REGISTRO DE REVISÕES

Número de revisão	Data	Seção	Alterações realizadas
00	2018/04/16	Todo o documento	Criação da política
01	2020/07/23	2, 4.3, 4.7, 4.9, 4.11 e glossário	2. Mudança na área que aprova a política (anteriormente o Conselho de Administração, agora o Comité de Auditoria), e as responsabilidades da Direcção de Risco de Informação e Conformidade. 4.3 Os aspectos de protecção estão incluídos, independentemente de onde se acede à informação. 4.4 O estudo de segurança está incluído na política. 4.7 O estudo de segurança está incluído. 4.9 O termo plano de formação é modificado para programa cultural. 4.11 O termo Ciber-segurança está incluído. Glossário, incluindo definições de Segurança da Informação e Ciber-segurança.
02	2022/04/01	Todo o documento	Alteração do nome da empresa para Veículo de Investimento 1 Limited.
03	2022/11/10	Todo o documento	Alteração da responsabilidade do Comité de Auditoria; alteração do nome do Departamento de Riscos e Conformidade com a Informação e inclusão de novas responsabilidades; alinhamento com os critérios de classificação da informação; actualização das referências documentais.
03	2023/10/26	Todo o documento	O documento foi revisado e não modificações.
03	2024/06/24	Todo o documento	O documento foi revisado e não modificações.
04	2025/04/30	Todo o documento	O documento foi revisado e não modificações.
05	2025/10/03	2.2., 2.3., 3.6. 3.10, 3.12, Glossário e Documentos de referência	• Ajustes ou novas funções ou responsabilidades da Direção de Riscos e Conformidade e da Organização, seus funcionários, diretores, funcionários (diretos ou terceirizados) e terceiros vinculados (fornecedores e contratados). • Alteração do termo “colaboradores” por “funcionários” • Foram incluídas diretrizes ou conceitos associados a: Inteligência artificial, Sistema de Gestão de Segurança da Informação,

			Continuidade do negócio, trabalho remoto, proteção da cadeia de fornecimento de terceiros, identidade digital, obsolescência tecnológica. • Atualização de documentos de referência.

CONTEÚDO

1. OBJETIVO E ALCANCE

1.1 Objetivo

O objectivo desta política é estabelecer as diretrizes de segurança da informação e segurança cibernética necessárias para a proteção da informação de Investment Vehicle 1 Limited ("a Empresa") e de qualquer uma das suas subsidiárias (a "Organização"), contra situações que possam afetar a Confidencialidade, Integridade e Disponibilidade (como definido abaixo) das informações da Organização e que possam causar impacto financeiro, jurídico, competitivo e/ou reputacional da Organização.

1.2 Alcance

O âmbito inclui todas as informações e recursos valiosos (Tecnologias de Informação e Comunicação -TICs-, Instalações e Tecnologias Operacionais -OTs-) associados ou pertencentes à Organização ou administrados por Terceiros (fornecedores e contratados), fazem parte do alcance. o formato, meio, em todas as suas formas (digital, manuscrita, falada, impressa), apresentação e/ou local onde se encontra, incluindo o ciberespaço.

2. RESPONSABILIDADES

O Departamento de Riscos e Conformidade com a Informação, é a área responsável por formular a Política, divulgá-la, revisá-la pelo menos uma vez por ano e mantê-la atualizada; monitorizar o cumprimento, de acordo com a missão e visão da Organização, e o cumprimento da regulamentação aplicável a à Organização, reportando ao Comitê de Auditoria da Empresa (o "Comité de Auditoria") os assuntos relevantes sobre Segurança da Informação e Segurança cibernética.

Diferentes instâncias participam da governança de Segurança da Informação e Segurança cibernética em todas as empresas descritas no alcance, que possuem as responsabilidades a seguir:

2.1. Aprovação da política

O Comitê de Auditoria é responsável por ratificar esta política e suas atualizações, monitorar o perfil de risco da informação, promover a cultura da Informação e Segurança cibernética, promover o cumprimento de suas diretrizes, alocar recursos para compliance, bem como o monitoramento geral do cumprimento desta Política.

