Vicomtech's Information Security Policy

INDEX

Contents

1. Approval and entry into Force

This Policy has been proposed and reviewed by the **Information Security Committee** of Vicomtech and approved on 28/03/2025 by the Management of **Vicomtech**.

This Information Security Policy is effective from that date and until it is replaced by a new Information Security Policy.

The entry into force of this Information Security Policy constitutes the repeal of any other previously existing policy.

This Information Security policy **will be reviewed at least once a year** and whenever there are significant changes in the organization, to ensure that it is aligned with the strategy and needs of the organization.

In the event of conflicts or different interpretations of this information security policy, the Management will be called upon for their resolution, after consulting the **Information Security Committee**.

2. Mission, objectives and Good Governance of Vicomtech

Vicomtech's mission is:

- To respond to the needs of companies and institutions in our region for Applied Research, Development, and Innovation in Information Technologies, especially the convergence of Computer Graphics and Computer Vision (Visual Computing), Data Analytics and Intelligence, Interactive Digital Media, and Language Technologies, in order to address new economic and social challenges and improve their competitiveness in a global market.
- To promote Knowledge Generation and the Transfer of our Technologies, developing prototypes of new products and facilitating new lines of business in cooperation with industry, supported by original Intellectual Property.
- To pursue excellence in scientific, technical, internal organizational, and customer service aspects, complying with the highest quality standards and regulations recognized in the scientific and industrial fields.
- To contribute to universal knowledge by training researchers and publishing the results of applied research in prestigious international journals and conferences.

- To develop alliances with leading strategic partners (academic, applied research, and industrial), both local and international, to promote networked applied research, train researchers, and jointly generate knowledge.
- To foster an environment of professional excellence and quality, enabling our staff to develop the skills necessary to work as a team and be drivers of technological change and innovation in general, both within the centre itself and in its expansion into industry or other scientific and technological fields.

Vicomtech's main objectives are:

- To establish a Critical Research Mass that meets the criteria established by the Basque Government and possesses Excellent Research Profiles through co-supervision of doctoral theses in collaboration with Basque universities.
- To promote the Publication of Research Articles in top-tier journals.
- To transfer the knowledge generated to industry and society through: contracting applied research projects, protecting and transferring assets, transferring human talent, and impacting new technology-based companies.

These objectives must be met while ensuring the Centre's Good Governance, the pillars of which are: culture, ethics, responsibility, transparency, efficiency, risk management, and integrity.

Vicomtech uses information systems that must be protected effectively and efficiently.

3. Objectives and Mission of the Information Security Policy

This **Policy** establishes the guidelines and lines of action on Information Security that govern the way **Vicomtech** manages and protects its information and services, as well as the communication with its customers and other stakeholders.

Vicomtech has established an information security management framework according to the Royal Decree 311/2022, of May 3rd, which regulates the **National Security Scheme**, hereinafter **NSS**, and the Information Security Management System **ISO/IEC 27001**, hereinafter **ISMS**, integrated within the Integrated Management System, hereinafter **IMS**.

The management of information security must guarantee the proper functioning of the activities of control, monitoring and maintenance of the infrastructures and general installations necessary for the adequate provision of services, as well as the information derived from the functioning of

these. To this end, the following are established as **general** information security **objectives**:

- To contribute from the management of information security to comply with the mission and Good Governance established by Vicomtech.
- To have the necessary control measures in place to comply with the legal requirements that may be applicable as a consequence of the activity carried out, especially with regard to the protection of personal data and the provision of services through electronic means.
- 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.
- To protect Vicomtech's information resources and the assets used for their processing, against threats, internal or external, deliberate or accidental, in order to ensure compliance with the confidentiality, integrity, availability, authenticity and legality of the information.

Vicomtech's **Management** is clearly **committed** to the dissemination, consolidation and compliance with this **Information Security Policy**.

4. Scope

This Policy shall be applicable to and mandatory for all Vicomtech's activities, to all its resources and work centres and to the processes affected by the NSS/ISMS and the GDPR, whether internal or external, linked to the entity through contracts or agreements with third parties.

The different departments must ensure that information security is an integral part of every stage of the system's lifecycle, from its conception through development or acquisition decisions and operational activities to its decommissioning.

Each member of Vicomtech, affected by the scope of the NSS/ISMS, **has the obligation to know and comply with this Security Policy**, as well as the Information Security procedures that complement it, being the responsibility of the Information Security Committee to arrange the necessary means for the information to reach the affected personnel.

