T: +34 937 880 333
E: info@flexxible.com

TLP:CLEAR

Information Security and Privacy Policy

Index

1. Approval and entry into force

Text approved on April 14, 2026 by the management of Flexxible Information Technology, S.L., hereinafter referred to as the company.

This Information Security and Privacy Policy is effective from the date of approval and remains in force until it is replaced by a new Policy.

This text repeals the previous version, which was approved on September 15, 2025, by the company's management.

2. Organization objectives

The organization's main objective is to help companies harness the potential of end-user IT infrastructure and to have the confidence, knowledge, and power to use it in the way that best suits them.

The company relies on its information systems to achieve its strategic goals. Therefore, the diligent management and protection of these systems are a priority. Appropriate measures, based on risk assessment, must be applied to safeguard them from any incident—intentional or accidental—that could compromise the authenticity, traceability, integrity, or confidentiality of the information, or the availability of services.

The primary goal of information security and privacy is to ensure the continuous operation of the company, enabling it to fulfill its functions and deliver high-quality services. To achieve this, it is essential to adopt a preventive approach, actively monitor daily operations, and respond swiftly to any incident.

ICT systems are exposed to a dynamic threat landscape that could negatively impact the confidentiality, integrity, availability, intended use, and value of information and services. To defend effectively, an adaptable security and privacy strategy is required—one that adjusts to environmental changes. This means each department must implement the mandatory security measures of the National Security Framework (ENS), continuously monitor service delivery levels, analyse detected vulnerabilities, and have incident response plans in place to ensure business continuity.

It is imperative that ICT security be a fundamental pillar at every stage of a system's lifecycle: from its conception and development to its acquisition, operation, and eventual decommissioning. Security requirements and funding needs must be identified and incorporated into planning, as well as into requests for proposals and tender specifications for projects that handle personal data, involve the procurement of ICT services, or affect our information systems.

3. Scope

This policy applies to all information systems of the company, to the individuals who make up the organization, and to the company's ICT service providers or solution vendors.

4. Mission

Flexxible Information Technology, S.L. provides management, remediation, automation, user experience, and monitoring tools for physical or virtual workstations to its partner network and clients.

The security objectives that the company aims to ensure through this Policy are:

- Guarantee the confidentiality, integrity, and authenticity of information, as well as the continuity of service delivery.
- Implement security measures based on risk.
- Train and raise awareness among company members regarding information security.
- Implement security measures that enable access traceability and uphold, among others, the principle of least privilege, while reinforcing users' duty of confidentiality concerning the information they access in the course of their duties.
- Deploy and control physical security to ensure that information assets are located in secure areas, protected by access controls, and aligned with identified risks.
- Establish secure communication management through the necessary procedures, ensuring that information transmitted over communication networks is adequately protected.
- Control the acquisition, development, and maintenance of information systems throughout all phases of their lifecycle, ensuring security by default.
- Monitor compliance with security measures in service delivery, maintaining control over the acquisition and integration of new system components.
- Manage security incidents to ensure their proper detection, containment, mitigation, and resolution, adopting the necessary measures to prevent recurrence.
- Protect personal data by adopting technical and organizational measures based on the risks associated with processing, in accordance with data protection legislation.
- Continuously monitor the security management system, improving and correcting identified inefficiencies.

5. Guiding Principles of the Policy

- Strategic Scope: Information security must have the commitment and support of all levels of the company and should be coordinated and integrated coherently with other strategic initiatives.
- Comprehensive Security: Security is understood as a comprehensive process involving all technical, human, material, and organizational elements related to information systems, avoiding isolated actions or temporary fixes. Information security must be considered part of regular operations, present and applied from the initial design of ICT systems.
- Risk-Based Security Management: Managing security based on identified risks allows for maintaining a controlled environment, minimizing risks to acceptable levels. Security measures will be established according to the risks to which information and its systems are exposed and will be proportional and justified. Risks identified in the processing of personal data will also be considered.
- Prevention, Detection, Response, and Preservation: This involves implementing preventive actions against incidents, minimizing detected vulnerabilities, avoiding the materialization of threats, and, when they occur, responding swiftly to restore information or services, ensuring the secure preservation of information.
- Defense-in-Depth: The company's security strategy is designed and implemented in layers.
- Continuous Monitoring and Periodic Reassessment: The company implements mechanisms to detect and respond to anomalous activities or behaviors, as well as others that allow for continuous evaluation of the security status of assets. A continuous improvement process will also be in place to periodically review