O Departamento de Riscos e Conformidade com a Informação, tem autoridade para gerenciar a revisão da Política e a sua apresentação ao Comité de Auditoria para ratificação.

2.2. Departamento de Riscos e Conformidade com a Informação

- Definir o âmbito do programa de Segurança da Informação e Segurança cibernética para proteger a confidencialidade, integridade e disponibilidade da informação da empresa,

garantindo a conformidade regulamentar e implementando boas práticas e metodologias de reconhecido valor técnico aplicáveis à indústria.

- Promover a gestão eficaz dos riscos cibernéticos e de segurança da informação, através da identificação, análise, avaliação e tratamento dos mesmos.
- Definir processos para a atualização permanente das novidades dos marcos regulatórios relacionados à Segurança da Informação e Segurança cibernética.
- Apoio no atendimento e resposta a alertas e incidentes de segurança da informação e segurança cibernética identificados por funcionários, terceiros relacionados e derivados do monitoramento feito através das plataformas de gestão de segurança da informação que afetam os processos, recursos tecnológicos e sistemas da Organização.
- Definir um programa de gestão de recuperação tecnológica para garantir a disponibilidade e continuidade das operações definidas pela BIA (Business Impact Analysis) como críticas para o negócio, diante de eventuais interrupções.
- Com o apoio do Departamento Geral Jurídico, monitorizar o nível de cumprimento das leis e regulamentos aplicáveis sobre Segurança da Informação e Segurança cibernética.
- Monitorar o cumprimento do programa de Sistema de Gestão de Segurança da Informação e Segurança cibernética, de acordo com a missão e visão da Organização, e o cumprimento da regulamentação aplicável a cada uma de suas empresas.
- Através do Departamento Jurídico, estabelecer e manter contatos com as autoridades, grupos especiais ou de interesse relevantes para a segurança da informação e segurança cibernética.
- Apoiar a Organização nas ações para implementação de medidas ou controles para o cumprimento desta política.

2.3. A Organização, os seus funcionários, directores, empregados (directos ou subcontratados) e terceiros relacionados (fornecedores e contratantes) que têm acesso às informações da Organização, quer numa base regular ou ocasional, no desempenho das suas funções, são responsáveis por:

- O conhecimento da Política e cumprimento da mesma juntamente com qualquer manual, procedimento ou instrução estabelecidos para a sua aplicação e mencionados no final do documento.
- A implementação da Política juntamente com quaisquer manuais, procedimentos ou instruções estabelecidas para a aplicação da Política.
- Assumir a gestão do risco do tratamento da informação da organização e a implementação das acções relevantes para a sua mitigação.
- Considerar os requisitos de segurança da informação e segurança cibernética em seus processos, iniciativas, projetos e contratos.
- Identificar e comunicar o Departamento de Riscos e Conformidade com a Informação potenciais eventos ou incidentes que ameacem ou possam prejudicar a informação corporativa o cumprimento das políticas e/ou procedimentos de segurança da informação.
- Monitorar o nível de conformidade com as leis e regulamentos aplicáveis sobre segurança da informação e segurança cibernética.
- Usar os recursos tecnológicos ou as informação da organização com responsabilidade e somente, em ambientes ou aplicações aprovados pela CIO (incluindo os relacionados com IA) para fins autorizados.
- Identificar e alertar o Departamento de Riscos e Conformidade para as actuais e emergentes ameaças cibernéticas e riscos cibernéticos que possam afectar a organização.

- Cumprir as práticas da Organização para uso adequado e seguro de informações ou ferramentas de autenticação (senhas, códigos de acesso, MFA, Passwordless).
- Gerenciar as identidades digitais e atribuição de privilégios mínimos para acesso às informações em seus diferentes meios e de acordo com as responsabilidades; bem como solicitar a eliminação oportuna das identidades digitais e acessos quando não forem necessários.
- Os líderes dos processos devem garantir o cumprimento do princípio da segregação de funções, de forma a minimizar o risco de concentração de responsabilidades críticas numa única pessoa.
- Definir planos de contingência operacionais ou tecnológicos necessários para manter a continuidade dos processos ou serviços críticos da empresa. Estes devem ser testados periodicamente para se manterem eficazes.

