REVIEW REGISTER

Revision Number	Date	Section	Changes Made
00	2018/04/16	Entire document	Creation of the Policy
01	2020/07/23	2, 4.3, 4.7, 4.9, 4.11 and glossary	2. Change in the approving entity (before the Board, then the Audit Committee), and the responsibilities of Information Risk and Compliance Department 4.3. Information protection aspects regardless of where the information is accessed are included. 4.7. A security study is included. 4.9. The term training plan is changed to culture program. 4.11. The term Cybersecurity is included. Glossary. Definitions of information security and cybersecurity are included.
02	2022/04/01	Entire document	Change of the company's name to Investment Vehicle 1 Limited
03	2022/11/10	Entire document	Change in the responsibility of the Audit Committee; change in the name of the Information Risk and Compliance area and inclusion of new responsibilities; alignment with information classification criteria; update of documentary references.
03	2023/10/26	Entire document	Review of the document without modifications.
03	2024/06/24	Entire document	Review of the document without modifications.
04	2025/04/30	Entire document	Review of the document without modifications.
05	2025/10/03	2.2., 2.3., 3.6. 3.10, 3.12, glossary and referenced documents	• Adjustments or new functions or responsibilities of the Risk and Compliance Department and the Organization, its officers, directors, employees (direct or subcontracted), and third parties (suppliers and contractors). • Guidelines or concepts associated with the following were included: Artificial intelligence, Information Security Management System, Business continuity, Remote working, Third-party supply chain protection, Digital identity, technological obsolescence. • Updating of reference documents.

CONTENT

1. PURPOSE AND SCOPE

1.1 Purpose

This policy seeks to establish the information security and cybersecurity guidelines required for the protection of the information of Investment Vehicle 1 Limited (the "Company") and any of its subsidiaries (with the Company the "Organization"), against situations that may affect the Confidentiality, Integrity and Availability (as defined below) of the information of the Organization and that may cause financial, legal, competitive and/or reputational impact on the Organization (the "Policy").

1.2 Scope

The scope includes all the information and valuable resources (Information and Communications Technologies -ICTs-, Facilities, and Operational Technologies -OTs-) associated to or that belongs to the Organization or that is managed by third parties (suppliers and contractors), regardless of the format, medium, in all its forms (digital, handwritten, spoken, printed), presentation and/or place where it is located, including cyberspace.

2. RESPONSIBILITIES

The Risk and Information Compliance Department, is the area responsible for formulating the Policy, disclosing it, reviewing it at least once a year and keeping it updated; monitoring that it is complied with, in accordance with the mission and vision of the Organization, and compliance with the regulations applicable to the Organization, reporting to the Audit Committee of the Company (the "Audit Committee") the relevant matters on information security and cybersecurity.

In the governance of Information Security and Cybersecurity, different instances participate in all the companies described in the scope which have the following responsibilities:

2.1. Policy approval

The Audit Committee is responsible for ratifying this policy and its updates, monitoring the information risk profile, promoting the culture of information security and cybersecurity, encouraging compliance with its guidelines, allocating resources for compliance, as well as generally monitoring compliance with this Policy.

The Risk and Information Compliance Department has the authority to manage the review of the Policy and its submission to the Audit Committee for its ratification.

2.2. Information Risk and Compliance Department functions

- Define the scope of the Information Security and Cybersecurity program that seeks to protect the Confidentiality, Integrity and Availability of the Organizations information, ensuring

regulatory compliance and implementing best practices and methodologies of recognized technical value applicable to the industry.

- To promote the effective management of cyber and information security risks, through the identification, analysis, evaluation, and treatment of these risks.
- Define processes for the permanent updating of new developments in the regulatory frameworks related to Information Security and Cybersecurity.
- Support the response to information security and cybersecurity alerts and incidents identified by employees, related third parties and derived from the monitoring done through the information security management platforms that affect the processes, technological resources and systems of the Organization.
- Define a technology recovery management program to ensure the availability and continuity of critical business functions or process in the event of interruptions.
- With the support of the Legal Department, monitor the level of compliance with applicable laws and regulations on Information Security and Cybersecurity.
- Monitor compliance with the Information Security and Cybersecurity program and management system, in accordance with the Organization's mission and vision, and compliance with the regulations applicable to each of its companies.
- Through the Legal Department, establish and maintain contacts with authorities, special or interest groups relevant to information security and cybersecurity.
- Support the Organization in actions for the implementation of measures or controls for compliance with this policy.

