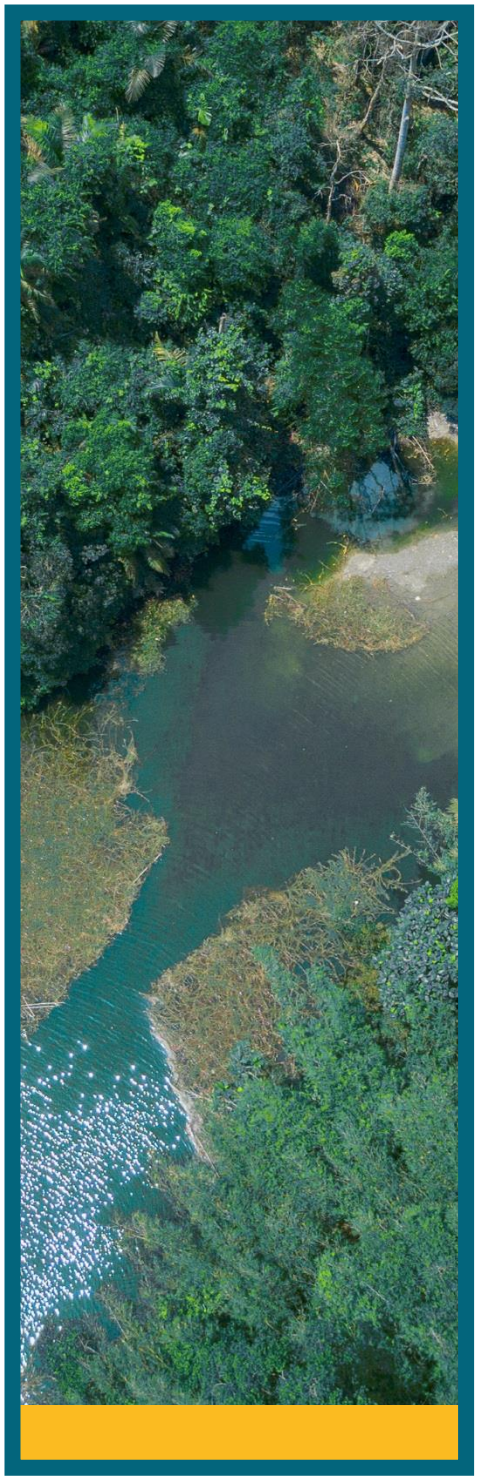

General Policy

Information Security Policy

Contents

1 Introduction

Indra regards information as one of its most critical assets and, for this reason, all duties relating to the management of Information Security must be performed in a coordinated way through the implementation of a model that is aligned with the Company's culture, processes, structure and strategy.

With this in mind, Indra has established an Information Security Model that will ensure that all the security risks to which it may be exposed are identified and assessed and, as a consequence, the most efficient security strategies are adopted, in line with the Company's own business strategies, through the efficient use of resources in a way that brings the greatest possible value for stakeholders.

Information Security therefore forms an integral part of all the Company's processes and is included as part of Indra's strategic planning.

2 Purpose

The main purpose of the Company's Information Security policy is to establish a framework for action that will allow it to protect information belonging to Indra and other stakeholders.

It is therefore necessary to establish appropriate measures in all places in which information is stored, processed or transmitted, in order to ensure:

- Its confidentiality, ensuring information can only be accessed by authorised persons;
- Its integrity, ensuring information and the methods used to process it are accurate and complete, avoiding any unauthorised modifications; and
- Its availability, ensuring authorised users have access to information and its associated assets when required.

3 Scope

This Policy is applicable to and binding on all Indra Group companies.

4 Principles

To achieve its aim of protecting the confidentiality, integrity and availability of information, the Company has established the following fundamental principles:

- **Cyber hygiene:** Applying basic measures to guarantee a minimum level of security in all the Company's assets.
- **Awareness:** Remaining aware of the risks associated with information security, and learning about and applying the practices required to protect information.
- **Security Risk Management:** Adequately assessing, managing and processing the risks associated with information security in order to achieve an acceptable level of risk, prioritising the measures and controls that are to be implemented according to the risks identified and the business targets pursued.
- **Compliance:** Complying with all legal, regulatory, sector-based and contractual obligations that affect information security.

