SECURITY POLICY

DOCUMENT CONTROL

Document information

Classification:	Public
Circle of distribution:	
Version number:	1.0
Document title:	Security Policy
Responsible for document:	Matthias Klinski
Approval:	Board of directors
Inspection interval:	Annually

Approval

As a result of the board's approving and implementing the "Security Policy", all employees are obligated to comply with the information security management system (ISMS) specifications and to put the rules into practice.

Karl Weidlinger	Adolf Scheuchenpflug
Peter Gal	Walter Pertl

DOKUMENTENLENKUNG

Dokumenteninformation

Klassifikation:	Öffentlich
Verteilerkreis:	
Versionsnummer:	1.0
Dokumententitel:	Sicherheitspolitik
Dokumentenverantwortlich:	Matthias Klinski
Freigabe:	Vorstand
Revisionsintervall:	Jährlich

Freigabe

Durch die Freigabe und Inkraftsetzung der „Sicherheitspolitik“ durch den Vorstand sind alle Mitarbeiterinnen und Mitarbeiter verpflichtet, sich an die Vorgaben des Informationssicherheitsmanagementsystem (ISMS) zu halten und die Regelungen umzusetzen.

Karl Weidlinger

Adolf Scheuchenpflug

Peter Gal

Walter Pertl

TABLE OF CONTENTS

1 INTRODUCTION

As one of the leading companies in Austria's construction industry, SWIETELSKY is committed to its employees, customers and contractual partners to implement the highest standards throughout all group units.

Due to the legal requirements imposed on the company, and also because of commercial needs, close attention is therefore paid to information security within the company.

SWIETELSKY defines information security as the protection of physical and electronic information as well as the systems necessary to process information with regard to their confidentiality, integrity and availability.

2 SCOPE OF APPLICATION

The scope of this Security Policy covers Swietelsky as a group and its subsidiaries with all their employees, locations and services.

3 PRINCIPLES

3.1 By order of management

The SWIETELSKY Board of Directors hereby adopts the Information Security Policy as an integral part of its corporate strategy.

The board supports the goals and principles of information security in line with the business strategy and business objectives.

By establishing an Information Security Management System (ISMS) and providing the necessary resources, the board of directors is laying the groundwork for achieving the goals of the ISMS. As the highest governing authority of the ISMS, the board of directors actively contributes to the success of the ISMS.

3.2 The significance of information security

SWIETELSKY's business operations largely depend on the availability of information and increasingly on its information systems working properly. Information processing and digitalisation is becoming more and more important in the construction industry. Networks within the company as well as with customers, suppliers and joint ventures lend support to the provision of services to a considerable extent. Core system failures can cause damage to the business as well as to SWIETELSKY's reputation within a short amount of time.

Information security creates the necessary trust, both internally and towards customers and partners, to further advance digitalisation and to address the risks it poses. For this reason, the board of directors (or a coordinator appointed by the board) actively pursues information security in terms of legal, technological, and organisational matters.

4 ORGANISATIONAL CONTEXT

In 1936, Dipl. Ing. Hellmuth Swietelsky founded the construction company. Today, SWIETELSKY AG is one of the most important companies in Austria's construction industry, employing a workforce of more than 10,000 on average.

With subsidiaries in 4 core countries (Austria, Germany, Czech Republic, Hungary) and 15 other countries, SWIETELSKY is a privately held company. SWIETELSKY'S operations cover all branches of the construction industry. The Group offers projects of any dimension with the highest quality and flexibility, while always adhering to schedules.

"Profit centre decentralisation, delegated responsibility and profit participation has inspired our motivated and competent employees to have the mindset of entrepreneurs in the company." – The philosophy of SWIETELSKY

4.1 Internal context

SWIETELSKY is a decentralised organisational structure with various independent divisions operating throughout Europe and Australia. Common services, such as personnel, finance or IT, are managed centrally.

In order to fulfil customer wishes, tender requirements and to control measures, SWIETELSKY also operates other management systems in addition to ISMS. These are operated independently by the respective coordinator, whereby regular coordination ensures that the management systems work in unison.

