Política de Segurança Cibernética, Segurança da Informação e Continuidade de Negócios

Grupo Starboard

É vedada a reprodução, alteração e transmissão por qualquer forma ou meio deste documento, em parte ou em sua totalidade, sem a autorização expressa do Grupo Starboard.

1. Objetivo

A presente Política de Segurança Cibernética, Segurança da Informação e Continuidade de Negócios ("Política") estabelece normas, diretrizes, princípios e responsabilidades referentes ao acesso a informações, segurança cibernética e procedimentos , bem como a respeito das normas de utilização de equipamentos, de endereços eletrônicos ("e-mails"), de gravação de arquivos, *downloads*, conexões externas, rede privada virtual ("VPN"), controle de instalações físicas e de programas e ferramentas de trabalho da Starboard Holding Ltda., da Starboard Asset Ltda. e da Starboard Restructuring Partners Consultoria em Negócios Ltda. ("Starboard").

Esta política (i) foi elaborada a partir da identificação e da avaliação de riscos relacionados a segurança da informação, segurança cibernética e continuidade das atividades da Starboard, e têm por objetivo mitigar e minimizar tais riscos; e (ii) é aplicável a todos que compõem os quadros social e funcional da Starboard ("Colaboradores"), bem como a quaisquer terceiros com os quais a Starboard mantenha relação comercial, contratual ou de confiança, incluindo parceiros e fornecedores da Starboard ("Terceiros"), que tiverem acesso a informações confidenciais.

Esta Política foi elaborada em observância ao disposto na Resolução CVM nº 21, de 25 de fevereiro de 2021, e nas Regras e Procedimentos de Deveres Básicos do Código de Administração e Gestão de Recursos de Terceiros da Associação Brasileira dos Mercados Financeiro e de Capitais – ANBIMA, e deve ser interpretada em consonância com as demais políticas, normas internas e procedimentos da Starboard.

2. Atribuições da Área de Riscos e Compliance

A Área de Riscos e Compliance é responsável pelos temas de riscos e *compliance* da Starboard, e possui autonomia e independência para executar suas funções, sendo certo que:

- Suas atividades serão desempenhadas com recursos humanos capacitados no assunto, com os recursos materiais e financeiros necessários ao cumprimento de suas funções, bem como com os poderes, acesso direto à Alta Administração e às informações necessárias para o desenvolvimento de suas atividades;
- A Diretoria de Riscos e Compliance será sempre confiada a pessoa com reputação ilibada e qualificação adequada para o exercício de suas funções; e
- Serão realizadas as medidas necessárias para manter a independência e a adequada autoridade do Diretor de Riscos e Compliance para apuração de possíveis irregularidades cometidas por Colaboradores de qualquer hierarquia do quadro da Starboard.

Caberá ao Diretor de Riscos e Compliance, no exercício de suas atribuições:

- Promover ou auxiliar diretamente nos treinamentos para manter os Colaboradores constantemente atualizados em relação ao conteúdo da presente Política;
- Garantir que a comunicação quanto ao conteúdo desta Política seja efetiva aos seus Colaboradores e Terceiros;
- Verificar e avaliar a adequação e efetividade desta Política, bem como sua aderência às normas legais e regulamentares às quais a Starboard está submetida;
- Monitorar as situações em relação ao acesso a informações que possam acarretar conflitos de interesse;
- Prestar suporte à Diretoria da Starboard a respeito da observância das normas legais e regulamentares aplicáveis à Starboard, mantendo-os informados sobre as atualizações relevantes em relação a tais temas;
- Supervisionar as medidas previstas nesta Política e no Plano de Resposta a Incidentes e prestar esclarecimentos e orientações aos Colaboradores e Terceiros, sempre que necessário;
- Auxiliar na condução das investigações acerca de incidentes de segurança ou, caso realizadas por empresas ou escritórios independentes, acompanhar e supervisionar o seu andamento;
- Revisar anualmente a presente Política e, sempre que necessário, propor alterações e ajustes, de acordo com a legislação e com melhores práticas de mercado, a fim de minimizar preventivamente eventuais riscos à segurança da informação e consequentes eventuais paralisações de operação;
- Garantir que os processos e atividades operacionais cuja interrupção ou indisponibilidade não programados podem provocar impacto negativo significativo nos negócios da Starboard ("Processos Críticos de Negócio") estejam devidamente mapeados de forma atualizada; e
- Elaborar relatório, com periodicidade mínima anual, contendo (i) descrição detalhada e atualizada dos controles internos implantados, (ii) da metodologia aplicada para escolha e realização de testes de segurança e (iii) dos procedimentos realizadas para análise das deficiências encontradas, bem como (iv) detalhamento dos testes realizados e das conclusões obtidas quanto à eficiência e eficácia dos controles internos para garantir o cumprimento da presente Política, (v) recomendações quanto às eventuais deficiências que tenham sido identificadas no exercício de referência do relatório com o (vi) estabelecimento de planos de ação e de (vii) cronogramas de saneamento para correção, quando for o caso, (viii) avaliação de riscos para a Starboard em relação aos seus controles internos e (ix) quanto à sua vulnerabilidade a ataques cibernéticos, com manifestação do Diretor de Riscos e Compliance a respeito das deficiências encontradas.

