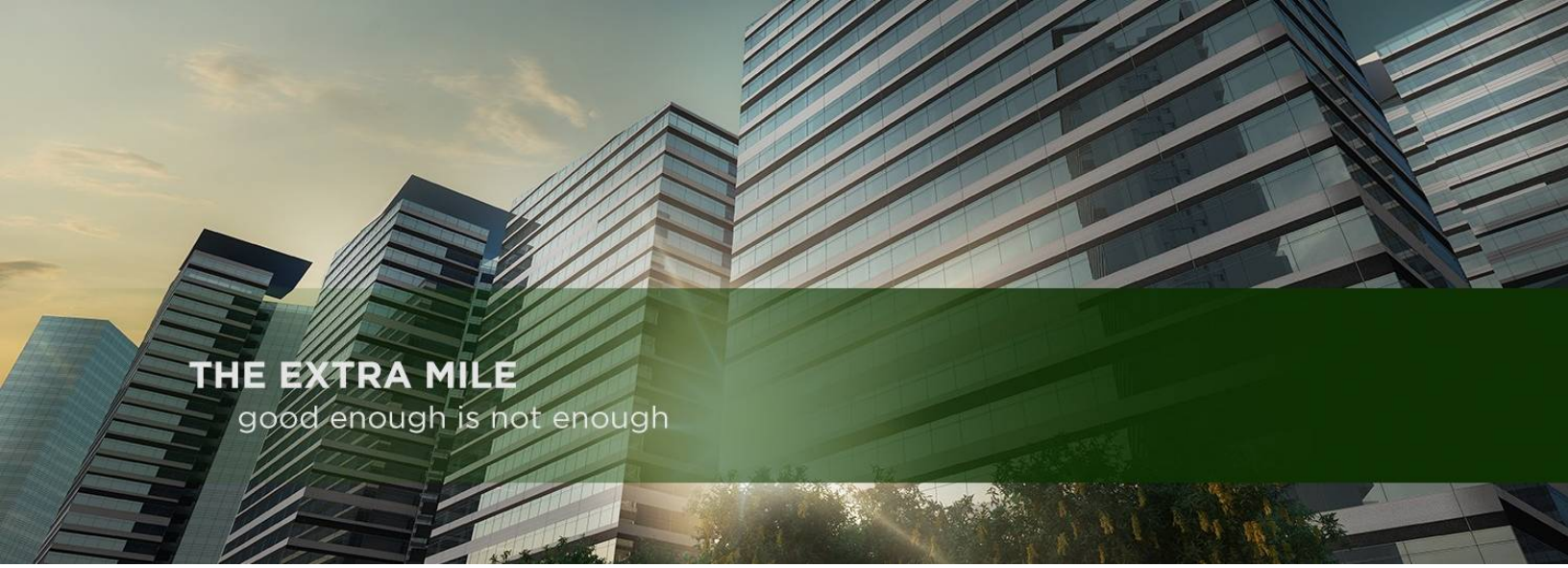

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento de Normas e Diretrizes da Administração

~~Setembro~~Outubro de 2021

SUMÁRIO

1. INTRODUÇÃO

A presente Política de Segurança da Informação (“Política”) se aplica a (i) HSI Administradora e Participações Ltda. (“HSI Administradora”); (ii) HSI Gestora ~~- Crédito Imobiliário~~de Ativos Financeiros Ltda (“HSI ~~Crédito Imobiliário~~Ativos Financeiros”); (iii) HSI Gestora ~~-~~de Special ~~Oportunities~~Opportunities Ltda (“HSI Special ~~Oportunities~~Opportunities”); (iv) HSI Gestora ~~-~~de Real Estate Private Equity Ltda (“HSI Real Estate”); e (v) HSI - Hemisfério Sul Investimentos Ltda. (“HSI Hemisfério Sul”, e quando em conjunto com a HSI Administradora, HSI ~~Crédito Imobiliário~~Ativos Financeiros, HSI Special ~~Oportunities~~Opportunities e HSI Real Estate, designadas “Grupo HSI”).

A Política de segurança da informação se refere às iniciativas que asseguram a integridade e a disponibilidade das informações, garantindo ainda que estas sejam acessadas apenas por pessoas autorizadas.

A Política de Segurança da Informação do Grupo HSI é o documento formal que estabelece e orienta os procedimentos para proteção das informações. As normas e procedimentos estabelecidos nesta política foram previamente corroborados pelo Comitê de Risco e Compliance.

2. PAPÉIS E RESPONSABILIDADES

É de responsabilidade do Comitê de Risco e Compliance assegurar a atualização periódica, publicação e disponibilização desta política para todos os usuários de ativos de informação (desktop, notebook, e-mails, servidores). Todos os colaboradores do Grupo HSI (qualquer integrante, executivo, diretor, estagiário, trainee e terceirizados), sem distinção de cargos e posições e, também, os terceiros (contratados para prestação de serviços por meio de empresa intermediária ou profissional autônomo mediante contrato) são responsáveis por garantir a segurança das informações que estão sobre sua guarda ou posse, executando os procedimentos estabelecidos na Política de Segurança da Informação. A adesão à esta política, ~~através da assinatura do~~ao Termo de Ciência e Concordância (Anexo~~1) e Termo de Confidencialidade (Anexo 2),~~ 1), através do formulário de aceite eletrônico fornecido pelo Grupo HSI é obrigatória.

