Viskase Companies Inc.

Política de Segurança de Dados Corporativos

15 DE JANEIRO DE 2020

FICHA DE CONTROLE DE ATUALIZAÇÕES

Título do Documento	**Política de Segurança de Dados Corporativos**
Autor(es)	Departamento de TI
Número da Versão	1.0
Data de Modificação	01/15/2020

Tabela 1 – Identificação do Documento

Histórico	**Data**	**Status**	**Aprovação**
Versão 1.0	08/01/2019	Emissão Inicial	CEO
Versão 1.1	01/15/2020	Modificado para atender às regulamentações de privacidade da França, Alemanha, Itália, Polônia, Espanha, México, Filipinas e Brasil	CEO

Tabela 2 – Histórico do Documento

Índice

1.0 DECLARAÇÃO DA POLÍTICA

1.1 Declaração de Objetivo

A Viskase Companies Inc. e suas subsidiárias ao redor do mundo, incluindo a Viskase Brasil Embalagens Ltda ("Viskase", "Companhia" ou "companhia") é considerada a titular de dados de todos os dados da Companhia, e os dados pessoais (ou seja, qualquer informação relacionada a uma pessoa natural identificada ou identificável) são incluídos como parte da Viskase. Pessoa individual ou departamentos poderão ter responsabilidades de administração por partes dos dados da Companhia.

A criação de uma politica de segurança de dados é necessária para o estabelecimento de uma estrutura que proteja todos os dados de riscos da Companhia, incluindo, entre outros, a destruição; modificação; divulgação; acesso, uso e remoção não autorizada. Essa politica descreve medidas e responsabilidades exigidas para proteger os dados e recursos da Companhia.

1.2 Escopo

Essa política é aplicável a todos os colaboradores, consultores, equipe temporária e outros trabalhadores da Viskase Brasil Embalagens Ltda., que criarem, receberem, utilizarem, transmitirem e/ou armazenarem dados da Companhia. Ela é aplicável a todos os dados administrativos, todos os dados desenvolvidos por usuários e sistemas que possam acessar esses dados, independentemente do ambiente o qual os dados estejam inseridos (incluindo sistemas, servidores, computadores pessoais, notebooks, dispositivos portáteis, etc.). Essa política é aplicável independentemente da mídia na qual os dados estiverem inseridos (incluindo eletrônica, microficha, impressões, CD, etc.) ou a forma que eles possam tomar (texto, gráficos, vídeo, voz, etc.).

Contratadas, consultores e fornecedores são obrigados a cumprir com essa política ao trabalhar em nome da Companhia. Caso informações confidenciais precisarem ser acessadas ou compartilhadas com esses terceiros, eles devem ser vinculados por contrato para cumprir com as políticas de segurança de dados da Viskase (consulte a Seção 6.1).

Essa política deve ser lida juntamente com outras políticas relacionadas à segurança e privacidade, tais como Políticas de Privacidade de Colaboradores, Notificações de Proteção de Dados de Colaboradores e/ou Política de Senhas. Se você não tiver certeza ou dúvidas com relação à abrangência de determinadas informações por essa Política, entre em contato com o Oficial de Segurança da Informação antes de enviar as informações a partes externas.

Diretrizes Gerais

Dados devem ser mantidos de maneira segura, precisa e confiável e estarem prontamente disponíveis para uso autorizado. Medidas de segurança de dados serão implementadas proporcionalmente ao valor, sensibilidade e risco dos dados. Para implementar segurança no nível apropriado, estabelecer diretrizes para conformidade legal/regulatória, e reduzir ou eliminar normas e controles conflitantes, os dados devem ser classificados em uma das seguintes categorias:

1. Confidenciais - Dados que forem legalmente regulados, inclusive dados pessoais, e dados que forneçam acesso a informações secretas, privadas ou restritas.
2. Apenas Para Uso Interno - Dados cujos Proprietários de Dados decidiram NÃO publicar ou tornar públicos e dados protegidos por obrigações contratuais.
3. Públicos - Dados sobre os quais não há expectativa para privacidade ou confidencialidade.

Dados "Confidenciais" e "Apenas Para Uso Interno" exigirão medidas de segurança variáveis adequadas ao grau que a perda ou corrupção dos dados implicaria nos negócios, resultaria em perda financeira, ou violasse a lei, política ou contratos da Companhia. Medidas de segurança para dados são mutuamente acordadas pelo Oficial de Segurança da Informação, Departamento de Tecnologia da Informação e os respectivos Proprietários de Dados.

Consulte a seção de Classificação de Dados abaixo para obter detalhes adicionais.

2.0 FUNÇÕES E RESPONSABILIDADES

As funções e responsabilidades do pessoal são definidas abaixo. Os nomes específicos do pessoal agindo dentro de cada função podem ser encontradas na seção de Contatos dessa Política.

2.1 Oficial de Segurança da Informação

O Oficial de Segurança da Informação possui responsabilidade de supervisão pelo programa de segurança de dados, bem como pela conformidade com as regulações, políticas de segurança, normas e diretrizes relevantes.

O Oficial de Segurança da Informação é responsável pelo seguinte:

- Análises periódicas da Política de Segurança de Dados Corporativos para garantir alinhamento com as práticas e exigências regulatórias atuais.
- Supervisão de políticas de segurança de dados e seu cumprimento.
- Trabalho com Monitores de Regulação e Proprietários de Dados para garantir a conformidade com a Política de Segurança de Dados Corporativos.
- Aviso sobre violações de política relatadas e inclusão em investigações de segurança de dados.
- Trabalhos com a pessoa responsável por inquéritos externos envolvendo problemas de conformidade com segurança de dados.

