FILHORINI
ADVOGADOS ASSOCIADOS

Política de Segurança de Dados

1. REFERÊNCIAS LEGISLATIVAS

Esta **POLÍTICA DE SEGURANÇA DE DADOS** ("**PSD**") refere-se, sem prejuízo da referência a outros diplomas legais de escopo mais geral, aos seguintes diplomas legais, com os quais devem, no mínimo, se conformar, exceto se padrão mais alto for aqui estabelecido:

- Lei nº 8.906/1994, Estatuto da Advocacia
- Código de Ética e Disciplina da Ordem dos Advogados do Brasil
- Lei nº 12.965/2014, Marco Civil da Internet
- Lei nº 13.709/2018, Lei Geral de Proteção de Dados ("**LGPD**") e seu Regulamento

As referências acima incluirão, automaticamente, as alterações que venham a ser introduzidas nesses diplomas e a sua eventual substituição e, em todos os casos, a aplicação desta PSD deverá ser orientada pelas boas práticas.

2. OBJETIVO, DEFINIÇÕES E ABRANGÊNCIA

Esta **PSD** é aplicável e deve ser observada por todos os sócios, empregados e colaboradores a todo e qualquer título (**USUÁRIO**) da **FILHORINI ADVOGADOS ASSOCIADOS** (**SOCIEDADE**) e tem o objetivo de estabelecer as diretrizes e padrões de operação dos recursos de informática, com vistas a assegurar a segurança, disponibilidade, integridade, confidencialidade, legalidade, autenticidade, acuracidade, completude e auditabilidade dos dados tratados pela **SOCIEDADE.**

O termo **RECURSOS DE INFORMÁTICA** compreende todos os equipamentos de

comunicação, processamento e armazenamento de dados de propriedade da **SOCIEDADE** ou por ela contratados para esse fim, incluindo microcomputadores e unidades de armazenamento autônomas, bem como todos os softwares, o que compreende desde sistemas operacionais, firewall, VPN, antivirus, programas e aplicativos diversos, por ela contratados para o processamento dos dados inerentes às atividades do objeto social da **SOCIEDADE**, sua proteção e bom funcionamento (doravante, conjuntamente, **RECURSOS DE INFORMÁTICA**).

A **SOCIEDADE** contratará e manterá em funcionamento adequado e permanente, ferramentas de segurança física e lógica de equipamentos, sistemas e dados, bem como de monitoramento contínuo de segurança, de forma a assegurar o bom funcionamento e a segurança dos **RECURSOS DE INFORMÁTICA**.

O termo "tratamento" nesta **PSD**, quando associado a dado ou informação, deve ter o significado previsto na Lei 13.709/18, a LGPD, ainda que tal dado não seja necessariamente um dado pessoal.

Considera-se um **DADO** (ou **DADOS**, no plural) toda e qualquer informação em meio digital para tratamento pelo **RECURSOS DE INFORMÁTICA** da **SOCIEDADE.** A definição de **DADO** inclui todo e qualquer dado ou informação além daqueles definidos como pessoais pelo Marco Civil da Internet e na LGPD, como também aqueles considerados sigilosos ou confidenciais pelo Estatuto da Advocacia, pelo Código de Ética e Disciplina da OAB. Os **DADOS** em outros meios físicos, tais como correspondências, procurações, certidões, entre outros, são igualmente protegidos de conformidade com política específica, não compreendida nesta **PSD**.

Esta **PSD** objetiva informar, padronizar e assegurar que seja dispensado tratamento bom e seguro aos **DADOS** da **SOCIEDADE**. Todavia, ela não exaure a matéria e, no cumprimento das diretrizes estabelecidas nesta **PSD**, conforme venha a ser alterada

de tempos em tempos, cumprirá ao **USUÁRIO** pautar-se pelo princípio da precaução, ou seja, em caso de qualquer dúvida, não se deve realizar o procedimento duvidoso e buscar ajuda junto ao **ADMINISTRADOR DO SISTEMA**, ou a quem ele delegar as tarefas de suporte.

Os **USUÁRIOS** serão responsáveis pela correta utilização dos **RECURSOS DE INFORMÁTICA** e pelo bom e seguro tratamento dos **DADOS**, mediante cumprimento das diretrizes estabelecidas nesta **PSD**, conforme atualizada de tempos em tempos, extendendo-se aos **USUÁRIOS** não advogados todas as obrigações legais e éticas aplicáveis por lei àqueles advogados no que concerne ao escopo da presente.