Todas e quaisquer atividades executadas pelos colaboradores e terceiros devem estar em acordo com a legislação vigente, com a normatização dos órgãos e entidades reguladoras e atender integralmente a esta política.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes do Grupo HSI poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. É também obrigação de cada colaborador se manter atualizado em relação a esta Política e aos procedimentos e normas relacionadas, buscando orientação do seu

gestor ou da Departamento de TI sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

3. OBJETIVOS

Este documento visa auxiliar a implementação de controles e processos para seu pleno atendimento, bem como aumentar a qualidade e a integração das informações, com foco nos seguintes objetivos:

- **Confidencialidade**: garantir que as informações sejam de conhecimento exclusivo de pessoas autorizadas;
- **Integridade**: garantir que a informação preserve o seu conteúdo original, durante a guarda ou transmissão, sem quaisquer modificações propositais, indevidas ou acidentais;
- **Disponibilidade**: garantir a disponibilidade das informações, sempre que necessário, a todas as pessoas autorizadas a utilizá-las.

Somente os colaboradores que estão devidamente autorizados a falar em nome do Grupo HSI para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

4. CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do gestor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (lógica ou física) gerada por sua área.

Todo gestor deve orientar seus subordinados a não circularem informações e/ou mídias confidenciais, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

É também obrigação de cada colaborador se manter atualizado em relação a esta política e aos procedimentos e normas relacionadas, conforme Termo de Ciência e Concordância ~~(“Anexo 1”)~~, buscando orientação do seu gestor ou dos responsáveis da área de TI sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações~~, conforme Termo de Confidencialidade assinado pelo colaborador no momento da contratação~~.

Falhas no sigilo da informação, integridade ou disponibilidade da informação trazem grandes prejuízos à Organização, expressos em perdas financeiras diretas, perdas de competitividade e produtividade ou imagem do Grupo HSI, podendo levar à extinção das operações ou prejuízos graves ao crescimento.

Nenhuma informação confidencial poderá ser repassada para terceiros sem o consentimento do Comitê de Risco e Compliance.

Para melhor entendimento desta Política por “informações confidenciais”, entende-se: todas informações confidenciais, reservadas ou privilegiadas, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre o Grupo HSI, seus sócios e clientes, aqui também contemplados os próprios fundos de investimento, incluindo:

- Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
- Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos de investimento administrados e/ou geridos pelo Grupo HSI;
- Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridos pelo Grupo HSI;
- Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários do Grupo HSI ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação do Grupo HSI e que ainda não foi devidamente levado à público;
- Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos e das companhias investidas pelos fundos;
- Transações realizadas e que ainda não tenham sido divulgadas publicamente;
- Informações de clientes que devem ser protegidas por obrigatoriedade legal, incluindo dados ~~cadastrais~~pessoais (CPF, RG etc.), que identifica ou pode identificar uma pessoa física, situação financeira e movimentação bancária;
- Informações sobre produtos e serviços que revelem vantagens competitivas do Grupo HSI frente ao mercado;
- Todo o material estratégico do Grupo HSI (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
- Quaisquer informações do Grupo HSI, que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes; e

- Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

5. PRINCÍPIOS E DIRETRIZES

5.1. Gestão de acessos

5.1.1. Concessão de Acessos

A concessão de acessos deve ser devidamente formalizada e aprovada. O acesso a novos colaboradores ou temporários deverá ser solicitado pelo RH via e-mail, para help_desk@hsinvest.com e cópia para o COO da respectiva sociedade do Grupo HSI informando os dados do colaborador, a área em que irá atuar e o seu gestor. Após receber a aprovação do COO, a área de TI irá conceder um acesso padrão à rede e e-mail corporativo. Havendo necessidade de acessos específicos à rede e às aplicações, o gestor terá de formalizar a solicitação destes acessos via e-mail para o Help Desk com cópia para o COO.

Em caso de mudança de departamento e/ou cargo, a área de TI, juntamente com o COO, terá de validar se os acessos antigos do colaborador ainda são apropriados, e fazer os ajustes necessário.

5.1.2. Revogação de Acessos

As revogações de acessos também devem ser formalizadas. Quando houver desligamento de um colaborador ou terceiro, o departamento de RH deve enviar via e-mail para a área de TI com cópia para COO. Após receber o e-mail, e com aprovação do COO, os acessos dos colaboradores ou terceiros, devem ser revogados imediatamente.

5.1.3. Revisão de Acessos

As revisões de acessos fazem parte do processo de gestão de acesso que visa identificar qualquer acesso indevido. É necessário que sejam efetuadas revisões de todos os acessos ativos tanto na rede quanto nos sistemas críticos. As revisões devem ser feitas semestralmente pela área de TI enviando a relação de usuários de cada área para seu respectivo gestor, solicitando ao gestor que valide os acessos recebidos.

Após avaliar cada um dos usuários de sua área e os respectivos acessos à rede e às aplicações, o gestor deve formalizar uma aprovação via e-mail para o endereço: help_desk@hsinvest.com.

5.2. Uso da Internet

A internet deve ser utilizada apenas para atividades do Grupo HSI e não para trabalhos de terceiros. O uso para atividades pessoais não deve impactar o desempenho das funções dos colaboradores ou terceiros.

Todas as regras atuais do Grupo HSI visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o Grupo HSI, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela. O acesso à internet é monitorado pela área de TI, sendo registrados os logs (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo em que acessou a internet e quais páginas navegou.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do Grupo HSI, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Política.

