Greenbay
Investimentos

POLÍTICA DE SEGURANÇA E SIGILO DAS INFORMAÇÕES

GREENBAY INVESTIMENTOS LTDA

MARÇO 2022 – VERSÃO 2.0

SUMÁRIO

1. INTRODUÇÃO E OBJETIVO

1.1. Nos termos da Res. CVM nº 50, de 31 de agosto de 2021 ("Res. CVM 50"), a Política de Segurança e Sigilo das Informações da GREENBAY INVESTIMENTOS LTDA ("Gestora") visa proteger as informações de sua propriedade e/ou sob sua guarda, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas ("Política").

1.2. Esta Política em conjunto com a Política de Privacidade, disponível publicamente no *website* da Gestora, tem por objetivo atender também a Lei 13.853 de 8 de julho de 2019 – Lei Geral de Proteção de Dados Pessoais ("LGPD").

1.3. Sendo assim, nenhuma informação confidencial, reservada ou privilegiada e sensível deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Gestora, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais relacionadas à empresa.

1.4. Qualquer informação sobre a Gestora, ou de qualquer natureza relativa às atividades da empresa e a seus sócios, colaboradores e clientes, obtida em decorrência do desempenho das atividades normais do colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos se houver consentimento prévio ou solicitação do titular, ou situação de exceção de consentimento prevista na legislação como para o cumprimento de obrigação de requisição de autoridades.

1.5. Esta Política aplica-se a todos os sócios, diretores, funcionários, trainees e estagiários da Gestora (em conjunto os "Colaboradores" e, individualmente, o "Colaborador"), prestadores de serviços, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Gestora, ou que a Gestora acesse informações a ela pertencentes.

1.6. Todo e qualquer usuário de acessos computadorizados ou digitais da Gestora tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

2. RESPONSABILIDADE

2.1 A Diretora de Riscos e *Compliance* é responsável por esta Política.

3. SEGURANÇA DE INFORMAÇÕES

3.1 As medidas de segurança da informação utilizadas pela Gestora têm por finalidade minimizar as ameaças ao patrimônio, à imagem e aos negócios da empresa.

3.2 Para fins desta Política, considera-se:

I. Informação pública:

II. Informação restrita:

III. Informação confidencial:

IV. Informação reservada ou privilegiada:

V. Informação sensível:

3.3 Todas os documentos da Gestora devem ser classificados, nos termos descritos acima, pela área de Riscos e *Compliance*. As definições de que trata o item anterior devem ser de conhecimento de todos os Colaboradores.

3.4 O acesso às informações previstas no item 3.2. desta Política são controlados pela área de Riscos e *Compliance* da Gestora. A área de Riscos e *Compliance* faz o monitoramento dos acessos, e, caso haja desligamento de Colaborador, ou transferência de Colaborador para outra área da Gestora, a área de recursos humanos informará imediatamente à área de Riscos e *Compliance* para que os acessos sejam bloqueados ou alterados, conforme o caso.

3.5 Todos os Colaboradores devem assinar, de forma manual ou eletrônica, documento de confidencialidade sobre as informações confidenciais, sensíveis, reservadas ou privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais, excetuadas as hipóteses permitidas em lei. Os terceiros contratados que tiverem acesso às informações confidenciais, sensíveis, reservadas ou privilegiadas que lhes tenham sido confiadas no exercício de suas atividades, devem assinar o referido documento, podendo este ser excepcionado quando o contrato de prestação de serviço possuir cláusula de confidencialidade.

3.6 Cabe ressaltar que, em relação a informações de caráter sensível, confidencial, reservadas ou privilegiadas da empresa ou de clientes serão armazenados em diretórios de rede com acesso restrito, e controlado pela equipe de Riscos e *Compliance* da Gestora. É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis da Gestora e circulem em ambientes externos à empresa sem prévia autorização da Diretora de Riscos e *Compliance*.

3.7 A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora. 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. Ainda, qualquer impressão de documentos deve ser

prontamente retirada da impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Gestora.

3.8 O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação, sendo recomendável o seu descarte total.

3.9 Adicionalmente, os Colaboradores devem se abster da utilização de pen-drives, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora.

3.10 É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente autorizados. Novos equipamentos e/ou sistemas deverão ter suas configurações feitas pela equipe de TI. Todo acesso a USB para armazenamento é bloqueado via *software* nos equipamentos.

3.11 Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. Será obrigatória a alteração de senha de acesso aos equipamentos (*login* de usuário) em uma periodicidade definida, utilizando modelo de definição de senha de difícil identificação por parte de potenciais "*hackers*" externos. Tal processo será auditável e rastreável eletronicamente baseado no sistema de *logon* do sevidor e serviços de informação.

