HPI implements standardized procedures and actions to safeguard information integrity and security, proportional to HPI's scale and operations. Mechanisms are in place to detect and prevent information security breaches, including the misuse of data, networks, and IT systems at a level appropriate to HPI's technical environment.

Core Objectives

HPI's Information Security Policy aims to:

- Safeguard highly confidential business information on clients and / or project partners
- Protect personal and sensitive data in accordance with GDPR provisions and related data protection laws
- Respect all customer and user rights through effective handling of complaints and queries related to information security
- Protect HPI's reputation by upholding high ethical and legal standards in all information management practices

Security Framework Principles

HPI's Information security framework, managed by the designated IT Security Manager, ensures:

- Confidentiality – restricted access to data and information assets to only those authorized by project roles and partnership agreements
- Integrity – maintaining data completeness, accuracy, and reliable IT system operation
- Availability – ensuring timely access to information and IT systems for authorized users, including staff and external collaborators, when required

Access Control and Authorization

Access to information is restricted to HPI staff and scientific partners-users directly involved in a project, with roles and rights defined on a per-project basis by the Scientific Director. Authorization to restricted databases and information is granted exclusively by the Scientific Director.

Access to HPIs network and server (physical or not) is conducted through a unique login process requiring password authentication. Comprehensive monitoring records all access events (both successful and failed) according to user, date, and time, proportional to the size and technical environment of HPI.

IT Security Management

A designated IT Security professional (IT Security Officer):

1) Maintains system access and activity logs for a minimum 60 days

2) Monitors system use, reports suspicious activity, and responds to any actual or attempted HPI server breaches.

Data Classification System

Retained and processed data and information are classified into 3 categories for effective access authorization and data utilization:

(a) High risk class - Data subject to legal protection (e.g. personal sensitive data under GDPR)

(b) Confidential class - Data not legally protected but deemed business-sensitive or non-public, for instance non-public information about projects, operations, performance, technology, products, or employees

(c) Public information class - Data that are cleared for open dissemination (e.g. public reports, news releases) approved by the Scientific Director

The Scientific Director determines both data classification and preservation standards for integrity appropriate to each level and proportionate to project and team needs.

Technical Security Measures

Protective operational mechanisms include:

- Up- to date anti-malware software
- Firewall systems as appropriate to infrastructure
- Encryption methods for high-risk or sensitive data where relevant
- Strict ban on unauthorized data transfer
- Clear backup and recovery protocols, as described in the HPI Disaster Recovery Plan.

Staff Compliance and Responsibilities

All personnel and project partners are responsible to follow information security procedures, including maintaining of data confidentiality and integrity. Any non-compliance is subject to disciplinary action. All users are expected to act in accordance with the prevailing information security policy to ensure highest possible standards of confidentiality, integrity and availability.

Personal Information Management

HPI may collect personal information only for legitimate, project-specific business needs. This information is stored for as long as required by law or project commitments. HPI also takes precautions to safeguard security in personal information collection, processing, storage, and transfer, including proper notice and consent, as required by corresponding legal standards.

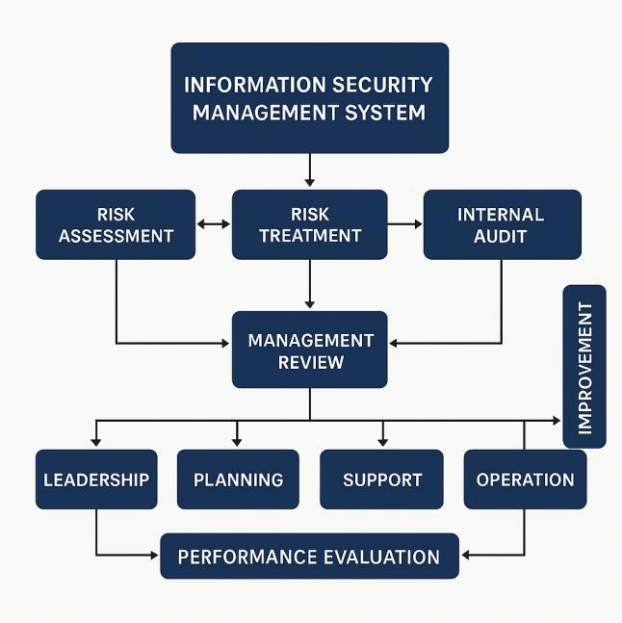
Information Security Management System (ISMS)

HPI has established, implemented, and continuously improves a practical information security management system (ISMS), proportional to the structure and resources of the organization. All information security processes which are already part of the ISMS are

presented in the diagram below. The necessary processes and their interactions are visually mapped and regularly reviewed to:

1) Clarify process relationships and responsibilities among HPI staff, project partners, and system users
2) Promote stakeholder understanding of security and compliance interactions, including incident response and continuous improvement
3) Align with relevant international standards (ISO 27001, ISO 9001, ISO 37001) in a structured, efficient manner that supports and improves HPI's collaborative operations.

This approach enables HPI to maintain high ethical standards, effective risk managements, and trusted service delivery for all clients and partners.



Chair of the Board of Directors

Professor Souliotis Kyriakos