O Grupo HSI, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. 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 instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.

Como é do interesse do Grupo HSI que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Apenas os colaboradores autorizados ~~pela instituição~~ pelo Grupo HSI poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal, Lei Geral da Proteção de Dados e demais dispositivos legais. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ~~ou~~, patentes de terceiros ou direito a privacidade.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pelo Departamento de TI.

Os colaboradores não poderão em hipótese alguma utilizar os recursos do Grupo HSI para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de entretenimento, jogos, músicas (em qualquer formato) ou mídias sociais poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado do Grupo HSI ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos do Grupo HSI para, deliberadamente, propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (UTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (Messenger, Whatsapp, Skype e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente ao Departamento de TI.

Não é permitido acesso a sites de proxy ou relacionados.

5.2.1. Usuários Visitantes

Os visitantes que necessitem ter acesso a rede Wi-Fi estão sob as mesmas regras que os colaboradores do Grupo HSI, tendo que cumprir as mesmas regras de segurança. Os usuários visitantes receberão uma senha de acesso provisória para conexão via Wi-Fi e somente poderão navegar na internet após ler e aceitar os temos de responsabilidade de uso da rede. A senha de acesso à rede Wi-Fi Guest deverá ser trocada a cada 30 dias pelo Departamento de TI.

5.2.2. Realização de Downloads de Arquivos

O download de programas executáveis com extensões .exe, .bat, .com (Windows) e .dmg (Mac OSX), é bloqueado para evitar a instalação de software malicioso. Caso o usuário precise baixar algum software, será necessário contatar a área de TI para assistência.

Downloads de arquivos com tamanho superiores a 1024 MB (1GB) podem exigir muita banda de acesso à internet, causando redução de velocidade e comprometendo a navegação dos demais usuários. O colaborador deverá formalizar uma solicitação para help_desk@hsinvest.com caso precise realizar um download maior do que 1024 MB (1GB).

5.3. Uso de E-mail

O correio eletrônico corporativo fornecido pelo Grupo HSI (e-mail) é um instrumento de comunicação interna e externa para a realização do negócio do Grupo HSI. As mensagens devem ser escritas em linguagem profissional, não devendo comprometer a imagem do Grupo HSI, assim como observando a legislação vigente e o Código de Ética do Grupo HSI.

O colaborador é responsável por todas as mensagens enviadas pelo seu endereço de e-mail. Visando a proteger a rede interna do Grupo HSI de vírus e malwares, a área de TI poderá bloquear o recebimento de e-mails provenientes de domínio público.

Os colaboradores deverão desconfiar de todos os e-mails com assuntos estranhos e não reenviar e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, descontos, promoções, etc.

Deve-se utilizar o e-mail para qualquer comunicação interna que não necessite do meio físico, diminuindo o custo com impressão e aumentando a agilidade na entrega e leitura.

Em hipótese alguma, usuários que não sejam colaboradores ou terceiros do Grupo HSI terão acesso às contas de correio eletrônico do Grupo HSI.

A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o Grupo HSI e não cause impacto no tráfego da rede.

É proibido aos colaboradores o uso do correio eletrônico do Grupo HSI:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo do Grupo HSI;
- reenviar e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, descontos, promoções, etc.
- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou ao Grupo HSI ou suas unidades vulneráveis a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do Grupo HSI estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
  - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do Grupo HSI;
  - contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
  - contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
  - vise obter acesso não autorizado a outro computador, servidor ou rede;
  - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
  - vise burlar qualquer sistema de segurança;
  - vise vigiar secretamente ou assediar outro usuário;
  - vise acessar informações confidenciais sem explícita autorização do proprietário;
  - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
  - inclua imagens criptografadas ou de qualquer forma mascaradas;
  - tenha conteúdo considerado impróprio, obsceno ou ilegal;
  - seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
  - contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
  - tenha fins políticos locais ou do país (propaganda política);
  - inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador
- Nome da empresa
- Telefone(s)
- Correio eletrônico

Anexos grandes devem ser evitados. Precisando transmitir um volume grande de informação, o colaborador deve consultar o Departamento de TI para alternativas.

5.4. Instalação E Manutenção De Softwares

O Grupo HSI provê software devidamente licenciados para o cumprimento das rotinas diárias a todos os usuários. Em hipótese nenhuma o usuário deve desinstalar ou reconfigurar o software instalado, muito menos os softwares relacionados à segurança da rede do Grupo HSI. Caso o usuário julgue necessária uma manutenção de software, deverá encaminhar um pedido para o Departamento de TI com as devidas justificativas.

Se o usuário necessitar da instalação de qualquer software, plugin, ou atualização, deverá encaminhar uma solicitação para help_desk@hsinvest.com, que, por sua vez, responderá de forma imediata qual o tempo necessário para a execução do serviço, solicitando a aprovação do gestor da área, se julgar necessário.

O Departamento de TI deverá, obrigatoriamente, protocolar todas as solicitações recebidas dos usuários e, antes de qualquer procedimento, deverá confirmar o horário programado para a respectiva execução. Fica permanentemente proibida a instalação de quaisquer softwares sem licença de uso.

O Departamento de TI poderá desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso.

