POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES

BLUE STAR ASSET E MANAGEMENT LTDA.
CNPJ/MF 10.757.089/0001-99
NIRE 35223119864

Estas Políticas de Segurança Cibernética e de Segurança das Informações da **BLUE STAR ASSET E MANAGEMENT LTDA.** ("Políticas", ou individualmente, "Política"), sociedade limitada com seu contrato social devidamente arquivado na Junta Comercial do Estado de São Paulo - JUCESP sob o NIRE 35.223.119.864, inscrita no CNPJ/MF sob o nº 10.757.089/0001-99, com sede na Cidade de São Paulo, Estado de São Paulo, na Rua Helena, nº 285, conjunto 112, Vila Olímpia, CEP 04552-050 ("Sociedade" ou "Blue Star") encontram-se sob a responsabilidade de sua respectiva Diretoria de *Compliance*.

POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES

Definição

A Política de Segurança das Informações da Blue Star tem como objetivo estabelecer regras que orientem o controle de acesso a informações confidenciais pelos Colaboradores da Sociedade, inclusive através do estabelecimento de regras para a utilização de equipamentos e *e-mails* da Sociedade, para gravação de cópias de arquivos, para *download* e instalação de programas nos computadores da Sociedade dentre outras.

Disposições

Todos os Colaboradores da Sociedade tomarão conhecimento e expressamente anuirão com o quanto segue:

(i) os arquivos físicos com os dados e informações relativas a cada uma das atividades desenvolvidas pela Sociedade ficarão alocados no respectivo espaço físico de cada uma das áreas. Desta forma, somente os Colaboradores, cujas atividades forem relacionadas com o mercado financeiro e de capitais, terão acesso a informações confidenciais e sigilosas relativas à sua atividade;

(ii) os equipamentos e computadores disponibilizados aos Colaboradores da Sociedade deverão ser utilizados com a finalidade de atender aos interesses

comerciais da Sociedade, sendo permitida a sua utilização para fins particulares de forma moderada;

(iii) a gravação de cópias de arquivos e instalação de programas em computadores da Sociedade deverá respeitar as regras estabelecidas em Capítulo do Manual de Compliance, referente a Política de Sigilo e Confidencialidade;

(iv) *downloads* de qualquer natureza podem ser realizados, desde que de forma ponderada, respeitando o espaço individual de cada usuário. Periodicamente, a critério do Comitê de Compliance e Risco, poderão serão realizadas inspeções nos computadores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos;

(v) o correio eletrônico disponibilizado pela Sociedade ("*E-mails* Corporativos") caracteriza-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo sua utilização preferencial voltada para alcançar os fins comerciais aos quais se destina. É permitida a utilização pessoal de forma moderada;

(vi) as mensagens enviadas ou recebidas por meio de *E-mails* Corporativos, seus respectivos anexos e a navegação por meio da rede mundial de computadores por meio de equipamentos da Sociedade ou dentro das instalações da Sociedade poderão ser monitoradas;

(vii) os *E-mails* Corporativos recebidos pelos Colaboradores da Sociedade, quando abertos, deverão ter seu conteúdo verificado pelo Colaborador, não sendo admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem. Os arquivos de *E-mails* Corporativos poderão ser inspecionados pela Sociedade, a critério do Comitê de Compliance e Risco, a qualquer tempo e independentemente de prévia notificação;

(viii) todos os programas de computador utilizados pelos Colaboradores da Sociedade devem ter sido previamente autorizados pelo responsável pela área de informática da Sociedade. Os computadores podem ser inspecionados pela Sociedade a qualquer tempo para a verificação da observância do disposto na Política de Sigilo e Confidencialidade;

(ix) cada um dos Colaboradores da Sociedade, no momento de sua contratação, receberá uma senha secreta, pessoal e intransferível para acesso aos computadores, à rede corporativa e ao correio eletrônico corporativo da Sociedade;

(x) o acesso a informações confidenciais e sigilosas será restrito e poderá ser diferenciado conforme os níveis hierárquicos e as funções desempenhadas pelos Colaboradores da Sociedade a critério do Comitê de Compliance e Risco. O controle de acesso a tais informações será realizado por meio das senhas pessoais dos Colaboradores, que, a critério do Comitê de Compliance e Risco, poderão respeitar uma ordem de graduação com diferentes níveis de acessibilidade a arquivos, pastas e diretórios da rede corporativa; e

(xi) cada Colaborador terá acesso a pastas eletrônicas diretamente relacionadas às atividades desenvolvidas pela sua área. Apenas o administrador do sistema, o prestador de serviços de tecnologia e os diretores da Sociedade terão acesso a todas as pastas.

Medidas Adicionais

Em complementação aos procedimentos acima, que deverão ser observados por todos os Colaboradores, a Sociedade instalará *firewall* de segurança nos servidores para acesso à sua rede, visando manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados. O sistema de prevenção a ataques de vírus será atualizado diariamente. O *backup* de arquivos será realizado de forma sistemática com unidade de disco externa ao servidor e os *links* são dedicados e seguros.

Adicionalmente, o *backup* de arquivos será feito periodicamente e os dados atualizados serão armazenados em local seguro. Novas tecnologias de solução de back-up, serão estudadas para futuras implementações, conforme necessidade da Sociedade e orientação do Comitê de Compliance e Risco, ouvidos os técnicos de informática e o setor responsável. Através de *software* de monitoramento remoto seguro o prestador de serviços de tecnologia poderá otimizar o controle sobre a rede.

São Paulo, 12 de fevereiro de 2019.

* * *