kentkart

SECURITY POLICY

Rev No	Explanation of Revision	Date of Revision

Text adopted on the date indicated in the table. The document is effective from that date until it is replaced by a new version. This text annuls the previous one, which was approved according to the indications in the previous table.

It will be reviewed annually, with a new version being prepared only in the event of changes. The annual review will be reflected in the Management Review report.

Date-Document No	Written by	Reviewed by	Approved by
BGYS-ENS-PO01 R0 10.02.2026	Security Officer	Security Committee	Management Board

kentkart

SECURITY POLICY

INDEX

kentkart

SECURITY POLICY

1. DECLARATION OF PRINCIPLES

KENTKART (hereinafter KENTKART) is an organisation specialising in Supply,Sales,Installation,Operation and Maintenance of Hardware and Softwares of Electronic Fare Collection Systems ,CCTV Surveillance Systems, Real Time Passenger Information, Vehicle Tracking and Smart City Technologies.. To this end, it assumes values that it considers essential for the achievement of its objectives, such as the preservation of information and personal data, both its own and that of other interested parties, and the professional and personal development of all the members of its work team.

Due to our activity, at KENTKART we are aware that information is an asset with a high value for our organization and requires, therefore, adequate protection and management in order to give continuity to our line of business and minimize possible damage caused by failures to the integrity, availability and confidentiality of information. Likewise, both current legislation relating to the protection of personal data (GDPR and LOPDGDD), and KENTKART's commitment to our customers make us especially sensitive to the processing of personal data to which we have access in the exercise of our activity.

To this end, KENTKART establishes a set of management activities that aim to preserve the principles of Confidentiality, Integrity, Availability, Authenticity, Traceability, as well as Regulatory Compliance of the information. In turn, these principles are defined as follows:

- Confidentiality: it is the property that guarantees that access to information can only be exercised by the persons authorized to do so.
- Integrity: is the property of safeguarding the accuracy and completeness of information assets.
- Availability: is the quality that ensures that authorized persons can access and process information at any time when it is necessary.
- Authenticity: it is the property or characteristic consisting of an entity being who it claims to be or that guarantees the source from which the data comes.
- Traceability: is the property or characteristic consisting of the fact that the actions of an entity can be attributed exclusively to that entity.
- Regulatory Compliance: is the property that ensures that the 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. To defend against these threats, a strategy that adapts to changes in environmental conditions is required to ensure the continuous delivery of services.

This implies that the different departments must apply the minimum security measures required by the National Security Scheme and ISO 27001, as well as continuously monitor the levels of service provision, monitor and analyze reported vulnerabilities, and prepare an effective response to incidents to ensure the continuity of the services provided.

Different departments in the organization must ensure that SECURITYis an integral part of every stage of the system's lifecycle, from conception to decommissioning, development/acquisition decisions and operational activities. Security requirements and funding needs should be identified and included in planning, in the request for proposals, and in tender documents for projects.

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

Within the protection of the above, the protection of privacy is embedded. Our systems process sensitive personal data and therefore, the protection of privacy stands as an essential pillar within the ISMS framework and is constituted as a social need that companies must respect and protect, as well as subject to specific legislation and/or regulation around the world.

2. GENERAL OBJECTIVES

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 signature policies, as well as the defined procedures.

These actions from the point of view of security and privacy are selected and implemented based on the risk analysis and the balance between acceptable risk and cost of the measures.

The objective of the Security Policy is to establish the framework for action necessary to protect information and data resources against threats, internal or external, deliberate or accidental.

The information and data can exist in a variety of formats, with both electronic supports such as paper or other media, and sometimes includes critical data about the operations, strategies or activities of KENTKART and its customers and even, where appropriate, data of a sensitive nature established by the regulations on the protection of personal data. The loss, corruption, or theft of information or the systems that manage it has a high impact on our Firm.

KENTKART is convinced that effective Information Security and Privacy Management is an enabling element for the organization to fully understand and act appropriately to the risks to which the

information is exposed, as well as to be able to respond and adapt efficiently to the growing requirements of regulatory bodies. laws, and of course their clients.

