Roadtrip Technologies B.V.

Information Security Policy

Roadtrip Technologies B.V.
Version: 1.1
Approved by management: approved by CPO

1 Context and goals

Roadtrip Technologies B.V. is the company behind Explorer, an innovative analytical tool for recruitment marketing. Explorer helps companies gain insights into the actual value of their recruitment marketing efforts and optimize them accordingly.

This policy document describes the information security management system (or ISMS) that our company uses. Anyone in our company (or at key positions at suppliers) that is handling confidential or sensitive data should be aware of this policy and act in accordance with it. Also, if anyone observes something in our company that is not in line with this policy, he or she should report this immediately. The entire management team of our company has been involved in creating this policy and is fully committed to making sure we are compliant.

2 Scope

The scope of the Roadtrip Technologies B.V. ISMS is:

> *Information security related to the development and operation of a platform for recruitment marketing insights*

The scope includes all processes, systems, and staff involved in handling, processing, or storing sensitive information related to our core operations and services.

Within this scope, we provide the following main activities and provides the following services to customers:

- **Integration of Application Data**: We integrate information about applications from ATSses with existing analytical tools, allowing us to attribute data regarding the quality of applications to specific marketing channels and the careersite.
- **Data-Driven Optimization:** We utilize this data to automatically send signals to marketing channels, optimizing recruitment marketing activities.
- **Consultancy Services:** We offer consultancy services based on the insights gathered from the collected data.

The following departments are in scope of this policy

- IT
- Sales & Marketing
- Customer Success

At this point in time, no departments or business activities have been specifically declared out of scope of this policy. Our company has the following office locations and working locations that are in scope of this policy:

- Main office: Oudwijkerveldstraat 67, 3581JH, Utrecht, The Netherlands

Roadtrip Technologies B.V. does not directly manage any data centers. DigitalOcean is used as provider of IT infrastructure.

3 Stakeholder analysis

The management team is responsible for maintaining regular contact with stakeholders, understanding the information security requirements and expectations from stakeholders and making sure that the ISMS is aligned with the stakeholder requirements and expectations. The resulting information is documented in the stakeholder analysis, which will be updated annually.

4 Leadership

The entire management is aware of the information security policy and is committed to support this effort on an ongoing basis. Jelmer Koppelmans is the management representative that interfaces directly with the security team.
There is an information security team that is responsible for implementing and maintaining information security.
All other staff of the company are regularly updated by the information security team and are responsible for following policies and guidelines.

5 Resources, awareness and training

Management is responsible for making sure employees executing information security tasks are knowledgeable on the subjects they work on. They receive security awareness training after onboarding, and after that again at least once a year. Staff involved in product design and development or staff with additional security responsibilities will receive additional training suitable to their role.

6 Operations

Roadtrip Technologies B.V. has a register of goals and objectives (E14 - Roadtrip Objectives and monitoring.xlsx). These goals are established by top management, and reviewed on an annual basis. When establishing these goals, top management makes sure to include the organizational context and stakeholder requirements.

7 Performance evaluation

The management team will review that effectiveness of the ISMS annually in a management review. If needed, external support will be sought by external partners, such as additional technical advice, independent security testing, or audits by independent parties.

8 Continuous improvement

The management is committed to continuously improving the information security management system.