Disponibilidade – Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
VI. Estação de Trabalho – Conjunto de equipamentos de informática mínimos necessários (monitor, gabinete, teclado e mouse), destinados aos usuários, para realização do trabalho.
VII. Grupos – Canais de comunicação coletivos, que envolvem a troca de mensagens para vários usuários simultaneamente.
VIII. Integridade – Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
IX. Login – Processo de identificação e autenticação de um usuário para permitir o seu acesso a um sistema.
X. Malwares – Malware, forma reduzida de malicious software (software malicioso), é um software usado por atacantes para comprometer a operação de um computador, colher informações sensíveis ou ganhar acesso a sistemas computacionais privados.
IX. Privilégio do Administrador – Pessoa com permissão para realizar alterações e/ou modificações em nível lógico nos computadores institucionais e na rede, como, por exemplo, instalação de programas.
X. Política de Uso Aceitável – Documento que define como os recursos computacionais de uma instituição podem ser utilizados. Também define os direitos e responsabilidades dos usuários destes recursos.
XI. Quebra de segurança: Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
XII. Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive a s sigilosas.
XIII. Recursos de Tecnologia da Informação e Comunicação – consideram-se recursos de tecnologia da informação o conjunto formado pelos bens e serviços de TI que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação. Entre os recursos estão Computadores, Sistemas, Portais, Impressoras, Internet, dentre outros.
XIV. Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
XV. Sistemas de Informações – Conjunto de componentes da estrutura organizacional, TI, Dados e Pessoas (Usuários e Equipe de TI), através do qual é processado, de forma ordenada, o fluxo de comunicações internas e externas da organização. O sistema de informações processa dados e gera informações as quais fornecem subsídios para o processo de tomada de decisões.
XVI. Suporte Técnico – É um serviço que presta assistência intelectual, tecnológica e de material a uma pessoa ou setor, a fim de resolver um problema específico.
XVII. Tecnologia da Informação (TI) – Envolve a aplicação de computadores e equipamentos de telecomunicação para armazenar, recuperar, transmitir e manipular dados, no contexto empresarial.
XVIII. Usuários – Compreende todos os envolvidos que utilizam algum dos recursos de TI da instituição. Os usuários podem ser internos ou externos.

Utilização dos recursos de TI

A utilização da infraestrutura tecnológica e demais recursos de TI é destinada ao desenvolvimento das atividades públicas e administrativas realizadas pelos usuários da Prefeitura, sendo disponibilizada exclusivamente como ferramenta de trabalho e apoio administrativo. Dessa forma, esta política estabelece parâmetros para o uso aceitável dos recursos de TI.

O setor de Tecnologia da Informação da PMM poderá, a seu critério, monitorar e manter histórico de uso de todos os recursos de TI disponibilizados, para efeito de auditoria, conformidade, diagnóstico de problemas e produção de estatísticas. Essas informações poderão ser disponibilizadas à administração mediante solicitação o formal.

Uso aceitável

É considerado uso aceitável dos recursos de TI pelo servidor, considerando-se o Art. 137 da LC Nº 001 DE 09 DE MAIO DE 1990:

I. Garantir a segurança e integridade do recurso de TI em uso, mantendo-o nas condições originais. É de responsabilidade dos usuários zelar pela conservação e boas condições da infraestrutura e equipamentos.
II. Comunicar imediatamente ao setor de TI à ocorrência de qualquer anomalia no uso dos recursos de TI.
III. Notificar ao setor de TI quando ocorrerem alterações que venham a afetar o cadastro do usuário como setor de trabalho, ramal, cargo ou função.
IV. Efetuar a manutenção de suas áreas pessoais, como caixa de e-mails e pastas de armazenamento, evitando ultrapassar o limite estabelecido e garantindo o seu funcionamento contínuo.
VI. Armazenar dados e informações da Prefeitura em pastas compartilhadas seguras, conforme orientação do setor de TI para garantir a segurança dos dados, já que o backup é feito apenas nessas unidades. Não há garantia quanto aos dados salvos fora desses servidores. Os arquivos gravados em diretórios temporários das estações, áreas de trabalho, e pastas pessoais podem ser formatadas, excluídos ou perdidos.
VII. Utilizar senhas que contenham, pelo menos, oito caracteres, compostos de letras, números e símbolos, evitando o uso de nomes, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com o usuário ou palavras constantes em dicionários. As senhas temporárias devem ser alteradas imediatamente. As senhas são sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese.
VIII. Alterar as senhas no mínimo a cada trimestre.
IX. Solicitar de suporte (instalação, manutenção, prevenção, configuração e correção), pelo usuário, através dos canais de atendimento da Central de Serviços, para abertura e acompanhamento de chamados, atendendo a ordem de prioridade do serviço.
Uso não aceitável