Em caso de dúvidas ou para demais esclarecimentos, o Diretor de Riscos e Compliance pode ser contatado pelo e-mail compliance@starboardpartners.com.br ou pelo telefone (11) 3077-5300.

3. Segurança da Informação

3.1. Nossa Visão

A Starboard compreende o dinamismo inerente ao mundo virtual e a facilidade de acesso às informações. No entanto, a troca e o acesso às informações devem ser feitas estritamente de acordo com os princípios adotados pela Starboard e pelas regras a ela aplicáveis.

A segurança da informação é pautada nos seguintes princípios que devem ser observados por todos os Colaboradores:

- **Confidencialidade**: para garantir que as informações somente serão acessadas por pessoas autorizadas;
- **Integridade**: para garantir que as informações não sofram modificações não autorizadas;
- **Autenticidade**: para garantir que as informações advêm do remetente correto; e
- **Disponibilidade**: para garantir que as informações sejam disponibilizadas em casos autorizados.

Para assegurar a observância de tais princípios, os Colaboradores deverão gerenciar e proteger adequadamente as informações contra roubo, fraude, perdas, vazamentos e outras ameaças.

Por esse motivo, a Starboard solicita que todos os seus Colaboradores leiam as regras indicadas abaixo, assinem o Termo de Ciência, Adesão e Comprometimento (**Anexo I**), e se comprometam a zelar e manter a confidencialidade das informações obtidas, direta ou indiretamente, bem como seguir todos os procedimentos corporativos no exercício de suas atividades profissionais.

3.2. Divisão de informações: SB Restructuring e SB Asset

É estritamente proibida a troca e a disponibilização de informações entre a Starboard Asset Ltda. ("SB Asset") e a Starboard Restructuring Partners Consultoria em Negócios Ltda. ("SB Restructuring") que possam violar as regras da Comissão de Valores Mobiliários ("CVM"), a legislação aplicável ou os princípios estabelecidos nas políticas internas da Starboard. Dessa forma:

- Os arquivos físicos que contêm dados e informações relativas às atividades desenvolvidas pela SB Asset ficarão alocados no seu respectivo espaço físico, de forma que somente os Colaboradores relacionados diretamente à SB Asset, que atuem no âmbito do mercado financeiro e de capitais, terão acesso às informações confidenciais e sigilosas;
- Cada Colaborador terá acesso somente às pastas eletrônicas da rede diretamente relacionadas às atividades desenvolvidas pela área em que atua, através de sua estação

de trabalho individual e de usuário e senha pessoal intransferível;

- O acesso a arquivos que contêm informações sensíveis ou confidenciais é restrito a Colaboradores autorizados;
- É mantido registro dos Colaboradores com acesso a informações confidenciais; e
- Apenas o administrador do sistema e o prestador de serviços de tecnologia da Starboard terão acesso a todas as pastas da rede.