3. SENIOR MANAGEMENT COMMITMENT

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

To this end, the management declares the commitment of KENTKART to:

- To establish as a primary objective the services and productions of fare collection systems, fleet management systems, passenger information systems, smart mobility systems 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 at its disposal.
- Apply the principle of continuous improvement to all the processes of the organization, with the additional objective of achieving the highest degree of customer satisfaction.
- Ensure compliance with the applicable legal and regulatory requirements (in particular those relating to the protection of personal data), as well as those that the organisation has voluntarily assumed in the development of Corporate Social Responsibility and in the Code of Conduct.
- To promote the participation, communication, information and training of the professional team with the aim of making them feel part of the work of the organisation as a whole.
- Promote the commitment to responsibility among the members of the team in accordance with the quality requirements, as well as those related to privacy and information security agreed both internally and with customers, through appropriate and regular training and awareness actions.
- Ensure business continuity by developing continuity plans in accordance with recognized methodologies.
- To carry out 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 the projects and services underway and to minimise risks through the development of specific policies, technical solutions and contractual agreements with specialised organisations.
- Commitment to information to interested parties.
- Selection of suppliers and subcontractors based on criteria related to privacy and information security.

The management of KENTKART undertakes to support and promote the principles established in this Policy, for which it asks the staff of KENTKART to assume and abide by the provisions of the documented management system for the ENS.

4. PRINCIPLES OF SECURITY

Following the guidelines of chapter II, the basic principles by which KENTKART is governed are the following:

a) Security as an integral process, made up of all the elements related to the information system, paying special importance to the awareness of all participants.
b) Risk-based security management, as described in paragraph 10 of this document.
c) Prevention, detection, response and conservation. Developed in section 6 of this document.
d) Existence of lines of defence made up of multiple layers of security organised into organisational, physical and logical measures.
e) Continuous monitoring and periodic re-evaluation, which allows the detection of anomalous behaviour and its response, as well as measuring its evolution by detecting vulnerabilities and deficiencies in the configuration, periodically verifying its effectiveness, which can lead to a rethinking of our security design.
f) Differentiation of responsibilities, as developed in section 7 of this document.

To do this, we will apply the following minimum requirements.

a) Organization and implementation of the security process.
b) Risk analysis and management.
c) Personnel management.
d) Professionalism.
e) Authorisation and access control.
f) Protection of the facilities.
g) Acquisition of security products and contracting of security services.
h) Minimal privilege.
i) System integrity and updating.
j) Protection of information in storage and in transit.
k) Prevention of other interconnected information systems.
l) Activity logging and detection of harmful code.
m) Security incidents.

n) Continuity of activity.

o) Continuous improvement of the security process.

These minimum requirements are in proportion to the risks identified in our systems, in accordance with the provisions of Article 28 and are developed in the ENS management system documents.

5. CRITERIA FOR DETERMINING THE LEVEL OF SECURITY

KENTKART will establish the **criteria to determine the level of security required** for the information and services, in accordance with the framework established in Article 40 of the ENS and the general criteria defined in Annex I.

In particular:

- The level of information and systems security shall be determined on the basis of:
  - The impact an incident would have on the **confidentiality, integrity, availability, authenticity and traceability** of information.
  - The nature of the information processed (e.g. personal data, sensitive information, public information).
  - The applicable legal, regulatory and contractual requirements.
- KENTKART will apply the categorization of systems established in the ENS, assigning a **Basic, Medium or High** level to each information system.
- The categorisation criteria and the resulting level of security will be reviewed periodically and whenever there are relevant changes in the systems, information or risk context.

6. RESPONSIBILITY FOR INFORMATION

KENTKART will explicitly establish those **responsible for each type of information** handled by the information systems(asset list,risk analysis,roles and resp.etc) ensuring that there is a clear assignment of responsibilities.

Likewise, a General Information Officer has been appointed as the ultimate responsible person in the Security Committee, whose responsibilities are those indicated in the corresponding section of this policy.

7. DOCUMENTATION MANAGEMENT

This Security Policy complements KENTKART's security policies in different areas and will be developed by means of security regulations that address specific aspects. The security regulations will be available to all members of the organization who need to know them, in particular for those who use, operate or manage information and communications systems.

