DGSI01

SECURITY POLICY

CYPE Ingenieros

EDITION	00
CHANGE	First edition
DATE	17/12/2024
DEVELOPED BY	Head of Security
REVIEWED AND APPROVED BY	General management

TABLE OF CONTENTS

1. DECLARATION OF PRINCIPLES 3

1.1. General aims 4

1.2. Top Management Commitment 5

1.3. Development of the Security Policy 6

2. POLICY 7

2.1. Prevention 7

2.2. Detection 7

2.3. Response 7

2.4. Recovery 8

2.5. Security Organisation 8

2.5.1. Security Committee 9

2.5.2. Roles: Duties and responsibilities 11

2.5.3. Designation procedures 13

2.5.4. Review of the Security Policy 13

2.6. Personal data 13

2.7. Risk management 13

2.8. Staff obligations 14

2.9. Third parties 14

3. APPLICABLE LAW 14

1. DECLARATION OF PRINCIPLES

CYPE INGENIEROS S.A, hereinafter **THE COMPANY**, has more than 40 years of experience in the marketing, distribution and after-sales of technical software for **Architecture, Engineering and Construction** professionals. THE COMPANY offers a variety of innovative programs that are designed to assist professionals in the performance of structural analysis, project management and quality control in an efficient and accurate manner both nationally and internationally.

Due to our activity, at THE COMPANY we are aware that information is an asset with a high value for our organisation and therefore requires adequate protection and management in order to provide continuity to our line of business and minimise the possible damage caused by failures to the integrity, availability and confidentiality of the information. Likewise, both the current legislation on the protection of personal data (European regulation GDPR and Spanish regulation for the protection of personal data and guarantee of digital rights LOPDGDD) and the commitment of THE COMPANY to our customers, means that we are particularly aware of the processing of personal data to which we have access in the course of our business.

To this end, THE COMPANY establishes a set of management activities aimed at preserving the principles of confidentiality, integrity, availability, authenticity, traceability and regulatory compliance of information. In turn, these principles are defined as follows:

- **Confidentiality:** this property ensures that access to information can only be exercised by those authorised to do so.
- **Integrity:** is the property of safeguarding the accuracy and integrity of information assets.
- **Availability:** is the quality that ensures that authorised persons can access and process the information at any time when required.
- **Authenticity:** is the property or characteristic whereby an entity is who it claims to be, or guarantees the source from which the data originates.
- **Traceability:** is the property or characteristic whereby the actions of an entity can be traced back to that entity only.
- **Regulatory compliance:** is the property that ensures that information is managed in accordance with the ethical, professional and legal principles established by the regulations that are applicable in each context.

Systems must be protected against rapidly evolving threats with the potential to impact information and services. Defence against these threats requires a strategy that adapts to changing environmental conditions to ensure the continued provision of services.

This implies that the different departments must implement the minimum security measures required by the Spanish security framework in the use of electronic media related to public administration ‘Esquema Nacional de Seguridad’ (hereinafter ENS), as well as continuously monitor service delivery levels, track and analyse reported vulnerabilities, and prepare an effective response to incidents to ensure the continuity of the services provided.

The organisation's different departments must ensure that security is an integral part of every stage of the system's lifecycle, from its conception through development or procurement decisions and operational activities to its removal. Security requirements and funding needs should be identified and included in planning, requests for tenders and tender documents for ICT projects.

Departments must be prepared to prevent, detect, react to and recover from incidents, following Article 8 of the ENS.

The protection of privacy is embedded throughout all of the above. THE COMPANY's systems process sensitive personal data and, therefore, privacy protection is an essential pillar in the framework of an information security management system (ISMS) and constitutes a social necessity that companies must respect and protect, as well as an object of specific legislation and/or regulation worldwide.

1.1. General aims

The Security Policy provides the basis for defining and delimiting the objectives and responsibilities for the various technical, legal and organisational actions required to guarantee information security and privacy, complying with the applicable legal framework and the global and specific policies of THE COMPANY, as well as the defined procedures.

