POLÍTICA DE SEGURANÇA CIBERNÉTICA DA INFORMAÇÃO

CHIMERA CAPITAL ASSET MANAGEMENT LTDA.

São Paulo - Dezembro de 2024

I. PREÂMBULO

1. A presente política dispõe acerca da Política de Segurança Cibernética e da Informação ("**Política Cibernética**") da Chimera Capital Asset Management Ltda. ("**Sociedade**"), tendo como objetivo estabelecer regras que orientem o controle de acesso a Informações Confidenciais (conforme adiante definido) pelos sócios, diretores, empregados e prestadores de serviços (com habitualidade) ("**Colaboradores**"), bem como o seu uso e preservação, inclusive por meio 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. A fim de resguardar a observância integral a presente Política Cibernética, todos os Colaboradores da Sociedade firmarão o Termo de Adesão, na forma do Anexo I, afirmando seu conhecimento e expressa anuência.

3. O Diretor de Compliance é a pessoa responsável na Sociedade para tratar sobre as questões da presente política. Caso seja verificada a 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 da Sociedade, sendo realizadas as recomendações de proteções adequadas.

II. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

4. O ativo de maior valor da Sociedade são as Informações Confidenciais (conforme adiante definido) da própria Sociedade, dos seus clientes, dos ativos que compõem a carteira dos fundos de investimentos geridos pela Sociedade e eventualmente de outras companhias as quais a Sociedade, seus clientes ou sócios tenham vínculo ("**Ativos**") que possuem natureza privilegiada e, por isso, os sistemas de segurança visam preservar o sigilo dessas informações.

5. Para fins desta política, Informações Confidenciais significam toda e qualquer informação e/ou dado de natureza confidencial, incluindo, mas sem limitação, todas as informações técnicas, financeiras, operacionais, econômicas, bem como as demais informações comerciais, know-how, 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 Sociedade, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridos pela Sociedade, 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, clientes, bem como os dados pessoais de seus 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 relacionadas diretamente aos serviços prestados pela Sociedade ou às transações aqui contempladas.

6. Não serão consideradas como Informações Confidenciais todas e quaisquer informações que (a) sejam ou venham a se tornar de domínio público, sem a violação do disposto nesta Política Cibernética; ou (b) tenham sido recebidas de boa-fé pelo Colaborador ou de terceiros que tenham o direito de divulgá-las ou que não esteja vinculado a qualquer obrigação de confidencialidade.

7. 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 relativas à sua atividade.

8. Os equipamentos e computadores disponibilizados pela Sociedade aos Colaboradores deverão ser utilizados com a finalidade de atender aos interesses comerciais da Sociedade, sendo permitida a sua utilização para fins particulares de forma moderada e pontual.

9. 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 Sociedade com estes arquivos, uma vez que tais arquivos possuem Informações Confidenciais.

10. A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem feitos em prol da execução e do desenvolvimento dos negócios e dos interesses da Sociedade. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha Informação Confidencial será o responsável direto por sua boa conservação, integridade e manutenção da confidencialidade.

11. A Sociedade disponibiliza a seus Colaboradores correio eletrônico ("**E-mails Corporativos**") que se caracteriza como corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo sua utilização preferencialmente voltada para alcançar os fins comerciais da Sociedade aos quais se destina. É permitida a utilização pessoal de forma moderada e pontual, observando-se, principalmente os parâmetros éticos.

12. 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, a fim de que seja resguardado o atendimento às normas contidas nesta Política Cibernética e legislação vigente.

13. As comunicações recebidas por meio dos E-mails Corporativos, recebidos pelos Colaboradores da Sociedade, quando abertas, deverão ter seu conteúdo verificado pelo Colaborador, não sendo admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem. Os arquivos de E-mails Corporativos poderão ser inspecionados pela Sociedade, a critério do Diretor de Compliance, a qualquer tempo e independentemente de prévia notificação.

