Vision One®

Política de Segurança da Informação

A Política de Segurança da Informação ("Política" ou "PSI") é o documento que orienta e estabelece as diretrizes corporativas da Vision One, suas subsidiárias e afiliadas ("Vision One" ou "Empresa"), para a proteção dos ativos de informação e a prevenção de responsabilidade legal de seus destinatários. Deve, portanto, ser cumprida e aplicada em todas as áreas da Empresa, inclusive por todas as pessoas físicas e jurídicas, sejam sócios, diretores, administradores, funcionários, estagiários, menores aprendizes, prestadores de serviços, parceiros e/ou quaisquer outros terceiros ("Colaboradores") que, no âmbito de sua relação com a Vision One, possam vir a ter acesso às áreas, equipamentos, informações, arquivos, redes e dados de titularidade da Empresa, cujo acesso seja controlado.

ÍNDICE

1) OBJETIVOS

A presente Política apresenta os princípios gerais de conduta e as obrigações a serem seguidas pelos Colaboradores, a fim de mitigar eventuais riscos relacionados às ameaças externas ou internas, deliberadas ou acidentais, que possam impactar as informações da Vision One quanto à sua integridade, confidencialidade e disponibilidade.

2) APLICAÇÕES DA PSI

Esta PSI é aplicável a toda Vision One, contemplando todo uso de dispositivos, acesso a servidores, conexões à rede e à internet e quaisquer outros usos de recursos tecnológicos ou que contenham informações da Vision One.

Em razão da sensibilidade da informação trafegada na Vision One, esta poderá, nos limites da lei aplicável e conforme necessário, monitorar, gravar e registrar os ambientes, sistemas, serviços, computadores e redes da Vision One para garantir a disponibilidade e a segurança das informações utilizadas. É obrigação de cada Colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e às normas relacionadas.

3) INFORMAÇÕES PROTEGIDAS

Todo e qualquer dado ou informação que o Colaborador desenvolva ou venha a ter acesso em virtude do seu vínculo com a Vision One ou do desempenho de suas atividades contratadas pela Empresa ("Informações Protegidas") será considerada de exclusiva propriedade da Vision One, salvo disposição contratual diversa, sendo expressamente proibida a sua reprodução, divulgação, publicação, transmissão, cessão ou facilitação de acesso a quaisquer terceiros, direta ou indiretamente, total ou parcialmente, salvo se autorizado por esta Política ou, previamente e por escrito, pelos representantes legais da Empresa.

O Colaborador poderá ser responsabilizado por eventual uso indevido que fizer da Informação Protegida. A Vision One reserva-se o direito de monitorar o uso das Informações Protegidas pelo Colaborador e analisar todos os dados e evidências relacionados, para fins de obtenção de provas que poderão ser eventualmente utilizadas nos processos investigatórios e na adoção das medidas legais cabíveis.

A qualquer tempo, caso seja solicitado pela Vision One ou em caso de término da relação do Colaborador com a Empresa, independentemente da causa, o Colaborador restituirá à Vision One todas as cópias, bancos de dados, reproduções ou adaptações que, porventura, tiver realizado das Informações Protegidas. O Colaborador reconhece, ainda, que as obrigações e proibições previstas neste item permanecerão válidas durante toda a existência do vínculo do

Colaborador com a Empresa e mesmo após o término de tal vínculo, independentemente do motivo.

Qualquer Informação Protegida cuja divulgação seja exigida por Lei, ordem judicial, determinação de autoridades administrativas competentes ou acordos celebrados pela Vision One com terceiros somente poderá ser divulgada após análise e validação do departamento Jurídico da Vision One.

4) CLASSIFICAÇÃO DAS INFORMAÇÕES PROTEGIDAS

Para assegurar a proteção adequada das Informações Protegidas, é necessário que sejam classificadas de acordo com a importância que representam para os negócios da Empresa, aplicando-se o grau de sigilo conforme sua classificação:

(i) Informação Interna: informação que guarde assuntos exclusivamente pertinentes à esfera interna da Vision One, cujo acesso é liberado apenas às pessoas internas da Empresa designadas para tal. Embora a Vision One não tenha interesse em divulgá-la a indivíduos externos, a disponibilização dessa informação não tem potencial de causar danos sérios à Empresa;

