BARN CONSULTORIA E GESTÃO DE RECURSOS LTDA.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

V001

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

HISTÓRICO DE MODIFICAÇÕES DO DOCUMENTO

Data	Responsável	Versão	Alterações/Inclusões
Julho/2021	Diretor de Compliance e Riscos	001	Criação da Política

A Política de Segurança da Informação ("Política") tem caráter permanente. O conteúdo deste documento poderá ser modificado a qualquer momento de acordo com as necessidades vigentes. Os profissionais da Barn e seus prestadores de serviço deverão, sempre que necessário, consultar a última versão disponível. Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

1. TERMOS GERAIS

A presente Política aplica-se a todos os níveis hierárquicos da Barn: sócios, dirigentes, empregados, consultores, funcionários, trainees, estagiários e prestadores de serviços ("Colaboradores") e todos os Colaboradores estão cientes de que devem conhecer e respeitar todas as normas aqui dispostas, estando cientes de que o descumprimento de tais normas poderá acarretar a imposição pelo Diretor de Compliance e Riscos das seguintes sanções administrativas a depender do grau de gravidade da conduta: (i) assinatura de termo de compromisso; (ii) advertência escrita ou verbal; (iii) censura; (iv) suspensão; ou (v) demissão/término da relação contratual.

A presente Política tem como objetivo central apresentar e disseminar entre todos os Colaboradores da Barn as políticas e os procedimentos definidos pelo Diretor de Compliance e Riscos para garantir a integridade das informações produzidas e gerenciadas dentro do ambiente de trabalho.

A Barn estabelece que é responsabilidade de cada um de seus Colaboradores garantir a total confidencialidade e integridade das informações diariamente produzidas em razão de e/ou no ambiente de trabalho, sendo essencial que todo Colaborador tenha plena consciência acerca de sua importância no processo de garantia do cumprimento dos procedimentos definidos por meio desta Política.

Todos os Colaboradores estão cientes de que toda informação gerada internamente pela Barn e/ou recebida de clientes para o desenvolvimento de trabalhos de qualquer natureza é estritamente confidencial e deve manter-se íntegra durante toda a sua existência. Além disso, os Colaboradores, ao utilizarem qualquer meio eletrônico (chats, Skype, e-mails, internet, entre outros) para o desenvolvimento de suas atividades, devem considerar seu uso como ferramenta de trabalho e, como tanto, de propriedade da empresa para uso profissional e de interesse da organização. A utilização de meios eletrônicos para fins particulares é terminantemente proibida. Vale salientar, ainda, que os acessos a e-mails e à internet, assim entendidos como ferramentas de trabalho de propriedade da Barn, passam por backups diários e poderão ser objeto de auditorias e revisões a qualquer momento, estando à total disposição da administração da empresa.

A responsabilidade do Colaborador e/ou prestador de serviços em questão de confidencialidade e integridade das informações é válida até mesmo após o seu desligamento e deve ser cumprida de acordo com os itens desta Política.

O Colaborador está ciente de que o não cumprimento das disposições acima previstas e dos demais termos desta Política será considerado infração grave, passível de advertência formal e sujeito à imposição de sanções administrativas, as quais, em casos extremos, incluem o desligamento do profissional embasado em legislação vigente, trabalhista ou não. Eventuais violações às disposições previstas nesta Política serão tratadas de maneira individual e levadas imediatamente à avaliação do Diretor de Compliance e Riscos da Barn.

Ciente de que o acesso a informações pessoais recebidas por cada um de seus Colaboradores não pode ser coibido, a Barn cordialmente solicita o não fornecimento de endereços eletrônicos profissionais para fins pessoais. Adicionalmente, a Barn recomenda prudência e cautela para a abertura de arquivos anexos a mensagens eletrônicas e páginas da internet, em especial no que tange a conteúdo inapropriado. O acesso a conteúdo não condizente com o ambiente de trabalho será alvo de investigação e, caso constatado, estará sujeito às sanções cabíveis, conforme parágrafo anterior.