5.5. Software Compartilhadores De Arquivos (P2p)

O uso de software para compartilhamento de arquivo, tais como uTorrent, BitTorrent e eMule, não é permitido pelo Grupo HSI. As máquinas dos colaboradores não permitem instalações desse tipo de software sem o suporte do Departamento de TI.

5.6. Segurança Física

Os colaboradores deverão portar seus respectivos crachás para acesso ao prédio e às dependências do Grupo HSI. Apenas colabores de TI terão acesso às áreas exclusivas deste setor, como à sala destinada ao servidor e outras dependências especificadas pelo Departamento de TI.

O fluxo dos visitantes deverá restringir-se apenas à área destinada às salas de reuniões. Eventuais acessos às dependências comuns dos funcionários do Grupo HSI deverão ser autorizados pela Diretoria ou pelos gestores e devidamente justificados.

O usuário deverá fechar qualquer documento que esteja manipulando ou redigindo quando necessitar ausentar-se de sua mesa, deixando a proteção de tela ativada no modo de login.

Os papéis referentes a assuntos confidenciais que não sejam mais necessários, antes de serem levados ao lixo, devem ser processados na máquina fragmentadora, disponível na área de impressão.

As impressões de documentos deverão ser apenas referentes aos assuntos do Grupo HSI, não sendo autorizada a utilização de impressões de cunho pessoal.

O uso de telefone do Grupo HSI deverá ser exclusivo para uso a serviço do Grupo HSI, não devendo ser utilizado para fins pessoais.

5.7. Direitos de Propriedade

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pelo Grupo HSI pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

O Grupo HSI, por meio do Departamento de TI, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

5.8. Equipamentos particulares/privados

Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes do Grupo HSI sem prévia e expressa autorização da área de TI.

5.9. Mesa Limpa

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não. Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

5.10. Conversas em Locais Públicos e registro de informações

Não discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de texto, exceto quando encaminhadas aos colaboradores do Grupo HSI.

6. DAS RESPONSABILIDADES ESPECÍFICAS

6.1 Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição. Será de inteira responsabilidade de cada colaborador todo prejuízo ou dano que vier a sofrer ou causar ao Grupo HSI e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

6.2 Dos Colaboradores em Regime de Exceção (Temporários)

Os colaboradores temporários devem entender os riscos associados à sua condição especial e cumprir rigorosamente esta Política. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

6.3 Dos Gestores de Pessoas e/ou Processos

Os colaboradores que ocupam cargos de gestão devem ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão. Devem também atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento desta Política.

Antes de conceder acesso às informações do Grupo HSI, os gestores deverão exigir a assinatura de Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

7. DOS CUSTODIANTES DA INFORMAÇÃO

7.1 Da Área de Tecnologia da Informação (TI)

A Área de TI possui as seguintes responsabilidades:

(i) Realizar testes periódicos para verificar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;

(ii) Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política;

(iii) Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada colaborador e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações. O Grupo HSI possui segurança especial para sistemas com acesso público,

garantindo a guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;

(iv) Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, serão implantados controles de integridade para torná-las juridicamente válidas como evidências;

(v) Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o Grupo HSI;

(vi) Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela;

(vii) Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

(viii)Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

(ix) Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário
- os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

(x) Proteger continuamente todos os ativos de informação do Grupo HSI contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

(xi) Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção do Grupo HSI em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

(xii) Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

(xiii)Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento do Grupo HSI, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

(xiv) Garantir que todos os servidores, estações e demais dispositivos com acesso à rede do Grupo HSI operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

(xv) Informar o gestor da informação previamente ao fim do prazo de retenção da informação, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

(xvi) Monitorar o ambiente de TI, gerando indicadores e históricos de:

- uso da capacidade instalada da rede e dos equipamentos;
- tempo de resposta no acesso à internet e aos sistemas críticos do Grupo HSI;
- períodos de indisponibilidade no acesso à internet e aos sistemas críticos do Grupo HSI;
- incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

~~***7.2 Da Área de Segurança da Informação***~~

~~A Área de Segurança da Informação possui as seguintes responsabilidades:~~

- ~~Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.~~
- ~~Propor e apoiar iniciativas que visem à segurança dos ativos de informação do Grupo HSI.~~
- ~~Publicar e promover as versões desta Política aprovadas pelo Comitê de Risco e Compliance.~~
- ~~Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio do Grupo HSI, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.~~
- ~~Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.~~

- ~~Analisar criticamente incidentes em conjunto com o Comitê de Risco e Compliance.~~
- ~~Apresentar as atas e os resumos das reuniões do Comitê de Risco e Compliance, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.~~
- ~~Manter comunicação efetiva com o Comitê de Risco e Compliance sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar o Grupo HSI e~~
- ~~Buscar alinhamento com as diretrizes corporativas do Grupo HSI.~~

8. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta Política, o Grupo HSI poderá:

- implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Risco e Compliance;
- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

9. IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o Grupo HSI e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados no Grupo HSI, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

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

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o Grupo HSI e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado. É proibido o compartilhamento de login para funções de administração de sistemas.

O Departamento de Recursos Humanos do Grupo HSI é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

O Departamento de TI responde pela criação da identidade lógica dos colaboradores na instituição, nos gerenciamentos de contas de grupos e usuários.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. Esta conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

10. POLÍTICA DE SENHAS

O colaborador é responsável por todos os atos executados com seu identificador (login/sigla), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia. Os colaboradores devem:

- Manter a confidencialidade através da memorização. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcd1234”, “Nome123”, entre outras.
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del ou Windows + L).

