Information Security Policy 2021

SOWISO B.V, including its trademarks
- Bolster Academy
- Online Mathematics Placement Test
- PassYourMath

Version: 2.04 - January 2021
Owner: Max Cohen, CTO
Confidentiality level: Public
Approved by management

1 Context and goals

Founded in 2010, SOWISO provides an interactive, personalized and adaptive e-learning technology for mathematics and other exact sciences. SOWISO is currently faced with the following external issues:

- Digitalisation of higher education, especially the need to do digital examinations. This is a growth opportunity for SOWISO but also means that SOWISO will manage more confidential personal data, like individual test results.
- Customers are more aware of security and privacy. This leads to more detailed questions about SOWISO security measures and procedures
- Increased popularity of learning analytics: people (students, teachers) are interested in data about the learning process. This means that we track and store more data.

Next to that, SOWISO has the following internal issues:

- International growth. SOWISO is expanding, and intends to expand, into other European countries and North America. International clients have new or different needs when it comes to security and privacy and may require more detailed agreements.
- A need to improve and extend the current course content. This requires an effort from authors, developers and sales and marketing to understand what content is needed and how it can be evaluated.
- Growth from diversifying from pure mathematics to STEM. This may require new question types, different content and in general an increased need to handle content securely.

The vision of SOWISO is to continuously improve the STEM learning experience through digital technologies.

The SOWISO strategic objectives for 2020 and 2021 are summarized as follows:

1. Scale, in terms of; users, revenue, employees, content.
2. Product. Offer the best solution in our niche e-learning platform for STEM in higher education.
3. Content. Deliver high quality content. Our educational material should be top notch.
4. Customer success. Help our partners be successful.

Information security is an important aspect of our business in all aspects: We need to protect the data from our own company, our customers and users of our technology.

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. This can be done either by informing our information security officer, or to any member of the security team. The entire management team of our company has been involved in creating this policy and is fully committed to making sure we are compliant.

1 Scope

The scope of the SOWISO information security management system is the development and provisioning of e-learning solutions.

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

- The SOWISO platform and digital math courses, including our brands Bolster Academy, OMPTest and PassYourMath
- Custom software development
- Entrance / Placement tests for students

The following departments are in scope of this policy:

- Marketing & Sales
- Research & Development
- IT
- Customer service

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: Science Park 402

SOWISO does not directly manage any data centres. Amazon Web Services and Google LLC are used as a provider of IT infrastructure.

2 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. The stakeholder analysis will cover at least:

Customers
Users
Regulatory requirements such as GDPR

The CEO stakeholder analysis falls under the responsibility of the CEO.

3 Leadership

The entire management is aware of the information security policy and is committed to support this effort on an ongoing basis. Max Cohen 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 is regularly updated by the information security team and is responsible for following policies and guidelines.

4 Risk assessment and treatment

The security team uses a methodology for continuous improvement. Using this methodology, the security team is aware of the company goals, defines actions, checks if the actions are effective and makes changes if needed. The methodology chosen is Plan-Do-Check-Act, a well-known methodology also referred to as the Deming cycle (https://en.wikipedia.org/wiki/PDCA). The risk assessment and treatment falls under the responsibility of the CTO.

5 Resources, awareness and training

The 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

We maintain concrete measurable goals to assess the health of our ISMS that are periodically reviewed and updated. These goals are managed by the CTO and stored in document 'KPI's en Doelstellingen'

7 Performance evaluation

The management team will review that effectiveness of the ISMS annually in a management review. The CEO is responsible for maintaining an internal audit programme that establishes whether the ISMS conforms to ISO 27001:2013 and SOWISO's own requirements.

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 improve the information security system. This is done by documenting and analysing stakeholders, consulting external sources of expertise.

9 Appendix 1: Information Security team composition

The team consists of the following roles:

1. CTO
2. CEO
3. Security Officer

The team can be extended with other senior staff members if needed.