Com o objetivo de garantir maior alinhamento da conduta de todos os seus Colaboradores, este documento abordará alguns itens de maneira direta e específica. Vale salientar, entretanto, que esta Política não deve se restringir aos aspectos tratados a seguir e que eventuais dúvidas e/ou questionamentos devem ser imediatamente levados ao conhecimento do Diretor de Compliance e Riscos da Barn.

2. UTILIZAÇÃO DE SENHAS

A utilização de senhas para acesso às estações de trabalho, correios eletrônicos (e-mails), software e demais dispositivos que se façam necessários é obrigatória, cabendo a cada Colaborador a responsabilidade pelo respectivo resguardo e confidencialidade, não as repassando a terceiros. As senhas deverão possuir validade máxima de 1 (um) ano e podem ser substituídas a qualquer momento por decisão do Diretor de Compliance e Riscos ou por solicitação formal do Colaborador.

3. UTILIZAÇÃO DA INTERNET

Como já explorado anteriormente, a utilização da internet no ambiente da Barn deve restringir-se a assuntos profissionais. Ainda assim, a Barn solicita a cada um de seus Colaboradores que empregue os mais elevados padrões éticos para a utilização deste meio e define as seguintes diretrizes para sua utilização:

(a) a internet não pode ser utilizada como ferramenta para download ou distribuição de software ou dados não legalizados, acesso a páginas de jogos, material pornográfico, sites de compras, sites de relacionamento, entre outros de conteúdo impróprio;

(b) a internet não deve ser utilizada como ferramenta para a divulgação de informações confidenciais em grupos de discussão, Instant Messenger ou “salas de bate papo”, não importando se a divulgação foi deliberada ou inadvertida;

(c) caso a Barn julgue necessário, haverá bloqueios de acesso a arquivos e/ou domínios que possam comprometer o uso de banda ou que impactem o bom andamento dos trabalhos;

(d) a Barn possui controle de todo conteúdo considerado confidencial acessado pelos Colaboradores;

(e) o acesso à internet deve, obrigatoriamente, ser realizado por meio do programa Internet Explorer, ou Google Chrome, ou outro software desde que devidamente homologado pelo Diretor de Compliance e Riscos da Barn; e

(f) as áreas de armazenamento da BARN (DROPBOX) não devem ser utilizadas para arquivamento de itens de natureza pessoal.

4. UTILIZAÇÃO DO CORREIO ELETRÔNICO (E-MAIL)

É proibida a utilização do correio eletrônico para:

(a) envio de mensagens ofensivas, difamatórias, preconceituosas, ou que possam causar hostilidade de qualquer espécie (de conteúdo religioso, sexual, político ou racial), ou que comprometam a imagem da Barn;

(b) envio de mensagens por outros usuários que não os responsáveis pelo login e pela senha de acesso ao sistema;

(c) envio de mensagens que solicitem inscrição em listas de distribuições de mensagens na internet de assuntos não relacionados aos negócios da Barn;

(d) envio de mensagens com o objetivo de prejudicar o serviço de indivíduos e/ou empresas (quantidade ou tamanho excessivo de mensagens, código malicioso etc.);

(e) envio de mensagens que levem o destinatário a incorrer em erro de identificação do emitente (se passar por outra pessoa);

(f) envio de mensagens cujo objetivo seja a venda de serviços e/ou produtos não relacionados aos negócios da Barn;

(g) envio de mensagens, cujo conteúdo seja confidencial ou restrito à Barn e não possa se tornar público;

(h) execução de arquivos anexados a mensagens recebidas de emitentes desconhecidos ou suspeitos;

(i) prática de ato que, de qualquer forma, possa ferir a legislação em vigor, as regras de sigilo bancário e direitos autorais;

(j) prática de ato em contraste com os deveres profissionais e com os interesses da Barn, ou a fim de violar esta Política;

(k) recebimento de arquivos do tipo vídeo (*.avi, *.mpeg, entre outros).

(l) o recebimento de arquivos do tipo "executáveis" (programas) será controlado por programa antivírus contido nos equipamentos de controle de mensagens; e

(m) a assinatura de e-mail será atribuída de forma automática (não é necessário assinar durante a composição da mensagem) e seguirá o seguinte padrão:

Nome do Funcionário
Barn
[telefone]
[e-mail]
[Disclaimer relativo à confidencialidade das informações, devidamente aprovado pelo Diretor de Compliance e Riscos].