3.12 O acesso a sites e blogs, bem como o envio ou repasse por e-*mail* de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo também é terminantemente proibido, como também o envio ou repasse de *e-mails* com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Gestora.

3.13 Programas instalados nos computadores, principalmente via internet (*downloads*), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia, além de avaliação de segurança pela empresa contratada para prover suporte de TI. Não é permitida a instalação de nenhum *software* ilegal ou que possuam direitos autorais protegidos, ou mesmo legal, sem prévia autorização da Diretora de Riscos e *Compliance*. Não é permitido a instalação de *software* nos equipamentos sendo restrito à equipe de tecnologia.

3.14 Todo conteúdo que está na rede pode ser acessado pelos sócios ou pela Diretora de Riscos e *Compliance* caso haja necessidade, inclusive *e-mails*. Arquivos pessoais salvos em cada computador poderão ser acessados, caso seja necessário. A confidencialidade dessas informações deve ser respeitada, e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais, ou em atendimento a determinações judiciais ou administrativas. O acesso à rede é restrito e baseado na liberação definida previamente.

3.15 Por fim, convém ressaltar que a Gestora conta com sistemas e ferramentas contratados para arquivamento (rede), *firewall*, antivírus, *backup*, prevenção de invasão e linha de contingência.

4. INFORMAÇÕES PRIVILEGIADAS

4.1 É considerada como informação privilegiada qualquer Informação Relevante (conforme definido abaixo) a respeito de alguma empresa, que não tenha sido publicada e que seja conseguida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um Cliente, com colaboradores de empresas estudadas ou investidas ou com terceiros, ou em razão da condição de Colaborador.

4.2 Considera-se Informação Relevante, para os efeitos deste Manual de *Compliance*, qualquer informação, decisão, deliberação, ou qualquer outro ato ou fato de caráter político-administrativo, técnico, negocial ou econômico-financeiro ocorrido ou relacionado aos seus negócios da Gestora que possa influir de modo ponderável: *(a)* na rentabilidade dos valores mobiliários administrados pela Gestora; *(b)* na decisão de Clientes de comprar, vender ou manter cotas de fundos de investimento administrados pela Gestora; e *(c)* na decisão dos Clientes de exercer quaisquer direitos inerentes à condição de titular de cotas de fundos de investimento administrados pela Gestora.

4.3 As informações privilegiadas precisam ser mantidas em sigilo por todos que a acessarem, seja em função da prática da atividade profissional ou do relacionamento pessoal.

4.4 Em caso de o Colaborador ter acesso a uma informação privilegiada que não deveria ter, deverá transmiti-la rapidamente à Diretora de Riscos e *Compliance*, não podendo comunicá-la a ninguém, nem mesmo a outros membros da Gestora, profissionais de mercado, amigos e parentes, e nem usá-la, seja em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se, igualmente, relatar o ocorrido à Diretora de Riscos e *Compliance*.

4.4.1 Insider Trading e "Dicas"

4.4.1.1 *Insider trading* baseia-se na compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou para terceiros (compreendendo a própria Gestora e seus Colaboradores).

4.4.1.2 "Dica" é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada como benefício para a compra e venda de títulos ou valores mobiliários.

4.4.1.3 É proibida a prática dos atos mencionados anteriormente por qualquer membro da empresa, seja agindo em benefício próprio, da Gestora ou de terceiros.

4.4.1.4 A prática de qualquer ato em violação desta Política pode sujeitar o infrator à responsabilidade civil e criminal, por força de lei. O artigo 27-D da Lei nº 6.385, de 07 de dezembro de 1976 tipifica como crime a utilização de informação relevante ainda não divulgada ao mercado, da qual o agente tenha conhecimento e da qual deva manter sigilo, capaz de propiciar, para si ou para outrem, vantagem indevida, mediante negociação, em nome próprio ou de terceiro, com valores mobiliários. As penalidades previstas para esse crime são tanto a pena de reclusão, de 1 (um) a 5 (cinco) anos, bem como multa de 3 (três) vezes o montante da vantagem ilícita obtida em decorrência do crime. Além de sanções de natureza criminal, qualquer violação da legislação vigente e, portanto, desta Política, poderá, ainda, sujeitar o infrator a processos de cunho civil e administrativo, bem como à imposição de penalidades nesse âmbito, em conformidade com a Lei nº 6.404, de 15 de dezembro de 1976 e a Instrução CVM nº 358, de 03 de janeiro de 2002 ("Instrução CVM 358").

