SUMÁRIO

1. APLICAÇÃO

Este documento se aplica a **Exclusive Seguros**.

INTRODUÇÃO:

A informação é um ativo crítico para as empresas e, por esse motivo, precisa ser

devidamente protegida. O uso cada vez mais intenso da tecnologia da informação e da interconectividade pelas empresas expõe as informações a ameaças e vulnerabilidades, tornando cada vez mais necessário garantir a sua segurança, integridade, confidencialidade, disponibilidade e autenticidade. De acordo com a ABNT NBR ISO/IEC 27002 (2005, p. X), “seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada e armazenada, é recomendado que ela seja sempre protegida adequadamente”.

A presente Política de Segurança da Informação - a PSI - está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes no Brasil. Outras PSIs foram consultadas e utilizadas como referências de normas e procedimentos de segurança da informação.

Tais normas são fornecidas a título de orientação aos colaboradores e demais envolvidos. Caso os procedimentos ou normas aqui estabelecidos sejam violados, o Comitê de Segurança da Informação, a área de TI e o Departamento Jurídico juntamente com a direção da EXCLUSIVE, reservam-se no direito de aplicar as punições cabíveis aos colaboradores responsáveis pela violação da política.

2. OBJETIVO:

Definir normas e procedimentos de segurança que visem disciplinar o uso da tecnologia de informação e, consequentemente, garantir a segurança da informação, e orientar os colaboradores quanto à sua importância, conduta e procedimentos adotados pela EXCLUSIVE.

3. CONDIÇÕES GERAIS:

3.1. DESCRIÇÃO:

Esta PSI aplica-se a qualquer colaborador com acesso às informações da EXCLUSIVE, e dá ciência de que seus sistemas, computadores e redes poderão ser monitorados, com prévia informação, conforme previsto nas leis brasileiras.

É obrigação de cada colaborador manter-se atualizado em relação aos procedimentos e normas aqui relacionadas, buscando orientação sempre que não estiver absolutamente seguro quanto à obtenção, uso e/ou descarte de informações.

Esta política estará sempre disponível para consulta dos colaboradores no Departamento Pessoal, cabendo ao mesmo divulgar através da Comunicação Interna.

3.2. PRINCÍPIOS:

A informação produzida ou recebida pelos colaboradores é resultado de sua

atividade profissional e pertence à EXCLUSIVE.

Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade intelectual, industrial (Lei nº 9279) e de direitos autorais (Lei nº 9610).

A segurança da informação depende de pessoas comprometidas, da execução dos processos gerenciais de controle definidos e da correta utilização dos sistemas de informação.

3.3. COMITÊ DE SEGURANÇA DA INFORMAÇÃO:

A EXCLUSIVE instituiu um Comitê para gerenciar a segurança da informação. Ele é formado por um representante de cada uma das seguintes áreas: TI, Diretoria e Financeiro.

O Comitê deverá se reunir formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a EXCLUSIVE.

3.4. RESPONSABILIDADES:

A EXCLUSIVE entende que a Política de Segurança da Informação somente será eficaz com o comprometimento de TODOS!

São objetos da PSI os serviços e recursos colocados à disposição dos colaboradores, tais como: computadores, telefones celulares, notebooks, correio eletrônico, Internet (*wi-fi*, e rede cabeada), informações armazenadas em arquivos físicos ou em diretórios da rede, nuvem corporativa e mídias digitais, além de sistemas de aplicação.

As normas descritas no decorrer deste documento devem sofrer alterações sempre que necessário, sendo que estas devem ser registradas e divulgadas pela empresa, considerando-se o tempo hábil para que eventuais providências sejam tomadas.

Caberá aos responsáveis hierárquicos zelar pelo cumprimento das responsabilidades. Cada colaborador será informado acerca de quem se reportará para fins desta Política.

3.4.1. Usuários

- ✓ Respeitar esta Política de Segurança da Informação;
- ✓ Assinar e praticar o Termo de Responsabilidade, Sigilo e Confidencialidade (no fim deste documento) como condição imprescindível para que seja concedido o acesso aos ativos e recursos cedidos pela EXCLUSIVE;
- ✓ Responder pela guarda e proteção dos recursos computacionais colocados à sua

disposição para o trabalho;

- ✓ Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- ✓ Ativar suas senhas de proteção para Correio Eletrônico (e-mail) e Sistema Operacional, sob orientação da área de TI;
- ✓ Buscar conhecimento necessário para a correta utilização dos recursos de *hardware* e *software*, consultando a área de TI, quando necessário;
- ✓ Garantir os cuidados mínimos com a segurança da informação, quando as atividades forem executadas fora dos escritórios da EXCLUSIVE, como no caso de reuniões externas, trabalhos em casa, viagens etc.;
- ✓ Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus etc.;
- ✓ Assegurar que as informações e dados de propriedade da EXCLUSIVE ou dos clientes e parceiros externos não sejam disponibilizados a terceiros ou utilizados para outros fins, a não ser com autorização por escrito do responsável hierárquico e do cliente;
- ✓ Relatar para o seu responsável hierárquico e à área de TI o surgimento da necessidade de um novo *software* para suas atividades;
- ✓ Devolver os recursos colocados à disposição pela EXCLUSIVE ao término do contrato de trabalho, nas mesmas condições em que recebeu, assinando a devolução do Termo de Responsabilidade da TI pelos recursos;
- ✓ Responder pelo prejuízo ou dano que vier a provocar à EXCLUSIVE ou a terceiros em decorrência da não obediência às diretrizes e normas aqui referidas.

3.4.2. Responsáveis Hierárquicos:

- ✓ Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para os colaboradores sob a sua gestão;
- ✓ Exigir a assinatura do Termo de Compromisso, Sigilo e Confidencialidade dos colaboradores como condição imprescindível para que seja concedido o acesso aos ativos de informação pela empresa;
- ✓ Exigir a assinatura do Termo de Responsabilidade da TI pelos recursos da EXCLUSIVE, como condição imprescindível para que sejam concedidos os recursos de informática pela empresa;
- ✓ Atribuir, na fase de contratação e de formalização dos contratos individuais de trabalho CLT, prestação de serviços ou de parceria, a responsabilidade pelo cumprimento da PSI EXCLUSIVE;
- ✓ Autorizar o acesso e definir o perfil do usuário junto à área de TI;
- ✓ Autorizar as mudanças no perfil do usuário junto à área de TI;
- ✓ Orientar os usuários sobre os princípios e procedimentos de Segurança da Informação,
- ✓ Comunicar à área de TI, antecipadamente, a data de saída de colaboradores a fim

de assegurar os procedimentos de bloqueio de acesso aos sistemas e de devolução de recursos informacionais disponibilizados;