and update security measures based on their effectiveness and the evolution of risks and protection systems.
- Security by Design and by Default: Systems must be designed and configured to ensure security by default. They will provide only the minimum functionality necessary to deliver the intended service.
- Separation of Duties: In accordance with this principle, the roles of the Security Officer and the System Owner must be clearly differentiated.

6. Certification Scope

The information systems that support the Flexxible Odin Service in service mode (provided in both public and private cloud), with reference to the current System Statement of Applicability and System Categorization.

7.Regulatory framework

- 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, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights.
- Law 34/2002 of 11 July on Services of the Information Society and Electronic Commerce.
- Royal Decree 311/2022 of 3 May, regulating the National Security Framework.
- Royal Decree 1777/2004 of 30 July, approving the Corporate Tax Regulation.
- Royal Legislative Decree 2/2015 of 23 October, approving the revised text of the Workers' Statute Law.
- Organic Law 10/1995 of 23 November, Criminal Code.
- Law 25/2007 of 18 October, on the retention of data relating to electronic communications and public communications networks.
- Law 6/2020 of 11 November, regulating certain aspects of trusted electronic services (repealing Law 59/2003).
- Royal Legislative Decree 1/1996 of 12 April, approving the revised text of the Intellectual Property Law, regularizing, clarifying and harmonizing the legal provisions in force on the matter.
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.

8. Responsibilities and organization of the Security and Privacy of the information

a. STIC Committee (ICT Security)

ICT activities are coordinated through the STIC committee. This committee is composed of technical personnel from different departments for decision-making.

The ICT security committee will be formed by:

POSITION
Manager (*)
Responsible for the information (*)
Service Manager (*)
Security Manager (**)
System Manager (**)

(*) These functions may be performed by the same person.
(**) The person responsible for Security will be different from the person responsible for the system.

The Director chairs the STIC Committee and is primarily responsible for:

- Use the casting vote to agree on the appropriate decisions when there is no agreement within the team.
- Implement, maintain and improve the Information Security and Privacy Management System.
- Allocate the necessary resources and approve the budget.
- Assign and communicate the roles, specifically of the owners of information security and privacy risks and quality risks.

Other roles of great relevance within the Information Security and Privacy system are:

POSITION	RESPONSIBILITIES
ICT Systems Administrator	Responsible for the implementation, configuration and maintenance of ICT-related security and privacy services.
ICT systems operators	Continuity Team. They are responsible for the daily operation of the Security and Privacy services related to ICT.

b. Roles and responsibilities

STIC Committee

- Establish, review and approve the scope of the Information Security and Privacy Management System, in addition to the Information Security and Privacy policy.
- Ensure that the Information Security and Privacy policies, processes, procedures and laws and regulations reflect business requirements and are aligned with the requirements of internal and external stakeholders.
- In addition to establishing, reviewing and approving the ISMS objectives and checking whether they are effectively implemented and maintained.
- Monitor significant changes in Information Security and Privacy.
- Review Information Security and Privacy incidents and agree on necessary actions, if appropriate.
- Approve major initiatives to maintain Information Security and Privacy and the established quality level.
- Conduct Management Reviews at planned intervals.
- Ensure that personnel are aware of the importance of complying with security and privacy requirements, legal and regulatory requirements, contractual obligations, quality requirements, quality levels and service level agreements.