5. Regulatory Framework

This security policy is established in accordance with the basic principles indicated in Chapter II of Royal Decree 311/2022, of 3 May, which regulates the National Security Scheme and shall be

developed by applying the minimum requirements established in ARTICLE 12. SECURITY POLICY AND MINIMUM SECURITY REQUIREMENTS.

The information security management framework also covers the protection of personal data and takes into account the provisions of **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016**, hereinafter referred to as the GDPR, as well as national data protection legislation.

Likewise, it shall be in accordance with the provisions of Law 59/2003 by the '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 add the 'Law 6/2020 of 11 November, regulating certain aspects of electronic trust services'.

Furthermore, any other rules that regulate **Vicomtech's** activity within the scope of its competences and any other rules aimed at ensuring the access, integrity, availability, authenticity, confidentiality, traceability and conservation of the data, information and services used in the electronic media managed by the Centre also in the exercise of its competences shall be applicable.

6. Information Security Principles

6.1. Integral Security

Security shall be understood as an integral process that applies to all activities of the organisation, and is constituted by all technical, human, material and organisational elements related to information systems.

6.2. Risk-based security management

Risk analysis and risk management shall be an essential part of the security process and shall be kept constantly up to date, enabling the maintenance of a controlled environment, minimising risks to acceptable levels.

6.3. Prevention, detection, response and recovery

Vicomtech **will prevent and avoid**, as far as possible, that information or services are harmed by security incidents. To this end, its responsible bodies shall implement the minimum security measures determined by the NSS/ISMS and by the GDPR, as well as any additional controls identified through a threat and risk assessment.

These measures and controls, as well as the security roles and responsibilities of all personnel, shall be clearly defined and documented in the **Integrated Management Manual**, ensuring that adequate

prevention, detection, response and preservation are guaranteed to ensure compliance with this **Information Security Policy**.

6.4. Lines of defence

The system shall have a protection strategy consisting of multiple layers of security, arranged in such a way that, when one of the layers fails, it allows:

- The development of an adequate reaction to incidents that could not be prevented, reducing the likelihood of the system as a whole being compromised to ensure business continuity.
- To minimise the final impact on it.

The lines of defence will consist of measures of an organisational, physical and logical nature.

6.5. Continuous monitoring and periodic reassessment

Audits will be conducted to review and verify the compliance of **Vicomtech's** ISMS/NSS with the requirements of ISO/IEC 27001 for the ISMS and with the Royal Decree 311/2022, which regulates the National Security Scheme, so that the staff affected by the scope of these audits must be collaborative for the effectiveness of the audits, as well as in the implementation of corrective actions that are derived for continuous improvement.

Security measures and controls shall be periodically re-evaluated and updated within the Information Security Management System in order to adapt their effectiveness to the constant evolution of risks and protection systems, including a security rethink, if necessary.

6.6. Security as a distinct function

In line with Article 10 of the National Security Scheme, a distinction shall be made between the person responsible for the information, the person responsible for the service, the person responsible for information security and the person responsible for the system. Responsibility for the security of information systems shall be differentiated from responsibility for the provision of services.

The person responsible for the information shall determine the requirements for the information processed; the person responsible for the service shall determine the requirements for the services provided; and the person responsible for information security shall determine the decisions to satisfy the information and service security requirements.

The person responsible for the system shall be responsible for the operation of the Information System in accordance with the determined security measures.

7. Information Security Organisation

In general, **each and every user of Vicomtech's information systems is responsible for the security of the information assets** through a correct use of them, always in accordance with their professional and academic attributions.

In order to better respond to security incidents, Vicomtech will maintain cooperative security relations with the competent authorities, IT or communication service providers, as well as public or private organisations dedicated to promoting the security of information systems.

7.1. Committees: Roles and Responsibilities

7.1.1. Steering Committee

In the area of information security, **Vicomtech's Steering Committee** has the following functions:

- To approve Vicomtech's Information Security Policy and any other sectorial policy complementary to the previous one that allows compliance with the National Security Schemes and the General Data Protection Regulation.
- To approve the organisational development proposed by the **Information Security Committee**.
- To appoint and dismiss the members of the **Information Security Committee**.
- To adopt the relevant information security measures, at the proposal of the **Information Security Committee**.
- To appoint **Vicomtech's** Data Protection Officer.

7.1.2. Information Security Committee

The **Information Security Committee** will be in charge of coordinating information security at Vicomtech.

It shall be made up of the following officers to be defined by the Steering Committee:

- ✓ Responsible for the information.
- ✓ Service Manager.
- ✓ Information Security Officer.
- ✓ System Manager.

