Agilis Statistics & Informatics SA
General Commercial Registry # 2823801000
Theanous 15, Athens, 118 54, Greece
t: +30 211 100 3310 – e: contact@agilis-sa.gr
www.agilis.gr

Information Security Policy

Agilis acknowledges the importance of the needs and expectations of our customers, software users, stakeholders and all interested parties for information security as well as the criticality of information security for ensuring that the company will be able to fulfil its mission and achieve its business purpose.

This public Information Security Policy documents the strategic commitment of the company, at the highest management level, to implement all the necessary technical and organisational measures necessary to achieve and maintain the high level of information security required for our business environment, and to the establishment, operation and continual improvement of an Information Security Management System appropriate for this purpose.

Information Security Policy Principles

1. Definition of Information Security

In the context of this policy, *information security* should be regarded in a broad sense as the protection of the *confidentiality* (i.e. protection from unauthorised access), *integrity* (i.e. accuracy, consistency and completeness, as well as reliability of systems), and *availability* (i.e. the ability to access data when needed), of data and information involved in the company's operations and activities, *in any form they may be present*, from external or internal *threats* of accidental or voluntary nature.

This encompasses data in information systems, including information systems managed by third parties such as cloud services used by the company or cloud services offered by the company to customers, documents in any format, electronic or hardcopy, as well as knowledge and tacit information, which should be protected while being processed, stored and retained as well as in transit, i.e. during exchange with external parties.

2. Scope and extent of the Information Security Policy

Our information security policy applies to all our operations and technological systems which are necessary to fulfil our business purpose and is adapted to the specific requirements implied by it. These operations include different areas, each with different information security needs and requirements:

- the provision of managed clinical data management cloud software;
- the provision of clinical data management, biostatistics and other expert services for clinical research;
- software development and consulting services;
- hosting of information systems we may develop for our customers;
- internal information and processes necessary to ensure our business performance and continuity;
- our own usage of managed cloud services by third-party service providers;
- access to information by subcontractors and service providers when outsourcing processes.

Thus, our information security policy covers the operation of technological systems used to provide cloud software as a service and host customer data, the internal operations for processing customer information and data or producing and delivering information to customers and the technological systems used to support these operations, as well as internal operations and outsourcing.

3. Information Security Requirements

For all our services and operations we take into account and analyse all applicable *statutory and regulatory requirements* concerning confidentiality, integrity and availability of information, including legislation and regulations for personal data protection and conduct of clinical studies, at the national, European and international levels, and we follow up closely new developments in the statutory and regulatory areas.

We also analyse and take into account information security requirements implied by applicable *international standards and guidance*, as well as requirements expected by our customers and all interested parties according to industry established best practices and technological state-of-the-art.

Moreover, we take into account requirements stemming from current or projected *information security threats*, as well as lessons learned from security incidents.

These requirements are not only taken into account in the design and operation of our Information Security Management System and policies, but also in our Quality Management System. The coverage of these information security requirements is explicitly accounted for in all our operating procedures and processes, as are all potential information security implications.

Furthermore, for each specific contract, product or service, specific information security requirements, either explicitly requested by customers, or implied by the nature of each project, should be analysed and documented from the specifications and design phases and should be taken into account in product and service specifications, development, testing, validation and quality control.

4. Effective Commitment to Information Security Requirements Compliance

We commit ourselves to the fulfilment all the above information security requirements by including them in detail in *contractually binding agreements* as well as *standard service terms and conditions*, and other binding documentation such as published specifications and technical documents.

We regularly audit internally the effective compliance to the above requirements, record, evaluate, and analyse all potential cases of non-conformity, including information security incidents, and take appropriate corrective and preventive actions and we are open to information security audits by our customers.

As part of our public commitment to compliance to information security requirements, we seek to have our information security system independently audited by external auditors and certified by accredited certification bodies according to international standards.

5. Information Security Priorities and Objectives

Based on the analysis of the needs and expectations of customers and interested parties, our information security policy sets a framework for setting specific *information security objectives* along the following priorities:

- systematic identification and assessment of information security risks and threats, and the active prevention and management of information security incidents;
- protection of confidentiality, integrity and availability of the data and information entrusted to us by customers, partners and users;
- ensuring compliance to information security requirements, incl. regulatory compliance and contractual requirements;
- establishing appropriate measures and plans for ensuring business continuity and disaster recovery;
- develop software following a SDLC (Software Development Life Cycle) process based on secure software development principles and practices;
- ensure the information security protection level specifically required for the provision of cloud software as a service.

For each of these priority areas specific measurable information security objectives are set by Management, monitored during regular management review, and revised to ensure the effectiveness and continual improvement of the information security management system.