Responsible for Information

- It has the authority to establish the requirements, in terms of security and privacy, of the information managed. If this information includes personal data, the requirements derived from the corresponding legislation on data protection must also be considered.
- Determines the levels of security and privacy of the information.

Responsible for the Service

- It has the authority to establish the requirements, in terms of Security and Privacy, of the services provided.
- Determines the levels of security and privacy of the service.

Security Manager

Responsible for the definition, coordination and verification of compliance with the requirements of Security and Privacy of information defined according to the objectives.

The functions of the Head of Information Security are:

- Coordinate and control the measures of Security and Privacy of information and data protection.
- Supervise the implementation, maintain, control and verify compliance with:
    - The Information Security and Privacy strategy defined by the Security and Privacy Committee.
    - The rules and procedures contained in the Information Security and Privacy Policy.
    - Supervise the Security and Privacy incidents.
    - Disseminate among the company's personnel the rules and procedures contained in the Information Security and Privacy management system, as well as the functions and obligations in the field of Information Security and Privacy.
    - Supervise and collaborate in the internal or external audits necessary to verify the degree of compliance with the Security and Privacy Policy, development regulations and applicable laws on personal data protection and Information Security and Privacy.
- Advise on Security and Privacy of information to the different operational areas of the company.
- Approve the system categorization.

System Manager

The system manager, by himself or through his own or contracted resources, is in charge of developing the specific way of implementing Security and Privacy in the system and of supervising the daily operation of the system, being able to delegate it to administrators or operators under his responsibility.

The system manager shall take the necessary corrective measures derived from the security and privacy audit reports once they have been analyzed by the security manager and the latter has presented his conclusions to the system manager.

The system manager shall be different from the security manager, and there shall be no hierarchical dependence of any kind between the two profiles.

PII Treatment Organization Point of Contact and Privacy Officer

The Company has designated a specific point of contact for our customers regarding processing Personally Identifiable Information (PII).

The designated point of contact will be available for:

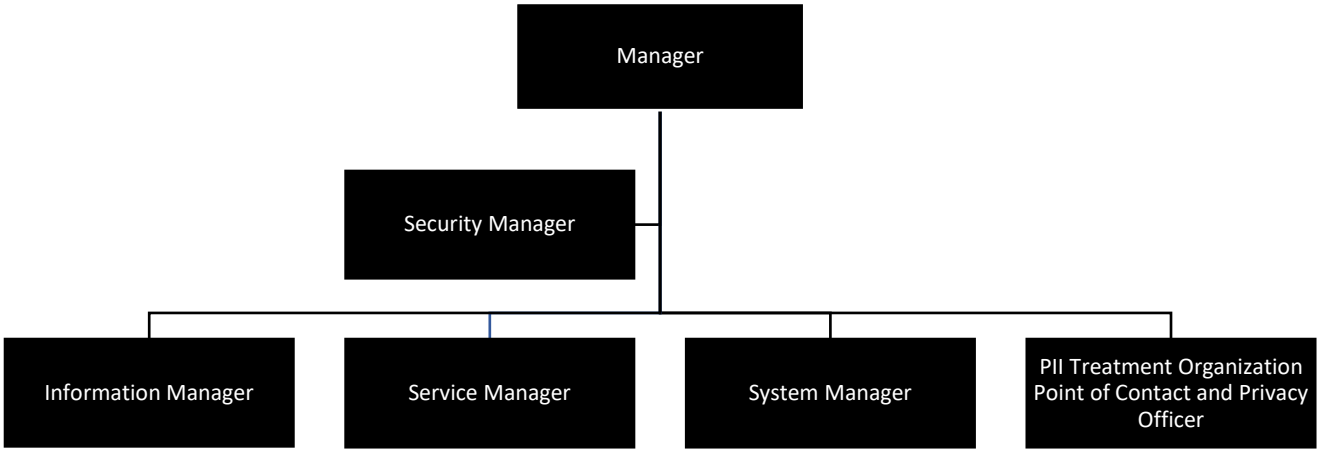
- Answering inquiries,
- Assist and
- Facilitate communication between our customers and the team responsible for treating PII in our organization.