From a security and privacy perspective, these actions are selected and implemented based on risk analysis and the balance between acceptable risk and cost of the measures.

The Security Policy aims to set the framework for action needed to protect information and data resources against threats, whether internal or external, deliberate or accidental.

Information and data can exist in a variety of formats, including both electronic and paper or other media, and may include critical data about the operations, strategies or activities of THE COMPANY and its clients, including, where appropriate, sensitive data as required by personal data protection regulations. The loss, corruption or stealing of information or the systems that manage it has a high impact on THE COMPANY.

THE COMPANY is convinced that the effective management of information security and privacy is a key enabler for the organisation to fully understand and act appropriately to the risks to which information is exposed, as well as to be able to respond and adapt efficiently to the increasing requirements of regulatory bodies, laws, and of course its customers.

1.2. Top Management Commitment

The purpose of the Information Security Management System is to ensure that information security and privacy risks are known, understood, managed and minimised in a documented, systematic, structured, repeatable, manageable manner and adapted to changes in risks, environment and technologies.

To this end, the Management declares THE COMPANY's commitment to:

- Establish as a primary objective the service of foreign travel with absolute respect for quality standards, preserving the information, with special attention to the sensitivity of the personal data processed, with all the necessary measures within its reach.
- Apply the principle of continuous improvement to all the organisation's processes, with the additional objective of achieving the highest degree of customer satisfaction.
- Ensure compliance with applicable legal and regulatory requirements (in particular those related to the protection of personal data), as well as those that the organisation has assumed voluntarily.
- Promote the participation, communication, information and training of the professional team to make them feel involved in the work of the organisation as a whole.
- Promote a commitment to responsibility among team members following quality requirements, as well as those relating to privacy and information security agreed upon both internally and with clients, using appropriate and regular training and awareness-raising actions.
- Ensure business continuity by developing business continuity plans following recognised methodologies.
- Conduct and periodically review a risk analysis based on recognised methods that allow us to establish the level of both personal data privacy and information security at a general level and of ongoing projects and services and minimise risks through the development of specific policies, technical solutions and contractual agreements with specialised organisations.
- Inform interested parties.
- Select suppliers and subcontractors based on criteria related to privacy and information security.

With specific regard to the protection of personal data, THE COMPANY is committed to complying with the principles set out in the relevant legislation. These are:

- **Principle of ‘lawfulness, transparency and fairness’**. Data must be processed lawfully, fairly and transparently for the individual concerned.

- **Principle of ‘purpose’**. Data must be processed for one or more specified, explicit and legitimate purposes, and data collected for specified, explicit and legitimate purposes may not be further processed in a way incompatible with those purposes.

- **Principle of ‘data minimisation’**. Implement technical and organisational measures to ensure that only data that is necessary for each of the specific purposes of the processing is processed, reducing the extent of the processing and limiting the storage period and its accessibility to what is necessary.

- **Principle of ‘accuracy’**. To take reasonable steps to ensure that data is kept up-to-date, erased or amended without delay if it is inaccurate about the purposes for which it is processed.

- **Principle of ‘retention time limitation’**. The retention of data must be limited in time to the achievement of the purposes for which the data is processed.

- **Principle of ‘security’**. A risk analysis should be carried out in order to determine the technical and organisational measures necessary to ensure the integrity, availability and confidentiality of the personal data processed.

- **Principle of ‘active accountability’ or ‘proven accountability’**. Maintain due diligence on an ongoing basis to protect and guarantee the rights and freedoms of the natural persons whose data is processed according to an analysis of the risks that the processing represents to those rights and freedoms so that we can guarantee and demonstrate that the processing complies with the provisions of the GDPR and the LOPDGDD.

- To direct, support and supervise the information security management system, following the provisions of the Spanish Royal Decree 311/2022 and subsequent amendments, and to ensure that its objectives are achieved.

THE COMPANY Management is committed to supporting and promoting the principles set out in this Policy by requesting the company's employees to assume and adhere to the provisions of the documented management system for the ENS.