14. Cada Colaborador da Sociedade, no momento de sua contratação, receberá uma senha secreta, pessoal e intransferível para ter acesso aos computadores, à rede corporativa da Sociedade e ao E-mail Corporativo, que será imediatamente desativada no caso de desligamento do respectivo Colaborador. As senhas devem ser alteradas com periodicidade não maior do que 6 (seis) meses.

15. 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.

16. 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.

17. A senha da rede de internet principal da Sociedade e das respectivas camadas de segurança são mantidas de forma segura e não são compartilhadas com todos os usuários.

III. AÇÕES DE PREVENÇÃO E PROTEÇÃO DOS ATIVOS DA SOCIEDADE

18. A fim de conferir maior segurança ao acesso à parte restrita da rede da Sociedade, o respectivo Colaborador possuirá uma combinação de login e senha para autenticar sua credencial e 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.

19. 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.

20. 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.

21. Todos os computadores devem ter um antivírus atualizado e rodando o tempo todo e, em caso de não funcionamento deste software, é obrigação do Colaborador-usuário notificar, prontamente, a equipe responsável para solução do problema.

22. Cada Colaborador é responsável por manter o controle sobre a segurança das Informações Confidenciais, armazenadas ou disponibilizadas, nos equipamentos que estão sob sua responsabilidade. Será obrigatória a alteração de senha de acesso aos equipamentos (login de usuário) sempre que for identificado qualquer caso adverso ou quando assim solicitado pelo Diretor de Compliance, utilizando modelo de definição de senha de difícil identificação.

23. Todas as instalações da Sociedade são protegidas e segregadas por áreas de atuação, com controles de entrada apropriados para garantir a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade de todas e quaisquer Informações Confidenciais.

IV. MONITORAMENTO E TESTES PERIÓDICOS

24. Apenas os equipamentos e softwares disponibilizados, homologados e/ou autorizados pela Sociedade e setor de tecnologia podem ser instalados nas máquinas dos Colaboradores e conectados à rede comum.

25. Downloads de qualquer natureza podem ser realizados, desde que de forma ponderada e 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.

26. Como forma de proteger e assegurar que as informações da Sociedade não sejam amplamente acessíveis, terceiros somente poderão acessar as dependências das Sociedade quando na recepção e na sala de reunião, desde que previamente requisitado a um dos Colaboradores e assim autorizado. O acesso físico a áreas em que Informações Confidenciais 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 das demais áreas da Sociedade e seguras.

27. 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.

28. 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 de terceiros aos sistemas. O Colaborador deve manter em local seguro suas senhas e outros meios de acesso aos sistemas, bem como não os divulgar a terceiros em qualquer hipótese.

29. A Sociedade promoverá regularmente backup das Informações Confidenciais, de modo que (i) para a garantia das Informações Confidenciais, o backup deverá armazená-las nos servidores específicos de armazenamento; (ii) não haverá garantia de backup para arquivos armazenados nas estações de trabalho; e (iii) o backup de dados armazenados nos servidores em nuvem será realizado de forma automatizada de tempos em tempos, conforme política do prestador de serviço (Dropbox). Caso seja necessário, o *restore* de dados, a ação deve ser solicitada aos profissionais contratados pela Sociedade para a execução dos serviços de informática e será realizada 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.

30. 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 recuperar versões anteriores, se necessário.

31. 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.

32. 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 técnica 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.

33. De modo a proteger o vazamento de Informações Confidenciais de propriedade da Sociedade são adotados, principalmente, os seguintes mecanismos: (i) realização de backup regularmente; (ii) controle de acesso às Informações Confidenciais; (iii) proteção física; (iv) manutenção técnica dos aparelhos eletrônicos; e (v) atualização dos softwares antivírus.

