POLÍTICA DE SEGURANÇA E FLUXO DE DADOS:

1- INTRODUÇÃO:

O Cartório de Notas e Protesto de Toritama (PE) estabelece através desse documento que será de conhecimento amplo de todos os seus colaboradores as diretrizes de segurança e de privacidade dos dados em consonância com as disposições legais estabelecidas pela LEI nº 13.709/18 (LEI GERAL DE PROOTEÇÃO DE DADOS) e que devem ser cumpridas em sua integralidade.

2- OBJETIVOS:

Traçar diretrizes para que o tratamento de dados coletados em função da atividade pública para qual foi delegada pelo Poder Judiciário para as Serventias Extrajudiciais, cujos atos são realizados para o cumprimento de obrigação legal ou regulatória pelo controlador, nos termos do art. 7º, Inc.II, da Lei 13.709/18, sejam executados visando a privacidade dos dados pessoais com eficiência, eficácia e competitividade, de modo seguro, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

Estabelecer as condutas adequadas para em relação aos tratamentos de dados, bem como limites, competências e responsabilidades de cada operador visando uma política de segurança e privacidade de dados a que tem acesso em virtude do exercício das suas atribuições legais.

3- APLICABILIDADE:

Esse documento é elaborado contendo as decisões do CONTROLADOR no que tange ao tratamento de dados e deve ser de conhecimento e aplicabilidade

rigorosa nos limites aqui estabelecidos pelos os colaboradores, estagiários, prestadores de serviços, terceirizados, conveniados, credenciados, fornecedores, clientes, menores aprendizes, ou quaisquer outros indivíduos ou entidades que venham a ter acesso e/ou utilizar, direta ou indiretamente, os dados sensíveis ou pessoais do Cartório de Notas e protesto de Toritama(PE).

4- DAS VEDAÇÕES

São vedados aos agentes contidos no item 3 do presente instrumento:

I- O uso de dados pessoais e sensíveis em publicações mesmo que de cunho acadêmico.
II- As informações prestadas sem que seja por meio de certidões.
III- Exigir e arquivar quaisquer documentos que não tenha finalidade direta com o ato ou que não esteja previsto nas normas legais ou tabela de fluxo.
IV- Descartar materiais que contenham dados pessoais e sensíveis sem observar a desfiguração do documento.
V- Compartilhar por qualquer meio dados sensíveis ou pessoais que tenha obtido das suas atribuições na serventia e por meio da sua atividade regular.
VI- Utilizar dados ou mesmo quaisquer signo distintivo da serventia sem o conhecimento prévio do controlador.
VII- Todas as informações que forem obtidas por meio do exercício de atribuições da serventia são sigilosas e não podem ser compartilhadas sem prévia autorização do controlador.
VIII- Descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador
IX- Vedação do uso de internet para fins pessoais, bem como download, sites suspeitos ou que violem os bons costumes ou a legislação vigente, sendo permitido o uso de e-mail e whatsapp e whatsappweb para fins profissionais e comunicadores instantâneos que após usado fora do horário de expediente normal não configuram sobrejornada, sobreaviso ou plantão do colaborador, visto que isso pode ocorrer por ato de liberalidade e/ou conveniência do próprio colaborador sem expressa e prévia requisição da Serventia de Notas e protesto de Toritama(PE).
X- É vedado os uso de dispositivos particulares sem que seja devidamente verificada a ocorrência de alguns malware ou vírus através do programa antivírus.
XI- É vedado o uso de mídias sociais em nome da serventia sem autorização do controlador e a sua qualquer referência à serventia deve estar relacionada às atividades profissionais. O colaborador é responsável por sua conduta no uso das mídias sociais, vedado o uso de conteúdos não autorizados que violem o sigilo profissional
XII- É vedado o compartilhamento de senha e o uso de hardware do cartório por terceiro, salvo por autorização do controlador.
XIII- É vedado o compartilhamento de senhas e uso indevido do certificado digital do controlador instalado em cada máquina para fins de uso nas centrais do Colégio Notarial do Brasil, busca de indisponibilidade, nas Central de Protesto e envio da DOI, caso seja apurado uso irregular do certificado digital pelo operador caberá procedimento administrativo para apurar a responsabilidade pelo uso indevido.

5- Gestão de acesso pelos Operadores da

O acesso aos computadores da serventia é realizada mediante senha do Windows mudada periodicamente a cada 02 (dois) meses e o acesso ao sistema que opera os atos digitais é realizado por senha pessoal e intransferível.

As atividades de cada operador é efetuada por determinação do controlador, cabendo somente a este a responsabilidade de indicar ao sistema quais atividades podem ser praticadas por cada operador.