(ii) Informação Confidencial: informação sigilosa que não deve ser divulgada. Seu uso é restrito a um determinado número de pessoas para desempenharem as suas atividades vinculadas à Empresa. A sua divulgação não autorizada pode causar prejuízos para a Empresa (tais como perda de pacientes e parceiros, danos financeiros, depreciação da imagem etc.), propiciando vantagens aos seus concorrentes, pacientes e parceiros, bem como revelando estratégias e resultados de negócios; e

(iii) Informação Secreta: informação sigilosa, com acesso controlado e liberado apenas às pessoas nomeadas para tanto, que contém matérias de ordem vital para a Empresa ou seus pacientes e parceiros, cuja divulgação, inexatidão e disponibilidade (total ou parcial) podem causar danos graves à Empresa, morais e/ou patrimoniais. Sempre serão consideradas Informações Secretas as informações de saúde (p. ex. prontuários médicos de pacientes e exames médicos de Colaboradores), os procedimentos de segurança e outras informações de notável sensibilidade para os negócios da Empresa.

Além das Informações Protegidas, há também a Informação Pública, destinada ao público em geral e já divulgada pela Empresa, cuja utilização por quaisquer indivíduos independe de autorização e não pode gerar prejuízos para a Vision One ou para terceiros.

Caso o Colaborador receba uma informação que não esteja classificada, ele deve considerar, obrigatoriamente, essa informação como sendo, no mínimo, uma Informação Confidencial. Se o Colaborador tiver conhecimento de que Informações Internas, Confidenciais ou Secretas estejam sendo tratadas inadequadamente, tal Colaborador deverá comunicar o Departamento Jurídico.

5) PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Esta PSI aplica-se a dados, incluindo dados pessoais e dados pessoais sensíveis, sobre os Colaboradores, pacientes e prestadores de serviços relacionados à Vision One. É vedado, sem a prévia autorização da Vision One, o uso desses dados para finalidades diversas das que lastrearam a coleta, o uso, o armazenamento e qualquer outra hipótese de tratamento dos dados, nos termos desta PSI e das demais políticas referentes à privacidade e proteção de dados pessoais.

A Vision One usa provedores de serviços externos. Se os dados que estão sendo processados são pessoais, firmamos acordos contratuais apropriados e medidas organizacionais foram implementadas de acordo com a legislação aplicável para assegurar a proteção dos dados.

O Colaborador garante que todos os dados pessoais a que tiver acesso não serão divulgados ou compartilhados sem autorização expressa da Empresa, bem como não serão transmitidos ou acessados por terceiros não autorizados. O Colaborador garante, ainda, que adotará as melhores práticas de segurança da informação durante todo o ciclo de vida dos dados dentro da Vision One, não se limitando àquelas descritas nesta PSI.

6) MONITORAMENTO E AUDITORIA DO AMBIENTE

TODO AMBIENTE FÍSICO E DIGITAL DA EMPRESA É OU PODERÁ SER MONITORADO, RESPEITADOS OS LIMITES PREVISTOS NA LEGISLAÇÃO VIGENTE, INCLUINDO O ACESSO, USO OU TRÁFEGO DE INFORMAÇÕES EM TAL AMBIENTE POR QUALQUER MEIO (TAL QUAL, POR EXEMPLO, E-MAIL) COM O OBJETIVO DE APURAR O CUMPRIMENTO DAS NORMAS DE SEGURANÇA E PROTEÇÃO DE DADOS DA EMPRESA.

OS COLABORADORES ESTÃO CIENTES DE QUE A VISION ONE PODERÁ:

(i) MONITORAR TODOS OS SERVIDORES, REDES, CONEXÕES DE INTERNET, SOFTWARE, EQUIPAMENTOS E DISPOSITIVOS CORPORATIVOS, MÓVEIS OU NÃO, CONECTADOS À REDE CORPORATIVA;

(ii) REALIZAR INSPEÇÕES FÍSICAS NOS EQUIPAMENTOS E NAS ESTAÇÕES DE TRABALHO DO COLABORADOR, PERIODICAMENTE OU SOB FUNDADA SUSPEITA DE INFRAÇÃO ÀS NORMAS INTERNAS DA EMPRESA.

