



## INFORMATION SECURITY POLICY

SIPO-08-V1

Pública

Página 1 de 4

### 1. REACH

This policy is applied to the whole organization, collaborators, contractors and thirds of **AS•NET**.

### 2. DEFINITIONS

- **Information assets:** Anything that has a value to the organization. Also understood for any information or system related with the information treatment of the same that has value to the organization. Is any asset that store, process or transmit information, which has a value and it is necessary to realize missional and operative processes of AS•NET.
- **Confidentiality:** Property of the information that is not available or is disclosed to individuals, entities or unauthorized processes.
- **Availability:** Property accessible and usable on demand for an authorized entity.
- **Integrity:** Property of accuracy and completeness.
- **Risk:** Uncertainty effect about the objectives
- **SGSI.** (Sistema de Gestión de Seguridad de la Información) management of information security system

### 3. POLICIES

The management of **AMERICAN SMART SYSTEMS & NETWORKS** (now on **AS•NET**), understanding the importance of an adequate management of the information, is now committed with the implementation of a management o information security system -SGSI based in the NTC-ISO-IEC 27001:2013 Looking to stablish a framework of trust in the exercises with the interest parts, all framed in the strict fulfillment of the corresponding laws and norms in concordance with the mission and vision of the organization.

For **AS•NET**, the protection of the information pretends the decrease of the impact generated on the assets of information, for the risks identified in a systemic way with the purpose of maintaining the integrity, confidentiality and availability of itself, according to the needs of the different groups of interest identify. According to the above, this policy applies to the whole organization, which includes all the collaborators, thirds, apprentices, interns, suppliers and interested parts in general, taking into account the principles in which the development is based of the actions or taking decisions next to de SGSI will be determined with the next indications.

- Minimize the risk of missional processes of the organization.
- Accomplish with the principles of security of the information.
- Maintain the trust of their clients partners and collaborators
- Support technological innovation.



## INFORMATION SECURITY POLICY

SIPO-08-V1

Pública


Página 2 de 4

- Protect information assets.
- Establish policies, procedures, standard of configuration and instructive in information security matters.
- Boost the security of information culture with collaborators, thirds, apprentices, interns and clients of **AS•NET**.
- Guarantee the continuity of the business against incidents

**AS•NET** decide to define, implement, operate and improve in a continuous way a management of information security system, supporting the clear guidelines line up to the needs of the business and regulatory requirements.

Next, there are establish 12 principles of security that support **SGSI** of **AS•NET**:

- The responsibilities of the information security will be known, understand, accept and accomplish for each of the collaborators, suppliers, strategic allies or thirds.
- **AS•NET** will protect the information generate, process guard by the business process, its technological infrastructure and information assets of the risk that generate the given access to thirds (e.g.: suppliers or costumers) or any result of an inner service in outsourcing.
- **AS•NET** will protect the information created, processed, transmitted or saved by its business process in order to minimize financial, operative or legal impacts because of a wrong use of it. For that it is fundamental the application of controls according to the classification of the information of their property or custody.
- **AS•NET** will protect the information from threats originated from the personal.
- **AS•NET** will control the operation of the processes of business and guarantee the security of the information assets.
- **AS•NET** will implement access controls to the information assets.
- **AS•NET** will seek that the safety be an integral part of a cycle of life of the information systems.
- **AS•NET** will assure through and adequate management of the events of security and weaknesses associated with the information systems, and improvement effective by the SGSI
- **AS•NET** will watch for the availability of the process of the business and the continuity of it operation based in the impacts that incidents can generate
- **AS•NET** will accomplish its legal, regulatory and contractual establish obligations

	<b>INFORMATION SECURITY POLICY</b>		
	<b>SIPO-08-V1</b>	<b>Pública</b>	<b>Página 3 de 4</b>

### 3.1. OBJECTIVES

The information security objects are:

- Preserve the confidentiality of the information, avoiding its divulgation and access to people, entities and unauthorized processes
- Maintain the integrity of the information ensuring its accuracy, completeness and avoiding deterioration.
- Ensure the availability of the information in all storage supports and backup media when it is required.
- Identify risks and establish controls, limiting and preventing the consequences of the different incidents, for assure le immediate recovery of the operation and minimize the damage to the organization.
- Train and consent continuously the personal in themes related with information security.
- Guarantee the protection and the safety of the information that is supplied by our clients for the development of the project.
- Manage efficiently the accessibility of the information of AS•NETs collaborators in accordance with the defined profile, looking for minimize the information security risks.
- Manage incidents in information security matter, using the guidelines established by **AS•NET**.
- Guarantee the continuity of the business, minimizing the possible impacts to the provided services
- Protect the assets of information and manage its vulnerabilities

Improve continually the **SGSI**, checking its performance and efficiency.

### 3.2. FULFILLMENT LEVEL

All the collaborates, suppliers, strategic allies and thirds should accomplish the policies describe in this document.

### 3.3. POLICY REVIEW

This policy id available for all the interested parts in **AS•NET** intranet and website, also, it will be object of update at least once per year or when significant changes occurred in the inner and external of **AS•NET** or when there is a security incident that deserve the update of the same.



## INFORMATION SECURITY POLICY

SIPO-08-V1

Pública

Página 4 de 4

### 4. REFERENCE DOCUMENTS

- PCI DSS 3.2.1 Norma de seguridad de datos. Requisitos y procedimientos de evaluación de seguridad.
- ISO-IEC 27000:2014 Sistemas de Gestión de Seguridad de la Información – Vocabulario
- NTC-ISO-IEC 27001:2013 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos
- GTC-ISO-IEC 27002:2015. Tecnología de la Información. Técnicas de Seguridad, Código de Práctica para Controles de Seguridad de la Información.

### 5. CHANGES CONTROL

Date	Version	Item change	Modification
18/06/2019	1	-	Documento Inicial

<b>Elaborated by:</b> Erika Pulido Garzón	<b>Revised:</b> Comité de Seguridad de la Información	<b>Approved</b> José Fernando Rodríguez
<b>Position:</b> Analista de Seguridad de la Información	<b>Position:</b> Comité de Seguridad de la Información	<b>Position:</b> CEO