Gavdi’s Information Security Policy

The overall objectives with this policy are to protect:

- Gavdi’s ability to handle prioritised tasks and services to our clients
- The integrity and confidentiality of Gavdi’s stakeholders
- The integrity and confidentiality of Gavdi’s information
- From illegal actions, accidents, fraud, and unintended incidents
- Assets which are under management of Gavdi
- Internal Gavdi processes (HR, Finance, IT, Legal requirements, etc.)

The following information security key principles for Gavdi are:

- All information security-related work shall be an integral part of Gavdi’s ordinary operation and shall support Gavdi to achieve objectives for quality and effectiveness.
- Compliance with legislative, regulatory, statutory, and contractual requirements across all organisational units and countries Gavdi is present in at any time.
- Information security risks and mitigation actions & controls will be identified by performing structured risk analysis work.
- All employees shall have the necessary knowledge and awareness, including being trained to act according to the information security policy in their daily work.
- Access control will be established in all information systems and physical premises to avoid unauthorised usage.
- If unwanted security breaches happen, all information security-related actions shall limit the damage and ensure normal operation as soon as possible
- Change control will be executed according to defined procedures. Major changes to information resources will be tested and approved by authorised personnel. All major changes will be traceable.
- Proper management of security incidents, including management of business continuity, is critical to Gavdidue to the nature of Gavdi’score business –development of HR and Payroll solution and support of the solutions.

Information is a very important asset to Gavdi. Information security covers actions and controls to protect assets, information, and ability to solve tasks, by securing:

- **Confidentiality**: no personnel will have access to information unless it is job-related tasks.
- **Integrity**: information and systems shall be correct and trustworthy.
- **Availability**: information and systems shall be available to authorised users when needed: need to know principle.