O Colaborador também está ciente de que o monitoramento poderá identificá-lo e apresentar dados sobre o seu uso da infraestrutura técnica da Vision One e do material e conteúdo manipulado pelo Colaborador, sendo certo que todas as informações coletadas no curso do

monitoramento são guardadas nos backups da Empresa para fins de auditoria e poderão ser utilizadas como provas de eventual violação das regras e condições estabelecidas pela Vision One ou pela legislação em vigor. Caso solicitado pelos órgãos competentes, essas informações poderão ser divulgadas na medida em que houver razão legal ou determinação judicial para tanto.

O Colaborador entende que o monitoramento pode ser realizado para resguardar a segurança não só dos sistemas da Empresa e das Informações Protegidas, como também do próprio Colaborador. **Os dados e as informações monitoradas somente poderão ser acessadas pelos departamentos competentes e para finalidades legítimas**, como a apuração de denúncias e condução de investigações no ambiente laboral. Todo e qualquer tratamento de dados para esses fins será fundamentado no relatório de auditoria ou em outro instrumento apropriado para tanto e cumprirá as normas específicas sobre privacidade e proteção de dados pessoais.

7) MANUSEIO DAS INFORMAÇÕES PROTEGIDAS

O Colaborador é responsável pelo uso que fizer das Informações Protegidas. Assim, as regras abaixo deverão ser observadas para garantir um nível mínimo de Segurança da Informação.

7.1. CUIDADOS COM IMPRESSORAS E COPIADORAS

Os Colaboradores estão cientes de que todo e qualquer uso dos equipamentos, como copiadoras e impressoras, deve ser feito exclusivamente no âmbito das suas atividades profissionais, sendo vedado o uso para fins pessoais. Deve-se evitar imprimir documentos contendo Informações Secretas e, para todos os tipos de informação, os documentos impressos ou copiados devem ser retirados imediatamente dos equipamentos.

7.2. USO DE INFORMAÇÕES PROTEGIDAS

O Colaborador deve tomar o máximo de cuidado com o uso que faz das Informações Protegidas, atentando-se para não deixar anotações ou manipular documentos que contenham Informações Protegidas em locais de circulação, como salas de reunião ou espaços públicos, como cafés e aviões. É proibida a reutilização de papéis para rascunho que contenham Informações Protegidas.

Nos casos envolvendo a contratação de serviços de terceiros que justifiquem a necessidade de compartilhamento de Informações Protegidas pelo Colaborador, estas somente poderão ser compartilhadas após a assinatura de Acordo de Confidencialidade ou de outros instrumentos contratuais pertinentes firmados com tais terceiros.

7.3. COMUNICAÇÃO VERBAL

Sempre que as 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 a comunicação 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 Empresa, o parceiro ou o paciente durante o diálogo.

(ii) Telefones, Celulares 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 pelos 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, por telefone ou outros meios de transmissão, informações como senhas, telefones, endereços (físicos e eletrônicos) ou outras informações de acesso restrito e deve estar atento para não repetir em voz alta essas informações quando forem lhe passadas 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 em aplicativos de conversa etc.

7.4. RECEBIMENTO, ENVIO E COMPARTILHAMENTO DE ARQUIVOS

O Colaborador é responsável pelos arquivos que recebe, envia e compartilha por meio eletrônico e pela infraestrutura tecnológica da Empresa, seja equipamentos de propriedade da Empresa disponibilizados para o uso do Colaborador, equipamentos do próprio Colaborador (quando autorizado pela Vision One, conforme as regras do item 13 - *Dispositivos*), ou ainda, serviços de *cloud* (nuvem).

Para garantir níveis mínimos de segurança da infraestrutura tecnológica da Vision One, é vedado ao Colaborador:

(i) <u>receber, enviar e compartilhar arquivos que</u>: (a) tenham finalidades diversas e não relacionadas às atividades de interesse da Empresa ou relativas aos seus negócios; (b)

contenham pornografia ou conteúdo de cunho racista, discriminatório ou qualquer outro que viole a legislação em vigor, a moral e os bons costumes; (c) violem direitos de terceiros, em especial direitos de propriedade intelectual, direitos autorais, direitos de imagem, entre outros; (d) caracterizem infração civil ou penal e/ou possam causar prejuízos à Empresa e a terceiros; e (e) configurem concorrência desleal ou quebra de sigilo profissional; e

(ii) enviar, compartilhar e baixar: (a) arquivos que contenham malware, como vírus e outros códigos maliciosos; (b) Informações Internas, Confidenciais ou Secretas em ambiente externo; e (c) qualquer arquivo executável (.exe) que não seja autorizado pela Vision One.

