GENERAL POLICY for INFORMATION SECURITY SYSTEMS

Document Control

Document	
File Name	PGM05.1 - GENERAL POLICY for INFORMATION SECURITY SYSTEMS – GP-ISS
Doc. reference	ISMS-DOC-PGM05.1

Version Control				
Version	**Date**	**Author**	**Release Type**	**Changes**
ISMS-DOC-PGM05.1	06/10/2021	Hassan LAHOUIRI	PGM05.1	General Information Systems Security Policy

Document Approval		
Name	**Role**	**Signature**
Frédéric SIPAHI	Chief Executive Officer	08/10/2021
Jean-François KOEGLER	Chief Information Officer	06/10/2021
Hassan LAHOUIRI	Information Security Manager	06/10/2021

Document Distribution R=Read, N=No Access, WS=Read/Write/Sign, W=Read/Write, RS=Read/Sign, O=Owner			
Name	**Organization**	**Role**	**Permission**
WW	Sogefi Group	End User	R
IT-Security Team	Sogefi Group	Document Owner	Owner

Document Administration

Terms and Conditions

The contents of this Document are both privileged and confidential and may not be disclosed, copied, modified or transmitted (in full or in part) without the express authorization of SOGEFI Group Management or the document Owner.

Document review Process

This document will be reviewed at least annually as part of the group information security policy review, which is the responsibility of the Group Information Security Officer. This document may be reviewed periodically by internal and external auditors.

It may also require review in response to any significant changes in the organizations data, processes and/or architecture.

Target Audience

This policy document should be communicated to all SOGEFI Group employees in all regions. While it is not necessary to make the actual document available to employees and partners, the contents of this document must be communicated via recurrent training and information sessions and the full document should be available anytime to the employee who wish to reference it.

Effectiveness

This policy shall be effective as from the day following the approval date.

Related Documents

POM05.2 - Policy - Information Security Policy

Table of content

1 CONTEXT OF THE ORGANIZATION

1.1 Commitment of general management

As a modern, forward-looking business, SOGEFI GROUP recognizes at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, SOGEFI GROUP has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001 and VDA recommendations on information security in the automotive industry (TISAX)

The operation of this ISMS has many benefits for the business, including:

- Protection of revenue streams and company profitability
- Ensuring the supply of goods and services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements

An Information Security Policy is available in both paper and electronic form and will be communicated within the organization and to all relevant stakeholders and interested third parties.

Commitment to the delivery of information security extends to senior levels of the organization and will be demonstrated through the information security policy and the provision of appropriate resources to establish and develop the ISMS.

Top management will also ensure that a systematic review of performance of the program is conducted on a regular basis to ensure that information security objectives are being met and relevant issues are identified through the audit program and management processes.

1.2 Background

SOGEFI is a company constantly in search of innovations because it evolves in the field of new technologies. The SOGEFI company designs solutions for its customers in the Automotive sectors.

By strengthening its presence at trade fairs and in clusters, SOGEFI increases its visibility with potential customers, but also exposes itself to its main competitors.

SOGEFI's know-how needs to be protected against external threats. To do this, SOGEFI has decided to put in place policies and measures that meet the criteria of security, availability, integrity and confidentiality.

SOGEFI has 40 physical sites in 23 countries. It employs more than 6,500 people.

1.3 Definition of issues

1.3.1 Internal issues

- Create and disseminate an information security culture,
- Protect the company's know-how against any loss of confidentiality and integrity,
- Control strategic and operational risks,
- Ensuring continuity of service to customers.

1.3.2 External issues

- Respect customer requirements in terms of compliance,
- Protect the confidentiality of customer information,
- Promote the safety approach in order to gain access to new markets.