4.2 External context

SWIETELSKY'S operations cover all branches of the construction industry. In order to fulfil its tasks, it is necessary to closely cooperate with various suppliers, clients, subcontractors and other competitors in the form of joint ventures.

5 INTERESTED PARTIES

There are various interested parties that have requirements of an ISMS from SWIETELSKY.

5.1 Contracting parties (customers, suppliers, joint ventures)

Contracting parties can reasonably expect that due care is given to their data when handled and also that, above all, operations run smoothly, ensuring the availability of the services.

5.2 Internal parties (business units, employees)

Internal parties expect services that work and are available at all times. Downtimes should be kept as short as possible and should never be unscheduled. Security should take place in the background and, if possible, should not influence or complicate the tasks at hand. Occasionally, confidentiality demands high standards.

5.3 Shareholders (management, owners)

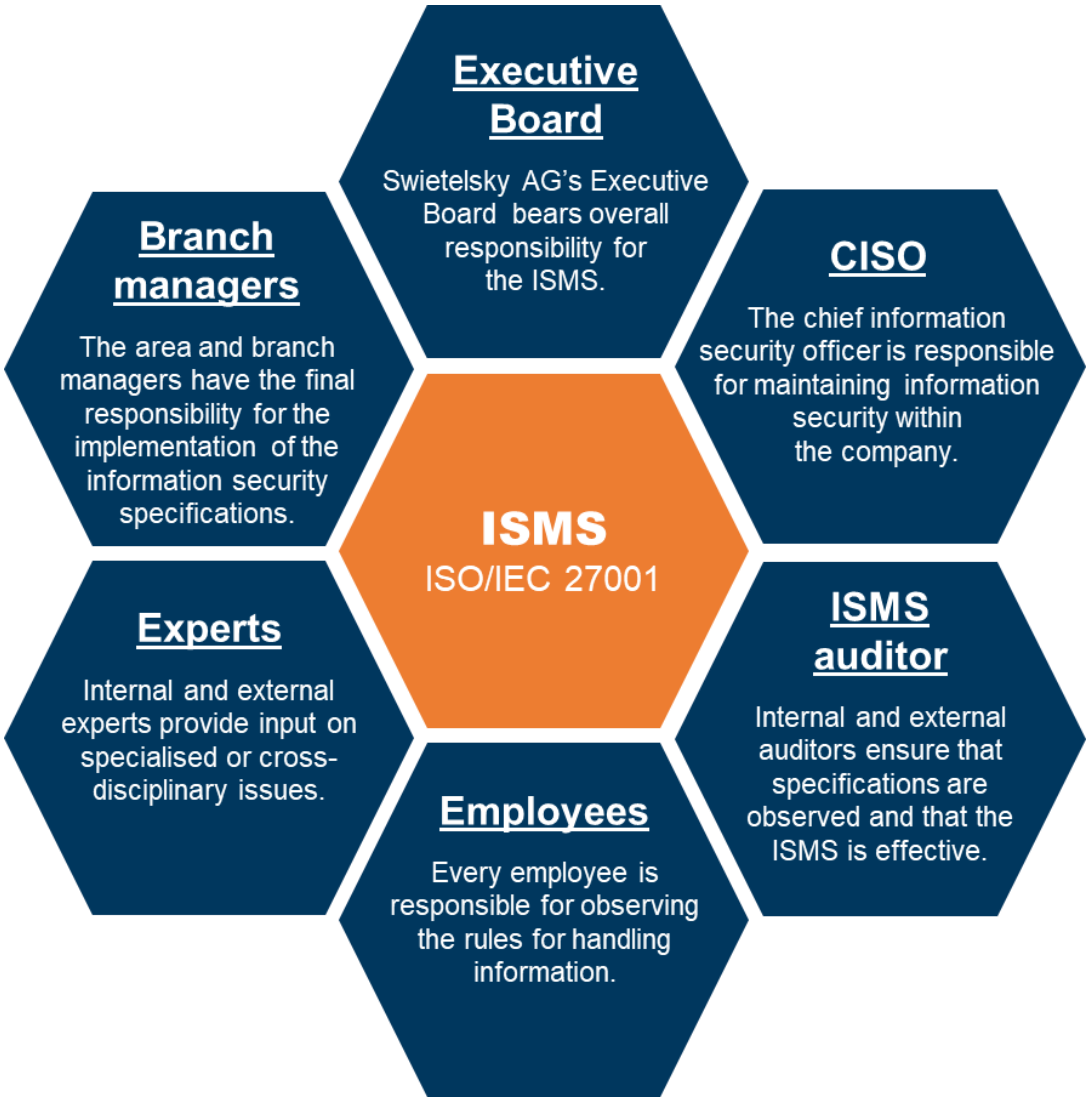
Shareholders expect to be protected against business, legal and reputational risks. The ISMS is meant to use resources more efficiently, with certification generating competitive advantages.