- ✓ Comunicar à área de TI, antecipadamente, quando um usuário for promovido ou transferido de área/gerência, para que sejam feitas as adequações necessárias para o acesso do referido usuário aos sistemas da EXCLUSIVE.
- ✓ Efetuar revisão periódica das credenciais a cada 30 dias, com validação dos perfis atribuídos pelo Gestor da Área;
- ✓ Notificar imediatamente ao gestor da área de TI quaisquer vulnerabilidades e ameaças à quebra de segurança;
- ✓ Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação;
- ✓ Advertir formalmente e aplicar sanções cabíveis ao usuário que violar os princípios ou procedimentos de segurança, relatando imediatamente o fato ao gestor da área de TI;
- ✓ Obter aprovação técnica do gestor da área de TI antes de solicitar a compra de *hardware*, *software* ou serviços de informática;
- ✓ Orientar os colaboradores quanto à devolução dos recursos colocados à disposição pela EXCLUSIVE ao término do contrato de trabalho, nas mesmas condições em que recebeu, assinando a devolução do Termo de Recebimento e Responsabilidade pelos recursos;
- ✓ Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

3.4.3. Área de TI

- ✓ Configurar os equipamentos, sistemas e redes para cumprir os requerimentos desta PSI;
- ✓ Testar a eficácia dos controles utilizados e informar aos gestores sobre os riscos residuais;
- ✓ Restringir o acesso de colaboradores aos logs e trilhas de auditoria das suas próprias ações, de forma a garantir que não sejam excluídos;
- ✓ Garantir segurança do acesso público e manter evidências que permitam a sua rastreabilidade para auditoria ou investigação;
- ✓ Controlar o acesso aos recursos de processamento da informação da EXCLUSIVE e ao processamento e comunicação da informação por colaboradores externos;
- ✓ Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;
- ✓ Administrar, proteger e testar as cópias de segurança dos programas e dados ao negócio da EXCLUSIVE;
- ✓ Gerenciar o descarte de informações, em qualquer formato, a pedido do dono da informação (custodiante);
- ✓ Garantir que as informações de um usuário sejam removidas antes do descarte ou

mudança de usuário;

- ✓ Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
- ✓ Criar e gerenciar credenciais de acesso aos colaboradores na EXCLUSIVE, para uso de computadores, sistemas, bases de dados e qualquer outro ativo de informação;
- ✓ Certificar que não exista em hipótese alguma, perfis ou usuários duplicados – cada usuário deverá ter EXCLUSIVAMENTE uma credencial;
- ✓ Proteger todos os ativos de informação da EXCLUSIVE contra códigos maliciosos e ou vírus;
- ✓ Garantir que processos de mudança não causem vulnerabilidades e/ou fragilidades no ambiente de produção;
- ✓ Definir as regras formais para instalação de *software* e *hardware*, exigindo o seu cumprimento dentro da EXCLUSIVE;
- ✓ Realizar inspeções periódicas de configurações técnicas e análise de riscos;
- ✓ Garantir, assim que solicitado, o bloqueio de acesso de usuários por motivo de desligamento da EXCLUSIVE;
- ✓ Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;
- ✓ 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 pode ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- ✓ Monitorar o ambiente de TI, a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso à internet e aos sistemas críticos da EXCLUSIVE, indisponibilidade aos sistemas críticos, incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante), a atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, *upload*/*download* de arquivos, entre outros);
- ✓ Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação do gerente (ou superior);
- ✓ Orientar os colaboradores externos que utilizam redes fora dos escritórios da EXCLUSIVE, sobre os cuidados mínimos com a segurança da informação;
- ✓ Realizar inspeção física nas máquinas de propriedade da EXCLUSIVE;
- ✓ Receber e conferir os recursos colocados à disposição para os colaboradores ao término do contrato de trabalho, garantindo as mesmas condições em que foram entregues para execução do trabalho;
- ✓ Gerenciar o relacionamento com os prestadores de suporte de TI.

3.4.4. Comitê de Segurança da Informação

- ✓ Propor as metodologias, sistemas e processos específicos que visem a aumentar a segurança da informação;
- ✓ Promover a conscientização dos colaboradores em relação à importância da segurança da informação;
- ✓ Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços;
- ✓ Buscar alinhamento com as diretrizes corporativas da EXCLUSIVE;
- ✓ Revisar essa PSI a cada 6 meses ou 1 ano ou, se necessário, quando houver algum incidente de segurança da informação e consequente mudança de procedimentos e normas;
- ✓ Comunicar aos colaboradores qualquer mudança nos procedimentos de controles que possam afetar a execução do seu trabalho e a segurança da informação.

3.5. RECURSOS COMPUTACIONAIS:

Os recursos de TI alocados pela EXCLUSIVE aos seus colaboradores são destinados exclusivamente às atividades relacionadas ao trabalho.

É proibida a intervenção do colaborador para manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, bem como a transferência e/ou a divulgação de qualquer *software*, programa ou instruções de computador para terceiros (pirataria).

Quando o contrato de trabalho terminar ou não estiverem sendo mais utilizados os recursos informacionais concedidos pela EXCLUSIVE, estes deverão ser encaminhados a área de TI pelos colaboradores que os receberam para a remoção das informações, descarte ou reuso. A área de RH deverá ser comunicada da devolução ou troca de qualquer recurso informacional por meio de chamado via **Portal GLPI**.

3.6. CONTROLE DE IDENTIFICAÇÃO (*LOGIN* E SENHA):

Senhas são um meio comum de validação da identidade do usuário para obtenção de acesso a um sistema de informação, serviço ou dispositivo/mídia (telefone corporativo, notebook, mídias, máquinas fotográficas etc.). A concessão de senhas deve ser controlada, considerando:

1- Senhas temporárias devem ser alteradas imediatamente, e não devem ser armazenadas de forma desprotegida;
2- A troca de senha será exigida a cada 45 dias para todos os colaboradores que utilizarem computadores e é recomendada essa periodicidade, também, para os demais recursos informacionais da EXCLUSIVE.

3- As senhas serão bloqueadas após cinco tentativas sem sucesso, sendo que o administrador da rede e o usuário devem ser notificados sobre estas tentativas. Para o desbloqueio é necessário que o usuário entre em contato com a área de TI.

As responsabilidades dos administradores dos sistemas e da rede incluem o cuidado na criação e alteração das senhas dos usuários, além da necessidade de manter atualizados os dados deles.

As responsabilidades do usuário incluem, principalmente, os cuidados com a manutenção da segurança dos recursos, tais como sigilo das senhas.