1.4 Definition of objectives

By defining its safety management system, SOGEFI has set itself the safety objective:

- **OBJ.01** Increase the maturity, in terms of security, of the company by obtaining TISAX certification in 2022
- **OBJ.02** Ensure the availability of business services
- **OBJ.03** Protect the confidentiality of data entrusted by customers and protect access to business platforms
- **OBJ.04** Ensure traceability of operations

1.5 Interested parties

The implementation of the ISMS must aim to ensure for the interested parties the respect of the following expectations:

Source	Title	Requirements
External	All customers	• Respect customer requirements in terms of compliance • Protect the confidentiality of customer information
External	Regulation authorities of each country where SOGEFI is present	• Compliance with the laws and regulations in force
Internal	All employees	• Internal trust and respect for a quality work climate
Internal	Direction	Investment protection Protection of SOGEFI's image

2 ORGANIZATION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

2.1 Field of application : Definition and scope of ISMS

Systematic control and review of information security is achieved through the establishment, operation and development of an Information Security Management System (ISMS). The ISMS defines processes and procedures in order to achieve information security objectives that concern the confidentiality, availability and integrity of company assets on the basis of a security policy.

ISS governance applies to the SOGEFI entity, and to persons contractually attached to SOGEFI This scope includes the following sites:

World Sites Contact

SOGEFI's ISMS excludes entities: ISSA joint venture (Spain NULES and ALSASUA sites)

2.2 Declaration of applicability

To protect information assets and manage information processing facilities, the Statement of Applicability indicates which TISAX controls and policies are enforced by the organization. It is an integral part of the mandatory documentation that must be presented to an external auditor when the ISMS is subject to an independent audit. The exclusions of the Declaration of Applicability are systematically justified.

The declaration of applicability is formalized by document VDA-ISA_EN_5.0.4

2.3 Security Policy

The information security policy is a set of requirements rules applied to the ISMS, resulting from risk analysis and related risk coverage measures.

The details of the requirements are formalized in the document PSSI_SOGEFI [10/2021].

2.4 Roles and responsibilities on the ISMS

The sponsor

The general management of SOGEFI is involved, as a sponsor, in the ISMS to keep it up to date and improve it.

SOGEFI's CEO is responsible of the ISMS, he must:

- Chair the Information Security Steering Committee (ISSC)
- Approve this GENERAL POLICY for INFORMATION SECURITY SYSTEMS (GP-ISS), as well as the Information Systems Security Policy (ISSP)
- Ensure that information security objectives are established and are compatible with SOGEFI's strategy
- Ensured the integration of the ISMS
- Provide guidance on their choices and priorities in relation to the Information System
- Validate the Information System and all decisions relating to security with the IS and Infrastructure Manager

The ISMS Manager

The SOGEFI ISMS must:

- Communicate the sponsor's guidelines on Information Security, based on:
  - business strategy,
  - the overall risk management strategy,
  - the security risks identified by SOGEFI.
- Report on the effectiveness of the ISMS
- Organize and lead the management review, the Information Security Steering Committee (ISSC) and the ISMR and ISMB meetings
- Bring up the subjects raised during the ISSSC for the sponsor's decision to be made;
- Ensure that the GISSP and the ISSP are well communicated to all employees of the organization;
- Monitor performance indicators and the progress of the ISMS action plan;
- Analyze the conclusions of the audit reports, formalize an action plan and address to the sponsor;
- Supervising the document review and validation process by the sponsor.
- It proposes, for arbitration and validation, the IS orientations to the sponsor of SOGEFI during the management review.

The Chief Information Security Officer (CISO)

SOGEFI's CISO sets out the overall information system security strategy by:

- Identifying the appropriate annual and multiannual action plans;
- Building and updating the risk analysis;
- Defining the security requirements to be applied to cover the major risks identified;
- Defining operational security control objectives to measure the application and efficiency of security requirements;
- Collecting performance indicators and keeping the action plan up to date;
- Supervising the implementation of IS security measures;
- Overseeing security incident management processes and associated corrective and preventive actions.
- Reporting to the sponsor:
  - the level of coverage of IS security risks identified by SOGEFI,
  - the new risks identified,
- During operational committees, ensuring that supporting documents are available, proposing agendas and drafting meeting reports in the form of information reports, actions and decisions;
- Ensuring periodic revisions of technical documents, in accordance with the document management policy.