- **Security by design:** Incorporating information security as an essential part of the design and development of products, solutions and services.
- **Management of security incidents:** Acting in an appropriate and coordinated way to prevent, detect and respond to incidents that could affect information security.
- **Continuous improvement:** Improving the efficacy and efficiency of the security controls that have been implemented in order to adapt to risks and new technological environments as they emerge.
- **Re-appraisal:** Regularly reviewing and appraising the security of information systems, both internally and externally, taking the measures necessary to correct any divergence that may be detected.

5 Governance model

Bearing in mind the recommendations set out in the international regulations, Indra has drawn up an Information Security Governance Model which, through its supervisory bodies, ensures the coordination of Information Security between the Company's organisational bodies and Management, who are responsible for ensuring application of the fundamental principles of Information Security at Indra.

5.1 Supervisory bodies

The governance of Information Security involves the following supervisory bodies:

- The Information Security Department (ISD) is the body charged with ensuring Information Security, and it is responsible for managing the Information Security Committee.
- The Information Security Committee (ISC) is the body charged with managing Information Security at Indra Group. Its main purpose is to promote Information Security, with support and backing from the Company's Management, and to this end it defines strategic security targets and plans as required, along with business targets and processes.
  Attendance at meetings of the Information Security Committee is mandatory for all of its members, who are responsible for establishing, developing and implementing any decisions that are taken.

In addition, on a regular basis, and at least once a year, the Chief Information Security Officer (CISO) reports to the Board's Auditing and Compliance Committee and to the Risk Coordination Unit, both of which are independent bodies, informing them of the Committee's performance and any potential incidents that have occurred during the financial year.

5.2 Roles and responsibilities

To ensure the proper performance and integration of the Information Security Governance Model at Indra Group, an organisational structure has been defined and roles have been allocated, based on duties and responsibilities, in order to ensure the correct performance of the Group's activities.

The following figure shows the divisions and the communications between the organisational units, supervisory bodies and the individual roles involved.

Figure I - Organisational structure and roles

The duties allocated to each role will depend on the goals set for the different security processes, since definition of the roles and responsibilities of the people who are to be charged with establishing and performing each of the activities associated with the implementation of Information Security processes will depend on these goals.

The roles identified in Indra's Information Security Governance Model are described below:

- The Chief Information Security Officer (CISO), who is head of Information Security at Indra Group, is responsible for developing Information Security strategy, objectives and plans, in coordination with all of the organisational units.

- The Local Information Security Officer (LISO) is responsible for coordinating Information Security at each of the organisational units, in accordance with the regulations, policies and guidelines established by Indra Group's Information Security Department, thus ensuring compliance and providing a global overview of security at the organisational unit in question, anticipating any risk according to the unit's individual characteristics and assisting the decision-making process.

- Country Managers, represent Indra Group in each of the countries in which it has a presence. They are responsible for Information Security at the organisational units that are active in the countries that fall within their remit.

- Directors are responsible for Information Security in the Markets and Corporate Divisions that fall within their remit. The duties allocated to each role will depend on the goals set for the different security processes, since definition of the roles and responsibilities of the people who are to be charged with establishing and performing each of the activities associated with the implementation of Information Security processes will depend on these goals.

At an operational level, the model for the governance of Information Security becomes one in which Information Security is a shared duty.

Figure II - Model for Responsibility for Information Security

6 Channel for reporting incidents

With a view to ensuring the swift detection and effective management of security incidents, Indra has created an internal incident management team, "Indra CSIRT", which provides the services detailed in document RFC2350. This document can be found on the corporate website at: https://www.indracompany.com/sites/default/files/d7/Documentos/Sobre-Indra/SeguridadInformacion/rfc2350.txt.

Any suspicious occurrence or vulnerability that might affect Indra's information systems must be reported to csirt@indra.es.

7 Approval

By approving this policy, the Board of Directors expresses its determination and commitment to achieve a level of security appropriate to the needs of the business that guarantees the protection of assets in a homogeneous manner in all Indra Group companies.