

Portima Information Security Policy

Version 1.2

Document summary	This document outlines Portima's commitment to protecting the confidentiality, integrity, and availability of information. The purpose of this policy is to ensure the protection of information assets and reduce the risk of information security incidents.		
Intended Audience	Portima employees, contractors and any other individuals who access Portima's systems and data.		
Process	Information Security		
Issue date	24/01/2024		
Next review date	02/2025		
Document manager	Portima ISMS Coordinator		
Approval level	CODIR		
Classification level	Public		
Reference	ISMS 001 POL		
Version	V.1.2		
Status	Approved	Date	25/01/2024

The latest approved version of this document is available at:

Sharepoint and portima.com

History

Version	Updated by	Date approval	Description of changes
1.0		09/08/2023	First approved version
1.1	ISMS Coordinator	24/08/2023	Classification level adapted from internal to public Audience for Data Privacy Policy
1.2	ISMS Coordinator	25/01/2024	Roles and responsibilities

Table of Contents

1. Introduction	4
2. Scope.....	4
3. Portima’s commitment to information security	5
4. Information security policy framework.....	5
5. Information Security Risk Management	6
6. Information security roles and responsibilities.....	7
7. Data Classification	9
8. Training and Awareness.....	10
9. Review and Auditing.....	10
10. Policy enforcement.....	10
11. Reference.....	11
12. Glossary	11

1. Introduction

This policy outlines Portima's commitment to protecting the confidentiality, integrity, and availability of information. The purpose of this policy is to ensure the protection of information assets and reduce the risk of information security incidents.

The information security policy describes Portima's responsibility to:

- Protect the confidentiality, integrity, and availability of business-critical information, based on good practices;
- Ensure that the aforementioned information is exchanged with external parties (e.g., stakeholders, customers and/or suppliers) in a secure manner;
- Prevent or minimizing the impact of information security incidents or breaches.
- Protect Portima's business, reputation and to safeguard our people; and
- Ensure that Portima's employees understand their roles and responsibilities.

It also defines procedures, baselines, and practices for the aforementioned resources to acquire adequate knowledge of the security policy and how to protect information from unauthorized use or disclosure.

2. Scope

This policy applies to all employees, contractors, and any other individuals who access Portima's systems and data. It's considered as an umbrella above other policies (see section 4).

This policy covers all information assets, including physical, electronic, and confidential information, stored in any format or location. Either these information assets are owned or controlled by Portima, including but not limited to:

- Cloud infrastructure;
- All servers, workstations, laptops, mobile devices, and other computing devices;
- All network infrastructure, including routers, switches, and firewalls; and
- All data stored on Portima's systems, including but not limited to: financial information, personal information, confidential business information, and intellectual property.

3. Portima's commitment to information security

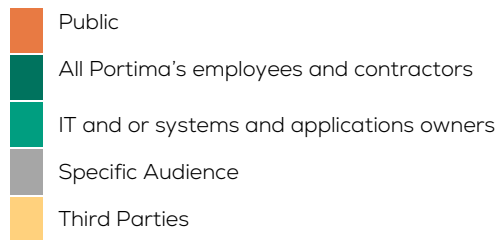
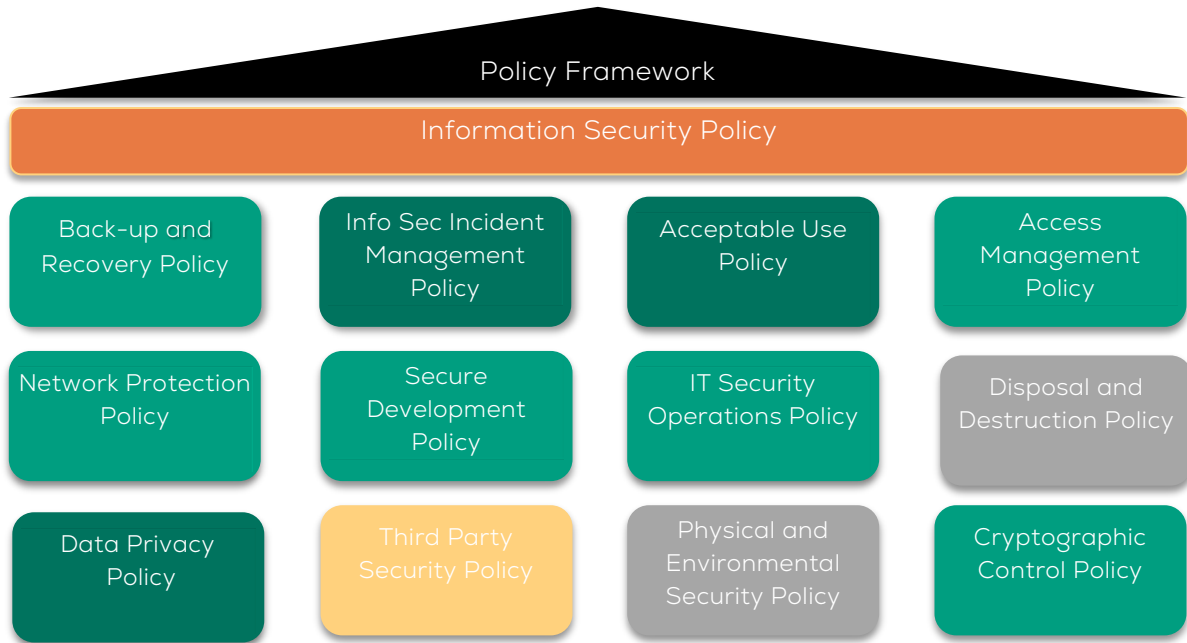
Portima's CODIR acknowledges the expectations of both internal and external stakeholders regarding the information security posture of the organisation. More specifically, Portima's CODIR is committed to achieve the following objectives:

- [1] Protect the business processes and infrastructure related to software development, deployment and support of Brio and Portima Connect.
- [2] Safeguarding the confidentiality, integrity, and availability of its data, using a risk-based approach.
- [3] Complying with the legal requirements and meeting its business partners' expectations.

In order to support this commitment and achieve the information security objectives Portima established and operates an Information Security Management System (ISMS). This ISMS is comprised of information security policies, standards and procedures designed to maintain, review and continually improve information security across Portima from a risk-based perspective.

4. Information security policy framework

As part of the risk-based ISMS, Portima established an information security policy framework comprised out of information security policies outlining the information security requirements to be adhered to by Portima employees and contractors. This information security policy framework is subject to the ISMS' continual improvement process ensuring that these policies are maintained, reviewed and updated when relevant.



5. Information Security Risk Management

The Chief information security officer shall ensure that a risk assessment is conducted at least annually or when significant changes occur to Portima's organisation or IT environment. This risk assessment shall be conducted in line with Portima's Risk Assessment Methodology. The assessment shall provide a comprehensive explanation of the information security risks currently faced by Portima and determine specific treatment actions to manage these risks.

6. Information security roles and responsibilities

Information security roles and responsibilities are defined and assigned at the different levels of Portima’s organisation while ensuring the segregation of duties. These roles and responsibilities are outlined and documented as part of the organisation’s ISMS Manual.

Role	Description	Name
CEO	<ul style="list-style-type: none"> The CEO is accountable for the overall information security within Portima. The CEO approves and validates the information security objectives escalated by the CIO 	Jan Peeters
Chief Information Officer (CIO)	<ul style="list-style-type: none"> The CIO reports the ISMS performance, risks and overall security posture towards the CODIR. The CIO participates in the Portima CODIR Meeting and ensures information security is taken into account within IT. 	Christophe Cloesen
Chief Information Security Officer (CISO)	<ul style="list-style-type: none"> The Chief Information Security Officer (CISO) has the overall responsibility for the management of information security and the management of the ISMS. The CISO ensures that Portima’s information security objectives are captured in information security policies. Monitors compliance to information security policies. Create and maintain information security awareness for all Portima staff and relevant third-parties. The CISO coordinates the Risk Management within the ISMS.(e.g., follow up on treatment actions status). The CISO defines ISMS key performance indicators to be reported to the ISMS Forum. The CISO is responsible for registering, tracking & handling information security incidents & non-conformities towards policies and standards, problems & corrective actions. The CISO maintains contact with different interested parties & information security subject-matter experts and fora. The CISO reports to the CIO. 	Mohamed Amine Youssef