- He proposes, for arbitration and validation to the sponsor, the changes to be made to the action plan during the year.
- He operationally steers the action plan and coordinates the various ISS contributors on a daily basis.
- In case of detection of an anomaly or an information security incident, it supervises the processing and, if necessary, alerts the departments concerned and / or the competent persons.

Collaborators

All employees within the ISMS perimeter must:

- Respect the entirety of the PSS
- Be aware of security
- Report incidents to the RSSI or ISMS
- Participate in the construction of risk analysis and risk coverage plans

The Data Protection Officer (DPO)

The DPO must:

- Ensure the compliance of the company's personal data with the general data protection regulations (GDPR).
- Ensured that the processing register was kept up to date.
- Inform the general management of potential non-conformities with the GDPR.

Asset owners

The purpose of the following rules is to set up and maintain appropriate protection for the assets of the SOGEFI Group and its customers:

- During the risk analysis, each department manager carries out and maintains an inventory of all the information assets essential to its proper functioning. This inventory includes in particular internal technical data, customers as well as financial and commercial data.

- Support assets are also identified: systems and network infrastructure equipment, applications, database, etc.

- Each asset has a designated owner;

The owner of an asset:

- Is responsible for the maintenance of this asset, its control, its classification in terms of confidentiality and its protection;

- Defines the rules allowing the use of this asset under good security conditions. These rules are documented in the ISMS (policies, procedures, instructions, charters and safety standards);

- Enforce these rules and monitor their implementation.

Risk owners

Each department manager is responsible for the choice of risk treatment methods on the assets of which he owns, for validating the action plans intended to deal with these risks and for allocating the resources necessary for carrying out the plans. actions.

Indeed, the role of risk owners is assumed by asset owners.

3 MANAGEMENT OF THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

3.1 Comitology

The ISMS information security management bodies are:

- ISSC (Information Security Steering Committee), carried out annually, in the presence of the sponsor. It is the decision-making body of the sponsor for monitoring the risks and monitoring the maturity of the ISMS.

- The ISMB (Information Security Meeting Build), monthly, including department managers. It represents the technical monitoring of action plans, security solutions and operational aspects of risk analysis, as well as security indicators.

- The ISMR (Information Security Meeting Run) monthly deals with security incidents, change management, etc.

Committee	Frequency	Participants	Agenda	Deliverables
ISMR (Run Meeting)	Monthly	IT Security Team CIO Service managers	• Security incident management • Change management • Follow-up of CPSSI reviews and CR checks (email possible)	ISMR Meeting Minutes
ISMB (Build Meeting)	Monthly	IT Security Team CIO Service managers	• Monitoring of ISMS indicators • Monitoring the progress of action plans • Monitoring risk treatment plan	ISMB Meeting Minutes
ISSC	Annual	ISSC Sponsor	• Review of the performance of the ISMS over the past year • Review of safety objectives and action plans for the coming year CR of RDD	ISSC Meeting Minutes

3.2 Document management

Document management follows a formalism for IS documents which are:

- Policies
- Procedures
- Technical instructions (operating modes)
- Records

For each of these documents, it is necessary to set up:

- Unique identification
- A cycle of creation, modification, approval and validation
- A classification in terms of confidentiality, according to four levels: public, internal, restricted and confidential
- Their shelf life and storage time

Documentation should be reviewed on a regular basis. All of these rules and practices are defined within the document management procedure P-07.3 Management of documented information.

3.3 Evaluation of performance

3.3.1 KPI

KPIs are indicators that make it possible to measure objectives. They are built by all the players in the ISMS perimeter, consolidated by the ISMS Manager and presented during security meetings All KPIs are centralized in IT Security PowerBI Dashboard

3.3.2 Internal and external audits

The purpose of the following rules is to ensure the compliance of information systems with SOGEFI group security policies:

- Security audits on projects can be carried out by the ISMS Manager, in order to verify that the activities carried out comply with the Group's security policies and rules;
- The compliance of the ISMS with the requirements of the TISAX standard is verified annually (minimum).