3. CONTEÚDO

- **Aspectos gerais e específicos da política.**

3.1 A Organização reconhece que a informação é um insumo indispensável para a execução de processos, tomadas de decisão no desenvolvimento de objetivos de negócios e para a concepção e definição de produtos e serviços que constituem o diferencial do que estamos diante de nossos clientes, funcionários e associados. Também reconhece a importância de prevenir riscos de segurança da informação e segurança cibernética ao longo de seu ciclo de vida; essa proteção é emoldurada por 3 propriedades:

- **Confidencialidade**: As informações não devem ser disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados.
- **Integridade**: A precisão, confiabilidade e integridade das informações devem ser preservadas.
- **Disponibilidade**: As informações devem ser acessíveis e utilizáveis quando solicitadas por um indivíduo, área ou processo autorizado e quando necessário.

3.2 Devem ser identificadas as informações e recursos valiosos associados às informações que a Organização utiliza para o desenvolvimento de seus objetivos de negócios; as informações e outros recursos associados devem ser atribuídos a uma pessoa responsável, que deve tomar as decisões pertinentes à sua proteção, de acordo com os requisitos internos e regulamentos aplicáveis a cada empresa.

3.3 Todas as informações, independentemente do meio em que são encontradas ou do local de onde são acessadas, devem ser classificadas para estabelecer sua sensibilidade (o nível de confidencialidade que deve ser mantido sobre seu conteúdo) e sua criticidade (o nível de disponibilidade exigido para que as operações comerciais não sejam interrompidas). É responsabilidade de todos os membros da Organização conhecer a classificação das informações que utilizam para o desenvolvimento de suas atividades; e dos responsáveis pelos processos de definição dos controles para proteger a informação de acordo com a classificação tratada por cada empresa que faz parte da organização.

3.4 Organização identifica as seguintes informações, entre outras, como informações confidenciais ou privilegiadas, uma vez que a definição de informações confidenciais deve ser feita numa base casuística:

- Ações na bolsa de valores, informações estratégicas e financeiras, informações sobre alianças estratégicas, relatórios sobre projeções, resultados e/ou divulgações financeiras.
- Informações sobre clientes, funcionários, acionistas, terceiros relacionados, empreiteiros, fornecedores, viajantes, usuários, investidores.
- Informações privilegiadas para eventos importantes e confidenciais da empresa.
- Informação material não pública. Exemplos incluem informação sobre fusões, projectos estratégicos, alienações, alterações na política de dividendos, informação sobre parceiros de negócios, informação sobre accionistas, entre outros.
- Informações comerciais que a organização é obrigada a proteger, patentes, invenções, acordos comerciais, contratos, código-fonte de desenvolvimento de software ou outros que tenham potencial para fornecer vantagem competitiva.
- Práticas para otimizar receitas, preços, taxas líquidas.
- Informações sobre a operação e seus processos associados.
- Relatórios de segurança, riscos, conformidade, relatórios de auditoria interna e externa, incidentes operações, incidentes de segurança da informação e segurança cibernética, investigações e questões legais relacionados com qualquer um dos acima referidos.
- Relatórios para ou de entidades reguladoras que incluam informação confidencial.
- Chaves, pinos, senhas ou informações de usuários de rede e/ou aplicativos corporativos.
- Informações sujeitas às leis de proteção de dados pessoais (inclui dados de cartões de pagamento) nas diversas jurisdições em que a Organização está localizada ou opera.

As informações acima referidas, e quaisquer outras informações que, em virtude da sua classificação, sejam consideradas confidenciais ou privilegiadas, não podem ser utilizadas para benefício pessoal de qualquer director, funcionário ou terceiro que a elas tenha acesso, nem para fins diferentes dos inicialmente previstos para tais informações.

