INFORMATION SECURITY POLICY

1. Policy Summary:

Information must always be protected, regardless of how it is shared, communicated or stored.

2. Introduction:

Information can exist in various forms: printed or written on paper, stored online, transmitted by mail or electronic means, shown in projections or spoken in conversation.

We must also consider that the core of the business for our organization involves processing information from our clients, thus being our most valuable asset along with the people who are part of the company.

Information security refers to the protection of information against a wide range of threats in order to ensure business continuity, minimize business risks and maximize return on investment and business opportunities.

3. Scope:

This policy supports the organization's general Information Security Management System policy. This policy concerns all members of the organization.

4. Information Security Objectives:

- Understand and address operational and strategic risks in information security so that they remain at acceptable levels for the organization.
- Protect the confidentiality of information related to clients and development plans.
- Maintain accounting record integrity.
- Verify that publicly accessible websites and internal networks meet the required availability specifications.
- Understand and cover the needs of all stakeholders.

Prepared by	Revised by	Approved by
Gustavo Passione	Diego Sansone	Diego Sansone

Date of Issue	Change Description
08/19/2021	First Issued

5. Principles of Information Security:

- This organization faces risk-taking and tolerates risk that, based on available information, are understandable, controlled and addressed when necessary. The details of the methodology adopted for risk assessment and the treatment thereof are described in this ISMS policy.
- All staff will be informed and responsible for information security, as deemed relevant to their work performance.
- Financing will be available for the operational management of controls related to information security and in the management processes for their implementation and maintenance.
- The possibilities of fraud related to the abusive use of information systems within the global management of information systems will be taken into account.
- Regular reports with information on the security situation will be made available.
- Information security risks will be monitored and relevant measures will be adopted when there are changes that entail an unacceptable level of risk.
- Risk classification and acceptance criteria are stated in the ISMS policy.
- Situations that may expose the organization to breach of laws and legal regulations will not be tolerated.

6. Responsibilities:

- Management is responsible for ensuring that information security is properly managed throughout the organization.
- Each Area Manager is responsible for ensuring that the people reporting to them protect information in accordance with the organization’s standards.
- The Security Manager advises Management, provides specialized support to staff and ensures that information security reports are available.
- Each company employee is responsible for maintaining information security within their work-related activities.

7. Key Indicators:

- Information security incidents will not result in serious and unexpected costs, or a serious disruption of services and business activities.
- Fraud-related losses will be identified and the necessary measures will be adopted to avoid recurrence.
- Client acceptance of products or services will not be adversely affected by information security issues.

8. Related Policies:

Policies that provide principles and guidance on specific information security aspects are listed below:

PO-01.- INFORMATION SECURITY POLICY.
PO-02.- TELEWORK POLICY.
PO-03.- OPERATIONS SECURITY POLICY.
PO-04.- HUMAN CAPITAL POLICY.
PO-05.- BUSINESS CONTINUITY POLICY.
PO-06.- ACCEPTABLE USE OF ASSETS POLICY.
PO-07.- PHYSICAL SECURITY AND ACCESS CONTROL POLICY.
PO-08.- REMOVABLE MEDIA ACCEPTABLE USE POLICY.
PO-09.- CRYPTOGRAPHY POLICY.
PO-10.- CLEAN DESK POLICY.
PO-11.- MOBILE DEVICE POLICY.

At a lower level, **the information security policy must be supported by other standards or procedures** on specific topics that requires information security controls to be applied even more so, typically being structured to address needs of certain groups within an organization or to cover certain topics.

Examples of these policy topics include:

1. Access control.
2. Classification of information.
3. Physical and environmental security.

Or those addressed directly to users:

1. Acceptable use of assets.
2. Clear screen and clean desk.
3. Transfer of information.
4. Mobile devices and telecommuting.
5. Software installation and use restrictions.
6. Backup.
7. Transfer of information.
8. Protection against malware.
9. Technical vulnerability management
10. Cryptographic controls.
11. Security communications.
12. Privacy and protection of personal identifiable information.

These policies/standards/procedures must be communicated to employees and external stakeholders. The need for internal information security standards varies from organization to organization.
When some information security standards or policies are distributed outside the organization, **care should be taken not to disclose confidential information**.

All these policies must serve as support to identify risks by providing controls regarding a point of reference that can be used to identify system design and implementation deficiencies,

and the treatment of risks through the possible identification of appropriate treatments for localized vulnerabilities and threats.
This risk identification and treatment is part of the processes defined in the Principles section within the security policy or is usually part of the ISMS policy itself, as shown below.

ISMS POLICY

Given the importance for the **correct development of business processes**, information systems must be adequately protected.
Reliable protection allows the organization to perceive its interests better and efficiently fulfill its information security obligations. **Inadequate protection affects the company's overall performance** and can negatively affect the image, reputation and trust of its clients and also potential investors who place their trust in the organization for the strategic international growth of our activities.
Information security intends to ensure business continuity within the organization and minimize the risk of damage by preventing security incidents and reducing their potential impact when unavoidable.
To achieve this, **the organization has developed a risk management methodology that allows us to regularly analyze the extent of exposure of our important assets** against any threats that may take advantage of certain vulnerabilities and introduce adverse impacts to our staff's activities or our organization's important processes.
The successful use of this methodology stems from the experience and contributions of all employees in terms of safety, and through the communication of any relevant consideration to their Direct Managers in semester meetings established by Management, in order to locate possible changes in the levels of protection and assess the most effective options in cost/benefit of risk management at all times and where appropriate.
The principles outlined in the security policy attached to this policy were developed by the security information management group to **make sure that future decisions are based on preserving the confidentiality, integrity and availability of information relevant to the organization**.
The organization counts on the collaboration of all its employees in applying the proposed security policies and guidelines.
The daily use of computer equipment by all employees determines compliance with the requirements of these principles and an inspection process to confirm that they are respected and fulfilled by the entire organization. In addition to this policy, and the organization's security policy, there are specific policies for the different activities.
All security policies in force will remain available on the organization's internal network/Dropbox and will be regularly updated. Access is direct from all workstations connected to the organization's network and with a click of the button from the main website in the Information Security section. The policy is intended to **protect the organization's information assets against all internal and external threats and vulnerabilities**, whether deliberate or accidental.

MANAGEMENT IS RESPONSIBLE FOR APPROVING AN INFORMATION SECURITY POLICY THAT ENSURES THAT:

1. Information will be protected against any unauthorized access.
2. Confidentiality of information, especially information related to the personal details of employees and clients.
3. Information integrity in relation to the classification of information (especially "internal use" information) will be maintained.
4. The availability of information complies with the relevant deadlines to develop critical business processes.
5. The requirements of current legislation and regulations are met, especially with Data Protection and Electronic Signature Laws.

6. Plans for business continuity will be maintained, tested and updated at least every year.
7. Safety training is sufficiently completed and updated for all employees.
8. All events related to information security, whether real or supposed, will be reported to the Security Manager and looked into.

There are also **support procedures** that specifically include how the general guidelines indicated in the policies by designated Managers must be carried out.

Compliance with this policy, as well as with the information security policy and any procedure or documentation included in the ISMS documentation repository, **is mandatory and applies to all company staff**.

Visitors and external staff who access our facilities are bound to comply with the obligations indicated in the ISMS documentation, and internal staff will observe compliance therewith.

Should there be any questions or queries, or for more information on the use of this policy and how to apply the content herein, please call or e-mail the ISMS Manager, formally designated in the Idea Translations' organization chart.