

**MANUAL DE COMPLIANCE**

**H2 ASSET MANAGEMENT LTDA.**

**São Paulo – 26 de janeiro de 2026 – v.02/2026**

1. O presente Manual de Compliance (o “**Manual de Compliance**”) da H2 Asset Management Ltda. (a “**Sociedade**” ou “**H2**”), dispõe acerca das políticas estabelecidas pela Sociedade, tendo como objetivo instituir as regras e controles internos alinhados às melhores práticas de mercado.
2. Este Manual aplica-se a todos os diretores, empregados e prestadores de serviços (com habitualidade) (“**Colaborador**” ou, em conjunto, “**Colaboradores**”) da Sociedade, em plena conformidade com a Resolução CVM nº 21 (a “**RCVM 21**”), de 25 de fevereiro de 2021, devidamente atualizada. O Manual tem seus capítulos estruturados por pertinência temática, conforme divisão abaixo especificada:
  - **Capítulo 01** (fls. 03–05): Política de Sigilo, Confidencialidade e Propriedade Intelectual
  - **Capítulo 02** (fls. 06-10): Política de Segurança Cibernética da Informação
  - **Capítulo 03** (fls. 11-12): Política de Treinamentos
  - **Capítulo 04** (fls. 13-20): Política de Regras e Procedimentos de Compliance
  - **Capítulo 05** (fls. 21-27): Plano de Contingência e Continuidade dos Negócios
  - **Capítulo 06** (fls. 28-29): Plano de Certificação
3. Todos os Colaboradores da Sociedade deverão respeitar as regras estabelecidas nos termos do presente Manual de Compliance. Para isto, cada Colaborador deverá firmar um Termo de Adesão, anexo a este Manual de Compliance na forma do “**Anexo I**”, atestando expressamente seu conhecimento acerca das políticas aqui estabelecidas, comprometendo-se a cumprir as regras determinadas.
4. O presente Manual deve ser lido em conjunto com as demais políticas e manuais aprovados e/ou aderidos pela Sociedade.
5. A H2 disponibiliza o seguinte canal de denúncia, que poderá ser utilizado por qualquer Colaborador ou qualquer terceiro em relação à denúncia sobre uma violação ao presente Manual: [canaldedenuncia@h2-asset.com.br](mailto:canaldedenuncia@h2-asset.com.br)

## CAPÍTULO 01

### POLÍTICA DE SIGILO, CONFIDENCIALIDADE E PROPRIEDADE INTELECTUAL

1. A presente política dispõe acerca da política de sigilo e confidencialidade e de propriedade intelectual (“**Política de Sigilo, Confidencialidade e Propriedade Intelectual**”) da Sociedade tendo como objetivo estabelecer regras de sigilo, confidencialidade e propriedade intelectual que se aplicam a todos os Colaboradores da Sociedade.
2. **Objetivo.** As regras estabelecidas nesta Política de Sigilo e Confidencialidade visam resguardar a Sociedade e seus clientes da divulgação de informações confidenciais obtidas por meio da atividade de administração de ativos e carteiras de valores mobiliários, bem como da divulgação, utilização por terceiros, alienação ou cessão de negócios, projetos, técnicas, materiais, planilhas, formulários, projetos, desenvolvimentos de estratégias, produtos ou serviços que constituem propriedade intelectual da Sociedade.
3. Para fins da presente Política de Sigilo, Confidencialidade e Propriedade Intelectual, serão consideradas:

“**Informações Confidenciais**”: Todas e quaisquer informações e/ou dados de natureza confidencial, incluindo, sem limitação, todas as informações técnicas, financeiras, operacionais, econômicas, bem como demais informações comerciais, *know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador, organização societária, situação financeira, informações relacionadas a estratégias de investimento, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela H2, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridos pela H2, as informações sobre os créditos e ativos integrantes da carteira de fundos geridos pela Sociedade, inclusive seus devedores e garantias, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Sociedade, seus sócios e clientes, bem como os dados pessoais dos clientes e quaisquer cópias ou registros dos mesmos, contidos em qualquer meio físico ou eletrônico, que tenham sido direta ou indiretamente fornecidos ou divulgados em razão da atividade de administração de ativos desenvolvida pela Sociedade, mesmo que tais informações e/ou dados não estejam relacionados diretamente aos serviços ou às transações aqui contempladas.

“**Informações não confidenciais**”: As Informações Confidenciais não incluem informações que: (a) sejam ou venham a se tornar de domínio público sem violação do disposto nesta Política de Sigilo e Confidencialidade; ou (b) tenham sido recebidas de boa-fé pelo Colaborador, de terceiros que tenham o direito de divulgá-las, sem obrigação de confidencialidade.

4. Nesse sentido, todos os Colaboradores da Sociedade, ao firmar o Termo de Adesão anexo ao presente Manual de Compliance na forma do Anexo I, deverão tomar conhecimento e expressamente anuir com o quanto segue:
- (i) os Colaboradores expressamente obrigam-se a manter o sigilo das Informações Confidenciais que lhes tenham sido transmitidas, fornecidas e/ou divulgadas sob ou em função de seu vínculo com a Sociedade ou de relacionamento com clientes da Sociedade, comprometendo-se a não utilizar, reproduzir ou divulgar as referidas Informações Confidenciais, inclusive a pessoas não habilitadas ou que possam vir a utilizá-las indevidamente em processo de decisão de investimento próprio ou de terceiros, exceto mediante autorização expressa e escrita do respectivo titular e da Sociedade e na medida do estritamente necessário para o desempenho de suas atividades e/ou obrigações;
  - (ii) todos os negócios, técnicas, materiais, planilhas, formulários, projetos, desenvolvimentos de estratégias, produtos ou serviços elaborados, desenvolvidos e/ou utilizados pela Sociedade e/ou por seus clientes, mesmo que tenham significativa participação de qualquer Colaborador, sempre serão de propriedade da Sociedade, sendo vedado a qualquer Colaborador divulgá-los, utilizá-los para si ou terceiros, cedê-los ou aliená-los, seja a que título for.
  - (iii) os Colaboradores expressamente reconhecem ser de propriedade da H2 todos os direitos autorais e/ou intelectuais existentes e advindos de projetos, técnicas, estratégias, materiais, planilhas, formulários, desenvolvimentos de contratos ou serviços, métodos e/ou sistemas atualmente existentes ou que vierem a ser desenvolvidos durante seus respectivos vínculos com a Sociedade, nada podendo vir a reclamar a esse título;
  - (iv) caso qualquer Colaborador seja obrigado a divulgar Informações Confidenciais por determinação judicial ou de autoridade competente, o Colaborador deverá comunicar para a Sociedade da existência de tal determinação previamente à divulgação e se limitar estritamente à divulgação da Informação Confidencial requisitada;
  - (v) para os propósitos do disposto na Política de Sigilo e Confidencialidade, caberá ao Colaborador o ônus de provar o caráter não confidencial de qualquer informação;
  - (vi) o acesso às Informações Confidenciais será restrito e poderá ser diferenciado conforme os níveis hierárquicos e as funções desempenhadas pelos Colaboradores da Sociedade, a critério do Diretor de Compliance. O controle de acesso a tais informações será realizado por meio das senhas pessoais dos Colaboradores, que, a critério do Diretor de Compliance, poderão respeitar uma ordem de graduação com diferentes níveis de acessibilidade a arquivos, pastas e diretórios da rede corporativa;
  - (vii) a obrigação do Colaborador de observar as regras previstas na presente Política de Sigilo e Confidencialidade será válida mesmo após o término do vínculo dele com a H2, estando sujeito a responsabilização na esfera cível e penal; e

(viii) em caso de término do vínculo do Colaborador com a Sociedade, este deverá restituir imediatamente para a Sociedade todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder.

