<table>
<tr><td rowspan="2">  </td><td colspan="2">POLÍTICA</td></tr>
<tr><td colspan="2">Título: Regulamento Interno de Utilização dos Recursos de Informática</td></tr>
<tr><td rowspan="2"></td><td colspan="2">Objetivo: Estabelecer as regras de utilização dos recursos de informática do Grupo Halex Istar por todos os seus Colaboradores e Terceiros.</td></tr>
<tr><td>Nº.: 9</td><td>Versão: 01</td><td>Supervisão: Comitê de Auditoria, Compliance e Finanças</td></tr>
<tr><td>Revisor:</td><td>Cargo: [•]</td><td rowspan="2">Data de vigência: [•]</td></tr>
<tr><td>Aprovador: [•]</td><td>Cargo: [•]</td></tr>
</table>

REGULAMENTO INTERNO
DE UTILIZAÇÃO DOS RECURSOS DE INFORMÁTICA
DO GRUPO HALEX ISTAR

ÍNDICE:

CAPÍTULO I - ESCOPO DE ATUAÇÃO

Artigo 1º O presente Regulamento de Utilização dos Recursos de Informática ("Regulamento") estabelece as regras de utilização e preservação de todos os recursos de informática do Grupo Halex Istar pelos seus Colaboradores, Terceiros e eventuais visitantes que venham a se utilizar de qualquer recurso ou serviço disponibilizado pelo Departamento de Tecnologia da Informação.

Artigo 2º Este Regulamento é aplicável a todos os Colaboradores do Grupo, independentemente do seu nível hierárquico, da função e do cargo exercidos e da localidade que se encontram.

Parágrafo único. Todos os Colaboradores devem, quando da sua efetivação, tomar a devida ciência deste Regulamento e obrigatoriamente preencher o Termo de Adesão ao Regulamento, Anexo II deste Regulamento, antes de receber ou ter qualquer contato com quaisquer recursos de informática do Grupo.

Artigo 3º Caso as disposições da legislação local, em qualquer local em que o Grupo desenvolva suas atividades, sejam mais restritivas que as disposições deste Regulamento, serão aplicáveis as disposições da legislação mais restritiva.

Artigo 4º Este Regulamento será supervisionado, implementado e aplicado pelo Departamento de Tecnologia da Informação e pela área responsável por *Compliance.*

CAPÍTULO II - DEFINIÇÕES

Artigo 5º Para fins deste Regulamento, são adotadas as seguintes definições técnicas descritas a seguir:

a) *Hardware:* Equipamento de Informática (tal como um PC, laptop, smartphone, tablets ou qualquer outro equipamento informático) ou conjunto de componentes físicos de um equipamento ou seus periféricos, peças e outros elementos físicos de informática;

b) *Software:* Conjunto dos componentes que não fazem parte do equipamento físico propriamente dito e que incluem as instruções em forma de linguagem de programação, bem como os dados e códigos a eles associados, empregados durante a utilização do sistema (programa de computador);

c) *Internet*: Conjunto de computadores interligados em uma rede de abrangência mundial, que se comunicam utilizando o protocolo TCP/IP;

d) *Intranet*: Conjunto de computadores e outros equipamentos de uma instituição, que formam uma rede utilizando o protocolo TCP/IP e são ligados à Internet usualmente através de um sistema de proteção (*Firewall*);

e) *Extranet*: Conjunto de mecanismos capazes de prover níveis específicos de acesso a dados e sistemas pertencentes à intranet de uma determinada instituição a pessoas que estejam acessando estes sistemas a partir da *Intranet*;

f) Correio eletrônico (*e-mail*): Serviço que possibilita a troca assíncrona e ubíqua de mensagens através de recursos da Internet;

g) Página da Internet (*site)*: Conjunto de documentos apresentados ou disponibilizados na rede mundial (*web*) por um indivíduo, empresa ou instituição, que pode ser acessado em um endereço específico da rede Internet, através de uma URL (*Uniform Resource Locator*), podendo ser subdividido em páginas com endereços específicos e próprios;

h) Bancos de dados: Quaisquer arquivos estruturados de dados, acessíveis segundo determinados critérios, que sejam centralizados, descentralizados ou distribuídos de modo funcional ou geográfico;

i) Suporte: Assessoria prestada por pessoal especializado visando solucionar problemas e imperfeições em sistemas e equipamentos de informática;

j) Documentos Digitais: Documentos que exprimem um fato ou uma vontade, por meio de representação aceitável em computador e um software específico;

k) Certificação digital: Conjunto de técnicas criptográficas, que permitem verificar a autenticidade, autoria e integridade de um documento em formato digital;

l) *Download*: Obtenção de cópia, em máquina local, de um arquivo originalmente armazenado em máquina remota, *links*, Anti Virus, Cyber ataque, *pen drive* ou em rede;

m) Antivírus: Software que detecta, impede e atua na remoção de programas de software maliciosos. São programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, a fim de dar mais segurança ao usuário;

n) *Link*: Palavra, texto ou imagem que quando é clicada pelo usuário, o encaminha para outra página de internet, que pode conter outros textos ou imagens;

o) *Pen Drive*: Dispositivo de armazenamento constituído de memória flash, capaz de fazer a gravação de dados através de uma ligação USB; e

p) Cyber ataque: Ataque efetuado geralmente através da internet, no qual são violados sistemas informáticos, com o objetivo de espiar, provocar danos, roubar dados, etc.