1.3. Development of the Security Policy

This Security Policy complements the security policies of THE COMPANY in different areas and will be developed using security regulations that address specific aspects. The security regulations will be available to all members of the organisation who need them, and in particular to those who use, operate or administer the information and communications systems.

Information Security documents shall be classified into three levels, whereby each document at one level builds on the documents at a higher level:

- **First level**: Security policy.
- **Second level**: Security regulations and procedures.
- **Third level**: Reports, logs and electronic evidence.

2. POLICY

2.1. Prevention

Departments should avoid, or at least prevent where possible, information or services from being compromised by security incidents. To this end, departments should implement the minimum security measures determined by the ENS, as well as any additional controls identified through a threat and risk assessment. These controls, and the security roles and responsibilities of all staff, should be clearly defined and documented.

To ensure compliance with the policy, departments should:

- Authorise systems before going into operation.
- Regularly assess security, including assessments of configuration changes made on a routine basis.
- Request periodic review by third parties in order to obtain an independent assessment.

2.2. Detection

Since services can degrade rapidly due to incidents, ranging from a simple slowdown to a standstill, services must monitor the operation on a continuous basis to detect anomalies in service provision levels and act accordingly as set out in Article 9 of the ENS.

Monitoring is particularly relevant when establishing lines of defence in accordance with Article 8 of the ENS. Detection, analysis and reporting mechanisms shall be established that reach the responsible parties on a regular basis and when a significant deviation from the parameters that have been pre-established as normal occurs.

2.3. Response

Departments should do the following:

- Establish mechanisms to respond effectively to security incidents.
- Designate a point of contact for communications regarding incidents detected in other departments or other agencies.

- Establish protocols for the exchange of information related to the incident. This includes two-way communications with computer emergency response teams (CERTs).

2.4. Recovery

To ensure the availability of critical services, departments should develop systems continuity plans as part of their overall business continuity plan and recovery activities.

2.5. Security Organisation

This policy applies to all systems within THE COMPANY and to all members of the organisation, with no exceptions.

THE COMPANY is committed to providing its services in a managed way and in compliance with the requirements set out in its integrated management system so as to ensure uninterrupted service in accordance with the requirements of availability, security and quality to customers.

Due to our activity, at THE COMPANY we know that information is an asset with a high value for our organisation, especially that of our customers, and therefore requires adequate protection and management in order to give our line of business continuity and minimise possible damage caused by failures in the security of information.

To this end, the organisation will:

- Adequately protect the confidentiality, availability, integrity, authenticity and traceability of its information assets by implementing a range of controls to manage relevant security risks.

- Prioritise the protection and safeguarding of customers and customer data as a business priority.

- Establish, implement, monitor, maintain and continually improve its information security management as part of its wider business management approach, and maintain accredited certification to appropriate standards.

- Manage any information security breaches in a timely and responsible manner, and invest in appropriate detection, response and remediation strategies.

- At planned intervals, test its information security controls and responses to scenarios that may cause a threat to its operations.

- Provide adequate resources to the organisation to establish, maintain and enhance the security environment as appropriate to the changing risk landscape.

- Invest in staff skills to carry out their tasks and provide staff with appropriate training and awareness relevant to their role and the information to which they have access.

- They will ensure that their suppliers and partner organisations do the same, and that they set and enforce security standards on those to whom any information is passed.

2.5.1. Security Committee

The members of the Security Committee shall be designated in a founding act, indicating the person designated and the position to be held.

The secretary of the Security Committee shall be the head of security and will be responsible for the following functions:

- Calling Security Committee meetings.
- Preparing the topics to be discussed at Committee meetings, and providing information for decision-making.
- Drawing up the minutes of the meetings.
- Delegating or directly executing the Committee's decisions.
- The Security Committee will report to the general manager.

The Security Committee shall have the following functions:

- Addressing the concerns of Top Management and the different departments.

- Reporting regularly on the status of information security to Top Management.

- Promoting the continuous improvement of the information security management system.