A regra de composição de senhas deve atender às seguintes premissas:

- Todos os usuários deverão ter senha de tamanho variável, possuindo no mínimo 8 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ % ! &) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.
- A senha é individual e intransferível, de conhecimento e uso exclusivo do próprio colaborador, não podendo ser divulgada, cedida e/ou compartilhada;
- Haverá mudança obrigatória de senha a cada 90 (noventa) dias (não podendo ser repetidas as 3 (três) últimas senhas), ou a qualquer momento dentro deste prazo se houver indicação ou suspeita de que a senha tenha sido violada ou se o colaborador desejar. Eventuais exceções devem ser tratadas com o Departamento de TI;
- Não utilizar senhas triviais, de fácil identificação, evitando itens como: meses do ano, dias da semana ou qualquer outro dado relativo a datas, nomes de familiares, iniciais, placas de carro, nomes comuns ao Grupo HSI, números de telefone, identificação do colaborador (login), nome do colaborador, grupo do colaborador, sequência numérica com mais de dois caracteres idênticos consecutivos, etc.;
- Após 5 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o Departamento de TI do Grupo HSI. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).
- Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer à área técnica responsável para cadastrar uma nova.

11. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade do Grupo HSI, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do Departamento de TI do Grupo HSI, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Departamento de TI, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado através do e-mail help_desk@hsinvest.com.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio do Grupo HSI (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores deverão ser salvos em drives de rede. 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 usuário.

Os colaboradores do Grupo HSI e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização do Departamento de TI.

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

- todos os computadores de uso individual deverão ter senha de BIOS para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Departamento de TI do Grupo HSI, que terá acesso a elas para manutenção dos equipamentos.
- 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 da Departamento de TI do Grupo HSI ou por terceiros devidamente contratados para o serviço.
- todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e do Departamento de TI.

- é expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
- o colaborador deverá manter a configuração do equipamento disponibilizado pelo Grupo HSI, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.
- deverão ser protegidos por senha (bloqueados), todos os terminais de computador e impressoras quando não estiverem sendo utilizados.
- todos os recursos tecnológicos adquiridos pelo Grupo HSI devem ter imediatamente suas senhas padrões (default) alteradas.
- os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.
- acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do Grupo HSI:
- tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- burlar quaisquer sistemas de segurança.
- acessar informações confidenciais sem explícita autorização do proprietário.
- vigiar secretamente outrem por dispositivos eletrônicos ou softwares, 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 atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

12. DISPOSITIVOS MÓVEIS

O Grupo HSI deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pelo Departamento de TI, como: notebooks, smartphones e pen drives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

O Grupo HSI, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O Grupo HSI reserva-se o direito de inspecionar a qualquer tempo os dispositivos móveis concedidos por ele. Os dispositivos móveis particulares não são passiveis de inspeção, porém devem ser usados conforme esta política. Caso um colaborador seja identificado em desacordo com esta política, poderá sofrer as sanções previstas na Política de Consequências.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do Grupo HSI (BYOD - Bring Your Own Device) deverá submeter previamente tais equipamentos ao processo de autorização do Departamento de TI.

Equipamentos portáteis, como smartphones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão submetidos à padronização e a manutenção.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais default (aplicativos originais) dos equipamentos, em especial os referentes à segurança da informação e à geração de logs. Alterações das configurações serão feitas exclusivamente pela área de TI, que avaliará a necessidade da solicitação junto ao gestor do colaborador.

Os notebooks de propriedade do Grupo HSI concedidos aos colaboradores devem possuir um sistema de criptografia a nível de disco (Hard Disk ou SSD), a fim de proteger as informações no caso de roubo ou extravio do equipamento.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no Grupo HSI, mesmo depois de terminado o vínculo contratual mantido com a instituição.

O suporte técnico aos dispositivos móveis de propriedade do Grupo HSI e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pelo Grupo HSI.

Todo colaborador deverá utilizar senhas de desbloqueio para seu dispositivo móvel.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Departamento de TI do Grupo HSI. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pelo Grupo HSI constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

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

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

13. CPD INTERNO

O acesso ao CPD interno é limitado aos profissionais previamente autorizados, e por meio de crachá. Todo acesso ao CPD interno deverá ser registrado (usuário, data e hora) mediante utilização dos crachás.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.

O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em emergências, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável do Departamento de TI. Deverão existir duas cópias de chaves da porta do CPD. Uma das cópias ficará de posse do coordenador responsável pelo CPD, a outra, de posse do coordenador de infraestrutura.

O CPD deverá ser mantido limpo e organizado. Não é permitida a entrada de nenhum tipo de alimento, bebida ou produto inflamável.

A entrada ou retirada de quaisquer equipamentos do CPD somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável Departamento de TI.

No caso de desligamento de empregados ou colaboradores que possuam acesso ao CPD, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação e da lista de colaboradores autorizados.

14. PROCEDIMENTOS DE BACKUP E RESTORE

Os procedimentos de backup são registrados e geridos automaticamente pela 2MI. Os backups são diários e mensais, armazenados em disco ou fita.

A empresa Iron Mountain é responsável por guardar as fitas de backup que não estão em uso no Grupo HSI. Duas vezes por semana, a Iron Mountain substitui as duas fitas mais recentes com as mais antigas e coleta essas últimas para armazenamento em suas dependências. É necessário atualizar o inventário de fitas a cada troca.