2.2 Monitores de Regulação

Monitores de Regulação possuem responsabilidade de supervisão por uma ou mais regulações. Monitores de regulação ficam a par das atualizações de suas respectivas regulações, garantem que políticas estejam atualizadas e notificam o Oficial de Segurança da Informação e Proprietários de Dados sobre alterações.

As regulações que envolvem segurança de dados e que impactam diretamente a Viskase incluem as seguintes:

- HIPAA – V.P. e Diretor de Pessoas
- Regulação de Proteção de Dados Geral da UE e outras leis de privacidade de dados – Diretor de Compliance

- Demais leis de privacidade – Diretor de Compliance
- Lei estadual de notificação de violação de dados dos EUA – Diretor de Compliance
- Normas Federais de Procedimentos Civis – Diretor Jurídico
- Sarbanes-Oxley – Diretor Financeiro

2.3 Controladores de Dados

Cada filial da Viskase é uma Controladora de Dados nos termos das leis de proteção de dados aplicáveis, inclusive a Lei Geral de Proteção de Dados (Lei nº 13.709/2018). A Companhia, individualmente ou em conjunto com outros, determina os propósitos e meios do processamento de dados pessoais.

A Viskase Brasil Embalagens Ltda. é a Controladora de Dados no Brasil.

Adicionalmente à essa Política, os Controladores de Dados devem fornecer aos proprietários dos dados guias e instruções sobre como processar os dados pessoais para os propósitos relevantes às operações dos Controladores de Dados.

2.4 Proprietários de Dados

Proprietários de Dados são tipicamente colaboradores de nível gerencial, o qual possui responsabilidades de planejamento e tomada de decisão em suas áreas funcionais. Os Proprietários de Dados, como um grupo, são responsáveis por treinar Usuários de Dados sobre o manuseio adequado de dados.

Proprietários de Dados, como indivíduos, possuem responsabilidade a nível operacional pelas atividades de gerenciamento de informações relacionadas à captura, manutenção e disseminação de dados. Proprietários de Dados são responsáveis por garantir que Usuários de Dados estejam adequadamente informados sobre as obrigações de segurança associadas a seu acesso a dados, bem como pela análise periódica de acesso de usuários a seus dados confidenciais.

Dados e a responsabilidade pelos dados são tipicamente organizados ao longo de linhas funcionais; portanto, o Proprietário de Dados atual pode ser encontrado nos seguintes departamentos funcionais:

- Contabilidade / Dados Financeiros
- Dados de Engenharia
- Laboratório de Alimentos
- Saúde e Segurança
- Recursos Humanos
- Tecnologia da Informação
- Auditoria Interna / Conformidade
- Jurídico
- Logística
- Manutenção
- Marketing
- Operações
- Pagamento
- Planejamento de Produção
- Compras
- Controle de Qualidade
- P & D
- Vendas
- VEP

2.5 Usuários de Dados

Usuários de Dados são aqueles que visualizam, copiam ou baixam os dados como parte de suas tarefas designadas ou no cumprimento de suas funções na Companhia. Todos os Usuários de Dados possuem obrigação de compreender as responsabilidades de segurança associadas a seus níveis de acesso a dados. Usuários de Dados com acesso à Dados Confidenciais e/ou de Uso Interno, devem assinar declaração de confidencialidade apropriada.

2.6 Departamento de Tecnologia da Informação

O Departamento de Tecnologia da Informação é responsável por fornecer uma estrutura segura no suporte de dados, incluindo, entre outros, fornecer segurança física, backup e processos de recuperação, concedendo privilégios de acesso a usuários do sistema conforme autorizado por Controladores de Dados, e implementar e administrar controles sobre as informações.

3.0 CLASSIFICAÇÃO DE DADOS

Dados da Companhia podem ser classificados em uma d três categorias. Cada categoria exige diferentes níveis de segurança, armazenamento, transmissão e aprovação para distribuição. Consulte a **Matriz de Classificação de Dados - Apêndice 1** para obter detalhes sobre as classificações de dados e exigências de segurança que envolvem cada uma. As descrições das categorias são apresentadas conforme segue.

3.1 Dados Confidenciais

Essa classificação é aplicável a informações sensíveis da Companhia que são destinadas a uso apenas dentro da organização. Sua divulgação não autorizada poderia impactar de forma séria e adversa a organização, seus colaboradores e seus parceiros de negócios.

Exemplos incluem, entre outros:

- Documentos de aquisição e Fusão
- Planos estratégicos de nível corporativo
- Informações de Litígio
- Dados financeiros
- Informações de Compras
- Contratos de Clientes e Fornecedores
- Projetos de engenharia – Classe 3, 4 e 5
- Dados pessoais

3.2 Apenas Para Uso Interno

Essa classificação é aplicável a todas as outras informações que não se adequam de forma clara a outras classificações. Não se espera que a divulgação, modificação ou destruição não autorizada dessas informações impactem de forma séria ou adversa a organização, seus colaboradores ou seus parceiros de negócios.

Exemplos incluem, entre outros:

- Desenhos de engenharia – Classes I e II

- Novos materiais de treinamento de colaborador (não-manutenção)
- Manuais de política interna.

3.3 Dados Públicos

Essa classificação é aplicável a informações que se encontram disponíveis ao público geral e são destinadas a distribuição fora da organização. Essas informações poderão ser livremente disseminadas sem prejuízo potencial.

Exemplos incluem, entre outros:

- Brochuras de produtos e serviços
- Anúncios
- Anúncios de abertura de vaga de trabalho
- Comunicados de Imprensa

4.0 SEGURANÇA DE DADOS INTERNOS

Usuários de Dados são responsáveis por proteger todos os dados da Companhia e por garantir que Dados Confidenciais sejam protegidos ao salvar arquivos em um servidor/pasta interno (a) na rede da Companhia ou em sites de SharePoint da Companhia.

