Manual de Regras, Procedimentos e Controles Internos

1. DEFINIÇÕES

Os termos empregados neste documento iniciados em letra maiúscula têm os seguintes significados:

"ANBIMA"	Significa a Associação Brasile Entidades dos Mercados Financeiro e de Capitais.
"Código ANBIMA"	Significa o Código ANBIMA de Administração de Recursos de Terceiros.
"Colaboradores"	Significam os sócios, administradores, funcionários, estagiários, menores aprendizes do Grupo VBI e prestadores de serviços alocados no Grupo VBI.
"Comitê"	Significa o Comitê de Compliance e Riscos.
"CVM"	Significa a Comissão de Valores Mobiliários.
"Fundos"	Significam os fundos de investimento geridos pelo Grupo VBI.
"Manual"	Significa o presente Manual de Regras, Procedimentos e Controles Internos.
"Políticas"	Significam as políticas referidas no item abaixo.
"Relatório Anual de Aderência"	Significa o relatório de teste de conformidade realizado anualmente.
"Grupo VBI"	Significa em conjunto VBI, VBI Administração, VBI Asset, VBI Capital, VBI Securities e quando o contexto assim permitir, suas empresas controladas.
"VBI"	Significa a VBI Real Estate Gestão de Carteiras S.A.
"VBI Asset"	Significa a VBI Asset Management Ltda.
"VBI Administração"	Significa a VBI Administração Fiduciária e Gestão Ltda.
"VBI Capital"	Significa a VBI Capital Ltda.
"VBI Securities"	Significa a VBI Securities Ltda.

2. OBJETIVO

No exercício de suas atividades, o Grupo VBI está sujeito à legislação que rege o funcionamento do mercado de capitais brasileiro, especialmente às normas editadas pela CVM.

O objetivo deste Manual é estabelecer regras, procedimentos e controles internos a serem observados como parâmetros nas atividades do Grupo VBI, visando o permanente atendimento às leis e regulamentações vigentes, aos melhores padrões ético e profissional e à adequação das modalidades de investimento e da própria atividade de gestão de carteiras de valores mobiliários.

O conteúdo deste Manual visa a garantir o permanente atendimento às normas, políticas e regulamentações vigentes, bem como disseminar a cultura de controles para garantir o cumprimento das normas estabelecidas pelos órgãos reguladores e autorreguladores, e não tem como objetivo o tratamento exaustivo de toda a regulação aplicável às suas atividades.

2.1. POLÍTICAS

Além das políticas anexas ao presente Manual, o Grupo VBI adota, ainda, os seguintes códigos e políticas, que devem ser observados por seus Colaboradores e que estão disponíveis no sistema Compliasset e em seu website:

(i) Código de Ética e Conduta;

(ii) Política de Gestão de Riscos;

(iii) Política de Rateio e Divisão de Ordens;

(iv) Política de Voto;

(v) Política de Investimentos Pessoais;

(vi) Política de Aquisição e Monitoramento de Ativos de Crédito Privado;

(vii) Política de Aquisição e Monitoramento de Ativos Imobiliários;

(viii) Política de Seleção e Contratação Terceiros em Nome dos Fundos;

(ix) Política de Prevenção à Lavagem de Dinheiro e Combate ao Crime de Financiamento ao

Terrorismo; e

(x) Política de Certificação.

3. ABRANGÊNCIA

As orientações contidas neste Manual e seus Anexos devem ser seguidas por todos os Colaboradores, independentemente do nível hierárquico ou duração da prestação dos serviços, zelando para que todas as normas éticas e legais sejam cumpridas por todos aqueles com quem são mantidas relações de cunho profissional, comunicando imediatamente qualquer violação a equipe de Compliance na forma indicada neste Manual.

4. PERFIL CORPORATIVO GRUPO VBI

O Grupo VBI presta serviços de gestão de carteiras a fundos de investimento locais com foco no setor imobiliário brasileiro e ativos relacionados. As principais áreas de alocação dos recursos no mercado de capitais e no setor imobiliário brasileiro são:

(i) projetos residenciais (residential);

(ii) projetos de habitação para estudantes (student housing);

(iii) projetos de loteamentos (subdivison land);

(iv) projetos de complexos logísticos (industrial);

(v) projetos de shopping centers (retail);

(vi) projetos edifícios comerciais (office); e

(vii) crédito estruturado, instrumentos financeiros de ativos relacionados ao setor imobiliário.

5. SÓCIOS DO GRUPO VBI

Os sócios do Grupo VBI são responsáveis, de forma colegiada, pelas seguintes atividades:

(i) avaliar as propostas de alterações dos controles internos do Grupo VB;

(ii) aprovar as políticas e códigos do Grupo VBI, incluindo aqueles cuja implementação ou atualização sejam recomendados pelo Comitê; e

(iii) garantir a efetividade do gerenciamento do risco de compliance.

6. DIRETOR DE COMPLIANCE

O Diretor de Compliance é responsável pelos controles internos e pelo compliance do Grupo VBI, devendo exercer as seguintes atividades:

(i) auxiliar os sócios do Grupo VBI a assegurar a efetividade dos processos de controles internos e compliance, atuando no gerenciamento efetivo de tais atividades no seu "dia a dia";

(ii) monitorar as atividades do Comitê, garantindo seu adequado funcionamento e o registro em ata das decisões tomadas; e

(iii) monitorar e exercer os controles e procedimentos necessários ao cumprimento das normas aplicáveis.

