Information Security Policy

Our clients, partners, employees, and other data subjects count on us to keep their data secure and maintain their privacy.

Inizio is committed to protecting our professional assets, our relationships, the personal data we control and process, and our reputation. Inizio maintains this policy and a related suite of supporting processes to do so.

Aim and foundation of this policy

The aim of this policy is to communicate how Inizio protects the confidentiality, integrity, and availability of our information assets. Inizio utilizes the U.S. Department of Commerce's National Institute of Standards and Technology Cyber Security Framework as the basis for this policy and its associated processes and documentation.

Scope of this policy

Inizio's Information Security Policy applies and pertains to:

- All of our locations, divisions, businesses, and affiliates,
- All employees, contingent workers, and contractors, and
- Any other persons who have access to Inizio information systems and assets.

Minimum standards and local-level exceptions

This policy establishes minimum information security standards for all Inizio business and subsidiaries.

Any exceptions to this policy, including exceptions pertaining to local legal, regulatory, or business-level information security requirements, must be approved by Inizio's Chief Information Security Officer.

Group Information Security

The Inizio Information Security team will:

- Communicate this Information Security Policy and related processes,
- Promote and increase the awareness of information security,
- Keep the Information Security Policy updated in-line with legal and regulatory requirements, current threats, and business objectives,
- Ensure this Information Security Policy and the related suite of supporting processes safeguard three main objectives:
  - **Confidentiality:** Data and information assets are confined to those with authorised access,
  - **Integrity:** Keeping data intact, complete, and accurate, and
  - **Availability:** Ensuring information systems are available to authorised users when required,
- Monitor and report on compliance with this policy and the related suite of supporting processes, and
- Periodically review and report on the effectiveness of this policy and its related processes.

Our Leaders and Managers

Business leaders, functional heads, and managers across Inizio are expected to:

- Support and encourage staff to adhere with this Information Security Policy and all applicable supporting processes that relate to such,
- Encourage staff to provide feedback to the information security teams,
- Support Group Information Security in ensuring information assets and systems are compliant with this Information Security Policy and all applicable supporting processes that relate to such,
- Ensure all information security awareness training requirements are fulfilled, and
- Report to Group Information Security in a timely manner any non-compliance with this policy and its related processes.

Our People and those who work with us

Keeping our data and systems secure is the responsibility of all employees, contingent workers, and contractors who access Inizio's information systems and assets. Those accessing our information systems must ensure:

- Any security awareness training assigned to you is completed satisfactorily and within required timelines,
- You understand the information you are accessing and how to protect it from unauthorised disclosure or use,
- You adhere to local regulations and legal requirements whilst maintaining the controls highlighted in this Information Security Policy and detailed within its related processes, and
- **Immediately report any suspected information security incidents to your local IT Service Desk or to: informationsecurity@inizio.health**

This policy, together with supportive internal processes, and our Code and Commitments form Inizio's Information Security framework. Please contact informationsecurity@inizio.health with any questions pertaining to the specifics of this policy or our framework.