É exigido que todos os Usuários de Dados:

- Acessem dados apenas para a condução dos negócios da Companhia, os quais estejam expressamente designados ao Usuário de Dados, consideradas as permissões e privilégios de acesso ao dado.
- Solicitem apenas o mínimo necessário de Dados Confidenciais para realizar suas atividades comerciais.
- Respeitem a confidencialidade e privacidade de indivíduos cujos registros eles possam vir a acessar.
- Cumpram com todas as restrições ética aplicáveis a dados aos quais tiverem acesso.
- Saibam sobre e cumpram com as leis ou políticas aplicáveis com relação a acesso, uso, ou divulgação de dados.

O Departamento de Tecnologia da Informação deve aprovar o uso de qualquer sistema ou aplicação que processe, armazene ou transmita eletronicamente dados da Companhia. A Viskase reserva o direito de escanear eletronicamente todos os recursos detidos pela Companhia e recursos conectados à rede interna para Dados Confidenciais. O monitoramento realizado pela Companhia é descrito na específica Política de Privacidade de Colaboradores. Caso sejam encontrados Dados Confidenciais em localizações não autorizadas, o Oficial de Segurança da Informação é responsável por acompanhar junto ao Proprietário de Dados para corrigir a situação.

4.1 Computadores, Notebooks, Telefones Móveis e Tablets.

Computadores e Notebooks da Companhia são protegidos por meio de diversas técnicas de segurança e são considerados localizações de armazenamento seguro para dados da Companhia. Os dados em computadores e notebooks da Companhia não possuem backup completo. Arquivos

salvos no desktop de um usuário ou na pasta “Meus Documentos” versões do Windows 7 anteriores ou a pasta “Documentos” para versões do Windows 10 possuem backup automático em um servidor de rede interno, mas outras pastas e locais de arquivo não possuem. Portanto, um Usuário de Dados deve salvar seus dados criados e/ou usados no desenvolvimento de suas funções designadas na Companhia em seu desktop ou na pasta Meus Documentos/documentos para se proteger da possibilidade de perda.

Telefones móveis e tablets da Companhia contém Sistemas de Gerenciamento de Dispositivos, os quais asseguram a conformidade dos sistemas com as regras de segurança da Companhia e com esta Política. Antes do primeiro acesso ao e-mail da Companhia, o colaborador deverá concordar eletronicamente com os termos e condições que determinam as responsabilidades dos colaboradores e o direito da Viskase sobre o e-mail e sobre os dados da Companhia nos telefones móveis e tablets.

A Companhia se reserva ao direito de desconectar qualquer software ou aplicação configurada em telefones móveis ou tablets da Companhia, ou a desabilitar serviços da Companhia relacionados sem notificação. A Companhia se reserva ao direito de desligar remotamente qualquer informação da companhia e/ou qualquer serviço de seus telefones móveis e tablets sem qualquer prévia notificação.

4.2 Mensagens Eletrônicas

Mensagens Eletrônicas incluem E-mail, mensagem de voz, mensagens instantâneas, mensagens pessoais, mensagem por texto SMS, FAX, pager ou qualquer outro método eletrônico para transferir dado a outros. Mensagens eletrônicas tipicamente não são um método seguro de transmitir dados da Companhia. A transmissão de E-mails, e não das próprias mensagens do E-mail, é protegida pela codificação, caso for enviada a partir dos servidores de E-mail da Companhia a destinatários internos e externos. No entanto, alguns serviços de mensagem eletrônica não oferecem codificação, como mensagens de texto, FAX e pagers. Portanto, Usuários de Dados não devem esperar privacidade ao utilizar mensagem eletrônica não protegida, já que mensagens podem ser interceptadas e lidas por outros, caso não forem codificadas.

Usuários de Dados não devem enviar Dados Confidenciais da Companhia ou dados Apenas Para Uso Interno para ou de nenhuma conta de mensagem eletrônica pessoal. O uso de contas de mensagens eletrônicas pessoais (como conta pessoal do Gmail) para Dados Confidenciais ou dados Apenas Para Uso Interno é estritamente proibido e praticar tal ato levará a ações disciplinares, e eventualmente à rescisão, de acordo com a legislação aplicável, exceto por documentos de RH próprios do colaborador, documentos relacionados a benefícios e folha de pagamento, tais como análises de desempenho, formulários de inclusão / seleção de seguro e benefícios, e formulários de folha de pagamento de tributos (i.e. formulários W-2, declarações de previdência social do empregador, outros formulários tributários específicos).

Se um Usuário de Dados possuir E-mails ou arquivos contendo Dados Confidenciais ou dados Apenas Para Uso Interno em uma conta de E-mail pessoal ou em um computador privado pessoal, ele deve deletar os E-mails e arquivos imediatamente, caso contrário ele estará sujeito àà

ação disciplinar, e eventualmente à rescisão, de acordo com a legislação aplicável. O uso de smartphones pessoais e celulares pessoais para fins comerciais é abordado na seção 4.5 abaixo.