2.3. The Organization, its officers, directors, employees (direct or outsourced) and related third parties (suppliers and contractors) who have access to the Organization's information, whether on a regular or occasional basis, in the performance of their duties, are responsible for:

- The knowledge and compliance with this Policy, and the related manuals, procedures, or instructions at the end of the document.
- The implementation of the Policy along with any manual, procedure or instruction established for the implementation of it.
- Assuming the risk management of handling the Organization’s information and the implementation of pertinent actions for its mitigation.
- Considering information security and cybersecurity requirements in its processes, initiatives, projects and contracting.
- Identifying and reporting to the Information Risk and Compliance Department potential events or incidents that threaten or might have the ability to risk compliance with information security policies and/or procedures.
- Follow up on the level of compliance with applicable laws and regulations on information security and cybersecurity.
- Using the Organization´s technological resources or information responsibly, in environments or applications approved by the CIO (including those associated with AI) and only for authorized purposes.
- Identification and reporting alert the Information Risk and Compliance Department of current and emerging cyber threats and cyber risks that may affect the Organization.
- Complying with the Organization's practices for the protected and secure use of authentication information or authentication tools (passwords, access codes, MFA, passwordless).

- and assignment of minimum privileges for access to information in its different media. Manage digital identities and assign minimum privileges for access to information in its various media and in accordance with responsibilities; as well as request the deletion of digital identities and accesses when they are no longer necessary and in a timely manner.
- Process leaders must ensure that processes comply with the principle of Segregation of Duties, in order to minimize the risk of concentrating critical responsibilities in a single person.
- Definition of operational or technological contingency plans necessary to maintain the continuity of the company's critical processes or services. These must be tested periodically to ensure they remain effective.

3. CONTENT

- **General and specific aspects of the Policy.**

3.1 The Organization recognizes that information is an indispensable input for the execution of processes, decision making in the development of business objectives and for the design and definition of the products and services that constitute the differentiating factor of what we are to our customers, collaborators and associates. It also recognizes the importance of preventing information security and cybersecurity risks throughout their lifecycle; such protection is framed by 3 properties:

- **Confidentiality**: The information must not be made available or disclosed to unauthorized individuals, entities or unauthorized processes.
- **Integrity**: The accuracy, reliability, and completeness of the information must be preserved.
- **Availability**: The information must be accessible and usable when requested by an authorized individual, area or process, and at the time it is required.

3.2 The information and valuable resources associated with the information that the Organization uses for the development of its business objectives must be identified; the information and other associated resources must have a responsible person assigned to them, who must make the decisions that are pertinent for their protection, in accordance with the internal requirements and regulations applicable to each company.

3.3 All information, regardless of the medium in which it is found or the location from which it is accessed, must be classified to establish its sensitivity (the level of reserve that must be maintained on its content) and its criticality (the level of availability required so that business operations are not interrupted). It is the responsibility of the members of the Organization to know the classification of the information they use for the development of their activities; and of those responsible for the processes to define the controls to protect the information according to the classification handled by each Company that is part of the Organization.

3.4 The Organization identifies as confidential or privileged information, the following information, among other, as the definition of confidential information must be made on case by case basis:

- Stock exchange shares, strategic and financial information, information on strategic alliances, reports on projections, results and/or financial disclosures.
- Information related to clients, collaborators, shareholders, related third parties, contractors, suppliers, travelers, users, investors.
- Insider information for important and confidential company events.
- Material non-public information. These are some examples, merger information, strategic projects, disposal, change in dividend policy, business partner information, shareholders information, among other.
- Business information that the organization is obligated to protect, patents, inventions, commercial agreements, contracts, software development source code or other information that has the potential to provide competitive advantage.
- Practices to optimize revenues, prices, net fares.
- Information on the operation and its associated processes.
- Security reporting, risk, compliance, internal and external audit, incidents operational, information security and cybersecurity incidents, investigations, and legal matters regarding any of the above.
- Reports from or to regulatory agencies regarding confidential information.
- Keys, pins, passwords, or information for user corporate networks and/or applications.
- Information subject to personal data protection laws (including payment card data) in the various jurisdictions where the Organization is located or develops its business.

The aforementioned information, and any other that is considered due to its classification as confidential or privilege information may not be used for the personal benefit of any administrator, collaborator or third party that has access to, or for any purpose other than that originally intended for such information.

