Simacan Information Security Policy

rev. version/2019.2-3-gcdb0

Simacan

simacan

Contents

Information Security Policy (0007)

Key	Value
Confidentiality label:	Public
Reference:	ISMS-0007
Author:	Ruggero Montalto, Simke Kamphorst
Owner:	Simacan BV
Reviewer:	Management Team
Distribution:	All Simacan employees, available on Simacan's website to any third party interested www.simacan.com/security

1 Introduction

Information should always be protected, whatever its form and however it is shared, communicated or stored. Simacan has many critical information assets which are crucial in conducting business, maintaining customers' trust, and keeping the future of the company strong. The present policy outlines Simacan's commitments to its employees, its customers, and its suppliers, regarding how all business-critical information assets will be handled by Simacan.

Information can be sensitive by its nature, and can also be sensitive due to regulations and industry standards. Sensitive information can include: customers' information, financial information, business records and planning materials, copyrighted materials, both which Simacan creates and those which Simacan obtains under license from others, company patents, business plans, and several other types of intellectual property.

Information may reside on Simacan's computing (cloud) systems, online and offline, it may traverse the networks, be on paper, or even be in people's minds. All these locations must be properly controlled.

The rules by which information is handled are determined by laws and regulations, business requirements, and the commitments Simacan undergoes with its customers and employees.

Every Simacan employee, every customer, every supplier and every partner must be aware of the significance of the information being handled, and ensure that proper controls are applied to prevent unauthorized disclosure, loss or lack of accessibility of the information.

This Information Security Policy is part of the overall security and privacy effort carried out by Simacan. Other policies and controls may also apply, these are available in the Handbook of Information Security and at the company's backoffice.

Penalties for violating these policies may include disciplinary actions up to termination of employment, or termination of the business relationship with Simacan.

Simacan relies upon employees, customers, suppliers and partners to properly develop, maintain, and operate its systems, networks, and processes which keep sensitive information safe and properly used. This means that every person and organization handling Simacan's information has the responsibility to keep the information safe, no matter where the information is located. This includes computing systems, networks, paper copies, business processes, and verbal transmission of information.

2 Information Security Policy

2.1 Scope

This policy supports Simacan's general security policy and applies to all of the organization as well as to external parties who are stakeholders in the activities of Simacan's Information Security Management System (ISMS).

Simacan will meet all applicable requirements in properly protecting the information, including laws, regulations, industry standards, and contractual commitments with employees, customers, and suppliers.

2.2 Information Security Objectives

- Provide a SaaS service where the customer's information is safe. (*Het leveren van een SaaS dienst waar de informatie van de klant veilig is.*)

- Increase the market value of our demonstrably secure SaaS products. (*Bijdragen aan de marktwaarde van onze aantoonbaar veilige producten.*)
- Comply with applicable information security-related laws and regulations. (*Het voldoen aan toepasselijke wet- en regelgeving rondom informatieveiligheid.*)
- Comply with the ISO27001 standard and maintain our certificate. (*Het voldoen aan de ISO27001 standaard en het behouden van ons certificaat.*)

Next to the above mentioned general objectives Simacan has a list of specific objectives (KPI Dashboard), these objectives are monitored by the Management Team.

2.3 Information Security Principles

Simacan tolerates risks that might not be tolerated in conservatively managed organizations, provided that information risks are understood, monitored, and treated when necessary.

1. All Simacan employees will be made aware and accountable for information security as relevant aspect of their job-role. A clause is included in each employee's contract concerning their responsibility for the confidentiality of customers' data, and at the start of employment, every employee receives an ISMS awareness training, concluded by a signed acknowledgement that he or she is aware of the information security principles therein.
2. Provisions will be made for funding information security controls in operational and project management processes.
3. The possibility of dangerous, abusive, or malicious use associated with information systems will be taken into account in the overall management of information systems.
4. Information security status reports will be available.
5. Information security risks will be monitored and action taken when changes result in risks that are not acceptable.
6. Systematic criteria for risk classification and risk acceptability will be adopted in Simacan's ISMS.
7. Situations that could place the organization in breach of laws and statutory regulations will not be tolerated and will always result in immediate action towards a solution.

2.4 Responsibilities

1. Simacan's management is responsible for ensuring that information security is adequately addressed throughout the organization.
2. Simacan's management is responsible for ensuring that all people working under their control protect information in accordance with the policies, the procedures, and the standards embraced by Simacan.

3. The CISO advises the management concerning information security related matters, provides support and training for the employees, and ensures that information security status reports are available.
4. Every Simacan employee undergoes information security responsibilities as part of their employment contract with Simacan.

2.5 Key Outcomes

1. Information security incidents will not result in serious disruptions of service for the customers or business activities for Simacan.
2. Concerns about information security will not adversely affect the customer's acceptance of Simacan's products.
3. Information security incidents will not result in serious unexpected costs.
4. Losses will be known and will be kept within acceptable bounds.
5. Continual improvement of the information security management system.

2.6 Related Policies

The protections Simacan applies to information assets will be in proportion to the value and sensitivity of the information,. They will balance the sensitivity of the information against the impact of the controls on the effectiveness of business operations and the risks of disclosure, modification, destruction, or unauthorized use of the information.

Simacan will protect all types of sensitive information, and will ensure that these controls are accepted by all employees, customers, suppliers, partners, service providers, representatives and associates of our company who may have access to our information. This includes ensuring that all personnel at all levels are aware of, and are held accountable for safeguarding information assets.

Simacan will ensure that access to information is controlled, and based upon job function and need-to-know criteria. Simacan will maintain proper business continuity and security procedures, including information systems, networks, resources, and business processes.

Simacan will comply with other related policies, regulations and laws, including the Dutch and the European privacy policies, and will report any suspected or actual breach of these policies, and will cooperate with investigative agencies.

The following detailed policies provide principles and guidance on specific aspects of information security. These are internally available at Simacan's office.

- Simacan's Handbook of Information Security;
- Simacan's Handbook of Internal Procedures.

3 Privacy Policy for Employees

Simacan values each employee, and so has a commitment to protect the personal information which it handles on behalf of the employee. It is Simacan's policy that:

- Simacan will collect only that information about employees which is needed and relevant.
- Simacan will strive to make certain that personal information about employees is kept accurate and up-to-date.
- Simacan will use appropriate controls to ensure that this information is kept secure, and is only viewed or used by the proper personnel.
- Information about employees will not be disclosed to any external parties unless appropriate.
- Employees will be told how they can review information about them, make updates, and report problems.
- Simacan will comply with applicable laws, regulations, and industry standards when protecting employee information.
- Simacan holds her employees, vendors, contractors, suppliers, and trading partners to meet this same set of policies.

4 Privacy Policy for Customers

It is a part of Simacan's core values that Simacan will properly value and protect any information entrusted to it about its customers. This policy describes how we will safeguard personal and company information, to ensure peace of mind when dealing with Simacan. It is Simacan's policy that:

- Simacan will collect only that information about customers which is needed and relevant.
- Simacan will not disclose information to other parties unless customers have been properly notified of such a disclosure.
- Simacan will strive to make certain that information about customers is kept accurate and up-to-date.
- Simacan will use appropriate controls to ensure that this information is kept secure, and is only viewed or used by the proper personnel.
- Simacan will comply with applicable laws, regulations, and industry standards when protecting customer information.
- Simacan holds its employees, vendors, contractors, suppliers, and trading partners to meet this same set of policies.