5.4 Public administration (authorities, legislators)

Public administration expects all laws to be abided by. All transmitted information must arrive correctly and completely in due time at the public authority.

6 ORGANISATION

The following key roles and responsibilities are defined for the ISMS:



7 GOALS

The goals of the ISMS are derived from the principles of SWIETELSKY's Code of Conduct.

The strategic objectives of the ISMS described here are assigned to the operational objectives. They are measured annually using KPIs.

7.1 We protect the assets of the company

7.1.1 Avoiding unscheduled downtime of central IT services

Failures of centralised services can have an impact on business operations within a short amount of time and lead to financial loss.

7.1.2 Preventing financial loss from cybercrime

Criminal activities via electronic media can cause serious financial damage.

7.2 We treat business documents and information confidentially

7.2.1 Protecting the confidentiality of information

Unintentionally disclosing or publishing information can have a critical impact on SWIETELSKY's reputation and have legal ramifications and contractual implications.

7.3 We observe IT security and data protection standards

7.3.1 Establishing a state-of-the-art IT level of security

By establishing an ISMS and aligning security measures according to ISO/IEC 27001 as well as an external certification, we prove to third parties that we have a state-of-the-art level of security.

7.4 We continue to develop

7.4.1 Raising awareness among the workforce

Continuous training courses are the basis for further developing the awareness of Swietelsky's employees.

7.4.2 Continuously improving the ISMS and security measures

The establishment of a continuous improvement process as part of the ISMS ensures that existing measures are constantly evaluated and further developed and that new, risk-based measures are identified.

8 IMPLEMENTATION

To implement this Security Policy, the following core components and processes are established within the ISMS:

9 ISO/IEC 27001 SCOPE

Although the scope of this Security Policy and the ISMS covers the entire organisation, external ISO/IEC 27001 certification is limited to the following scope:

The ISMS scope includes the company-wide provision and operation of central IT services and the therefore needed infrastructure in Austria.

Services

The central IT services and the operation of the IT infrastructure are the relevant services for the scope of application.

Processes

The IT operations process is considered the primary object of consideration for the tasks within the scope of application.

Department/units

The IT & Processes unit with the IT User Service, IT Infrastructure, ERP & Processes and Cyber Security departments are responsible for the scope of application.

Locations

The scope of application includes central IT offices, server and backup rooms as well as IT backup locations in Austria.

Interfaces

Within the scope of application, various interfaces closely cooperate, such as HR, quality management, digitisation, facility management, legal as well as service providers and outsourcing partners.

IT systems & applications

The scope includes mobile and stationary IT equipment, storage solutions and related backups, access control and user administration, as well as construction and personnel software.

Legal units

All processes, persons, departments and locations relevant to the scope of application are part of SWIETELSKY.

Information

The scope of application includes all information relevant for providing services.

APPENDIX
VERSION HISTORY

Date	Author	Version	Description
13/07/2020	Matthias Klinski	1.0	Initial preparation