3.5 It is the duty of all those responsible for processes, project or initiative leaders and contract managers to ensure that information risks are identified, analyzed, evaluated, treated and monitored, in accordance with the procedures of the Information Risk and Compliance Department, ensuring that the corresponding risks are kept within the risk levels acceptable to the Organization as stipulated in the following link: MA_AVSG04_054 INFORMATION RISK MANAGEMENT MANUAL

3.6 Information resources such as: equipment, business applications, Internet services, Intranet, collaborative tools (e-mail, chat, cloud storage), among others, are provided to all employees of the Organization for the exclusive use of the Organization. Access to and use of these resources must be authorized by the person responsible for each resource and in accordance with the responsibilities of his or her function. Information resources must be returned immediately to the administrator when they are no longer needed.

3.7 The Organization must ensure that its employees, any officer, manager or any person in charge of information management processes implement information security measures such as, but not limited to: checks and investigations on personal references, work references, work experience, complementary tests, security survey, aptitude and knowledge test, in a manner that supports security policies and in compliance with local regulations.

3.8 All employees and related third parties undertake to handle the confidentiality of the Organization's information regardless of whether they have signed a confidentiality agreement at the time they join the Organization and are responsible for the confidentiality of the information even after the end of their relationship with the Organization.

3.9 The Organization shall have a permanent information security and cybersecurity culture program to keep all its personnel informed about policies, information security responsibilities and the continuous threats that put the information it manages and/or processes at risk.

3.10 Those responsible for contracts and contracting should ensure that the information security responsibilities of third parties and their supply chain who access, process, store or distribute information of value to the Organization are documented in contracts or other service delivery agreements and should monitor compliance throughout the completeness of the term of the contractual relationship.

3.11 It is the duty of all The Organization and related third parties to report any suspicion, abnormal condition or violation of the policies, responsibilities and procedures of information security and cybersecurity that threaten the Confidentiality, Integrity and Availability of The Organization's information immediately through the channels established by the Organization.

In the event that the situations described above affect or have the possibility of affecting or having any economical, material, reputational, legal or operational impact for the Organization, they must be reported immediately to the Information Risk and Compliance Department through the channels established by the latter.

The Information Risk and Compliance Department shall evaluate the incident reports and determine whether they meet the materiality criteria, in which case it shall inform the Investor Relations Department so that it complies with the Policy on Disclosure of Relevant Financial and Non-Financial Information to Shareholders, Market, Stakeholders and Interested Third Parties.

3.12 The Organization has the responsibility of implementing guidelines and technical measures for the protection of information that is stored, processed, or transmitted; according to its classification and considering, but not limited to:

- Information risk management
- Identification and classification of information assets
- Controls for secure data storage and transfer.
- Protection against threats, such as malware and/or possible computer attacks.
- Digital identity management and Access control to information, applications, infrastructure and networks.

- Security management in own or personal mobile/laptop devices at the service of the Organization.
- Proper use of resources allocated by the organization (internet, corporate technology devices, collaborative sites: SharePoint, OneDrive, Teams, email, others.).
- Network and telecommunications security
- Security in the acquisition, development and maintenance of technological resources (including systems and processing environments, and management of technological obsolescence).
- Removable storage media management
- Safety of internal personnel and third parties
- Technical vulnerability management
- Cloud Security
- Security logs, events and incidents management
- Physical and Environmental Security of Data Processing Centers
- Controls for software installation, development, and storage
- Continuity management, information backup and recovery of technological platforms in case of disasters.
- Remote or off-site work.
- Responsible use or development of artificial intelligence (AI) technologies.

3.13 The Information Risk Department may carry out monitoring activities in any Company of the Organization, on an exclusive basis, to determine the level of compliance with the guidelines established in this Policy. Including third parties and subcontracted companies that provide management, monitoring, and administration services for Investment Vehicle 1 Limited technology platforms.

- **Current legal regulation applicable to the policy.**

3.14 The Organization, its Board of Directors and its executive group must commit to the compliance with the information security requirements established in its internal security policies, as well as those requested by the applicable laws and regulations, such as and without limitation: SOX (Sarbanes-Oxley Act), PCI DSS (Payment Card Industry Data Security Standards), international personal data protection laws, aviation sector regulations, industry or contractual agreements, licensing, intellectual property and others related to information security and cybersecurity.

3.15 In case of non-compliance with the established or subsequent security policy and/or procedures, the Organization will take the appropriate legal, administrative and/or disciplinary actions, in accordance with the provisions of the internal regulations of each of its companies and/or the applicable international and/or local information security, cybersecurity and personal data protection laws and regulations.