7.5. GUARDA E DESLOCAMENTO DE INFORMAÇÕES

Todas as Informações Protegidas que devam ser armazenadas em suporte físico ou digital, quando da sua guarda pelo Colaborador, devem respeitar regras de ciclo de vida dos dados da Empresa, bem como os seguintes cuidados, de acordo com a classificação da informação:

(i) Suporte físico. Todos os documentos contendo Informações Internas, Confidenciais e Secretas devem ser armazenados em arquivos físicos próprios indicados pela Vision One, de acordo com os métodos de identificação do conteúdo, também indicados pela Empresa, incluindo sua data de arquivamento. Documentos utilizados pelo Colaborador em sua estação de trabalho, quando não estiverem sendo utilizados, devem sempre ser guardados em gaveta ou armário, garantindo que tais gavetas e armários permaneçam trancados quando se tratar de Informações Secretas. Nenhuma anotação relacionada às Informações Protegidas deve ser deixada à mostra, seja em cima da mesa, do computador ou em divisórias, mesmo quando o Colaborador estiver presente. Quando o Colaborador não estiver nas dependências da Empresa, os documentos contendo Informações Internas, Confidenciais e Secretas não devem ficar expostos.

(ii) Suporte digital. Todo e qualquer arquivo que contenha Informação Interna, Confidencial ou Secreta deve ser salvo na rede corporativa da Vision One, em diretório específico, que inviabilize o acesso por Colaboradores não autorizados. Caso o arquivo deva ser armazenado em dispositivo móvel (como, por exemplo, em notebooks, por conta de reuniões externas), é indispensável que o Colaborador remova o arquivo do dispositivo após a sua utilização.

Todo e qualquer documento ou arquivo que contenha Informações Confidenciais ou Secretas somente poderá ser alterado, copiado e/ou movimentado se houver a possibilidade de

recuperação, controle de versão ou análise dos registros de tal arquivo ou documento em caso de falhas de segurança que acarretem a perda ou o extravio das Informações Protegidas.

7.6. DESCARTE DE INFORMAÇÕES

O descarte de um documento físico e/ou a exclusão de um arquivo digital da rede da Vision One que contenha Informações Protegidas deverá seguir as seguintes regras de descarte:

(i) Suporte físico: os documentos que tiverem Informações Públicas poderão ser descartados no lixo comum; já aqueles que possuírem Informações Internas, Confidenciais e Secretas devem ser destruídos manualmente ou, preferencialmente, por um aparelho fragmentador antes do descarte. No caso de Informações Secretas, o uso de aparelho fragmentador é obrigatório e, na ausência de tal aparelho, o Colaborador deverá acionar o gestor responsável para que este tome as medidas cabíveis.

(ii) Suporte digital: arquivos que contenham Informações Protegidas e estejam armazenados em suporte digital flexível, tais como CD ou DVD, deverão ser destruídos por meio de aparelho fragmentador e, na ausência de tal aparelho, o Colaborador deverá acionar o gestor responsável para que sejam tomadas as medidas necessárias. Já aqueles arquivos armazenados em suporte digital rígidos, como disco rígido (HD) e pen drive, devem ser encaminhados ao Departamento de Tecnologia, em caixa lacrada, para destruição adequada, conforme o procedimento interno adotado.

Somente o responsável pela geração ou pelo armazenamento do arquivo ou documento a ser descartado tem competência para descartá-lo ou deletá-lo, salvo quando o responsável conferir expressa autorização para que terceiro o faça. Ainda, todo descarte deve ser registrado, a fim de manter um histórico que possibilite a realização de auditorias, caso necessário. No caso de informações que envolvam dados pessoais, o Colaborador seguirá os procedimentos descritos na Política de Retenção e Descarte de Dados da Empresa.