5. Ao firmar o Termo de Adesão, anexo ao presente Manual de Compliance na forma do **Anexo I, cada um dos Colaboradores expressamente toma ciência que poderá responder civil e criminalmente pelo descumprimento de qualquer regra estabelecida nesta política**, o que ensejará a imediata propositura das medidas cíveis e criminais cabíveis por parte da Sociedade, nas quais poderá, inclusive, ser pleiteados perdas e danos, lucros cessantes, danos morais, bem como a aplicação de qualquer outra penalidade e/ou ressarcimento ou pagamento de valores, seja a que título for.
6. Além das Informações Confidenciais, os Colaboradores também devem manter em absoluto sigilo e observar as regras estabelecidas na presente política sobre as informações privilegiadas, compreendidas, como qualquer informação relevante a respeito de uma companhia, que não tenha sido divulgada publicamente e que seja obtida de forma privilegiada pelo Colaborador em decorrência da relação profissional ou pessoal mantida com um cliente, com pessoas vinculadas a empresas analisadas ou investidas ou com terceiros, em razão da função exercida na H2.
7. Caso tenham conhecimento de que qualquer Colaborador tenha infringido a presente política, os demais Colaboradores obrigam-se a reportar tal falta ao Diretor de Compliance, sob pena de ser considerado corresponsável com o infrator.
8. Quaisquer terceiros contratados que, em razão do vínculo com a Sociedade, vierem a ter acesso às Informações Confidenciais, deverão firmar o termo de confidencialidade atestando o conhecimento acerca da presente Política de Sigilo, Confidencialidade e Propriedade Intelectual.
9. A H2 pode tratar dados Pessoais com finalidade diversas, sendo elas, exemplificativamente, (i) a execução de contratos, (ii) cumprimento de obrigações legais ou regulatórias, ou (iii) para atender seus legítimos interesses ou de terceiros. Nos termos da Lei nº 13.709, de 14 de agosto de 2018 (“**LGPD**”), todos os tratamentos de dados pessoais serão enquadrados em base legal para tratamento, sendo inclusive requerido o consentimento do titular, nos casos aplicáveis.
10. Nos termos da legislação aplicável, no que diz respeito ao tratamento de dados, a H2 garante ao titular a apresentação de solicitações baseadas nos seguintes direitos, sempre que atuar como controlador:
  - i confirmação da existência de tratamento dos dados em conformidade com a LGPD;
  - ii acesso aos dados;
  - iii correção de dados incompletos, inexatos ou desatualizados;

- iv anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
  - v portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
  - vi eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no artigo 16 da LGPD;
  - vii informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
  - viii informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e
  - ix revogação do consentimento, nos termos do § 5º do artigo 8º da LGPD.
11. Todos os dados pessoais serão guardados em base de dados próprias da H2, ou em base de dados mantidas por fornecedores de serviços contratados. Em ambos os casos, serão adotadas medidas de segurança de acordo com a legislação aplicável, com o intuito de preservação dos dados pessoais dos titulares, conforme orienta esta política.
12. As informações coletadas poderão ser compartilhadas pela H2 com os terceiros listados abaixo, respeitado os limites estabelecidos na legislação aplicável:
- i demais empresas do H2, incluindo empresas não domiciliadas no Brasil, as quais se comprometam a utilizar as informações confidenciais nos termos e finalidades aqui descritos;
  - ii para proteção dos interesses da H2 em qualquer tipo de conflito;
  - iii eventuais Colaboradores contratados pela H2;
  - iv no caso de transações e alterações societárias envolvendo a H2, hipótese em que a transferência das informações será necessária para a realização da transação assim como continuidade dos serviços; ou
  - v mediante decisão judicial, administrativa ou solicitação de autoridade competente.
13. O Diretor de Compliance visará promover a aplicação da presente Política de Sigilo, Confidencialidade e Propriedade Intelectual, bem como o controle, a supervisão e a aprovação de exceções em relação à mesma, sendo sua responsabilidade assegurar a implementação de mecanismos eficientes capazes de resguardar o sigilo das Informações Confidenciais, bem como a identificação de quaisquer infrações às regras aprovadas na forma da presente Política de Sigilo, Confidencialidade e Propriedade Intelectual.

## CAPÍTULO 02

### POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

1. A presente política dispõe acerca da política de segurança cibernética e da informação (“**Política de Segurança Cibernética e da Informação**”) da Sociedade, tendo 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.
2. Nesse sentido, todos os Colaboradores da Sociedade firmarão o Termo de Adesão anexo ao presente Manual de Compliance na forma do Anexo I, tomando conhecimento e expressamente anuindo com o quanto segue:
  - (i) os arquivos físicos com os dados e informações relativos à atividade de gestão de fundos de investimento desenvolvida pela Sociedade ficarão alocados na sede social da Sociedade, sendo que apenas os Colaboradores, cujas atividades forem relacionadas com a gestão, terão acesso às informações confidenciais e sigilosas relativas à sua atividade;
  - (ii) os equipamentos, softwares, programas 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 apenas de forma moderada e caso necessário;
  - (iii) não é permitido salvar cópia de informações confidenciais em computadores pessoais ou outros dispositivos eletrônicos que não sejam disponibilizados pela Sociedade, a não ser com a expressa autorização do Compliance;
  - (iv) apenas os equipamentos, programas e softwares disponibilizados e/ou homologados autorizados pela H2 podem ser instalados e conectados à rede;
  - (v) *downloads* de qualquer natureza podem ser realizados, desde que de forma ponderada, respeitando o espaço individual de cada usuário. Periodicamente, a critério do Diretor de Compliance, poderão ser realizadas inspeções nos computadores para averiguação de *downloads* impróprios, não autorizados ou gravados em locais indevidos, sem qualquer comunicação ou anuência prévia do respectivo Colaborador;
  - (vi) 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 apenas de forma moderada;

- (vii) 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, não sendo necessária outra anuência ou comunicação prévia;
  - (viii) 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, ilegal, 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 Diretor de Compliance, a qualquer tempo e independentemente de prévia notificação;
  - (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, que será imediatamente desativada no caso de desligamento do respectivo Colaborador;
  - (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 Diretor de Compliance. O controle de acesso a tais informações será realizado por meio das senhas pessoais dos Colaboradores, que, a critério do Diretor de Compliance, poderão respeitar uma ordem de graduação com diferentes níveis de acessibilidade a arquivos, pastas e diretórios da rede corporativa;
  - (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;
  - (xii) todos os computadores devem ter um antivírus atualizado e rodando o tempo todo e, em caso de não funcionamento do software antivírus instalado em cada computador, é obrigação do usuário notificar prontamente a equipe responsável para solução do problema; e
  - (xiii) a senha da rede de internet principal da H2 e das respectivas camadas de segurança são mantidas de forma segura e não são compartilhadas com todos os usuários.
3. Os Colaboradores são proibidos de comentar, publicar ou discutir assuntos referentes à Sociedade, seus clientes e sócios, ou prestar informações estratégicas, inclusive de investimento, em qualquer meio de comunicação das mídias sociais, sem a aprovação prévia e formal do Diretor de Compliance.
4. As combinações de login e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte restrita da rede da H2 necessária ao exercício de suas atividades.