- ✓ System Security Administrator.
- ✓ Integrated Management System Technician.

The **Information Security Committee** shall have the following functions:

- To develop **Vicomtech's** information security evolution strategy and promote continuous improvement.
- To coordinate the efforts of the different areas regarding information security, to ensure that efforts are consistent, aligned with the strategy decided on the matter, and to avoid duplication.
- To draft (and regularly review) the Information Security Policy for approval by the Steering Committee.
- To develop and approve training and qualification requirements for administrators, operators and users from an information security point of view.
- To identify non-compliance and propose sanctions
- To establish the level of acceptable risk, approve residual risks and communicate them to asset managers.
- To monitor the main residual risks assumed by **Vicomtech** and recommend possible actions regarding them.
- To monitor the performance of security incident management processes and recommend possible actions in this regard. In particular, to ensure the coordination of the different security areas in the management of information security incidents.
- To promote the performance of periodic security audits to verify compliance with the organisation's security obligations.
- To approve Vicomtech's information security improvement plans and, in particular, ensure the coordination of different plans that may be carried out in different areas.
- To prioritise security actions when resources are limited.
- To ensure that information security is taken into account in all projects from initial specification through to implementation.
- To resolve conflicts of responsibility that may arise between the different people in charge, raising those cases in which it does not have sufficient authority to decide.
- To report regularly on the state of information security to the Management Committee.

7.2. Roles: Functions and Responsibilities

The roles and responsibilities of each figure on the Information Security Committee shall be as follows:

7.2.1. Responsible for the Information

The person responsible for the Information shall have the ultimate responsibility for the use made of certain information and, therefore, for its protection, being ultimately liable for any error or negligence leading to an incident of confidentiality or integrity.

His/her functions are:

- To ensure the proper use of information and therefore its protection.
- To be ultimately responsible for any error or negligence leading to a confidentiality or integrity incident.
- To establish information security requirements.
- To determine the levels of information security.
- To formally approve the level of information security.

7.2.2. Service Manager

It has the power to establish the security requirements of the service, i.e. the power to determine the security levels of the services.

His/her functions are:

- To establish the security requirements of the service, including accessibility and availability requirements.
- To determine service security levels.
- To formally approve the security level of the service.

7.2.3. Information Security Officer

He/she will perform functions relating to the security of Vicomtech's information systems, including determining decisions to meet the security requirements of the information and services used at **Vicomtech**.

His/her functions are:

- To maintain the appropriate level of security of the information handled and the services provided by the systems.
- To carry out or promote the periodic audits required by the ENS to verify compliance with its requirements.

- To carry out the analysis and management of risks in the system.
- To manage training and awareness-raising in information security.
- To check that the existing security measures are adequate for the entity's needs.
- To review and complete all documentation related to the security of the system.
- To determine the category of the system, in collaboration with the person responsible for the system, for eventual approval by the Information Security Committee.
- To manage security incidents from notification to resolution, issuing periodic reports on the most relevant incidents to the Information Security Committee.

7.2.4. System Manager

This figure will be in charge of the operations of the system and whose functions are:

- To manage the Information System throughout its life cycle, from specification, installation to monitoring of its operation.
- Defining the criteria for use and the services available in the system.
- Defining the policies for user access to the system.
- To approve changes that affect the security of the system's mode of operation.
- To determine the authorised hardware and software configuration to be used in the System and approve major modifications to this configuration.
- To provide the person responsible for information security and/or the Security Committee with advice in determining the System Category.
- To approve changes to the current configuration of the Information System.
- To implement and control the specific security measures of the system.
- To establish contingency and emergency plans, conducting frequent drills to familiarise staff with them.
- To suspend the handling 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.

7.2.5. System Security Administrator

It shall administer the security functionalities determined by the above responsible persons, and its functions shall be:

- The implementation, management and maintenance of the security measures applicable to the Information System.

- The management, configuration and updating, where appropriate, of the hardware and software on which the security mechanisms and services of the Information System are based.
- Management of the authorisations granted to system users, in particular the privileges granted, including monitoring that the activity carried out in the system complies with what is authorised.
- The application of the Security Operating Procedures.
- Ensuring that established security controls are strictly adhered to.
- Ensuring that approved procedures for managing the information system are applied.
- Monitor hardware and software installations, modifications and upgrades to ensure that security is not compromised and that at all times they conform to the relevant authorisations.
- Monitor the security status of the system provided by the security event management tools and technical audit mechanisms implemented in the system.
- Report any security-related anomalies, compromises or vulnerabilities to the persons responsible for security and the system.
- Collaborate in the investigation and resolution of security incidents, from detection to resolution.

