GLOBAL CORPORATE POLICY

Information Security Policy

Effective date	12 12 2023
Approved use	Approved for external dissemination

Content

1. Purpose

This Corporate Policy establishes guidelines and basic principles relating to the mission, scope and objectives of the Information Security (IS) function in ALMIRALL.

The objectives of this Corporate Policy Global Information Security are:

1. To define Almirall's Governance structure to ensure the protection of Information Security's key dimensions (defined in "Scope").
2. To define guidelines for risk management on Information Security.

2. Scope

This Corporate Policy applies to all Almirall organizations, areas, processes and systems relevant to Information Security risks including Business Continuity in the context of Information Security.

Risks managed by IS are those affecting the key dimensions: confidentiality, integrity, availability of information and processes.

People, Processes and Technology (Information Technology as well as Operational Technology) are under the scope of Information Security.

3. Policy elements

Principles

1. Information Security responsibility spans from the IS strategy definition to IS operations.
2. Information Security must have regular links to the MB members and Senior Leadership to facilitate that the IS strategy is aligned with business objectives and strategy.
3. Information Security must identify and assess risks with strong independence with regards to those functions responsible for implementing the recommended risk mitigation controls.
4. Risks are owned by the corresponding Business Directions. Key decisions regarding risk mitigation and risk acceptance must be made by the Business Directions with the support of Information Security, or Information Technology if needed.
5. Collaboration with expert third parties and associations is a crucial part of Information Security to keep updated in a constantly evolving threat environment.
6. Security measures and controls should be implemented following a risk-oriented approach. This applies to the entire life cycle of the information and systems, both in the IT Infrastructure and the Operational Technology in Manufacturing or R&D plants.

7. Information assets should be classified in terms of confidentiality, availability and traceability, also ensuring that they are only accessible to authorised users, according to the level assigned.
8. The information processed and exchanged with natural or legal persons, regardless of its owner, must comply with the requirements in relation to Almirall's information security, as well as current legislation applicable, including Privacy regulations such as GDPR.
9. All employees with access to Almirall information, should be trained on a regular basis, and made aware of risks.
10. Risks and maturity in Security processes must be regularly assessed and reported based on recognized standards. See chapter "Information Security Management System".

Risk Management

IS will establish a defined, repeatable and effective methodology for Risk Management, aligned with standards and consistent with the Enterprise Risk Management guidelines set out by Internal Audit.

Information Security Management System (ISMS)

The ISMS acts as a global framework to ensure Almirall application of recognised best practices in IS.

Almirall's Information Security Management System is defined in the Information Security SOP.

Confidentiality levels in information management

Five (5) levels have been defined to classify the information confidentiality in Almirall (see SOP).

The owner of each information asset is responsible for appropriately labelling the information, so that the receiver of the information is aware of the confidentiality level, and so that information protection measures that are proportionate to the confidentiality level, that is, to the information's value.

Non-compliance management / Exceptions Management

The purpose of the non-compliance (Exceptions Management) procedure defined in the SOP is to ensure proper internal control, visibility on risk situations, and corresponding risk mitiagation measures.

Exceptions to security measures and controls, when above risk thresholds defined by IS, must be documented, evaluated, and formally approved.

All users are responsible for notifying IS of any detected non-compliance.

Information Security incident management

Information Security Incidents will be managed based on the **Protocol for Information Security Incidents** and derived technical procedures.

Involvement and decision-making at MB level is key in the event of severe information

security incidents.

IS will manage contact details of all MB members in the event of such situations.

4. Governance

Corporate Policy Sponsor: General Counsel		
Corporate Policy Owner: Information Security Director		
Overview of changes	Version	Effective Date
New Policy	1.0	12 December 2023

All employees are required to report any suspected violation of the Corporate Policies in accordance with Almirall Code of Ethics and other internal guidelines. Suspected violations can be reported to your direct manager, People & Culture, your local Compliance or Legal representative or through the SpeakUp! channel (include link)

5. Appendix 1

Terms of Use of Almirall's Equipment and Information Systems

Name and surname(s): **Date: / /**

National ID No. (DNI)/Tax ID no. (NIF):

(To be signed at the end of the document)

These Terms of Use are formally included in the Global Corporate Information Security Policy and its Standard Operating Procedures and are therefore mandatory for all Almirall Employees.