O Data Protector registra todos os logs gerados pelas rotinas cadastradas. Erros no procedimento deverão ser analisados e corrigidos pela área de TI dentro de 24 horas, acompanhado de um relatório de exceção completo.

O cadastro de novas rotinas no Data Protector deverá ser feito exclusivamente pela área de TI, conforme normas e alçadas da área.

O área de TI deverá manter o Data Protector atualizado em sua última versão, verificando o ciclo de vida e monitorando a garantia do fabricante.

As mídias de backup devem ser acondicionadas em local seco, climatizado, seguro, com portas corta fogo e distantes o máximo possível do datacenter.

Além dos procedimentos de backup, testes de restore serão conduzidos às segundas-feiras, seguido do registro dos resultados na rede para posterior consulta. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Todos os backups devem ser automatizados por sistemas de agendamento para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores ou empresas terceiras responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

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

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade junto a gestão do Departamento de TI.

Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis a gestão do Departamento de TI.

Para formalizar o controle de execução de backup e restore, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo gestor do Departamento de TI.

15. AUTONOMIA DO DEPARTAMENTO DE TI

O Departamento de TI tem total autonomia para atuar sobre os equipamentos de informática disponibilizados pelo Grupo HSI. Os procedimentos abaixo poderão ser realizados sem prévio aviso aos usuários:

- Realização de auditoria (local ou remota);
- Definição dos perfis de usuários cujos privilégios não permitam a realização de atividades tidas como nocivas ao sistema operacional ou à rede como um todo;
- Instalação de software de monitoramento;
- Desinstalação de qualquer software considerado nocivos à integridade da rede; e
- Credenciamento/descredenciamento de usuários.

16. PENALIDADES

As situações abaixo são exemplos de infrações e suas respectivas penalidades de acordo com a Política de Consequências*:

- Ausentar-se da mesa e deixar o computador desbloqueado ou informações sensíveis sobre mesa: orientação verbal (feedback) e/ou realização/reforço de treinamento/coaching

- Acesso proposital a websites proibidos, download de programas nocivos, deixar de reportar infrações dessa política: advertência verbal ou escrita dependendo das consequências da infração
- Vazamento de informações, utilização de informações privilegiadas para vantagens pessoais, introdução intencional de vírus na rede: demissão ou demissão por justa causa e ainda possíveis medidas judiciais.

Essa lista não é exaustiva e apenas ilustra as situações que podem configurar descumprimento desta política.

17. CONTATO

Os usuários que tiverem ou presenciarem problemas referentes à segurança da informação, devem entrar em contato com a área de TI por meio do e-mail: help_desk@hsinvest.com.

Todos os casos devem ser formalizados no e-mail indicado e tratado pela área de TI de acordo com a gravidade do problema definida na Política de Consequências.

18. VALIDADE E VIGÊNCIA

A presente política passa a vigorar a partir da data de sua homologação e publicação como Portaria Interna do Grupo HSI, sendo válida por tempo indeterminado, devendo ser atualizada sempre que necessário.

19. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do Grupo HSI. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

HISTÓRICO DE REVISÕES

Revisão	Data	Modificação
0	2020-09-17	Emissão inicial.
1	2021-09	1ª Revisão.

~~ANEXO 1 - *Termo de Concordância com a Política de Segurança da Informação do Grupo HSI*~~ANEXO 1 – TERMO DE CIÊNCIA E CONCORDÂNCIA

~~Declaro estar ciente das normas e procedimentos referentes à Política de Segurança da Informação do Grupo HSI.~~

~~Tenho ciência de que a leitura e cumprimento de todas as normas desse documento é fundamental para o bom funcionamento dos processos de trabalho.~~

~~***FUNCIONÁRIO:*** _____~~

~~***SETOR:*** _____~~

~~***ASSINATURA:*** _____~~

~~***LOCAL E DATA:*** _____~~

Reconhecendo a relevância de todas as orientações, obrigações, princípios e faculdades dispostos nas Políticas, Códigos e Manuais do Grupo HSI para o exercício de minhas funções como colaborador, para o bom funcionamento das atividades do Grupo HSI, bem como para o cumprimento de seus deveres fiduciários, declaro:

a) ter tido acesso;

b) sanado todas as minhas dúvidas;

c) estar de pleno acordo com o inteiro teor das seguintes Políticas, Códigos e Manuais do Grupo HSI, comprometendo-me a cumpri-las integralmente:

- Política de Investimentos Pessoais;
- Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e
- Manual de Cadastro;
- Código de Ética e Política de Controles Internos;
- Política de Valor Justo de Mercado;

- Política de Certificação Continuada;
- Política de ESG;
- Política de Exercício de Direito de Voto em Assembleia;
- Política de Gestão de Riscos;
- Política de Segurança da Informação;
- Política de Rateio e Divisão de Ordens; e
- Política de Consequências, sem prejuízo de outras que sejam apresentadas a mim
- pela Área de Risco e *Compliance* após a assinatura deste Termo.