Assim, cada login está vinculado a uma senha única, de forma que todas as atividades realizadas por tal Colaborador ficarão registradas e poderão ser monitoradas para fins de averiguar quaisquer condutas suspeitas.

5. As senhas para acesso aos computadores, e-mails e arquivos confidenciais devem ser criadas de acordo com as orientações e recomendações dos profissionais especializados na área de tecnologia da informação contratados pela Sociedade.
6. Os Colaboradores da Sociedade devem dispensar especial atenção ao abrir anexos enviados por e-mail, devendo certificar a procedência do documento ainda que o remetente seja conhecido.
7. Todas as instalações da Sociedade são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade de todas e quaisquer informações.
8. O acesso de terceiros à H2 somente é permitido na recepção e na sala de reunião. O acesso físico a áreas em que informações confidenciais ou proprietárias possam estar presentes ou ser discutidas é limitado e restrito aos Colaboradores da respectiva área. As reuniões com terceiros não poderão ser conduzidas nas salas dos Colaboradores e quaisquer trabalhos em projetos confidenciais deverão ocorrer em áreas fisicamente separadas e seguras.
9. As estações de trabalho são fixas, com computadores seguros e as sessões abertas devem ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.
10. É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Sociedade e circulem em ambientes externos à H2 com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais.
11. A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da H2. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.
12. Todo Colaborador que tiver acesso aos sistemas de informação da Sociedade é responsável por tomar as precauções necessárias a fim de impedir o acesso não autorizado aos sistemas. O Colaborador deve manter em local seguro suas senhas e outros meios de acesso aos sistemas, e não divulgá-los a terceiros em qualquer hipótese.

13. O ativo de maior valor da Sociedade são as Informações Confidenciais e privilegiadas da própria H2, dos seus clientes, dos ativos que compõe a carteira dos fundos de investimentos geridos pela Sociedade e eventualmente de outras companhias as quais a Sociedade, seus clientes ou sócios tenham vínculo, por isso, os sistemas de segurança visam preservar o sigilo dessas informações.
14. O Diretor de Compliance é a pessoa responsável na Sociedade para tratar sobre as questões da presente política. Caso seja verificada necessidade, serão contratados terceiros especializados nesta área para, juntamente com o Diretor de Compliance, analisar no caso concreto a vulnerabilidade, ameaças e impactos sobre os ativos de informação da H2, sendo realizadas as recomendações de proteções adequadas.
15. O backup se dará da seguinte forma: (i) para a garantia do backup das informações da H2, estas devem ser armazenadas nos servidores de armazenamento; (ii) não haverá garantia de back-up para arquivos armazenados nas estações de trabalho; (iii) o backup de dados armazenados nos servidores em nuvem é realizado de forma automatizada de tempos em tempos, conforme política do prestador de serviço (Dropbox); (iv) o backup é armazenado automaticamente nos servidores de armazenamento do fornecedor; (v) o *restore* de dados deve ser solicitado aos profissionais contratados para a execução dos serviços de informática e será realizado de acordo com os procedimentos específicos do mesmo, de acordo com a política de armazenamento e *restoring* do serviço contrato do provedor de armazenamento de dados.
16. Serviços de armazenamento de código de linguagem computacional se utilizado pela equipe de gestão será realizado através de serviços em nuvem, com backups realizados automaticamente, seguindo o mesmo procedimento descrito acima. O versionamento de código e as alterações serão mantidos em softwares específicos, que permitem verificar qualquer alteração e realizar *rollback* para versões anteriores, se necessário.
17. Novas tecnologias de solução de *backup*, serão estudadas para futuras implementações, conforme necessidade da Sociedade e orientação do Diretor de Compliance, ouvido os técnicos de informática e o setor responsável, as quais poderão ser implementadas sem aviso prévio aos colaboradores, sempre respeitados os parâmetros de confidencialidade aqui descritos.
18. Periodicamente serão realizados testes de segurança no sistema de informação da Sociedade, incluindo as seguintes práticas: (i) alteração das senhas de acesso dos Colaboradores; (ii) testes no *firewall*; (iii) manutenção dos aparelhos eletrônicos; (iv) testes nos sistemas de *backup*, mediante a comparação do conteúdo da cópia de segurança com os dados no disco; (v) testes nas eventuais restrições impostas aos diretórios; e (vi) testes de invasão externa e *phishing*.
19. Dessa forma, de modo a proteger o vazamento de Informações Confidenciais de propriedade da Sociedade são adotados os mecanismos mencionados na presente Política de Segurança Cibernética e da Informação, quais sejam, realização de *backup*

regularmente, controle de acesso às informações, proteção física e manutenção dos aparelhos eletrônicos e atualização dos antivírus.

20. Ainda assim, caso seja verificado o vazamento de informações da Sociedade ou dos seus clientes, independentemente de descumprimento da presente política, a Sociedade tomará todas as medidas cabíveis e com a menor brevidade possível para amenizar as consequências do vazamento das referidas informações. Além disso, fica estabelecido no Plano de Contingência e Continuidade de Negócios as medidas a serem tomadas nas situações de risco.
21. Toda violação ou desvio, tais como instalação (intencional ou não) de vírus de informática, uso de software ilegal e tentativas de acesso a informações restritas, por exemplo, é investigada para a determinação das medidas necessárias e definição de possíveis sanções, visando à correção da falha ou reestruturação de processos e evitando que casos análogos se repitam.
22. Se verificado que qualquer Colaborador infringiu as normas aqui estipuladas, principalmente, em relação a Política de Segurança Cibernética da Informação este poderá ser responsabilizada pelas perdas e danos incorridos em razão da sua conduta irregular, além das demais sanções a serem aplicadas pelo Diretor de Compliance.
23. Anualmente ou sempre que entender necessário, o Diretor de Compliance irá avaliar e revisar os procedimentos adotados pela Sociedade para garantia da segurança cibernética e das informações. Além disso, sempre que possível serão tomadas medidas para atualização da avaliação dos riscos aos quais a H2 esteja exposta.
24. O Diretor de Compliance visará promover a aplicação da presente Política de Segurança Cibernética e da Informação bem como o controle, a supervisão e a aprovação de exceções, sendo sua responsabilidade assegurar a implementação de mecanismos eficientes capazes de resguardar a segurança das informações de propriedade da Sociedade ou de terceiros em relação às quais a Sociedade tenha tido acesso, bem como a identificação de quaisquer infrações às regras aprovadas nesta Política de Segurança Cibernética e da Informação.