Information Security documentation will be classified into three levels, so that each document at one level is based on those at a higher level:

- First level: Security policy.
- Second level: Security regulations and procedures.
- Third level: Electronic reports, records and evidence.

Staff will have access to relevant information in the following repository

SHAREPOINT, (INTRANET), DMS (DOC.MNG.SYSTEM) CANIAS ERP,JIRA

8. INCIDENT MANAGEMENT

9. Prevention

Departments should avoid, or at least prevent as much as possible, information or services from being harmed by security incidents. To do this, departments must 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 SECURITYroles and responsibilities of all personnel, must be clearly defined and documented.

To ensure compliance with the policy, departments must:

- Authorize systems before they go into operation.
- Regularly assess security, including assessments of configuration changes made on a routine basis.
- Request periodic review by third parties for the purpose of obtaining an independent evaluation.

10.Detection

Since services can be rapidly degraded due to incidents, ranging from a simple slowdown to a stoppage, services must monitor the operation on an ongoing basis to detect anomalies in service delivery levels and act accordingly as set out in Article 9 of the ENS.

Monitoring is especially relevant when lines of defence are established in accordance with Article 8 of the ENS. Detection, analysis and reporting mechanisms will be established that reach those responsible regularly and when there is a significant deviation from the parameters that have been pre-established as normal.

11.Reply

Departments must:

- Establish mechanisms to respond effectively to security incidents.
- Designate a point of contact for communications regarding incidents detected in other departments or in other agencies.
- Establish protocols for the exchange of information related to the incident. This includes two-way communications with Emergency Response Teams (CERTs).

12.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.

13.SECURITY ORGANIZATION

14.Security Committee

The members of the Security Committee will be designated in a founding act, which will indicate the person appointed and the position he or she must hold.

The Secretary of the Security Committee shall be the PERSON RESPONSIBLE FOR SECURITY and shall have the following functions:

- Convene the meetings of the Security Committee.
- Prepares the topics to be discussed in the meetings of the Committee, providing timely information for decision-making.
- Prepare the minutes of the meetings.
- It is responsible for the direct or delegated implementation of the Committee's decisions.
- The Security Committee shall report to the Director General.

The Security Committee shall have the following functions:

- To attend to the concerns of Senior Management and the different departments.
- Regularly report on the state of information security to Senior Management.
- Promote continuous improvement of the information security management system.
- Develop the Organization's strategy for the evolution of information security.
- Coordinate the efforts of the different areas in the area of information security, to ensure that efforts are consistent, aligned with the strategy decided on the matter, and avoid duplication.
- Prepare (and regularly review) the Security Policy for approval by Management.
- Approve information security regulations.
- Coordinate all security functions of the organization.
- Ensure compliance with the applicable legal and sectoral regulations.
- Ensure that security activities are aligned with the objectives of the organization.
- Coordinate the Continuity Plans of the different areas, to ensure seamless action in case they need to be activated.
- Coordinate and approve, where appropriate, the project proposals received from the different security areas, being responsible for managing a regular control and presentation of the progress of the projects and announcing possible deviations.
- Receive security concerns from the entity's management and transmit them to the relevant departmental managers, obtaining from them the corresponding responses and solutions that, once coordinated, must be communicated to the management.

- Obtain regular reports from departmental security managers on the state of the organization's security and possible incidents. These reports are consolidated and summarized for communication to the entity's management.
- Coordinate and respond to the concerns transmitted through the departmental security managers.
- Define, within the Corporate Security Policy, the assignment of roles and the criteria to achieve the relevant guarantees in relation to segregation of duties
- Develop and approve the training and qualification requirements for administrators, operators and users from the point of view of information security.
- Monitor the main residual risks assumed by the Organization and recommend possible actions regarding them.
- Monitor the performance of security incident management processes and recommend possible actions regarding them. In particular, to ensure the coordination of the different security areas in the management of information security incidents.
- Promote the performance of periodic audits to verify compliance with the body's obligations in terms of safety.
- To approve plans to improve the Organization's information security. In particular, it will ensure the coordination of different plans that may be carried out in different areas.
- Prioritise actions in the field of security when resources are limited.
- Ensure that information security is taken into account in all projects from their initial specification to their commissioning. In particular, it should ensure the creation and use of horizontal services that reduce duplication and support a homogeneous operation of all ICT systems.
- Resolve conflicts of responsibility that may arise between the different managers and/or between different areas of the Organization.