34. Na hipótese de ser verificado o vazamento de Informações Confidenciais da Sociedade ou dos seus clientes, independentemente de descumprimento da presente política, a Sociedade tomará todas as medidas cabíveis, com a menor brevidade possível, para amenizar as consequências do vazamento das referidas informações. Além disso, no Plano de Contingência e Continuidade de Negócios da Sociedade estão estabelecidas as medidas a serem tomadas nestas situações de risco.

V. PLANO DE RESPOSTAS

35. Uma vez identificada a interrupção de quaisquer dos recursos essenciais às atividades da Sociedade, os responsáveis pela área de Compliance devem ser imediatamente comunicados a fim de tomar as providências cabíveis, e no menor prazo possível, nos termos do Plano de Contingência e Continuidade de Negócios da Sociedade.

36. Todos os colaboradores devem possuir os contatos telefônicos e e-mail dos responsáveis pela área de Compliance, de modo a possibilitar a comunicação de eventual contingência ocorrida, bem como a solução mais rápida do problema, ou quando não possível obter uma solução imediata, a opção do fluxo alternativo mais viável.

37. Em caso de falha de fornecimento de energia, a Sociedade 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 Sociedade, ainda que remotamente.

38. A Sociedade conta com acesso remoto aos seus bancos de dados virtuais e disponível a todos os Colaboradores autorizados pelo Diretor de Compliance. Em caso de evacuação, impedimento à entrada na sede social ou incêndio com danos à infraestrutura local, os recursos e todas as aplicações podem ser acessados remotamente através dos notebooks configurados especificamente para utilização da Sociedade e que são de uso constante dos seus Colaboradores. Os servidores de acesso em nuvem permitem a realização de todas as atividades da Sociedade de forma remota e segura.

39. O serviço de e-mail da Sociedade é garantido por servidor que provém suporte 24/7, serviço de antispam, antivírus, recuperação de informação e site de recuperação de desastre.

40. A Sociedade contrata serviço de vídeo conferências de alta qualidade, sendo possível a realização de reunião a partir de qualquer computador com acesso à internet, com a segurança necessária.

41. Em caso de falhas nos computadores utilizados pelos colaboradores, caberá ao respectivo Colaborador informar, imediatamente, ao Diretor de Compliance a fim de que a máquina seja devidamente reposta. A Sociedade conta com máquinas de contingência para utilização nestes casos, já previamente configuradas.

42. Links da rede mundial de internet de diferentes provedores garantem a redundância da rede e a alta disponibilidade entre sistemas/informações da Sociedade e clientes e fornecedores de serviços. A disponibilidade do link principal e redundante é monitorada 24/7, com alertas em casos de indisponibilidade.

43. Todas as atividades dos Colaboradores são compartilhadas com os demais Colaboradores que façam parte da mesma equipe, de forma a evitar que a ausência de um Colaborador impeça a continuidade das atividades rotineiras do respectivo departamento ou da Sociedade. São feitas planilhas proprietárias para que os demais Colaboradores da Sociedade possam desenvolver suas atividades.

VI. PROTEÇÃO DE DADOS PESSOAIS

44. A Sociedade está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis que forem coletados ou aos quais tiver acesso em função do uso do site ou por conta do desempenho de suas atividades, e com o cumprimento das leis e regulamentos em vigor.

45. Por conta disso, estabeleceu, as diretrizes, princípios e regras previstas nesta política, as quais servirão de guia para a coleta, registro, processamento, armazenamento, uso, compartilhamento e eliminação de dados pessoais, fornecendo o arcabouço para o correto tratamento e proteção dos dados pessoais em seu poder.

46. Essas diretrizes, princípios e regras se aplicam a todos os Colaboradores da Sociedade, e englobam os dados pessoais que se encontrem armazenados em qualquer meio, e abrangem toda e qualquer forma de tratamento que possa ser empregada e esteja disponível para a Sociedade.