3.5 É dever de todos os responsáveis pelos processos, líderes de projetos ou iniciativas e administradores de contratos, assegurar que os riscos de informação sejam identificados, analisados, avaliados, tratados e monitorados, de acordo com os procedimentos do Departamento de Riscos e Conformidade com a Informação, assegurando que os riscos correspondentes são mantidos dentro dos níveis de risco aceitáveis para a Organização de acordo com as disposições do MA_AVSG04_054 INFORMAÇÕES MANUAL DE GESTÃO DE RISCO.

3.6 Recursos de informação como: equipamentos, aplicativos de negócios, serviços de Internet, Intranet, ferramentas colaborativas (e-mail, chat, armazenamento na nuvem), entre outros; são fornecidos aos funcionários para uso exclusivo do negócio. O acesso e uso destes devem ser autorizados pelo responsável por cada um dos recursos e de acordo com as responsabilidades de sua função. Os recursos de informação devem ser devolvidos imediatamente ao administrador quando não forem mais necessários.

3.7 A Organização deve assegurar que os seus funcionários, qualquer oficial, gestor ou qualquer pessoa implementem medidas de segurança da informação, tais como e não se limitam a: verificações e investigações sobre referências pessoais, trabalho, experiência de trabalho, testes complementares, estudo de segurança, aptidão e teste de conhecimento, de forma que apoiem políticas de segurança e em conformidade com as regulamentações locais.

3.8 Todos os funcionários e terceiros relacionados são considerados obrigados a lidar com a confidencialidade das informações da Organização independente, tendo assinado ou não um acordo de confidencialidade no momento em que entram na Organização; e são responsáveis pela reserva de informações mesmo após o término de seu relacionamento com a Organização.

3.9 A Organização deve ter um programa de cultura permanente em segurança da informação e segurança cibernética que permita manter todo o seu pessoal informado sobre as políticas, responsabilidades de segurança da informação e as ameaças contínuas que colocam em risco as informações que gerencia e/ou processa.

3.10 Os responsáveis pelos contratos e contratações devem garantir que as responsabilidades de segurança da informação de terceiros e da sua cadeia de abastecimento, que tenham acesso para processar, armazenar ou distribuir informações de valor à organização, estejam documentadas nos contratos ou outros acordos de prestação de serviços e devem monitorar o cumprimento durante todo o ciclo de vida da relação contratual.

3.11 É dever de toda a Organização e de terceiros relacionado comunicar qualquer suspeita condição anormal ou violação das políticas, responsabilidades e procedimentos de segurança da informação e Segurança cibernética que ameacem a Confidencialidade, Integridade e Disponibilidade das informações da Organização imediatamente através dos canais estabelecidos pela Organização.

Caso as situações acima descritas afectem ou tenham a possibilidade de afectar ou ter um impacto económico, material, reputacional, legal ou operacional na Organização, devem ser imediatamente comunicadas ao Departamento de Riscos e Conformidade através dos canais estabelecidos por este último.

O Departamento de Riscos e Conformidade com a Informação deve avaliar os relatos de incidentes e verificar se atendem aos critérios de materialidade, devendo, nesse caso, informar o Departamento de Relações com Investidores para que cumpra a Política de Divulgação de Informações Financeiras e Não Financeiras Relevantes para investidores e terceiros interessados.

3.12 A Organização tem a responsabilidade de implementar medidas técnicas para a proteção da informação que é armazenada, processada ou transmitida; de acordo com sua classificação e considerando, mas não limitado a:

- Gerenciamento de risco da informação
- Identificação e classificação de ativos de informação
- Controles para o armazenamento seguro e transferência de dados.
- Proteção contra ameaças, como software malicioso e/ou possíveis ataques ao computador.
- Gestão de identidades digitais e controle de acesso a informações, aplicativos, infraestrutura e redes.
- Gestão da segurança em dispositivos móveis/portáteis próprios ou pessoais ao serviço da Organização.
- Uso adequado dos recursos atribuídos pela organização (internet, dispositivos tecnológicos corporativos, sites colaborativos: Sharepoint, Onedrive, Teams, e-mail, outros)
- Segurança em redes e telecomunicações
- Segurança na aquisição, desenvolvimento e manutenção de recursos tecnológicos (incluindo sistemas e ambientes de processamento e gestão da obsolescência tecnológica).
- Gerenciamento de mídia de armazenamento removível
- Segurança do pessoal interno e terceiros
- Gestão de vulnerabilidades técnicas
- Segurança na nuvem
- Gerenciamento de logs, eventos e incidentes de segurança
- Segurança física e ambiental em centros de processamento de dados ou locais críticos.
- Controles para instalação, desenvolvimento e armazenamento de software.
- Continuidade do negócio, backup e recuperação de informações de plataformas tecnológicas em caso de desastres.
- Trabalho remoto ou fora das instalações.
- Uso ou desenvolvimento responsável de tecnologias de Inteligência Artificial (IA).

3.13 O Departamento de Risco de Informação poderá realizar atividades de monitoramento e auditoria em qualquer empresa da Organização, exclusivamente, para determinar o grau de cumprimento das diretrizes estabelecidas nesta política. Incluindo terceiros e empresas subcontratadas que prestam serviços de gestão, monitoramento e administração de plataformas tecnológicas da Investment Vehicle 1 Limited technology.

- **Regulamento legal vigente aplicável à política.**

3.14 A Organização, o seu Conselho de Administração e o seu grupo executivo devem estar empenhados no cumprimento dos requisitos de segurança da informação estabelecidos em suas políticas internas de segurança, bem como aqueles exigidos pelas leis e regulamentos aplicáveis, tais como e não limitados a: SOX (Sarbanes-Oxley Act), PCI DSS (Payment Card Industry Data Security Standards), leis internacionais de proteção de dados pessoais, regulamentos do setor aeronáutico, acordos industriais ou contratuais, licenciamento, propriedade intelectual e outros relacionados à segurança da informação e segurança cibernética.

3.15 Em caso de descumprimento da Política e/ou dos procedimentos de segurança estabelecidos ou subsequentes, a Organização avançará com as medidas legais, administrativas e/ou disciplinares cabíveis; de acordo com as disposições do Regulamento Interno de cada uma de suas empresas e/ou leis e regulamentos internacionais e/ou locais aplicáveis de segurança da informação, segurança cibernética e proteção de dados pessoais.

- **Data de vigência da política.**

3.16 Esta política é eficaz a partir do momento da sua publicação e permanecerá em vigor indefinidamente, a menos que seja alterada para a actualizar de acordo com as mudanças no ambiente organizacional, circunstâncias comerciais e/ou condições legais. Em relação a terceiros, a política entrará em vigor quando as autorizações correspondentes (assinaturas de contrato) tiverem sido obtidas.

- **Precedência.**

3.17 Em caso de conflito entre os Protocolos do Conselho de Administração, o Acordo de Investidor e esta Política, a ordem de precedência dos documentos será a seguinte (i) o Acordo de Investidor, (ii) os Protocolos do Conselho de Administração, (iii) esta Política.

- **Glossário.**

Acordo do investidor: Acordo dos accionistas da empresa.

Cadeia de abastecimento: No âmbito da segurança da informação, é o conjunto de processos, organizações, pessoas, atividades, tecnologias e terceiros vinculados (fornecedores, parceiros e contratados) envolvidos no ciclo de vida de produtos, serviços ou informações, cujo funcionamento adequado, confiança e proteção são essenciais para garantir a confidencialidade, integridade e disponibilidade das informações da organização.

Centro de Processamento de Dados (Data Centre): Site físico ou nebuloso (virtual) para a manutenção da infra-estrutura tecnológica e electrónica, onde são processadas as informações necessárias para a execução dos processos da Organização.