3.3. Regras Gerais para uso das ferramentas de trabalho

Os Colaboradores deverão observar as seguintes regras de uso das ferramentas de trabalho, que são entendidas como todo instrumento fornecido pela Starboard para fins profissionais – como e-mails, computadores, celulares e outros dispositivos:

- Os equipamentos e computadores disponibilizados aos Colaboradores deverão ser utilizados para a estrita finalidade corporativa de interesse da Starboard;
- A realização de *downloads* deve ter estrita ligação com a natureza das atividades desempenhadas pelos Colaboradores e não deve afrontar o dever de confidencialidade ou as regras estabelecidas nesta Política ou no Código de Ética e Conduta;
- Os e-mails corporativos disponibilizados pela Starboard devem ser utilizados exclusivamente para fins corporativos;
- Os e-mails recebidos pelos Colaboradores da Starboard em contas corporativas deverão ter seu conteúdo verificado pelo Colaborador, não sendo admitida, em nenhuma hipótese, a troca, a manutenção ou o arquivamento de mensagens que tenham conteúdo ofensivo, discriminatório, pornográfico, vexatório ou com suspeitas de vírus ou ameaças semelhantes;
- A utilização dos programas de computador utilizados pelos Colaboradores da Starboard deve ser previamente autorizada pelo responsável pela área de Tecnologia da Informação da Starboard;
- O Colaborador deve realizar as atualizações necessárias assim que estas forem disponibilizadas; e
- Os computadores devem ser desligados ao final do dia de trabalho, salvo quando o procedimento seja impeditivo para a realização de atividades profissionais.

Os Colaboradores deverão ler e assinar o Termo de Responsabilidade pela Guarda e Uso dos Equipamentos (**Anexo II**), comprometendo-se a zelar e a mantê-los em perfeito estado de conservação, conforme exposto acima.

3.4. Informações Confidenciais

De acordo com o Código de Ética e Conduta da Starboard, é dever de todos os Colaboradores exercer suas funções de forma ética e comprometida com a confidencialidade necessária aos temas sigilosos tratados na Starboard.

Os Colaboradores devem sempre atuar em defesa dos interesses da Starboard e devem manter sigilo sobre os negócios, operações e informações confidenciais às quais tenham acesso. É considerada "confidencial" qualquer informação que tenha sido obtida em razão de cargo ou função dentro da Starboard, ainda que indiretamente, e que não tenha sido divulgada publicamente. Além disso, devem submeter à aprovação prévia da Área de Riscos e Compliance qualquer fator que represente um potencial risco às atividades, finanças e reputação da Starboard. Sendo assim:

- É proibida a utilização, divulgação e gravação de informações confidenciais para benefício próprio ou de terceiros; e
- É proibida a produção de cópias de dados de um dispositivo de armazenamento para que outro possa ser restaurado, incluindo servidores locais ou remotos, como o *Cloud Microsoft*, por qualquer meio ou forma, de qualquer dos documentos confidenciais fornecidos ao Colaborador ou de documentos que tenham chegado ao seu conhecimento em virtude de sua relação de emprego ou trabalho com a Starboard e que estejam submetidos ao dever de sigilo.

3.5. Regras de Acesso

3.5.1. Acesso às ferramentas e senhas

Cada Colaborador da Starboard, no momento de sua contratação, receberá uma senha para acesso aos computadores, à rede corporativa e ao correio eletrônico corporativo da Starboard. A senha fornecida quando da admissão do Colaborador deverá ser alterada assim que iniciadas as atividades na Starboard.

A senha é secreta, pessoal e intransferível, sendo terminantemente proibida a autorização de uso das senhas por terceiros, ainda que outros Colaboradores.

A criação da senha deve seguir os seguintes parâmetros para garantia de eficácia e de segurança:

- Mínimo 8 (oito) caracteres;
- Mínimo 1 (um) caractere especial (*e.g.* @, #, $, %, etc.);
- Mínimo 1 (uma) letra maiúscula.