O descumprimento de conduta ou procedimento previsto nesta **PSD**, independente do resultado verificado e sem prejuízo das sanções legais aplicáveis, será tido como violação grave das Regras Internas, sujeitando o **USUÁRIO** descumpridor às sanções administrativas, inclusive, de cunho trabalhista.

3. UTILIZAÇÃO DOS RECURSOS DE TECNOLOGIA

Os **RECURSOS DE INFORMÁTICA** estão disponíveis aos colaboradores da **SOCIEDADE** para o desempenho das atividades do seu objeto social e todos os colaboradores são responsáveis pela boa utilização, segurança e preservação do sigilo dos **DADOS** manuseados.

Somente sócios, empregados e prestadores de serviços da **SOCIEDADE** poderão possuir login de **USUÁRIO**, o qual será atribuído pelo **ADMINISTRADOR DO SISTEMA**. Visitantes não terão acesso aos **RECURSOS DE INFORMÁTICA** e, na eventualidade de isso ser necessário, por qualquer razão, um login especial, com acesso temporário, limitado e supervisionado deverá ser requisitado ao

ADMINISTRADOR DO SISTEMA.

Apenas o prestador de serviços de Informática está autorizado a alterar configurações dos computadores, efetuar atualizações de versões de software, remanejar equipamentos e outras atividades similares.

4. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A suspeita de qualquer quebra ou fragilidade de segurança da informação, ainda que simplesmente potencial, ou de evento que seja decorrente de falha técnica em **RECURSO DE INFORMÁTICA** (qualquer deles, um "**EVENTO DE SEGURANÇA**"), deve ser imediatamente comunicada ao **DEPARTAMENTO ADMINISTRATIVO** (incluindo o **ADMINISTRADOR DO SISTEMA**) e ao **ENCARREGADO** (**DPO - DATA PROTECTION OFFICER**), de forma a permitir a tomada de ação corretiva no menor prazo possível.

Quando qualquer **EVENTO DE SEGURANÇA** decorra de conduta comissiva ou omissiva de **USUÁRIO**, culposa ou dolosa, a comunicação também deve ser extendida a pelo menos um dos **SÓCIOS ADMINISTRADORES**, para as medidas cabíveis.

A comunicação de qualquer **EVENTO DE SEGURANÇA** deve conter a descrição dos fatos e elencar todas as evidências que, no entender do comunicante, indiquem para a ocorrência de Evento de Segurança, a ser imediatamente investigado e, se caso, aferido e corrigido.

Suspeita de Quebra de Segurança de Dados Pessoais. Em caso de **EVENTO DE SEGURANÇA** que envolvam **DADOS PESSOAIS**, mesmo que haja apenas suspeita, a **SOCIEDADE** deverá tomar imediatamente **(i)** todas as medidas destinadas a fazer cessar as causas de tais eventos e mitigar seus efeitos, **(ii)** identificar o universo de

DADOS afetados, ainda que potencialmente, **(iii)** ainda que não haja comprovação, deverá comunicar a ocorrência ou possibilidade de ocorrência de **EVENTO DE SEGURANÇA** tão logo possível **(iii.a)** o(s) titutar(es) dos dados e a **(iii.b)** Autoridade Nacional de Proteção de Dados (ANPD) dando conta da situação, das medidas tomadas e, se pertinente, das recomendações para cessar ou mitigar danos e prejuízos, **(v)** investigar o **EVENTO DE SEGURANÇA** exaustivamente, documentando-o e promovendo todas as correções e remediações cabíveis, e **(v)** investigar e acompanhar a ocorrência junto à ANPD e aos titulares dos **Dados** afetados ou potencialmente afetados, até seu completo encerramento, com comunicação formal a todos os envolvidos.