- ✓ As senhas são sigilosas, individuais e intransferíveis, não devendo ser divulgadas em nenhuma hipótese;
- ✓ Tudo que for executado com a senha de usuário da rede ou de sistema será de inteira responsabilidade do usuário. As senhas são efetivas apenas quando usadas corretamente e sua escolha e uso requerem alguns cuidados como:
  1- Não utilizar informações pessoais fáceis de serem obtidas, como o número de telefone, nome da rua, nome do bairro, cidade, data de nascimento etc.;
  2- Não utilizar senhas somente com dígitos ou com letras;
  3- Utilizar senha com pelo menos, oito caracteres;
  4- Misturar caracteres maiúsculos e minúsculos;
  5- Misturar números, letras e caracteres especiais;
  6- Incluir pelo menos um caractere especial;
  7- Utilizar um método próprio para lembrar a senha, de modo que ela não precise ser escrita em nenhum local, em hipótese alguma;
  8- Não anotar a senha em papel ou em outros meios de registro, e muito menos deixando a anotação visível e de fácil acesso;
  9- Não utilizar o nome do usuário;
  10- Não utilizar o primeiro nome, o nome do meio ou o sobrenome;
  11- Não utilizar nomes de pessoas próximas, como da esposa (o), dos filhos, de amigos;
  12- Não utilizar palavras que estão no dicionário (nacionais ou estrangeiras);
  13- Não utilizar senhas com repetição do mesmo dígito ou da mesma letra;
  14- Não fornecer sua senha para ninguém, por razão alguma;
  15- Utilizar senhas que podem ser digitadas rapidamente, sem a necessidade de olhar para o teclado.

3.7. DISPOSITIVOS PESSOAIS:

É proibida a utilização, pelo Colaborador, de dispositivos móveis particulares ou de terceiros (tais como celulares, smartphones, notebook, tablets, entre outros) para o desenvolvimento das atividades profissionais vinculadas à EXCLUSIVE. Excepcionalmente o Colaborador poderá utilizar seus dispositivos móveis particulares

quando houver uma justificativa que fundamente esse uso, sendo necessária a autorização expressa da EXCLUSIVE.

Excepcionalmente, o GSI poderá aprovar que determinados colaboradores possam configurar a conta de e-mail corporativa em seus dispositivos pessoais móveis (em especial, celular), desde que esse dispositivo possua função de encriptação de seu conteúdo. Nesta hipótese, a configuração deve sempre ser realizada pelo Departamento de TI, e o Colaborador desde já concorda que o Departamento de TI poderá configurar a opção de proteção do conteúdo do dispositivo por meio de criptografia. É importante ressaltar que, uma vez configurada a conta de e-mail corporativa, os dispositivos pessoais do colaborador também estarão sujeitos a monitoramento do uso do e-mail.

Todo e qualquer software da EXCLUSIVE que precise ser instalado em dispositivos pessoais, deverá ser aprovado pelo GSI.

3.8. TELA E MESAS LIMPAS:

A partir desta data, o papel de parede e proteção de tela de todos os micros deverá seguir a padronização da EXCLUSIVE;

O usuário deve cuidar para que papéis, mídias e imagens nos monitores não fiquem expostos ao acesso não autorizado. O cuidado com as mesas limpas deve ser ponto crítico de atenção, principalmente, nos escritórios em que os clientes, parceiros e públicos dos projetos transitam facilmente.

Os computadores deverão ser bloqueados quando não estiverem sendo utilizados. Quando o computador ficar em *stand-by* por mais de um minuto a sessão será finalizada, solicitando *login* e senha novamente ao usuário.

3.9. MÍDIAS REMOVÍVEIS E DA PORTA USB:

Mídias removíveis são dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Pen Drive, cartão de memória, HDs portáteis, telefones celulares, entre outros. A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais.

Tal vulnerabilidade não pode ser contida com firewalls já que os dispositivos são acoplados aos equipamentos pelos próprios funcionários da empresa. Para minimizar os riscos de exposição e perda de dados sensíveis mantidos pela empresa e reduzir os riscos de proliferação de malwares nos computadores, a transferência de informações para dispositivos removíveis é bloqueada nos equipamentos da empresa.

A liberação das portas USB dos desktops e notebooks é feita somente se o uso for justificado e aprovado pelo responsável do solicitante. O dispositivo USB deve ser preferencialmente adquirido pela empresa, está criptografado e protegido por senha. O

dispositivo só é liberado para utilização na sua diretoria. Mesmo em equipamentos liberados o tráfego de dados entre as unidades USB e os computadores é monitorado através relatórios providos pelo sistema de gerenciamento, auditorias internas e externas, e validações feitas pelo comitê de segurança da informação e compliance.

3.10. DESCARTE DE MÍDIAS:

Mídias contendo informações de propriedade da EXCLUSIVE ou dos projetos e seus clientes deverão ser destruídas antes de seu descarte.

CDs, DVDs, e documentos em papel deverão passar pelo triturador antes de serem encaminhadas ao lixo. HDs e *pendrive*s devem ser encaminhados a TI para a destruição da informação ou *backup* antes do descarte ou reutilização.

3.11. CLASSIFICAÇÃO DA INFORMAÇÃO:

O gestor de cada área ou projeto deve estabelecer os critérios relativos ao nível de confidencialidade da informação produzida por sua área em: Público, Interno, Confidencial ou Restrito, para garantir um nível adequado de proteção. Esses critérios garantirão a definição de como as informações serão tratadas e protegidas.

Para a classificação da informação deverá ser levado em conta o valor, requisitos legais, sensibilidade e criticidade para a EXCLUSIVE. Assim sendo, os níveis de classificação da informação devem ser:

a. Público: Pode ser disponibilizado e acessível a qualquer pessoa.
b. Interno: Acessado apenas por colaboradores da empresa.
c. Confidencial: Acessível apenas para um grupo de pessoas.
d. Restrito: Acessível apenas para pessoas selecionadas.

Como parâmetro para classificar as informações, pode-se realizar as seguintes perguntas baseadas nos níveis exemplificados acima:

Pode enviar para fora da empresa? Se sim, Pública, se não Interno.

Pode enviar para todos da empresa? Se sim, Interna, se não Confidencial.

Pode enviar para um colaborador que faz parte da minha equipe de trabalho? Se sim, confidencial, se não restrito.

3.11.1. SIGILO E CONFIDENCIALIDADE:

Toda informação disponibilizada ou coletada pelo colaborador, em razão do desempenho de suas funções e atividades, é de propriedade da EXCLUSIVE, classificada

como confidencial, tendo seu uso restrito às suas atividades, incluindo-se, dentre outras, todas e quaisquer informações orais e/ou escritas, transmitidas e/ou divulgadas pela empresa.

