POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Introdução

A presente Política de Segurança da Informação ("Política") foi elaborada pela Município De Rondonópolis – Estado De Mato Grosso, pessoa de direito público, situada à Avenida Duque De Caxias nº 1.000, Vila Aurora, na Município De Rondonópolis, Estado do Mato Grosso, inscrita no CNPJ sob o nº 03.347.101/0001-21 ("Prefeitura" ou "Nós") a fim de proteger os dados sob controle da Prefeitura, bem como os ativos físicos e tecnológicos por onde eles passam ou estão armazenados.

O principal objetivo da segurança da informação é proteger os dados e não somente os ativos físicos e tecnológicos por onde eles passam ou estão armazenados. A partir dessa premissa, existe uma independência nos conceitos da informação em relação à tecnologia

2. Critérios Gerais

A Política deve ser conhecida e acatada por todos os servidores, bem como estagiários, terceiros e prestadores de serviços que utilizam os recursos de processamento da informação de propriedade da Prefeitura, sendo de responsabilidade de cada um o seu cumprimento.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelos servidores, bem como estagiários, quando na utilização dos recursos de processamento da informação da Prefeitura. ou em ferramentas de comunicação privada não homologadas quando utilizadas em suas atividades laborais, ficando os transgressores sujeitos às sanções previstas pela Lei laboral (CLT – Consolidação das Leis do Trabalho), Civil (Código Civil) e Criminal (Código Penal).

Os documentos, programas e/ou sistemas produzidos pelos servidores, bem como estagiários, terceiros e prestadores de serviços por intermédio dos recursos de processamento da informação da Prefeitura são de propriedades da Prefeitura.

As informações de propriedade da Prefeitura devem ser utilizadas apenas para os propósitos definidos no Contrato Individual de Trabalho ou Contrato de Prestação de Serviços. Os servidores bem como estagiários, terceiros e prestadores de serviços não podem em qualquer tempo ou sob qualquer propósito, apropriar-se dessas informações.

3. O que queremos proteger e quem são os responsáveis

É obrigação de todos os usuários dos sistemas da Prefeitura proteger os ativos de tecnologia e informação da Prefeitura. Essas informações devem ser protegidas contra acesso não autorizado, roubo e destruição. Os ativos de tecnologia e informação da Prefeitura são constituídos pelos seguintes componentes.

• Hardware de computador, CPU, disco, e-mail, web, servidores de aplicativos, sistemas de PC, software de aplicativo, software de sistema etc.

• Software de sistema, incluindo: sistemas operacionais, sistemas de gerenciamento de banco de dados e software de backup e restauração, protocolos de comunicação e assim por diante.

• Software de aplicação: utilizado pelos diversos departamentos da Prefeitura. Isso inclui aplicativos de software personalizados e pacotes de software de prateleira.

• Hardware e software de rede de comunicações, incluindo: roteadores, tabelas de roteamento, hubs, modens, firewalls, softwares e ferramentas de gerenciamento de rede associados.

4. Política de Senha/PIN

Um número de identificação pessoal (PIN) é um código de segurança para verificar sua identidade. Semelhante a uma senha, seu PIN deve ser mantido em sigilo porque permite o acesso a serviços importantes, como transações financeiras. Os PINs podem ser usados para qualquer coisa digital e que requeira acesso. Isso pode incluir dispositivos de comunicação, bloqueios de carro, bloqueios de casa e muito mais.

A segurança sempre será uma preocupação. Usar um PIN seguro é crucial para prevenir o acesso não autorizado às suas informações, contas e ativos.

Em hipótese alguma o PIN do usuário deverá ser escrito ou divulgado a servidores, terceiros, mídias sociais e qualquer outra forma inclusive à servidores do TI.

Após a identificação do usuário usando seu PIN pessoal na rede ou nos sistemas da Prefeitura, a responsabilidade por toda e qualquer atividade será única e exclusiva do usuário.

É proibida a divulgação do PIN e este não pode ser utilizado por terceiros em nenhuma circunstância.

Quaisquer ações indevidas efetuadas através do acesso autenticado serão de total responsabilidade do usuário identificado, ainda que seja durante eventual uso de seu PIN por terceiros, sujeitando o usuário às penalidades cabíveis.