5. AÇÕES COORDENADAS

A segurança da informação também é preservada por meio de ações coletivas coordenas, entre as quais:

- Caberá ao responsável pelos assuntos de Recursos Humanos:
  - Divulgar internamente, principalmente ao **ADMINISTRADOR DO SISTEMA**, as contratações, remanejamentos e desligamentos de pessoal, para fins de aprovação ou remoção de acessos de **USUÁRIOS**.
  - Organizar treinamentos de recepção de novos colaboradores e, também, periódicos a todos os **USUÁRIOS** sobre as políticas internas da **SOCIEDADE** quanto à SEGURANÇA DE DADOS E PRIVACIDADE E MELHORES PRÁTICAS, inclusive esta **PSD** e outras que as venham substituir ou completar.
- Cabe ao **ADMINISTRADOR DO SISTEMA**:
  - Conceder ou remover os acessos de acordo com as informações do responsável pelo RH e recursos tecnológicos existentes;
  - Revisar periodicamente os acessos;

- A atividade de **ADMINISTRADOR DO SISTEMA** poderá ser terceirizad para pessoa física ou jurídica, e será responsável pela operação dos **RECURSOS DE INFORMÁTICA**, sob a supervisão dos Sócios Administradores.

➢ Cabe aos Sócios Administradores, como medida integrante dos procedimentos de COMPLIANCE promover:

- O controle das alçadas em relação a disponibilização de acessos;
- Monitoramento dos acessos e informações;
- Divulgação desta **PSD** aos novos membros da **SOCIEDADE** e, quando aplicável, aos contratados;
- A avaliação da adequação e suficiência dos controles e procedimentos de segurança existentes e sua verificação permanente e auditoria periódica com vistas à identificação de deficiências e irregularidades que possam comprometer a segurança e o desempenho organizacional, promovendo a sua correção e atualização permanente

Boas Práticas e Princípio da Precaução. As práticas acima não pretendem ser exaustivas nem literais, não excluem o bom senso e as boas pátricas de mercado, que devem sempre pautar-se com base no PRINCÍPIO DA PRECAUÇÃO, que recomenda a abstenção com relação a qualquer ato quanto ao qual possa haver dúvida quanto aos resultados ou a extensão destes, hipótese em que a assistência do **ADMINISTRADOR DO SISTEMA** deve ser buscada.

6. SEGURANÇA FÍSICA E DE AMBIENTE

A **SOCIEDADE** mantém uma estrutura física e de ambiente adequadas ao seu porte e a suas atividades, que conta com procedimentos de prevenção a acessos físicos não autorizados, danos às instalações, fraude e sabotagem.

Áreas Restritas. Nenhum terceiro, prestador de serviço, visitante e/ou cliente,

poderá acessar os perímetros seguros sem estar acompanhado por, pelo menos, um membro da **SOCIEDADE**, a quem cumprirá então a obrigação de fazer com que sejam respeitadas as disposições desta **PSD**, inclusive, quanto a tal terceiro.

Entende-se por perímetro seguro todas as salas reservadas aos sócios, advogados, serviços de escritórios e demais colaboradores, além dos locais físicos onde estão instalados os **RECURSOS DE INFORMÁTICA**, notadamente, racks e servidores de informática e telefonia.

Considera-se estarem fora do perímetro seguro, os banheiros e as salas de reunião. Nesses locais deverá ser proporcionado acesso WiFi à internet, com estrutura que não passe pelos **RECURSOS DE INFORMÁTICA**.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade de cada sócio estabelecer critérios relativos ao nível de confidencialidade dos **DADOS** (documentos, relatórios e/ou mídias) tratados por sua área, de acordo com os seguintes critérios:

(1) **PÚBLICA** / (2) **INTERNA** / (3) **CONFIDENCIAL**

Informação Pública: É a informação que pode ser acessada por qualquer **USUÁRIO,** clientes, fornecedores, prestadores de serviços e público em geral e que não possui caráter de confidencialidade. Em geral, trata-se de informações sobre a Sociedade e trabalhos realizados pela Sociedade de caráter informativo que podem ser disponibilizadas no sítio da **SOCIEDADE** na rede mundial de computadores.

Informação Interna: É a informação, direta ou indiretamente relacionada às atividades da **SOCIEDADE** e que somente pode ser acessada pelos sócios e

advogados. O sigilo de toda Informação Interna, os **DADOS**, deve ser preservado e sua divulgação a terceiros é vedada, exceto àquelas pessoas que dela precisem tomar conhecimento para realizar suas atividades.

Informação Confidencial: É a informação que somente pode ser acessada por pessoas qualificadas, entre elas, exemplificativamente:

(a) **Dados pessoais** de sócios, advogados, contratados e colaboradores a qualquer título, deverão ser restritas ao departamento Pessoal e aos Sócios;

(b) **Contratos da Sociedade**. Os Contratos da Sociedade com outros escritórios e profissionais de advocacia, prestadores de serviços e outros são de acesso exclusivo dos Sócios e da Administração.