<p>ISMS Coordinator</p>	<ul style="list-style-type: none"> • The Information Security Management System (ISMS) coordinator is responsible for the day-to-day management of the ISMS. • The ISMS coordinator ensures compliance to the ISO 27001:2022 standard. • The ISMS coordinator follows-up on the different tasks tracked within the ISMS. • The ISMS coordinator tracks ISMS key performance indicators to be reported to the ISMS Forum. • The ISMS coordinator drives the ISMS management review in the Portima's CODIR meeting and ISMS Forum. • The ISMS coordinator coordinates External and Internal audits. • Review of the statement of applicability. • The ISMS coordinator reports to Cécile Louvrier (CODIR member) and works in close collaboration with the CISO under the state of ISMS. 	<p>Valérie Dechamps</p>
<p>System owner</p>	<ul style="list-style-type: none"> • Responsible for the security aspect related to system such as approving authentication, hardening. 	<p>Cécile Louvrier (PO Portima Connect) Christophe Cloesen</p>
<p>Data Protection Officer (DPO)</p>	<ul style="list-style-type: none"> • Ensures that Portima is compliant with data protection regulations. • Collaborates with the CISO to identify data protection requirements to be considered in IT projects and operations. 	<p>Valérie Dechamps</p>
<p>Chapter lead Product Owner</p>	<ul style="list-style-type: none"> • The PO / CL is responsible for information security and privacy aspects for products within his/her responsibility. • The PO / CL is responsible to serve as first point of contact regarding information security requirements and incident for products within his/her responsibility. 	<p>Cécile Louvrier (Portima Connect) Matthieu Legros (Portima Connect) Daniel Wuidart (Brio) Koen Ramakers (Brio) Jean-Luc Loroy (Infra) Bart Pollet (Infra) Christophe Arnould (BCC) John Croon (Facility Mgr)</p>

Risk Officer	<ul style="list-style-type: none"> • Establish and maintain security risk methodology • Coordinate with CIO, CISO, DPO, PO and CL to regularly identify and assess security risks of ISMS • Maintain a security risk register • Coordinate with CIO, CISO, DPO, PO and CL to define security risk treatments • Maintain a security risk treatment plan 	Caline Villacres
Product security champion	<ul style="list-style-type: none"> • The immediate contact for the security of the product within his/her responsibility. • Responsible to serve as first point of contact regarding information security requirements and incident within his/her product. 	Mohamed Amine Youssef

7. Data Classification

All Portima’s employees should classify and handle information based on Portima classification scheme outlined below:

Classification Levels	Description
Confidential	Confidential data is information available only for authorised users who really need access to the information (e.g., strategic information, broker client data).
Internal use	By default, all documents and data belonging to Portima are considered “internal use”, except if they are classified “public” or “confidential”
Public	Public data is information that everyone has access to. It’s public information, freely accessible and can thus be openly used, reused and shared.

8. Training and Awareness

Portima shall provide regular information security training and awareness activities (eg: phishing campaigns) to raise resources having access to its systems and data awareness regarding information security.

During onboarding, the employee/contractor shall also attend awareness sessions on the following topics:

- General ICT Security awareness
- GDPR
- Phishing reporting
- Human firewall

All those trainings and security awareness activities are mandatory.

9. Review and Auditing

Portima shall review and audit in a yearly basis its security policies and practices to ensure that they are effective, up-to-date and reflect changes in technology, business processes, and regulatory requirements.

10. Policy enforcement

The policy statements containing the terms “shall” and “shall not” indicate a requirement, while the terms “should” and “should not” indicate a recommendation.

Violation of this information security policy or any of Portima security policies or security procedures, whether through negligence or with malicious intent might be subject to administrative discipline and possible criminal pursuit.

11. Reference

ISO 27001:2022 Controls (Annex A)
5. Leadership
6. Planning
A.5.1 Policies for information security
A.5.2 Information security roles and responsibilities
A.5.12 Classification of information
A.5.13 Labelling of information
A.5.24 Information security incident management planning and preparation

12. Glossary

Term	Description
Availability	A principle of assuring that information is accessible to and usable by an authorised individual or entity when required.
Confidentiality	Preserving authorized access to ensure that information and systems are only accessible to authorised users.
Integrity	The guarding against improper information modification or destruction.
Information	Knowledge concerning objects, such as facts, events, things, processes, or ideas that, within a certain context, has a particular meaning.
Information security	The set of the administrative and the technical measures (practices and methods) taken to ensure the protection of the Portima’s information and information systems.
Information security incident	A single or a series of unwanted or unexpected cyber security events that are likely to compromise organisational activities.

Risk	The degree of danger that a threat might materialise if one or more vulnerabilities in an information system were to be exploited.
ISMS	A management system comprised of information security policies, roles and responsibilities to structurally identify and manage cyber risks while creating visibility on Portima's information security posture.