7.2.6. Integrated Management System Technician

His/her functions are:

- Review, complete and every documentation related to the security of the system.
- Support in the management of information security training and awareness.
- Support and supervise the investigation of security incidents from notification to resolution, issuing periodic reports on the most relevant incidents to the Information Security Committee.

7.2.7. Other possible roles

When the Information Security Committee deems it appropriate, it may involve other responsible persons in Vicomtech in its meetings in an advisory capacity.

7.2.7.1. Data Protection Officer

Person responsible for ensuring that personal data is processed and protected in accordance with the General Data Protection Regulation (GDPR EU 2016/679).

7.2.7.2. Security Officer

At Vicomtech, Classified Information that may affect national security is sometimes handled. The

Security Officer is the person in charge of knowing which of the centre's projects are classified under this category and what requirements they must meet.

8. Risk Analysis and Management

All systems subject to this Policy shall be subject to risk analysis and risk management, assessing the assets, threats and vulnerabilities to which they are exposed and proposing appropriate countermeasures to mitigate the risks.

The review of the risk analysis shall be carried out at the following intervals:

- At least once a year, to be approved by minutes of the Information Security Committee.
- When significant changes occur in the information and/or services provided.
- When a serious security incident occurs or serious vulnerabilities are detected.

9. Information Classification

Documented information shall be classified as: public, internal, restricted, confidential and classified, with appropriate use according to such classification.

- **Public Information**: Information that is intended for transmission by any means to third parties as part of business processes, which, if disclosed, would have no consequences for the organisation.
- **Internal use**: This is the type of information to which only Vicomtech staff should have access, i.e. its public circulation outside the organisation is not permitted. Its uncontrolled disclosure and/or loss could be an inconvenience for management, although it would not entail a financial loss or damage to its image.
- **Restricted Information**: Sensitive, internal area or project information to which only a department, project participants, a committee, etc. should have controlled access, but not the entire company. Disclosure or use of restricted information by unauthorised personnel could result in minor losses.
- **Confidential Information**: Sensitive information that can only be known and used by a small, authorised group of people to perform their duties. Disclosure of confidential information to unauthorised persons could result in serious material and reputational loss or legal liability for the organisation. This includes information containing personal data.
- **Classified Information:** It concerns information that may affect national security. Only

states or supranational organisations can determine what information is classified and to what degree. In Vicomtech's case, it affects a very low percentage of cases, so the detail of the protocol to be followed in these cases is dealt with under the coordination of Vicomtech's Security Officer. Any project leader or member of the project (even in the proposal development phase) who knows, believes, or has doubts that classified information may be handled should contact the project leader or member of the project (even in the proposal development phase).

10. Personal Data

The provisions of the GDPR and national legislation shall apply to this effect.

Vicomtech will only collect and process personal data when they are adequate, relevant and not excessive and when they are in relation to the scope and purposes for which they have been obtained. Likewise, Vicomtech will adopt the necessary technical and organisational measures to comply with the Data Protection regulations.

11. Awareness and Training

Maximum attention shall be paid to the awareness of the people involved in the security process and their hierarchical managers, so that neither lack of knowledge, nor lack of organisation and coordination, nor inadequate instructions, are sources of risk for the security of information systems.

All personnel involved with information and systems should be trained and informed of their security duties and obligations. Their actions should be monitored to verify that established security procedures are being followed.

Vicomtech staff will receive specific training and information necessary to ensure the security of the information technologies applicable to the systems and services provided.

An ongoing awareness programme will be established for all Vicomtech staff, in particular for new recruits.

The safety of the systems shall be monitored, reviewed and audited by qualified, dedicated and trained personnel at all stages of their life cycle: installation, maintenance, incident management and decommissioning.

12. Staff Duties

All personnel of the organisation and/or interested parties performing services of any kind contracted by Vicomtech, or otherwise provided under the control and/or direction of Vicomtech, are required to be familiar with and comply with this **Information Security Policy** and **the Information Security Regulations** documented in the Integrated Management System.

Staff shall use the security incident reporting procedures provided for this purpose, in the event that a potential incident is detected.

In Donostia-San Sebastian, 3rd April 2025

Signed by the General Management

72429210W JULIAN FLOREZ (R: G75051912)

Digitally signed by 72429210W JULIAN FLOREZ (R: G75051912)
Date: 2025.04.03 14:57:47 +02'00'

Date	Description	Authors	Revision	Version
28/03/2025	Creation of Vicomtech's Security Policy	Information Security Committee	-	1