Informação confidencial significa, sem se limitar a, toda e qualquer informação de qualquer natureza - técnica, operacional, comercial e jurídica -, incluídas em descrição ou documentos que envolvam o know-how da empresa, planos de negócios, métodos de contabilidade, técnicas e experiências acumuladas, documentos técnicos e administrativos, contratos, papéis, estudos, pareceres, pesquisas, transmitidas pela empresa ao (a) colaborador (a) ou por ele (a) coletada.

- ✓ O colaborador concorda em usar as informações confidenciais recebidas da empresa com o propósito restrito de se fazer cumprir o estabelecido e acordado no contrato de trabalho.
- ✓ O colaborador que receber informação confidencial somente poderá usá-la para o propósito estabelecido no item anterior, e zelará para que tal informação confidencial não seja, de qualquer forma, divulgada ou revelada a terceiros.
- ✓ Exceto quando imprescindíveis ao desenvolvimento das ações da EXCLUSIVE e integre as suas atividades, não será permitido ao colaborador que receberá informação confidencial, produzir cópias ou backup, por qualquer meio ou forma, de qualquer um dos documentos a ele fornecidos ou documentos que tenham chegado a seu conhecimento em virtude do contrato, considerando que todas sejam informações confidenciais.
- ✓ Quando fornecida ou revelada por outras pessoas ou clientes, toda informação permanecerá sendo de sua propriedade, somente podendo ser usada pela EXCLUSIVE ou pelos colaboradores para os fins de execução do contrato. Tais informações confidenciais, incluídas as cópias realizadas, serão retornadas às pessoas e clientes, ou então destruídas pela empresa, tão logo tenha terminado a necessidade de seu uso ou tenha sido solicitado por eles e, em qualquer caso, na hipótese de término da vigência do contrato, observados as condições nele estabelecidas.
- ✓ O colaborador que receber informação confidencial se obriga a:
    1- Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor dessas informações, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objeto referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o seu uso indevido por qualquer pessoa que, por qualquer razão, tenha tido acesso a elas.
    2- Responsabilizar-se por impedir, por qualquer meio em direito admitido, a divulgação ou a utilização de informações.
    3- Restituir imediatamente o documento (ou outro suporte/mídia) que contiver as informações confidenciais às pessoas ou clientes, sempre que este as solicitar ou sempre que estas deixarem de ser necessárias, e não guardar para si, em nenhuma hipótese, cópia, reprodução ou segunda via das

mesmas.

- ✓ Fica ciente o colaborador que receber informação confidencial que as obrigações de confidencialidade, tanto quanto as outras responsabilidades e obrigações, vigorarão durante e após todo o contrato de trabalho, mesmo após o seu desligamento da empresa.
- ✓ O colaborador que recebe e tem conhecimento de informação confidencial, reconhece e aceita que, na hipótese de violação de quaisquer dos tópicos mencionados acima, estará sujeito (a) as sanções e penalidades legais, em especial a prevista no art. 482, da Consolidação das Leis do Trabalho, que trata da rescisão do contrato de trabalho por justa causa, sem prejuízo das perdas e danos que der causa, estas estimadas pela empresa, inclusive as de ordem moral ou concorrencial, bem como as de responsabilidades civis e criminais respectivas.

3.11.2. COMUNICAÇÃO VERBAL:

Sempre que Informações Protegidas forem transmitidas por meio de comunicação verbal, o Colaborador deverá respeitar as regras dispostas abaixo, de acordo com o meio de transferência da informação:

(i) Presencial. Informações Internas, Confidenciais e Secretas somente podem ser discutidas em locais privados de acesso controlado, para impedir que terceiros não autorizados escutem a conversa e tenham acesso a tais informações. Quando não for possível trocar tais informações em ambiente privado, o Colaborador deverá tomar, no mínimo, as seguintes cautelas:

(a) sempre verificar se alguém está escutando a conversa; e

(b) nunca identificar a EXCLUSIVE durante o diálogo.

(ii) Telefones, Celulares, Smartphones e Rádios. É vedada a transmissão de informações confidenciais e secretas por rádio ou telefone (fixo ou móvel). Caso o Colaborador não possa evitar que tais informações sejam transmitidas por ligações telefônicas ou outros meios de transmissão, o Colaborador deve redobrar o cuidado, sendo objetivo e discreto ao transmitir tais informações. Da mesma forma, o colaborador também não deve fornecer informações como senhas, telefones, endereços (físicos e eletrônicos), informações pessoais ou outros dados de acessos restrito por telefone ou outros meios de transmissão e deve estar atento para não repetir em voz alta essas informações quando forem lhe passar por terceiros. Ainda, o colaborador entende e concorda que é vedada a gravação de Informações Confidenciais e Secretas em equipamentos eletrônicos, como caixa postal, secretária eletrônica, áudios no WhatsApp ou aplicativos similares.

(iii) VOIP. Os colaboradores que tiverem acesso autorizado à ferramenta de VOIP devem se atentar às mesmas regras do uso de telefones, celulares e rádio de comunicação. Ainda, devem estar cientes que tal ferramenta é de titularidade

exclusiva da EXCLUSIVE, podendo somente ser utilizada para realização das atividades relacionadas aos negócios e interesse da EXCLUSIVE.

3.12. PROTEÇÃO: ANTIVÍRUS:

A EXCLUSIVE, por intermédio da área de TI, disponibiliza *software* corporativo de antivírus instalado para todos os colaboradores.

O antivírus é atualizado automaticamente na estação de trabalho do usuário sempre que uma nova versão é disponibilizada pelo fabricante através do aplicativo servidor.

A área de TI da EXCLUSIVE não autoriza que o usuário remova ou altere as configurações do antivírus a fim de não comprometer a segurança que o *software* proporciona.

As checagens do disco rígido (HD) da estação de trabalho estão programadas para execução periódica automática, conforme definições da área de TI.

É importante a instalação de antivírus nos telefones corporativos, a fim de garantir segurança das informações acessadas nos dispositivos.

Nos casos em que é permitido ao usuário o uso de mídias externas, como *pendrive*s e HDs, são programados escaneamentos assim que for conectado ao computador.

