

Information Security Declaration

version 1.0

Effective Period	Effective upon approval by the Executive Board; reviewed at least once a year
Version	1.0
Date	September 29, 2026
Prepared/modified by	Prof. Dr. Gökmen Zararsız
Approved by	Executive Board, Hematainer Biotechnology and Health Products Inc. Kayseri, Türkiye
Reasons for modification	Initial version

1. Introduction

Protecting the confidentiality, integrity and, when needed, availability of information generated within the MAS® product family, analytical services, research projects and OmegaTree is embraced by Hematainer management as a corporate responsibility. This declaration sets out the general security principles that employees and business partners must follow, together with management's commitment to improvement.

2. Scope and Assets

The scope comprises physical and digital records, biological samples and sample identifiers, raw metabolomic and lipidomic data, analysis results, bioinformatics code and models, OmegaTree development data, intellectual property, technical files, supplier and customer information, and the devices, software and services that process them. The principles apply to employees, researchers, interns, consultants and service providers granted access, regardless of their role or position.

3. Management Commitments

- ✓ Information assets are classified; risk-based protection is applied in particular to health and genetic data, identity links, unpublished research and trade secrets.
- ✓ Access is granted on a need-to-know basis, reviewed regularly, and revoked upon a change of role or departure. Authentication, logging and appropriate technical security controls are applied to sharing and system access according to the level of risk.
- ✓ Processes for data transfer, storage, backup and restore, device security and physical access are defined; the security and confidentiality obligations of service providers are set out in contracts.
- ✓ Research data and personally identifying information are kept separate as far as possible; use outside the project purpose, as well as unauthorised copying or sharing, is prevented.
- ✓ Information security incidents are reported promptly; their impact is contained, they are recorded, their root causes are assessed, and the necessary corrective actions are followed up. Notification obligations relating to personal data breaches are assessed separately.
- ✓ Business continuity requirements are determined; backup and recovery arrangements for critical data and services are tested.

4. Roles and Rules of Conduct

Management is responsible for security objectives and resources; process owners monitor their own assets and risks. Everyone with access to information is responsible for using it within their authorisation, protecting their credentials, reporting without delay incidents such as suspicious e-mails, lost devices, misdirected transmissions or unauthorised access, and complying with confidentiality obligations. Training and awareness activities are carried out in line with the risks of each role.

5. Compliance and Review

The Turkish Personal Data Protection Law No. 6698, research ethics, contracts, and regulations applicable to product and laboratory activities are taken into account. Controls are updated whenever risks, incidents, technology or business partnerships change. The status of implementation and improvement needs are evaluated by management at least once a year.

Contact for security and privacy notifications: info@hematainer.com. Depending on the nature of the incident, a secure communication channel is designated by the Hematainer team.

Approved on: September 2026

This document is signed by all co-founders of Hematainer Biotechnology and Health Products Inc.

Prof. Dr. Mehmet Doğan



Prof. Dr. Halef Okan Doğan



Prof. Dr. Gökmen Zararsız