## CAPÍTULO 03

### POLÍTICA DE TREINAMENTOS

1. O presente Manual de Compliance dispõe acerca da política de treinamentos (“**Política de Treinamentos**”) da Sociedade e tem como objetivo estabelecer regras que orientem o treinamento de seus Colaboradores, de forma a torná-los aptos a seguir todas as regras dispostas nas políticas e códigos da Sociedade, no exercício de suas funções.
2. Nos termos do artigo 24, inciso III, da Resolução CVM 21, todos os Colaboradores da Sociedade, especialmente aqueles que tiverem suas atividades profissionais relacionadas à administração de ativos e carteiras de valores mobiliários, no momento de sua contratação, deverão receber um treinamento que aborde todos os temas, objeto de políticas específicas tratadas em códigos ou políticas aprovados pela Sociedade, inclusive as seguintes:
  - (i) Segregação física de atividades;
  - (ii) Sigilo e confidencialidade de informações;
  - (iii) Segurança cibernética e de informações;
  - (iv) Prevenção e combate à lavagem de dinheiro;
  - (v) Investimentos pessoais;
  - (vi) Compliance; e
  - (vii) Ética.
3. Os treinamentos abordarão as normas dispostas nas políticas e códigos aprovados pela Sociedade relativas a cada um dos temas, apresentando aos Colaboradores seus principais aspectos e os mecanismos de execução dos mesmos, bem como as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras. Assim, deverão proporcionar aos Colaboradores uma visão geral das políticas adotadas pela Sociedade, de forma que os mesmos se tornem aptos a exercer suas funções aplicando conjuntamente todas as normas nelas dispostas.
4. Não obstante, a H2 entende que é fundamental que todos os Colaboradores, especialmente aqueles que tenham acesso a informações confidenciais ou participem de processos de decisão de investimento, tenham sempre conhecimento atualizado dos seus princípios éticos, das leis e normas.
5. Neste sentido, a Sociedade adota um programa de reciclagem dos seus Colaboradores, à medida que as regras e conceitos adotados pela H2 sejam atualizados, com o objetivo

de fazer com que eles estejam sempre atualizados, estando todos obrigados a participar de tais programas de reciclagem.

6. A Sociedade disponibilizará a todos os seus Colaboradores ferramentas eletrônicas de recebimento de informações financeiras, regulamentares, geopolíticas e estratégicas a nível global. Ademais, incentivará a participação de todos os seus Colaboradores em eventos pertinentes ao mercado financeiro e cursos específicos para determinadas necessidades.
7. A Sociedade poderá, por deliberação dos seus diretores, financiar cursos de aprimoramento profissional, desde que julgue viável e interessante o conteúdo a ser lecionado. Caberá aos diretores responsáveis pela área de administração de carteiras e pela administrativa e financeira da Sociedade a aprovação de participação em cursos, eventos ou palestras pelo Colaborador solicitante.
8. O controle e a supervisão das práticas profissionais dos Colaboradores em relação a esta Política de Treinamentos é responsabilidade do Diretor de Compliance, que visará promover a aplicação conjunta da presente Política de Treinamentos com as normas estabelecidas nos outros capítulos da presente política e demais códigos e políticas aprovadas pela Sociedade. O Diretor de Compliance poderá, ainda, conforme achar necessário, promover treinamentos esporádicos visando manter seus Colaboradores constantemente atualizados em relação às políticas da Sociedade e regulamentação do setor.
9. O Diretor de Compliance poderá contratar profissionais especializados para conduzirem o treinamento inicial e programas de reciclagem, conforme as matérias a serem abordadas.
10. Ao firmar o Termo de Adesão na forma do Anexo I, expressamente atestam a adesão a esta Política de Treinamentos, confirmando que recebeu o treinamento aqui determinado.

## CAPÍTULO 04

### POLÍTICA DE REGRAS E PROCEDIMENTOS DE COMPLIANCE

1. A presente Política de Regras e Procedimentos de Compliance da H2 (“**Política de Compliance**”), aprovada pela totalidade dos sócios, dispõe acerca das políticas relativas ao monitoramento, fiscalização, verificação e aplicação das medidas e penalidades relacionadas ao cumprimento do disposto em todas as políticas e códigos da Sociedade, bem como na legislação, regulamentação e autorregulação aplicável às atividades da Sociedade.
2. Esta Política de Compliance aplica-se a todos aqueles que possuem cargo, função, relação societária, empregatícia, comercial, profissional, contratual ou de confiança com a Sociedade, inclusive os diretores, empregados e Colaboradores da Sociedade.
3. Todos os Colaboradores da Sociedade deverão respeitar as regras estabelecidas nos termos da presente política. Para isto, cada Colaborador deverá firmar um Termo de Adesão a esta Política, atestando expressamente seu conhecimento acerca das políticas aqui estabelecidas e comprometendo-se a cumprir as regras determinadas.
4. Ao Diretor de Compliance será atribuída a responsabilidade por atos de fiscalização e controle, nos termos especificados na Política de Compliance, observado sempre a regulação da Comissão de Valores Mobiliários, cabendo a este: (i) a avaliação dos procedimentos e processos aqui estabelecidos objetivando assegurar o cumprimento desta Política; (ii) a propositura de alterações e ajustes das políticas estabelecidas na presente política, de acordo com o juízo de prudência do Diretor de Compliance para fins de adaptação à realidade da Sociedade; (iii) a definição de meios de sanção e desestímulo a condutas lesivas ou potencialmente atentatórias às normas estabelecidas nesta Política, bem como de mecanismos de reparação dos danos delas decorrentes em face da Sociedade ou de terceiros.
5. O Diretor de Compliance também terá a função de acompanhar as novas tendências legislativas relacionadas às regras, procedimentos e controles internos a incidirem sobre o exercício profissional de administração de carteiras de valores mobiliários, propondo as alterações necessárias à presente Política, para aprovação pelos sócios da H2.
6. Caso existam dúvidas sobre como agir em determinadas situações, os Colaboradores deverão obter esclarecimentos com seu superior hierárquico ou diretamente com a área de Compliance.

## **I. Objetivos**

7. Este Capítulo objetiva assegurar, em conjunto com as outras disposições contidas na presente Política de Compliance e demais códigos ou manuais aprovados, a adequação, fortalecimento e o funcionamento do sistema de controles internos da Sociedade, procurando mitigar eventuais riscos decorrentes da complexidade dos negócios da Sociedade, bem como disseminar a cultura de controles para assegurar o cumprimento às leis e regulamentação aplicáveis à Sociedade, relacionadas ao exercício de administração de carteira de valores mobiliários.
8. Todos os Colaboradores da Sociedade que tiverem suas atividades profissionais relacionadas com a administração de ativos e carteiras de valores mobiliários devem atuar de forma condizente com as regras, normas e procedimentos estabelecidos pela H2, sendo importante que, em caso de dúvidas ou necessidade de aconselhamento, busquem auxílio imediato junto ao Diretor de Compliance.
9. Todos os profissionais que tiverem suas atividades profissionais relacionadas com as áreas de Compliance e gestão de risco devem possuir qualificação técnica e experiência necessárias para o exercício das atividades por eles desempenhadas, sendo de responsabilidade do Diretor de Compliance a fiscalização.
10. Esta Política de Compliance visa, ainda, garantir o efetivo cumprimento das atividades relacionadas à administração de ativos e carteiras de valores mobiliários, nos termos do artigo 22 e 27, inciso I, da RCVM 21. As regras aqui contidas deverão ser observadas por todos os Colaboradores da Sociedade a fim de assegurar o estrito cumprimento das políticas estabelecidas pela Sociedade.

## **II. Setor de Compliance – Disposições Gerais**

11. O controle e a supervisão das práticas profissionais dos Colaboradores em relação a presente política é de responsabilidade do Diretor de Compliance, nomeado pelos sócios da Sociedade.
12. O Diretor de Compliance deverá ser escolhido entre pessoas com reputação ilibada e com qualificação técnica e experiência para o exercício das atividades que lhes são atribuídas. O Diretor de Compliance deverá, ainda, buscar se qualificar e atualizar, visando atender as demandas impostas pelo cargo assumido.
13. As regras que norteiam a atuação do Diretor de Compliance deverão ser revistas imediatamente antes da contratação da Sociedade para o exercício de qualquer atividade de administração de carteira de valores mobiliárias que difiram das atividades atuais.