(c) **Contrato com Clientes**. Os Contratos de Prestação de Serviços e Honorários são de acesso exclusivo dos Sócios e da Administração da Sociedade

(d) **Documentos de Clientes**. Documentos de clientes que venham a ser definidos como sigilosos, como rendimentos, informações tributárias, dados de identificação, dados relacionados à saúde.

(e) **Casos Estratégicos ou Confidenciais**. Restritos aos Sócios e advogados que estejam trabalhando no caso.

Como regra geral, por tratar-se o objeto da Sociedade de serviços jurídicos, as Informações Internas deverão sempre e desde logo serem tratadas como confidenciais e sigilosas.

A classificação "Informação Confidencial", em geral, refere-se a informações sobre os clientes e sobre os assuntos relacionados a sua representação pela **SOCIEDADE**,

cujo grau de confidencialidade e sigilo é determinado por lei e cuja divulgação não apenas pode configurar crime, mas potencialmente pode causar danos e prejuízos morais ou patrimoniais não apenas a terceiros como também ao mercado, como seria o caso de informações estratégicas sobre negócios, mudanças de políticas laborais, ou mesmo privadas como aquelas associadas a divórcios e inventários.

Em qualquer caso, é importante ter sempre em mente que, mesmo dentro de trabalhos mais amenos e ordinários, é possível que hajam documentos confidenciais que devam ser segregados e tratados como tal, cabendo essa responsabilidade aos Sócios e advogados responsáveis pelo caso.

O acesso a Informação Confidencial por prestadores de serviços está condicionada a formalização de Acordo de Confidencialidade.

Todos requerimentos, condições e necessidades deverão ser formalmente comunicadas ao **ADMINISTRADOR DO SISTEMA**.

8. PROPRIEDADE DA INFORMAÇÃO

Todos os **DADOS**, ou seja, as informações geradas, manuseadas e armazenadas no ambiente tecnológico da **SOCIEDADE** são de sua propriedade, independente da origem, conteúdo ou propósito, incluindo o conteúdo dos e-mails, mensagens e correspondências.

9. GUARDA DA INFORMAÇÃO E DESCARTE

Os sócios e advogados devem observar as seguintes regras gerais:

- Guardar em gavetas ou armários providos de fechadura ou de outros mecanismos de proteção, documentos, papéis e mídias estritamente necessários, que contenham informações sensíveis ou críticas da **SOCIEDADE** e dos clientes;
- Nas ausências temporárias e no encerramento do expediente, obrigatoriamente, devem ser guardados todos os materiais de trabalho que comprometam a Segurança da Informação;
- Somente efetuar a impressão e a extração de cópia de documentos quando essencialmente necessário e descartar os documentos adequadamente assim que não forem mais utilizados;
- Retirar imediatamente da impressora os documentos impressos, principalmente os que contenham informações sensíveis e classificadas como confidenciais;
- Ao efetuar o descarte de papéis, verificar o conteúdo da informação, sendo esta de caráter restrito, picotar ou triturar o papel antes de descartá-lo.
- Quando o trabalho for efetuado na residência, manter documentos físicos guardados em locais próprios e adequados, somente quando estritamente necessários para a prestação de serviços, sem deixá-los à vista de terceiros, e descartá-los adequadamente quando seu uso não for mais necessário.

10. TOKENS E SENHAS DE ACESSO

Os membros dA **SOCIEDADE** possuem senhas individuais e personalizadas para acesso às informações, que de acordo com a atividade de cada colaborador, permitem incluir, excluir, alterar e consultar dados.

As senhas devem observar as seguintes configurações:

- Não conter partes significativas do nome da conta do usuário ou o nome todo;

- Ter pelo menos seis caracteres;
- Conter caracteres de três das quatro categorias a seguir:
  - Caracteres maiúsculos do inglês (A-Z)
  - Caracteres minúsculos do inglês (a-z)
  - Caracteres númericos (0-9)
  - Caracteres não-alfabéticos (por exemplo, !, $, #, %)

Os requisitos de complexidade são impostos quando as senhas são criadas ou alteradas.

As senhas devem ser alteradas sempre que solicitado pelo sistema e periodicamente pelo **USUÁRIO**, a cada três meses. É recomendável que o **USUÁRIO** altere a senha por inteiro, e não apenas um único caractere.