In addition, we have designated the person responsible for developing, implementing, maintaining, and monitoring our organization-wide privacy and governance program to ensure compliance with all applicable laws and regulations regarding the treatment of PII.

It will perform the following responsibilities:

- Be independent and report directly to the appropriate management level of the organization to ensure effective privacy risk management.
- Participate in the management of all issues related to the treatment of PII.
- Be an expert in data protection legislation, regulation, and practice.
- Act as a point of contact for the supervisory authorities.
- Inform senior management and employees of the organization of their obligations concerning treating PII.
- Provide advice concerning privacy impact assessments conducted by the organization.

Role dependencies



9. Designation and renewal of security and privacy roles

Management is ultimately responsible for designating the different Security and Privacy roles. This designation will be formally made with the approval of this policy. The original signed by Management will be filed by the Security Manager.

The established organization chart will reflect these designations.

The designation will be renewed in the following cases:

- Medium- or long-term leave of designated personnel.
- Staff leaves the company indefinitely.
- Lack of competencies
- Management criteria based on HR management and strategic reasons.

10. Conflict Resolution

In the event of conflicts between the different responsible parties, the Information Security Committee may resolve the discrepancies.

11. Risk management

Assets subject to this Security and Privacy Policy must undergo a risk analysis, assessing potential threats and identifying the risks to which they may be exposed. This analysis shall be repeated:

- regularly, at least once a year.
- when changes occur in the information handled.
- when changes occur in the services provided.
- when a serious security incident occurs.
- when serious vulnerabilities are reported.
- when modifications are made to the data protection risk analysis or impact assessments.

To harmonize risk analyses, the Information Security Committee shall establish a reference assessment for the different types of information handled and the various services provided. The Committee shall promote the availability of resources to meet the security and privacy needs of the different systems, encouraging horizontal investments.

Data protection risks shall be taken into account, with input from the Data Protection Officer, and risk treatment plans shall be coordinated.

12. Resources

For the effective application of the Information Security and Privacy Policy in the company, the Management will provide the necessary resources for its proper development, both in the activities of implementation and operation and improvement of said policy and of the information Security and Privacy controls established at any given time.

The protection of the information assets of the company and its customers is vital for the correct alignment with the business objectives. To this end, an Information Security and Privacy Management System has been

established that implements all the processes and controls necessary to establish the way in which information assets are protected.

The Information Security and Privacy Management System is continuously updated and improved to meet the needs of the business, customers and stakeholders, new objectives are established periodically, and business processes are regularly evaluated.

13. Personal Data

The company processes personal data as described in the Record of Processing Activities. The company must assess the risks related to the personal data processed and propose an action plan to correct any risks that exceed the authorized threshold.

The risk analysis shall be periodically reassessed, with the advice and supervision of the Data Protection Officer, and in any case, when high-risk processing is detected, an impact assessment must be carried out if applicable. The implementation of the risk treatment plan shall be coordinated with the National Security Framework (ENS), as well as with other security procedures or standards and the obligations related to data protection, especially regarding service provider control and response to incidents and/or personal data breaches.

14. Development of the Information Security and Privacy Policy

This Information Security and Privacy Policy complements the company's Integrated Policy on Quality and Environmental Management.

Its development will be carried out through specific security regulations that will address various technical, organizational, and procedural aspects. These regulations will be available to all members of the organization who need to be aware of them, especially those who use, operate, or manage information and communication systems.

The regulations will be accessible through various means, including the corporate intranet, thus ensuring their dissemination and consultation.

Additionally, personnel involved in the use or management of information systems must receive specific training in information security. Providers will also be evaluated and must have properly qualified and trained personnel according to the services they provide.