O Diretor de Compliance se reporta aos sócios do Grupo VBI, tendo autonomia para indagar a respeito de práticas e procedimentos adotados nas suas operações e atividades, devendo adotar medidas que coíbam ou mitiguem os efeitos nelas porventura reputados inadequados, incorretos e/ou inaplicáveis.

7. COMITÊ DE COMPLIANCE

7.1. COMPOSIÇÃO E CONVIDADOS

O Comitê é formado pelos seguintes membros: (i) Diretor de Compliance; (ii) Diretor de Gestão de Risco; e (iii) sócios fundadores do Grupo VBI.

Outros Colaboradores e assessores externos podem ser convidados a se manifestar perante o Comitê, bem como participar das reuniões e discutir as matérias ali tratadas, sem direito a voto.

7.2. FINALIDADE

Fortalecer a cultura "de estar em conformidade com", visando identificar, garantir e controlar a mensuração correta dos riscos, do desempenho do Grupo VBI, da aderência aos controles internos, a observância às normas, políticas e regulamentações vigentes, incluindo as políticas, códigos e instruções do Grupo VBI, da ANBIMA e da CVM, de acordo com os parâmetros, métodos e padrões estabelecidos internamente e pelas autoridades reguladoras e autorreguladoras.

7.3. ATRIBUIÇÕES

(i) orientar a implantação de estruturas de controles que contemplem registros bem documentados, que identifiquem claramente as responsabilidades e autorizações descritas, conforme aplicável;

(ii) analisar a criação de novos controles, bem como melhorias naqueles considerados deficientes e monitorar as correções das eventuais deficiências identificadas;

(iii) acompanhar o desenvolvimento das atividades voltadas para o estabelecimento de novos normativos, cuidando para que estas definam claramente as responsabilidades de cada área, bem como estabeleçam os pontos de controle dos riscos;

(iv) intermediar o relacionamento entre as áreas, resultante de pontos divergentes para o estabelecimento de conformidade;

(v) orientar a adequada segregação de funções e separação de responsabilidades, para evitar o conflito de interesses e para evidenciar pontos de controle;

(vi) monitorar permanentemente o cumprimento das políticas, regras, normas, procedimentos e legislação que regulam os negócios do Grupo VBI, auxiliando na sua implementação, assegurando sempre a preservação da imagem da instituição perante o mercado de modo geral;

(vii) definir ações em caso de denúncias ou informações relacionadas a descumprimento das Políticas e demais normas internas ou obrigações existentes nos termos de normas ou documentos firmados;

(viii) avaliar situações identificadas de não conformidade, além de sanções e punições a violações às Políticas e demais normas internas por Colaboradores, conforme aplicável;

(ix) avaliar a efetividade e a conformidade das Políticas e processos internos;

(x) avaliar e aprovar transações ou contratações que envolvam potenciais conflitos de interesse e forma de mitigar ou resolver referidos conflitos quando relacionadas as Políticas;

(xi) aprovar transações ou contratações que envolvam riscos regulatórios ou reputacionais ou em relação aos quais tenham sido identificados red flags;

(xii) acompanhar as políticas, procedimentos, responsabilidades e definições pertinentes à

estrutura de gestão dos riscos mapeados; e

(xiii) reportar-se diretamente aos sócios do Grupo VBI.

7.4. QUÓRUM

Para a instalação das reuniões do Comitê será necessária a presença de, ao menos, a maioria de seus membros, com presença obrigatória do Diretor de Compliance ou suplente por este indicado. As deliberações serão aprovadas mediante votos afirmativos da maioria dos presentes à reunião.

7.5. PERIODICIDADE DAS REUNIÕES

O Comitê deve se reunir, por convocação de qualquer de seus membros, sempre que necessário, inclusive, sem limitação, na ocorrência de violações às Políticas ou normas interna e/ou alteração de legislação relevantes às atividades do Grupo VBI, observada a periodicidade mínima das reuniões que venha a ser exigida pela regulamentação ou autorregulação aplicáveis.

7.6. FORMALIZAÇÃO DAS REUNIÕES

As reuniões serão formalizadas em ata escrita, com o registro das decisões tomadas. O processo deste registro em ata inclui a redação, verificação, assinatura pelos membros do Comitê e arquivamento do material elaborado. Este arquivo é mantido nos arquivos do Grupo VBI pelo período mínimo de 5 (cinco) anos.

8. VIGÊNCIA E DIVULGAÇÃO

Este Manual e seus Anexos revogam e substituem todas as suas versões anteriores bem como quaisquer outras disposições anteriores em contrário ao disposto neste Manual ou em seus Anexos contidas em quaisquer outros documentos.

Este Manual e seus Anexos serão revisados sempre que oportuno ou obrigatório em virtude de legislação ou regulamentação superveniente.

Este Manual e seus Anexos serão disponibilizados no Sistema Compliasset e no website do Grupo VBI.

9. SEGREGAÇÃO DE ATIVIDADE

O acesso de cada Colaborador é restrito de acordo com a equipe a qual pertence e ao seu nível hierárquico, de forma que apenas os Colaboradores devidamente autorizados terão acesso a sistemas, bem como aos arquivos, diretórios e/ou pastas na rede do Grupo VBI, mediante segregação física e lógica.