Segurança de PIN
Como os PINs protegem muitas das suas informações e recursos, é aconselhável usar um PIN que seja difícil de adivinhar. Evite incluir os seguintes itens em seu PIN:

- Sequências de números simples como 1234 ou 0000
- Sequências de números repetidos como 1122 ou 2233
- Datas importantes, como seu ano de nascimento ou aniversário do cônjuge
- Qualquer parte do seu número de Seguro Social

- Qualquer parte do seu endereço ou número de telefone

PINs mais longos são mais seguros do que PINs mais curtos. Se você usar um PIN de quatro dígitos, há 10.000 variações possíveis (começando com 0000, 0001, 0002 e assim por diante). Com um PIN de seis dígitos, existem 1 milhão de códigos possíveis.

PINs mais longos funcionam bem porque são necessárias mais tentativas para adivinhá-los. A maioria dos sistemas de segurança bloqueia sua conta após um determinado número de tentativas. Isso garante que seja mais difícil para ladrões e programas de computador adivinharem o seu PIN.

Métodos para criar PINs seguros
Criar um PIN memorável pode ser difícil. Usar uma estratégia de PIN pode facilitar a criação de uma que você consiga lembrar.

Estratégia # 1: O Método da Palavra
Uma maneira de criar e lembrar um PIN é criá-lo a partir de uma palavra. Pense nos números e letras do teclado de um telefone. Você já usou a opção "discar por nome" para encontrar alguém na lista telefônica de uma empresa? Usando o mesmo conceito, você pode basear seu PIN em uma palavra, tornando-o mais fácil de lembrar.

Por exemplo, a palavra "WORD" é convertida no PIN 9673. O W está no 9, o O está no 6 e assim por diante.

Estratégia # 2: o método de data aleatória
Outra maneira de criar e lembrar um bom PIN é usar uma data não relacionada a você de forma alguma.

Estratégia # 3: o método de contato por telefone celular falso
Seu celular provavelmente possui dezenas ou centenas de contatos. Adicione um novo contato falso e oculte seu PIN no número de telefone desse contato. Por exemplo, se o seu PIN for 3282, você pode adicionar o número de telefone 555-923-3282, exceto usar um número de telefone de aparência local - não um com o código de área 555 fictício. Isso faz uso do conceito de "esconder-se à vista de todos".

5. Uso da Internet/Web

Existem vários hábitos que você deve desenvolver para melhorar a segurança de suas atividades online. Embora a lista a seguir possa parecer muito para gerenciar, a maioria dessas recomendações é simples e segui-las aumentará significativamente a segurança de sua navegação.

Mantenha o software do navegador atualizado: isso é crucial, pois novos patches são frequentemente lançados para corrigir vulnerabilidades existentes no software do navegador. Esta recomendação não se aplica apenas ao software do navegador - é fundamental manter o software do sistema operacional e qualquer outro software atualizado pelo mesmo motivo.

Execute o software antivírus: o software antivírus fornece proteção ao verificar e remover arquivos maliciosos do computador. Existem muitas opções excelentes de software de proteção contra vírus (pagos e gratuitos), portanto, cabe a você fazer uma pequena pesquisa e selecionar o programa que melhor se adapta às suas necessidades.

Verifique os arquivos antes de fazer o download: é importante evitar fazer download de nada até ter certeza de que é seguro. Se você tiver alguma suspeita de que um arquivo pode não ser legítimo ou estar infectado, verifique-o com um software antivírus antes de fazer o download.

Cuidado com o phishing: os ataques de phishing usam comunicações online (geralmente e- mail) para induzir os usuários a fornecer suas informações confidenciais. Muitas vezes, essas mensagens parecem ser de bancos, sites de mídia social, sites de compras ou processadores de pagamento. As mensagens de phishing frequentemente contêm links que levam a versões falsificadas de sites populares. Você pode evitar ser vítima de esquemas de phishing, ignorando mensagens não solicitadas e não clicando em hiperlinks ou anexos em e-mails (digite ou copie / cole o URL como ele aparece).

Não reutilize senhas: usar a mesma senha para vários sites torna mais fácil para os invasores comprometerem suas informações confidenciais. Em vez disso, controle suas diferentes senhas com uma lista manuscrita que você mantém em um lugar seguro ou crie seu próprio algoritmo para criar senhas exclusivas que só você saberá. Também é recomendável que você altere suas senhas a cada 90 dias.

Use HTTPS: O “s” em “https” significa seguro, o que significa que o site está usando criptografia SSL. Verifique se há um “https:” ou um ícone de cadeado na barra de URL do seu navegador para verificar se um site é seguro antes de inserir qualquer informação pessoal.