8) E-MAIL CORPORATIVO

Os endereços de e-mail fornecidos pela Vision One aos Colaboradores são individuais e destinados exclusivamente para fins corporativos e relacionados às atividades do Colaborador dentro da Empresa. As mensagens de e-mail sempre deverão incluir assinatura com o formato padrão da Vision One. Acrescentamos que é proibido aos Colaboradores o uso do e-mail da Vision One para:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao uso legítimo da Vision One;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Vision One e as suas unidades vulneráveis a ações judiciais e/ou administrativas;
- divulgar informações não autorizadas, incluindo, sem limitação, imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo responsável;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas; e
- apagar mensagens pertinentes de e-mail quando qualquer uma das unidades ou Colaboradores da Vision One estiverem sujeitos a algum tipo de investigação.

9) INTERNET

Todas as regras da Vision One visam basicamente ao desenvolvimento de um comportamento ético e profissional no uso da internet. Para garantir a utilização racional desses recursos, bem como a segurança dos dados e softwares, a Empresa se reserva o direito de utilizar ferramentas para verificar o conteúdo dos e-mails corporativos e monitorar o uso da internet e da rede corporativa.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao Colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que, nesses casos, a Empresa cooperará ativamente com as autoridades competentes.

Os Colaboradores com acesso à internet poderão fazer o download somente de software ligados diretamente às suas atividades na Vision One e deverão providenciar o que for necessário para regularizar a licença e o registro desses softwares, sempre buscando a aprovação do Departamento de Tecnologia.

Os Colaboradores não poderão:

(i) utilizar os recursos da Vision One para fazer o download ou a distribuição de softwares ou dados sem as licenças adequadas;

(ii) efetuar *upload* ("subir"), para seus pacientes, parceiros e outros terceiros, de qualquer software licenciado à Vision One ou dados de sua propriedade, sem expressa autorização do responsável pelo software ou pelos dados; e

(iii) utilizar a rede de visitantes (rede de internet segregada) com seus dispositivos de trabalho, hipótese em que serão aplicáveis todas as limitações de uso aqui previstas.

10) REDES SOCIAIS E E-MAIL PESSOAIS

A Vision One poderá suspender, sem aviso prévio e a seu exclusivo critério, o uso e o acesso a redes sociais, e-mails pessoais e serviços de mensagens para fins pessoais, ou ainda, suspender o uso e o acesso a quaisquer sites que não tenham relação com a função do colaborador nas dependências físicas e nos dispositivos conectados à rede da Vision One, por questões de governança e/ou de segurança da informação.

11) ACESSO À REDE DE ARQUIVOS

O acesso às informações armazenadas na infraestrutura técnica da Vision One poderá ser realizado de maneira diferente (por meio físico, lógico ou remoto), a depender do tipo de formato. Para cada tipo de formato serão aplicadas regras de conduta distintas, a saber:

11.1. ACESSO FÍSICO ÀS INFORMAÇÕES

Os locais onde estão instalados os datacenters ou armazenados os arquivos físicos da Empresa são considerados parte crítica da sua infraestrutura tecnológica, razão pela qual o cuidado com a proteção e segurança deve ser obrigatoriamente redobrado. Há diferentes tipos de acessos e, para cada um deles, diferentes regras e restrições, conforme consta abaixo:

(i) <u>acessos permanentes:</u> permitidos somente aos empregados e funcionários da Empresa que tenham a necessidade de acesso liberado para executar suas atividades;

(ii) <u>acessos esporádicos:</u> permitidos a outros Colaboradores ou a visitantes externos, mediante autorização prévia da Vision One, com acesso registrado pela equipe de Tecnologia (nome, data e hora) e desde que haja acompanhamento em tempo integral pela equipe responsável; e

(iii) <u>acessos externos:</u> permitidos àqueles que não sejam Colaboradores internos da Empresa (contratantes externos), mediante autorização e desde que tenham contrato vigente com a Vision One que justifique esse acesso.

11.2. ACESSO LÓGICO

O acesso às informações armazenadas na infraestrutura tecnológica da Empresa será restrito a cada Colaborador, a depender do perfil de acesso que lhe for atribuído pelo Departamento de Tecnologia, conforme as regras dispostas no item 12 – *Identificação e Senhas*. Cada perfil pressupõe a liberação do acesso de determinados diretórios dentro da rede da Empresa, que são atribuídos pelo Departamento de Tecnologia, de modo que as informações poderão ser acessadas de acordo com o nível de acesso definido pela Vision One.