3.13. E-MAIL CORPORATIVO:

Quanto à utilização do e-mail corporativo (usuario@exclusiveseguros.com.br):

- ✓ Acessar com frequência o e-mail corporativo, a fim de se informar sobre as atividades da EXCLUSIVE;
- ✓ Manter a conta de e-mail atualizada, evitando acúmulo de e-mails e arquivos desnecessários;
- ✓ Observar a cota máxima de e-mails armazenados, estipulada e gerenciada pela área de TI;
- ✓ Utilizar o padrão abaixo para o corpo do texto e assinatura dos e-mails:

- ✓ Não utilizar o e-mail corporativo da EXCLUSIVE para o envio ou recebimento de

mensagens não relacionadas ao trabalho, correntes, spams ou e-mails enviados em grande quantidade e/ou para vários destinatários que não sejam solicitados ou autorizados pela empresa. É proibido utilizar o e-mail corporativo para reenviar ou propagar mensagens em cadeia, correntes ou pirâmides, independente da vontade do destinatário de receber tais mensagens;

- ✓ Não utilizar o e-mail corporativo da EXCLUSIVE para o envio de mala direta, publicidade, material comercial, anúncios, informativos, campanhas ou propagandas que não tenham sido previamente solicitados ou autorizados pela empresa;
- ✓ Não enviar e-mails para os grupos de e-mail da EXCLUSIVE que não sejam estritamente relacionados ao trabalho e autorizados pela EXCLUSIVE ou por seus representantes;
- ✓ Não fornecer ou cadastrar o e-mail corporativo da EXCLUSIVE em sites de propaganda, redes sociais, notícias, compras ou qualquer outro site que não seja de total interesse e autorizado pela empresa.
- ✓ Não alterar quaisquer das informações do cabeçalho do remetente;
- ✓ Não enviar e-mails a destinatários que não os queiram receber. Quando um destinatário solicitar a interrupção do envio de e-mails, o usuário deverá acatar imediatamente a solicitação, e informar a EXCLUSIVE e seus representantes casos o envio tenha sido por eles solicitado;
- ✓ Caso o Comitê de Segurança da Informação julgue necessário, as seguintes ações poderão ser tomadas pela área de TI:
    1- bloqueio de e-mails com arquivos anexos que comprometam a segurança, o uso da rede ou o andamento das atividades relacionadas ao trabalho;
    2- bloqueio de e-mails para destinatários ou domínios que comprometam a segurança, o uso da rede ou o andamento das atividades relacionadas ao trabalho;
    3- bloqueio de e-mails para vários destinatários, ou que possam caracterizar o domínio Exclusiveadvogados.com.br como propagador de spam.
    4- bloqueio de e-mails quando estes ferirem a Lei Geral de Proteção de Dados nro 13.709/2018.

- ✓ Mensagens recebidas de origem desconhecida deverão ser pré-visualizadas e eliminadas imediatamente, sem leitura de seu conteúdo, para evitar contaminação por vírus e outros riscos.
- ✓ O uso indevido do e-mail é de inteira responsabilidade do usuário, podendo o mesmo ser responsabilizado por eventuais danos causados.
- ✓ As mensagens trafegadas sob o domínio da EXCLUSIVE poderão ser auditadas, mediante solicitação, conforme definição do TST - Tribunal Superior do Trabalho. Desta forma, é proibida a utilização particular.
- ✓ Em nenhuma hipótese a EXCLUSIVE será responsabilizada perante quaisquer usuários ou terceiros pela perda de mensagens e/ou respectivo conteúdo.

3.14. A REDE DA EXCLUSIVE:

3.14.1. Direito de Uso:

A rede EXCLUSIVE e os equipamentos que a compõem têm como finalidade única e exclusiva de permitir aos seus usuários a prática de atividades relacionadas ao trabalho, à pesquisa e à disseminação de informações de interesse da EXCLUSIVE e de suas unidades.

Têm direito de uso da rede os empregados, diretores, prestadores de serviços terceirizados e demais usuários autorizados pela EXCLUSIVE.

O uso da internet, acesso à rede e criação de e-mail corporativo **(*usuário@exclusiveseguros.com.br*)** serão previamente autorizados pela EXCLUSIVE, ou por seus representantes através de comunicação à área de TI por meio de chamado.

O direito de uso da rede cessa quando o usuário encerrar seu vínculo regular com a EXCLUSIVE, seja através do desligamento por qualquer motivo, suspensão do contrato de trabalho ou serviço prestado ou pelo encerramento de atividades que justifiquem seu acesso à rede.

Caso o usuário venha a exercer nova atividade relacionada à EXCLUSIVE após o encerramento do vínculo regular, deverá ter sua autorização de uso da rede e acessos revisados, não podendo fazer uso dos direitos que lhe foram concedidos em situação anterior.

3.14.2. Responsabilidades Individuais:

O usuário tem as seguintes responsabilidades na segurança e sigilo da rede da EXCLUSIVE:

a. Zelar pela rede e pelos equipamentos que utiliza, não sendo permitida qualquer remoção, desconexão de partes, substituição, reconfiguração ou qualquer alteração nas características físicas ou técnicas dos equipamentos integrantes da rede;
b. Estar ciente de que o *login* de acesso ou senha à rede é pessoal e intransferível, devendo, portanto, proceder de forma responsável, garantindo o sigilo de sua senha, trocando-os de acordo com as orientações da EXCLUSIVE e escolhendo códigos de difícil decodificação;
c. Respeitar áreas de acesso restrito, não executando tentativas de acesso a áreas e/ou equipamentos alheios as suas permissões de acesso;
d. Não tomar atitude ou ação que possa, direta ou indiretamente, danificar ou indisponibilizar recursos da rede por qualquer intervalo de tempo;
e. Não executar programas que tenham como finalidade a decodificação de

senhas, a monitoração da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilização de serviços;

f. Não instalar ou executar programas, instalar equipamentos ou executar ações que não sejam previamente autorizados pela EXCLUSIVE ou que possam facilitar o acesso à rede de usuários não autorizados;
g. Não fazer uso de direitos especiais de acesso ou de qualquer outro privilégio já extintos com o término do período de ocupação de cargo ou função dentro da EXCLUSIVE;
h. Utilizar a rede corporativa de maneira profissional, ética, segura e legal, mesmo em horários de intervalo e fora do horário de trabalho;
i. Em caso de dúvidas em relação à utilização e segurança da rede, contatar previamente a área de TI através de e-mail ou outros meios de comunicação que venham a ser oferecidos, e seguir suas orientações.

3.15. DISPOSITIVOS MÓVEIS:

A EXCLUSIVE deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis. Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência, como: notebooks, smartphones e tablets.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos. A EXCLUSIVE, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança. O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na EXCLUSIVE, mesmo depois de terminado o vínculo contratual mantido com a instituição.