As medidas de segregação e proteção incluem, ainda, padrões de definição de senha com complexidade adequada, trilhas de auditorias na rede e nos sistemas utilizados a fim de permitir a identificação das pessoas que tenham acesso a elas, bem como back-up periódico a fim de preservar as informações e garantir sua segurança.

As informações a que os Colaboradores venham a ter acesso em razão do exercício de suas funções não poderão ser transferidas a pessoas não habilitadas, ou que possam utilizá-las de forma indevida, sejam elas outros Colaboradores ou não. Ainda, os Colaboradores não devem compartilhar informações confidenciais em áreas comuns abertas, tais como copa, corredor, elevadores etc.

As reuniões devem ocorrer em salas fechadas, devendo os Colaboradores dispensar especial atenção para não deixar papéis, rascunhos, materiais e apresentações de cunho confidencial em salas de reunião compartilhadas. Ao terminar uma reunião, o Colaborador deve verificar que não há material esquecido, tampouco sistemas abertos, ou qualquer outro dado que possa ser confidencial.

10. COMUNICAÇÃO AOS ÓRGÃOS REGULADORES E AUTORREGULADORES

O Grupo VBI buscará sempre atender as exigências na prestação de obrigações e informações legais aos órgãos reguladores. Toda desconformidade em temas de conduta pessoal e profissional deve ser submetida ao Comitê para conclusão e deliberação dos passos a serem dados a respeito.

11. TREINAMENTOS

O Grupo VBI nos termos da regulamentação e autorregulação vigente realizam treinamentos obrigatórios para todos os Colaboradores em periodicidade no mínimo anual. Cada treinamento será registrado no sistema Compliance ou mediante assinatura de lista de presença, arquivada em pasta digital relacionada ao assunto.

12. RELATÓRIO ANUAL DE ADERÊNCIA

Para verificação dos controles internos, sua efetividade e consistência com a natureza, complexidade e riscos das operações realizadas pelo Grupo VBI, serão realizados testes anuais de aderência, os quais deverão ser formalizados por meio do Relatório Anual de Aderência. O Relatório Anual de Aderência conterá, ao menos, as informações exigidas na regulamentação vigente e ficará disponível para consulta da CVM na sede do Grupo VBI.

O Relatório Anual de Aderência é de responsabilidade do Diretor de Compliance e, após será encaminhado aos sócios fundadores do Grupo VBI, com conteúdo relativo à análise do ano civil imediatamente anterior.

13. ANEXOS

São anexos ao presente Manual os elencados abaixo:

- Anexo I: Termo de Compromisso
- Anexo II: Política de Segurança da Informação
- Anexo III: Plano de Contingência e Continuidade de Negócios
- Anexo IV: Política de Atividades Externas

14. TERMO DE COMPROMISSO

Cada Colaborador receberá um termo individual de compromisso por meio do qual aderirá ao inteiro teor deste Manual e demais Políticas do Grupo VBI, cujo modelo encontra-se no Anexo I a este Manual, que deverá ser assinado pelo Colaborador e entregue ao Departamento Pessoal, no momento de sua admissão.

Este Manual é parte das normas que guiam a relação de trabalho dos Colaboradores, os quais, ao assinar o Termo de Compromisso, concordarão com as regras nele fixadas.

A desobediência a qualquer das normas aqui expostas, além daquelas incluídas no contrato individual de trabalho, será tida como infração contratual, sujeitando o respectivo Colaborador às sanções cabíveis.

Até a máxima extensão permitida por lei, o Grupo VBI não se responsabilizará perante terceiros por Colaboradores que violam a lei ou cometam infrações no desempenho de suas atividades. Caso o Grupo VBI seja penalizado ou tenha prejuízo de qualquer natureza por ações de seus Colaboradores, exercerá o direito de regresso ou indenização em face dos responsáveis.

15. DÚVIDAS, ORIENTAÇÕES E COMUNICAÇÃO DE OCORRÊNCIAS

Em relação a este Manual ou seus Anexos, qualquer solicitação que envolva orientação ou esclarecimento deve ser enviada para o e-mail: compliance@vbirealestate.com ou através do Canal de Denúncia do Sistema Compliasset.

Todos os Colaboradores têm a responsabilidade de informar a equipe de Compliance, por meio do endereço de e-mail acima indicado ou do Canal de Denúncias, quaisquer suspeitas de casos de atividades ilegais, condutas de má-fé, violações às normas, políticas e procedimentos internos, sendo resguardado o sigilo da fonte.

16. HISTÓRICO DE REVISÕES

Segue abaixo um quadro indicando o histórico de revisões do presente Manual:

VERSÃO	DATA DE APROVAÇÃO
1	Julho de 2021
2	Julho de 2024

ANEXO I – TERMO DE COMPROMISSO

Nome:

Doc. de Identidade - Nº: Doc. de Identidade - Tipo: CPF:

Declaro que li integralmente o Manual de Regras, Procedimentos e Controles Internos e anexos ("Manual") do Grupo VBI, o qual está diretamente ligado ao exercício de minhas funções.

