Information Security Policy

jtsec Beyond IT Security SL

Version: 1.5

1   INTRODUCTION

jtsec Beyond IT Security SL is a limited liability company with CIF B93551422 and head office in AV. DE LA CONSTITUCIÓN, 20, OF 208, 18012 GRANADA (SPAIN).

jtsec may be contacted through e-mail: management@jtsec.es or by phone: (+34) 858-981-999

The Board of Directors of **jtsec Beyond IT Security SL**, hereinafter referred to as **jtsec**, is aware and assumes that one of the most important objectives of the company is the protection of information assets from any threat, whether internal or external, deliberate or accidental, that poses a risk to the confidentiality, integrity or availability of information.

jtsec considers that the planning, implementation of controls, monitoring and continuous improvement of information security are essential management processes to ensure the competitiveness and sustainability of the business, considering security by default a management priority.

2   MISSION AND OBJECTIVES

The services offered by jtsec to its clients are the following:

- Security Certification Consulting like:
    o Common Criteria Consulting
    o FIPS 140-2 & FIPS 140-3 Consulting
    o PCI-PTS & PCI-CPOC Consulting
    o Other Security Norms Consulting
    o Training
- Security Certification Evaluation like:
    o LINCE evaluation
    o Common Criteria evaluation
    o IEC62443-1 and IEC62443-2 evaluation
    o ETSI TS 103 701 evaluation
    o CCN-MEMEC Evaluatioon
    o FIPS 140-X Evaluation
- Ethical Hacking services like:
    o ICT Product Testing
    o Systems Audit
    o SME Cybersecurity

The evaluation activities carried out by jtsec in conformance to UNE-EN ISO/IEC 17025 and subject to this quality manual are the followings:

- LINCE in conformance to [CCN-STIC-2001] and [CCN-STIC-2002].
- Common Criteria in conformance to [CCP1], [CCP2], [CCP3] and [CEM]
- IEC62443-4-1 and IEC62443-4-2 standards in conformance to [IEC62443-4-1] and [IEC62443-4-2].
- ETSI TS 103 701 standard in conformance to [ETSI-TS-103701]
- EVMco in conformance to [SBMP-EM], [SBMP-ELR] and [SBMP-EP]
- CCN-MEMEC in conformance to [CCN-MEMEC]
- FIPS 140-X in conformance to ISO/IEC 24759.

Additionally, jtsec develops innovative frameworks to smooth the certification processes.

The main objective of jtsec is to support our clients using our innovative and exclusive framework automatizing the process and saving time and money.

3   COMMITMENT TO SECURITY

This is why the Management assumes this responsibility and commits itself to:

1. Implement, maintain and continually improve an Information Security Management System for the activities set out in our Protection Manual.
2. To contribute from information security management to fulfil the mission and objectives established by **jtsec**
3. To have the necessary control measures in place to comply with the legal requirements applicable as a result of the activity carried out, especially with regard to the protection of personal data and the provision of services by electronic means.
4. To adopt the appropriate security measures for the processing of personal data, following the guidelines of the European Data Protection Regulation and maintaining sufficient diligence to comply with the principle of proactive responsibility and the principle of accountability.
5. To ensure access, integrity, confidentiality, availability, authenticity, traceability of information and the continuous provision of services, acting preventively, supervising daily activity and reacting promptly to incidents.
6. To protect **jtsec's** information resources and the technology used to process them against threats, internal or external, deliberate or accidental, in order to ensure compliance with the confidentiality, integrity, availability, legality and reliability of the information.
7. To raise awareness and train **jtsec** staff and its collaborators in Information Security.
8. To evaluate and deal with the risks and threats to which **jtsec's** information, services and systems are exposed.
9. Provide the human and material resources necessary to carry them out. In particular, to ensure that the functions and responsibilities of the Information Security Management System are defined and communicated.
10. Ensure that, for any acquisition of products, both software and hardware, security requirements are taken into account.
11. Implement the necessary measures for the recording of activity and the analysis of the same in search of abnormal patterns and the implementation of the appropriate actions for their treatment.

4   PRINCIPLES AND GUIDELINES

jtsec's Information Security Management System is based on the following principles and guidelines:

➢ **Prevention: jtsec** must prevent, and avoid, as far as possible, that information or services are harmed by security incidents. To this end, the Management must implement the minimum security measures determined by the National Security Scheme regulated by Royal Decree 3/2010 of 8 January, as well as any additional controls identified through a threat and risk assessment.

To this end, the **jtsec** Management must:

- Authorise systems or services prior to going into operation.
- Regularly assess security, including assessments of configuration changes made on a routine basis.
- Request periodic review of compliance with the ENS and the requirements of the UNE-ISO/IEC 27001 Standard by third parties.

➢ **Detection: jtsec** Management must ensure that the operation is continuously monitored to detect anomalies in service delivery levels and act accordingly. Similarly, it must establish appropriate mechanisms to ensure that any security incident is reported to the Protection Manager.

➢**Response: jtsec** management should establish mechanisms to respond effectively to security incidents.