Usuários de Dados devem tomar precauções especiais na transmissão de Dados Confidenciais e dados Apenas Para Uso Interno via mensagens eletrônicas a um dispositivo não pertencente a Companhia, relacionada à Companhia ou serviço eletrônico de mensagem relacionado a Companhia (como smartphone ou conta de E-mail de um cliente ou fornecedor). Precauções especiais incluem o seguinte:

- Transmitir Dados Confidenciais via mensagem de texto, FAX ou pager é estritamente proibido.
- Transmitir dados Apenas Para Uso Interno via mensagem de texto, FAX ou pager deve ser evitado.
- Garantir que o endereço do destinatário esteja correto antes de a mensagem ser enviada.
- Considerar proteger mensagens contendo Dados Confidenciais conforme segue:
    - E-mails que contêm Dados Confidenciais devem incluir redação na seção de Assunto como “Estritamente Confidencial”, “Confidencial” ou “Produto de Trabalho de Advogado Privilegiado e Confidencial” dependendo das circunstâncias.
    - E-mails enviados a partes externas contendo Dados Confidenciais podem ser protegidos adicionalmente ao usar uma das configurações de “Permissão” de e-mail que não a configuração de “Acesso irrestrito”.
        - Configurações de permissões podem ser encontradas sob a aba “Opções” de qualquer e-mail criado no Outlook.
        - Codificar mensagens eletrônicas a dispositivos não pertencentes à Companhia/serviços de mensagem sempre que possível.
    - Documentos que contém Dados Confidenciais devem possuir formato imodificável, como arquivo protegido por senha com bloqueio de modificações adicionais.
- As exigências de Segurança de Fornecedor (seção 6.0) descritas abaixo devem ser seguidas.

Não use serviços eletrônicos de mensagem como instalação de armazenamento de dados ou retenção de dados. Caso a mensagem for a única localização onde os Dados Confidenciais ou dados Apenas Para Uso Interno residirem, e tais dados precisarem ser retidos para fins futuros, então tais dados devem ser salvos em um local da rede interna (Vide item 4.1 acima).

4.3 Discos de Rede Interna e Locais de SharePoint

Discos de rede interna e locais de SharePoint são recursos protegidos, onde usuários podem compartilhar seus arquivos com outras pessoas. A proteção desses recursos depende do Controlador de Dados e administrada pelo Proprietário de Dados. O Usuário de Dados que solicitou e/ou aprovou a solicitação de acesso a uma pasta da rede interna ou local de SharePoint é considerado o Proprietário de Dados. Algumas pastas da rede interna e locais de SharePoint contêm informações que devem ser acessíveis a diversos outros usuários. Outras redes internas/locais de SharePoint contêm Dados Confidenciais onde o acesso deve ser restrito.

O Proprietário de Dados é responsável por identificar seus discos de rede e locais de SharePoint onde os Dados Confidenciais residem e por informar o Oficial de Segurança da Informação de

sua localização. O Oficial de Segurança da Informação encaminhará as informações sobre localização ao Departamento de Tecnologia da Informação para que a rede interna/local de SharePoint seja protegida.

Permissões de acesso de usuário a pastas da rede interna ou a locais de SharePoint que contêm Dados Confidenciais ou dados Apenas Para Uso Interno devem ser analisadas periodicamente. É responsabilidade do Proprietário de Dados entrar em contato e trabalhar com o Departamento de Tecnologia da Informação para analisar periodicamente o acesso de usuários a seus dados. Usuários que não deveriam possuir acesso aos dados devem ser removidos imediatamente.

4.4 Mídia Removível

Mídia removível inclui flash drives USB (pendrives), Discos Compactos (CDs) discos Zip, disquetes, discos rígidos externos, câmeras digitais, smartphones, cartões de memória e qualquer outro dispositivo de armazenamento de dados eletrônico que seja externo a um computador ou notebook.

O uso de mídia removível deve ser limitado a Dados Públicos. Salvar Dados Confidenciais ou dados Apenas Para Uso Interno em mídias removíveis é proibido, exceto em casos de emergências, onde problemas técnicos impeçam o uso de dispositivos da Companhia, serviços eletrônicos de mensagem da Companhia ou o uso de rede interna. Caso Dados Confidenciais ou dados Apenas Para Uso Interno forem salvos em mídias removíveis em tal emergência, os dados devem ser imediatamente excluídos da mídia removível assim que os problemas técnicos forem resolvidos ou a emergência não exista mais.

Quando Dados Confidenciais ou Apenas Para Uso Interno forem salvos em mídias removíveis, principalmente quando os dados contiverem informações pessoalmente identificáveis, o Usuário de Dados é responsável por garantir que todos os Dados Confidenciais e dados Apenas Para Uso Interno sejam codificados antes de serem salvos na mídia removível, ou que a própria mídia removível seja protegida por senha e forneça codificação de arquivos armazenados na mídia.

4.5 Dispositivos Móveis Pessoais

Dispositivos Móveis Pessoais incluem qualquer notebook, tablet, smartphone, celular ou qualquer outro dispositivo de computação que possa ser facilmente carregado e utilizado por um indivíduo, e que não seja detido pela Companhia.

Em nenhum momento é permitido que um Dispositivo Móvel Pessoal se conecte fisicamente à rede ethernet da Companhia. Conexões físicas incluem o uso de cabo de rede, como cabo Ethernet CAT5, que pode ser inserido em uma porta de comunicação de um Dispositivo Móvel Pessoal e uma saída Ethernet ou tomada de parede. E em nenhum momento será permitido que um Dispositivo Móvel Pessoal seja conectado ao Wi-Fi da Companhia, exceto pela rede de Wi-Fi de convidado.

Não é exigido e-mail da Companhia em Dispositivos Móveis Pessoais para que colaboradores cumpram suas funções. Ao contrário, o uso do e-mail da Companhia em Dispositivos Móveis Pessoais é oferecido como conveniência aos colaboradores e somente mediante sua solicitação. Ao efetuar tal solicitação, o colaborador reconhece e aceita que o uso do e-mail no Dispositivo Móvel Pessoal não dá o direito a qualquer compensação. O acesso ao e-mail da Companhia em

um Dispositivo Móvel Pessoal não corresponde a trabalho em horário extraordinário ou tempo à disposição da Companhia, exceto se especificamente solicitado pela Companhia, de acordo com os procedimentos internos aplicáveis. O reembolso pelo uso de Dispositivos Móveis Pessoais para fins comerciais é detalhado na Política de Viagem Corporativa.

