INFORMATION SECURITY POLICY

EIQSH has established and implements standardized procedures and actions to safeguard information integrity and security, as well mechanisms to detect and forestall the compromise of information security such as misuse of data, networks, computer systems and applications (where applicable).

Basic aims which are pursued in the frame of EIQSH is policy:

- To safeguard highly confidential business information of its clients
- To protect personal and sensitive data in accordance with GDPR provisions
- To observe the rights of the customers and users providing effective mechanisms for responding to complaints and queries concerning real or perceived non-compliances with the policy is one way to achieve this objective.
- To protect the reputation of the company with respect to its ethical and legal responsibilities regarding information protection.

Information security framework of EIQSH is deemed to safeguard three main objectives:

- Confidentiality – data and information assets must be confined to people authorized to access and not be disclosed to others;
- Integrity – keeping the data intact, complete and accurate, and IT systems operational;
- Availability – an objective indicating that information or system is at disposal of authorized users when needed.

Access to information is restricted to authorized staff and scientific partners-users that are involved in the projects' realization by a set role as defined by the Project Manager.

The Executive Secretary and the Project Manager grant authorization and access to restricted business database and information.

Access to EIQSHs network and files whether or not in the physical sense is conducted via unique login process via Microsoft 365 Business Premium.

Data transfer is strictly prohibited.
Data backup media, procedures and recovery actions are performed via Microsoft 365 Business Premium.

All staff complies with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so, results to disciplinary actions. Each member of staff, partners are responsible for the operational security for the information system that they use in the frame of their EIQSH duties. Each user complies with the security requirements that are currently in force, and ensures, also that the confidentiality, integrity and availability of information they use is maintained to the highest standard.

EIQSH may collect personal information only in the frame of conducting business correspondence or in the frame of realizing partnerships with persons (staff, external partners); however, it only collects such information for legitimate business purposes and retain it only as long as is necessary or required by law. In addition, the EIQSH takes precautions to safeguard the security of personal information when it is collected, processed, stored, and transferred, and will provide notice and obtain consent prior to obtaining personal information, consistent with applicable laws and regulations.