Information Security Policy

The Management of JUNE, located at Große Johannisstraße 3, 20457 Hamburg operating as a Marketing Technology Software as a Service (SaaS) Developer and Agent, are committed to preserve the confidentiality, integrity, and availability as well as privacy of all physical and electronic information and assets — aligned with ISO 27001.
JUNE's management is committed to preserve cashflow, profitability, legal and regulatory as well as contractual compliance and JUNE's image through the preservation of assets.
The ISMS implemented and documented within JUNE is mainly managed in 'ClickUp' and contains all relevant information or links to information as well as information security requirements in order to continue to align with JUNE's objectives, enable information sharing and electronic operations to reduce the risks to an acceptable level.
JUNE's current ISMS including but not limited to the Information Asset Management Policy, Risk Management Policy, IT Security Policy and Secure Coding Policy provide the guidelines for identifying, assessing, evaluating and controlling information security risks through active use of the ISMS and the work attitude of each employee throughout the establishment. Information related risks shall be controlled as defined and outlined in the procedure of the Risk Management Policy and Statement of Applicability aligned with the ISO Controls (Annex A ISO/IEC 20771:2022). To ensure availability of information also during holiday time, staff shall follow the holiday workflow and create holiday handover documents to ensure that all relevant information and accesses are available to the covering person. The ISMS manager is responsible for the management and maintenance of the Risk Register. The Risk Treatment Plan will be revised as required and suitable or latest 12 months after implementation. Essential processes are documented and fundamental for this policy and the work ethic within JUNE. The Incident Response and Escalation Plan defines Roles and guidelines for the business continuity, incident response and Incident Reporting.
Additionally to regulatory requirements, JUNE set IT-Security Objectives which include, but are not limited to, availability, confidentiality, and integrity. Objectives are annually reviewed by JUNE's management and supported by policies and procedures. Information Security Objectives are developed in accordance with the business objectives and the results of the risk assessment and risk treatment plan incorporated in the annual Management Review. The objectives are tied to the continual improvement cycle and shall support JUNE’s management and staff in keeping the ISMS aligned with business goals and evolving security needs.
JUNE applies open communication with all our employees and address security risks and goals on a regular basis according to a communication matrix. JUNE is committed to meeting or exceeding applicable legal, regulatory, and contractual requirements related to information security. We actively monitor and review security measures to ensure adherence to these requirements.

JUNE's staff are regularly trained and expected to comply with this policy and all requirements implemented in the ISMS. All employees and if required external parties will be provided with the required training to comply with this policy and the security objectives.
The ISMS is subject to continuous, systematic annual review and improvement to comply with ISO27001 and Best-Practice-Security-Standards.
This Information Security Policy is documented, maintained, and reviewed periodically. Any changes are recorded and made available to all relevant personnel and stakeholders.

Henning Borchers, June 2024
Founder and Chief Executive Officer