CAPÍTULO III - UTILIZAÇÃO DE COMPONENTES FÍSICOS (HARDWARE)

Artigo 6º Integram o patrimônio físico de informática do Grupo:

a) Os equipamentos de informática, incluindo microcomputadores, PCs, smartphones, laptops, tablets, servidores, periféricos e afins, adquiridos e/ou utilizados por meio de comodato pelo Grupo; e

b) O conjunto de equipamentos necessários para a manutenção daqueles já existentes, incluindo peças, periféricos e outros elementos físicos de informática.

Artigo 7º Somente será permitida a adição ou substituição de peças, periféricos e outros elementos físicos de informática, em equipamentos que integrem o patrimônio físico de informática do Grupo, em casos previamente autorizados pelo Departamento de Tecnologia da Informação, segundo padrões previamente determinados pela Diretoria e o Departamento de Tecnologia da Informação.

Artigo 8º A adição e/ou substituição não autorizada de peças, periféricos, outros elementos físicos de informática, bem como de equipamentos do Grupo, podem implicar em adulteração do patrimônio, de forma que o Grupo eventualmente possa propor a adoção de medidas disciplinares assim previstas na legislação vigente, bem como a responsabilização de danos causados, se houver.

Artigo 9º A distribuição de equipamentos físicos deve observar as necessidades estabelecidas pelo Grupo, dentro de critérios objetivos previamente aprovados pela Diretoria e o Departamento de Tecnologia da Informação.

Artigo 10 A utilização de equipamentos físicos, tais como *pen drives, tablets*, câmeras e/ou qualquer tecnologia USB e afins, deve observar as necessidades estabelecidas pelo Grupo, dentro de critérios previamente aprovados pela Diretoria e o Departamento de Tecnologia da Informação. A utilização não autorizada de tais equipamentos em rede e/ou equipamento do Grupo pode implicar na adoção de medidas disciplinares assim previstas na legislação vigente, e normas internas, bem como a responsabilização de eventuais danos causados, se houver.

Parágrafo único. É vedado o acesso interno à rede própria do Grupo de equipamentos de cunho particular, tais como computadores, *notebooks, pendrives, iPod's, MP3 players, MP4 players,* câmeras e quaisquer outros equipamentos com tecnologia USB, *bluetooth*, infravermelho e/ou outra tecnologia utilizada para transferência de arquivos, sem prévia autorização do Departamento de Tecnologia da Informação, ficando o usuário infrator sujeito a medidas disciplinares assim previstas na legislação vigente.

CAPÍTULO IV - UTILIZAÇÃO DE EQUIPAMENTOS E SISTEMAS QUE NÃO SEJAM FÍSICOS (SOFTWARE)

Artigo 11 Integram o patrimônio de informática do Grupo:

a) As licenças de uso de aplicativos e softwares adquiridos; e

b) Os sistemas aplicativos e respectivos códigos fontes desenvolvidos ou adquiridos como ferramenta para atender às finalidades específicas.

Parágrafo único. As condições de uso e de instalação de aplicativos originalmente estabelecidas por seus fabricantes devem ser rigorosamente observadas, em todos os casos.

Artigo 12 O Grupo pode adotar o uso de softwares chamados "livres" em quaisquer áreas, designados àqueles que possuem o código fonte aberto e cujo uso não enseja o pagamento de licenças de uso, observadas as condições estabelecidas para sua disponibilização e tão somente segundo o padrão definido pelo Departamento de Tecnologia da Informação.

Artigo 13 Compõem o conjunto básico de aplicativos de cada máquina do Grupo:

a) Um sistema operacional de uso difundido;

b) Um navegador para uso na Internet;

c) Um aplicativo de correio eletrônico;

d) Um processador de texto;

e) Uma planilha eletrônica de cálculos;

f) Um sistema de detecção e eliminação de vírus de computador;

g) Uma ou mais ferramentas de detecção e eliminação de outras pragas virtuais;

h) Uma ou mais ferramentas de manutenção do sistema operacional e aplicativos instalados.

§1º Outros aplicativos podem ser instalados em cada máquina, dependendo da necessidade específica do usuário, em casos devidamente autorizados pelo Departamento de Tecnologia da Informação.

§ 2º É vedada a instalação de aplicativos não autorizados pelo Departamento de Tecnologia da Informação, mesmo que o usuário possua licença para sua instalação, sendo o mesmo responsável por observar as normas atinentes previstas neste Regulamento.

§3º É vedada a inserção, em qualquer meio de armazenamento, de arquivos de conteúdo não relacionados às atividades funcionais dos Colaboradores, salvo em casos previamente autorizados pelo Departamento de Tecnologia da Informação.

§ 4º Os aplicativos e conteúdos instalados em máquinas de propriedade do Grupo são passíveis de verificação a qualquer tempo e sem necessidade de ciência ou anuência prévia do usuário, caso tal verificação seja julgada como necessária pela Administração do Grupo, por qualquer motivo, conforme previsto no Artigo 52 deste Regulamento.

CAPÍTULO V - UTILIZAÇÃO DOS SISTEMAS DE REDE

Artigo 14 O Grupo deve desenvolver e aperfeiçoar um sistema de integração, por rede de todas as suas máquinas, propiciando a integração e a comunicação de todos em um ambiente único e de comum acesso.

Parágrafo único O Departamento de Tecnologia da Informação deve proporcionar o acesso ao sistema de rede mediante senha pessoal e intransferível, sendo o usuário responsável pela utilização e guarda desta informação.

Artigo 15 É responsabilidade do Departamento de Tecnologia da Informação determinar a política e indicar os responsáveis pela execução e restauração das cópias de segurança (backup) dos meios de armazenamento compartilhados em rede.

Parágrafo único A cópia de segurança e restauração de informações armazenadas em dispositivos locais de acesso exclusivo é de responsabilidade dos seus respectivos usuários.