4.4.1.5 É de responsabilidade da Diretora de Riscos e *Compliance* verificar e processar periodicamente as notificações recebidas a respeito do uso pelos Colaboradores de informações privilegiadas, *insider trading* e "dicas". Casos envolvendo o uso de informação privilegiada, *insider trading* e "dicas" devem ser analisadas não só durante a vigência do relacionamento profissional do Colaborador com a Gestora, mas mesmo após o término do vínculo, com a comunicação do ocorrido às autoridades competentes, conforme o caso.

5. SERVIÇOS DE REDE

5.1 As redes de serviços são segmentadas para garantia à segurança e desempenho entre elas. Está implantado um sistema de prevenção de invasão na rede e nos equipamentos para garantir a segurança da informação e disponibilidade de serviços.

6. ARMAZENAMENTO DE DADOS

6.1 O armazenamento de dados (*backup*) é realizado diariamente em *cloud* e localmente, sendo disponível para *restore* após liberação do responsável de segurança da informação.

7. INSTALAÇÕES FÍSICAS DE TECNOLOGIA / ACESSO FÍSICO

7.1 Para garantir o ambiente em alta disponibilidade está implantado um *nobreak* central para assegurar problemas de energia até a entrada do gerador. O sistema de ar-condicionado está implantado no CPD. O acesso físico ao CPD é controlado e autorizado somente para pessoas da equipe de tecnologia da informação ou afins.

8. INDISPONIBILIDADE DE ACESSO A INFORMAÇÕES

8.1 Em caso de problemas de indisponibilidade de acesso à informação, o processo de contingência é acionado, sendo avaliado o impacto sobre o negócio (conforme Plano de Continuidade do Negócio)

9. TREINAMENTO DE SEGURANÇA DAS INFORMAÇÕES

9.1 A Gestora entende essencial que o seu treinamento anual, supervisionado pela Diretora de Riscos e *Compliance*, abranja todos os preceitos contidos na presente Política, de modo que seus Colaboradores estejam sempre cientes e consonantes aos procedimentos de segregação e segurança das informações.

10. RELATÓRIO DE TESTES DE SEGURANÇA DAS INFORMAÇÕES

10.1 Anualmente, a Gestora realizará testes dos seus sistemas de segurança de informações, bem como de todos os preceitos contidos na presente Política, incluindo, mas não se limitando, aos procedimentos de descarte de informações pelos Colaboradores, individualização dos usuários, dentre outros.

10.2 Todos os resultados desses testes, bem como os procedimentos para saneamento de eventuais problemas, serão descritos no Relatório Anual de Controles Internos da Gestora.

10.3 Estes testes serão realizados pela equipe de suporte de TI contratada, e buscará cobrir os seguintes pontos:

a. Identificação e avaliação de potenciais riscos cibernéticos, envolvendo ativos de hardware e software, além de processos que necessitem de proteção. Importante estimar impactos financeiros, operacionais e reputacionais em caso de evento;

b. Estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade de identificação de riscos, de forma buscar evitar eventuais ataques cibernéticos aos dados e equipamentos da empresa;

c. Detecção de possíveis anomalias e/ ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados;

d. Criação de um plano de resposta e recuperação de incidentes, que contenha comunicação interna e externa, se necessário. Tal plano será elaborado em conjunto entre as áreas internas de Riscos e *Compliance*, e da empresa de TI contratada, e terá testes anuais para validar sua eficiência. O plano identificará papéis e responsabilidades, com previsão de acionamento de colaboradores e contatos externos;

e. Manter tal programa de segurança cibernética atualizado, identificando novos e potenciais riscos, ativos e processos.

10.3 As documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigantes, deverão ser mantidas em diretório interno da área de Riscos e *Compliance* como evidência em eventuais questionamentos internos ou de órgãos reguladores ou autorreguladores.

10.4 Os temas relacionados à segurança da informação serão tratados trimestralmente no Comitê de Riscos e *Compliance*, de forma ordinária, ou mesmo em reunião específica, em casos de eventos extraordinários, para que sejam tomadas de forma tempestiva medidas de recuperação, limitação de danos, e resposta relevante.

11. VIGÊNCIA E ATUALIZAÇÃO

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

Versão	**Data**	**Alteração**	**Responsável**
1.0	Outubro/2020	Versão Original	Diretora de Riscos e *Compliance*
1.1	Dezembro/2021	Revisão	Diretora de Riscos e Compliance
2.0	Março/2022	Adequação à LGPD	Diretora de Riscos e *Compliance*