11.3. ACESSO REMOTO

Quando o Colaborador não se encontrar nas dependências da Vision One, ele poderá acessar a rede privada da Empresa de forma remota, por meio de tecnologias autorizadas pela Vision One, podendo incluir o uso de VPN. O acesso remoto somente será concedido ao Colaborador nos casos em que houver necessidade comprovada. Verificada a necessidade, o acesso remoto somente será permitido após aprovação formal escrita da Vision One e será concedido apenas àquela parte da rede relacionada com o perfil do Colaborador, sendo vedado o acesso remoto à rede integral da Empresa.

O acesso remoto somente é permitido para a execução das atividades profissionais do Colaborador que estejam vinculadas à Empresa, de forma que tal acesso não poderá ser realizado por dispositivo ou software particulares do Colaborador ou de propriedade de terceiros. O Colaborador é responsável por todas as atividades realizadas quando do seu acesso remoto, respondendo por qualquer uso irregular, inclusive por outra pessoa na posse de seu acesso. No caso de furto, roubo ou extravio de equipamento móvel que tenha o acesso remoto à VPN da Empresa configurado, o Colaborador deverá imediatamente procurar uma autoridade policial para lavrar um boletim de ocorrência e, na sequência, comunicar o incidente à equipe de Tecnologia, apresentando cópia do boletim de ocorrência lavrado.

Todos os acessos remotos serão registrados pela equipe de Tecnologia e tais registros ficarão disponíveis para consulta em caso de auditoria.

12) IDENTIFICAÇÃO E SENHAS

Todos os Colaboradores têm determinados privilégios de acesso a Informações Protegidas, de acordo com seu cargo e as suas atribuições, conforme as regras dispostas no item 11 – *Acesso à Rede de Arquivos*. Alguns exemplos de privilégio são acesso externo ao e-mail, liberações no acesso à internet e no acesso lógico, utilização externa de determinados equipamentos da Empresa, liberação de espaço em disco rígido, utilização de dispositivos móveis, entre outros.

O Colaborador receberá um login e uma senha, de acordo com o perfil que lhe for atribuído, que lhe permitirá ser identificado quando do acesso à infraestrutura da Empresa. Assim, o Colaborador somente terá acesso às áreas da infraestrutura da Vision One que forem autorizadas considerando o seu perfil. A Vision One reserva-se o direito de revisar, a qualquer momento e sem aviso prévio, por meio dos departamentos competentes, os privilégios de qualquer Colaborador, a fim de resguardar os níveis de segurança da informação da Empresa.

O login e a senha do Colaborador são pessoais e, consequentemente, o Colaborador é o responsável pelo sigilo e pela manutenção segura da sua senha vinculada ao login, sendo proibido o compartilhamento de login e senha com terceiros, inclusive outros Colaboradores, sob pena de arcar com as sanções não só previstas nesta Política, mas também as penalidades civis, criminais e trabalhistas, respondendo, inclusive, por todo e qualquer dano que causar à Empresa.

Além do login do Colaborador, ele também receberá uma identificação física que lhe concederá acesso a determinadas áreas físicas da Empresa. Tal identificação será feita por meio de um crachá, cujo uso é pessoal e intransferível.

13) DISPOSITIVOS

Os dispositivos físicos capazes de armazenar Informações Protegidas, como computadores, celulares, notebooks, tablets e outros, disponibilizados aos Colaboradores para a execução de suas atividades, são de propriedade da Vision One, 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 pelo Departamento de Tecnologia.

Os equipamentos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos. Os computadores devem ter o recurso de atualizações automáticas do sistema operacional habilitada por padrão e software antivírus instalado, ativado e atualizado frequentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o Departamento de Tecnologia.

Arquivos pessoais e/ou não pertinentes ao negócio da Vision One (fotos, músicas, vídeos etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento no disco do computador. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente.

Documentos imprescindíveis para as atividades dos Colaboradores e/ou para os negócios da Empresa deverão ser salvos em diretório sincronizado, como serviço de *cloud*, garantindo o backup e a disponibilidade em qualquer computador. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio Colaborador.

