Corticeira Amorim

General Cybersecurity Policy

(Version 2.0, approved by the Board of Directors of Corticeira Amorim, S.G.P.S., S.A. at the meeting held on 30 March 2026)

Table of Contents

1. BACKGROUND

Information and information systems play a critical role in the development and sustainability of the business activities of Corticeira Amorim, S.G.P.S., S.A. and its Companies (the group of companies over which Corticeira Amorim exercises a controlling relationship, regardless of whether their registered offices are located in Portugal or in another country), hereinafter collectively referred to as "Corticeira Amorim". These systems are exposed to an increasing number of operational risks that may result in adverse impacts for Corticeira Amorim, namely:

i. Losses to Corticeira Amorim's business.

ii. Impact on operations and quality of the services provided.

iii. Damage to Corticeira Amorim's image

iv. Non-compliance with legal, regulatory or contractual obligations.

This risk context requires the existence of regulations regarding cybersecurity. This document formalises Corticeira Amorim's General Cybersecurity Policy.

2. OBJECTIVE

The General Cybersecurity Policy aims to regulate Corticeira Amorim's cybersecurity, in line with the principles and guidelines contained in Corticeira Amorim's mission:

i. To contribute to maintaining the confidence of customers, workers, shareholders and regulatory bodies in Corticeira Amorim's ability to protect the information under its responsibility from cyber-threats or others, accidental or intentional, that may compromise its confidentiality, integrity and availability.

ii. To comply with the legal, regulatory and contractual obligations applicable to Corticeira Amorim.

iii. To enable a capacity for the timely detection of events that may be indicative of actions aimed at compromising Corticeira Amorim's information and information systems.

iv. To provide an effective and efficient response capacity in the event of cybersecurity incidents.

v. To operationally implement Corticeira Amorim's cybersecurity strategy, considering the current and future challenges to which Corticeira Amorim must respond, depending on technological evolution.

3. SCOPE

The General Cybersecurity Policy establishes the framework of cybersecurity at Corticeira Amorim, and applies to:

i. The information and information systems that are under the responsibility of Corticeira Amorim;

ii. All workers at Corticeira Amorim are responsible for contributing to the implementation of this Policy, whether by upholding and observing the principles of good governance, also set out in the Company's Code of Ethics and Professional Conduct, or through direct responsibilities in cybersecurity matters. This policy is aimed at both an internal and external group:

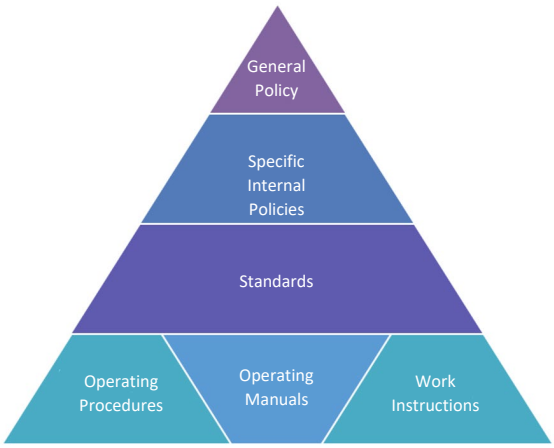
   a) The internal group includes all workers (including members of the governing bodies, directors and other workers) of any company that is part of Corticeira Amorim, as well as all temporary workers. Corticeira Amorim and its workers will base their decisions and actions on the principles established in this Policy, fulfilling their obligations in a professional, responsible and dutiful manner, at all times pursuing excellence in performance

and promoting an appropriate working environment, while upholding Corticeira Amorim's reputation and contributing to its sustainability;

b) The external group comprises all entities that have an economic, institutional or corporate relationship with Corticeira Amorim. External stakeholders (Corticeira Amorim's shareholders and investors, customers, business partners and suppliers) are expressly required to respect and adhere to the principles established in this policy, to the extent that the values, principles and standards established herein may be applicable to them.