The computer systems, corporate network, devices, software, applications, and all the information processed by them are property of ALMIRALL.

These Terms of Use are provided to ensure the proper use of the equipment, systems, network and information made available to ALMIRALL's Employees (hereinafter, the "Employee" or the "User"), as well as to ensure the protection of ALMIRALL's technological assets and information.

1 RULES FOR THE PROPER USE OF IT TOOLS

The Employee must make proper use of the equipment, network and systems that ALMIRALL provides in accordance with his/her job position.

The Employee is aware and accepts that his/her activity and information may be included in monitoring operations carried out by ALMIRALL's authorised personnel, including without limitation any information encrypted or protected by private user sessions (technically known as "https" sessions) set up from ALMIRALL's systems, as described in Section B of these Terms of Use. Under no circumstance shall the Employee have an expectation of privacy with respect to the use of ALMIRALL's equipment and systems.

The protection of information is essential for ALMIRALL. Consequently, the Employee must report to the Service Desk, as soon as he/she becomes aware of any incident that occurs on the information systems to which he/she has access, (i.e. any irregularity that damages or could damage the security of the information in ALMIRALL).

In any case, the Employee is responsible for the observance and the strictest compliance of the following **Confidentiality**, **Integrity**, **Traceability** and **Availability** requirements, as well as the **Additional Security Measures** set out in these Terms of Use:

Confidentiality

1. The protection of information based on the confidentiality levels defined by ALMIRALL Information Security is a responsibility of each Employee. The use of information shall always be subject to the levels of confidentiality defined for each type of information (secret, confidential, restricted, internal, public). ALMIRALL's business secrets, including but not limited to procedures, methods and any other material that form part of ALMIRALL's R&D, industrial or commercial strategy, as well as ALMIRALL's financial information and any Personal Data, shall be considered as "Secret" or "Confidential" information.
2. In the absence of contractual arrangements between ALMIRALL and a Service Provider of Artificial Intelligence (AI) solutions, the AI shall be deemed to be public and therefore any information entered into the AI may ultimately be disclosed without the possibility of ALMIRALL exercising any control. ALMIRALL information classified as "**Confidential**", "**Secret**", "**Restricted Use**" or "**For Internal Use**" must not be used in public AI solutions. This will be considered a breach of the Global Corporate Information Security Policy.
3. The Employee must maintain the strictest confidentiality and must not disclose or directly use any Personal Data, documents, methodologies, keys, analytics, programs, or any other information they come across during its employment relationship with ALMIRALL, either personally or through third parties, regardless of whether it is in written or electronic form. This obligation shall remain in effect even after the termination of the employment relationship with ALMIRALL.
4. The Employee is responsible for ensuring that ALMIRALL's information is always stored in the location on the network specifically designated, regardless of the device (mobile phone, tablet, laptop or desktop computer) from which the Employee has access to the information. Extractions from physical media (i.e. using USB keys, external drives) must be expressly authorised by the relevant Head of Department and only using encrypted external devices. Storage of ALMIRALL information outside of the ALMIRALL network must also obtain the prior explicit approval from ALMIRALL Information Security.
5. The Employee must use the ALMIRALL email account for registration on professional external websites. Notwithstanding the above, it is forbidden to use the same password used to access to the ALMIRALL network.