Artigo 16 O sistema de rede única deve permitir a plena comunicação entre seus integrantes, e de seus integrantes com a rede Internet, nos moldes estabelecidos neste capítulo.

Artigo 17 A utilização de *login* de acesso a sistemas, redes e/ou qualquer outro tipo de recurso computacional do Grupo deve ser exclusivo para cada usuário. É absolutamente vedado qualquer tipo de compartilhamento de acesso e senhas entre usuários, sendo se houver a violação destas regras, estas serão tratadas conforme as leis em vigor e normas internas, estabelecidas pelo RH e pelo Código de Conduta e Ética.

Artigo 18 A senha inicial do domínio deve ser definida pelo Departamento de Tecnologia da Informação, sendo obrigatória a alteração no primeiro acesso do usuário. A nova senha deve satisfazer os requisitos de complexidade e de comprimento mínimo de 6 caracteres e ainda conter 1 caractere especial, não podendo repetir as últimas 5 senhas utilizadas. O prazo de validade de cada senha não pode passar de 60 dias.

Parágrafo único. Não devem ser cadastradas senhas que façam analogia ao próprio nome, sequências numéricas lógicas (ex. 123456) e/ou palavras e expressões de cunho popular.

Artigo 19 Cabe ao Departamento de Tecnologia da Informação certificar, através do POP 6108, e mediante o nome completo do solicitante, a existência de uma conta de *logon* no *Active Directory*, no intuito de evitar duplicidade na criação de usuários.

Artigo 20 Caso haja a tentativa incorreta de *logon* por 3 vezes consecutivas por parte de um usuário, o acesso deste usuário deve ser bloqueado temporariamente. A solicitação de desbloqueio deve ser feita pelo seu superior ou encarregado imediato, através de abertura de solicitação ao Departamento de Tecnologia da Informação via e-mail (ticket).

- **DIREITO DE ACESSO**

Artigo 21 Os direitos de acesso ao domínio dos usuários da rede corporativa são concedidos, mantidos e/ou revogados diretamente no *Active Directory* e em cada sistema que o Colaborador irá utilizar.

Parágrafo único. A revisão aos direitos de acesso é realizada uma vez por ano, normalmente em novembro.

- **CONCESSÃO DE DIREITOS DE ACESSO**

Artigo 22 O usuário faz a solicitação de direito de acesso a uma ou mais unidades de acesso por e-mail ao time de suporte de TI e ao gestor, para aprovação.

§ 1º Se aprovada, a solicitação é encaminhada para o setor de atendimento do Suporte. Este setor analisa e, se necessário, transforma a solicitação para que esta represente a real necessidade do usuário.

§ 2º Em seguida, a solicitação é encaminhada, através de e-mail, para a aprovação do responsável pela unidade de acesso.

§ 3º Uma vez aprovada, a solicitação é encaminhada por e-mail para as áreas responsáveis pela sua execução, que irão conceder o acesso solicitado, conforme autorizado.

§ 4º Todo usuário criado deverá conter um identificador único.

- **COLABORADORES ADMITIDOS**

Artigo 23 Durante o processo de admissão e contratação de um novo colaborador a área de Recursos Humanos será responsável pelo envio de um comunicado, com uma semana de antecedência ao início deste, informando ao Departamento de Tecnologia da Informação, que entrará em contato com o responsável da área solicitante da contratação que definirá os necessários direitos de acesso que deverão ser concedidos ao funcionário para que ele possa exercer suas funções em adequação ao seu perfil. Este processo é executado através do *Active Directory*.

§ 1º Quando da transferência de colaboradores, o gestor da área informará ao Departamento de Tecnologia da Informação, para que sejam providenciadas as necessárias alterações do perfil de acesso do usuário. Este processo é executado através do *Active Directory*.

§ 2º O responsável pelo suporte do Departamento de Tecnologia da Informação realizará um levantamento de todos os recursos de informática utilizados pelo usuário na sua área de origem e informará às gerências de origem e destino do funcionário.

§ 3º As gerências das áreas de origem e destino do funcionário em transferência deverão estabelecer, quais direitos de acesso deverão ser revogados, quais serão mantidos e quais deverão ser criados para que o funcionário possa executar suas novas funções.

§ 4º Se for necessário um período de transição, durante o qual antigos direitos de acesso precisem ser mantidos, tais direitos, bem como a duração do período de transição, devem ser especificados pelas gerências envolvidas. Após o término do período de transição os direitos de acesso serão sumariamente revogados também pelo *Active Directory.*

- **COLABORADORES DESLIGADOS**

Artigo 24 No caso de desligamento de colaborador, a área de Recursos Humanos fornecerá ao Colaborador desligado o "Termo de Desligamento", contendo toda a formalização do processo de desligamento que deverá ser apresentado ao responsável pelo Departamento de Tecnologia da Informação para desativar o seu acesso à rede e ao correio eletrônico para revogação dos direitos deste funcionário, que deve ocorrer em até 24 horas da ocorrência do desligamento.

- **DESENVOLVIMENTO DE SISTEMAS**

Artigo 25 A concessão de direitos de acesso aos responsáveis pelo desenvolvimento de sistemas (terceiros contratados pelo Grupo Halex Istar) será procedida através do *Active Directory* aprovado pelo Departamento de Tecnologia da Informação.