6. Information Security Topic Specific Policies

The information security policy is implemented in practice through a series of *topic specific policies*, including for

- controlled access to information systems and services, incl. cloud information services managed by third party providers and used by the company internally of for the provision of our own cloud services
- specific information security requirements for the provision of our cloud services, including controlled access by external users
- information classification and confidentiality protection
- third-party data retention and data return
- secure exchange of confidential information
- protection of data integrity during clinical data management and information exchange

- usage and management of endpoint devices
- personal data protection
- incident management, forensics and communication to affected third parties
- backup, disaster recovery, and business continuity, incl. for the use of managed cloud information services
- secure software development, incl. information security testing and validation
- management of vulnerabilities, threats and risks and networking security

These topic specific policies may be documented as policy documents, binding for all staff, or Standard Operating Procedures, are approved by management and communicated and acknowledged by relevant personnel and relevant interested parties.

7. Information Security Policy Monitoring

The implementation of the information security policy and topic specific policies, as well as the status and effectiveness of the information security management system, are regularly monitored in terms of specific objectives, and based on management review, key performance indicators and regular internal audits.

8. Commitment to Continual Improvement

Due to the ever evolving information security threats and risks, the continual improvement of the information security management system is endorsed by Management as one of the main pillars of its success. Initiatives for improvement are encouraged at all levels and for all personnel.

The information security policy and the related topic specific policies are regularly reviewed and revised to improve their effectiveness and to face new and emergent information security threats as they arise.

Management is committed to directly support all persons in charge of information security implementation, provide strategic direction and priorities and to closely cooperate with them for information security planning.

All personnel, and especially staff at management roles at all levels, is actively encouraged to contribute to the effectiveness of the information security management system in their respective domains, and motivated to undertake initiatives for the continual improvement of information security management.

9. Risk Management

A systematic risk management approach is applied, in an iterative and continuous way, to identify and assess information security risks as they emerge, decide on their proactive treatment and determine resulting information security needs and requirements for their prevention, as well as to ensure preparedness with appropriate incident response, disaster recovery and business continuity plans.

10. Effective Integration into the the Company’s Processes

Our Information Security Management System (ISMS) is an integral part of our overall Quality Management System (QMS), and it is managed, monitored, audited and reviewed using the same methods and standard operating procedures as used for the overall QMS, including for change control, management of non-conformities, internal audits and training.

Moreover, the entire QMS is designed so as to evaluate and take into account relevant information security requirements in all QMS procedures, even if they are not directly relevant to information security management as such.

11. Commitment of Resources

The company is committed to the allocation of the resources required for the effective design, operation and continuous improvement of the ISMS, including planning and budgeting for technical resources, infrastructure and tools, as well as for high-level specialised external support and expert consultancy where needed.

Budget allocated to information security is used as one of the indicators for the monitoring of the implementation of this policy.

12. Authority and Responsibility

The company has endorsed with all the necessary personal authority and responsibility a suitably qualified Information Security Officer (ISO) in charge of closely overseeing and managing the implementation of this policy. The ISO reports directly to the Managing Director and decides corrective actions or interventions in case of security incidents.

The role of the ISO is communicated internally to all personnel as well as to customers, partners and users, and the ISO can be directly contacted for any information security issue.

Moreover, the company has endorsed our IT Director with complete and exclusive responsibility and authority for the implementation of technical measures and controls.

To avoid conflicts of interest there is a complete segregation of duties between the ISO and the IT Manager or Team Leaders in charge of implementing information security measures and practices. Segregation of duties between implementation and inspection / approval is applied in several other aspects of information security management, such as change control, access rights management, software development and code review etc. Whenever this is not possible audit trails ensure that actions can be audited.

13. Awareness and Training

The Information Security Policy also communicated internally to all the company's personnel as a tool to raise awareness and cultivate an information security company culture. The information security policy and where applicable related topic specific policies are acknowledged by all personnel.

Agilis commits the necessary resources for planning and executing activities for in-house awareness raising and training in information security matters in order to communicate the importance of information security to all the company's personnel and ensure that information security is an integral aspect of the company's culture. Specific information security requirements are communicated and discussed in dedicated town-hall meetings and company-wide training sessions.

Apart from general awareness, it is ensured, in a documented way, that personnel involved in the application of ISMS procedures, or other procedures with information security impact, are adequately trained to effectively apply the procedures and respect information security requirements.

14. Transparency

This Information Security Policy is made publicly accessible to all interested parties, including customers, partners and users of the company's software services entrusting information to us, other stakeholders as well as external auditors.

Customers and or any other party with legitimate interest have the right to request specific detailed information and documentation, as well as inspect or audit our information security management system.

N.B.: This Information Security Policy takes into account the specific requirements of ISO/IEC 27017:2015 "Code of practice for information security controls based on ISO/IEC 27002 for cloud services", as well as ISO/IEC 27002:2022 and ISO/IEC 27003:2017.

Review and Approval

Grigorios Farmakis

Grigorios Farmakis
29.06.2023 11:58

Gregory Farmakis
President & Managing Director

Document Code: (v2) IST-020-Q: Information Security Policy / 26 June 2023