6. Passwords assigned to the Employee are secret, personal, and non-transferable, and cannot be shared. The Employee is responsible for the consequences of the disclosure or loss of his/her password.
7. The Employee is responsible for ensuring that ALMIRALL's information is disclosed or exchanged only to individuals duly authorised to know or process such information. This includes all technical and non-technical means of dissemination or extraction, digital collaboration spaces or social media networks.
8. The Employee must not read, delete, copy or modify e-mail messages or files of other Employees, unless explicitly authorised to do so.
9. The Employee can only access the areas to which he/she has been authorized in due form. Such authorisations of access shall be granted by the relevant Head of Department in each case.
10. Personal Data can only be made available to third parties using the tools recommended by ALMIRALL Information Security.
11. Before disclosing Personal Data or other information to third parties, the Employee must ensure (i) there is a legitimate business reason, (ii) that adequate contractual guarantees and safeguards are in place and, (iii) the disclosure is made on a need-to-know basis only.
12. The use of non-Corporate instant messaging tools to exchange Confidential or Secret information is prohibited.
13. It is prohibited to store ALMIRALL's information in third-party cloud technologies or systems unless previously approved by ALMIRALL Information Security. Exceptions to this prohibition shall be managed through the Service Desk and shall require a risk assessment.
14. When information becomes obsolete or unnecessary, it must be securely destroyed, including the destruction of any external storage devices, as required.

Integrity

1. It is prohibited to destroy, alter, render unusable, or in any other way damage ALMIRALL's data, information, computer programmes or electronic documents.
2. It is prohibited to import, download from the Internet, reproduce, use, or distribute computer programmes not explicitly authorised by ALMIRALL. Works or materials subject to third parties' copyright shall require a prior license or contractual authorization from the relevant third-party before its use.

3. Connecting external devices (e.g. USB storage devices) to ALMIRALL's equipment in general is not permitted unless such devices originate from known sources.
4. It is prohibited to connect USB storage devices not previously validated by ALMIRALL to any manufacturing equipment (ALMIRALL Production Sites).
5. Remote connections to ALMIRALL network (e.g., a service provider interacting with industrial systems) is only allowed through the communication channels explicitly authorised by ALMIRALL Information Security.
6. When in doubt about the validity of a message, email, phone call, or the identity of the sender, the Employee must immediately report it to the Service Desk for verification. Opening attachments or clicking on URLs is only allowed if they originate from trustworthy sources and do not exhibit any signs of being illegitimate.

Traceability

1. It is strictly prohibited to remove, disable, or bypass ALMIRALL's security settings on systems and equipment. Situations where the security settings need to be modified and/or lifted must be duly justified and submitted to the IT Department. Such situations shall always be subject to risk assessment by ALMIRALL Information Security in any case.
2. The use of the ALMIRALL ID and password provided to the Employee implies the acknowledgment and acceptance of the recordings (technically referred as “system logs”) generated in each system as evidence of the activity performed. System logs recorded under the Employee’s ALMIRALL ID shall be presumed as carried out by the respective Employee.
3. It is strictly prohibited to manipulate or falsify system logs.

Availability

1. The Employee must ensure that his/her activity does not prevent or jeopardise other users from accessing the Corporate network or the information stored in ALMIRALL's systems.
2. It is strictly prohibited to engage in activities that excessively consume computer resources, that cause damage, interruptions, or errors in the systems, including without limitation cryptocurrency mining and peer-to-peer file sharing.
3. It is prohibited to delete programs or to intentionally introduce any program that may damage the security of ALMIRALL.

Additional Security Measures:

The Employee must observe and comply with the following Additional Security Measures when using equipment, systems, network, and information:

(i) **Mobile Devices**:

1. The Employee must ensure that the ALMIRALL mobile devices are always equipped with the most up-to-date software and supported apps, unless specifically instructed otherwise by ALMIRALL.
2. The Employee is prohibited from storing any ALMIRALL's information or Personal Data outside of the authorized email app, web browser, or any other app approved for connecting to ALMIRALL's systems.
3. Should an Employee edit ALMIRALL documents on a mobile device, such documents must be deleted from the internal memory of the device after sending them via email.
4. The Employee can make a personal use of mobile devices provided due security and privacy settings are arranged to avoid damaging ALMIRALL's security.
5. The Employee shall report immediately to the Service Desk -or directly to ALMIRALL Information Security- an incident involving a mobile device lost, stolen, or suspected to be involved in a security incident.
6. Actions that damage or could damage the mobile device's software (i.e. jailbreaking Apple iOS devices or rooting Android devices) or that bypass ALMIRALL's configuration are strictly prohibited.
7. ALMIRALL reserves its right to install and use geo-positioning systems to track mobile devices in the event of theft or loss.