Espaço cibernético: Ambiente resultante da interação de pessoas, softwares e serviços na Internet por meio de dispositivos tecnológicos conectados à referida rede, que não existe em nenhuma forma física. (Circular Externa da Superintendência Financeira 007, 2018)

Segurança cibernética: É o desenvolvimento de capacidades de negócios para defender e antecipar ameaças cibernéticas para proteger e proteger dados, sistemas e aplicativos no espaço cibernético que são essenciais para a operação da entidade. (Circular Externa da Superintendência Financeira 007, 2018)

IA: Inteligência Artificial.

Identidade: Refere-se à identificação de pessoas nas aplicações da organização. Para os funcionários, a identidade está registrada no SAP SSFF (SuccessFactors) e é reconhecida pelo número de funcionário. No caso de terceiros vinculados, as identidades são registradas no Mestre de terceiros da ferramenta de Gestão de Identidades e são reconhecidas pelo número de identificação; em países onde a legislação de dados pessoais assim o exigir, serão utilizados outros dados, como carteiras de habilitação, número fiscal ou outro identificador permitido. Para criar um usuário em um aplicativo, é imprescindível que a identidade esteja registrada e ativa.

Identidade digital: Conjunto de informações sobre uma pessoa que existe no ambiente digital e que permite identificá-la de forma única.

Incidente de segurança cibernética: Ocorrência de uma situação que afete a proteção ou segurança dos dados, sistemas e aplicações da entidade que sejam essenciais para o negócio. (Circular Externa da Superintendência Financeira 007, 2018)

Risco (NTC-ISO31000): Efeito da incerteza sobre os objetivos.
NOTA 1: Um efeito é um desvio do que era esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças.
NOTA 2: Os objetivos podem ter diferentes aspectos e categorias, e podem ser aplicados em diferentes níveis.
NOTA 3: O risco é muitas vezes expresso em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades.

Risco de Informação (NTC-ISO/IEC 27005): Potencial para uma determinada ameaça explorar vulnerabilidades em ativos ou grupos de ativos, causando danos à organização. É medido em termos de uma combinação da probabilidade de um evento acontecer e suas consequências.

Risco de segurança cibernética (NISTIR 8286 com base no ISO Guide 73 e NIST SP 800-60 Vol. 1 Rev. 1): Um efeito de incerteza em ou dentro de um contexto digital. Os riscos de segurança cibernética estão relacionados à perda de confidencialidade, integridade ou disponibilidade de informações, dados ou sistemas de informação (ou controle) e refletem os possíveis impactos adversos nas operações da organização (ou seja, missão, funções, imagem ou reputação) e ativos, indivíduos, outras organizações e a Nação.

Segurança da informação: Conjunto de políticas, estratégias, metodologias, recursos, soluções informáticas, práticas e competências para proteger, garantir e preservar a confidencialidade, integridade e disponibilidade da informação armazenada, reproduzida ou processada nos sistemas informáticos da entidade ou outros meios. (Circular Externa da Superintendência Financeira 007, 2018)

Segregação de funções: Uma medida que separa as responsabilidades das diferentes actividades envolvidas nos processos críticos da Empresa.

- **Documentos de referência:**

Política de continuidade do negócio

MSG-016 Manual Geral de Segurança da Informação. Corporativo

MSG-017 Manual de Diretrizes Específicas de Segurança da Informação – Áreas de Tecnologia da Informação

Manual interno para a proteção de dados pessoais

Manual de Gestão de Riscos da Informação

Manual do Sistema de Gestão da Segurança da Informação

Manual Plano de Recuperação em caso de Desastres DRP

IN_SO0113_01 Usuários e senhas de segurança

Procedimento de inteligência de ameaças de segurança da informação e segurança cibernética
PR_SO0114_02 Procedimento para tratamento e resposta a incidentes de Segurança da Informação e Segurança cibernética

IN_AVSG04_008 Instruções para comunicação interna e avaliação de materialidade de Incidentes Cibernéticos.

Outros procedimentos e instruções associados ao quadro normativo da segurança da informação.