Informal Translation

Corticeira Amorim

General Cybersecurity Policy

(Approved at the meeting of the Board of Directors of Corticeira Amorim, S.G.P.S., S.A. on 23 February 2022)

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, SGPS, SA. They are exposed to a growing number of operational risks that may result in negative 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, in order to:

i. Contribute to maintaining the confidence of clients, employees, 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. Comply with the legal, regulatory and contractual obligations applicable to Corticeira Amorim.
iii. 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. Provide an effective and efficient response capacity in the event of cybersecurity incidents.
v. Operationally implement Corticeira Amorim's cybersecurity strategy, considering the current and future challenges to which Corticeira Amorim must respond, depending on technological evolution.

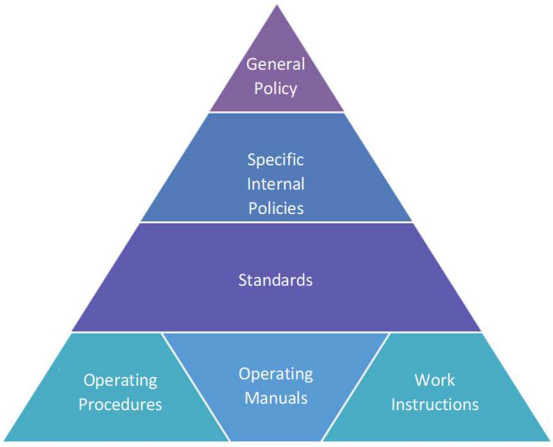
3. SCOPE

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. Corticeira Amorim's employees.

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. 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 their role with regard to cybersecurity and defined in Corticeira Amorim's cybersecurity body of rules.

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 employee 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 employee's job, considering the principles of segregation of duties.

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.

7. RESPONSIBILITIES

The Board of Directors of Corticeira Amorim is responsible for approving Corticeira Amorim's General 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.

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 Cybersecurity Policy.

Each Corticeira Amorim employee is responsible for their actions related to the protection of the information and information systems that they access or handle in the course of their duties and must take care of Corticeira Amorim's security.

8. COMMUNICATION

The regulatory structure that makes up Corticeira Amorim's Cybersecurity Policy is disclosed and published in accordance with the rules established by Amorim, according to the security classification level of the respective standards.

All entities outside Corticeira Amorim must be informed of their responsibilities and obligations regarding Corticeira Amorim's cybersecurity, in accordance with the directives of Amorim's Cybersecurity Policy.

9. MANAGEMENT OF THE CYBERSECURITY POLICY

The exceptions to Corticeira Amorim's 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 Cybersecurity Policy is 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.

Corticeira Amorim's General Cybersecurity Policy and its amendments are approved by Corticeira Amorim's Board of Directors and published on Corticeira Amorim's website. The Specific Internal Policies are approved by the Executive Committee of the Board of Directors of Corticeira Amorim and made available on the Corticeira Amorim Intranet. They are disclosed to all employees as well as to other external entities involved in Corticeira Amorim's activities, with access to Corticeira Amorim's information, according to the directives of Corticeira Amorim's Cybersecurity Policy.

10. CONFORMITY

Each employee 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 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 Cybersecurity Policy must be addressed to the Cybersecurity Area.

ANNEX I - GLOSSARY

Availability	Guarantee that information or systems are available for access, whenever requested by an authorised entity.
Confidentiality	Attribute of information security that ensures that information is accessible only by authorised entities.
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.
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.
Employees	Employees, suppliers, consultants, including the employees of external entities or other entities and/or people who access Corticeira Amorim information and/or information technology.
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.
Integrity	Attribute of information security that ensures that information is altered or suppressed in an authorised manner.
Life Cycle	Relevant stages of information's existence, from its creation, use, transport and destruction.
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.