Atesto, ainda:

d) ter informado à Área de Risco e *Compliance*, todas as participações acionárias em sociedades e outros investimentos nos mercados financeiro e de capitais, que estejam ou possam entrar em conflito com as Políticas, Códigos e Manuais acima mencionados e me comprometo a informar, quaisquer investimentos futuros que assim possam ser classificados;

e) ter informado à Área de Risco e *Compliance*, qualquer situação que possa sugerir conflito de interesses envolvendo Agentes Públicos, comprometendo-me a proceder do mesmo modo, caso tal situação venha a se configurar posteriormente à assinatura deste Termo;

f) estar ciente de que a empresa adota as seguintes políticas para se adequar à Lei Geral de Proteção de dados: Política de Privacidade, Política de Gestão de Incidentes, Política de Retenção de Dados, Política Geral de Proteção de Dados e a Política de Segurança de Informação e, que tenho a opção de buscar mais informações das mesmas com a área de *Compliance* em qualquer momento.

g) serem de minha exclusiva responsabilidade, eventuais custos incorridos ou perdas, reais ou potenciais, que eu possa sofrer, em razão da necessidade de cancelar investimentos existentes ou de me ver privado de fazê-los, em razão do que determinam as referidas Políticas, Códigos e Manuais; e

h) estar ciente de que a apresentação de falsa declaração me sujeitará não somente às penalidades da Política de Consequências do Grupo HSI, mas também às penalidades da Lei.

Declaro ter lido, compreendido e aceitado integralmente o que determina o presente Termo de Ciência e Concordância, bem como reconheço que o sistema pelo qual recebi e encaminharei o presente Termo será capaz de me identificar para todos os fins aqui dispostos.

(As informações aqui dispostas podem ser preenchidas por qualquer meio digital disponibilizado pelo Grupo HSI ao colaborador. Trata-se de mero modelo ao qual o Grupo HSI não está vinculado.)

ANEXO 2 - Termo de Confidencialidade

Eu, sirvo-me do presente para confirmar que, no exercício de minhas funções, de forma temporária ou permanente, na (i) HSI Administradora e Participações Ltda. ("HSI Administradora"); e/ou (ii) HSI Gestora – Crédito Imobiliário Ltda ("HSI Crédito Imobiliário"); e/ou (iii) HSI Gestora – Special Oportunities Ltda ("HSI Special Oportunities"); e/ou (iv) HSI Gestora - Real Estate Private Equity Ltda ("HSI Real Estate"); e/ou (v) HSI - Hemisfério Sul Investimentos Ltda. ("HSI Hemisfério Sul", e quando em conjunto com a HSI Administradora, HSI Crédito Imobiliário, HSI Special Oportunities e HSI Real Estate designadas "Grupo HSI"), terei, acesso a informações confidenciais de natureza financeira, técnica, comercial e jurídica, conforme definidas na Política de Segurança da Informação.

Este acesso a informações confidenciais abrange, ainda, informações da mesma natureza sobre sociedades controladas, interligadas, investidas, administradas e/ou fundos de investimentos do Grupo HSI, sujeitos a controle comum ou que o Grupo HSI tenha participação ou interesse ou com a qual venha associar-se.

Adicionalmente, reconheço que no processo de análise e de acompanhamento das atividades das empresas em que o Grupo HSI venha a realizar investimentos ou com a qual venha a associar-se, terei ou poderei ter acesso a informações transmitidas por terceiros ao Grupo HSI sob compromisso de confidencialidade assumido pelo Grupo HSI, cuja violação de minha parte ensejará não apenas na minha responsabilização pessoal, como também a responsabilização do Grupo HSI.

Tendo em vista tais circunstâncias, assumo neste ato, compromisso de não divulgar a quaisquer terceiros estranhos ao Grupo HSI, a qualquer título e sob qualquer pretexto, qualquer informação confidencial a que eu venha ter ou já tenha tido acesso com relação às matérias aqui dispostas.

Obrigo-me a zelar para que, por ação ou omissão involuntária, tais informações confidenciais, bem como os documentos que reflitam (inclusive os registros eletrônicos e em meio magnético para uso em computadores, aqui compreendidos, para todos os efeitos desta carta, no conceito de documentos), não venham a ser de conhecimento por parte de terceiros, bem como me comprometo a não reproduzir, para meu uso ou arquivo pessoal, nem permitir que sejam reproduzidas por terceiros estranhos ao Grupo HSI, as informações confidenciais referidas nesta carta.

Tenho conhecimento de que o compromisso de estrita confidencialidade aqui assumido compreende também a vedação a qualquer tipo de discussão pública sobre assuntos de interesse ou relacionados ao Grupo HSI de caráter confidencial, ainda que com acionistas, administradores, funcionários ou colaboradores do Grupo HSI.

Tendo em vista a necessidade da transmissão de tais informações para que auditores, advogados ou outros prestadores de serviços contratados pelo Grupo HSI desempenhem suas atividades, obrigo-me a fazer com que, na medida necessária, os mesmos zelem para o sigilo das informações a eles transmitidas, que serão sempre por mim limitadas ao necessário para o fim aqui previsto.

Reconheço, ainda, que o cumprimento da obrigação de confidencialidade ora assumida depende de uma atenção permanente, obrigando-me a colaborar com os demais integrantes e colaboradores do Grupo HSI para que não ocorram violações aos compromissos por eles igualmente assumidos.