14. Caberá ao Diretor de Compliance, promover a aplicação das políticas estabelecidas pela Sociedade, especialmente em relação aos códigos e políticas elaborados e aderidos por ela, observado o disposto nesta Política de Compliance.
15. O Diretor de Compliance deverá, com periodicidade a ser definida por ele, promover treinamentos visando manter seus Colaboradores constantemente atualizados em relação às políticas da Sociedade, e a outros códigos de autorregulação aos quais a Sociedade tenha aderido ou venha a aderir, bem como garantir o conhecimento dos Colaboradores acerca da legislação atual aplicável às atividades da Sociedade e às regras de compliance e controles internos constantes deste capítulo. O Diretor de Compliance também deverá se manter capacitado para ocupar o cargo, participando de treinamentos sempre que entender necessário.
16. O Diretor de Compliance deve verificar periodicamente as notícias, decisões e publicações disponibilizadas pela Comissão de Valores Mobiliários - CVM e ANBIMA em seus *websites* e veiculá-las internamente de acordo com a relevância das mesmas às áreas que possam ser impactadas.
17. Todos os funcionários ou demais colaboradores que vierem a ser contratados pela Sociedade receberão uma cópia das políticas e códigos aprovados pela Sociedade, entregue pelo Diretor de Compliance, que deverá ser estudado cuidadosamente sendo que para complementar este período de adaptação, dentro de até uma semana do ingresso do Colaborador na Sociedade, este participará de um treinamento individual, durante o qual serão apresentados a ele todos os pontos das políticas e códigos em vigor da Sociedade, e, durante esta oportunidade, o Colaborador poderá esclarecer quaisquer eventuais dúvidas que tenha sobre tal documentação, inclusive sobre as regras acerca da política de investimentos pessoais.
18. O Diretor de Compliance, visando assegurar que a Sociedade opere em conformidade com a presente política, normas e orientações aos quais a Sociedade se sujeita deverá, ao menos uma vez por ano, avaliar e revisar os procedimentos da Sociedade, tanto no âmbito das relações com terceiros (externas), como nas relações internas, no que concerne às atualizações, implementações de novas estratégias e/ou políticas e aditamentos e retificações dos mecanismos de controle interno, a fim de minimizar preventivamente eventuais riscos operacionais e de descumprimento do disposto nesta Política.
19. Sempre que julgar necessário, o Diretor de Compliance estabelecerá normas, procedimentos e controles internos para a Sociedade, determinando as atualizações, implementações de novas estratégias e políticas ou, ainda, aditamentos e retificações dos mecanismos de controles internos.
20. Será assegurado pelo Diretor de Compliance, em conjunto com a Diretoria da Sociedade, que a estrutura organizacional da Sociedade determine, com clareza, a responsabilidade, autoridade e autonomia de cada área e a quem cada colaborador se reporta, a fim de promover altos padrões éticos e de conduta, demonstrando a todos os



Colaboradores a importância do comprometimento com todos os controles internos implementados.

21. O Diretor de Compliance exerce as suas funções com total independência e autonomia, não se subordinando à equipe de gestão de recursos. Em nenhuma hipótese o Diretor de Compliance atuará em funções relacionadas à administração de carteiras de valores mobiliários, à intermediação e distribuição ou à consultoria de valores mobiliários, ou em qualquer atividade que limite a sua independência, quer seja na H2 ou fora dela.

### **III. Diretor Responsável por Compliance**

21. Caberá ao Diretor de Compliance, as seguintes atribuições:

- (i) fiscalizar os atos dos administradores da Sociedade e de qualquer de seus Colaboradores, verificando o cumprimento de seus deveres legais, estatutários e nos termos da presente política e demais políticas aos quais estes ou a Sociedade venham a aderir;
- (ii) estabelecer controles internos em relação a práticas e procedimentos, bem como verificar a adequação e efetividade de referidos controles;
- (iii) descrever, avaliar e revisar os procedimentos das áreas de atuação de cada um dos Colaboradores, visando minimizar preventivamente riscos operacionais, sempre que entenderem necessário e, obrigatoriamente, uma vez por ano, devendo o resultado da avaliação e revisão constarem do relatório anual de suas atividades;
- (iv) avaliar os processos e procedimentos utilizados para assegurar o cumprimento do disposto nos códigos e políticas aos quais a Sociedade venha a aderir;
- (v) avaliar eventuais atos que possam caracterizar, direta ou indiretamente, um descumprimento pelos Colaboradores, do disposto no presente Manual de Compliance e demais códigos, manuais e políticas aos quais a Sociedade venha a aderir;
- (vi) sempre que julgar conveniente e, para fins de apurar fatos cujo esclarecimento seja necessário ao desempenho de suas funções, formular questões a serem respondidas por Colaboradores ou, se for caso, por peritos indicados pela Diretoria da Sociedade;
- (vii) definir procedimentos para a repressão de atos praticados em desacordo com a presente política e demais códigos, manuais e políticas aos quais a Sociedade venha a aderir, em linha com o disposto na cláusula V abaixo, bem como estabelecer as penalidades ou mecanismos para a reparação de danos sofridos pela Sociedade ou terceiros em função do descumprimento.
- (viii) rever a presente política e demais códigos, manuais e políticas aos quais a Sociedade tenha aprovado ou venha a aderir, e, sempre que julgar necessário, propor alterações e ajustes a referidos documentos, de acordo com melhores práticas de mercado, bem como avaliar e revisar ao menos uma vez por ano, os procedimentos e condutas da Sociedade tanto no âmbito das relações com terceiros (externas), como nas relações internas, no que concerne às atualizações,

- implementações de novas estratégias e/ou políticas e aditamentos e retificações dos mecanismos de controle interno;
- (ix) prestar suporte a todas as áreas da Sociedade no que concerne a esclarecimentos dos controles e do disposto nas políticas e manuais aprovados e/ou aderidos pela Sociedade;
  - (x) acompanhar a conformidade das atividades da Sociedade com as normas regulamentares (externas e internas, inclusive, mas não exclusivamente, conforme estabelecidas nos capítulos da presente política) em vigor;
  - (xi) fiscalizar os controles internos da Sociedade, em particular no que diz respeito às seguintes atividades desempenhadas pela Sociedade: (a) execução dos controles de corretagens; sempre que aplicável (b) controle das contas pendentes da Sociedade que deverão ser pagas/quitadas;
  - (xii) informar à CVM da ocorrência ou suspeita de violação da legislação imposta pela autarquia no tocante à atividade de administração de carteira de valores mobiliários, no prazo máximo de 10 (dez) dias úteis contados da sua constatação;
  - (xiii) analisar situações que possam ser caracterizadas como conflitos de interesses entre os interesses da Sociedade ou do Colaborador e do cliente, aplicando as medidas cabíveis; e
  - (xiv) tratar todos os assuntos que chegue ao seu conhecimento dentro do mais absoluto sigilo e preservando os interesses e a imagem institucional e corporativa da H2, como também dos Colaboradores envolvidos.
22. O Diretor de Compliance atuará também como Diretor responsável pela verificação do cumprimento das políticas relacionadas ao combate e prevenção de lavagem de dinheiro, acompanhando de forma próxima e corriqueira as atividades da Sociedade.
23. No mais, o Diretor responsável pelo Compliance, tendo em vista que participará ativamente da administração da Sociedade, com dedicação pessoal, atuará também de forma direta e efetiva, como responsável pela aplicação das penalidades cabíveis sempre que ocorrer qualquer desvio no cumprimento de regras estabelecidas e aprovadas pela Sociedade, assim como de regras regulamentares aprovadas pela CVM e das regras constantes dos Códigos de Autorregulação aos quais a Sociedade pretende aderir.
24. Dessa forma, caberá ao Diretor de Compliance, decidir sobre a aplicabilidade de penalidades, bem como definir a natureza da pena a ser aplicada, em relação a qualquer infração, suspeita ou ameaça de infração, que venha a ser de conhecimento deste.
25. Adicionalmente, o Diretor de Compliance será responsável por apresentar um relatório anual de suas atividades, bem como um plano de ação anual para a administração da Sociedade, cabendo a este monitorar o cumprimento de prazos e o nível de excelência dos trabalhos desenvolvidos pelo setor de compliance. Referido relatório será apresentado até o último dia útil do mês de janeiro de cada ano, referente ao ano civil imediatamente anterior à data de entrega, contendo: (i) as conclusões dos exames efetuados; (ii) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; (iii) a manifestação

