POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA SONNTAG – CORRETORA DE SEGUROS E ADMINISTRADORA LTDA.

1. OBJETIVOS E PRINCÍPIOS

A SONNTAG - CORRETORA DE SEGUROS E ADMINISTRADORA LTDA. (a "Sonntag Seguros") busca sempre, em todas as suas atividades, garantir a privacidade e a segurança das informações de cada um de seus clientes, parceiros e colaboradores.

Neste sentido, esta Política de Segurança da Informação ("PSI") tem por objetivo orientar e estabelecer as diretrizes corporativas da Sonntag Seguros para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários, devendo ser obrigatoriamente cumprida e aplicada em todas as áreas da empresa.

Desta maneira, a Sonntag Seguros está comprometida em cumprir os três princípios basilares da Segurança da Informação, quais sejam:

- **Confidencialidade**: garantia de que a informação acessível somente por pessoas autorizadas;

- **Integridade**: garantia de que a informação seja mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais; e

- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2. USO DE CRIPTOGRAFIA E OUTROS RECURSOS DE PROTEÇÃO DE DADOS

A Sonntag Seguros se compromete a sempre realizar a criptografia das informações, ou seja, realizar a codificação e decodificação dos dados armazenado em seu Banco, através da ferramenta **"*Acronics*"**.

3. NORMAS DE BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento para que sejam preferencialmente executados fora do horário comercial e em período "diário/semanal/mensal" pelo provedor do software da Sonntag.

As mídias de backup (como NUVEM, DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro e distantes o máximo possível do Datacenter.

Na situação de erro no backup automatizado, é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado o problema.

4. POLÍTICAS DE SENHAS E RESTRIÇÕES DE ACESSO

Os usuários dos sistemas da Sonntag são pessoalmente responsáveis pelo uso correto de suas credenciais perante a empresa e terceiros, nos termos da legislação em vigor.

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

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha, conforme as orientações apresentadas.

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 armazenadas em arquivos eletrônicos compreensíveis por linguagem usual (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, etc; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Os usuários devem, também, utilizar senhas diferentes para cada sistema e/ou dispositivo, que deverão ser alteradas, pelo menos, a cada trimestre. Os sistemas em questão, portanto, devem forçar a troca das senhas dentro desse prazo.

Todos os acessos a sistemas e dispositivos 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 à Consultoria de TI, a fim de que essa providencia 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 ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

5. USO DA INTERNET

Todas as regras atuais da Sonntag Seguros visam ao desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet, seja no escritório físico da empresa ou fora deste.

A internet disponibilizada pela Sonntag Seguros aos seus colaboradores e visitantes, independentemente de sua relação contratual, é uma ferramenta de trabalho da empresa e não pode ser utilizada para fins pessoais, razão pela qual a Sonntag Seguros, nos termos da legislação, se ressalva a monitorar e registrar todos os acessos realizados em sua rede.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da empresa, 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 privadas da rede, visando a assegurar o cumprimento de sua Política de Segurança da Informação.

Apenas os colaboradores autorizados pela Sonntag Seguros poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à Política de Privacidade da empresa, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

Os colaboradores com acesso à internet poderão fazer o download somente se autorizados pela administração, e somente de programas ligados diretamente às suas atividades na Sonntag Seguros, devendo providenciar o que for necessário para regularizar a licença e o registro desses programas.

6. USO DE COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponibilizados aos colaboradores são de propriedade da Sonntag Seguros, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da empresa, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências 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 da Consultoria de TI da Sonntag Seguros, ou de quem este determinar.

Os sistemas e computadores devem ter os softwares de antivírus e antimalware escolhidos pela empresa instalados, ativados e atualizados permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a Consultoria de TI mediante registro de chamado no service desk.

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

Documentos necessários às atividades dos colaboradores da empresa deverão ser salvos em drives de rede da Sonntag Seguros, sob responsabilidade do próprio usuário.