15.Roles: Roles and responsibilities

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

Information Controller

- Ultimate responsibility for the use made of certain information and, therefore, for its protection.
- Ultimately responsible for any error or negligence that leads to an incident of confidentiality or integrity (in terms of data protection) and availability (in terms of information security).
- Establish the requirements for information on security matters.
- Determine and approve information security levels.

- Approve the categorization of the system with respect to information.
- Those that are indicated in the documents within the scope of the ENS.

Service Officer

- Establish the requirements of the service in terms of security.
- Determine the security levels of the services.
- Approve the categorization of the system with respect to services.
- Those that are indicated in the documents within the scope of the ENS.

Security Officer

Its functions will be as follows

- Maintain 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 organization's Information Security Policy.
- Promote training and awareness in information security within its area of responsibility.
- Approve the declaration of applicability.
- Channel and supervise both compliance with the security requirements of the service provided or solution provided, as well as communications related to information security and incident management for the scope of said service (POC).
- Those that are indicated in the documents within the scope of the ENS.

The Security Officer will be the secretary of the Security Committee with the functions indicated in section 7.2 of this policy.

In accordance with the principle of "segregation of functions and tasks" set out in Article 10 of the ENS, the Security Manager will be a figure differentiated from the System Manager.

System Manager

Its functions will be as follows:

- Develop, operate and maintain the information system throughout its life cycle, including its specifications, installation and verification of its correct operation.
- Define the topology and management of the information system, establishing the criteria for use and the services available in it.
- Ensure that security measures are properly integrated into the overall security framework.
- Power to propose the suspension of the processing of certain information or the provision of a certain service if it detects serious security deficiencies that could affect the satisfaction of the established requirements.

- Those that are indicated in the documents within the scope of the ENS.

Privacy Officer

Its functions will be as follows:

- Coordinate all aspects related to the adequacy of KENTKART's actions in terms of personal data protection.
- Coordinate, together with the Security Officer, compliance with the ENS with respect to the protection of personal data.

16.Appointment procedures

The Security Officer will be appointed by the Security Committee. The appointment will be reviewed every 2 years or when the position becomes vacant.

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

17.Security Policy Review

The Security Committee's mission will be the annual review of this Security Policy and the proposal for its revision or maintenance. The Policy will be approved by Senior Management and disseminated so that it is known to all affected parties.

18.Conflict resolution

In the event of conflicts between the different controllers, the Information Security Committee shall have the authority to settle the discrepancies.

19.PERSONAL DATA

KENTKART, in the provision of its service, processes particularly sensitive personal data.

The related documentation, to which only authorised persons will have access, includes the records of data processing activity affected and the corresponding data controllers. All KENTKART's information systems will comply with the security levels required by the regulations for the nature and purpose of personal data.

With regard specifically to the protection of personal data, KENTKART undertakes to comply with the principles indicated in the reference legislation. These are:

- Principle of "lawfulness, transparency and loyalty". The data must be processed in a lawful, loyal and transparent manner for the interested party.
- Principle of "finality". The data must be processed for one or more specific, explicit and legitimate purposes and, on the other hand, it is prohibited for the data collected for specific, explicit and legitimate purposes to be subsequently processed in a manner incompatible with those purposes.
- Principle of "data minimization". Apply technical and organisational measures to ensure that data that are only necessary for each of the specific purposes of the processing are processed, reducing the extent of the processing, limiting the storage period and its accessibility to what is necessary.
- Principle of "accuracy". Have reasonable measures to ensure that the data is updated, deleted or modified without delay when it is inaccurate with respect to the purposes for which it is processed.
- Principle of "limitation of the retention period". The retention of data must be limited in time to the achievement of the purposes pursued by the processing.
- Principle of "security" Carry out a risk analysis aimed at determining the technical and organisational measures necessary to guarantee the integrity, availability and confidentiality of the personal data they process.
- Principle of "active responsibility" or "demonstrated responsibility". To maintain due diligence on an ongoing basis to protect and guarantee the rights and freedoms of the natural persons whose data are processed based on an analysis of the risks that the processing represents for those rights and freedoms, so that we can guarantee and demonstrate that the processing complies with the provisions of the GDPR and the LOPDGD.
- Direct, support and supervise the information security management system, as established in RD 311.2022 and subsequent amendments, as well as ISO 27001, and seek to achieve its objectives.