Leia as políticas de privacidade: as políticas de privacidade e acordos do usuário dos sites devem fornecer detalhes sobre como suas informações estão sendo coletadas e protegidas, bem como como esse site rastreia sua atividade online. Sites que não fornecem essas informações em suas políticas geralmente devem ser evitados.

Monitore regularmente seus extratos bancários: ficar de olho em seus extratos on-line permitirá que você reaja rapidamente no caso de sua conta ser comprometida.

Evite Wi-Fi público ou gratuito: os invasores costumam usar farejadores sem fio para roubar informações dos usuários à medida que são enviadas por redes desprotegidas. A melhor maneira de se proteger disso é evitar o uso dessas redes por completo.

Desative as senhas armazenadas: Quase todos os navegadores e muitos sites em geral oferecem para lembrar suas senhas para uso futuro. Habilitar esse recurso armazena suas senhas em um local no computador, tornando mais fácil para um invasor

descobrir se o sistema foi comprometido. Se você tiver esse recurso ativado, desative-o e apague suas senhas armazenadas.

Ative o bloqueador de pop-ups do seu navegador: o bloqueio de pop-ups agora é um recurso padrão do navegador e deve ser ativado sempre que você estiver navegando na web. Se for necessário desativá-lo para um programa específico, ative-o novamente assim que a atividade for concluída.

6. Controles de Dispositivo

Os servidores estão mais familiarizados com seus próprios pertences, então não há virtualmente nenhuma curva de aprendizado quando eles vão para a mobilidade. Sua produtividade pode aumentar. Podem otimizar o tempo entre atividades pessoais e corporativas. Podem complementar seu acesso a tecnologias emergentes, mantendo-se atualizados com as últimas tendências.

Equipamentos cobertos por esta política:

- Desktops, laptops e tablets
- Smartphones (definido como qualquer telefone celular que se conecta à Internet via Wi- Fi ou rede de operadora de celular)
- Flash, memória e / ou pen drives
- Discos rígidos externos
- iPods, iTouches e dispositivos de entretenimento e música portáteis semelhantes que se conectam a redes WiFi
- Consoles de entretenimento e jogos que se conectam a redes Wi-Fi e são usados para acessar e-mail e sistemas da organização
- Dispositivos vestíveis, como relógios, fones de ouvido de RV e óculos de realidade aumentada com WiFi ou Bluetooth

Servidores que façam uso de notebooks, laptops, IPADs, Smartphones e outros dispositivos móveis contendo informações da Prefeitura, devem zelar pela segurança física do equipamento.

Tais dispositivos não devem ser expostos em locais públicos e devem-se tomar cuidados especiais para evitar-se perda ou roubo destes.

Dados em mídia removível, como por exemplo, DVDs, CD-ROM, pen drives e outros, quando não utilizados, devem estar armazenados em locais seguros, como por exemplo, cofres, gavetas com chave e outros.

7. Correio Eletrônico

Fica proibido o uso do correio eletrônico corporativo para cadastramento em sites do tipo: Compras Coletivas (Grupon, Clickon, Peixe Urbano etc.), Recrutamento e Seleção (Linkedin, Catho, Vagas etc.), Redes Sociais (Facebook, Instagram, Tik Tok,

Youtube, etc.), Comércio Eletrônico (Mercado Livre, Lojas Americanas etc.) entre outros.

Estão terminantemente proibidas mensagens eletrônicas que possuam conteúdo ofensivo, preconceituoso ou discriminatório de qualquer natureza, como por exemplo, raça, sexo, religião, pornográfico ou obsceno, piadas, correntes, venda de produtos, caridade e outros.

Também fica proibida a utilização de aplicativos de mensagens instantâneas (Whatasapp, Telegram, etc.) e/ou redes sociais (Facebook, Instagram, etc.) para a realização de comunicações referentes aos dados e ativos da Prefeitura, seus clientes e fornecedores, seja para comunicação interna ou externa. Para a realização de comunicações internas ou externas devem ser utilizados os meios de comunicação oficiais e outorgados pela Prefeitura.

Todas as mensagens eletrônicas enviadas ou recebidas e/ou armazenadas nos computadores são de propriedade da Prefeitura.