- **Effective date of the Policy.**

3.16 This Policy is effective from the moment of its publication and is understood to be in force indefinitely unless it is modified or update in accordance with changes in the organizational environment, business circumstances and/or legal conditions. Regarding third parties where the approval of a corporate body is required for its adoption or the consent of a third party, the policy will come into effect when the respective authorizations are obtained.

- **Prevalence.**

3.17 In case of conflict between the Board Protocol, the Investment Agreement and this Policy, the following will be the order of precedence of the documents: (i) the Investment Agreement, (ii) the Board Protocol, (iii) this Policy.

- **Glossary.**

AI: Artificial Intelligence

Board Protocol: The effective Company's Board of Directors Protocol.

Cyberspace: Environment resulting from the interaction of people, software and services on the Internet through technological devices connected to such a network, which does not exist in any physical form. (Superintendencia Financiera Circular externa 007, 2018)

Cyber security: It is the development of business capabilities to defend against and anticipate cyber threats in order to protect and secure the data, systems and applications in cyberspace that are essential to the entity's operation. (Superintendencia Financiera Circular externa 007, 2018)

Cyber security incident: Occurrence of a situation that affects the protection or assurance of the entity's data, systems and applications that are essential to the business. (Superintendencia Financiera Circular externa 007, 2018)

Data Processing Centers (Data Center): Physical or cloud (virtual) site to maintain the technological and electronic infrastructure, where the information necessary for the execution of the company's processes is processed

Digital Identity: Set of information about a person that exists in the digital environment and allows them to be uniquely identified.

Identity: Refers to the identification of individuals in the applications of the organization. For employees, identity is registered in SAP SSFF (SuccessFactors) and recognized by employee number. In the case of related third parties, identities are registered in the Third-Party Master of the Identity Management tool and are recognized by their identification number; in countries where personal data legislation requires it, other data will be used, such as driver's licenses, tax numbers,

or other permitted identifiers. To create a user in an application, it is essential that the identity is registered and active.

Information Security and cybersecurity program: Set of policies, strategies, methodologies, resources, IT solutions, practices and competencies to protect, secure and preserve the confidentiality, integrity and availability of information that is stored, reproduced or processed in the entity's IT systems or other media. (Superintendencia Financiera Circular externa 007, 2018)

Investment Agreement: The effective Company's Shareholders Agreement.

Risk (NTC-ISO31000): Effect of uncertainty on objectives.
NOTE 1: An effect is a deviation from what was expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.
NOTE 2: Objectives can have different aspects and categories, and can be applied at different levels.
NOTE 3: Risk is often expressed in terms of sources of risk, potential events, their consequences and their probabilities.

Information Risk (NTC-ISO/IEC 27005): Potential for a given threat to exploit vulnerabilities in assets or groups of assets causing damage to the organization. It is measured in terms of a combination of the probability of an event occurring and its consequences.

Cybersecurity Risk (NISTIR 8286 based on ISO Guide 73 and NIST SP 800-60 Vol. 1 Rev. 1): An effect of uncertainty in or within a digital context. Cybersecurity risks relate to the loss of confidentiality, integrity or availability of information, data or information systems (or control) and reflect potential adverse impacts on the organization's operations (i.e., mission, functions, image or reputation) and assets, individuals, other organizations and the Nation.

Segregation of duties: Measure that separates the responsibilities of the various activities involved critical processes of the Company.

Supply chain: In the context of information security, this refers to the set of processes, organizations, individuals, activities, technologies, and related third parties (suppliers, partners, and contractors) involved in the life cycle of products, services, or information, whose proper functioning, trustworthiness, and protection are essential to ensuring the confidentiality, integrity, and availability of the information of the company.

- **Reference documents** (Ctrl + Click on each document)**:**

Business Continuity Management policy
MSG-016 General Information Security Corporate Manual
MSG-017 Specific Information Security Guidelines Manual - Information Technology Areas
Internal manual for the protection of personal data
Information Risk Management Manual
IN_SO0113_01 Security Users and Passwords

Information security and cybersecurity threat intelligence procedure PR_SO0114_02 Information security and cybersecurity incident response procedure

IN_AVSG04_008 Instructions for internal reporting and materiality assessment of Cyberincidents.

Other procedures and instructions are associated with the regulatory framework for information security.