De acordo com este termo, comprometo-me a:

(i) adotar e cumprir as diretrizes indicadas no Manual;

(ii) comunicar imediatamente a equipe de Compliance qualquer violação do Manual de que eu venha a ter conhecimento, independentemente de qualquer juízo individual, materialidade ou relevância da violação.

Estou ciente e concordo que meus acessos físicos, lógicos, biométricos, de voz e de imagem podem ser objeto de monitoramento.

Desde já, aceito incondicionalmente atender e cumprir quaisquer novas diretrizes e normas que possam vir a ser considerados partes integrantes do Manual, sem a necessidade de apor assinatura em novo termo de compromisso, bem como, em caso de negligência ou imprudência na aplicação do Manual, tenho total ciência da responsabilidade disciplinar que recairá sobre tal inobservância.

_____, _____ de _____ de 20_____.

_____

Assinatura do Colaborador

ANEXO II
POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

1. DEFINIÇÕES

Os termos empregados neste documento iniciados em letra maiúscula têm os significados indicados no quadro abaixo, ou, caso não estejam aqui definidos, aqueles atribuídos no Manual.

"Equipe de TI"	Significa a equipe responsável pela Tecnologia da Informação do Grupo VBI.
"Informações Confidenciais"	São as informações de propriedade ou referentes ao Grupo VBI ou às suas atividades, seus Colaboradores que não pertencerem ao domínio público e, em especial, as que: identifiquem dados pessoais, patrimoniais ou estratégicos; sejam objeto de acordo de confidencialidade celebrado com terceiros; identifiquem ações estratégicas dos negócios da empresa, seus clientes ou dos portfólios sob gestão, cuja divulgação possa prejudicar a gestão dos negócios ou reduzir sua vantagem competitiva; consistam em informações técnicas, jurídicas ou financeiras, escritas ou arquivadas eletronicamente que digam respeito às atividades do Grupo VBI e que sejam devidamente identificadas como sendo confidenciais, constituam propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral; sejam assim consideradas face a determinação legal, previsão legal e/ou regulamentar; o Colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás) de uso pessoal e intransferível.
"Manual"	Significa o Manual de Regras, Procedimentos e Controles Internos.
"Política"	Significa esta Política de Segurança da Informação.

2. OBJETIVO

A presente Política tem por objetivo descrever a forma de conduta adequada para o manuseio, controle e proteção da informação, ressaltando a vedação à divulgação indevida e aos acessos não autorizados, de forma culposa ou dolosa.

A Política é de entendimento amplo e seu escopo abrange informação veiculada sob qualquer forma, seja escrita, visual ou oral, tanto em situações formais e informais. Independentemente da forma de divulgação, a segurança da informação abaixo descrita deverá ser sempre observada.

3. ABRANGÊNCIA

O conteúdo deste documento deve ser conhecido e obedecido por todos os Colaboradores, sendo responsabilidade de cada um observar e fazer com que os terceiros (incluindo visitantes e prestadores de serviços) que, sob sua responsabilidade, tenham acesso às instalações ou sistemas do Grupo VBI, observem as suas diretrizes e normas.

4. PRINCÍPIOS E DIRETRIZES

A conduta dos Colaboradores quanto à segurança da informação deve sempre se pautar nos princípios e diretrizes elencados abaixo:

4.1 PRINCÍPIOS

(i) Confidencialidade: somente pessoas devidamente autorizadas devem ter acesso às informações mantidas pelo Grupo VBI;

(ii) Disponibilidade: as pessoas autorizadas devem ter acesso à informação sempre que necessário; e

(iii) Integridade: a informação deve ser mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

4.2 DIRETRIZES

(i) somente atividades lícitas, éticas e administrativamente permitidas devem ser realizadas por meio dos sistemas do Grupo VBI;

(ii) toda identificação é única, pessoal e intransferível e é de responsabilidade de cada Colaborador o seu armazenamento adequado e com o mais absoluto sigilo. O uso da identificação é exclusivo para os fins descritos no termo de responsabilidade de cada controle de acesso;

(iii) o Grupo VBI reserva-se o direito de monitorar o tráfego de dados e informações que transitam por sua rede de comunicação;

(iv) para serem considerados seguros, equipamentos, sistemas e periféricos devem ter a homologação da Equipe de TI previamente à sua instalação e/ou uso;

(v) os equipamentos utilizados para o desenvolvimento das atividades do Grupo VBI devem estar sempre atualizados, incluindo sistemas operacionais, antivírus e firewalls, garantindo assim maior proteção às informações inseridas em tais equipamentos;

(vi) devem ser feitas cópias de segurança (back-ups) dos repositórios de dados eletrônicos do Grupo VBI, com atualizações periódicas, conforme os padrões de segurança mais altos disponíveis no mercado;

(vii) é obrigação de todos os Colaboradores notificarem a equipe de Compliance caso presenciem, saibam, ou mesmo desconfiem de qualquer fato que contrarie as normas escritas nesta Política;

(viii) a concessão de acessos às Informações Confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;

(ix) o Colaborador que receber as Informações Confidenciais deverá mantê-las em caráter sigiloso, bem como limitar seu acesso e controlar quaisquer cópias; e

(x) não é permitido alterar qualquer configuração técnica dos softwares que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pela Equipe de TI.