5. UTILIZAÇÃO DE SOFTWARE

Tendo em vista que os equipamentos de informática disponibilizados pela Barn se destinam exclusivamente ao desempenho de atividades profissionais, a utilização de software limita-se aos programas aprovados e devidamente homologados pelo Diretor de Compliance e Riscos da Barn. A instalação de arquivos executáveis nas estações de trabalho ou na rede é terminantemente proibida, a não ser em casos em que haja expressa autorização do Diretor de Compliance e Riscos.

6. ACESSO A SISTEMAS, BASES DE DADOS E REDES

O acesso a sistemas, bases de dados e redes é restrito e definido em função do perfil de cada Colaborador da Barn. O detalhamento do perfil de acesso de cada Colaborador (incluindo operadores e eventuais prestadores de serviços) é realizado no momento da contratação e criteriosamente analisado pelo Diretor de Compliance e Riscos para cada caso. A liberação do acesso a qualquer sistema, base de dados ou endereço de rede depende de prévia aprovação do Diretor de Compliance e Riscos.

Diante do exposto acima, ficam aqui estabelecidas as seguintes diretrizes:

(a) tentativas para obtenção de acesso não autorizado (fraude de autenticação de usuário ou segurança de qualquer servidor, rede ou conta) não são permitidas. Inclui-se neste ponto o acesso a dados não disponíveis para o usuário, bem como a tentativa de conexão a servidores ou contas cujo acesso não tenha sido expressamente autorizado e situações que coloquem à prova a segurança de outras redes;

(b) tentativas de interferência nos serviços de qualquer outro usuário, servidor ou rede não são permitidas. Inclui-se neste ponto ataques do tipo “negativa de acesso”, congestionamento em redes, bem como tentativas deliberadas de sobrecarga e/ou invasão de um servidor;

(c) materiais de conteúdo inapropriado (ex.: pornografia) não podem ser expostos, armazenados, distribuídos, editados ou gravados por meio do uso dos recursos computacionais da rede;

(d) a pasta TRANSFERÊNCIA (ou similar) não deverá ser utilizada para armazenamento de arquivos que contenham materiais de natureza sigilosa ou sensível;

(e) a armazenagem de arquivos inerentes às atividades profissionais desempenhadas por cada um dos Colaboradores da Barn nos servidores de arquivos é obrigatória. Tal medida visa assegurar a realização de backups de segurança; e

(f) a varredura simples ou em massa, visando a descoberta de endereços ou portas e/ou qualquer ataque ou tentativa de invasão é terminantemente proibida.

7. UTILIZAÇÃO DAS ESTAÇÕES DE TRABALHO

As estações de trabalho destinam-se exclusivamente ao exercício e ao desempenho de atividades profissionais por cada um dos Colaboradores da Barn. A responsabilidade pela manutenção da integridade física das estações de trabalho cabe a cada um dos Colaboradores da empresa, sendo vedada a realização de qualquer alteração em termos de configuração, sem prévio consentimento por escrito do Diretor de Compliance e Riscos. Da mesma forma, cabe a cada um dos Colaboradores bloquear a respectiva estação de trabalho virtual durante período de ausência, de forma a garantir a total confidencialidade e integridade das informações manipuladas por este.

Cada Colaborador deve manter sua mesa de trabalho limpa e organizada, não deixando papéis de trabalho, relatórios ou qualquer documento confidencial em cima da mesa. Isso também é valido para scanner e impressora, ao utilizar os equipamentos, os documentos escaneados e impressos devem ser retirados imediatamente.

8. UTILIZAÇÃO DE MENSAGEIROS ELETRÔNICOS

Conforme informações apresentadas anteriormente, todo e qualquer dispositivo de mensagens eletrônicas deve ser encarado como ferramenta de trabalho e, como tanto, é de propriedade da empresa e destina-se a assuntos profissionais e de interesse da organização. Por se tratar de ferramenta de trabalho, todos os dispositivos estão sujeitos aos mecanismos de controle impostos pela Barn e terão os respectivos históricos gravados e devidamente arquivados para utilização em caso de necessidades.