- Drawing up the organisation's strategy for the development of information security.

- Coordinating the efforts of the different areas regarding information security, ensuring that the efforts are consistent, and aligned with the strategy decided, and avoiding their duplication.

- Drawing up and regularly reviewing the Security Policy for approval by the Management.

- Approving information security regulations.

- Coordinating all the organisation's security functions.

- Ensuring compliance with the applicable legal and sectorial regulations.

- Ensuring that security activities are aligned with the organisation's objectives.

- Coordinating the continuity plans of the different areas, ensuring seamless action if they need to be activated.

- Coordinating and approving, where appropriate, the project proposals received from the different security areas, regularly monitoring and presenting the progress of the projects and reporting any possible deviations.

- Receiving the security concerns of the entity's Management and transmitting them to the relevant departmental managers, obtaining from them the corresponding responses and solutions which, once coordinated, must be communicated to Management.

- Collecting regular reports from departmental security managers on the state of the organisation's security and possible incidents. These reports are consolidated and summarised for communication to the organisation's Management.

- Coordinating and responding to the concerns transmitted through the departmental head of security.

- Defining the assignment of roles and the criteria for achieving the relevant guarantees about the segregation of functions within the corporate security policy.

- Developing and approving training and qualification requirements for administrators, operators and users from an information security point of view.

- Monitoring the main residual risks assumed by the organisation and recommending possible actions to address them.

- Monitoring the performance of security incident management processes and recommending possible actions to address them. More specifically, ensuring the coordination of the different security areas in the management of information security incidents.

- Promoting periodic audits to verify compliance with the organisation's security obligations.

- Approving plans to improve the organisation's information security. In particular, to ensure the coordination of different plans that may be carried out in different areas.

- Prioritising security-related actions when resources are limited.

- Ensuring that information security is considered in all projects from initial specification through to implementation. More specifically, it must ensure the creation and use of horizontal services that reduce duplication and support the homogeneous operation of all ICT systems.

- Resolving conflicts of responsibility that may arise between the different people in charge and/or between different areas of the organisation.

2.5.2. Roles: Duties and responsibilities

The roles of those responsible for the organisation will be detailed below:

Head of information

Their duties shall be as follows:

- Ultimate responsibility for the use made of certain information and, therefore, for its protection.
- Ultimate responsibility for any error or negligence leading to an incident of confidentiality or integrity (for data protection) and availability (for information security).
- Establishing information security requirements.
- Determining and approving information security levels.
- Approving the categorisation of the system with respect to information.
- Fulfilling the duties as indicated in the documents within the scope of the ENS.

Head of service

Their duties shall be as follows:

- Establishing the security requirements of the service.
- Determining the security levels of the services.
- Approving the categorisation of the system with respect to services.
- Fulfilling duties as indicated in documents within the scope of the ENS.

Head of security

Their duties shall be as follows:

- Safeguarding the security of the information handled and the services provided by the information systems in their area of responsibility, in accordance with the provisions of the organisation's information security policy.

- Promoting information security training and awareness within their area of responsibility.
- Approving the applicability statement.
- Channelling and supervising compliance with the security requirements of the service or the solution provided, as well as communications relating to information security and incident management for the scope of said service (PoC).
- Fulfilling the duties that may be indicated in the documents within the scope of the ENS.

The head of security shall be the secretary of the Security Committee with the duties set out in section 2.5.1 of this policy.

Head of the system

Their duties shall be as follows:

- Developing, operating and maintaining the information system throughout its life cycle, including its specifications, installation and verification of its correct operation.
- Defining the topology and management of the information system, establishing the criteria for its use and the services available on it.
- Ensuring that security measures are properly integrated into the general security framework.
- The power to propose the suspension of the processing of certain information or the provision of a certain service if serious security deficiencies that could affect the fulfilment of the established requirements are identified.
- Fulfilling the duties that are indicated in the documents within the scope of the ENS.