Ainda, na criação da senha, sugere-se o cumprimento das seguintes diretrizes:

- Uma senha única para acesso ao sistema, que não seja a mesma utilizada para acesso a outros ambientes protegidos;
- Uso de números aleatórios;
- Uso de grande quantidade de caracteres;
- Uso de diferentes tipos de caracteres embaralhados;
- Evitar uso de dados pessoais, tais como nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones e datas;
- Evitar senhas associadas à proximidade entre os caracteres no teclado, como por exemplo “qwertyuiop” ou “1qaz2wsx”; e
- Evitar palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes etc.

A senha deverá ser alterada em periodicidade a ser estabelecida internamente pelo departamento de Tecnologia da Informação da Starboard.

3.6. Hábitos básicos de segurança

Com o objetivo de gerenciar e proteger adequadamente as informações, é importante que cada Colaborador adote hábitos básicos de segurança, tais como:

- Manter a mesa limpa, sem que documentos com informações confidenciais ou sigilosas estejam expostos;
- Utilizar tela com proteção de senha, pessoal e intransferível, sempre que se ausentar da estação de trabalho;
- Configurar o computador – seja ele laptop ou desktop – para que bloqueie automaticamente após 10 (dez) minutos em estado de ociosidade;
- Armazenar todos os arquivos eletrônicos em locais autorizados e apropriados;
- Descartar adequadamente materiais físicos ou eletrônicos sensíveis, de forma a impedir a leitura por terceiros;
- Evitar o armazenamento de dados pessoais nos sistemas da Starboard; e
- Adotar as necessárias precauções ao falar em público sobre assuntos confidenciais.

3.7. Inspeção, Monitoramento e Testes

Periodicamente, a critério do Diretor de Riscos e Compliance da Starboard, poderão ser realizadas inspeções nos computadores para averiguação de *downloads* impróprios, não autorizados ou gravados em locais indevidos, bem como para a verificação da observância do disposto nesta Política.

Poderão ainda ser realizados testes com o objetivo de detectar, em tempo hábil, anomalias no sistema tecnológico da Starboard, como a presença de usuários, componentes ou dispositivos não autorizados.

Além disso, as mensagens enviadas ou recebidas por meio de e-mails corporativos, seus respectivos anexos, bem como a navegação virtual poderão ser monitoradas, conforme exposto no Código de Ética e Conduta da Starboard e respectivo Termo de Ciência e Monitoramento, especialmente em casos de suspeitas de violações éticas.

3.8. Devolução de documentos

O Colaborador deverá devolver à Starboard todos os documentos a ele fornecidos, inclusive cópias, na data estipulada pela Starboard para entrega ou quando não for mais necessária a manutenção das informações confidenciais para fins corporativos, comprometendo-se a não reter quaisquer reproduções.

As informações confidenciais sobre as quais teve conhecimento ou acesso deverão ser mantidas sob sigilo pelo Colaborador mesmo após sua saída da Starboard.

4. Segurança cibernética

As regras estabelecidas nesta seção foram elaboradas a partir da identificação e da avaliação de riscos cibernéticos ("Avaliação de Riscos") e destinam-se, em adição ao Plano de Continuidade de Negócios de que trata a seção 5, a mitigar e minimizar a concretização de tais riscos previamente identificados pela Starboard.

4.1. Avaliação de Riscos

4.1.1. Visão Geral

A Starboard conduz avaliações de riscos relacionadas a todos os processos e ativos relevantes, incluindo equipamentos, sistemas e dados, necessários ao adequado funcionamento das atividades exercidas pela Starboard, de modo a identificar suas vulnerabilidades e possíveis cenários de ameaça. Uma vez definidos os riscos, ações de prevenção e proteção deverão ser tomadas de acordo com esta Política e conforme orientação da Área de Riscos e Compliance.

4.1.2. Assessment de Segurança

No prazo a ser definido pela Starboard, os Terceiros deverão prestar as informações requeridas pelo **Anexo III** desta Política ("Assessment de Segurança"), a fim de garantir que todos adotem e mantenham vigentes suas respectivas políticas de segurança da informação e cibernética, garantindo maior segurança e confiabilidade.