47. Importante observar que o escopo da proteção de dados pessoais no âmbito da Sociedade está, em grande parte, limitado aos dados pessoais de seus Colaboradores e de pessoas físicas e jurídicas com as quais tiver estabelecido relações jurídicas, com especial menção ao cumprimento da regulação aplicável à gestão de recursos de terceiros. Também estão abrangidos por esta proteção os dados de candidatos às vagas na Gestora, de fornecedores e outros com os quais a Sociedade manteve contato para atender alguma demanda relevante e específica.

48. Vale ressaltar que todo o tratamento de dados pessoais feito pela Sociedade está pautado nos requisitos do artigo 7º da Lei 13.709/2018 ("**LGPD**"), assim como nas premissas do artigo 11 da mesma Lei, quando aplicável.

49. A Sociedade compromete-se a obter dados pessoais de maneira justa e legal, e suas ações serão norteadas no princípio da boa-fé e nos princípios abaixo, os quais estão elencados no art. 6º da LGPD:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

50. Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18 da LGPD, o titular dos dados pessoais tem direito de solicitar à Sociedade, em relação aos seus dados, a qualquer momento e mediante requerimento expresso o que se segue.

a) confirmação de existência de tratamento;
b) acesso aos dados;
c) correção de dados incompletos, inexatos ou desatualizado;
d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei 13.709/2018;
e) 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;
f) eliminação dos dados pessoais tratados com o consentimento do titular, exceto em determinadas situações e respeitados os limites técnicos das atividades, conforme determinado na Lei;
g) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e
i) revogação do consentimento, nos termos da Lei.

51. A Sociedade disponibiliza canal de comunicação, através do endereço lgpd@chimeracapital.com.br, por meio do qual o seu Encarregado pelo Tratamento de Dados Pessoais, receberá quaisquer requisições, solicitações, comunicações e/ou manifestações dos titulares de dados pessoais para exercício dos direitos estipulados na Lei Geral de Proteção de Dados em consonância a sua Política de Privacidade. O Encarregado pelo Tratamento de Dados Pessoais, também conhecido como Data Protection Officer (DPO), é o responsável por auxiliar os controladores de dados pessoais em relação ao cumprimento de suas obrigações legais referentes à privacidade. Dessa forma, o DPO atua como uma ponte entre a Sociedade, os titulares dos dados (pessoas físicas) e a Autoridade Nacional de Proteção de Dados (ANPD).

52. Os dados pessoais serão armazenados pela Sociedade durante tempo necessário para o atingimento dos objetivos para os quais foram coletados. De todo modo, este período poderá ser ampliado

para o cumprimento de obrigação legal, regulatória ou contratual, pelo que, nestas hipóteses o prazo mínimo de armazenamento será de 5 (cinco) anos.

53. A divulgação de dados pessoais para o cumprimento de lei, determinação judicial, regulatória ou de órgão competente ao qual a Sociedade estiver sujeita somente ocorrerá nos estritos termos e nos limites requeridos para o cumprimento da obrigação, sendo que os titulares dos dados, na medida do possível e desde que não configure infração, inadimplemento ou cause prejuízo à Sociedade, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas. Adicionalmente, a Sociedade cooperará com a ANPD em qualquer problema em relação à proteção de dados e dentro dos limites previstos na LGPD e nas demais regulamentações sobre a matéria, porém sem renunciar a quaisquer defesas e/ou recursos disponíveis.

54. As matérias relacionadas aos dados pessoais, dados sigilosos e aos tratamentos destes serão apresentadas pelo Encarregado pelo Tratamento de Dados Pessoais para deliberação no Comitê de Gestão de Riscos e de Compliance.

55. Os Colaboradores estão obrigados a comunicar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais sobre toda e qualquer suspeita ou indício de evento que possa ter comprometido os dados pessoais de posse da Sociedade para a devida apuração. Caso necessário, o Encarregado pelo Tratamento de Dados Pessoais notificará, em prazo compatível com a severidade do evento, a ANPD, bem como todos os que porventura possam ter sido afetados pelo referido evento.