O suporte técnico aos dispositivos móveis de propriedade da EXCLUSIVE e aos seus usuários deverá seguir o mesmo fluxo de suporte estabelecido. Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da GSI.
O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da GSI. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos

autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, fornecedores e clientes. Em hipótese alguma, o dispositivo deverá se conectar a redes compartilhadas tais como: Hotéis – Aeroportos – LanHouses – Cafés. Caso o acesso ocorra, por motivos de urgência, a GSI deverá ser comunicada imediatamente.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela EXCLUSIVE, notificar imediatamente seu gestor direto e a GSI. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a EXCLUSIVE e/ou a terceiros.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da EXCLUSIVE, deverá submeter previamente tais equipamentos ao processo de autorização da GSI. Equipamentos portáteis, como notebooks, smartphones, tablets, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

3.16. HOME-OFFICE:

É expressamente proibido o uso de equipamentos particulares não autorizados pelo GSI, em conexões remotas ao ambiente da EXCLUSIVE. No caso de dispositivos habilitados e autorizados para acesso remoto, devem estar configurados pelo GSI, obrigatoriamente, com mecanismos de segurança tais como sistema de criptografia, antivírus, ferramentas para acesso seguro à VPN (Virtual Private Network) e firewall pessoal, visando assegurar confidencialidade e a integridade das informações da EXCLUSIVE. Os serviços remotos deverão ser interrompidos automaticamente após 5 (cinco) minutos de inatividade, porém, sempre que o colaborador/parceiro não estiver utilizando os recursos deve encerrar a sua sessão imediatamente.

3.17. Utilização de impressoras e outros recursos:

a. Utilizar as impressoras, copiadoras e outros dispositivos de hardware apenas para atividades relacionadas ao trabalho na EXCLUSIVE;
b. Zelar para que o número de cópias e impressões seja sempre o mínimo necessário, evitando desperdícios;
c. Otimizar o aproveitamento e reaproveitamento de papel sempre que possível;
d. Não deixar impressões e cópias se acumularem nas impressoras e copiadoras,

sobre os gaveteiros das impressoras ou sobre o mobiliário próximo a elas;

e. Recolocar folhas emitidas em branco pelas impressoras ou copiadoras nas bandejas de impressão;
f. Reabastecer as impressoras e copiadoras, ou solicitar o reabastecimento sempre que necessário, evitando o acúmulo de trabalhos na fila de impressão, e observando as regras locais para bandejas de papel para primeira utilização e bandejas de papel reutilizado (rascunho);
g. Zelar para que informações sensíveis não sejam impressas, e o documento reutilizado como rascunho;

3.17. Adição de recursos/equipamentos à Rede EXCLUSIVE:

É vedada aos usuários a adição de quaisquer recursos à rede, sejam eles microcomputadores, impressoras, ou outros equipamentos.

A adição de novos equipamentos pelo usuário deve ser solicitada por comunicação interna e deverá ser aprovada pela EXCLUSIVE e, uma vez aprovada, a adição será realizada apenas pela área de TI.

Todos os equipamentos ligados à rede devem obedecer aos padrões de instalação, de utilização e de designação de endereços e domínio estabelecidos pela TI.

O usuário está ciente que a adição de recursos sem a autorização da EXCLUSIVE, compromete a administração e a segurança da rede, assim como a assistência ao equipamento.

3.18. ARMAZENAMENTO DE ARQUIVOS DE TRABALHO:

Todos os arquivos contidos nos servidores de rede e no Sharepoint devem ser exclusivamente de interesse da EXCLUSIVE. É proibida a criação de pastas pessoais nos servidores da rede.

Todos os arquivos produzidos pelos colaboradores para os serviços da EXCLUSIVE devem ser salvos no Sharepoint do usuário ou no site adequado do setor.

Os usuários não deverão criar sites na estrutura organizacional do SharePoint da EXCLUSIVE.

É proibida, também, a produção e armazenamento de arquivos de trabalho em nuvens não corporativas (*OneDrive* pessoal, Dropbox etc.) e nas próprias máquinas, por não ter garantia de *backup* (poderão ser perdidos caso ocorra uma falha no computador) e compartilhamento com todos os colaboradores envolvidos.

A partir da implantação desta Política, todos os arquivos que não sejam do

interesse da EXCLUSIVE deverão ser excluídos dos equipamentos para evitar problemas futuros com as auditorias.

3.19. *BACKUP* DE ARQUIVOS:

Compete ao gestor da área TI criar e manter cópias de segurança (*backup*s) apenas dos dados armazenados nos servidores da rede, e locais previamente informados.

Todos os arquivos que estiverem armazenados no *SharePoint EXCLUSIVE,* estão resguardados por *backup* automático, além de controle de versionamento e responsáveis pelas alterações.

É de responsabilidade única e exclusiva do usuário a cópia de segurança (*backup*) e a guarda dos dados gravados localmente nos computadores.

3.20. UTILIZAÇÃO DA INTERNET:

A internet foi instalada para viabilizar a busca de informações e agilizar determinados processos da EXCLUSIVE, podendo ser utilizada para fins pessoais pelos seus colaboradores, desde que não prejudique o andamento dos trabalhos.

O uso indevido do acesso à Internet é de inteira responsabilidade do usuário, que pode ser responsabilizado legalmente por eventuais danos causados. A utilização indevida da internet promove riscos significativos para os ativos de informação e, por esse motivo, torna-se imprescindível seu monitoramento e controles de uso.

A auditoria dos acessos à internet pode levar ao conhecimento dos responsáveis hierárquicos, relatórios com nomes dos usuários, páginas consultadas, tempo de consulta e o conteúdo navegado. Utilização da internet e aplicativos:

a. Viabilizar as atividades relacionadas ao trabalho, à pesquisa e à disseminação de informações de interesse da EXCLUSIVE e de suas unidades;
b. Não instalar ou acessar sites ou *software*s de conteúdo impróprio ou não relacionado ao trabalho, como sites ou *software*s de conversação instantânea que não seja o MS Teams (ferramenta oficial), como redes sociais (ex. Facebook, LinkedIn), sites de compras, sites de entretenimento, jogos, vídeo e música, e outras comunidades ou sites, exceto quando autorizado pela EXCLUSIVE;
c. Não baixar ou instalar programas transmissores de músicas e afins para tocadores de MP3, MP4, rádios on-line, programas P2P como Kazaa, Emule, Edonkey, dentre outros.
d. Utilizar com parcimônia os serviços de streaming;
e. Não utilizar a rede para fazer *download*s ou *upload*s não autorizados ou não relacionados às atividades da EXCLUSIVE ou que não sejam previamente autorizados;

f. Utilizar apenas os *softwares* autorizados pela área de TI para a navegação na internet.