- **GERENCIAMENTO DE MUDANÇAS**

Artigo 26 Deve ser estabelecido um processo de Gestão de Mudanças para alterações em Sistemas de Informação, Sistemas Operacionais e Infraestrutura que garanta os seguintes requerimentos:

a) Definir papéis e responsabilidades adequadas ao processo, respeitando sempre a segregação de tarefas conflitantes entre diferentes recursos;

b) Revisão dos requerimentos de segurança e análise de capacidade dos ambientes;

c) Identificação dos riscos associados à tarefa;

d) Controle do processo através de Submissão/ Aprovação;

e) Separação dos arquivos de código com versão adequada para instalação;

f) Teste das mudanças com geração de evidências;

g) Documentação dos procedimentos necessários para desfazer a mudança em caso de problemas não previstos;

h) Disparo de possíveis ajustes necessários ao Plano de Continuidade de Negócio;

i) Documentação e pós-aprovação de todas as atividades que foram executadas em caráter de emergência;

j) Obrigação de atualização da documentação, caso exista, dos sistemas envolvidos.

§ 1º Em todas as operações envolvidas na fabricação de medicamentos, incluindo os medicamentos em desenvolvimento destinados a ensaios clínicos, deverá ser observada a Resolução da Diretoria Colegiada da ANVISA nº17, de abril de 2010, (RDC17) para gerir, aprovar e executar mudanças.

- **GERENCIAMENTO DE RISCOS DE FORNECEDORES DE TECNOLOGIAS**

Artigo 27 Será efetuada análise prévia de novas tecnologias, serviços e produtos antes de sua contratação, com o objetivo de identificar vulnerabilidade e se os fornecedores atuam de acordo com o previsto nas políticas do Grupo, sendo classificado seu risco e avaliada sua contratação ou não.

Parágrafo único. Tal análise deverá constar no documento de aprovação a ser enviado ao departamento Jurídico para elaboração ou avaliação de contrato.

- **ESTAÇÕES DE TRABALHO**

Artigo 28 As estações de trabalho devem ser protegidas através de protetores de tela ("screen savers") os quais somente permitem o acesso mediante digitação da senha de acesso.

§ 1º Após até 15 minutos de ociosidade, a tela será bloqueada. Esta regra será aplicada por GPO para todos os usuários.

§ 2º As contas de Administrador das estações de trabalho devem ter senha pré-definida, totalmente desconhecida pelos usuários, ficando em posse apenas do time de suporte e do Gestor de TI contratado, e não serão utilizadas pelos usuários. O usuário administrador local só será utilizado em casos especiais que envolvem manutenção no sistema ou na máquina pelo técnico da empresa responsável pelo TI.

§ 3º Sem o conhecimento da conta de Administrador, os usuários das estações terão o acesso à rede apenas com o login individual restrito, entretanto sem privilégios administrativos.

§ 4º O Servidor é dedicado e não necessita de nenhuma ação ou efetuar login local para estar operacional, não é permitido o acesso físico pelos usuários e seu login só pode ser efetuado através de conta de Administrador única, sujeita as mesmas regras descritas neste Regimento. O Acesso ao servidor só poderá ser feito por profissionais do Departamento de Tecnologia da Informação, equipes de infraestrutura e desenvolvimento em caso de manutenções e instalações necessárias.

§ 5º Todas as tentativas de acesso à rede malsucedidas seja de dentro das instalações do Grupo ou através de acesso remoto, são registradas em "log" e alertadas através de diretivas do firewall. Após um número predeterminado de tentativas malsucedidas = 5, a conta do usuário é bloqueada e somente poderá ser desbloqueada após a intervenção de um administrador da rede, que antes de efetuar o desbloqueio analisará o problema ocorrido.

§ 6º O Grupo dispõe de proteção por Firewall, equipamento de prevenção de intrusões que reage de forma automática às tentativas de invasão externas à rede da Companhia, bloqueando o ataque.

§ 7º No Firewall devem ser utilizadas regras de bloqueio a listas pré-estabelecidas de sites impróprios para fins corporativos.

§ 8º O Uso da Internet deve monitorado e se houver qualquer acesso a conteúdo indevido o mesmo deve ser bloqueado após a revisão dos acessos.

§ 9º A administração de liberações e bloqueios é dinâmica e deve ser solicitada sempre através de e-mail ao responsável colaborador de TI e testada pelo solicitante após a execução da mesma.

§ 10º As estações de trabalho e o servidor tem bloqueios de BOOT por qualquer outro dispositivo (USB, CD, etc.) estabelecido na BIOS do equipamento que só poderá ser habilitada mediante a senha conhecida apenas pelo responsável ou pelo colaborador de TI. O Boot só é permitido pelo HD local.

- **INTERNET**

Artigo 29 A Internet pode ser acessada por todos os usuários (Colaboradores), incluindo Terceiros que tenham acesso às dependências do Grupo, devendo ser utilizada prioritariamente para finalidades profissionais e visando o bom andamento das atividades dos Colaboradores. É vedada a utilização de *Chats* (Bate-papo), *softwares* e/ou serviços como *Messenger*, seja via *Web* ou por quaisquer outros tipos de *softwares,* salvo em casos autorizados pela Administração e devidamente implementados nos equipamentos pelo Departamento de Tecnologia da Informação.

Parágrafo único. Para o software *Skype* e/ou outros meios de videoconferência, o seu uso fica restrito à comunicação interna, comunicação profissional como as com representantes, fornecedores e/ou clientes, sendo vedada a utilização deste serviço para fins particulares e/ou para envio/recebimento de arquivos estranhos às atividades profissionais do Colaborador, sujeito o usuário infrator às medidas disciplinares assim previstas na legislação vigente.