A senha nunca deve ser divulgada a terceiros (verbal ou escrita em local público), nem memorizada em logins automáticos, macros ou teclas de função.

As senhas são de responsabilidade pessoal do **USUÁRIO** e todos os acessos sob seu código serão atribuídos ao seu responsável nominal.

As senhas não conferem ao **USUÁRIO** nenhum direito de privacidade.

11. SOLICITAÇÃO DE ACESSOS PARA NOVOS MEMBROS

Cabe exclusivamente ao responsável pelos assuntos de RH informar ao **Administrador do Sistema** a contratação de novos membros.

Os acessos à rede e sistemas por novos membros devem ser previamente aprovados pelos Sócios Administradores.

Do mesmo modo, o responsável pelos assuntos de RH deverá informar ao **Administrador do Sistema** os desligamentos para as devidas providências.

12. TROCA DE PERFIL DE ACESSO

O pedido para incluir/excluir acessos de **USUÁRIOS** deve ser apresentado ao prestador de serviços de Informática pelos Sócios Administradores ou pelo responsável pelos assuntos de RH, após aprovação expressa de um dos Sócios Administradores.

13. LOGOFF E LOGOUT DO EQUIPAMENTO

a) Proteção de Tela

Os computadores da **SOCIEDADE** possuem protetor de tela ativo (screensaver) por tempo de inatividade.

b) Logoff em Ausências Temporárias

Quando de ausência temporária da estação de trabalho (período de almoço, reuniões etc.), o **USUÁRIO** deve bloquear a senha através do "Bloquear Computador", protegendo-a contra acessos indevidos, sob sua responsabilidade.

c) Logout e desligamento do equipamento

Os computadores devem ser desligados no final do expediente, sendo cada **USUÁRIO** que tenha posse sobre o equipamento responsável por desligá-lo, ou

cuidar para que isso seja feito.

14. UTILIZAÇÃO DE LAPTOPS E EQUIPAMENTOS COMPUTACIONAIS

- A proteção do recurso computacional de uso individual é de responsabilidade do **USUÁRIO**;
- É de responsabilidade de cada **USUÁRIO** assegurar a integridade do equipamento, a guarda e confidencialidade das informações contidas no mesmo;
- O **USUÁRIO** não deve alterar a configuração do equipamento recebido.
- Como regra, o não deve manter armazenados no equipamento quaisquer **DADOS**, ao contrário, fora do local da Sociedade, deve se utilizar-se do acesso **VPN** aos dados em nuvem.

Alguns cuidados devem ser observados:

➢ **Fora dA SOCIEDADE:**

- Mantenha o equipamento sempre com você.
- Atenção em restaurantes, hall de hotéis, aeroportos, aviões e táxis.
- Quando transportar o equipamento em automóvel utilize sempre o porta malas ou lugar não visível.
- Evite transportar o equipamento na rua.
- Em hipótese alguma deve-se levar consigo o equipamento para academias, deixando-os em armários ou aos cuidados de roupeiros, a bares e restaurantes para eventos como happy hours, deixando-os em chapelarias ou em cadeiras nas mesas em local de grande movimento.

➢ **Em caso de furto e/ou roubo:**

- Registrar imediatamente a ocorrência em uma delegacia de polícia.

- Comunicar ao Sócio responsável e ao **Administrador de Sistemas.**
- Caso o equipamento permita, providenciar o apagamento remoto de dados.

15. VÍRUS DE COMPUTADOR

Como regra fundamental, a **SOCIEDADE** não utiliza nenhum software ilegal e proíbe a seus membros sua utilização nos **RECURSOS DE INFORMÁTICA**. Os Recursos de Informática da Sociedade conterão, exclusivamente, os programas e aplicativos homologados pelo Administrador do Sistema.

O uso de software ilegal ("pirata"), bem como de freeware e quetais estão diretamente associados à contaminação do sistema por vírus, worms, cavalos de tróia, ransamware e quetais, de modo que a instalação e utilização de tais aplicativos, mesmo que por intermédio da internet, é terminantemente proibida, considerada falta grave.

A Internet também é, provalmente, o meio mais comum de contaminação de sistemas, de forma que, por esse motivo, os **USUÁRIOS** não devem acessar sites inseguros, abrir arquivos ou links desconhecidos e/ou recebidos de desconhecidos ou em situação suspeita.