3.21. REDES SOCIAIS, WHATSAPP E E-MAIL PESSOAIS

O uso de redes sociais, serviços de e-mail e WhatsApp e outros mensageiros pessoais nas dependências físicas da EXCLUSIVE é autorizado, desde que:

(i) não sejam utilizados para acesso ou divulgação de qualquer Informações Protegidas;

(ii) não sejam utilizados para acesso ou divulgação de qualquer conteúdo não autorizado por esta Política;

(iii) não atrapalhe o exercício das atividades do Colaborador, bem como de qualquer outro Colaborador;

(iv) o Colaborador não compartilhe, poste, divulgue ou exponha qualquer imagem, foto, vídeo ou som captado no ambiente interno da EXCLUSIVE;

(v) o Colaborador não compartilhe, poste, divulgue ou exponha qualquer comentário ou texto que revele ou induza terceiros a acreditar que se trata de uma opinião ou posicionamento da EXCLUSIVE; e

(vi) o Colaborador abstenha-se de citar, em qualquer hipótese, o nome da EXCLUSIVE ou qualquer marca relacionada ou de titularidade da EXCLUSIVE.

O Colaborador é exclusivamente responsável pelo uso e guarda de suas senhas de acesso a redes sociais e e-mails pessoais, e a Companhia recomenda expressamente o uso de navegadores anônimos para o uso de aplicações particulares em equipamentos de propriedade da EXCLUSIVE.

A EXCLUSIVE poderá suspender, temporariamente e sem aviso prévio, o uso e o acesso a essas aplicações, a seu exclusivo critério, por questões de governança e/ou de segurança da informação, independentemente de comunicação prévia ao Colaborador.

3.22. USO ADEQUADO DE DADOS PESSOAIS

O uso dos dados e informações pessoais que identificam ou possam permitir a identificação de seus titulares está limitado às finalidades previstas neste documento. Para tanto compreende-se como:

(i) Dados pessoais: aqueles relacionados à pessoa natural que pode vir a torná-la identificada ou identificável, como por exemplo: nome, CPF, RG, endereço, e-mail etc.;

(ii) Dados sensíveis: dados pessoais que dependendo da finalidade do processamento que é feita podem levar a inferir um caráter discriminatório aos

titulares dos dados, tais como informações referentes à orientação religiosa, sexual, opiniões políticas, questões culturais, informações genéticas e de saúde etc.; e

(iii) Dados relativos à saúde: dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde, como por exemplo: dados médicos, registros de doenças, uso de remédios etc.

Os dados pessoais coletados devem ser utilizados apenas para finalidades específicas, informadas previamente ao titular.

Os Colaboradores deverão, no desempenho de suas atividades, coletar o mínimo de dados pessoais possível, coletando apenas o necessário para a realização de suas atividades.

Nos termos da lei 13.709/2018, artigos 18 a 21 os titulares possuem diversos direitos. A EXCLUSIVE disponibiliza um canal para contato com o encarregado pelo tratamento dos dados pessoais, a saber: https://exclusiveseguros.com.br/politica-de-privacidade/

Após atingida a finalidade para a qual os dados pessoais foram coletados e diante da ausência de justificativa legal que permita armazená-los, os dados pessoais devem ser descartados. Os prazos e instruções para descartes de dados pessoais estão contidos na Política de Armazenamento e Descarte de Dados.

O colaborador entende que todos os dados pessoais a que tiver acesso em razão do exercício de suas funções na EXCLUSIVE deverão ser reputados confidenciais, independente de nota ou disposição neste sentido, e jamais deverão ser divulgados, compartilhados ou dado acesso a terceiros sem a prévia e expressa autorização da EXCLUSIVE. O colaborador garante, ainda, que adotará as melhores práticas de segurança da informação durante a execução de suas atividades.

As disposições sobre proteção de dados pessoais são complementares àquelas incluídas na Política de Privacidade disponível em [https://exclusiveseguros.com.br/politica-de-privacidade/] caso de dúvidas, sobre como tratar dados pessoais, procure o encarregado através do e-mail **dpo@exclusiveseguros.com.br**

3.23. JOGOS:

Jogos estão terminantemente proibidos.

3.24. APLICATIVOS DE MENSAGENS INSTANTÂNEAS:

Os colaboradores da EXCLUSIVE se comprometem a:

- ✓ Utilizar os aplicativos de mensagem instantânea (Skype for Business, Whatsapp, Telegram ou correlatos) para fins corporativos somente quando necessário ou quando este for o único ou o melhor meio para promover a troca de informações urgentes, não sigilosas nem confidenciais.
- ✓ Em grupos criados para discussão de temas relacionados às atividades da empresa, devem restringir o conteúdo das mensagens aos assuntos corporativos.
- ✓ Não realizar a troca de mensagens com conteúdo relevante, de cunho sigiloso ou confidencial por meio desses aplicativos, em acordo com a PSI.
- ✓ Evitar o uso desses aplicativos para envio de arquivos relacionados ao trabalho, como relatórios, planilhas etc., em acordo com a PSI.
- ✓ Preferir sempre os serviços corporativos de e-mail e mensagens instantâneas para realizar contatos e trocar mensagens;
- ✓ Respeitar os horários regulamentares de folga dos demais colaboradores, fazendo contato fora do horário de trabalho apenas quando estritamente necessário;
- ✓ Preferir o uso do número corporativo para comunicação ou os aplicativos de mensagens instantâneas autorizados.
- ✓ Não divulgar a terceiros o conteúdo das mensagens instantâneas, sob qualquer hipótese, exceto quando autorizado pelos responsáveis hierárquicos.

3.25. *SOFTWARES*:

Os *software*s homologados e instalados nos computadores e servidores de rede são de propriedade exclusiva da EXCLUSIVE, sendo proibidas as cópias integrais ou parciais, bem como a instalação de *software*s piratas.

Pirataria é considerada crime e *software*s piratas causam prejuízos tanto materiais como funcionais, além de denegrir a imagem da empresa. Por esta razão, estão terminantemente proibidos.

A instalação de *software*s não autorizados (Pirataria) constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, e o infrator está sujeito à pena de detenção e multa.

A EXCLUSIVE mantém contratos especiais com alguns fabricantes de *software* e poderá estender a utilização de alguns deles nos computadores pessoais dos colaboradores, bastando ao colaborador solicitar a instalação à área de TI.

É proibido o uso de e-mails, correios eletrônicos ou mensagens instantâneas de forma contrária à lei, à moral, aos bons costumes, à ordem pública ou que infrinjam os

direitos à propriedade intelectual ou industrial pertencente a terceiros.

O conteúdo e a utilização de e-mails, correios eletrônicos ou mensagens instantâneas deve ser de caráter exclusivamente profissional.