Head of privacy

Their duties shall be as follows:

- Coordinating all aspects related to the adequacy of the actions of THE COMPANY concerning the protection of personal data.
- Coordinating the compliance of the ENS for the protection of personal data, in collaboration with the head of security.

2.5.3. Designation procedures

The head of security shall be appointed by the Security Committee. This appointment shall be reviewed every 2 years or when the position becomes vacant.

Likewise, the rest of the positions indicated in the previous section shall be appointed by the Security Committee by means of the minutes of the meeting.

2.5.4. Review of the Security Policy

The Security Committee will be responsible for the annual review of this Security Policy and the proposal to revise or maintain it. It shall be approved by Top Management and distributed so that all affected parties are aware of it.

2.6. Personal data

THE COMPANY, in the provision of its services, processes particularly sensitive personal data.

The related documents, to which only authorised persons will have access, contain the records of the data processing activity concerned and those responsible for it. All THE COMPANY's information systems shall comply with the security levels required by the regulations for the nature and purpose of the personal data.

2.7. Risk management

All systems subject to this policy shall perform a risk analysis, assessing the threats and risks to which they are exposed. This analysis shall be repeated:

- on a regular basis, at least once a year;
- when the information handled is changed;
- when the services provided are changed;
- when a serious security incident has occurred;
- when serious vulnerabilities are reported.

In order to harmonise risk analyses, the Security Committee shall establish a reference assessment for the different types of information handled and the different services provided. The Security Committee shall streamline the availability of resources to meet the security needs of the different systems, promoting horizontal investments.

2.8. Staff obligations

All THE COMPANY employees are obliged to know and comply with this Security Policy and the Security Regulations, and it is the responsibility of the Security Committee to provide all means necessary to ensure that the information reaches those affected.

All THE COMPANY employees will attend an information security awareness session at least once a year. An ongoing awareness programme shall be established to cater for all employees in THE COMPANY, particularly new employees.

Persons with responsibility for the use, operation or administration of systems shall receive training in the safe operation of systems to the extent required to perform their work. Training shall be mandatory before taking up a responsibility, whether it is their first assignment or a change of job or job responsibilities.

2.9. Third parties

When THE COMPANY provides services to other public or private organisations or handles information from other public or private organisations, they will be made aware of this Security Policy, channels will be established for reporting and coordinating the respective Security Committees and procedures will be established for reacting to security incidents.

When THE COMPANY uses third party services or transfers information to third parties, they shall be made aware of this Security Policy and the Security Regulations that apply to such services or information. Said third party shall be subject to the obligations established in said regulations, and may develop its own operating procedures to comply with them. Specific incident reporting and resolution procedures shall be established. Third party employees shall be provided with appropriate security awareness at least at the same level as that set out in this Policy.

Where any aspect of the Policy cannot be satisfied by a third party as required in the above paragraphs, a report from the head of security specifying the risks incurred and how they will be addressed shall be required. Approval of this report will be required from those responsible for the information and services concerned before proceeding further.

3. APPLICABLE LAW

The laws that are considered applicable to the ISMS are listed below, together with a definition of the area responsible for assessing their impact on the organisation.

LAW / REGULATION	RESPONSIBILITY

Spanish Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations.	Legal advice
Spanish Law 40/2015, of 1 October, establishes and regulates the bases of the legal regime of Public Administrations, the principles of the system of liability of Public Administrations and the power to impose penalties, as well as the organisation and functioning of the General State Administration and its institutional public sector for the development of its activities.	Legal advice
Spanish Royal Decree 311/2022 of 3 May, which regulates the ENS.	Legal advice
Spanish Law 1/2015 of 30 March 2015 amending Organic Law 10/1995 of 23 November 1995 on the Penal Code.	Legal advice
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.	Legal advice
Spanish Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights.	Legal advice
Spanish Law 34/2002 on Information Society Services (LSSI)	Legal advice
Spanish Law 22/11, of 11/11/1987, on Intellectual Property	Legal advice
Spanish Law 17/2001, of 7 December, on Trade Marks.	Legal advice
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.	Legal advice
Spanish Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.	Legal advice