INTEGRATED MANAGEMENT SYSTEM (IMS) POLICY

Document ID	**IMS_2**	**Classification**	**PUBLIC**
Version Number	V3	Initial Owner	Aurelijus Butkus
Issue Date	2023-09-01	Location	Sharepoint
Approved	2023-09-01	Approved by	Adriaan Hoogduijn

The Scope

The aim of this top-level Policy is to define the purpose, direction, principles and basic rules for *Hyarchis* information security management. The way in which we successfully operate our business is dependent on how we protect the confidentiality, integrity, and availability of our information, Personal Data stored in the Cloud and protection of personally identifiable information (PII) in clouds activities, the supporting IT systems, business process, client and personal data. This Policy applies to *Hyarchis* group companies, as defined in the ISMS Scope Document.

This policy applies to all *Hyarchis* group companies - staff, contractors and representatives of vendors and business partners, all interested parties specifically anyone who:

- ✓ uses or connects to *Hyarchis* computer resources;
- ✓ has access to personal or business confidential data held by *Hyarchis*;
- ✓ is involved in business processes that generate and receive electronic transmissions;
- ✓ control the Integrated Management system implementation, surveillance.
- ✓ uses computer systems, telephone systems or devices that are linked to, part of or manage the network or electronic resources (i.e. both fixed and mobile computerized system).

Legal and regulatory obligations

Hyarchis is fully aware of its legal obligations to confidentiality and therefore we comply with the following regulations and obtain updates from https://www.hyarchis.com/.

- ISO/IEC 27001:2022 and ISO/IEC 27018:2019
- ISO 9001:2015
- ISO 22301:2019
- Employment Law Act
- GDPR (25th May 2018)
- Cybernetic security legal requirements
- Articles of Association (Statuten)
- Company extract from Chamber of Commerce
- Overview of beneficiary ownership (UBO: previously provided)
- Collective labour agreements (CAO);
- Commit to satisfy other interested parties requirements.

Roles and Responsibilities

Our Chief Information Security Manager (This role is carried out by our UAB Hyarchis Baltic Chief Operational Officer in Kaunas, Lithuania and VDD IQware B.V. Chief Executive Officer in Eindhoven, the Netherlands) is responsible for randomly sampling records to ensure that all required data has been captured, and that data is accurate and complete.

It is the responsibility of all staff to ensure that all data is treated with the utmost confidentiality, and that no data is given out without the prior authority of any person affected.

Declaration of support for IMS implementation

Users of this document are all employees, contract, temporary and third-party staff working for and on behalf of *Hyarchis*, as well as relevant external parties.

Hereby **UAB Hyarchis Baltic** and **VDD IQware B.V.** top Management declare that IMS implementation and continual improvement will be supported with adequate resources in order to achieve all objectives set in this IMS Policy, as well as satisfy all identified requirements by:

- ✓ Ensuring the compliance with ISO/IEC 27001:2022, ISO/IEC 27018:2019, ISO 9001:2015, ISO 22301:2019 standards requirements.
- ✓ Ensuring the IMS policy and the IMS objectives are established and are compatible with the strategic direction of the organization.

- ✓ Deliver products and services at an acceptable predefined capacity during disruptions.
- ✓ Seek to enhance their resilience through effective IMS.
- ✓ Ensuring the integration of the information security management system requirements into the organization's processes.
- ✓ Ensuring the support to achieving compliance with applicable Information Security and Protection of Personally Identifiable Information legislation and the contractual terms between *Hyarchis* and clients, also comply with stakeholder requirements.
- ✓ Ensuring that the resources needed for the IMS are available.
- ✓ Communicating the importance of effective information security management and of conforming to the information security management system requirements.
- ✓ Ensuring that the information security management system achieves its intended outcome(s).
- ✓ Directing and supporting persons to contribute to the effectiveness of the information security management system.
- ✓ Promoting continual improvement of IMS.
- ✓ Comply business continuity policy and other information security policies;
- ✓ Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

IMS Policy is classified as a public document and is available to all the *Hyarchis* interested parties.

IMS Policies are consistent with the organization's activities and are used as guidelines for the organization's objectives in the field of IMS determination.

IMS Policy is constantly reviewed and updated if needed during management review in order to remain relevant and current.