Information Security Policy

Dätwyler IT Services AG, Gotthardstrasse 31, 6460 Altdorf, Schweiz
info@datwyler.com, www.datwyler.com

Datwyler is committed to ensuring the Confidentiality, Integrity and Availability of information. The security of information and information assets is regarded as fundamental for the successful business operation of Datwyler Group and IT Services Delivery Centers.
Datwyler has adopted an Information Security Management System (ISMS) comprising the information security policies, procedures, and a comprehensive risk management framework to effectively protect data/information of Datwyler and its customers from information security threats, whether internal or external, deliberate or accidental. ISMS in Datwyler is aligned with the requirements of ISO/IEC 27001:2022.
The management of Datwyler is committed to ensure that:

- ✓ Information security requirements arising from business, legal, regulatory, contractual, customer, industry and stakeholder expectations are identified, documented, maintained, and regularly reviewed to ensure all applicable obligations are met and effectively addressed within the Information Security Management System.
- ✓ Appropriate resources are allocated to implement, operate, and review an effective Information Security Management System
- ✓ Information security policies, procedures and related documented information are communicated and made available to relevant employees and, where applicable, external parties on need basis;
- ✓ The confidentiality of information is protected and unwarranted disclosure of valuable or sensitive information is prevented;
- ✓ The integrity of information is preserved to ensure its accuracy and completeness and relevance to current business and operational needs;
- ✓ The availability of information is maintained to meet business needs and client requirements and Business Continuity Plans are developed, maintained, and tested;
- ✓ Competence of the employees towards information security management system is enhanced through regular training and skill augmentation initiatives;
- ✓ Incident management process is established and implemented to ensure that all breaches of information security, actual or suspected are reported and investigated;
- ✓ Risks are mitigated to an acceptable level through a risk management framework;
- ✓ Changes to information security policies, procedures and related documented information are reviewed periodically, approved and communicated to relevant stakeholders in a timely manner;
- ✓ All applicable legal, regulatory and contractual requirements related to information security are met and regularly reviewed;
- ✓ Time specific objectives with relevant details of responsible person, resources needed, and target date are defined in the dedicated tool for SMART objectives;
- ✓ All stakeholders are responsible for implementation of respective information security policies and procedures within their area of operation, and oversee adherence by their team members;
- ✓ Non-conformance with information security policies and procedures is addressed through appropriate corrective, disciplinary, contractual or legal actions in accordance with applicable company procedures and laws.

The management of Datwyler acknowledges the need for continual improvement of the information security management system and practices the same through various strategic and operational initiatives.
Datwyler shall ensure that the Information Security Policy and related documented information is reviewed on a regular basis to ensure suitability, adequacy, and effectiveness of the ISMS framework.