do diretor responsável pela atividade de administração de carteira de valores mobiliários a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las; e (iv) relatório sobre revisão desta Política e demais códigos, manuais e políticas aos quais a Sociedade tenha aprovado ou venha a aderir, bem como eventual proposta de revisão do manual, código, política ou procedimento. Referido relatório deve ficar disponível para a CVM na sede da H2.

#### IV – Mecanismos Específicos de Controle e Fiscalização

26. O Diretor de Compliance ficará direta e pessoalmente responsável pela concretização dos mecanismos de controle e fiscalização abaixo discriminados, observando, inclusive, a periodicidade respectivamente prevista, devendo os demais Colaboradores, por sua vez, cooperarem com o Diretor de Compliance quando do exercício de suas funções institucionais:
- (i) as mensagens do e-mail corporativo da Sociedade poderão ser monitoradas, sendo que o espaço disponível em Drive C dos computadores dos Colaboradores e as mensagens enviadas e recebidas pelo e-mail corporativo poderão ainda ser verificadas e as conversas telefônicas poderão ser gravadas e escutadas, por solicitação do Diretor de Compliance, a qualquer momento, sem que seja necessária qualquer anuência ou comunicação prévia. Tais práticas não representam invasão da privacidade dos Colaboradores já que são ferramentas de trabalho disponibilizadas pela própria H2. A constatação de qualquer indício de desvio de conduta ensejará investigação imediata pela área de Compliance.
  - (ii) o Diretor de Compliance deverá verificar os cálculos dos valores das cotas dos fundos geridos pela Sociedade, conforme aplicável, mediante confrontação das notas de corretagem com o relatório do administrador responsável pelo cálculo da cota do respectivo fundo. Caberá também ao Diretor de Compliance verificar a adequação da avaliação atribuída aos valores mobiliários integrantes da gestão das carteiras e de fundos exclusivos que não sejam negociados em mercados organizados ao disposto no respectivo regulamento, na regulamentação aplicável e às melhores práticas de mercado; e
  - (iii) o Diretor de Compliance deverá verificar o enquadramento das carteiras e fundos geridos, no que concerne à política de investimento de cada um deles, risco de crédito, risco de preços (volatilidade), risco de contraparte e risco de liquidez. Se qualquer uma dessas medidas forem extrapoladas, o mesmo tem o dever de exigir da área de gestão o imediato desmonte de posições para que a carteira ou fundo volte a se enquadrar imediatamente. Em dias em que se realizam operações acima da média esse controle deverá ser feito durante o próprio horário de funcionamento do mercado, procurando-se assim evitar que no fechamento do dia haja alguma carteira ou fundo desenquadrado.
27. Considerando o atual porte da Sociedade e a expectativa razoável de seus administradores de que esta se mantenha relativamente estável no médio prazo, a

Sociedade compromete-se a, assim que esta atingir um número de funcionários e Colaboradores igual ou superior a 20 (vinte), avaliar a necessidade de contratação de uma auditoria externa especializada, com o objetivo específico de (a) rever e verificar a adequação dos procedimentos internos de controle e monitoramento adotados e (b) rever de forma específica as práticas, procedimentos e controles adotados e sua adequação ao disposto nos códigos e manuais aprovados pela Sociedade.

28. Ademais, na mesma hipótese de a Sociedade vir a ter um número de funcionários superior a 20 (vinte), ou ainda, caso o objetivo da Sociedade deixe de focar na gestão de carteiras de fundos diversos detidas e/ou investidos por investidores no Brasil e no exterior, que buscarão, no longo do prazo, superar seus respectivos *benchmarks* (índices de referência), os procedimentos para acompanhamento e monitoramento de atividades com vistas à verificação do cumprimento às normas estabelecidas pela Sociedade serão necessariamente revistos, em especial no que diz respeito à eventual necessidade de contratação de novos profissionais para reforçar a diretoria responsável pelas práticas de Compliance da Sociedade.

## V. Penalidades

29. A atuação do Colaborador em conformidade com a presente política, além das constantes nos demais códigos aprovados pela Sociedade e demais regras verbais ou escritas estabelecidas pela Sociedade ou, ainda a outros códigos e políticas que a Sociedade venha a aderir, é obrigatória. As violações podem resultar em responsabilidade administrativa, criminal ou civil para a Sociedade e para os Colaboradores envolvidos.
30. Todos os Colaboradores deverão reportar para o Diretor de Compliance todo e qualquer indício e/ou prova de violação aos códigos, políticas e manuais de quem tenham conhecimento. Caberá ao Diretor de Compliance apurar as informações recebidas, observado o direito de defesa do Colaborador envolvido.
31. Após a devida análise dos fatos e observadas as particularidades de cada caso concreto, o Diretor de Compliance aplicará uma das sanções abaixo previstas, levando em consideração os seguintes pontos: (i) a gravidade da conduta; (ii) eventual reincidência na violação das regras, procedimentos e políticas adotadas pela Sociedade; e (iii) a possibilidade de reparação dos danos causados pelo Colaborador.
32. Nesse sentido, os Colaboradores que descumprirem ou não observarem as disposições estabelecidas pela Sociedade, estarão sujeitos às seguintes medidas disciplinares:
- (i) advertência oral;
  - (ii) advertência escrita;
  - (iii) suspensão de até 30 dias corridos, quando aplicável; e

- (iv) rompimento do vínculo existente entre a Sociedade e o Colaborador infrator por justa causa, se aplicável, nos termos do artigo 482 da Consolidação das Leis do Trabalho – CLT.
33. Em nenhuma hipótese a Sociedade assumirá a responsabilidade de Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções. Em caso de responsabilização da Sociedade ou caso esta sofra prejuízo de qualquer natureza por atos de seus Colaboradores, a Gestora poderá exercer o direito de regresso contra os responsáveis.

## CAPÍTULO 05

### PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

#### Introdução

34. O presente Plano de Contingência e Continuidade de Negócios da H2 Asset Management Ltda. (o “**Plano de Contingência**” e a “**Sociedade**” ou “**H2**”, respectivamente) tem como objetivo definir os procedimentos a serem seguidos no caso de contingência, de modo a impedir a descontinuidade operacional da Sociedade por problemas técnicos.
35. Foram estipulados estratégias e planos de ação com o intuito de garantir que os serviços essenciais da H2 sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre. O Diretor de Compliance é o responsável pela implementação do presente Plano de Contingência.
36. O Plano de Contingência prevê ações que durem até o retorno à situação normal de funcionamento da Sociedade dentro do contexto de seu negócio.
37. O Plano de Contingência da H2 identifica duas variáveis para o funcionamento adequado da empresa: (i) infraestrutura; e (ii) processos.
38. A infraestrutura engloba todas as variáveis utilizadas para realização dos processos, em particular: (i) energia; (ii) telecomunicações; (iii) informática; e (iv) sistemas internos. Para cada um dos itens que compõem a infraestrutura existe uma ação a ser tomada.
39. Já os processos são as atividades realizadas para operar os negócios da H2. Os processos dependem da infraestrutura toda ou de parte da estrutura em funcionamento. Somente com os processos em andamento pode-se definir que o plano de ação foi bem executado.