4.3 DIVULGAÇÕES PERMITIDAS

Não caracteriza descumprimento desta Política a divulgação de Informações Confidenciais (i) em função de previsão legal ou regulamentar; (ii) pelo Colaborador, desde que na medida estritamente necessária ao desempenho de suas funções, incluindo, sem limitação, a divulgação a advogados e auditores externos e contrapartes; e (iii) em atendimento a ordens emitidas por quaisquer autoridades regulatórias, autorregulatórias, administrativas, legislativas, judiciárias ou arbitrais competentes.

5. NORMAS DE UTILIZAÇÃO DE INTERNET

Para o Grupo VBI, a internet é classificada como conexão de alto risco, sendo de suma importância que, ao navegar, o usuário saiba que está colocando em risco a confidencialidade, integridade e disponibilidade dos ativos do Grupo VBI.

A Equipe de TI é responsável por monitorar os acessos feitos a sites através de computadores e dispositivos de propriedade do Grupo VBI, para avaliação de eventual mau uso e bloqueio de acesso a sites proibidos.

Os Colaboradores deverão utilizar a internet respeitando uma conduta profissional e ilibada e atender os seguintes requisitos:

(i) devem ser respeitados os meios de controle de acesso à rede e à internet;

(ii) é absolutamente vedada a divulgação, facilitação ou compartilhamento de informações ou dados de interesse do Grupo VBI, sigilosos ou não, em fóruns, listas de discussão, salas de bate papo ou outros meios utilizando a internet;

(iii) é expressamente proibido efetuar upload de qualquer sistema, software ou dados sem autorização da Equipe de TI, exceto para fins legais, regulatórios ou autorregulatórios;

(iv) o download de sistemas e dados da internet deve sempre ser pautado pelo bom senso e com respeito aos contratos de licença, termos de uso e políticas de privacidades aplicáveis, sendo que os Colaboradores deverão consultar a Equipe de TI previamente ao download de qualquer dado ou sistema quando houver dúvida sobre a legitimidade da fonte ou suspeita de contaminação de programas maliciosos;

(v) a Equipe de TI poderá, a pedido da diretoria do Grupo VBI, implementar a geração de relatórios das páginas da internet visitadas, bem como a identificação do respectivo usuário que realizou tal ato;

(vi) o Colaborador é responsável pessoalmente por todas as atividades realizadas com a utilização de seu login, senha e demais dados de acesso;

(vii) o acesso à internet fora do local de trabalho utilizando periféricos ou equipamentos do Grupo VBI deverá ser feito para os fins profissionais, em função de reuniões ou teletrabalho (home office);

(viii) é expressamente proibido o acesso a sites e sistemas a partir de equipamentos e periféricos do Grupo VBI por meio de proxy.

6. NORMAS PARA UTILIZAÇÃO DE E-MAIL

Cada Colaborador será responsável pela conta corporativa de e-mail disponibilizada pelo Grupo VBI e deverá utilizá-la de forma diligente, ética e profissional. Os Colaboradores devem observar as seguintes boas práticas no uso do e-mail:

(i) somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos;

(ii) somente imprimir as mensagens quando necessário;

(iii) no caso de recebimento de mensagens que contrariem as regras estabelecidas pelo Grupo VBI, com título ou anexo suspeito, nunca as repassar, alertando o responsável da sua área e a Equipe de TI, se for o caso;

(iv) ao se ausentar do seu local de trabalho, mesmo que temporariamente, bloquear a estação de trabalho; e

(v) ao sair de férias ou se ausentar por períodos prolongados, o Colaborador deve utilizar o recurso de ausência temporária de *e-mail*.

É absolutamente proibido aos Colaboradores:

(i) o uso do *e-mail* para envio de arquivos e divulgação de Informações Confidenciais, exceto nas hipóteses descritas nesta Política;

(ii) o envio de *spam*, corrente ou demais instrumentos semelhantes;

(iii) o envio de material com conteúdo anônimo;

(iv) o envio de *e-mail* com conteúdo que viole quaisquer políticas internas do Grupo VBI, contenha qualquer ameaça, calúnia, difamação, injúria, extorsão, pedidos ou aceite de propina ou qualquer outro delito previsto na legislação vigente;

(v) o envio de códigos maliciosos de qualquer tipo, como, por exemplo, *trojans*, vírus etc.

(vi) o envio a terceiros, a qualquer título, da lista de endereços de *e-mail*s do Grupo VBI;

(vii) o envio ou abertura de arquivos executáveis recebidos com os seguintes sufixos exemplificativos .exe, .dat, .dll, .com, .bat, .pif, .is, .hta, .src, entre outros;

(viii) o uso de contas particulares de *e-mail* por meio de servidores POP, IMAP, SMTP;

(ix) divulgar propaganda ou anunciar produtos ou serviços particulares pelo *e-mail* corporativo; e

(x) redirecionar caixa de *e-mail* pessoal ou de outros provedores para a sua caixa de *e-mail* corporativa e vice-versa.

O Grupo VBI terá acesso irrestrito ao conteúdo de todos os e-mails enviados e recebidos por seus Colaboradores utilizando a conta corporativa de e-mail.

7. CONTROLE DE SENHAS E LOGINS

Todas as senhas são pessoais, sendo vedado o seu empréstimo. Aplicam-se as mesmas regras às senhas que atendam a mais de um Colaborador.

A senha deverá ser memorizada e não poderá ficar disposta em meios físicos ou na rede.