15. Staff Obligations

All company members are required to know and comply with this Information Security Policy and the rules, procedures, or guidelines that develop it. It is the responsibility of the company, through the Information

Security Committee and the HR department, to provide the necessary means to ensure that the information reaches those affected.

All company members will receive information security awareness training at least once a year. A continuous awareness program will be established to reach all company members, particularly new hires.

Individuals responsible for the use, operation, or administration of ICT systems will receive training for the secure handling of systems as needed to perform their duties. This training will be mandatory before assuming any responsibility, whether it is a first assignment or a change in position or responsibilities.

16. Third Parties / Service Providers / Solution Vendors

When the company provides services to other entities or handles information from others, they will be made aware of this Information Security Policy, without prejudice to compliance with data protection regulations if acting as a data processor in the provision of said services. Channels will be established for reporting and coordination between the respective Security Committees and procedures for responding to security incidents. Additionally, the Security Officer (or delegated person) will act as the Point of Contact (POC).

When the company uses third-party services or transfers information to third parties, they will be made aware of this Security Policy and the Security Regulations relevant to those services or information, without prejudice to other data protection obligations. In contracting service providers or acquiring products, the obligation of the contractor to comply with the National Security Framework (ENS) will be considered.

In acquiring cloud asset usage rights, the requirements established in the security measures of Annex II and the development guidelines will be taken into account.

Such third parties will be subject to the obligations established in the aforementioned regulations and may develop their own operational procedures to meet them, allowing the company to supervise or request evidence of compliance, including second- or third-party audits. Specific procedures for reporting and resolving incidents will be established and must be channeled through the third party's POC and, when personal data is affected, through the Data Protection Officer.

Third parties must ensure that their personnel are adequately trained in security matters, at least to the same level as established in this Policy or as specifically required in the contract.

If any aspect of the Policy cannot be met by a third party as required above, the Security Officer will issue a report detailing the risks involved and how they will be addressed. This report must be approved by the information and service owners before the start of the contracting process or, if applicable, the award. The report will be forwarded to the company representative who must authorize the continuation of the third-party contracting process, assuming the identified risks.

When the company acquires, develops, or implements an Artificial Intelligence system, in addition to complying with the applicable regulations, it must have a report from the Security Officer, who will consult the Information and Service Owners and, when necessary, the System Owner. The Data Protection Officer must also provide their opinion.

17. Security Incident Management

The company will have a procedure for the agile management of security events and incidents that pose a threat to information and services.

This procedure will be integrated with others related to security incidents from sectoral regulations, such as personal data protection or any other affecting the organization, to coordinate the response from different perspectives and communicate with the relevant supervisory bodies without undue delay and, when necessary, with law enforcement or judicial authorities.

18. Information Security and Privacy Management System

The Information Security and Privacy Management System is reviewed annually or when a significant change occurs in the business.

The implemented, operated, and improved Information Security and Privacy Management System, based on the National Security and Privacy Framework (CCN), ensures:

- That it establishes and maintains the context, determining the needs and expectations of interested parties.
- That roles, responsibilities, and authorities are assigned.
- That objectives for the Information Security and Privacy Management System are established, aligned with strategic goals.
- That indicators are established to measure control performance, and are analyzed and evaluated periodically.
- That a risk criterion is established for identifying, analyzing, evaluating, and treating risks.
- That all personnel receive training and awareness on Information Security and Privacy and the implemented policies (physical and logical access control, physical security, malicious code protection, backups, information classification, information handling, continuity, etc.).
- That the Management System operates based on approved documented information, policies, processes, procedures, etc.
- That compliance is verified through external audits, monitoring of objectives and indicators, and management reviews.
- That non-conformities and complaints are corrected through the implementation of corrective actions and evaluation of their results.
- That continuous improvement of the Information Security and Privacy Management System is carried out.

19. Strategic Information Security and Privacy Policy

The company has implemented an information security and privacy management system whose scope is:

The information systems that support the Flexxible Odin Service in Service mode (provision in both public and private cloud), with reference to the current System Applicability Statement and System Categorization.

