ALASKA
ASSET MANAGEMENT

Information Security and Cybersecurity Policy
Alaska Investimentos LTDA

Version 01.2022

Rua Bandeira Paulista, 600 – conj. 73
04532-001 Itaim Bibi – São Paulo – SP

Phone: (11) 4550-2950

ri@alaska-asset.com.br
www.alaska-asset.com.br

ALASKA
ASSET MANAGEMENT

TABLE OF CONTENTS

ALASKA
ASSET MANAGEMENT

1. INTRODUCTION

The Information Security and Cybersecurity Policy ("Policy") establishes the guidelines to be complied with by Alaska Investimentos LTDA ("Alaska" or "Manager") to ensure the protection of information in the possession of the manager.

Information Security is related to the protection of a set of data in order to preserve the value they have for an individual or organization. The basic characteristics of information security are the attributes of confidentiality, integrity, and availability, addressed in this document. Although usually addressed in digital media, security is not restricted to electronic information, storage systems or available printed documentation, it applies to all aspects of information and data protection.

This policy is applicable to all Alaska associates, partners or employees, as well as all service providers with a relationship with the manager.

In accordance with Anbima's Code for the Administration of Third-Party Resources, Alaska declares that it has, at its head office, a document providing for cybersecurity rules, procedures and controls, containing:

I. Risk assessment, which must identify the relevant assets, whether they are equipment, systems, data or processes, their vulnerabilities and possible threat scenarios;
II. Protection and prevention actions, aiming at mitigating the identified risks;
III. Description of the supervisory mechanisms for each identified risk, in order to
verify its effectiveness and identify potential incidents;
26
IV. Creation of an incident response plan, considering threat scenarios foreseen during the risk assessment, which allows business continuity or adequate recovery in more severe cases; and
V. Appointment of a person to be in charge, within the institution, in dealing with and responding to cybersecurity
issues.

2. PURPOSE

The purpose of this Policy is to establish Alaska's information security guidelines, promote the implementation of rules, procedures and controls for the adequately processing information and maintaining its commitment to the protection of information and cybersecurity, as well as guiding its associates and entities related to the manager.

3. INFORMATION SECURITY PROGRAM

3.1 CONCEPTS

The **concept of information** can be defined as: data, processed or not, that can be used for the production and transmission of knowledge, in any media or format.

The **information is usually stored** in digital media, such as file servers, databases, information systems, emails, messaging applications or pen-drives, or in physical media, such as documents, contracts and printed reports, or orally, such as a conversation in a public space.

All **information in Alaska's possession**, produced or received, is a content of its own value or of value to third parties under the responsibility of the manager.

Information security aims at protecting all data in the manager's possession against dangers and threats, implementing a set of rules, procedures and controls that minimize the occurrence of undesirable events and damage.

3.2 PRINCIPLES

In order to fully carry out its activities, Alaska, its associates and third parties must follow the 3 information security principles aiming at ensuring:

- *Availability*: access to data and information systems, whenever necessary, in authorized cases;

- *Confidentiality*: access to restricted information only by authenticated and specifically authorized persons;

- *Integrity*: protection of information content against undue changes, whether they are intentional or accidental.

3.2.1 AVAILABILITY

To ensure **availability**, Alaska must maintain a robust infrastructure of hardware such as servers, network equipment, firewalls, nobreaks and internet links with appropriate updates and preventive maintenance.

In order to mitigate potential unavailability due to equipment failures, Alaska works with a redundant environment of contingency and internet providers with "hot" synchronization of the file server and a maximum delay of 1 hour for the database.

Also, if needed, Alaska performs daily backups of the file server and hourly backups of the database in cloud storage.

3.2.2 CONFIDENTIALITY

To ensure **confidentiality**, the information is classified by department and stored in a structured manner, in different locations, with restricted access according to the profile of each user.

Alaska's systems and network infrastructure can only be accessed by authenticated users with a login provided by the IT area, and with access only to resources authorized by the *Compliance* Officer.

In the event of any doubts regarding the confidential nature of any information, the *Compliance* Officer must be consulted in advance for proper guidance.

3.2.3 INTEGRITY

To ensure **integrity**, in addition to information, resources and systems being accessible only to authenticated and authorized users, the infrastructure must maintain intrusion protection agents such as firewalls and antivirus tools on users' servers and workstations.

The tools hired by Alaska provide monitoring against external intrusion and data traffic anomalies . Additionally, all access or changes to files are recorded and monitored in real time by a specific tool that sends alerts in suspicious cases, which can even automatically block access.

3.3 THE PROGRAM

Alaska's information security program lists a set of measures aiming at the protection of information, as well as guidelines for the proper use by associates and third parties to support and sustain the activities of the manager.

For a robust program, it is necessary that everyone involved does their part, always acting with care when dealing with and sending information that goes beyond Alaska's domain.

For a better organization of the attributions and responsibilities, below we have the main actions and responsibilities that must be complied with, segregated by function:

3.3.1 RESPONSIBILITIES OF THE IT DEPARTMENT

The IT department must maintain an IT infrastructure that best supports the principles of availability, confidentiality and integrity.

Providing resources, equipment and software suitable for the associate's role.

Providing the network login and email only with access to necessary and authorized resources for the associate's role.

Providing secure VPN access to Alaska's internal environment to authorized associates.

Maintain specialized security resources and software to protect the infrastructure against threats (*firewall*, anti-virus, *anti-spam*), in line with best security practices.

Maintain monitoring tools with a log of network accesses and voice recording of extensions for auditing purposes.

Keep operational backup tools in physical and logical locations separate from the source location.