- Security audit and information systems security testing activities are planned to minimize the risk of business process disruption.
-

3.3.3 vs. Checks and revisions

During the year, checks and reviews are decided upon with employees during the weekly meeting.

The methodology chosen is as follows:

- Appointment of a person within a team,
- The designated person must take ownership of the target perimeter before carrying out the control of an ISMS subject,
- It carries out the inspection report before communicating it to the RISMS,
- The employee presents the results obtained during the following weekly meeting,
- The RISMS takes into account the results and supplements the safety improvement plan, if necessary.

In addition, all operational controls and reviews (review of system, application, network rights, PCA test, backup tests, etc.) are centralized in the file" Programme audits, revues et contrôles"

All documents, policies and procedures must be reviewed annually and validated during the management review.

3.4 Communication

Communication on internal and external issues of the ISMS is defined towards the interested parties.

The GP-ISS is communicated to business partners who request it or when a major change is deployed.

Internally, communication is carried out through:

- Regular awareness emails,
- Information during weekly meetings and various steering committees

Communication to the relevant interested parties (ANSSI, CNIL, Press) is also integrated into the crisis management process.

3.5 Continuous improvement

3.5.1 Management of non-conformities and corrective actions

Non-conformities are identified during internal and external audits, and continuously by employees. each non-conformity must give rise to a treatment:

- Root cause analysis
- Formalization of the correction
- Definition, presentation and validation of the corrective action plan with the CPSSI.

The summary of non-conformities is presented to the sponsor during the ISMR(Meeting Run).

3.5.2 Improvement action plan

A global action plan centralizes the various security projects, decided on from different sources: risk analysis, steering committees, results of audits, security incidents, vulnerabilities ...

4 Risk Identification and management

A risk analysis is carried out annually by the ISMS, It is based on the principles of the EBIOS methodology.

Its purpose is to identify and assess the gross risks, then to verify the effective reduction of the risks treated, to accept the level of residual risk, to take into account the new risks, to analyze the exemptions and to adjust the action plan if necessary.

An intermediate review can be triggered at the request of the steering committee outside of the annual planning, in the event of an event likely to have a significant impact on information security: major change (move, regulatory change, change organizational), critical security incident, etc.

4.1 Identification and assessment

The risk analysis at SOGEFI is based on the identification of:

- Essential assets and their classification,
- Inventory of support assets
- Analysis of attack scenarios on support assets made up of vulnerability and threat
- The characteristic of the risks which are the composition of the likelihood of the attack scenario with the impact on the essential asset

The acceptance criteria are determined in the scales defined in the risk analysis document.

The risk owners are defined and specified in the risk analysis.

4.2 Risk treatment plan

Once the risks have been assessed, the organization must propose a set of action plans to reduce these risks. These action plans are taken with reference to the control points of the TISAX standard.

All of these points must be regularly accepted by the sponsor during successive COSSIs and management reviews.

4.3 Review of risk analysis

Achievement criteria:

The risk analysis must be reviewed regularly, as well as at the end of any event that may affect the impact or likelihood factors of any risk. The change of the risk analysis is carried out on:

- major change,
- critical incident,
- monitoring and information relating to vulnerabilities,
- scheduled periodic reviews,
- results of audits and controls.

The following events should be taken into consideration during reviews:

- New security controls implemented since the last risk assessment,
- Incidents that have occurred since the last risk assessment within the scope of the analysis.

5 Exceptions

All of the rules set out in the GP-ISS (General Policy for Information Security Systems) constitute security requirements that must be observed.

However, exceptionally, exceptions may be established within a specific framework:

- Request expressed by an employee and formal approval of the CISO or ISMS sponsor in the form of a waiver sheet

- Keeping of a register of exemptions by the CISO

- Each exemption is limited in time and its relevance must be subject to regular monitoring, particularly during ISMR (Run Meetings). This monitoring is integrated into the control, audit and review plan