Dimension	Availability	Authenticity	Confidentiality	Integrity	Traceability	Category
Level assigned	High	Medium	High	High	Medium	HIGH

Points to be taken into account:

- Preserving the **confidentiality** of the information and preventing its disclosure and access by unauthorized persons.
- Maintaining the **integrity** of the information, ensuring its accuracy and avoiding its deterioration.
- Ensuring the **availability** of information in all media and whenever necessary.
- **Traceability** of records.
- And the **authenticity** of the data.

Information Security and Privacy must be flexible, effective and support the company's business model, therefore, the Management is committed to develop, implement, maintain and continuously improve its Information Security and Privacy Management System with the aim of continuous improvement in the way we provide our services and the way we treat our customers' information.

Therefore, we establish the following guidelines:

- Establishment of objectives in relation to Information Security and Privacy.
- Compliance with legal requirements and other requirements we may subscribe to.
- Conduct training and awareness-raising activities on Information Security and Privacy processes for all personnel.
- Development of risk analysis, management and treatment of information assets.
- Establish all actions required to mitigate or eliminate the risks detected.
- Establish the responsibility of employees in relation to the reporting of security and privacy incidents.
- Preserve the confidentiality, integrity and availability of information assets in compliance with this policy.
- Compliance by all personnel with the policies and procedures of the Information Security and Privacy Management System.

The Management assigns responsibilities and authority to the Security Manager on the maintenance of this policy, providing advice and guidance for its implementation and corrections in case of deviations in its compliance, as well as in the management of policies, procedures and activities of the ISMS.

This information security and privacy policy will always be aligned with the company's general policies.

20. Considerations in Defining the Information Security and Privacy Policy for Cloud Computing

We acknowledge the complexity and challenges associated with information security and privacy in the cloud computing environment. In defining our information security and privacy policy for cloud computing, we have taken the following considerations into account:

- We recognize that information stored in the cloud computing environment may be subject to access and management by the cloud service provider. Therefore, we are committed to implementing appropriate security and privacy measures to protect our confidential information in this environment.
- We understand that our assets, such as applications and programs, may reside in the cloud computing environment. We are committed to implementing adequate security and privacy controls to protect these assets against internal and external threats.
- We understand that processes may run in a virtualized multi-tenant cloud service. We are committed to implementing security and privacy measures to ensure proper segregation of data and resources among tenants in the cloud environment.
- We consider the different users of the cloud service and the context in which they use the service. We are committed to implementing strong access and authentication controls to protect our information from unauthorized access.
- We recognize that cloud service administrators from the provider may have privileged access to our data. We are committed to establishing procedures and monitoring controls to manage these privileges and prevent potential abuse appropriately.
- We consider the geographic locations of the cloud service provider's organization and the countries where the provider may store our data, even temporarily. We are committed to evaluating and addressing the risks associated with data storage in specific geographic locations in accordance with applicable data protection regulations.

This statement of considerations in defining the information security and privacy policy for cloud computing will be communicated to all employees and relevant stakeholders within our organization.

21. Considerations in Defining the Information Security and Privacy Policy for Compliance with Legislation and Contractual Terms on PII Protection in Public Cloud

We recognize the critical importance of complying with legislation on the protection of personally identifiable information (PII) and the contractual terms agreed with our cloud service clients. We are committed to ensuring the proper security and protection of sensitive information.

In line with this commitment, we affirm that our information security and privacy policies are complemented by an official statement expressing our support and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed with our cloud service clients.

We understand the importance of clearly assigning responsibilities among ourselves as public cloud PII processors, subcontractors, and cloud service clients. We acknowledge that the assignment of responsibilities may vary depending on the type of cloud service provided.

Therefore, we are committed to including explicit responsibility provisions in all our contractual agreements with cloud service clients. These provisions will be specific to the type of cloud service in question, ensuring that the appropriate security controls for each layer of the cloud architecture are properly addressed.