Não é permitido o envio de cópias de mensagens eletrônicas internas contendo informações sensíveis ou confidenciais da Prefeitura para endereços externos sem a prévia autorização da Secretaria responsável.

Não é permitida a leitura ou o envio de mensagens eletrônicas, utilizando a caixa postal de outro usuário. Em caso de férias ou afastamento é necessário que as mensagens recebidas neste período sejam direcionadas para o servidor que assumirá suas funções no respectivo período.

É proibido o recebimento de arquivos pessoais advindos de fontes externas e não relacionadas a Prefeitura. Tais arquivos podem conter vírus ou programas com conteúdo não aprovado pela Prefeitura.

Mensalmente, cada usuário deverá excluir de sua caixa postal (Caixa de Entrada e Mensagens Enviadas) as mensagens que não sejam mais necessárias às suas atividades profissionais, preferencialmente aquelas que contenham informação sensível ou confidencial. Com isso, ajuda-se a manter a segurança e evita-se o uso desnecessário dos recursos computacionais da Prefeitura.

8. Utilização dos Arquivos

Todos os arquivos críticos ou vitais para a operação da Prefeitura devem estar armazenados nos servidores de arquivos designados.

A definição dos arquivos críticos é de responsabilidade da Secretaria responsável. Desta forma, são garantidas a segurança e a proteção destas informações contra roubo, perda e indisponibilidade.

Os arquivos devem ser identificados corretamente na rede, tendo seu nome relacionado com seu conteúdo. Deve-se evitar o uso de nomes comuns (e.g., Prefeitura, procedimentos, relatório) que podem facilmente criar duplicidade na rede e dificuldade de identificação dos mesmos.

Os arquivos são armazenados através de estrutura departamental em diretórios restritos a cada Secretaria. Não é permitido o acesso a arquivos de outras Secretaria, a menos que estes estejam no diretório público da Prefeitura.

Arquivos que deixem de ter importância para Prefeitura devem ser removidos do sistema. Esta limpeza é de responsabilidade de cada usuário e deve ser realizada frequentemente.

9. Disponibilização de Informações

Todos os comunicados internos formais emitidos a grupos de servidores através de mensagens eletrônicas ou impressos em murais ou quadro de avisos da Prefeitura devem conter: data e ano do término do comunicado; nome, cargo, unidade e área de atuação do responsável pelas informações divulgadas.

É proibido fornecer dados ou alterações de configurações solicitadas por telefone ou qualquer outro meio de comunicação.

Ao convocar reuniões, envolver somente as pessoas que efetivamente estejam relacionadas ao assunto abordado ou que necessitem ter acesso a tais informações pela natureza da posição que ocupam.

Para a realização de reuniões, internas ou externas, deve-se restringir o número de cópias dos documentos ao número de participantes.

Documentos contendo informações sigilosas ou importantes da Prefeitura não podem ser deixados sobre as mesas de trabalho ou de reunião ao alcance de quaisquer outras pessoas. Devem ficar à mostra apenas durante o seu uso e ao final devem ser novamente guardados em armários trancados, quando não mais estiverem sendo utilizados. A prática da mesa limpa deve ser sempre verificada pelo gestor da Secretaria.

O mesmo deve acontecer para informações escritas em quadros-brancos ou em flip-charts durante reuniões. Os servidores da Prefeitura devem preocupar-se em recolher as folhas do flip-chart e apagar o quadro-branco após o uso.

Recomenda-se que, dentro do possível, os servidores evitem o armazenamento de informações de trabalho em documentos físicos, de modo que a impressão de documentos apenas deverá ser realizada quando estritamente necessário.

Não havendo obrigação legal ou regulatória de armazenamento e guarda dos documentos, recomenda-se a eliminação imediata, utilizando-se fragmentadora de papeis, após a sua utilização.

O servidor deve evitar conversas sobre informações confidenciais da Prefeitura, como por exemplo, lançamentos, movimentos organizacionais, iniciativas, projetos e outros em locais públicos, táxis, bares, restaurantes, etc. Pessoas mal-intencionadas podem escutar tais informações e usá-las de maneira incorreta, visando prejudicar a Prefeitura.

10. Responsabilidades do usuário

O usuário não deve tentar alterar ou desativar nenhuma configuração de segurança aplicada ao dispositivo pelo departamento de TI.

O usuário deve consultar o fabricante / fornecedor / operadora para obter suporte de seu dispositivo antes de solicitar assistência do departamento de TI.