(ii) Software and business apps:

1. Only software or business apps explicitly approved and provided by ALMIRALL can be used.
2. Third-party technologies, including multimedia apps or cloud-based services, must be evaluated by ALMIRALL Information Security before use or purchase.
3. It is prohibited to introduce or use ALMIRALL's information in apps intended for personal use.
4. Installing mobile apps from sources other than the official Apple App Store and Android

Market or others explicitly validated by Almirall is strictly prohibited.

(iii) Public Networks:

1. The use of public networks or wireless access points (WIFI) can entail security risks and should only be used when no other secure alternative is available. When using public networks, the Employee must avoid accessing ALMIRALL's systems or any secret, confidential, restricted or internal use only information.
2. Considering the above, the Employee shall disconnect from ALMIRALL's systems and close remote connections once the Employee finishes its business-related activities.

(iv) Physical Protection:

1. The Employee must activate the screen lock (i.e. *Windows* + *L*) when devices are left unattended, even at ALMIRALL's premises.
2. The Employee must take all necessary physical protection measures for safeguarding the devices (i.e. storing the device in lockable cabinets or drawers) when planning to leave the workstation for a significant period of time (e.g. two hours or more).
3. The Employee must also take all necessary protection measures for safeguarding the devices whenever the Employee is outside of ALMIRALL's premises, including when working remotely, (e.g. anchoring devices with a cable and padlock, or storing them securely in a locked drawer).
4. Use of privacy screens when handling Secret or Confidential information is strongly recommended when working on ALMIRALL´s premises. When working remotely, privacy screens are advisable at all times.

2 MONITORING POWERS

To (i) ensure the protection of ALMIRALL's technological assets and information, (ii) prevent information leaks and (iii) prevent criminal or cybercriminal activities, ALMIRALL reserves its right to monitor and access the information managed in its devices, systems, and corporate network.

In line with the above purposes, ALMIRALL may, in particular:

(i) monitor the performance of technological devices,

(ii) prevent the misuse of technological systems and devices,

(iii) resolve incidents in ALMIRALL's software or hardware;

(iv) verify compliance with ALMIRALL's policies, these Terms of Use, or applicable legislation.

ALMIRALL reserves its right to access, monitor, audit, intercept or review any Internet use or access conducted through its technological equipment or systems, as well as the files that are downloaded and stored. ALMIRALL owns the internet connection infrastructure and reserves its right to monitor all Employee's connections using ALMIRALL's network, including the websites accessed and duration of the connection. Additionally, ALMIRALL could block access to specific websites it deems inappropriate.

Any access to the technological systems or devices used by the Employee shall be justified and based in all cases on business purposes and always subject to the applicable legal requirements, including the standards of personal data protection and privacy. By signing these Terms of Use, the Employee is aware and accepts the monitoring of and access to information processed on ALMIRALL's technological equipment, systems, and corporate network, as described in this section B.

3 PERSONAL USE OF ALMIRALL DEVICES AND SYSTEMS

Personal use of ALMIRAL's equipment and systems is permitted unless more stringent local regulations prohibit so. Personal use shall always be responsible and shall never interfere with the Employee's professional performance. Personal use shall not entail a high cost to ALMIRALL or pose risks to ALMIRALL's image and security.

Any personal use must comply with all relevant ALMIRALL policies, laws and applicable regulations, and must not entail risks to the security of ALMIRALL´s processes and information. Furthermore, personal use cannot imply a significant burden on ALMIRALL's infrastructure.