➢**Recovery:** To ensure the availability of critical services, **jtsec** management should develop ICT systems continuity plans as part of its overall business continuity plan and recovery activities.

In compliance with Article 11 of the Royal Decree of the ENS, this Security Policy shall be developed by applying the following minimum requirements:

- Organization and implementation of the security process.
- Risk analysis and management.
- Personnel management.
- Professionalism.
- Authorization and access control.
- Protection of facilities.
- Procurement of products.
- Security by default.
- System integrity and updating.
- Protection of information stored and in transit.
- Prevention against other interconnected information systems.
- Logging of activity.
- Security incidents.
- Business continuity.
- Continuous improvement of the security process.

5 REGULATORY FRAMEWORK

The **regulatory framework** for **jtsec's** activities in this field is:

a) Royal Decree 311/2022 of 04 May, which regulates the National Security Scheme.
b) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR).
c) Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights.
d) Law 9/2017, of 8 November, on public sector contracts
e) Standard UNE-ISO/IEC 27001:2022
f) Order PRE/2740/2007, of 19 September, approving the Regulation on the Evaluation and Certification of Information Technology Security.
g) Royal Legislative Decree 1/1996 of 12 April 1996, approving the revised text of the Intellectual Property Law (LPI), regularising, clarifying and harmonising the legal provisions in vigour on the matter.
h) Law 06/2020 of 11 November on2020 electronic signature.
i) Royal Legislative Decree 2/2000 of 16 June, approving the revised text of the Law on Public Administration Contracts.
j) Resolution of 13 October 2016, of the Secretary of State for Public Administrations, approving the Technical Security Instruction in accordance with the National Security Scheme.
k) Law 34/2002 of 11 July on 2002 (LSSICE).

6   ORGANIZATIONAL STRUCTURE

The organizational structure of security management at the enterprise level is composed of a working group we call Protection Staff composed of a governance and supervisory role we call Protection Manager and an operational role reporting to management we call Protection Administrator.

Within the ENS, the Protection Manager assumes the responsibilities of:

- Information Responsible (Responsable de la Información).
- Security Responsible (Responsable de la Seguridad).
- Service Responsible (Responsable del Servicio).

Within the ENS, the Protection Administrator assumes the responsibilities of:

- System Responsible (Responsable del Sistema)
- Security Administrator (Administrador de la Seguridad)

Without prejudice to the possibility of delegating certain functions.

6.1   RESPONSIBILITIES OF THE PROTECTION MANAGER

6.1.1   AS INFORMATION RESPONSIBLE

- To enforce compliance with the provisions established in the National Security Scheme (ENS) when the information system is within the scope of application of the same and, where appropriate, issue guidelines.
- Ensure that the security risk of your information systems is managed, defining for each of them their acceptable residual risk level, i.e. the remaining risk in the information system after the implementation of the security measures established in the security plan and that can be assumed.

6.1.2   AS SECURITY RESPONSIBLE

Responsible for determining decisions to satisfy information and service security requirements.

It shall have the following functions:

- Determine the decisions necessary to satisfy the information and service security requirements established by their respective managers.
- Periodically carry out a process of analysis of the risks of the information system that allows identifying the risks to which it is exposed, and the measures to ensure the level of acceptable residual risk approved for each information system.
- Establish the set of projects and actions that will make up the security plan that will allow the implementation of the proposed security measures and submit it to the person in charge of the information system.
- To monitor and control the security status of the information system and verify that the security measures defined are adequate for the protection of the information and services.
- Perform periodic audits determined in each information system, including those related to data protection, to ensure the correct application of security measures and compliance with the rules and procedures in force in the organization.

- To draw up, when necessary, the statements of applicability of the information systems with respect to the National Security Scheme (ENS).

6.1.3 AS SERVICE RESPONSIBLE

It will implement the security measures related to its scope of competences included in the security master plan.

The Protection Manager, who is responsible for the maintenance of the technical infrastructures that support the services, without prejudice to the possibility of delegating certain functions, is designated as the person in charge of providing the service.

He/she will have the following functions:

- Implement the security measures that fall within its scope of action established in the security plan drawn up by the security manager and approved by the person responsible for the information system.
- To observe compliance with the established rules and procedures and normal operation of the information systems.
- Supervise and guarantee the management, configuration and updating, if necessary, of the resources that support the correct operation of the information systems and the provision of services.
- Collaborate in the audits carried out by the security manager and provide complete and accurate information on the status of the security measures implemented for which he/she is responsible.

6.2 RESPONSIBILITIES OF THE PROTECTION ADMINISTRATOR

6.2.1 AS SYSTEM RESPONSIBLE

Ultimately responsible for the operation of the services. The information system integrates all the company's information systems.

He/she assumes the following functions:

- Suspend, subject to the agreement of the information and service managers, the handling of certain information or the provision of a service if he is informed of serious security deficiencies.
- Adopt the necessary measures to ensure that personnel with access to an information system are aware of the security standards to be applied.
- Propose information security training and awareness plans within its area of responsibility, as well as establish dissuasive actions in favor of security.
- Determine the security requirements of the information handled in the organization.
- Identify and assess the criticality of the information handled within the scope of their functions and determine the security requirements to be met for each type of information.
- Determine the life cycle of the information handled and determine the procedures for its creation, treatment and destruction.
- Satisfy the rights of the data owners.
- To record the condition that legitimizes the processing.