We recognize that the type of cloud service may influence the assignment of responsibilities, especially regarding application layer controls. We are committed to adapting our policies and contractual agreements to reflect these differences and ensure clarity and transparency regarding the responsibilities of all parties.

This statement of considerations in defining the information security and privacy policy for cloud computing will be communicated to all employees and relevant stakeholders within our organization.

22. Statement of Commitment and Support for Compliance with Legislation and Contractual Terms on PII Protection

We recognize the importance and seriousness of complying with applicable legislation and regulations that protect personally identifiable information (PII) in all our operations and activities. We are committed to ensuring the integrity, confidentiality, and security of the PII we handle.

As part of our commitment, we produce and maintain an official statement expressing our support and commitment to achieving compliance with applicable PII protection legislation and regulations. This statement will be reviewed and updated periodically to reflect any changes in legislation or our contractual obligations with partners, subcontractors, and relevant third parties such as clients and providers.

We understand that assigning responsibilities between our organization and all parties handling PII is essential. Therefore, we are committed to including explicit provisions on responsibilities in all contractual agreements with our partners, subcontractors, and relevant third parties. These provisions will ensure a clear understanding of each party's responsibilities and obligations regarding the proper protection and management of PII.

We acknowledge that, as an organization dealing with PII—whether as a data controller or processor—it is essential to consider applicable PII protection legislation and regulations while developing and maintaining our information security and privacy policies. We are committed to integrating these into our policies and procedures related to information security and privacy.

This statement of commitment and support will be communicated to all employees and relevant stakeholders within our organization.

23. Security Category

The required Security Category is **HIGH**, within the framework established in Article 40 and the general criteria prescribed in Annex I of the National Security Framework (ENS). Some of the criteria determining this level include the fact that the process is fully defined. The process catalog is kept up to date and ensures consistency in actions across different parts of the organization.

In addition, established regulations and procedures exist to respond to any Security and Privacy incident, and these are regularly updated and maintained. Likewise, there is strong coordination between departments and the projects carried out.

The STIC Committee considers the possibility of modifying the required Security level.

The principles of the Information Security and Privacy Policy are embraced and promoted by Management, which provides the necessary means and equips employees with sufficient resources to ensure compliance, making them publicly known through this Information Security and Privacy Policy.

24. Minimum Security and Privacy Requirements

This Security and Privacy Policy has been established in accordance with the following minimum requirements:

a) Organization and implementation of the Security and Privacy process:

- Security and Privacy Structure: A Security Committee will be established to oversee the implementation and compliance with the Security and Privacy Policy.
- Roles and Responsibilities: Clearly define roles and responsibilities for all employees regarding information Security and Privacy.
- Documentation: Maintain up-to-date documentation on Security and Privacy policies, procedures, and standards.

b) Risk analysis and management:

- Risk Assessment: Conduct periodic risk assessments to identify, evaluate, and mitigate risks associated with information assets.
- Risk Mitigation: Implement appropriate controls to manage identified risks.
- Continuous Review: Regularly review and update risk analysis and mitigation measures.

c) Personnel management:

- Staff Selection: Conduct background checks and security evaluations for all employees.
- Training: Provide ongoing training in information Security and Privacy to ensure all staff are aware of relevant policies and procedures.
- Security and Privacy Awareness: Promote a culture of Security and Privacy through awareness and training programs.

d) Professionalism:

- Code of Conduct: Promote professional and ethical behavior in all activities related to information Security and Privacy.
- Professional Development: Encourage continuous improvement and updating of skills and knowledge for Security and Privacy personnel.

e) Authorization and access control:

- Access Control: Implement role-based access control systems to ensure users only access data and systems necessary for their duties.
- Access Audits: Conduct regular audits of access permissions and revoke unnecessary access.
- Authentication: Use strong and multi-factor authentication mechanisms.