O uso de centrais de compartilhamento de dados da Colégio Notarial do Brasil, pesquisa na central de indisponibilidade, DOI, Central de Testamento, e-notariado, é realizada através de certificado digital em nome do controlador e instalada em cada uma das máquinas da serventia.

O acesso a central nacional protesto é efetuada mediante login do Controlador.

O acesso ao SISCOAF é efetuado através de senha do controlador, sendo vedado revelar a terceiros o envio de tais informações de caráter sigiloso.

Após o desligamento do colaborador deve ser bloqueado o acesso do mesmo imediatamente ao sistema.

6- CONTROLE DE ACESSO AO AMBIENTE FÍSICO DA SERVENTIA

Ambientes Físicos: o acesso as dependências devem ser autorizados pelos operadores e controladores, mediante o uso de senha, sendo vedado a entrada de pessoas não autorizadas.

Áudio, Vídeos e Fotos: Qualquer atividade relacionada a gravação de áudio, vídeo ou foto dentro das dependências , deve ser autorizada pelo controlador, inclusive no âmbito acadêmico ou uso nas mídias sociais.

7- REMOÇÃO DE PROGRAMAS DE RASTREIO OU BLOQUEIO DE INTERNET E ANTI-VIRUS OU REMOÇÃO DE SOFTWARE

A remoção de quaisquer software somente pode ser efetuada pelos profissionais de TI da Serventia ou mediante autorização do controlador.

Os softwares de segurança, como antivírus e patches de segurança, não devem ser desinstalados sem a autorização prévia do Gestor de Segurança da Informação.

8- DESCARTES DE MATERIAIS CONTENDO DADOS PESSOAIS OU SENSÍVEIS

Todo e qualquer material a ser descartado deve seguir os preceitos da Corregedoria Geral de Justiça e do provimento 50 do CNJ, devendo antes do seu descarte físico ser devidamente digitalizado e mantido em dispositivo de armazenamento – HD externo e sendo vedado o uso fora da finalidade que tenha sido coletado.

Os descartes físicos devem ser efetuado através de desfiguração total dos dados através de trituradores de Papéis da serventia, sendo vedado o mero descarte sem as cautelas expostas nesse documento.

9- CONTROLE DOS DADOS NAS ESTAÇÕES DE TRABALHO

O acesso as estações de trabalho é pessoal e não deve ser compartilhada com terceiro estranho ao serviço.

Os dados sensíveis ou críticos, em papel ou em mídia de armazenamento eletrônicas, devem ser guardadas em lugar seguro quando não estiverem em uso, especialmente quando as dependencias físicas estiverem desocupadas. Quando em uso, o colaborador deverá tomar as medidas de segurança para evitar o vazamento ou uso indevido dos dados.

Os recursos de processamento de informação (computadores, notebooks, servidores, etc) devem ser mantidos desligados ou protegidos com mecanismo de tecla de bloqueio, senhas ou outros controles, quando não usados.

Os papéis que contenham dados pessoais ou sensíveis devem ser removidos das impressoras ou quaisquer dispositivos de scanner, digitalizadora, imediatamente após o uso.

10- ACESSO REMOTO

O trabalho e acesso é permitido somente ao suporte técnico de TI ou ao suporte técnico do sistema virtus, mediante solicitação de dos programas: anydesk e teamview, deve ser solicitado o acesso para o operador que estiver de uso da máquina, sendo vedado permitir acesso a terceiros que não especificados, salvo com autorização expressa do controlador.

O acesso remoto por colaborador deve ser feito somente através de comunicado e autorização do controlador.

11- DAS CLÁUSULAS PARA CONTRATAÇÃO DE PRESTADORES E SERVIÇOS E COLABORADORES

As contratações de prestadores de serviços e colaboradores que que lide com tratamento de dados e tenham acesso as informações da Serventia de Notas e Protesto de Toritama deve ser precedida de devem ser precedidos por termos de confidencialidade e cláusulas contratuais relacionadas à Segurança da informação e privacidade.

12- CÓPIA DE SEGURANÇA (BACKUP)

O cartório de Toritama mantém cópia de segurança extraída diretamente do servidor através de armazenamento na Nuvem e em dispositivo externo (HD).

13- COMPARTILHAMENTO DA SENHA DE INTERNET (VEDAÇÃO)

É vedado o compartilhamento da senha de internet usada pelo Cartório, devendo disponibilizar uma rede própria para acesso de clientes e mudanças periódicas da senha para evitar acessos indevidos.

14 – INSPEÇÃO REGULAR

A serventia de Notas e Protesto de Toritama(PE) solicitará a cada intervalo de 02 (dois) meses a inspeção e verificação pelo técnico de TI e sistema sobre a vulnerabilidade dos ativos.