- Limit the processing based on the consent of the data owner.
- Carry out the privacy impact assessment.

7 SECURITY COMMITTEE

The security committee is composed of the personnel member of the Board of Directors and personnel member of Protection Team.

The responsibility of the members is defined and approved in Constitution of Security Committee minutes document.

8 RISK MANAGEMENT

A process of risk analysis of the information systems will be carried out continuously, in accordance with the principles of 'risk-based security' management and 'periodic reassessment' established in the National Security Scheme.

The security responsible will be in charge of performing the information system risk analysis, ensuring that it is performed correctly and completely and communicating the results to Protection Staff.

The person responsible for the system is the owner of the risks on the information system, being responsible for its monitoring and control, without prejudice to the possibility of delegating this task.

9 SECURITY REGULATIONS

The present security policy must be developed in different security regulations that detail and specify the security requirements of the information and services, the necessary tasks to guarantee their compliance and the responsibilities of all the personnel involved in them.

These regulations are structured in the following levels:

1. The security policy. It establishes the general security strategy and is defined in this document.

2. The protection manual and other security manuals. The protection manual determines the security objectives and general guidelines in each specific area and establish the responsibilities of the personnel involved. Other security manuals are related to risks analysis, the statement of applicability and the GDPR. These manuals are named as JTSEC-M-[name].

3. Security procedures. Set of documents that describe explicitly and step by step how to perform certain tasks in order to comply with the stipulations of the security standards. Each procedure should at least detail under what conditions it should be applied, who should carry it out and what to do at any given time.

The security policy will be approved by the Board of Directors while the protection manual will be approved by the Protection Manager. Both will be mandatory throughout the organization. The security procedures are mandatory and require the approval of the System Responsible and Security Responsible and will be applicable in their corresponding area.

Any major incident will be communicated to the relevant or affected interested parties by the jtsec Board of Directors.

10 RESPONSIBILITY OF THE PERSONNEL

All personnel forming part of the company or collaborating with it in the exercise of their functions must be familiar with and apply this security policy, as well as the security rules and procedures of the information system to which they have access, within their scope of action. These rules and procedures will be provided to them by the information system responsible.

11 CONFLICT RESOLUTION

In case of conflict between the different persons in charge, this shall be resolved by their hierarchical superior. In the absence of the above, the decision of information responsible shall prevail.

12 TRAINING AND AWARENESS

The company will develop specific activities aimed at the training and awareness of its personnel in matters of information security, as well as the dissemination of this security policy and its regulatory development, particularly among newly hired personnel. To this end, the company's training plans shall include specific training activities on this subject.

The company will promote a culture of information security aligned with the security policy among those organizations and users of the company's information, and will also promote a culture of information security aligned with the security policy among those organizations and users of the company's information security policy.

13 INFORMATION CLASSIFICATION

The Protection Manager is responsible for the information managed by the system and for classifying the project information. The classification levels are; Public information, White information, and Black information.

The classification levels are defined in the Content Management Manual.

14 REFERENCES

Besides the documents that are part of the management system and listed in [JTSEC-L-LABDOCUMENTS], the following references are applicable:

Reference	Document Name
CCN-STIC-2001	Definición de la Certificación Básica de Seguridad v2.0 Marzo 2022
CCN-STIC-2002	Metodología de Evaluación para la Certificación Básica de Seguridad v2.0 Marzo 2022
CCP1	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 1: Introduction and general model
CCP2	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 2: Security functional components

CCP3	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 3: Security assurance components
CEM	Common Criteria Evaluation methodology, Version 3.1, Revision 5
CCN-MEMEC	Cryptographic Mechanisms Evaluation Methodology. Noviembre 2023
IEC62443-4-1	IEC INTERNATIONAL STANDARD IEC 62443-4-1:2018 Security for industrial automation and
IEC62443-4-2	IEC INTERNATIONAL STANDARD IEC 62443-4-2:2019 Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components
ETSI-TS-103701	ETSI TS 103 701 V1.1.1 (2021-08) Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements
SBMP-EM	EMVCo SBMP Security Evaluation Methodology, v1.8, jan 2024
SBMP-ELR	EMVCo SBMP Security Evaluation Laboratory Requirements for SBMP, v2.1, Jan 2024
SBMP-EP	EMVCo SBMP Security Evaluation Process, v1.7, Aug 2023

15 UPDATING AND PERIODIC REVIEW

This security policy shall be kept permanently updated in order to adapt it to the progress of the services, technological evolution and the development of the information society, as well as to international security standards.

The proposals for revision of the security policy shall be prepared by the Board of Directors which, for such purpose, shall regularly review the timeliness, suitability, completeness and accuracy of the provisions of the security policy in the use of electronic media.

The scope of this Information Security Policy covers all the processes and activities performed in jtsec.

The Board of Directors

In Granada, on 20 of May 2023