O Grupo VBI poderá estabelecer determinada periodicidade para troca de senha compulsória.

Em caso de desligamento do Colaborador, os seus acessos (incluindo logins e senhas) aos sistemas internos deverão ser bloqueados pela Equipe de TI.

Os gestores de cada área deverão comunicar ao departamento de TI eventuais alterações de atividades dos Colaboradores sob sua responsabilidade e a necessidade de revisão dos acessos destes em razão de tais alterações.

8. CONTROLE DE ACESSO FÍSICO A INFORMAÇÃO DE DADOS

É expressamente proibido deixar material confidencial ou restrito à vista sobre as mesas ou locais de trabalho após a jornada diária, assim como é vedado deixar informações em quadros nas salas de reuniões após o término da reunião. Ademais, ao usar uma impressora coletiva, o documento impresso deve ser imediatamente recolhido. As impressoras são de uso coletivo para cada área segregada

Todos os materiais com dados e Informações Confidenciais devem ser destruídos, quando aplicável, após sua utilização.

Os Colaboradores deverão destruir os materiais com dados e Informações Confidenciais observando às seguintes técnicas:

(i) Documentos escritos ou impressos devem ser triturados por máquinas apropriadas, ou na falta destes, até ficarem absolutamente ilegíveis e impossibilitados de serem reconstruídos;

(ii) CDs, chips e mídias eletromagnéticas devem ser destruídos fisicamente, se possível triturados ou, na impossibilidade, quebrados em mais de 6 (seis) pedaços; e

(iii) HDs ou partes de periféricos devem ser destruídos por ferramenta perfurocortante, preferencialmente, com o uso de furadeira de impacto.

9. COMPUTAÇÃO EM NUVEM

Os serviços de armazenamento de dados e computação em nuvem contratados pelo Grupo VBI passam por uma seleção interna rígida que avalia a necessidade da terceirização do serviço em questão e a confiabilidade técnica do fornecedor analisado, a fim de garantir que ele possua as qualificações de segurança necessárias.

Os Colaboradores não devem utilizar sistemas de computação em nuvem sem a prévia e expressa aprovação da Equipe de TI.

10. TESTES DE CONTROLES

A efetividade desta Política deverá ser verificada por meio de testes periódicos dos controles existentes, sob responsabilidade da Equipe de TI e reportados à equipe de Compliance. Os testes devem verificar se:

(i) os recursos humanos e computacionais são adequados ao porte e às áreas de atuação;

(ii) há adequado nível de confidencialidade e acessos às Informações Confidenciais, com identificação de pessoas que tem acesso a estas informações;

(iii) há segregação física e lógica;

(iv) os recursos computacionais, de controle e acesso físico e lógico, estão protegidos;

(v) a manutenção de registros permite a realização de auditorias e inspeções.

Anexo A
Termo de Confidencialidade

Nome:
CPF:

Declaro que li integralmente a Política de Segurança da Informação ("Política") do Grupo VBI, o qual está diretamente ligado ao exercício de minhas funções.

De acordo com este termo, comprometo-me a:

(i) manter a confidencialidade de informações que não sejam de domínio público produzidas ou custodiadas pelo Grupo VBI ou que tenha acesso em razão das funções desenvolvidas no Grupo VBI;

(ii) não revelar a qualquer pessoa natural ou jurídica sem que seja expressamente autorizado ou para a consecução de atividades em benefício do Grupo VBI, quaisquer Informações Confidenciais;

(iii) destruir imediatamente qualquer material ou documento que contenha Informações Confidenciais;

(iv) não usar as Informações Confidenciais em benefício próprio ou em benefício de qualquer pessoa natural ou jurídica que não seja o Grupo VBI, e, em nenhum caso, para fins não autorizados; e

(v) informar imediatamente ao Grupo VBI qualquer violação das regras de sigilo e responsabilidade estabelecidas neste Termo ou na Política de que tenha conhecimento, independentemente da existência de dolo, bem como qualquer divulgação ou reprodução de informações abrangidas por este Termo decorrente de exigência por autoridade competente, mediante ordem judicial ou administrativa.

[Local e Data]

_____
Assinatura do Colaborador

ANEXO III
PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

1. DEFINIÇÕES

Os termos empregados neste documento iniciados em letra maiúscula têm os significados indicados no quadro abaixo, ou, caso não estejam aqui definidos, aqueles que lhes são atribuídos no Manual.

"**Plano**"	Significa este Plano de Contingência e Continuidade de Negócios.
"**Sistemas**"	Significam todos e quaisquer sistemas operacionais utilizados pelos Colaboradores da VBI para o desempenho de suas funções.

2. OBJETIVO E ABRANGÊNCIA

Este documento tem como objetivo garantir a continuidade dos trabalhos operacionais e dos negócios do Grupo VBI em situações em que os sistemas operacionais do Grupo VBI estejam inoperantes ou, por algum motivo, os Colaborares estejam impedidos ou impossibilitados de acessar as instalações físicas do Grupo VBI, auxiliando os principais envolvidos no plano de contingência na adoção das ações e dos procedimentos necessários, até que se restabeleçam as condições normais de trabalho e de utilização dos sistemas do Grupo VBI.

A conscientização dos Colaboradores e o conhecimento deste Plano e dos pontos críticos nele mencionados facilitarão o diagnóstico de problemas e suas soluções.