O uso de Dispositivos Móveis Pessoais para negócios da Companhia será permitido apenas se as exigências a seguir forem atendidas.

- Colaboradores devem aceitar eletronicamente os termos e condições providos pelo sistema de Gerenciamento de Dispositivos Móveis antes do seu acesso ao e-mail da Companhia em seus Dispositivos Móveis Pessoais. Os termos e condições são específicos para cada país e descrevem as responsabilidades do colaborador e o direito da Viskase em relação ao e-mail da Companhia e os dados da Companhia no Dispositivo Móvel Pessoal do colaborador.

O seguinte detalha os riscos e responsabilidades relacionados ao uso de Dispositivos Móveis Pessoais para negócios da Companhia.

- O Oficial de Segurança da Informação possui o direito de restringir o uso de qualquer Dispositivo Móvel Pessoal específico para os negócios da Companhia caso ele acreditar que o modelo específico, sistema operacional, versão, etc., a ser utilizado crie um risco de segurança.
- A Companhia reserva o direito de desconectar Dispositivos Móveis Pessoais ou desabilitar serviços sem notificação. A Companhia reserva o direito de apagar remotamente o dispositivo sem notificação caso um dos seguintes incidentes aconteça:
    - O dispositivo for perdido ou roubado;
    - O colaborador rescindir seu contrato de trabalho; ou
    - Se houver evidência razoável de que o colaborador tenha violado a política da Companhia ou diminuído a capacidade de integridade do dispositivo, que possa resultar em vírus ou outra ameaça à segurança dos dados da Companhia ou infraestrutura da tecnologia.
- O colaborador é responsável por tomar precauções para impedir a perda de seus dados, como realizar backup periódico de seus dados pessoais.
- O colaborador deve notificar a operadora imediatamente se o dispositivo for perdido ou roubado, e ele deve notificar a Companhia dentro de 24 horas do momento em que foi sabido que o dispositivo foi roubado ou perdido.
- O colaborador não deve permitir que ninguém mais use seu dispositivo quando estiver conectado à rede, aplicação, sistema ou qualquer outro recurso da Companhia.
- O colaborador não deve dar acesso a ninguém às informações da Companhia no dispositivo, esteja o dispositivo conectado à rede da Companhia ou não.

4.6 Fotografia Dentro das Instalações

O uso de câmeras (fotográficas, de vídeo, smartphones ou celulares) em áreas operativas de uma instalação, sem autorização prévia do Diretor Geral, Gerente Geral ou Gerente da Instalação é estritamente proibido. Autorizações podem apenas ser fornecidas para casos específicos e devem ser documentadas por escrito sempre que possível. Autorizações ilimitadas não são permitidas.

Áreas operativas da instalação incluem, entre outras, área de extrusão, área de junção, salas de amadurecimento, salas químicas e qualquer área onde matérias-primas, materiais semiacabados e materiais acabados forem processados.

Imagens fotográficas e vídeos de áreas operativas são considerados Dados Confidenciais e todas as precauções e processos de segurança devem ser estritamente seguidos.

Imagens ou vídeos devem apenas ser feitos em dispositivos fornecidos pela Companhia, a menos que autorizado com antecedência pelo Diretor Geral, Gerente Geral ou Gerente da Instalação por escrito. A transmissão eletrônica de imagens e vídeos é permitida apenas por meio do sistema de E-mail da Companhia ou rede da Companhia.

5.0 SEGURANÇA EXTERNA DE DADOS

Usuários de Dados são responsáveis por proteger todos os dados da Companhia enviados para fora da rede da Companhia. Antes de os dados serem enviados, Usuários de Dados devem tomar determinadas precauções para garantir que os dados da Companhia sejam adequadamente protegidos e não sejam utilizados indevidamente.

5.1 Transmissões FTP / Internet

Dados Confidenciais (vide seção 3.0 e Anexo I) devem ser adequadamente protegidos ao quando transmitidos a partes externas. O Usuário de Dados deve tomar as seguintes precauções ao transmitir ou compartilhar Dados Confidenciais da Companhia com partes externas.

- O uso de sites FTP externos deve ser adequadamente protegido.
    - Sites protegidos utilizam https:// em seus endereços.
    - O site precisa de um ID de usuário e senha para acessar a página onde os dados podem ser armazenados.
- Sites FTP hospedados internamente que contêm Dados Confidenciais devem ser registrados com o Oficial de Segurança da Informação.
    - Permissões de acesso de usuário a sites FTP contendo Dados Confidenciais devem ser analisadas periodicamente pelo Proprietário de Dados.
- As exigências de Segurança de Fornecedores (seção 6.0) detalhadas abaixo devem ser seguidas.

5.2 Armazenamento em Nuvem

Armazenamento em nuvem é um modelo de serviço no qual dados são mantidos, gerenciados e passam por backup remotamente e são disponibilizados a usuários por uma rede, como a Internet. O uso de Armazenamento em Nuvem não aprovado hospedado na internet por um terceiro, como DropBox, Google Drive e iCloud Drive, é estritamente proibido para quaisquer e todos os dados da Companhia a menos que consentimento explícito por escrito seja obtido do Oficial de Segurança da Informação.

Observação: Armazenamento em Nuvem não inclui prestadores de serviço terceiros que utilizam aplicativos baseados em nuvem para processar e armazenar dados da Companhia, como ADP, LRN Treinamento Online e Microsoft Office365. Esses são considerados “Aplicativos Hospedados Externamente” e eles são abrangidos na seção a seguir.