4. STRUCTURE OF THE CYBERSECURITY POLICY

Corticeira Amorim's Cybersecurity Policy is framed by a set of regulations on cybersecurity that operationally implement it, according to the following hierarchical structure:



The **General Policy** defined in this document establishes global guidelines for the protection of Corticeira Amorim's information and information systems, and the responsibilities for their implementation.

The **Specific Internal Policies** regulate specific aspects of protection inherent to the various relevant cybersecurity domains, in compliance with Corticeira Amorim's business requirements and with applicable legal, regulatory and contractual obligations. These internal policies define the minimum security level to be implemented at Corticeira Amorim.

The **Standards** formalise the rules and requirements of cybersecurity that aim to operationally implement the Specific Policies.

The **Operating Procedures, Operating Manuals and Work Instructions** detail the operational activities necessary for the implementation of the cybersecurity Standards.

5. LEGAL AND REGULATORY FRAMEWORK

Corticeira Amorim's Cybersecurity Policy is aligned with the legal and regulatory provisions to which Corticeira Amorim is bound in the course of its activities.

6. REFERENCES

This policy includes Corticeira Amorim's stance on this issue and establishes principles in line with the main applicable international standards, such as:

- ISO/IEC 27001;
- NIST CSF.

7. PRINCIPLES

Corticeira Amorim's Cybersecurity Policy is based on a set of cybersecurity principles that must be followed and applied:

i. Comply with the responsibilities inherent to each role with regard to cybersecurity, as defined in Corticeira Amorim's cybersecurity regulatory framework;

ii. Identify the cybersecurity risks to which Corticeira Amorim's information and information systems are exposed, analyse them according to their potential impact and probability of occurrence, and implement control measures that mitigate the identified risks;

iii. Ensure that the access to Corticeira Amorim's information and information systems is:

- Controlled through the identification and authentication of the worker accessing the information and information systems and the equipment used for that access;
- Tracked by keeping a record of accesses made or attempted;

iv. Assign access only to the information and information systems necessary for the performance of each worker's job, taking into account segregation of duties principles;

v. Include security in the design and implementation of information systems;

vi. Continuously protect information and information systems against unauthorised access or use, throughout their life cycle;

vii. Plan and ensure the availability of information and information systems that support the continuity of Corticeira Amorim's business activities in the event of a major incident;

viii. Ensure that a continuous cybersecurity training programme is in place and implemented, as well as regular refresher and awareness-raising initiatives, aimed at all workers (including members of the governing bodies and directors).

8. RESPONSIBILITIES

The Board of Directors of Corticeira Amorim is responsible for approving Corticeira Amorim's General Cybersecurity Policy, while its Executive Committee is responsible for approving the Specific Internal Policies and backing the Cybersecurity Strategic Plan, as well as making the appropriate instruments and means available for the management of cybersecurity in Corticeira Amorim.

Cybersecurity forms part of the cross-functional support area "Information Technology and Systems", which is overseen by a member of Corticeira Amorim's Executive Committee.

The transversal management of cybersecurity is the responsibility of the Cybersecurity Area. The main responsibilities of the Cybersecurity Area are:

i. Define and control the implementation of the Cybersecurity Strategic Plan;

ii. Define and control the implementation of the General Policy and Specific Policies and coordinate their operational implementation in Standards, Operating Procedures, Operating Manuals and Work Instructions;

iii. Produce, monitor and report on the evolution of the internal and external cybersecurity indicators;

iv. Support Corticeira Amorim's structural units in assessing the cybersecurity risk and defining the respective mitigation plans.

It is Corticeira Amorim's responsibility to design, implement and maintain secure information systems, in accordance with Corticeira Amorim's General Cybersecurity Policy.

It is the responsibility of the Business Units to implement the Policy within the scope of their activities.

Each worker at Corticeira Amorim is responsible for their actions in relation to the protection of the information and information systems they access or handle in the course of their duties, and must safeguard Corticeira Amorim's security.