56. Os eventos reportados que tenham sido apurados e tiverem resultado no comprometimento de dados pessoais serão registrados no Relatório de Controles Internos e no Relatório de Impacto à Proteção de Dados Pessoais, inclusive de dados sensíveis, nos termos do artigo 38 da LGPD.

57. A Sociedade treinará seus Colaboradores sobre a proteção de dados pessoais e de dados sigilosos de acordo com a sua Política de Treinamento descrita no Manual de Compliance.

VII. GOVERNANÇA

58. As políticas e processos da Sociedade são revisados ao menos uma vez por ano e atualizados sempre que necessário, pelo Diretor de Compliance em conjunto com os gestores da Sociedade, em razão da edição de novas normas ou em razão da adoção de novos procedimentos para garantia da segurança cibernética e das Informações Confidenciais. Também em uma base anual, os Colaboradores da Sociedade têm treinamento sobre o referido plano e suas eventuais atualizações.

59. 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, será investigada para a determinar a adoção das medidas necessárias e definição de possíveis sanções ao(s) respectivo(s) Colaborador(es), visando à correção da falha ou reestruturação de processos e evitando que casos análogos se repitam.

60. Se verificado que qualquer Colaborador infringiu as normas estipuladas nas políticas da Sociedade, especialmente nesta Política Cibernética, este poderá ser responsabilizado pelas perdas e danos incorridos pela Sociedade em razão da sua conduta irregular, além das demais sanções a serem aplicadas pelo Diretor de Compliance, com ciência aos diretores da Sociedade.

61. O Diretor de Compliance visará promover a aplicação da presente Política Cibernética 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 Cibernética.

62. 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 o(s) Colaborador(es) envolvido(s).

63. 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, com ciência dos diretores da Sociedade, apurar as informações recebidas, observado o direito de defesa do(s) Colaborador(es) envolvido(s).

64. Após a devida análise dos fatos e observadas as particularidades de cada caso concreto, o Diretor de Compliance aplicará uma das sanções previstas na cláusula abaixo, levando em consideração: (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(s) Colaborador(es).

65. Nesse sentido, o(s) Colaborador(es) que descumprir(em) ou não observar(em) as disposições estabelecidas pela Sociedade, estará(ão) sujeito(s) 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.

66. 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 venha a sofrer prejuízos de qualquer natureza por atos de seus Colaboradores, a Sociedade poderá exercer o direito de regresso contra os responsáveis.

67. Esta Política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência.

CONTROLE DE VERSÕES	DATA	MODIFICADO POR	DESCRIÇÃO DA MUDANÇA
1.0	Julho/2022	Compliance	Versão inicial
2.0	Agosto/2023	Compliance	Atualização
3.0	Outubro/2023	RRZ Consultoria	Proteção de Dados
4.0	Dezembro/2024	Compliance	Revisão Anual

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO DA CHIMERA CAPITAL ASSET MANAGEMENT LTDA.

Eu,_____, portador da Cédula de Identidade RG nº_____, inscrito no CPF/ME sob o nº _____, declaro para os devidos fins que:

1. Tenho total conhecimento da existência da presente Política de Segurança Cibernética e da Informação ("**Política Cibernética**") da Chimera Capital Asset Management Ltda. ("**Sociedade**"), 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 desta Política Cibernética da Sociedade poderá implicar na caracterização de falta grave, fato que poderá ser passível da aplicação das penalidades cabíveis, inclusive demissão ou desligamento, conforme o caso.

3. As regras estabelecidas na presente Política Cibernética 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 nesta Política Cibernética é aderido, por meio do presente termo, em caráter irrevogável e irretratável, por prazo indeterminado, válido enquanto perdurar o 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 nas instruções publicadas na CVM, conforme alterada, acerca de divulgação e o uso de informações sobre ato ou fato relevante na negociação de valores mobiliários de emissão de companhias abertas.

São Paulo, [--] de [--] de 202[-].

_____

[Nome do Colaborador]