O Colaborador entende que é o responsável por todo e qualquer dano que causar nos equipamentos, por dolo ou culpa, e está ciente e concorda em observar as seguintes regras:

- O Colaborador é responsável pelos equipamentos e se compromete a empregar todos os cuidados necessários, como se o dispositivo fosse seu;
- Todos o acesso aos computadores deverá ter ser feito através de login e senha individuais e intransferíveis fornecidos pelo Departamento de Tecnologia da Vision One;
- Os dispositivos móveis devem estar sempre a seu alcance e não podem ser deixados em locais públicos, em veículos ou em qualquer outro local, fora das dependências da Vision One, em que possa haver acesso do equipamento por pessoas não autorizadas, a fim de evitar o furto e/ou roubo destes equipamentos, bem como o vazamento das Informações Protegidas nele contidas;
- Os Colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico de Tecnologia da Vision One ou por terceiros devidamente contratados para o serviço;
- O Colaborador deverá manter a configuração do equipamento disponibilizado pela Vision One, 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;
- É expressamente proibido o fumo na mesa de trabalho ou próximo aos equipamentos;
- Deverão ser protegidos por senha (bloqueados) todos os dispositivos, incluindo terminais de computador, quando não estiverem sendo utilizados;
- Todos os recursos tecnológicos adquiridos pela Vision One devem ter imediatamente suas senhas padrões (*default*) alteradas;
- Todos os dispositivos devem ser protegidos por senha e não devem ficar logados quando o Colaborador não estiver presente;
- Se, no decorrer do uso do dispositivo, o Colaborador tiver dúvidas sobre o seu manuseio ou constatar falhas que impliquem a necessidade de sua substituição ou manutenção, o Colaborador deverá abrir um chamado junto ao Departamento de Tecnologia que, por sua vez, além de fornecer os esclarecimentos necessários, deverá

orientá-lo a entregar o equipamento no local indicado para sua substituição ou conserto;

- Caso o uso de um dispositivo seja esporádico, o Colaborador deverá devolvê-lo ao Departamento de Tecnologia em perfeitas condições de uso, juntamente com eventuais acessórios que lhe tenham sido entregues, como bolsas, *cases*, películas etc., tão logo termine o período necessário para o uso. Em caso de não devolução do equipamento, no prazo e local determinado, o Colaborador será responsável por restituir os custos de tal equipamento à Empresa, sem prejuízo de outras medidas legais e administrativas a serem tomadas pela Vision One;
- No caso de perda, furto, roubo ou dano ao equipamento, o Colaborador deve comunicar imediatamente o Departamento de Tecnologia, que procederá com o bloqueio de seu usuário e senha da rede e sistemas corporativos; e
- O Colaborador também deverá procurar as autoridades policiais e realizar um boletim de ocorrência, que deverá ser apresentado ao Departamento de Tecnologia quando da comunicação do incidente.

O uso indevido dos dispositivos da Vision One sujeitará o Colaborador às sanções aplicáveis, a depender da gravidade da conduta praticada. São algumas hipóteses de uso indevido:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem a explícita autorização do proprietário;
- Vigiar secretamente outrem por dispositivos eletrônicos ou software, como, por exemplo, analisadores de pacotes (*sniffers*);
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de crimes ou atos ilícitos, como os de assédio sexual, constrangimento, perseguição (*stalking*) ou manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro conteúdo que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública; e
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

14) DATACENTER E CLOUD

A Vision One utiliza diversos softwares próprios e de terceiros no curso de suas operações e o Colaborador não poderá:

(i) utilizar tais softwares para fins pessoais ou de qualquer forma que comprometa a segurança da infraestrutura da Empresa;

(ii) excluir, modificar, copiar, transferir, realizar engenharia reversa ou ceder o acesso de tais softwares a terceiros, ou praticar qualquer ato que esteja em desacordo com a legislação aplicável; e

(iii) instalar na rede ou nos dispositivos da Empresa qualquer software pirata, não licenciado ou não autorizado pela área Tecnologia, sendo que qualquer software não autorizado baixado pelo Colaborador será excluído pela equipe de Tecnologia.

A Vision One disponibiliza apenas o(s) recurso(s) para o armazenamento externo de arquivos, softwares e sistemas. Assim, é proibido a utilização pelo Colaborador de serviços de armazenamento na nuvem não disponibilizados por meio da infraestrutura tecnológica da Empresa.