Artigo 30 É completamente vedado o acesso por qualquer usuário a sites que contenham:

a) Material atentatório à dignidade e à integridade da pessoa humana;

b) Material pornográfico, de pedofilia e assemelhados;

c) Propaganda de ideologias contrárias ao regime democrático, bem como façam a apologia do uso da violência (ex. Nazismo);

d) Material que faça apologia a atividades criminosas assim previstas no nosso país ou no exterior, bem como venha a ensinar ou facilitar a prática de crimes assim previstos nas legislações brasileiras ou no exterior;

e) Jogos de azar;

f) Exibição de material inconveniente ao ambiente de trabalho e cujo conteúdo cause desconforto ao ser humano médio;

g) Que tragam ao equipamento utilizado e às redes internas códigos maliciosos, artifícios de violação, vírus ou quaisquer outros elementos que possam

vir a alterar ou danificar as redes, os sistemas, os dados registrados e os equipamentos pertencentes à Empresa;

h) Rádios online, filmes, trailers, músicas ou outros conteúdos online de streaming e afins que possam afetar o desempenho geral da rede de dados do Grupo.

§ 1º. O Departamento de Tecnologia da Informação fica autorizado a rastrear, se aplicável, os acessos dos usuários à rede Internet e às páginas acima citadas, seja por meio direto ou por aplicativos específicos, em tempo real ou posteriormente ao uso, nos moldes que entender mais conveniente, mediante autorização expressa da Diretoria, conforme previsto no Artigo 63 deste Regulamento.

§ 2º. O ingresso comprovado a tais sites, pode implicar em procedimento disciplinar contra o usuário e aplicação das sanções legalmente previstas.

Artigo 31 Fica expressamente vedada a prática de *downloads* de arquivos da Internet, independentemente de sua natureza, sendo apenas permitidas àquelas operações previamente autorizadas pelo Departamento de Tecnologia da Informação, para finalidades específicas e preferencialmente de cunho profissional.

Artigo 32 Os usuários de equipamentos utilizados para conexão à Internet devem zelar pela segurança das máquinas utilizadas, sendo de sua responsabilidade a manutenção e atualização de sistemas de detecção de vírus e outros meios danosos aos equipamentos e à rede do Grupo, salvo os casos em que o Departamento de Tecnologia da Informação automatizar esses procedimentos.

- **CORREIO ELETRÔNICO**

Artigo 33 Os Colaboradores que receberem endereço eletrônico profissional (e-mail) próprio disponibilizado pelo Grupo (ex. nome.sobrenome@halexistar.com.br; nome.sobrenome@medicone.com.br; nome.sobrenome@isofarma.com.br) devem utilizar este sistema exclusivamente como meio de receber e enviar comunicações profissionais, com as seguintes características:

a) Informações gerais de interesse profissional;

b) Correspondência entre usuários;

c) Transferência de arquivos, desde que não contaminados por vírus e/ou códigos maliciosos;

d) Envio e recebimento de documentos/informações de interesse profissional.

Artigo 34 Fica expressamente vedado o envio de mensagens pelo sistema de correio eletrônico, entre quaisquer usuários ou mesmo externamente, que contenham:

a) Mensagens ou imagens atentatórias à dignidade e à integridade da pessoa humana;

b) Mensagens ou imagens pornográficas, de pedofilia e assemelhados;

c) Propaganda de qualquer espécie;

d) Material que signifique apologia a atividades criminosas assim previstas no nosso país ou no exterior;

e) Exibição de material inconveniente ao ambiente de trabalho e cujo conteúdo cause desconforto ao ser humano médio;

f) Tragam ao equipamento utilizado e às redes internas códigos maliciosos, artifícios de violação, vírus ou quaisquer outros elementos que possam vir a alterar ou danificar as redes, os sistemas, os dados registrados e os equipamentos pertencentes ao Grupo;

g) "Correntes", "boatos", anedotas e assemelhados;

h) Qualquer tipo de imagens/fotos com extensões tais como: .gif, .jpeg, .jpg, .bmp, .tif, .png e afins sem relação com as atribuições profissionais dos usuários;

i) Lista de destinatários diversos, podendo ser caracterizadas como envio de mensagem em massa (SPAM), salvos os casos em que sejam enviados comunicados internos pelos Departamentos de Comunicação do Grupo ou afins.

Artigo 35 Fica definido como *software* padrão para envio e recebimento de mensagens eletrônicas o *Microsoft Outlook*, ficando vedada a utilização de qualquer outro *software* sem prévia autorização do Departamento de Tecnologia da Informação. Deve ser configurado no *software*, apenas uma conta com senha previamente definida, identificando o usuário por Departamento – Nome, ficando vedada a configuração, bem como a utilização de outras contas de cunho particular.

Parágrafo único. Deve ser configurada pelo Departamento de Tecnologia da Informação uma assinatura padrão, a qual seguirá em cada mensagem eletrônica enviada, ficando vedado ao usuário alterar essa assinatura, salvo em casos previamente autorizados pela Gerência imediata ou Diretor da área, tais como: criação de utilização de assinaturas sazonais em situações como campanhas, feiras e eventos relevantes para o grupo.

- **SITES DAS EMPRESAS DO GRUPO**

Artigo 36 O Grupo mantém um *site* na Internet para cada empresa, com os endereços www.halexistar.com.br, www.medicone.com.br e www.isofarma.com.br, os quais devem conter informações relativas as empresas, suas marcas e produtos, endereços de outros *sites* e tantas outras informações que sejam entendidas como necessárias.

Artigo 37 As páginas do Grupo podem utilizar somente referências gerais de outras páginas externas ao Grupo através de hiperligações (*hyperlinks*), desde que seja mencionado somente o endereço base, sendo vedada a utilização de endereços diretos a páginas secundárias de um site da Internet, salvo prévia autorização do detentor do referido site.