#### Estrutura Operacional

40. A Sociedade tem como objeto a administração e gestão de recursos de terceiros, de modo que precisa contar com uma estrutura operacional desenvolvida e preparada para eventuais emergências. O suporte para essa estrutura operacional é um corpo funcional capacitado com áreas de apoio.

#### Análise de Risco

41. Com o objetivo de avaliar as medidas a serem tomadas em cada situação, serão analisados os cenários de risco e o potencial impacto nas operações da Sociedade, considerando sempre a probabilidade e a gravidade de ocorrência.

42. Dessa forma, considerando o impacto que pode ser causado para a H2 e seus clientes, é possível classificar os riscos em três categorias:

**Aceitável** – quando a probabilidade de ocorrência e gravidade são baixos. Não é necessário tomar nenhuma medida;

**Tolerável** – quando a probabilidade de ocorrência e gravidade são médios ou apenas um desses critérios é classificado como baixo ou grave. Nesta hipótese a Sociedade está preparada para suportar o risco e continuar com as atividades, sem necessidade de acionar o Plano de Contingência; e

**Intolerável** – quando a probabilidade de ocorrência e gravidade são altos. Deve ser aplicado o Plano de Contingência até que o risco seja controlado e as atividades possam voltar à normalidade.

### Eventos de Risco

43. Para avaliação dos eventos possíveis causadores de situação de risco, leva-se em consideração, o patrimônio dos clientes, as informações confidenciais e privilegiadas, os colaboradores, as instalações físicas, equipamentos de comunicação e informática.

**Inacessibilidade ou restrição às instalações físicas com danos aos equipamentos**

Hipótese de ocorrência: (i) eventos naturais; (ii) acidentes de grande natureza no entorno da sede social da Sociedade; (iii) desastres internos; e/ou (iv) pandemias

Probabilidade: Baixa

Gravidade: Baixa

Avaliação de Risco: Tolerável

### Colaboradores

Hipótese de ocorrência: falecimento dos principais colaboradores da Sociedade

Probabilidade: Baixa

Gravidade: Alta

Avaliação de Risco: Tolerável

### Falhas no sistema de Segurança Cibernética e da Informação

Hipótese de ocorrência: vazamento de dados ou informações confidenciais e privilegiadas, invasão dos sistemas da Sociedade e aparelhos de informática ou de comunicação

Probabilidade: Baixa

Gravidade: Alta

Avaliação de Risco: Tolerável

### **Serviços de telefonia, internet e energia**

Hipótese de ocorrência: interrupção temporária dos serviços terceirizados de telefonia, internet e energia elétrica

Probabilidade: Média

Gravidade: Baixa

Avaliação de Risco: Tolerável

### **Política e procedimentos para *backup***

44. O *backup* se dará da seguinte forma: (i) para a garantia do *backup* das informações da H2, estas devem ser armazenadas nos servidores de armazenamento em nuvens utilizados pela H2; (ii) não haverá garantia de *back-up* para arquivos armazenados nas estações de trabalho (desktops ou notebooks) de forma que o armazenamento diretamente nas estações de trabalho não está autorizado; (iii) o *backup* de dados armazenados nos servidores em nuvem é realizado de forma automatizada e periódico, de acordo com os procedimentos de *backup* e *restore* definidos conforme política dos serviços de armazenamento em nuvem contratados (*Droptbox*); (iv) o *backup* é armazenado automaticamente nos servidores de armazenamento do fornecedor e seguem os procedimentos padrões dos próprios serviços de armazenamento em nuvem contratados; (v) o *restore* de dados deve ser solicitado aos profissionais contratados para a execução dos serviços de informática e será realizado de acordo com os procedimentos específicos do mesmo, de acordo com a política de armazenamento e *restoring* do serviço contrato do provedor de armazenamento de dados.
45. Verificação e teste de restauração: sempre que possível o procedimento padrão de restauração dos serviços de armazenamento em nuvem contratados serão executados para verificar a validade dele. A verificação será realizada por meio da comparação do conteúdo da cópia de segurança com os dados no disco.
46. Serviços de armazenamento de código de linguagem computacional se utilizado pela equipe de gestão será realizado através de serviços em nuvem, com backups realizados automaticamente, seguindo o mesmo procedimento descrito no item 44 acima. O versionamento de código e as alterações serão mantidos em softwares específicos, que permitem verificar qualquer alteração e realizar *rollback* para versões anteriores, se necessário.
47. Também deverão ser observados os processos e procedimentos estabelecidos no Manual de Compliance, no capítulo de Política de Segurança Cibernética da Informação.



### Efetiva Contingência

48. **Imediata Comunicação da Interrupção.** Uma vez identificada a interrupção de quaisquer dos recursos essenciais às atividades, os responsáveis pela área de Compliance e de TI devem ser imediatamente comunicados a fim de tomar as providências cabíveis nos termos do presente Plano de Contingência.
49. Dessa forma, todos os colaboradores devem possuir os contatos telefônicos e e-mail dos responsáveis pela área de Compliance e TI, de modo a possibilitar a comunicação da contingência ocorrida e a solução mais rápida do problema, ou quando não possível obter uma solução imediata, a opção do fluxo alternativo mais viável.
50. **Falhas no sistema de energia.** Em caso de falha de fornecimento de energia, a H2 possui nobreak para suportar o funcionamento do ambiente de telecomunicações até que o fornecimento seja reestabelecido, ou em caso de longa interrupção, a utilização de armazenamento e/ou servidores em nuvem associados aos notebooks permitem a utilização de toda a infraestrutura necessária para o funcionamento da H2, ainda que remotamente, conforme melhor detalhado no item 51 abaixo
51. **Necessidade de Evacuação ou Impedimento de Acesso às Instalações da H2.**
- a) **Servidores de Armazenamento ou de Códigos de Computação.** A H2 conta com acesso remoto aos seus bancos de dados virtuais disponível a todos os colaboradores autorizados pelo Diretor de Compliance. Em caso de evacuação, impedimento à entrada no escritório ou incêndio com danos à infraestrutura local, os recursos de TI e todas as aplicações podem ser acessados remotamente através dos notebooks configurados especificamente para utilização da H2 e que são de uso constante dos seus colaboradores. Os servidores de acesso em nuvem permitem a realização de todas as atividades da H2 de forma remota.
  - b) **Email.** O serviço de e-mail da H2 é garantido por parceiro que provém suporte 24/7, serviço de AntiSpam, antivírus, recuperação de informação e site de recuperação de desastre.
  - c) **Reuniões virtuais.** A H2 contrata serviço de vídeo conferências de alta qualidade, sendo possível a realização de reunião a partir de qualquer computador com acesso à Internet.
52. **Falhas nos computadores individuais.** Em caso de falhas em computadores utilizados pelos colaboradores, a H2 conta com máquinas de contingência para utilização e já previamente configuradas.