O conteúdo deste documento deve ser conhecido e obedecido por todos os Colaboradores.

3. CONTROLES PREVENTIVOS

O Grupo VBI mantém infraestrutura interna e externa para minimizar os riscos de interrupção de suas atividades, em especial, sem limitação, aqueles descritos nos itens a seguir.

3.1. CONTROLES PREVENTIVOS INTERNOS

(i) back-up diário on-line de todas as informações e configurações de usuários em data center local;

(ii) sistema de controle de acesso às dependências do Grupo VBI;

(iii) data center equipado com controle de acesso, ar-condicionado dedicado, links redundantes de

telecomunicações com operadoras distintas, firewall, antivírus e sistema de back-up em localidade externa; e

(iv) no-breaks para atender o data center e as estações de trabalho.

3.2. CONTROLES PREVENTIVOS EXTERNOS

(i) as informações e versões eletrônicas de documentos referentes a fundos de investimento sob gestão do Grupo VBI estão total ou parcialmente replicados nos repositórios externos dos respectivos administradores e custodiantes; e

(ii) data center externo fornecido por empresa terceira.

4. PROCEDIMENTOS

O Plano prevê a adoção de procedimentos periódicos e pontuais para a prevenção e enfretamento de contingências, conforme indicados abaixo.

4.1. PROCEDIMENTOS PERIÓDICOS

(i) anualmente, e sempre que necessário, em virtude de novas atividades ou sistemas identificação e reavaliação de posições, sistemas críticos e potenciais riscos; e

(ii) anualmente realização de testes do Plano.

4.2. PROCEDIMENTOS DE RESOLUÇÃO DE CONTINGÊNCIA

Nesta ordem:

(i) ao constatar a ocorrência de incidente, o Colaborador deverá comunicar a Equipe de TI que, por sua vez, comunicará a Equipe de Compliance, conforme gravidade do ocorrido a esse respeito que comunicará o Comite;

(ii) o Comitê deverá decidir sobre o acionamento do Plano e, em caso positivo, as respectivas medidas de atuação para continuidade das operações;

(iii) a Equipe de TI em conjunto com a Equipe de Compliance comunicará os Colaboradores sobre as medidas a serem adotadas enquanto durar o incidente e, oportunamente, o plano de retomada das atividades;

(iv) após a conclusão da ocorrência a Equipe de TI informará a Equipe de Compliance causa do incidente, caso a origem não seja imediatamente aparente, bem como deverá reportar as medidas adotadas em resposta à ocorrência e o seu grau de êxito;

(v) a Equipe de Compliance informará o Comite que, diante das informações reportadas, avaliará a necessidade de realização de novos testes e adequação do Plano.

5. ANÁLISE PREVENTIVA

A Equipe de TI realizará testes periódicos incluindo a probabilidade de interrupção ou mau funcionamento dos Sistemas (locais e externos), equipamentos de fornecimento de energia elétrica (inclusive *no-breaks*) e telefonia; e (ii) administração predial os riscos referentes às instalações físicas do Grupo VBI.

Na hipótese de qualquer teste identificar uma potencial falha, a Equipe de TI deverá notificar imediatamente a Equipe de Compliance que por sua vez avaliará a necessidade de convocar e informar o Comitê para analise de correção preventiva.

6. AÇÕES CORRETIVAS

Exemplificativamente, a Equipe de TI poderá adotar as medidas descritas abaixo em resposta à ocorrência de incidentes. Outras medidas poderão ser identificadas pela Equipe de TI e comunicadas a Equipe de Compliance e conforme o caso ao Comite.

6.1. FALHA DE SISTEMA TOTAL

Hipótese na qual todos os Sistemas estão afetados. A Equipe de TI deverá verificar o diagnóstico de "pane geral", proceder ao desligamento e religamento geral, e verificar se a situação persiste. Caso a situação persista, a Equipe de TI deverá avaliar com a Equipe de Compliance a melhor forma de restaurar os Sistemas e necessidade de convocação do Comite.

6.2. FALHA DE SISTEMA PARCIAL

Hipótese na qual alguns Sistemas estão afetados. A Equipe de TI deverá identificar quais os Sistemas estão afetados, diagnosticar causas e identificar possíveis soluções e competências de intervenção técnica.

6.3. FALHA DE ENERGIA ELÉTRICA

No prazo de 4 (quatro) horas após o início da falta de energia elétrica, a Equipe de TI deverá identificar a abrangência e possíveis causas localizadas, procedendo:

(i) em caso de problema local, viabilizar solução imediata;

(ii) caso o problema não seja local e uma solução imediata não seja viável, os Colaboradores deverão ser orientados a trabalhar remotamente (*home office*).

6.4. FALHAS DE TELEFONIA

A Equipe de TI deverá, conforme a necessidade, requisitar o atendimento da operadora de telefonia e os Colaboradores deverão ser orientados a adotar as seguintes medidas alternativas ao atendimento telefônico:

(i) em caso de intermitência ocasionada por falta de energia:

(a) os Colaboradores poderão continuar o atendimento enquanto durar a autonomia garantia pelo *no-break* (aproximadamente 4 (quatro) horas); e

(b) em caso de falta de energia por maior tempo, os Colaboradores deverão usar a rede celular, bem como deverão realizar o desvio de chamadas da linha fixa para a linha móvel ou para outros Colaboradores não afetados.