Artigo 38 Colaboradores podem criar sites e/ou perfis profissionais na Internet para fins particulares, desde que não suplantem ou venham a concorrer com produtos e/ou serviços já prestados pelo Grupo. Nenhuma referência pode ser feita ao Grupo sem prévia autorização da Diretoria. Tais desenvolvimentos não poderão ser realizados dentro das dependências do Grupo tampouco no horário de trabalho dedicado ao Grupo.

- **BANCO DE DADOS**

Artigo 39 O Grupo pode instituir quantos bancos de dados entender necessários para o aperfeiçoamento de suas atividades, sendo que os dados ali existentes pertencem ao Grupo.

Artigo 40 Desde que tenham interesse público, e devidamente autorizado, podem ser divulgadas certas informações constantes nos bancos de dados do Grupo, podendo estes dados serem acessados por sistemas de pesquisa, desde que não possibilitem o levantamento de dados pessoais e/ou sensíveis sobre as pessoas e/ou negócios ali referidos.

Artigo 41 Os bancos de dados do Grupo que contiverem dados pessoais e/ou sensíveis devem ser tratados de forma confidencial, sendo que os dados devem ser utilizados para fins que justifiquem sua coleta e de acordo com o consentimento de seus titulares para sua coleta, uso e armazenamento.

Artigo 42 A adulteração interna ou externa de informações armazenadas em bancos de dados, bem como o seu acesso não autorizado por parte de Colaboradores e/ou Terceiros, pode ensejar medidas disciplinares previstas em Lei.

Artigo 43 Cabe exclusivamente ao Departamento de Tecnologia da Informação, ou a quem este previamente delegar poderes para tanto, preservar e restaurar as informações de banco de dados através de backups diários, semanais e mensais em mídias externas (nuvem, fitas, unidades de disco e etc.).

Parágrafo único. Os backups de todas as informações em banco de dados devem ser armazenados por no mínimo 5 (cinco) anos, contados de sua data original.

CAPÍTULO VI - SUPORTE TÉCNICO

Artigo 44 Cabe exclusivamente ao Departamento de Tecnologia da Informação, ou a quem este previamente delegar poderes para tanto, prestar suporte técnico aos usuários quanto ao patrimônio físico (hardware) e dos aplicativos (software) do Grupo.

Artigo 45 O suporte pode somente ser efetuado em equipamentos de propriedade do Grupo, bem como a aplicativos instalados pelo Departamento de Tecnologia da Informação.

Artigo 46 Cabe a cada usuário o uso adequado e a execução de medidas que venham a preservar os equipamentos e os aplicativos do Grupo, bem como zelar pela integridade dos dados e da rede, devendo atualizar os sistemas de detecção e eliminação de vírus e afins, salvo nos casos em que o Departamento de Tecnologia da Informação automatizar esses procedimentos.

Artigo 47 Cabe a cada usuário fazer eventual solicitação de atendimento pelo e-mail helpdesk@halexistar.com.br Nos casos em que ocorra a falta deste recurso, o usuário pode solicitar atendimento pelo telefone do Departamento de Tecnologia da Informação (ramal: 6301). O Departamento de Tecnologia da Informação procederá com os atendimentos segundo a ordem cronológica das chamadas recebidas.

CAPÍTULO VII - DOCUMENTOS DIGITAIS

Artigo 48 São considerados documentos válidos, além daqueles representáveis por meio físico, aqueles que, por meio de representação aceitável em computador e um software específico, exprimirem um fato ou uma vontade.

Parágrafo Único. São considerados documentos válidos também aqueles armazenados no servidor de arquivos, bem como aqueles que sejam de utilização da empresa, vedada a utilização da unidade de armazenamento para fins particulares, cabendo ao Departamento de Tecnologia da Informação excluí-los se necessário.

§1º Fica expressamente vedado o armazenamento de imagens, fotos, filmes e músicas nesta unidade, se não específicos e de interesse do Grupo.

§2º Cabe ao Departamento de Tecnologia da Informação disponibilizar uma área de transferência de arquivos (Documentos Públicos) para troca de arquivos em departamentos e usuários. Sendo área para arquivos temporários, estes serão excluídos perante avaliação em 7 dias.

Artigo 49 O Grupo pode adotar para utilização interna ou externa o uso de documentos digitais criptografados, assim considerados aqueles confirmados por meio de Certificação digital ou tecnologia assemelhada, e que possuem a garantia de autenticidade e integridade.

Artigo 50 Os documentos mencionados no artigo anterior têm plena validade para todos os efeitos legais, dispensando a apresentação de reproduções por meio físico, salvo exigência específica do órgão competente ou impugnação fundamentada de falsidade do meio digital, seja por adulteração voluntária ou involuntária.

Artigo 51 É de responsabilidade da parte remetente qualquer incorreção de dados, atraso ou qualquer motivo impeditivo que não permita que um documento seja corretamente recebido e lido pelo destinatário.

Artigo 52 O Departamento de Tecnologia da Informação deve fornecer aos usuários que venham a necessitar os meios necessários para Certificação digital de documentos, sendo cada código ou senha de atribuição pessoal e intransferível.

Artigo 53 O uso indevido dos meios de certificação de documentos eletrônicos, bem como a obtenção ou adulteração indevida de códigos pessoais ou senhas de terceiros, constitui infração disciplinar grave e, garantida a ampla defesa, pode ensejar penalidades previstas nos regulamentos internos do Grupo, sem prejuízo de demais consequências legais previstas na legislação vigente.