Seguindo a mesma linha de atuação imposta aos demais requerimentos definidos por meio desta Política, a utilização de dispositivos de mensagens eletrônicas sem a devida aprovação e liberação por parte do Diretor de Compliance e Riscos e/ou a utilização das ferramentas disponibilizadas pela Barn para a tratativa de assuntos pessoais serão alvo de constante fiscalização e poderão implicar em penalidades aos envolvidos, conforme definição estabelecida pelo Diretor de Compliance e Riscos.

9. PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

Como forma de preservar informações confidenciais detidas pela Barn, seguimos ainda as medidas de segurança abaixo:

(a) Sistema de Armazenamento de Dados. A Barn adota o sistema de servidores remotos da DROPBOX E GOOGLE GMAIL para gerenciar suas informações. Nesse sistema, os arquivos eletrônicos ficam armazenados remotamente em servidores seguros e com redundância. Por meio desse sistema, somente usuários com senha conseguem acessar as informações confidenciais, evitando que pessoas não autorizadas tenham acesso a tais informações. O acesso é feito com uso de senhas pessoais e intransferíveis, com procedimento de verificação em 2 (duas) etapas (login e senha) e

por meio de equipamento (computador, celular, tablet) previamente cadastrado e aprovado. Qualquer atividade na rede é monitorada, identificada (usuário, computador e IP que acessou o sistema), e pode ser revertida ou bloqueada. O sistema possui, ainda, diferentes níveis de acesso aos arquivos, sendo possível realizar restrições de nível de pasta e arquivo o que garante maior confidencialidade das informações e redução do risco de uso indevido dessas. Por fim, o sistema realiza um backup diário das informações armazenadas localmente e redundância no armazenamento das informações e arquivos nos servidores remotos, de modo que na ocorrência de problemas como perda de dados, os arquivos e as informações podem ser recuperados rapidamente dos servidores remotos sem grandes interrupções nas atividades da equipe.

(b) Trituração de Material Confidencial. Documentos considerados sensíveis são triturados previamente ao seu descarte, evitando assim o acesso fraudulento a nossas informações.

(c) Segregação de Informações Decorrentes de Atividades Distintas. A segregação das informações é realizada por meio de restrições ao acesso às informações de um departamento por Colaboradores de outro. Cada departamento possui um diretório próprio de armazenamento de documentos, o qual é acessado por meio de senhas e *logins* individuais.

(d) Testes de Segurança: A contratação, anualmente, de empresa especializada para a realização de testes de segurança e procedimentos para detectar falhas e vulnerabilidades nos sistemas da Barn.

10. CLASSIFICAÇÃO DAS INFORMAÇÕES

A fim de determinar o nível de proteção e garantir a segurança do compartilhamento de informações, a Barn classifica as informações que transitam em seu ambiente físico e eletrônico da seguinte maneira: (a) pública - informação sobre a qual não há restrições quanto à divulgação, acessível a qualquer pessoa sem causar quaisquer consequências danosas aos processos da empresa; (b) interna - informação que a organização não tem interesse de divulgar, cujo acesso por parte de indivíduos externos deve ser evitado. Entretanto, caso esta informação seja disponibilizada, não haverá danos sérios à empresa; e (c) confidencial - informação interna da organização, cuja divulgação pode causar danos financeiros ou à imagem da empresa. A divulgação ainda pode gerar vantagens a eventuais concorrentes e perda de clientes.

A presente Política deverá passar por processo de revisão, ao menos, a cada 2 (dois) anos pelo Diretor de Compliance e Riscos. Eventuais alterações serão prontamente comunicadas a todos os Colaboradores da Barn e disponibilizadas no website da Barn.

Eventuais dúvidas ou questionamentos devem ser diretamente encaminhados ao Diretor de Compliance e Riscos conforme abaixo:
Nome: Sergio Espier Spandri
E-mail: sergio@barninvest.com.br
Endereço: Avenida Nove de Julho, 5017, 12º andar, Jardim Paulista, CEP 01407-903, São Paulo/SP.