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

- O colaborador deverá manter a configuração do equipamento disponibilizado pela Sonntag Seguros, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da empresa, assumindo a responsabilidade como custodiante de informações;

- Deverão ser protegidos por senha (bloqueados) todos os terminais de computador e impressoras quando não estiverem sendo utilizados;

- Todos os recursos tecnológicos adquiridos pela Sonntag Seguros devem ter imediatamente suas senhas padrão (default) alteradas;

- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

7. USO DO E-MAIL CORPORATIVO

O uso do correio eletrônico da Sonntag Seguros é exclusivo para fins corporativos e relacionados às atividades do colaborador usuário dentro da empresa. A utilização desse serviço para fins pessoais não é permitida.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da Sonntag Seguros para:

- Enviar mensagens, não solicitadas, para múltiplos destinatários, exceto se relacionadas a uso legítimo da empresa;

- 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;

- Produzir, transmitir ou divulgar mensagem que viole, a qualquer título, a presente Política de Segurança da Informação, da Política de Privacidade da Sonntag Seguros ou a legislação em vigor.

8. CONTROLE DE ACESSO

Os acessos aos dados e informações da Sonntag Seguros serão disponibilizados aos colaboradores de acordo com a atividade inerente ao seu cargo.

A liberação de acesso só será efetivada após avaliação e aprovação dos sócios da Sonntag Seguros, para que se evite ameaças à integridade e sigilo das informações contidas na rede.

O cancelamento de acesso deverá ser realizado: (i) ao término do período solicitado ou do contrato do colaborador; (ii) quando encerrada a finalidade pela qual o acesso foi liberado; (iii) na hipótese de identificação de vulnerabilidade, risco de vazamento de dados ou uso indevido do acesso.

9. TRABALHO REMOTO

Quando necessária, a prática do *home office* será permitida aos colaboradores da Sonntag Seguros, desde que sejam observadas e seguidas as regras abaixo, visando a realização de um trabalho produtivo:

Espaço adequado:
A residência deverá ter conexão estável com a internet, essencial para a realização do trabalho a distância. Se positivo, deverá ser avaliado o melhor lugar para instalação do computador e utensílios de trabalho.

Disponibilidade:
É fundamental que o colaborador da Sonntag Seguros esteja 100% disponível durante todo o horário comercial, assim como estaria em condições normais.

Cuidados necessários:
Importante que o colaborador tenha zelo e cuidado com o computador e/ou material fornecido pela Sonntag Seguros para a realização de seu home office, além de utilizar os meios de comunicação adotados pelo escritório para suas tarefas e contatos com outros colaboradores.

Uso da rede:
Assim como no escritório, todos os documentos produzidos devem obrigatoriamente ser salvos na rede da Sonntag Seguros, não sendo permitido salvar ou manter qualquer documento salvo em pen drive ou no seu computador de uso pessoal. A confidencialidade das informações deve ser sempre preservada.

Confidencialidade:
Importante, ainda, ressaltar que muito embora o ambiente do home office não seja o do escritório, as informações devem continuar sendo adstritas e confidenciais, sendo vedada a discussão de assuntos sigilosos da Sonntag Seguros e/ou de seus clientes com familiares.

10. ROTINAS DE AUDITORIA

A Sonntag Seguros, bem como todos os seus gestores, são responsáveis por fiscalizar e prevenir a violação das normas estabelecidas nesta Política de Segurança da Informação, sendo certo que, caso constatada sua negligência ou inatividade, poderão ser, também, responsabilizados em eventual sanção.

Assim, para garantir as regras mencionadas nesta Política de Segurança da Informação, a Sonntag Seguros poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação da administração;

- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

11. PENALIDADES APLICÁVEIS

No caso de não cumprimento das normas estabelecidas nesta Política de Segurança da Informação, o funcionário ou colaborador poderá sofrer as seguintes penalidades:

- **Advertência verbal**: O colaborador será comunicado verbalmente que está infringindo as normas da Política de Segurança da Informação da Sonntag Seguros e será recomendado à leitura desta Norma;

- **Advertência formal**: A primeira notificação será enviada ao colaborador informando o descumprimento da norma, com a indicação precisa da

violação cometida. A segunda notificação será encaminhada para a chefia imediata do infrator.

- **Dispensa por justa causa ou rescisão do Contrato de Prestação de Serviços**: Na hipótese de violação reiterada da Política de Segurança da Informação, a despeito das advertências, o colaborador estará sujeito à dispensa por justa causa, nos termos da legislação em vigor, ou, se aplicável, à rescisão motivada do contrato de prestação de serviços.