SmartTrackers B.V.

Information Security Policy Statement
Christiaan Thijssen

15-02-2022

SmartTrackers B.V. provides SaaS solutions for accounting key performance indicators of their clients businesses, with a strong focus on sustainability, and supporting and simplifying formal certification processes.

The top management of SmartTrackers is committed to perserving the confidentiality, integrity and availability of all the information assets of the organisation. This especially applies to the data that is stored in our applications and the tools we use to provide the services to our clients.

SmartTrackers B.V. should focus on the information security to maintain its legal and contractual compliance, their competitive edge and their commercial image. We need to comply with the European GDPR for the personal data we store, but we also need to protect the, possibly strategic, business information of our customers.

SmartTrackers will implement and maintain an Information Security Management System (ISMS) based on the ISO 27001 standard and will periodically review the implementation and implement required changes to the system. Christiaan Thijssen and Peter van der Veeken will be the steering group of the ISMS project. The goal is to be ISO 27001 accredited in 2022. From this point on, the ISMS will continue to be maintained following the Plan-Do-Check-Act cycle.

Risks will be identified and will be classified based on impact and probability of occurance. For all the identified risks, it will be determined if the risk will be mitigated, accepted or transferred (for example by means of an insurance). When the risk mitigation requires additional actions, those actions will be assigned to an employee. This will all be administered in the ISO27001 survey of the SmarTrackers Assessments application. Christiaan Thijssen and Leo Smit will be responsible for the risk assessment.

Focus points of the ISMS will be: Update approaches and bug fix processes, a policy for Remote working, monitoring, incident resolving and reporting, backup plans, and preparing roll-over scenarios.
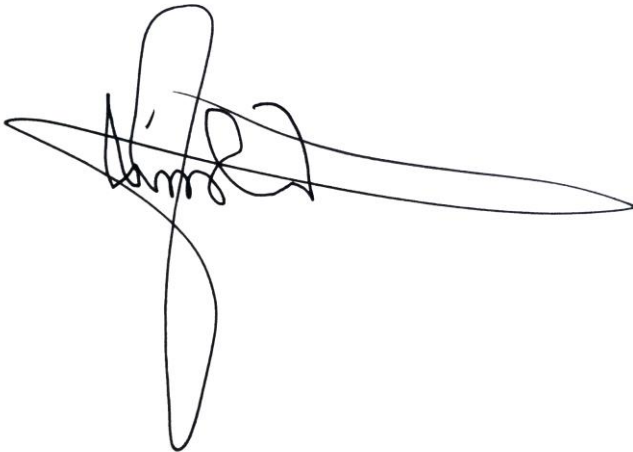
It is the responsibility of each employee to adhere to the information security policy. Employees will receive sufficient training about the subject of information security.

The policy covers (at least) the following topics:

- Beleid cryptographic controls

- Beleid teleworking

- Beleid testgegevens

- Beleid delen van gegevens

- Beleid incidentafhandeling

- Beleid nieuwe leverancier

- Beleid mobile devices

- Beleid toegangsrechten aanpassen Beleid nieuwe medewerker

- Beleid phishing

- Beleid bedrijfscommunicatie

- Beleid backups

- Beleid vertrekkende medewerker Beleid gebruikersaccounts

- Beleid beheer cryptografische sleutels Beleid clean desk + clear screen Beleid anti-malware

    - Beleid deployen naar productie

Signed:

--Leo

Smit, Director SmartTrackers B.V.

Date: 15-02-2022