53. **Falhas nos Links de acessos a Internet.** Links de internet de diferentes provedores garantem a redundância da rede e alta disponibilidade entre sistemas/informações da H2 e clientes e fornecedores de serviços. A disponibilidade do link principal e redundante é monitorada 24/7, com alertas em casos de indisponibilidade.
54. **Duplicidade de conhecimento de atividades e processos.** Todas as atividades dos colaboradores são compartilhadas com outros colaboradores que façam parte da mesma equipe de forma a evitar que a ausência de um colaborador impeça as atividades rotineiras do departamento ou da H2. São feitos manuais dos sistemas e planilhas proprietárias utilizadas pelos colaboradores da H2.

### Atualização

55. As políticas e processos referentes no presente Plano de Contingência são revisados ao menos uma vez por ano e atualizados sempre que necessário. Também em uma base anual, os colaboradores da Sociedade têm treinamento sobre o referido plano e suas eventuais atualizações.

## CAPÍTULO 06

### POLÍTICA DE CERTIFICAÇÃO

1. O presente Capítulo dispõe acerca das regras, procedimentos e diretrizes relacionados a identificação da necessidade dos Colaboradores da Sociedade possuírem certificados exigidos pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (“**ANBIMA**”), conforme disposto no Código de Administração Gestão de Recursos de Terceiros e nas Regras e Procedimentos de Certificação e demais documentos emitidos pela referida associação, conforme vigentes.
2. Tendo em vista as atividades desenvolvidas pela H2, os Colaboradores que atuarem diretamente na atividade de gestão de recursos de terceiros e tiver poder discricionário de investimento dos ativos financeiros integrantes das carteiras dos fundos de investimentos ou carteiras administradas geridos pela Sociedade devem possuir a certificação profissional ANBIMA para Gestores de Recursos de Terceiros (o “**CGA**”) ou a isenção atestada pela referida associação; ou para os fundos estruturados, a respectiva certificação para fundos estruturados (“**CGE**”), nos termos do Código de Regras e Procedimentos de Certificação.
3. O CGA ou CGE é pessoal, intransferível e válido por tempo indeterminado, desde que o Colaborador esteja exercendo a atividade de gestão de recursos e o CGA não esteja vencido a partir do início do vínculo com a H2, não existindo, conforme disposto no Código de Certificação Continuada, procedimentos de atualização obrigatórios.
4. Dessa forma, os Colaboradores que participarem de forma direta da atividade de gestão de recursos de terceiros com alçada de decisão sobre o investimento, desinvestimento e manutenção dos recursos dos veículos de investimento geridos pela H2, obrigatoriamente devem ser certificados pelo CGA ou terem sua isenção atestada pela ANBIMA; assim como os profissionais que tenham alçada/poder discricionário de investimento (compra e venda) de ativos integrantes das carteiras de fundos de investimento em participações deverão (“**FIP**”) possuir o respectivo CGE.
5. Já os Colaboradores que atuam na análise de ativos e valores mobiliários, bem como exercem outras atividades relacionados ao auxílio e munção de informações para tomada de decisão pelos Colaboradores devidamente certificados, não precisam ter a certificação CGA. Estes profissionais não terão, em nenhuma hipótese poder de decisão em relação aos ativos integrantes das carteiras geridas pela Sociedade.
6. Caberá ao Diretor de Compliance o acompanhamento e monitoramento periódico acerca da validade das certificações dos membros do departamento técnico da Sociedade que possuem poder discricionário de investimento e consequentemente, a necessidade do CGA ou CGE.
7. Os Colaboradores têm a obrigação de manter as certificações necessárias para a realização das suas atividades dentro da H2 devidamente atualizadas e regularizadas. Uma vez constatado que o Colaborador está desrespeitando o quanto disposto na presente Política de Certificação, este será imediatamente afastado das atividades de gestão de recursos até que sua situação seja regularizada e seja realizada a atualização

junto ao Banco de Dados ANBIMA. Neste período ele atuará exclusivamente em atividades auxiliares aos gestores certificados.

8. O Diretor de Compliance é o responsável pela atualização das informações constantes no Banco de Dados da ANBIMA, as quais precisam ser verdadeiras e atualizadas. As atualizações devem ocorrer, no mínimo, na ocorrência dos seguintes eventos: (i) contratação e desligamento de profissionais; (ii) alteração das funções exercidas pelos Colaboradores que sejam elegíveis de certificação; (iii) obtenção de nova certificação por Colaboradores; e (iv) perda de certificação pelos Colaboradores.
9. A contratação de novos profissionais para atuarem na Sociedade, bem como a transferência de Colaboradores dentro da própria Sociedade devem observar as regras dispostas na presente Política de Certificação, cabendo ao Diretor de Compliance e ao diretor responsável pela atividade de gestão verificar a necessidade de certificação por referido profissional, em razão das atividades a serem desenvolvidas por ele na Sociedade.
10. Todos os Colaboradores da Sociedade deverão respeitar as regras estabelecidas nos termos desta Política de Certificação e do Manual de Compliance por inteiro, tendo atestado expressamente o seu conhecimento acerca das regras previstas nesta política, comprometendo-se a cumpri-las, mediante assinatura do Anexo I ao presente.

Versão	Atualizada em	Responsável:
02	Janeiro/2026	[Felipe Ha Jong Kim]

## ANEXO I

### TERMO DE ADESÃO AO MANUAL DE COMPLIANCE DA H2 ASSET MANAGEMENT LTDA.

Eu, \_\_\_\_\_, portador da cédula de identidade RG nº \_\_\_\_\_, inscrito no CPF nº \_\_\_\_\_, declaro para os devidos fins que:

1. Tenho total conhecimento da existência do Manual de Compliance da **H2 Asset Management**, (“**Sociedade**”), atualizado em [•] de [•] de 2025, o qual recebi e li, sendo que me comprometo a observar integralmente seus termos e condições.
2. Sei, a partir desta data, que a não observância dos termos do Manual de Compliance da Sociedade poderá implicar na caracterização de falta grave, fato que poderá ser passível da aplicação das penalidades cabíveis, inclusive demissão por justa causa.
3. As regras estabelecidas no presente Manual de Compliance da Sociedade não invalidam nenhuma disposição relativa a qualquer norma interna estabelecida pela Sociedade, mas apenas servem de complemento e esclarecem como lidar com determinadas situações na execução de minhas atividades profissionais.
4. Estou ciente que o disposto no Capítulo 01 do presente Manual de Compliance, referente à Política de Sigilo e Confidencialidade e Propriedade Intelectual da Sociedade é aderido, por meio do presente termo, em caráter irrevogável e irretratável, por prazo indeterminado, válido indefinidamente mesmo após o término de meu vínculo com a Sociedade, não podendo ser rescindido sem expressa e inequívoca concordância da Sociedade.
5. Li e entendi a legislação e regulamentação aplicável a negociação de valores mobiliários, em particular, conforme disposto na Resolução CVM 44, de 23 de agosto de 2021, conforme alterada, e demais regulamentações vigentes, acerca de divulgação e o uso de informações sobre ato ou fato relevante na negociação de valores mobiliários de emissão de companhias abertas.
6. Em \_\_\_\_ de \_\_\_\_\_ de 20[-], participei do treinamento específico realizado em consonância com o Capítulo 03 do presente Manual de Compliance, referente à Política de Treinamentos da Sociedade, sendo que compreendi perfeitamente as regras estabelecidas pelo Manual de Compliance e demais manuais e políticas estabelecidas pela Sociedade e aderi ao mesmo, comprometendo-me a observar integralmente os termos e condições que me foram apresentados.

São Paulo, 26 de janeiro de 2026.

---

[NOME]