To ensure privacy when using ALMIRALL's equipment and systems for personal use, the Employee is strongly recommended to clearly identify personal communications or files as "private" or "personal". This can be achieved by including a label such as "private" in the subject line of an email or in the name of a file.

It is prohibited to store non-professional personal information on the ALMIRALL network.

Notwithstanding the above, and considering always the applicable local laws, regulations, agreements, and policies, including those relating to data protection, telecommunications, labour law and collective agreements (or similar agreements), ALMIRALL reserves its right to

access to items marked as "private" or "personal" in various circumstances, including but not limited to:

a) Whenever a reasonable suspicion of a business-related risk exists.

b) Whenever a reasonable suspicion that a criminal offence, a breach of labour law, of common law, a statute or any other type of law, or any other significant breach of ALMIRALL policies has or may be committed.

c) Whenever situations involving potential litigation, or internal or external investigations related to ALMIRALL's business take place.

In the event of unintentional access to personal items during the course of activities aiming to protect ALMIRALL's business, any copy or record shall be deleted once it is verified that item is private and not linked to ALMIRALL's business.

4 SUSPENSION AND TERMINATION OF THE EMPLOYMENT RELATIONSHIP WITH ALMIRALL

Suspension of the professional relationship

In the event that the Employee's employment agreement is temporarily suspended, ALMIRALL reserves its right to access the Employee's email account to ensure a proper continuity of the business and/or the security of the information. The Employee is aware of and agreed with this possible arrangement upon signature of these Terms of Use.

During the time of suspension, ALMIRALL reserves its right to set an automatic reply message in the email account. This message will inform the sender that: i) the employee is unavailable and unable to respond, and/or ii) the message may be forwarded to another ALMIRALL employee.

ALMIRALL reserves its right to request the Employee to return any equipment (i.e. laptops, mobile phones, etc.) during the time of suspension, unless the suspension is due to medical leave. If the equipment is not returned or returned damaged due to the Employee's unauthorised or wrongful use, ALMIRALL reserves its right to take the necessary measures to get compensated for any damages.

Termination of the employment relationship:

The Employee is hereby informed that, upon the termination of its employment relationship with ALMIRALL, regardless of the reason, the Employee will no longer have access to the ALMIRALL email account, to the equipment, systems, network, and information. In this sense, the Employee:

- must leave intact all files and documents used for professional purposes and refrain from accessing them thereafter. If there are any personal email messages, it is the responsibility of the Employee to delete these files before returning the equipment. After handing over the equipment, the Employee shall not have any expectation of privacy regarding personal items.
- must not retain any copies of ALMIRALL documents.
- must return all equipment (such as laptops, mobile phones, etc.) belonging to ALMIRALL. If the equipment is not returned, or damages due to misuse are detected, ALMIRALL reserves its right to take appropriate actions to remediate the damages caused.

  ALMIRALL's authorised personnel will deactivate the Employee's email account.

In the event of termination of the employment relationship, and in order to maintain ALMIRALL's business continuity, to mitigate business-related risks, to address potential breaches of applicable laws or ALMIRALL's Policies, or handle situations related to potential disputes or lawsuits, ALMIRALL reserves its right to review the following contents:

- Work documents;
- Computer hard drives or systems;
- Data from internet network connections;
- Outgoing emails;
- Incoming emails,

  always observing the applicable laws, fundamental rights and the safeguards outlined in these Terms of Use.

5 BREACH OF THE TERMS OF USE

Any breach of these Terms of Use may constitute a breach by the Employee of the employment agreement between ALMIRALL and the Employee. Depending on the nature and circumstances of each case, appropriate measures shall be taken. Furthermore, the Employee shall be held responsible for any damages incurred by ALMIRALL or third parties as a result of non-compliance with the requirements and measures outlined in these Terms of Use.

I confirm that I have read and understood these Terms of Use and I fully accept the provisions stated herein.

Signature and Date:

The Employee