Os Terceiros devem obrigatoriamente cumprir com todos os requisitos do Assessment de Segurança, bem como garantir a execução das análises de segurança e monitoramento da infraestrutura, seja hardware, software e/ou recursos humanos, demonstrando políticas para contratações, gerenciamento de acessos, seja físico ou remoto, controle de antivírus, firewall, segmentação de rede, criptografia entre outros.

4.2. Proteção e Prevenção

Com o objetivo de proteger e prevenir a concretização dos riscos verificados com a adoção das medidas mencionadas no item acima, a Starboard adota as seguintes ações, em linha com as práticas descritas no plano de continuidade de negócios descrito na seção 5 desta Política, bem como do Plano de Resposta a Incidentes da Starboard:

- instalação de *firewall* para manutenção da segurança nos servidores para acesso aos servidores e sistemas utilizados pela Starboard;
- utilização e constante atualização do sistema de prevenção aos ataques de vírus;
- realização de armazenamento de dados diários de todos os dados, envolvendo as operações diárias, em um servidor local e em servidores remotos no *Cloud Microsoft* ("*Backup*"); e
- instrução dos Colaboradores quanto à correta utilização dos sistemas e servidores da Starboard.

Além disso, cada Colaborador é responsável por proteger seu próprio banco de dados, composto pelas informações, planilhas, e-mails, conversas telefônicas ou por texto com clientes ou outros Colaboradores.

4.2.1. Testes Periódicos

A Starboard deve revisar e realizar testes anuais para monitorar a eficiência e eficácia desta Política. O resultado do teste e da revisão deve, em conjunto com a indicação dos pontos de aperfeiçoamento necessários, ser reportado aos principais sócios executivos da Starboard.

4.3. Plano de Resposta a Incidentes de Segurança

Em caso de incidentes cibernéticos, os Colaboradores deverão seguir o procedimento disposto no Plano de Resposta a Incidentes da Starboard.

5. Plano de Continuidade de Negócios

O presente Plano tem por objetivo estabelecer regras e procedimentos para identificação, mitigação e prevenção de eventuais contingências que possam causar impacto negativo considerável sobre os recursos humanos, materiais e tecnológicos que sejam essenciais para o pleno funcionamento das operações da Starboard e, consequentemente, sobre os interesses de seus clientes ("Contingências").

Para tanto, este Plano estabelece mecanismos com a finalidade de **(i)** proteger a integridade da Starboard e de todos os seus Colaboradores; **(ii)** garantir a guarda e proteção de todos os sistemas, dados, registros e arquivos da Starboard; e **(iii)** permitir a condução das operações da Starboard de forma não-disruptiva.

5.1. Análise de Riscos Potenciais e Mecanismos de Resposta

Como estratégia para preservar a integridade, segurança, qualidade, confidencialidade e acessibilidade dos dados e informações necessários às suas atividades, assegurando sua continuidade operacional em eventos de maior ameaça às operações, a Starboard adota as seguintes medidas:

- Realização de *Backup* em um servidor local e em servidores remotos no *Cloud Microsoft*;
- Manutenção de sistemas operacionais disponíveis em situações de verificação de Contingências, assegurando o acesso remoto dos Colaboradores à rede da Starboard; e
- Disponibilização a todos os Colaboradores das informações referentes aos procedimentos de *Backup* e dos procedimentos para acesso remoto à rede da Starboard.

Adicionalmente, a Starboard possui **(i)** mecanismos e procedimentos que permitem a identificação de potenciais ameaças internas e externas que possam comprometer a continuidade das operações da Starboard, e seus potenciais impactos às operações; bem como **(ii)** uma estrutura organizacional preparada para o gerenciamento de potenciais crises, suportada por níveis adequados de autoridade e competência, de maneira a minimizar ainda mais os impactos de eventuais Contingências em suas atividades.

5.1.1. Principais Contingências Mapeadas

A Starboard considera que as Contingências de maior impacto potencial em suas atividades são:

- Queda de energia elétrica;
- Incêndios;
- Impossibilidade de acesso às instalações físicas;

- Indisponibilidade de acesso à internet;
- Perda de dados, arquivos e documentos;
- Ataques aos sistemas da Starboard por *hackers*;
- Indisponibilidade do servidor de *e-mail*; e
- Indisponibilidade do servidor local.