O usuário deve utilizar de forma idônea sua(s) conta(s) de identificação na rede e nos sistemas de computadores.

O usuário deve manter o sigilo e não fazer o uso privado de informações geradas, adquiridas ou utilizadas pela Prefeitura, às quais tenha tido acesso no exercício de suas atividades.

O usuário deve manter o sigilo de suas senhas de acesso aos recursos, sistemas e serviços da rede de computadores.

O usuário deve manter segura as informações manuseadas no âmbito da rede de computadores da Prefeitura.

O usuário deve observar que as informações armazenadas na estação de trabalho e nos demais dispositivos móveis utilizados para o desempenho de suas funções serão de sua inteira responsabilidade, não havendo previsão de backup para tais unidades.

O usuário deve manter a guarda, a segurança e a integridade dos ativos físicos e lógicos que estejam sob sua responsabilidade.

O usuário deve responder por todos os atos efetivados por meio de seu identificador, tais como login de rede e endereço de correio eletrônico.

O usuário deve utilizar os sistemas e serviços de informação somente para fins legais.

O usuário deve manter o sigilo de informações sensíveis para Prefeitura, sob qualquer circunstância de terceiros que não tenham a devida autorização de acesso a estas.

Política de Segurança da Informação

Ao compartilhar assuntos de trabalho, em qualquer local, dentro ou fora do ambiente de trabalho, a partir de qualquer tipo de canal, mídia, ferramenta ou tecnologia, o servidor deve respeitar a ética, a legislação vigente no Brasil e cumprir com seu dever de sigilo profissional.

No caso de um usuário acreditar que um dispositivo de propriedade ou fornecido pessoalmente que está autorizado a se conectar aos recursos, sistemas ou redes da organização pode estar infectado com um vírus, infecção por spyware ou outra ameaça de malware ou pode estar de alguma forma comprometido, ele deve notificar imediatamente o departamento de TI por escrito sobre o risco potencial à segurança.

Se um usuário perder ou perder um dispositivo de propriedade pessoal ou fornecido pessoalmente que está autorizado a se conectar aos recursos, sistemas ou redes da organização, ele deve notificar imediatamente o departamento de TI por escrito sobre o risco potencial de segurança.

Sempre que um usuário desativa, se prepara para retornar ou de outra forma deixa de usar um dispositivo de propriedade pessoal ou fornecido pessoalmente que o diretor de TI autorizou para uso da organização, o usuário deve notificar o departamento de TI de que o dispositivo não será mais usado para se conectar aos recursos da organização, sistemas ou redes.

Os usuários não podem descartar dispositivos previamente autorizados até que o departamento de TI aprove o dispositivo para descarte.

É vedado ao usuário emitir opiniões anônimas na Internet e na Intranet (mídias sociais, correio eletrônico, bate-papo, entre outros).

É vedado ao usuário utilizar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material que viole a lei de direitos autorais – Lei 9.610 de 19 de fevereiro de 1998;

É vedado ao usuário tomar ação própria no intuito de conter um incidente de segurança dos ativos de TI sob qualquer circunstância.

É vedado ao usuário promover atividades comerciais próprias ou de terceiros, incluindo oferta de serviços ou produtos, salvo por meio de canais institucionais adequados.

É vedado ao usuário enviar mensagens não institucionais para grupos ou pessoas que não as solicitaram ou autorizaram.

É vedado ao usuário enviar mensagens cuja veracidade não possa ser confirmada.

É vedado ao usuário enviar mensagens que, de alguma forma, violem as legislações vigentes.

É vedado ao usuário enviar mensagens, imagens, vídeos ou áudios ofensivos, depreciativos ou que impliquem em humilhação ou assédio, para outros servidores ou em grupos de compartilhamento criados para tratar de assuntos laborais em ferramentas de comunicação privada não homologadas pela Prefeitura.

11. Revisão da Política

Esta Política pode ser atualizada de tempos em tempos pela Prefeitura para refletir qualquer mudança na legislação ou nos métodos e práticas da Prefeitura.

12. Aplicação da Política

A violação de qualquer um dos princípios dentro da Política pode resultar em uma ação disciplinar (no caso de empregados) ou uma grave quebra contratual (no caso de terceiros), podendo equivaler a uma transgressão grave, o que poderá resultar em demissão sumária com justa causa ou rescisão contratual.

Esta Política não se destina e não concede aos usuários quaisquer direitos contratuais.