(ii) em caso de interrupção da telefonia fixa:

(a) os Colaboradores deverão usar a rede celular para realizar os atendimentos, bem como deverão realizar o desvio de chamadas da linha fixa para a linha móvel ou para outros Colaboradores não afetados.

6.5. FALTA DE DADOS OU INFORMAÇÕES ORIUNDAS DOS PROVEDORES DE INFORMAÇÕES

A Equipe de TI deverá entrar em contato com os provedores, na maior brevidade possível, identificando causas e possíveis contribuições de restabelecimento de sinais.

6.6. LIQUIDAÇÃO FINANCEIRA – BANCOS E FORNECEDORES

(i) em virtude da impossibilidade de acesso ao escritório:

(a) os Colaboradores deverão utilizar o acesso aos bancos via *internet banking*, se disponível; e

(b) os Colaboradores autorizados via acesso remoto ao servidor do Grupo VBI deverão trabalhar remotamente (*home office*).

(ii) em virtude de falta de energia:

(a) os Colaboradores poderão continuar o atendimento enquanto durar a autonomia garantia pelo no-break (aproximadamente 4 (quatro) horas); e

(b) os Colaboradores autorizados via acesso remoto ao servidor do Grupo VBI deverão trabalhar remotamente (home office).

ANEXO IV
POLÍTICA DE ATIVIDADES EXTERNAS

1. DEFINIÇÕES

Os termos empregados neste documento iniciados em letra maiúscula têm os significados indicados no quadro abaixo, ou, caso não estejam aqui definidos, aqueles atribuídos no Manual.

"Atividades Externas"	Significa atividades exercidas pelos Colaboradores, com ou sem fins lucrativos, em qualquer organização, grupo ou sociedade da qual o Grupo VBI não seja acionista ou cotista e a atividade não seja relacionada com a função desenvolvida pelo Colaborador. Isso inclui, mas não se limita, as seguintes atividades: (i) Emprego externo; (ii) Participação em conselhos ou comitês de empresas ou organizações; (iii) Propriedade ou participação ativa em um negócio privado; (iv) Envolvimento ou atividade significativa cívica ou caritativa; (v) Qualquer outra atividade que possa atingir a imparcialidade do Colaborador.
"Política"	Significa esta Política Atividades Externas.

2. OBJETIVO

Mitigar os riscos atrelados ao exercício de determinadas atividades externas, tais como o risco de conflitos de interesse, risco de induzir clientes a erro ou mesmo risco reputacional, legal ou regulatório, o Grupo VBI divide as atividades externas em 3 (três) categorias: (i) atividades externas isentas de comunicação ou aprovação; (ii) atividades externas que necessitam aprovação; e (iii) atividades externas proibidas.

3. ATIVIDADES EXTERNAS ISENTAS DE COMUNICAÇÃO OU APROVAÇÃO

As atividades externas descritas abaixo não precisam ser comunicadas nem, tampouco, aprovadas:

- Empregos externos voltados à docência;
- Participação em equipe esportiva, exceto clubes de futebol de destaque nacional;
- Atividade artística recreativa;

- Grupo musical.

4. ATIVIDADES EXTERNAS QUE NECESSITAM DE COMUNICAÇÃO E APROVAÇÃO

- Ocupação de cargos de direção ou outros cargos em quaisquer sociedades, incluindo companhias de capital aberto;
- Participação em Conselho de Administração ou Fiscal ou Comitês ou quaisquer dos órgãos de administração, ou com funções técnicas e consultivas em companhia aberta;
- Vínculos empregatícios com outras instituições, empresas ou pessoas;
- Atividades de consultoria ou prestação de serviços de qualquer natureza, tais como consultorias jurídicas, palestras e confecção de artigos para mídia pública (neste caso atentar para as políticas internas de contato com a mídia e publicação de material); e
- Quaisquer atividades não descritas em um dos campos desta Política.

5. ATVIDADES EXTERNAS PROIBIDAS

- Cargo, emprego ou função em um concorrente ou em outro participante do mercado;
- Ocupação em cargos, emprego ou função políticos ou públicos;
- Atividades que possam expor a imagem do Grupo VBI (ex.: participação em reality shows, programas de rádio e TV); e
- Atividades voltadas ao público adulto.

6. PROCESSO DE COMUNICAÇÃO E APROVAÇÃO

Para as atividades que necessitem de comunicação e aprovação, a comunicação deverá ser feita através do e-mail compliance@vbirealestate.com ou do Canal de Compliance do Sistema Compliasset e deverá trazer as seguintes informações:

- **Nome do Colaborador;**
- **Área de Atuação dentro do Grupo VBI;**
- **Superior imediato; e**
- **Descritivo da atividade externa.**

Colaboradores devem, ainda, solicitar aprovação para toda e qualquer nova atividade externa a ser desenvolvida que dependa de aprovação, ainda que na mesma empresa ou instituição já previamente aprovada.

O Comite fará análise do caso e, desde já deixa claro que poderá negar a aprovação de atividades externas sempre que entender, a seu exclusivo critério, que tais atividades representem riscos ou

conflito de interesses do Grupo VBI. Da mesma forma, o Grupo VBI poderá solicitar o imediato término de atividades externas.