f) Facility protection:

- Physical Security: Implement physical security measures such as access controls, surveillance cameras, and alarm systems to protect facilities handling information assets.
- Restricted Access: Limit access to critical areas to authorized personnel only.

g) Acquisition of Security products and contracting of Security services:

- Security and Privacy Criteria: Establish Security and Privacy criteria for acquiring products and services.
- Supplier Evaluation: Conduct Security and Privacy evaluations of suppliers and contract only those meeting required standards.

h) Least privilege:

- Principle of Least Privilege: Apply the principle of least privilege, ensuring users and systems have only the minimum permissions necessary.
- Privilege Review: Periodically review access privileges and adjust as needed.

i) System integrity and updates:

- System Integrity: Implement procedures to ensure the integrity of systems and data.
- Software Updates: Perform regular software updates and apply Security and Privacy patches to protect against known vulnerabilities.

j) Protection of stored and transmitted information:

- Encryption: Use encryption techniques to protect information both at rest and in transit.
- Access Controls: Implement authentication and access control mechanisms to ensure only authorized users can access information.

k) Prevention regarding interconnected information systems:

- Connection Control: Implement Security and Privacy controls to manage and monitor connections with other information systems.
- Risk Assessment: Evaluate and mitigate risks associated with system interconnections.

l) Activity logging and malicious code detection:

- Activity Logging: Maintain detailed logs of all system activities and conduct regular audits.
- Malware Detection: Implement tools for detecting and preventing malicious code (malware).

m) Security and Privacy incidents:

- Incident Management: Establish procedures for managing Security and Privacy incidents, including identification, analysis, response, and reporting.
- Incident Drills: Conduct regular exercises and simulations to ensure preparedness for incidents.

n) Business continuity:

- Continuity Plans: Develop and maintain business continuity and disaster recovery plans.
- Regular Testing: Conduct regular tests of these plans to ensure their effectiveness.

ñ) Continuous improvement of the Security and Privacy process:

- Continuous Improvement Cycle: Implement a continuous improvement cycle (Plan-Do-Check-Act) to evaluate and enhance Security and Privacy policies and procedures.
- Periodic Reviews: Conduct periodic reviews of the Security and Privacy Policy to ensure it remains current and relevant.

25. Security in Cloud Services

Cloud services must be designed and implemented considering basic information security requirements, including protection against unauthorized access and encryption of data in transit and at rest.

Risks associated with authorized access will be evaluated and mitigated, ensuring that credentials and permissions are managed according to the principle of least privilege.

Isolation between clients in multi-tenant and virtualized environments will be ensured through technical controls that prevent data leakage and unauthorized access.

Cloud service provider personnel will have access to client assets only when strictly necessary, under continuous control and audit procedures.

Robust authentication will be implemented for administrative access to cloud services, including multi-factor authentication and session management mechanisms.

During change management processes in cloud services, clients will be informed in advance of modifications that may affect system security or availability.

Specific security measures will be adopted for virtualization, ensuring that virtual environments are protected against hypervisor attacks and other vulnerabilities.

Access to client data in the cloud will be restricted and protected through encryption techniques and role-based access control.

A secure lifecycle for cloud service client accounts will be defined, covering account creation, modification, suspension, and deletion.

Communication protocols will be established in case of security incidents, including timely notification to clients and information exchange with relevant authorities to support forensic investigations.

26. Policy approval and entry into force

Modifications to this Policy that involve changes or adaptations due to inefficiencies shall be made by the Information Security Committee, which must also review it annually.

If the changes involve a substantial modification of the principles or responsibilities of the policy, the Security Committee shall propose the changes, which must be approved, where appropriate, by the person or body with the appropriate authority.

A complete replacement of the Policy shall be initiated by the Information Security Committee and ratified by the person or body with the appropriate authority. Once approved, it will be properly communicated to the relevant stakeholders through the same channels used for its dissemination.

Management

April 14th, 2026