INFORMATION SECURITY POLICY

HPI 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 HPI 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 HPI (via the IT Manager) 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 Scientific Director.

The authorized HPI Board Member(s), the Scientific Director, grant authorization and access to restricted business database and information.

Access to HPIs network and server whether or not in the physical sense is conducted via unique

login process that requires authentication in the form of passwords. Monitoring on all systems is implemented to record logon attempts (both successful and failures) and exact date and time of login logoff.

IT security responsible person is the authorized professional for

1) Maintaining the following logs for at least 60 days

- System Access Logs
- Activity Logs

2) Reporting access violations and reacting to any suspicious activity or attempt of attack on the HPI server.

Retained and processed data and information is classified to the 3 below categories to effectively apply access authorization and utilization of data.

3) High risk class- data protected by state and federal legislation (the Data Protection Act, personal sensitive data under GDPR)

Confidential class -the data in this class does not enjoy the privilege of being under wing of law, but the data owner judges that it should be securely protected against unauthorized disclosure. Confidential information includes information about projects, operations, performance, technology, products, or employees that has not been publicly disclosed by an authorized spokesperson or is not available from public sources. Protecting confidential information is every employee's responsibility.

4) Class Public information-data that can be -or ought to be- freely distributed (marketing material, post and news releases all approved by the Scientific Director).

Scientific Director determines both data classification and the measures to be always taken to preserve the integrity in accordance to the respective level.

Protected operational mechanisms

- Up- to date anti-malware protection
- firewall
- encryption methods

Data transfer is strictly prohibited.

Data backup media, procedures and recovery actions are described in the HPI Disaster Recovery Plan

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 HPI 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.

HPI 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 HPI 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.