5.3 Aplicativos Hospedados Externamente

Aplicativos hospedados externamente também são referidos como Software como Serviço (SaaS), que é um modelo de distribuição de software no qual aplicativos são hospedados por um fornecedor ou prestador de serviço e disponibilizados a clientes por uma rede, tipicamente a Internet. Prestadores de SaaS comumente conhecidos utilizados pela Viskase incluem Concur, Egencia e UltiPro.

O uso de um aplicativo hospedado externamente exige consentimento explícito por escrito do Oficial de Segurança da Informação, consentimento esse que será retido em um local central. Assim que estiver em serviço, o Proprietário de Dados é responsável pelo seguinte:

- Obter e analisar o relatório SOC1 mais recente (também conhecido como SSAE18) (anteriormente conhecido como relatório SAS70 ou SSAE16) ou relatório semelhante, como um relatório ISAE 3402, anualmente para determinar o seguinte:
    - Os endereços de relatório e serviços utilizados pela Viskase
    - Se o parecer do auditor não é qualificado.
    - Implementar considerações de controle de usuário detalhadas no relatório.
    - Caso um relatório SOC1 não estiver disponível, o Oficial de Segurança da Informação deve ser consultado para obter aconselhamento.
- Analisar periodicamente permissões de acesso de usuários ao aplicativo no mínimo uma vez a cada 6 meses.

6.0 SEGURANÇA DE FORNECEDORES

6.1 Contrato de Confidencialidade

Usuários poderão ocasionalmente enviar Dados Confidenciais a terceiros e a outras partes. Antes desses dados serem enviados, o remetente é responsável por garantir que o fornecedor/terceiro possua um Contrato de Confidencialidade (NDA) em vigor no momento da transmissão.

Um banco de dados de confidencialidade será mantido pelo Administrador de Dados para facilitar a administração dessa política.

6.2 Projetos de Engenharia

Fornecedores poderão ser utilizados na criação de desenho de partes e máquinas. Qualquer contrato para serviços de engenharia deve incluir uma exigência dizendo que a Viskase manterá a titularidade de quaisquer desenhos e projetos criados pelo fornecedor externo em nome da Viskase.

7.0 SEGURANÇA FÍSICA

7.1 Documentos Impressos

Documentos em papel que contêm Dados Confidenciais devem ser armazenados em armários trancados quando não estejam sendo utilizados.

Quando Dados Confidenciais não forem mais necessários e não for exigido por lei que eles sejam retidos, o documento deve ser triturado utilizando um dispositivo aprovado pela Companhia antes de ser descartado; ou destruído por terceiro aprovada pela Companhia (vide Anexo I).

Usuários de Dados não devem levar nenhum documento, periódico, nota ou qualquer outro documento em cópia impressa que contenha Dados Confidenciais com eles quando saírem da Companhia, já que esses documentos são considerados propriedade da Companhia. Documentos impressos em cópia impressa devem ser entregues ao supervisor do Usuário de Dados mediante saída para destruição adequada.

7.2 Dispositivos e Mídia de Armazenamento Eletrônico

Dados da Companhia, quando salvos eletronicamente, residem em um dispositivo de armazenamento eletrônico físico, como uma unidade de disco, pendrive, computador/notebook, CD, disquete, microficha, etc. Usuários são responsáveis pela proteção de todos os dispositivos de armazenamento eletrônico físico.

Ao manusear dispositivos físicos que contenham Dados Confidenciais, os dispositivos devem estar em sua posse a todos os momentos; de outro modo, eles devem ser armazenados em local seguro (ex. sala trancada, ficheiro trancado, etc.) ao qual apenas indivíduos especificamente aprovados tenham acesso por meio de tranca e chave.

Quando Dados Confidenciais não forem mais necessários e não for exigido por lei que eles sejam retidos, as informações no dispositivo devem ser excluídas. Caso um dispositivo que contenha ou tenha contido Dados Confidenciais não for mais necessário, ou mediante saída do Usuário de Dados da Companhia, ele deve ser entregue ao pessoal de suporte ao Departamento de Tecnologia da Informação para a permanente remoção ou anonimização de dados pessoais, ou para a destruição apropriada do dispositivo..

7.3 Transporte de Documentos, Dispositivos e Mídia

O transporte físico de documentos, dispositivos e/ou mídia eletrônicos que contenham Dados Confidenciais deve ser feito apenas por meio de um método de entrega protegido e rastreável autorizado pela Companhia, como serviço de mensageiro, serviço de retenção de documento e Federal Express.

8.0 CUMPRIMENTO

O Oficial de Segurança da Informação investigará violações suspeitas e poderá recomendar ações disciplinares em conformidade com os códigos de conduta da Companhia, políticas, acordos coletivos ou leis aplicáveis. Sanções podem incluir uma ou mais das seguintes:

- Encerramento temporário ou permanente do acesso aos sistemas da Companhia e recursos eletrônicos;

- Ação disciplinar, podendo acarretar a rescisão do contrato de trabalho de acordo com as políticas locais de recursos humanos e/ou acordos coletivos;
- Penalidades civis ou criminais determinadas pelo juízo competente; ou
- Qualquer combinação das anteriores.

9.0 RELATO DE VIOLAÇÕES

Relatar suspeita de violações dessa política em seu escritório local, seguindo os procedimentos de denúncia, se aplicáveis. Violações graves devem ser levadas ao Oficial de Segurança da Informação e ao Diretor de Conformidade. Relatórios de violações são considerados dados "Confidenciais" até que sejam classificados de outro modo.