15) DESLIGAMENTO OU MOVIMENTAÇÃO DO COLABORADOR

Ao término do vínculo do Colaborador com a Vision One, o seu acesso à infraestrutura tecnológica da Empresa será revogado de forma imediata. O Colaborador deverá devolver, em perfeitas condições de uso, todos e quaisquer dispositivos de propriedade da Vision One que estejam em sua posse, juntamente com eventuais acessórios lhe tenham sido entregues. As obrigações de sigilo e não reprodução das Informações Protegidas, assumidas pelo Colaborador nessa PSI, permanecerão em vigor mesmo após o desligamento do Colaborador.

Em caso de não devolução do equipamento, no prazo e local determinado, o Colaborador será responsável por restituir os custos de tal equipamento à Vision One. Em caso de perda, furto ou roubo de equipamentos, as regras previstas no item 13 - *Dispositivos* - serão aplicadas.

Caso o Colaborador tenha acesso à conta de e-mail corporativa ou a qualquer outro software instalado em um dispositivo pessoal, o Departamento de TI e/ou Departamento RH poderá verificar o dispositivo para constatar a referida remoção da conta corporativa.

Caso o Colaborador mude de departamento ou de função dentro da Vision One, este também deverá ter seus acessos revistos, passando a visualizar apenas os sistemas e pastas de rede necessários ao desempenho de sua nova função.

16) REPORTE DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Para evitar a exposição indevida das Informações Protegidas, a Vision One emprega medidas de segurança, tanto internas quanto externas, as quais atendem as obrigações legais vigentes. Porém, essas medidas somente serão eficazes se o Colaborador cumprir com as obrigações de segurança assumidas nesta Política, uma vez que tais incidentes podem ocorrer em razão de falhas humanas, tecnológicas ou sistêmicas.

Caso o Colaborador tome conhecimento ou suspeite de qualquer acontecimento que viole as regras desta Política ou coloque em risco a segurança das informações da Empresa, ele deverá imediatamente comunicar a Vision One, que disponibilizará um canal de reporte anônimo. A Vision One, por meio de seu Departamento de Tecnologia, irá apurar as causas e os efeitos do incidente ocorrido, para, então, tomar as medidas de contenção, avaliação de impacto e necessidade de comunicação sobre o incidente ao órgão competente e/ou aos titulares das Informações Protegidas, conforme o Plano de Resposta a Incidentes da Vision One.

Para que seja realizada uma auditoria sobre o incidente, a Vision One analisará toda e qualquer informação, bem como as evidências disponíveis que possam identificar a causa do problema. As informações e evidências serão compiladas e anexadas a um relatório para formalização do ocorrido.

17) SANÇÕES

Caso o Colaborador não cumpra as regras desta Política, ele estará sujeito à aplicação de sanções que serão determinadas pela direção da Empresa de acordo com o grau de gravidade da conduta praticada pelo Colaborador, podendo variar entre:

(i) **advertência**: no caso de infrações consideradas leves;

(ii) **suspensão**: no caso de infrações consideradas graves ou quando for constatada a reincidência de uma conduta classificada leve; e

(iii) **encerramento do contrato**: no caso de infrações consideradas gravíssimas ou quando for constatada reincidência de uma conduta considerada grave. Tratando-se de Colaborador empregado, isso significa o desligamento do Colaborador e a rescisão de seu contrato de trabalho por justa causa. Tratando-se de Colaborador não empregado, isso significa a rescisão de contrato com a Vision One, que será realizada de acordo com as disposições do contrato firmado e com a legislação vigente.

Os Colaboradores que cometerem infração às regras desta PSI serão comunicados por escrito. Tal comunicação conterá a regra violada, a conduta praticada pelo Colaborador e a sanção aplicada pela Empresa.

18) DISPOSIÇÕES GERAIS

As exceções às regras estabelecidas por esta norma específica para atender alguma demanda específica devem ser apresentadas à Vision One para avaliação e aprovação.

Essa Política poderá ser revista, atualizada e alterada anualmente ou a qualquer tempo, a exclusivo critério da Vision One, sempre que algum fato relevante ou evento motive sua revisão antecipada.

Data da última atualização: 09 de março de 2022.