20.RISK MANAGEMENT

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

- Regularly, at least once a year
- When the information handled changes
- When the services provided change

- When a major security incident occurs
- When serious vulnerabilities are reported

For the harmonisation of risk analyses, the SECURITY Committee will establish a reference assessment for the different types of information handled and the different services provided. The Security Committee will boost the availability of resources to meet the security needs of the different systems, promoting horizontal investments.

21.AWARENESS AND TRAINING

It is the responsibility of the organization to achieve full awareness that information security affects all members of and all activities, in accordance with the principle of Security as an integral process contained in Article 6 of the ENS, as well as the articulation of the necessary means so that all the people involved in the process and their hierarchical managers have a sensitivity to the risks that are involved. they run. For this reason, KENTKART has a system implemented in all areas of the organization to train, inform and raise awareness among all personnel regarding their involvement in the achievement of SECURITYobjectives.

22.STAFF OBLIGATIONS

All members of KENTKART have the obligation to know and comply with this Security Policy and the Security Regulations, and it is the responsibility of the Security Committee to provide the necessary means for the information to reach those affected.

All members of KENTKART will attend an information security awareness session at least once a year. A continuous awareness programme will be established to serve all members of KENTKART , in particular those who have recently joined.

Persons with responsibility for the use, operation or administration of systems shall be trained in the safe handling of systems to the extent they need it to perform their work. Training will be mandatory before assuming a responsibility, whether it is your first assignment or if it is a change of job or responsibilities in it.

23.THIRD PARTIES

When KENTKART provides services to other public or private organizations or handles information from other public or private organizations, they will be made participants in this Security Policy, channels will be established for reporting and coordination of the respective Security Committees and action procedures will be established for the reaction to security incidents.

When KENTKART uses third-party services or transfers information to third parties, they will be made participants in this Security Policy and the Security Regulations that concern such services or information. This third party will be subject to the obligations established in said regulations, and may develop its own operating procedures to satisfy it. Specific procedures for reporting and resolving incidents will be established. It will be ensured that third-party personnel are adequately aware of security, at least at the same level as that established in this Policy.

Where any aspect of the Policy cannot be satisfied by a third party as required in the preceding paragraphs, a report from the Security Officer shall be required specifying the risks incurred and how to deal with them. Approval of this report by those responsible for the information and services concerned will be required before proceeding.

24.APPLICABLE LEGISLATION

Below are the laws that are considered applicable to the ISMS, along with a definition of the area responsible for assessing its impact on the organization.

Law/Regulation	Liability
Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations	Security Manager
Law 40/2015, of 1 October, establishes and regulates the bases of the legal regime of the Public Administrations, the principles of the system of liability of the Public Administrations and the sanctioning power, as well as the organisation and operation of the General State Administration and its institutional public sector for the development of its activities	Security Manager
Royal Decree 311/2022, of 3 May, regulating the National Security Scheme.	Security Manager
Organic Law 1/2015, of 30 March, amending Organic Law 10/1995, of 23 November, on the Criminal Code	Security Manager
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	Security Manager
Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights	Security Manager
Law 34/2002 on Information Society Services (LSSI)	Security Manager
Royal Legislative Decree 1/1996, of 12 April, approving the revised text of the Intellectual Property Law, regularising,	Security Manager

clarifying and harmonising the legal provisions in force on the subject.	
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	Security Manager
Law 6/2020, of 11 November, regulating certain aspects of electronic trust services.	Security Manager