Embora **A SOCIEDADE** possua programa antivírus instalado em todo seu parque de informática, com atualização automática e checagem em tempo real, o contato com arquivos contaminados pode trazer graves consequências.

No caso de dúvida sobre o remetente ou o conteúdo, ao receber um e-mail, não abra anexos ou clique em links. Comunique imediatamente o prestador de serviços de Informática e demais membros da equipe.

16. ACESSO À INTERNET

Não é permitido instalar programas provenientes da Internet nos computadores da **SOCIEDADE** sem expressa anuência do prestador de serviços de Informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais. Os **USUÁRIOS** devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De estações de rádio e TV.
- De conteúdo pornográfico ou imagens e vídeos relacionados a sexo.
- De sites de compartilhamento e distribuição de arquivos.
- Que defendam atividades ilegais.
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes.
- Que promovam a participação em salas de discussão.
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

O prestador de serviços de Informática está autorizado a efetuar monitoramento dos acessos. Os sócios podem analisar, aleatória ou direcionadamente, todos os acessos.

17. CORREIO ELETRÔNICO (OUTLOOK)

O correio eletrônico (e-mail) da **SOCIEDADE** é o Outlook e deve ser utilizado exclusivamente para fins profissionais. Todo o conteúdo e mensagens

armazenadas/trafegadas pelo Outlook são de propriedade da **SOCIEDADE** e poderão ser objeto de monitoramento.

Toda a informação veiculada através de e-mail deve ser tratada como Informação Confidencial e de propriedade da **SOCIEDADE**, incluindo eventuais e-mails pessoais.

Os colaboradores são responsáveis pelas mensagens enviadas em seu nome, atentando- se para os seguintes itens:

A opção "***Responder a todos***" deve ser utilizada apenas se justificada a ação, caso contrário, utilize "Responder" apenas para o remetente;

- As mensagens com arquivos anexados impactam fortemente no espaço em servidor. Nunca distribua mensagens com arquivos anexados sem necessidade;
- As mensagens de e-mail correspondem a documentos formais da **SOCIEDADE** e por esse motivo devem ser elaboradas com linguagem coerente com a atividade profissional;
- As mensagens não devem conter declarações difamatórias e/ou linguagem ofensiva;
- As mensagens não devem ser hostis;
- Não respondam a mensagens de "correntes" ou com conteúdo pornográfico, que possam prejudicar a imagem da **SOCIEDADE** e de seus membros.

18. MENSAGENS INSTANTÂNEAS (MSG)

O **USUÁRIO** deve ter em mente e observar que a comunicação por mensagens curtas de texto, seja diretamente na rede de celular seja por intermédio de aplicativos ou plataformas, deve se destinar exclusivamente a atos de coordenação como de

confirmação do envio de e-mails e arquivos, confirmação de reuniões, entre outros.

Embora vários de tais aplicativos tenham a capacidade de enviar e receber arquivos, o uso dessa facilidade deve ser evitado para fins de tráfego de informações profissionais, dando-se preferência ao envio pelo e-mail institucional do **USUÁRIO** na **SOCIEDADE**, notadamente, quando se tem em mente que certos aplicativos não compõem os **RECURSOS DE INFORMÁTICA** da **SOCIEDADE**, de forma que tais comunicações, se um lado, não estão compreendidas entre aquelas de que são regularmente feitas cópia de segurança e, de outra, tampouco são verificadas por aplicações anti-virus, de forma que o upload de tais arquivos pode colocar em risco os **RECURSOS DE INFORMÁTICA** como um todo.

Sem prejuízo do antecedente, os **USUÁRIOS**, entre si e com terceiros, devem preservar o tratamento formal e adotar forma de tratamento essencialmente profissional, evitando ambiguidades e comportamentos vedados.

19. VPN (VIRTUAL PRIVATE NETWORK) E ACESSO REMOTO

Os Recursos de Informática da **SOCIEDADE** incluem a utilização de dispositivos como firewall, antivirus e **VPN**, que permitem sua utilização remota por intermédio da internet.

Todavia, em acesso fora do ambiente interno dos **RECURSOS DE INFORMÁTICA**, o **USUÁRIO** é responsável pela guarda e confidencialidade das informações acessadas fora das dependências da **SOCIEDADE**, seja quanto à sua segurança física, carregando consigo no seu equipamento pessoal somente os dados e informações estritamente necessários, seja ainda utilizando-se da proteção do **VPN** da **SOCIEDADE** no acesso remoto e observando de forma redobrada as demais regras e recomendações contidas

nesta **PSD** .