10.0 CONTATOS

Diretor de Conformidade – Douglas Ochab
Diretor Financeiro – Michael Blecic
Administrador de Dados – Kathy Garrett
V.P. e Diretor de Pessoas – Jeff Bowen
Conselheiro Geral – Michael Schenker
Oficial de Segurança da Informação – Dominic Cesario

APÊNDICE 1: MATRIZ DE CLASSIFICAÇÃO DE DADOS

	Dados Confidenciais (maior, mais sensível)	**Apenas Para Uso Interno (nível moderado de sensibilidade)**	**Dados Públicos (baixo nível de sensibilidade)**
Descrição	Informações comerciais sensíveis que são destinadas a uso estritamente dentro da organização. Sua divulgação não autorizada poderia impactar de forma séria e adversa a organização, seus colaboradores e seus parceiros de negócios.	Dados cujos proprietários de dados decidiram não publicar ou tornar públicos. Não se espera que a divulgação, modificação ou destruição não autorizadas dessas informações impacte de forma séria ou adversa a organização, seus colaboradores ou parceiros comerciais.	Dados para os quais não há expectativa de privacidade ou confidencialidade. Informações que se encontram disponíveis ao público geral e são destinadas a distribuição fora da organização.
Exigências Legais	Proteção de dados é exigida por lei ou pela política da Companhia.	Proteção de dados a critério do proprietário ou depositário.	Não há requerimento legal ou da Companhia para proteção dos dados.
Risco de Reputação	Alto	Médio	Baixo
Acesso e Controle de Dados	Restrições legais, éticas, ou outras restrições impedem acesso sem autorização específica. Dados são acessíveis apenas para aqueles indivíduos designados com acesso aprovado e contratos de confidencialidade assinados.	Podem ser acessados por colaboradores e não colaboradores que possuírem "necessidade de saber" comercial.	Não há restrições de acesso. Dados encontram-se disponíveis para acesso público.

	Dados Confidenciais (maior, mais sensível)	**Apenas Para Uso Interno (nível moderado de sensibilidade)**	**Dados Públicos (baixo nível de sensibilidade)**
Transmissão	Transmissão de Dados Confidenciais por mensagem de texto, FAX ou Pager é proibida. Transmissões por meio de um sistema de E-mail operado pela Companhia são permitidas, mas medidas de segurança adicionais são necessárias. Transmissões para partes externas exigem um Contrato de Confidencialidade e um modo de transmissão protegido.	Transmissão de dados Apenas Para Uso Interno por mensagem de texto, FAX ou Pager deve ser evitada. Transmissões por meio de um sistema de E-mail operado pela Companhia são permitidas.	Nenhuma outra proteção é necessária para informações públicas; no entanto, cuidado sempre deve ser tomado para utilizar todas as informações da Companhia adequadamente.
Armazenamento	Armazenamento de dados eletrônicos Confidenciais deve sempre ser feito em locais aprovados, como em pastas protegidas ou servidores internos da Companhia. Armazenamento em mídia removível não é permitido, exceto em situações de emergência, e os dados devem ser excluídos da mídia assim que a emergência for resolvida. Documentos físicos que contenham Dados Confidenciais devem ser armazenados em um armário quando não estiver em uso.	Armazenamento de dados eletrônicos Apenas Para Uso Interno deve ser feito em locais protegidos, como pastas protegidas ou servidores internos da Companhia. Armazenamento em mídia removível não é permitido, exceto em situações de emergência e Dados de Uso Interno, e os dados devem ser excluídos da mídia assim que a emergência for resolvida. Caso o nível de proteção apropriado não for conhecido, verifique com o Oficial de Segurança da Informação para obter orientações.	Nenhuma proteção específica é necessária para dados públicos; exceto que cuidado sempre deve ser tomado ao usar e armazenar informações da Companhia.

	Dados Confidenciais (maior, mais sensível)	**Apenas Para Uso Interno (nível moderado de sensibilidade)**	**Dados Públicos (baixo nível de sensibilidade)**
Backup Documentado e Procedimentos de Recuperação	Backup Documentado e Procedimentos de Recuperação são necessários.	Backup Documentado e Procedimentos de Recuperação não são necessários, mas são fortemente recomendados.	Backup Documentado e Procedimentos de Recuperação não são necessários, mas são recomendados.
Política de Retenção de Dados Documentada	Política de Retenção de Dados Documentada é necessária.	Política de Retenção de Dados Documentada é necessária.	Política de Retenção de Dados Documentada não é necessária, mas é fortemente recomendada
Destruição / Descarte	Documentos em cópia impressa devem ser triturados por fornecedores ou dispositivos aprovados. Mídia eletrônica deverá ser devolvida ao pessoal de suporte de TI para descarte. Dados eletrônicos deverão ser apagados e mídia magnética deve ser desmagnetizada.	Documentos em cópia impressa deverão ser triturados. Mídia e dados eletrônicos deverão ser apagados.	Documentos em cópia impressa podem ser reciclados ou colocados no lixo. Mídia e dados eletrônicos devem ser apagados.
Controles de Auditoria	Proprietários de Dados responsáveis por Dados Confidenciais devem monitorar e analisar periodicamente relatórios de atividade do sistema e de permissão de	Proprietários de Dados responsáveis por dados Apenas Para Uso Interno devem monitorar e analisar periodicamente relatórios de atividade do sistema quanto	Nenhum controle de auditoria é necessário.