Artigo 54 A geração e a revogação de chaves públicas e privadas para certificações eletrônicas devem ser realizadas pelo Departamento de Tecnologia da Informação, devendo o Departamento de Tecnologia da Informação manter registro fiel da data e o destinatário de tais chaves.

Artigo 55 É vedado a alteração de qualquer parâmetro (data, hora, dll's, arquivos configuração Windows e sistemas) que descaracterize a instalação padrão realizada pelo Departamento de Informática.

- **DISPOSITIVOS MÓVEIS**

Artigo 56 Todo Colaborador do Grupo, 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 no Grupo, mesmo depois de terminado o vínculo contratual mantido com a instituição.

§1º O dispositivo móvel de propriedade do Colaborador pode ser utilizado para fins profissionais utilizando ferramentas como skype, e-mail, etc. Contudo o usuário não podendo acessar o workstation remotamente. Alternativamente, qualquer

Companhia do Grupo pode optar pela concessão de dispositivos móveis aos Colaboradores.

§2º 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 ao Grupo e/ou a terceiros.

- **MONITORAMENTO DA SEGURANÇA**

Artigo 57 Deve ser adotado um Firewall que registra todos os eventos suspeitos relacionados ao acesso à rede corporativa através da Internet e disponibiliza aos administradores um relatório com um resumo das ocorrências por período pré-determinado. De posse deste relatório, os eventos são analisados caso a caso e as devidas providências são tomadas.

§1º Os antivírus têm um mecanismo inteligente e automático sob a forma de quarentena de remoção de vírus ou arquivos suspeitos de infecção, qualquer bloqueio incorreto deve ser solicitado a equipe técnica sob o conhecimento do responsável.

§2º A Administração é remota, qualquer suspeita ou anormalidade no comportamento da máquina deve ser imediatamente comunicada a equipe técnica.

- **CLASSIFICAÇÃO DA INFORMAÇÃO**

Artigo 58 Os níveis de classificação da Informação são:

- **Confidencial** – Informações que podem afetar diretamente os negócios do Grupo, podendo expor negativamente a imagem do Grupo no mercado, informações relevantes dos Colaboradores ou clientes, que não podem ser divulgadas.

- **Interno** - Informações que podem afetar de alguma forma os negócios do Grupo. São de uso exclusivo de todos os funcionários.

- **Público** – Não impacta os negócios da Instituição. Não há restrição quanto à sua divulgação. S.

Artigo 59 Características dos níveis de classificação da informação:

Confidencial:
a) Deve conter o rótulo de CONFIDENCIAL em todo o seu conteúdo;
b) Afeta diretamente a estratégia ou o negócio do Grupo. Caso se torne pública, pode trazer prejuízo financeiro ou prejudicar a imagem da empresa;
c) Contém informações relevantes dos clientes, Colaboradores e parceiros;

d) Deve ser guardada de forma segura (cofre, criptografada, etc...) e contingenciada;
e) Deve ser lida/acessada em ambientes privados e seguros;
f) Deve ter uma data de expiração ou validade.

Interna:
a) Deve conter o rótulo de INTERNA em todo o seu conteúdo;
b) Afeta em parte o negócio do Grupo;
c) Se pública, pode trazer prejuízo financeiro ou prejudicar a imagem da empresa;
d) Expõe informações de Colaboradores e parceiros;
e) Deve ser guardada com contingência;
f) Dever ser lida/acessada através de ambientes privados e seguros;
g) Somente Colaboradores podem ter acesso.
h) Deve ter uma data de expiração ou validade;

Pública:
a) Não impactam a estratégia ou os negócios do Grupo;
b) Não há restrição quanto ao acesso.

- **REPORTE DE INCIDENTES**

Artigo 60 O objetivo é assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados e apurados, permitindo a tomada de ação necessária.

§1º A Empresa terceirizada de TI contratada pelo Grupo é a responsável pela gestão de incidentes de segurança da informação do Grupo.

§2º Todos os dados relacionados a incidentes devem ser mantidos protegidos e com acesso restrito.

§3º Todos os Colaboradores e Terceiros devem conhecer os canais de comunicação para o registro de incidentes de segurança.

§4º Apenas pessoas explicitamente identificadas e autorizadas estarão liberadas para tratar os incidentes.

§5º Ações para recuperação de violações de segurança e correção de falhas do sistema devem ser cuidadosas e formalmente controladas.

§6º Notificação de fragilidades e eventos de segurança da informação

§7º Os canais oficiais para registro e tratamento de incidentes são os seguintes:
- **E-mail:** helpdesk@halexistar.com.br

§8º Todo Colaborador e Terceiro deve relatar qualquer incidente de segurança da informação.

§9º Todos os registros de incidentes devem ser bem detalhados.

§10º São eventos e incidentes de segurança da informação:

a) Perda de serviço, equipamentos ou recursos;

b) Mau funcionamento ou sobrecarga de sistema;

c) Falhas humanas;

d) Não-conformidade com políticas e diretrizes;

e) Violações de procedimentos de segurança física;

f) Mudanças descontroladas de sistemas;

g) Mau funcionamento de software ou hardware; e

h) Violação de acesso.

§11º Todos os registros de incidentes de segurança devem ser coletados em um único ponto. Esta informação poderá ser analisada e correlacionada através da equipe de tratamento de incidentes. As informações podem ser utilizadas para determinar tendências e padrões de atividades de invasores e para recomendar estratégias de prevenção adequadas.

§12º A análise de incidentes deve ser feita, considerando o prazo de até 1 dia útil para retorno.