5.1.2. Ações Mitigadoras

A fim de assegurar a plena continuidade das suas operações, a Starboard adota as seguintes medidas de prevenção e mitigação dos riscos descritos no item 5.1.1 acima:

- O servidor local possui *no-break*, permitindo a manutenção do funcionamento e da integridade de dispositivos eletrônicos em caso de falta de energia ou oscilação da rede elétrica;
- As instalações físicas da Starboard possuem extintores de incêndio munidos de gás carbônico para uso em situações de fogo B e C, cuja manutenção é realizada anualmente;
- Plano de evacuação das instalações físicas;
- *Backup* diário extensivo de todos os aplicativos, programas e registros de *e-mails* armazenados remotamente no *Cloud Microsoft*;
- Digitalização de toda a documentação de importância para o pleno desempenho das atividades da Starboard;
- Manutenção de registro atualizado com todas as senhas de acesso aos softwares utilizados pelos Colaboradores da Starboard;
- Uso de solução de segurança *firewall* nos sistemas da Starboard;
- Possibilidade de os Colaboradores trabalharem remotamente (*home office*), caso necessário, sem prejuízo ao pleno desempenho de suas funções;
- Contrato terceirizado de manutenção de tecnologia da informação (TI) com presença rotineira na empresa e atendimento em casos de necessidade;
- Todos os Colaboradores utilizam *notebooks* individuais, o que garante a portabilidade operacional imediata e independência em eventuais situações de falta de energia;
- Todos os Colaboradores possuem celular com acesso às respectivas contas de *e-mail* corporativas, o que permite a manutenção da plena comunicação profissional mesmo em eventuais situações de falta de energia;
- Redundância no serviço de internet (link de *Backup*), evitando o risco de queda do sistema;
- Treinamento de seus Colaboradores sobre como atuar em situações de verificação de Contingências; e
- Testes de contingência, nos termos do item 5.2 abaixo.

5.2. Testes de Contingência

A Starboard realiza testes de contingências periódicos, a fim de avaliar se as medidas e os procedimentos adotados neste Plano são capazes de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade de negócios da Starboard e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se tais planos podem ser ativados tempestivamente.

Nesse sentido, os testes de contingência serão realizados pela equipe de TI com uma periodicidade mínima de 3 (três) meses, sob a coordenação do Diretor de Riscos e Compliance, que solicitará as seguintes verificações a determinados Colaboradores previamente indicados, sem prejuízo de outras medidas que eventualmente se façam necessárias:

- Acesso aos sistemas;
- Acesso ao *e-mail* corporativo;
- Acesso aos dados armazenados em *Backup*;
- Execução de algumas atividades operacionais chave no ambiente de acesso remoto; e
- Testes dos mecanismos de *no-break*, verificando o status de funcionamento e o tempo de suporte das baterias com carga.

Os resultados dos testes serão registrados em relatório e utilizados para a regularização de eventuais falhas apontadas, bem como para a identificação de pontos de aprimoramento dos procedimentos conduzidos e deste Plano.

5.3. Execução do Plano

Na ocorrência de alguma Contingência, os Colaboradores que dela tomarem conhecimento devem comunicá-la imediatamente ao Diretor de Riscos e Compliance, para que este avalie a gravidade do ocorrido e comunique a situação aos Colaboradores, conforme o caso, iniciando imediatamente as ações necessárias para a preservação das atividades e a retomada da normalidade.

Em razão da natureza das atividades da Starboard, a maioria das potenciais Contingências identificadas se relaciona com a impossibilidade de acesso a arquivos e sistemas de informação, razão pela qual as medidas adequadas para a sua solução serão sempre iniciadas imediatamente após a sua ocorrência. Nesses casos, o Diretor de Riscos e Compliance executará a seguinte sequência de ações:

- Comunicar a ocorrência do evento à equipe de TI contratada, para que dê suporte imediato ao acesso remoto dos Colaboradores a todos os sistemas;
- Validar a integridade dos sistemas e informações; e

- Delegar eventuais ações necessárias adicionais às demais equipes, dando continuidade às operações e atualizando os possíveis dados não recuperados no último *Backup*.