Alaska's infrastructure is supported and advised by two IT service providers, Strati Soluções e Serviços em TI Ltda. (www.strati.com.br) and Nuvme Ltda. (www.nuvme.com.br):

- **STRATI SOLUCOES E SERVICOS EM TI LTDA**: Company responsible for managing and monitoring Alaska's IT environments, including the office located in Itaim Bibi and the contingency environment in Morumbi;

- **NUVME LTDA**: Company responsible for managing and monitoring Alaska's environment on Amazon AWS, including file server, database, Alaska's website hosting and encrypted cloud backups.

The adoption of specialized IT companies adds greater knowledge and experience both in detecting and implementing responses and in the continuous monitoring of threats.

3.3.2 RESPONSIBILITIES OF THE COMPLIANCE DEPARTMENT

The *Compliance* department must ensure that Alaska's IT infrastructure has the necessary information security controls in accordance with the legislation in force.

Authorizing the use of equipment, access to network resources, email, database and other systems in accordance with the functions of the employees.

Assessing occurrences, suspicions or reports of behaviors contrary to the information security program, as well as working on the adoption of measures that can contribute to the mitigation of the problem.

In cases of leakage of confidential information, even if arising from involuntary actions, reporting the incident to associates and providing the first guidance regarding external inquiries. Then, organizing an Executive Committee to assess impacts and harm reduction actions, in addition to assessing additional measures necessary to mitigate the possibility of recurrence of similar impacts.

Ensuring strict compliance with all regulations to which Alaska is subject, such as the General Data Protection Act (GDPR).

3.3.3 RESPONSIBILITIES OF ALASKA ASSOCIATES AND THIRD PARTIES

All information in Alaska's possession available to associates and third parties must be treated in compliance with the rules of this program and its function assignments. Misuse or inappropriate use of the information will be subject to analysis and penalties may apply.

All equipment for individual use (desktops, notebooks or cell phones) owned by Alaska are resources made available for carrying out activities of interest to the manager.

Every associate receives their own network login and an email with temporary passwords that must be changed immediately. In third-party

systems, the recommendation is to register a single login per user whenever possible.

In all cases, users must use "strong" passwords and enable 2-factor authentication whenever available.

The user is co-responsible for protecting the integrity of the equipment, any software installation or settings adjustment must be requested to the IT department.

Transferring information for external use, whether via email, cloud storage, portable devices, or any other storage system external to Alaska's infrastructure, is prohibited, unless otherwise approved by the *Compliance Department* .

The use of personal resources (*desktops*, *notebooks* or cell phones) to carry out professional activities must be submitted for approval by the *Compliance* department. In case of approval, it is mandatory that the personal resource maintains an operating system with the appropriate security tools and original software always up to date.

4. BUSINESS CONTINUITY PLAN (PCN)

Also known as an operational continuity plan, the PCN defines the strategies adopted to maintain the operations fully running in cases of adversities caused by factors internal or external to the manager and that may cause unavailability of the environment or any resources needed in the operation.

Alaska has strategic work positions hired in the Morumbi neighborhood in partnership with the company Regus do Brasil LTDA. The company is responsible for the physical space, guaranteeing the availability of internet access, controlling the physical access and cleaning the environment.

Strati is responsible for monitoring the availability and periodic maintenance of the environment's hardware, while the company Nuvme is responsible for the availability of services replicated in the Amazon AWS cloud.

The contingency website is remotely monitored by the company Strati, with periodic software updates. In addition to the remote access we have to the environment, in-person tests are carried out periodically to assess the integrity of the systems.

5. SECURITY DISCIPLINES

The access as administrator to information management systems and cloud platform, or critical services to the internal infrastructure, are restricted to administrators or Alaska's IT. Exceptions must be authorized in advance.

5.1. ENCRYPTION

In order to ensure the security of information stored or transmitted, Alaska adopts encryption techniques. The resources are used to ensure the confidentiality, authenticity and security of data, in compliance with information security rules and security standards.

Encryption is applied both for transmitting and receiving data, as well as for data backups.

5.2. CREDENTIALS AND RECOMMENDATIONS

- Passwords are secret, personal and non-transferable, and sharing passwords with third parties is expressly prohibited. The passwords must be changed at intervals established internally based on risk factors;

- To ensure the security of local access to computers, it is necessary to lock the station when away from the machine and to configure the automatic screen lock after a period of inactivity;
- It is prohibited to store credentials (passwords) or confidential information in places that can be viewed by third parties, and it is necessary to keep the workstation organized;
- Confidential/sensitive physical or electronic materials must be properly disposed of to prevent access by third parties;
- In the event of the possibility of improper access or disclosure of any type of sensitive information, a communication must be immediately made to the Risk and IT Officer and the *Compliance* Officer;
- In case of dismissal of an employee or partner, access to Alaska's environment is immediately revoked.

5.3. PHYSICAL SECURITY OF THE ENVIRONMENT

Critical or sensitive information processing equipment and facilities are maintained in secure areas with appropriate levels and access controls, including protection against physical and environmental threats.

The contingency space in Morumbi also has restricted and limited access to people authorized by Alaska.

6. REVIEW AND UPDATE

This Policy may be revised or updated at any time to address new processes, identify new risks or reinforce the manager's commitment to the best information security practices.

7. INSTRUMENT OF AWARENESS

The Risk and Compliance Officers may have access to confidential data or data protected by law, and they must always access this data in a

diligent, confidential manner, with a valid purpose and for a maximum period until the due diligence is completed.

The Risk and Compliance Officers certify that all associates have read, understood and agreed to comply with the procedures described herein.