Declaro ainda ter conhecimento de que os investimentos e associações do Grupo HSI serão administrados, sempre que possível, de forma independente entre si e, em qualquer circunstância, independentemente das outras sociedades interligadas ao Grupo HSI ou a seus acionistas, direta ou indiretamente. Deste modo, no conceito de terceiros estranhos ao Grupo HSI estão incluídos também colaboradores de sociedades em que o Grupo HSI tenha gerido investimentos ou com a qual se tenha associado, ou de outras sociedades interligadas ao Grupo HSI, com as quais venha a realizar qualquer tipo de discussão sobre o assunto de seu interesse ou relacionado ao Grupo HSI, deverá ser previamente autorizado, por escrito, pelos acionistas do Grupo HSI, caso exceda as matérias de interesse comum entre o Grupo HSI e tais sociedades.

As obrigações por mim assumidas permanecerão válidas durante todo o período em que eu permaneça no quadro de colaboradores, funcionários, associados ou prestadores de serviço do Grupo HSI, bem como pelo prazo de 2 (dois) anos após a data em que minha vinculação com o Grupo HSI venha a cessar, por qualquer motivo.

Tendo em vista o fato de que serei ou poderei ser, no exercício de minhas atividades no Grupo HSI, depositário de documentos relativos às informações confidenciais aqui referidas (tanto os documentos que me tenham sido transmitidos, quanto o produto das análises e estudos que eu ou outros integrantes do quadro de colaboradores do Grupo HSI venhamos a desenvolver, inclusive

programas ou aplicações especializadas em programas para computadores), fico obrigado(a) a devolver todos estes documentos e os respectivos registros eletrônicos em meio magnético para uso no computador, sem conservar cópia em meu poder, caso venha a cessar minha vinculação com o Grupo HSI, a qualquer título, obrigação essa que também abrange meus sucessores a qualquer título.

Responsabilizo-me, assim, por qualquer prejuízo que o Grupo HSI, seus acionistas, administradores ou colaboradores venham a sofrer pela violação, por dolo ou culpa, das obrigações por mim aqui assumidas.

Ademais, declaro ter conhecimento de que as informações confidenciais aqui referidas, quando as sociedades a que digam respeito se encontrem registradas na Comissão de Valores Mobiliários (CVM) como companhias abertas, constituem informações privilegiadas cujo uso, para fins de negociação de valores mobiliários, contraria o disposto na Instrução CVM n° 358/02, conforme posteriormente alterada.

As obrigações aqui assumidas não limitam o uso de informações de conhecimento público anteriormente a data em que se foram transmitidas ou obtidas pelo Grupo HSI, ou que venham a ser, por forma que não envolva ação ou omissão do Grupo HSI, nem tampouco restrinja à obrigação legal de minha parte de divulgar informações à Administração Pública.

Mesmo assim e caso tais informações venham a ser de alguma forma solicitadas pela Administração Pública, obrigo-me a comunicar antecipadamente tal fato aos administradores do Grupo HSI, de sorte que possam ser tomadas as providencias legais cabíveis para que a divulgação de informações possa atender adequadamente ao disposto em lei, sem prejuízo dos interesses comerciais legítimos do Grupo HSI.

Declaro ainda ter conhecimento de que o domínio “hsinvest.com” é de titularidade exclusiva do Grupo HSI, razão pela qual autorizo expressamente que o Grupo HSI acesse todas e quaisquer mensagens eletrônicas (e-mails) por mim recebidas e/ou enviadas utilizando o domínio “hsinvest.com.br” durante e/ou após o término de meu vínculo com o Grupo HSI.

Qualquer dúvida relativa ao cumprimento das obrigações aqui assumidas deverá ser objeto de discussão com os diretores do Grupo HSI que indicarão um responsável com vistas a solucionar a eventual dúvida que possa surgir.

Confirmando que a presente serve como evidência legal das obrigações por mim assumidas, não dependendo de renovação periódica, subscrevo-me.

Fica eleito o foro da Comarca de São Paulo, Estado de São Paulo, para dirimir quaisquer questões oriundas deste Termo de Confidencialidade, com renúncia a qualquer outro, por mais privilegiado que seja.

FUNCIONÁRIO: _____

HISTÓRICO DE REVISÕES

SETOR: _____

ASSINATURA: _____

Revisão	Data	Modificação
0	2020-09-17	Emissão inicial.
1	2021-10	1ª Revisão.

LOCAL E DATA: _____

~~*(As informações aqui dispostas podem ser preenchidas por qualquer meio digital disponibilizado pelo Grupo HSI ao colaborador. Trata-se de mero modelo ao qual o Grupo HSI não está vinculado.)*~~

Document comparison by Workshare 9.5 on segunda-feira, 18 de outubro de 2021 15:34

Input:	
Document 1 ID	file://P:_Area Compartilhada\Equipe Fundos\Projetos Equipe\Projeto HSI\Políticas - Grupo Economico\Políticas Enviadas em 17.09.2021 - Sem Ajustes LGPD\Política HSI - Segurança da Informação.docx
Description	Política HSI - Segurança da Informação
Document 2 ID	file://\\SAOS1085\ProfileGeneral$\vbraschi\Desktop\Casos\Grupo HSI\Políticas HSI\Políticas Revistas - 15.10.2021\Política HSI - Segurança da Informação - 15.10.2021.docx
Description	Política HSI - Segurança da Informação - 15.10.2021
Rendering set	Standard

Legend:	
Insertion	
~~Deletion~~	
~~Moved from~~	
Moved to	
Style change	
Format change	
~~Moved deletion~~	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:	
	Count
Insertions	89
Deletions	100
Moved from	2
Moved to	2
Style change	0

Format changed	0
Total changes	193