9. ENGAGEMENT WITH STAKEHOLDERS

Corticeira Amorim incorporates the views, interests, needs and rights of stakeholders potentially affected by its activities into the definition of its policies, including the General Cybersecurity Policy. To this end, it regularly consults its stakeholders, namely workers, including those in the value chain, communities, consumers and end-users, customers, suppliers, and shareholders, among others.

10. COMMUNICATION

Corticeira Amorim takes appropriate measures to ensure dissemination of the General Cybersecurity Policy, making it available on Corticeira Amorim's corporate website (www.amorim.com, in Portuguese and in English), so that:

- All internal recipients are aware of the content of this Policy, understand its scope and adopt the principles and practices outlined within it, with the Human Resources Department being responsible for other appropriate internal communication measures;
- All external recipients are aware of the content of this Policy, understand its scope and respect or adhere to the principles set out in it, insofar as the values, principles and standards may be applicable to them.

11. MANAGEMENT OF THE GENERAL CYBERSECURITY POLICY

The exceptions to Corticeira Amorim's General Cybersecurity Policy are dealt with according to the rules established in specific regulations, which establish a formal risk management process for dealing with these situations.

The handling of exceptions is carried out through shared management by those responsible for the different functional or technical areas in their respective fields of competence, under the coordination of Corticeira Amorim's Cybersecurity Area.

All authorised exceptions are identified and recorded, so that such situations are included in the next review of Corticeira Amorim's Cybersecurity Policy or are formalised as exceptions.

Corticeira Amorim's General Cybersecurity Policy and its amendments are approved by Corticeira Amorim's Board of Directors.

12. CONFORMITY

Each worker is individually responsible for knowing, understanding and fulfilling their obligations in the correct use and protection of Corticeira Amorim's information and information systems.

Situations of non-compliance with the General Cybersecurity Policy, even if attempted, may give rise to disciplinary processes, as well as civil or criminal action being brought, in accordance with the applicable laws.

There are general measures in place to monitor internal and external communications and patterns of use of information and information technology, always in strict compliance with personal data protection laws and regulations.

Any doubts about Corticeira Amorim's General Cybersecurity Policy must be addressed to the Cybersecurity Area.

13. VALIDITY AND REVIEW

Corticeira Amorim's General Cybersecurity Policy will be periodically reviewed whenever justified as a result of significant changes in applicable laws and regulations, Corticeira Amorim's business strategy and/or Corticeira Amorim's risk profile.

14. VERSIONS

Version	Prepared by	Date	Approval	
			Name	Date
1.0	CISO / OSI	03/02/2022	Board of Directors of Corticeira Amorim, S.G.P.S., S.A.	23/02/2022
1.1	CISO / Amorim Cork IT	03/01/2024	Board of Directors of Corticeira Amorim, S.G.P.S., S.A.	19/01/2024
2.0	Cybersecurity / Amorim Cork IT Area	16/03/2026	Board of Directors of Corticeira Amorim, S.G.P.S., S.A.	30/03/2026

Mozelos, 30 March 2026

ANNEX I - GLOSSARY

Cybersecurity	Technological mechanisms, processes and practices that ensure the protection of confidentiality, integrity and availability of information and information systems, including communications infrastructure, against cyber-threats or against other threats.
Life Cycle	Relevant stages of information's existence, from its creation, use, transport and destruction.
Workers	Employees, suppliers, consultants, including the workers of external entities or other entities and/or people who access Corticeira Amorim information and/or information technology.
Confidentiality	Attribute of information security that ensures that information is accessible only by authorised entities.
Availability	Guarantee that information or systems are available for access, whenever requested by an authorised entity.
Cybersecurity Incident	Event or a set of events that compromise or may compromise information and/or information systems, including acts or omissions, deliberate or otherwise, that infringe Corticeira Amorim's cybersecurity policies.
Integrity	Attribute of information security that ensures that information is altered or suppressed in an authorised manner.
Segregation of Duties	Effective separation of incompatible or conflicting activities (e.g. authorisation and execution) in order to ensure that no user can perform both duties.
Information Systems	Any combination of devices, network equipment, platforms, processes, applications, interactive or not, totally or partially automated, that use, store, transport or transform information.