20. WIRELESS (REDE SEM FIO)

A **SOCIEDADE** possui acesso wireless à rede interna disponíveis para **USUÁRIOS** na maior parte das salas de trabalho e, também, nas salas de reuniões. O acesso para não **USUÁRIOS**, deve necessariamente ser feito por intermédio da rede wireless para visitante, que não permite acesso à rede interna da **SOCIEDADE**.

As senhas de acesso à rede Wireless para **USUÁRIOS** não devem em hipótese alguma serem disponibilizadas para terceiros, incluindo visitantes e prestadores de serviços que não necessitem ter acesso à rede interna da **SOCIEDADE**.

Na hipótese em que terceiros, sejam eles parceiros, visitantes, clientes, prestadores de serviços ou outros necessitem ter acesso à rede interna da **SOCIEDADE**, seja por acesso wireless ou por cabo, deve ser feito requerimento específico ao Administrador do Sistema que, uma vez aprovado, fornecerá senha e login específicos, com as permissões adequadas.

Na hipótese em que haja qualquer suspeita de que senha de **USUÁRIO** wireless tenha sido comprometida, sua substituição deverá ser providenciada imediatamente e esse fato (um **EVENTO DE SEGURANÇA**) deverá ser comunicado imediatamente ao Administrador do Sistema.

21. ARMAZENAMENTO DE DADOS

O armazenamento de dados da **SOCIEDADE** é feito em ambiente remoto (nuvem), onde são realizadas periodicamente cópias de segurança regulares (*back ups*).

A localização e nomenclatura das pastas de armazenamento (diretórios) deve obedecer às instruções específicas e padronizadas, via de regra orientando-se por cliente, caso e atividade, de forma a propriciar agilidade nas buscas para todos os **USUÁRIOS** com acesso àquela pasta.

Preferencialmente, o trabalho deve ser realizado utilizando-se informações contidas diretamente na pasta de trabalho na rede da **SOCIEDADE**, de forma a assegurar a utilização por todos do mesmo arquivo, na mesma versão e evitar a duplicação indevida e a propagação de cópias não autorizadas.

Excepcionalmente, o **USUÁRIO** poderá realizar cópia, seja em outro local da rede seja no seu equipamento pessoal, com vista a viabilizar a realização de trabalhos em que o acesso concorrente de vários **USUÁRIOS** possa dificultar o trabalho ou, ainda, em condições onde o acesso à internet seja ruim ou inexistente, sempre observando as demais regras e recomendações nesta **PSD** e as boas práticas.

Nessas hipóteses, o arquivo deverá ser identificado e manuseado adequadamente, de forma a não comprometer o trabalho de outros integrantes do grupo envolvidos na prestação de serviços afins. A cópia deverá ser excluída tão logo cessada a necessidade que lhe deu origem e o arquivo de trabalho, antes de ser gravado na rede (*upload*) deverá necessariamente ser testado e verificado para a detecção de vírus eletrônicos, *malwares*, cavalos de tróia e congêneres previamente ao seu *upload*, não sendo autorizado o *upload* caso essa verificação não tenha sido realizada.

O **USUÁRIO** deve evitar manter cópias de pastas no seu computador ou outro dispositivo, restringindo tais cópia aos trabalhos em andamento e nas hipóteses autorizadas acima, para evitar comprometer a segurança de dados em razão de perda ou furto de equipamento, ou hackeamento do computador (notebook ou

outro).

Particularmente, atenção especial deve ser dada a dispositivos de armazenamento externo, tais como discos rígidos e pen-drivers. Como regra geral, somente o **ADMINISTRADOR DO SISTEMA** poderá realizar cópias de dados em tais dispositivos, porém, em todos os casos, registrando sua existência.

Excepcionalmente, o uso de tais dispositos poderá ser autorizado em casos específicos para viabilizar o transporte e transferência de dados, quando não seja possível ou recomendável fazê-lo por intermédio da rede, seja por razões de segurança, seja por razões técnicas.

Em qualquer caso, quando cessarem as razões que autorizaram a utilização de tais dispositivos, os mesmos deverão ser apagados e formatados, preferentemente, pelo **ADMINISTRADOR DO SISTEMA**.