É considerado uso não aceitável dos recursos de TI pelo servidor, considerando-se o Art. 138 da LC Nº 001 DE 09 DE MAIO DE 1990:

I. Compartilhar informações sigilosas, classificadas ou proprietárias, inclusive senhas, com pessoas ou organizações não autorizadas.
II. Utilizar para fins estranhos às suas atividades profissionais os recursos de TI colocados a sua disposição pela Instituição. Esses recursos não devem ser utilizados para fins pessoais, utilização de redes sociais, incluindo entre estes o comércio, venda de produtos ou engajamento em atividades comerciais de qualquer natureza, de acordo com a legislação em vigor.
III. Fornecer informações reservadas a terceiros, exceto mediante autorização da administração.
IV. Fumar, comer ou beber próximo aos equipamentos de TI.
V. Difundir através dos recursos de TI, material ofensivo, obsceno, ilegal, antiético, comercial, pessoal, de propaganda, mensagens do tipo corrente, entretenimento, "spam" (envio de mensagem não solicitada), mensagens capazes de colocar em risco a segurança da Prefeitura, propaganda política interna ou externa à Prefeitura.
VI. Utilizar qualquer recurso de TI da Prefeitura, para propagação de trotes, boatos, “fake-news”, pornografia, propaganda comercial, religiosa ou político- partidária.
VII. Participar de grupos sociais, utilizando o serviço de internet da Prefeitura, que possam abordar assuntos alheios à instituição, suas secretarias e órgãos, exceto em casos de participação em Grupos sobre assuntos relacionados às atividades específicas desenvolvidos no órgão público;
VIII. Difundir malware (software malicioso) ou qualquer forma de rotinas de programação prejudiciais ou danosas à s estações de trabalho e ao sistema de correio;
IX. Conduzir qualquer tipo de ataque ou atividade de fim malicioso que vise tornar um serviço indisponível, obter vantagem indevida, escalar privilégios, prejudicar outros usuários ou conseguir acesso à informações protegidas.
X. Instalar ou utilizar softwares nos equipamentos da PMM que não estejam devidamente licenciados. É vedada a utilização de softwares que não possuam licenças, sejam elas pagas, gratuitas ou temporárias e/ou que não estejam registrados no nome da Prefeitura.
XI. Utilizar qualquer tipo de software e hardware diferentes dos já disponibilizados, sem autorização do setor de TI;
XII. Armazenar nas estações de trabalho, bem como na pasta pessoal, MP3, filmes, fotos, software(s) e outros arquivos com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria;
XIII. Outras atividades que possam afetar de forma negativa a Instituição, servidores, fornecedores e parceiros.

Outras Informações

● O acesso físico às áreas restritas relacionadas à TI (datacenter, shafts, etc.) é permitido apenas para os funcionários do setor de TI . É vedado o acesso de terceiros sem autorização prévia.
● O setor de TI poderá, a seu critério, utilizar mecanismos para controle de tráfego e acesso visando garantir a qualidade dos recursos disponibilizados.
• Em caso de exoneração ou alteração de lotação do servidor, deverá ser informado pelo chefe imediato ao setor de Gestão de Pessoas, a qual comunicará ao setor de TI a necessidade de desativação da conta de usuário e de todos os acessos do usuário/servidor.
● Os casos de utilização indevida citados nessa política, em razão de denúncia ou apurados pela administração, deverão ser encaminhados à administração para avaliar as condutas e adotar providências de acordo com os Art. 143 e Art. 149 da LC Nº 001 DE 09 DE MAIO DE 1990. Caberá ainda ao setor de TI fornecer as informações formalmente solicitadas pela administração.
• Sendo diagnosticado mau uso ou uso indevido dos recursos de TI, por parte do usuário, será tratado como inconformidade e aberto um processo de sindicância e reparação dos danos causados conforme previsto no Art. 165 da LC Nº 001 DE 09 DE MAIO DE 1990.

_____

Ciente e CPF