Na hipótese de ocorrência de qualquer Contingência cuja solução demande medidas não previstas neste Plano ou prazos mais extensos, o Diretor de Riscos e Compliance deverá, junto à diretoria da Starboard, definir o plano de ação a ser adotados à luz do caso concreto.

6. Disposições Finais

As normas e procedimento tratados nesta Política serão objeto de treinamento, conforme estabelecido no Código de Ética e Conduta da Starboard.

Todas as informações relacionadas a esta Política e documentação produzida em virtude de disposições aqui expostas devem ser mantidas pelo prazo mínimo de 5 (cinco) anos, ou por prazo superior quando assim determinado expressamente pelas normas legais e regulamentares aplicáveis.

Também deverão ser mantidos pelo prazo mínimo de 5 (cinco) anos toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício das funções da Starboard, sejam eles físicos ou eletrônicos.

Os Colaboradores poderão ser responsabilizados por violações às disposições desta Política e poderão ser objeto de investigação e aplicação das medidas disciplinares estabelecidas no Código de Ética e Conduta da Starboard, bem como eventuais sanções ou indenizações advindas de processos administrativos ou judiciais, conforme o caso.

7. Aprovação e Revisão

A presente Política será revisada pelo Diretor Riscos e Compliance sempre que necessário e, no mínimo, uma vez ao ano, notificando previamente todos os Colaboradores das alterações realizadas.

8. Controle de Versão

Válido a partir de: Maio de 2020
Área responsável: Riscos e *Compliance*
Data da última revisão: Abril de 2024
Versão: 2.1

Anexo I: Termo de Ciência, Adesão e Comprometimento da Política de Segurança Cibernética, Segurança da Informação e Continuidade de Negócios

Por meio deste Termo, declaro que recebi, li e compreendi a Política de Segurança Cibernética, Segurança da Informação e Continuidade de Negócios e, após ler e entender o seu conteúdo, concordo e me comprometo a cumprir todas as regras nela contidas.

Tenho ciência de que a divulgação de informações confidenciais pode ensejar medidas disciplinares contra mim, como advertências, desligamento e até responsabilização civil e criminal, conforme legislação aplicável.

Nome completo: _____

Data: _____

Assinatura: _____

Anexo II: Termo de Responsabilidade pela Guarda e Uso dos Equipamentos

Por meio deste Termo, declaro que recebi da empresa: [STARBOARD ASSET LTDA., CNPJ nº 15.032.609/0001-10 / STARBOARD RESTRUCTURING PARTNERS CONSULTORIA EM NEGÓCIOS LTDA., CNPJ nº 22.606.769/0001-90], a título de empréstimo, para meu uso exclusivo, conforme determinado na lei, os equipamentos especificados neste termo de responsabilidade, comprometendo-me a mantê-los em perfeito estado de conservação, ficando ciente de que:
1- Se o(s) equipamento(s) for(em) danificado(s) ou inutilizado(s) por emprego inadequado, mau uso, negligência ou extravio, a empresa me fornecerá novo equipamento e cobrará o valor de um equipamento da mesma marca ou equivalente ao da praça.

2- Em caso de dano, inutilização ou extravio do(s) equipamento(s) deverei comunicar imediatamente ao setor competente.

3- Terminando os serviços ou no caso de rescisão do contrato de trabalho, devolverei o(s) equipamento(s) completo(s) e em perfeito estado de conservação, considerando-se o tempo do uso do mesmo, ao setor competente.

4- Estando o(s) equipamento(s) em minha posse, estarei sujeito a inspeções sem prévio aviso.

PATRIMÔNIO: _____
MARCA: _____
MODELO: _____

São Paulo, _____de_____, 20__.

Ciente (Nome / Assinatura):_____

Devolução

Atestamos que o bem foi devolvido em ___/___/____, nas seguintes condições:
(__) Em perfeito estado (__) Apresentando defeito (__) Faltando peças/acessórios.

_____
(Data / assinatura / nome do responsável pelo recebimento)