- **FUNÇÕES E RESPONSABILIDADES**

Artigo 61 A Política deverá ser atualizada pelo menos uma vez ao ano, em revisões programadas, ou toda vez que uma mudança considerável ocorra nos serviços críticos executados pelo processo de negócio (ex. número de colaboradores, mudança para outra localidade etc.). Todo Colaborador ao ingressar no Grupo deverá ler essa Política e registrar seu entendimento e conhecimento em Termo de Ciência e Compromisso, bem como todo o Terceiro que venha a ter acesso aos recursos de informática do Grupo.

§1º Para todos os Terceiros contratados é necessária uma diligência antes da contratação, analisando sua experiência através do tempo de existência, clientes, qualidade do serviço prestado e verificação dos antecedentes criminais.

§2º Para todos os contratos firmados é necessário que conste previamente uma cláusula de confidencialidade entre os prestadores de serviços, assegurando assim a segurança das informações.

CAPÍTULO VIII - DISPOSIÇÕES FINAIS

Artigo 62 É vedado o uso de equipamentos de propriedade do Grupo para outros fins que não àqueles relacionados estritamente para fins profissionais necessários para condução das atividades do Grupo.

Artigo 63 Todo e qualquer conteúdo digital armazenado em equipamento de propriedade do Grupo é passível de verificação por parte do Grupo, a qualquer tempo. Não somente, o Departamento de Tecnologia da Informação fica autorizado a rastrear e analisar a origem, o destino e o conteúdo de mensagens de correio eletrônico profissional do Grupo a qualquer tempo, por se tratar de ferramenta de trabalho de propriedade do Grupo.

Parágrafo único. Os procedimentos técnicos para a verificação referida no item acima, são realizados diretamente pelo Gerente do Departamento de Tecnologia da Informação (TI) ou por um colaborador devidamente designado para a tarefa em caráter sigiloso., o qual apenas está autorizado a proceder com os mesmos, conforme as seguintes alçadas para a sua autorização: (i) ser devidamente autorizada pelo(s) Diretor(es) Estatutário(s) Responsável(is) pela área(s) envolvida(s), no caso de verificação quanto à Colaborador(es) abaixo deste(s); (ii) ser devidamente autorizada pelo CEO, no caso dos demais Diretores Estatutários; ou (iii) ser devidamente autorizada pelo Presidente do Conselho de Administração do Grupo, no caso do CEO.

Artigo 64 Os Colaboradores e Terceiros que infringirem as disposições do presente Regulamento podem ser questionados e penalizados de acordo com as circunstâncias de cada caso e eventuais prejuízos causados ao Grupo, sendo inteiramente responsáveis pela reparação dos danos resultantes de seus atos. Em relação aos Colaboradores, estes poderão ainda estar sujeitos à rescisão do contrato de trabalho por justa causa, com base no artigo 482 da CLT.

Parágrafo único. Adicionalmente, todos os Colaboradores e Terceiros têm o dever de reportar prontamente qualquer violação desta Política de que tiverem conhecimento, bem como violação de acesso ou qualquer outro evento ou incidente, que possa trazer riscos à segurança da informação de qualquer Companhia do Grupo.

Art. 65 Em caso de qualquer dúvida com relação aos termos desta Política entre em contato com o Departamento de Tecnologia da Informação e/ou com a Área Responsável por *Compliance* no e-mail compliance@halexistar.com.br.

Anexos

Anexo I – Termos Definidos

Anexo II – Termo de Adesão ao Regulamento

ANEXO I - Termos Definidos

Termo	Definição
Colaborador (es)	Qualquer sócio, acionista, administrador, conselheiro, diretor, executivo, empregado/funcionário (celetista ou não), colaborador, assessor, procurador ou agente de qualquer uma das Companhias.
Conselho de Administração	Órgão de governança do Grupo, na forma do seu Estatuto Social.
Terceiros	Inclui toda e qualquer pessoa física ou jurídica não pertencente ao Grupo, que atuem, direta ou indiretamente, de qualquer forma, em nome de qualquer Companhia ou Afiliada do Grupo, incluindo, mas não se limitando a prestadores de serviço, parceiros de negócio, consultores, distribuidores, representantes, fornecedores, despachantes, entre outros.

ANEXO II - Termo de Adesão ao Regulamento

Pelo presente, eu, [nome do Colaborador/ Terceiros], [nacionalidade], [estado civil], [profissão], portador da Carteira de Identidade [RG/RNE] nº. [●], inscrito no CPF/MF sob o nº. [●], [matrícula funcional nº. [●], residente e domiciliado na Cidade de [●], Estado de [●], [cargo/posição ocupada] na [nome da Companhia] (a "Companhia"), empresa integrante do Grupo Halex Istar, declaro, para os devidos fins, que:

Li e tomei conhecimento do inteiro teor do Regulamento de Utilização dos Recursos de Informática (o "Regulamento") do Grupo Halex Istar e estou de acordo com todas as suas disposições;

Comprometo-me a cumprir este Regulamento durante toda a duração do meu vínculo com a Companhia e/ou Grupo Halex Istar, a qualquer título; bem como após a eventual cessação do meu vínculo, no que se refere à obrigação de confidencialidade das informações a que tive acesso no âmbito de minha atuação no Grupo; e

Tenho total conhecimento de que qualquer violação às disposições deste Regulamento poderá resultar na aplicação de penalidades previstas pelos normativos internos do Grupo Halex Istar, além de demais consequências legais previstas em Lei.

Local e Data: [●], [●] de [●] de 20 [●].

_____

[Nome]
[Cargo]
[Empresa/unidade]

Documento a ser assinado por Colaboradores no momento de sua contratação e por Terceiros no momento que venham a ter acesso aos recursos de informática.