3.26. ACESSO FÍSICO AO CPD

O CPD da EXCLUSIVE é parte crítica da sua infraestrutura tecnológica, razão pela qual o cuidado com a proteção e segurança deve ser obrigatoriamente redobrado.

Por esse motivo, o acesso físico será restrito àquelas pessoas previamente autorizadas pelo GSI. Acessos permanentes serão permitidos somente aos colaboradores da EXCLUSIVE indicados pelo GSI, que tenham a necessidade de acesso liberado para executar suas atividades; acessos esporádicos por outros Colaboradores ou visitantes externos somente poderão ocorrer com autorização prévia do GSI e desde que, para fins de controle, o acesso seja registrado pela equipe de TI (nome, data e hora) e o Colaborador ou visitante seja acompanhado em tempo integral por alguém responsável da área de Infraestrutura; acessos de contratantes externos, que não sejam Colaboradores da Companhia, somente serão autorizados pelo GSI, desde que possuam contrato vigente com a EXCLUSIVE que justifique esse acesso.

Em caso de acesso do Colaborador ao CPD, o Colaborador não poderá:

(i) adentrar nas dependências do cpd sem o seu crachá de identificação;

(ii) portar, no local de armazenamento do cpd, alimentos, líquidos, materiais inflamáveis ou qualquer utensílio que possa danificar os equipamentos;

(iii) introduzir ou retirar equipamentos da sala do cpd, a menos que haja autorização prévia e por escrito do GSI; e

(iv) realizar a gravação de vídeos ou a captura de imagens dentro das dependências do CPD. Além disso, o Colaborador deverá certificar-se que as portas permaneçam sempre fechadas durante a sua permanência dentro da sala do CPD.

3.27. AUDITORIAS:

Auditorias serão realizadas e relatórios serão gerados periodicamente.

A Diretoria da EXCLUSIVE poderá solicitar, à área de TI, relatórios de auditoria contendo o nome, mensagens trafegadas, acessos à Internet e demais informações do usuário, conforme resolução do TST.

Todos os usuários da rede da EXCLUSIVE estão sujeitos à auditoria de redes. Os procedimentos de auditoria e de monitoramento de uso serão realizados periodicamente

ou sempre que solicitados pela diretoria ou área de TI ou profissional contratado para este fim, com o objetivo de observar o cumprimento das normas deste regulamento pelos usuários da rede e com vistas à gestão de desempenho e segurança da informação.

Havendo evidência de atividade que possa comprometer a segurança da rede ou que descumpra as regras estabelecidas por este regulamento, será permitido ao administrador da rede auditar e monitorar as atividades de um usuário, além de inspecionar seus arquivos, registros de acesso, contas de e-mail corporativo e acesso aos sistemas e sites de comunicação interna da empresa, sendo o fato imediatamente comunicado à Diretoria ou seus representantes. Os dados apurados no computador serão mantidos em sigilo pela direção da EXCLUSIVE.

A EXCLUSIVE poderá, a qualquer tempo, implantar aplicativos de segurança, monitoramento e gravação do uso da rede e internet, instalar *software*s e *hardware*s para proteger a rede e garantir a integridade dos dados e programas, inspecionar arquivos armazenados na rede, seja em disco local, virtual ou nas áreas privadas da rede, a fim de assegurar o cumprimento das regras aqui estabelecidas.

3.28. CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO:

Plano de Conscientização de Segurança da Informação Um plano de conscientização da segurança da informação deve ser elaborado e executado para atingir o seguinte objetivo: “Garantir que a Segurança da Informação não seja apenas conhecida, mas compreendida por todos os funcionários e colaboradores, conscientizando-os sobre melhores práticas, requisitos mínimos, riscos e responsabilidades existentes e quais medidas devem ser adotadas quando houver incidentes de Segurança de forma a atingir uma melhor utilização e proteção à informação.”
As diretrizes básicas são:

- Elaboração de um processo de treinamento continuado contemplando todos os níveis funcionais do Conglomerado;
- Divulgação de diversos materiais e alertas referente a Segurança da Informação para funcionários, colaboradores e clientes;
- Criação de procedimentos de aferição do nível de conhecimento dos usuários em geral;
- Organização de eventos que tenham o intuito de fortalecer a conscientização sobre diversos aspectos de segurança em geral;
- Revisão periódica do plano, adequando as ações às novas necessidades, evitando torná-lo repetitivo.

3.29. SANÇÕES

O descumprimento de quaisquer dispostos estabelecidos na presente política e nos demais documentos em referência que suportam sua implantação acarretará a imposição

de sanções a serem definidas pelo Comitê de Segurança da Informação, sendo cabíveis, ainda, as penalidades descritas na legislação vigente.

3.30. DISPOSIÇÕES FINAIS:

A segurança da informação deve ser entendida como parte fundamental da cultura interna da EXCLUSIVE. Qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os valores regidos pela instituição.

Todas as práticas que ameacem a segurança da informação serão tratadas com a aplicação de ações disciplinares, desde uma advertência verbal até rescisão contratual por justa causa, levando em consideração fatores como: função exercida pelo colaborador, período utilizado, local de utilização, horário de utilização, prejuízo real ou potencial causado à EXCLUSIVE, além de responder legalmente por atividades que descumpram a legislação brasileira, entre outros.

3.31. CONTATOS IMPORTANTES:

Para assuntos relativos aos *softwares*, redes e informática:

Responsável pela área de TI: Helem Sampaio
e-mail: helem.sampaio@exclusiveseguros.com.br

Responsável pela área de TI: Suprema Informática LTDA
e-mail: suporte.suprema@supremanet.com.br

Para assuntos relativos à restrição de acesso às pastas do servidor, bem como as regras de salvamento de arquivos:

Abertura de chamados via Portal GLPI: https://meettecnologia.verdanadesk.com/
e-mail: suporte.suprema@supremanet.com.br

Para comunicar qualquer incidência de risco ou violação de segurança da informação e dados Pessoais:

Nome: Luiz Siqueira
Email: dpo@exclusiveseguros.com.br

Responsáveis pelo Comitê de Segurança da Informação: gsi@exclusiveseguros.com.br

HISTÓRICO DE REVISÕES:

Data	Descrição das alterações	Responsável
03/04/2022	Emissão do documento	Everton Alves
08/06/2022	Revisão Iara – Chenut / Inclusão clausulas proteção de Dados.	Iara Peixoto Melo
09/09/2023	Validado - EXC	Vânia Lima
28/09/2023	Atualização da assinatura item 3.13 e logo Atualização do item 3.22 disponibilidade da politica de privacidade e contato do DPO. Revisão de conteúdo e retirada de comentários.	Gustavo Ferreira Helem Sampaio