	Dados Confidenciais (maior, mais sensível)	Apenas Para Uso Interno (nível moderado de sensibilidade)	Dados Públicos (baixo nível de sensibilidade)
	usuário quanto a potencial uso indevido e/ou acesso não autorizado.	a potencial uso indevido e/ou acesso não autorizado.	
Exemplos de Dados (não inclui todos, e não necessariamente todos os dados são elementos processados pela Viskase)	**Dados Comerciais/Financeiros** • Arquivos de contabilidade (faturas A/P, pagamentos de contratada) • Relatórios analíticos • Números de conta bancária • Despesas CapEx • Números de cartão de crédito com/sem datas de validade • Informações de clientes • Dados de receita – antes da liberação • Informações Financeiras • Atividade M&A • Informações de salário para cálculos de orçamentos e bônus • Planos Estratégicos – nível corporativo • Números de Previdência Social **Dados de Engenharia / Manutenção** • Programas de Controle • Desenhos - Classe III e IV • Desenhos – Bicos, Rolos de Coleta • Esquemas de controle de máquina • Especificações de máquina • Imagens de máquinas • Manuais de manutenção de treinamento - máquinas de coleta	**Dados Comerciais/Financeiros/Engenharia** • Dados não inclusos na lista de Dados Confidenciais ou Públicos, como: • Desenhos de engenharia – Classe I e II • Demonstrativos Financeiros - assim que receitas forem liberadas • Memorandos que não contenham informações confidenciais • Diretrizes • Informações sobre quadros de anúncio internos • Avisos internos de vagas de trabalho • Páginas da web da intranet • Material de marketing ainda não aprovado para liberação • Procedimentos operacionais • Políticas não confidenciais • Acordos de nível de serviço • Materiais de treinamento (não pertencentes à manutenção • Instruções de trabalho **Dados de Colaborador**	**Dados Comerciais** • Anúncios • Relatórios anuais assim que publicados • Brochuras • Catálogos • Locais da Companhia • Postagens de Trabalho • Páginas da web da intranet • Dados de marketing – aprovados para liberação • Comunicados de Imprensa

	Dados Confidenciais (maior, mais sensível)	Apenas Para Uso Interno (nível moderado de sensibilidade)	Dados Públicos (baixo nível de sensibilidade)
	• Componentes vitais **Laboratório de Alimentos** • Padrões de Produto • Procedimentos laboratoriais e de produção **Jurídico** • Pareceres de advogados sobre patentes • Contratos de confidencialidade • Documento rotulado "Privilegiado por Advogado e Confidencial" • Propriedade Intelectual (patentes e marcas registradas) • Memorandos de estratégia de litígio **Operações / Saúde e Segurança / VEP** • Documentos de Negociação Trabalhista • Detalhes de resíduos, produção e produtividade • Dados de Gerenciamento de Projeto • Relatórios de Segurança com PII	• Manuais de política interna. **Dados de Registro/Sistemas** • Registros de Evento de Servidor, não contendo ID/nome de usuário.	

	Dados Confidenciais (maior, mais sensível)	Apenas Para Uso Interno (nível moderado de sensibilidade)	Dados Públicos (baixo nível de sensibilidade)
	Compras / Logística • Informações de entrada / saída de carga / informações aduaneiras • Arquivos de logística (envios de transporte) • Fixação de Preço - matéria-prima • Pedidos de compra • Arquivos de Compra / licitações fechadas • Acordos de Fornecedor • Contratos de Fornecedor • Avaliações de Fornecedor **Qualidade** • Autorização de Envio Não Padrão Aprovada (ANSSA) • Aviso de Mudança de Engenharia (ECN) • Procedimentos Laboratoriais e de Embalagem • Normas e Procedimentos de Matérias-Primas e SF/Acabados • Solicitações de Execução Especial (SRR) **P&D** • Relatórios analíticos • Desenhos de desenvolvimento • Resultados de teste de FSI		

	Dados Confidenciais (maior, mais sensível)	Apenas Para Uso Interno (nível moderado de sensibilidade)	Dados Públicos (baixo nível de sensibilidade)
	• Patentes • Processos de produção • Projeto de rolo de coleta **Vendas** • Exceções de Preço de Clientes • Relatórios de Teste de Produto • Registros de Serviço de Tecnologia **Dados Pessoais.** Nota: Os seguintes dados são exemplos de dados pessoais, mas não necessariamente são dados processos pela Viskase. Informações relacionadas a pessoas naturais identificadas ou identificáveis, tais como: • Nome, sobrenome ou iniciais com qualquer um dos seguintes. • Título • Fotografia • Nacionalidade • Local de Nascimento • Telefone comercial • E-mail comercial • Informação de contato designada pelo proprietário como pessoal • Instituição de ensino • Gênero • Endereço • Data de Nascimento / Idade • Data de contratação		

	Dados Confidenciais (maior, mais sensível)	Apenas Para Uso Interno (nível moderado de sensibilidade)	Dados Públicos (baixo nível de sensibilidade)
	• Número de telefone residencial • Nº de carteira de habilitação • Nº de passaporte • Nº de Previdência Social / Nº de identificação nacional • Nº de identificação do Estado / Nº CURB • Invalidez • Classificação de crédito • Dados de localização • Dados financeiros (conta corrente, poupança, corretagem, CD, 401(k), etc.) • Número do cartão de crédito ou débito • Logs de servidor contendo nome/ID do usuário • Filiação ao sindicato **Dados de Colaborador** • Seleções de Benefícios • Ações Disciplinares • Análises de Desempenho • Reivindicações de invalidez ou Compensação do Trabalhador • Informações de saúde • Status de saúde • Pagamento de tratamento de saúde • Tratamento de saúde • Etnia/Raça* • Identidade sexual* • Biometria/Dados genéticos*		

	Dados Confidenciais (maior, mais sensível)	Apenas Para Uso Interno (nível moderado de sensibilidade)	Dados Públicos (baixo nível de sensibilidade)
	• Tipo sanguíneo* • Afiliação religiosa* • Afiliação política* • Registros criminais* *Dados considerados como sensíveis ou categorias especiais de dados pessoais e restrições especiais para o seu processamento, de acordo com as leis aplicáveis de proteção de dados.		