1. Starting point and scope

Wyssen Seilbahnen AG is certified according to the ISO/IEC standard 27001:2022 and is committed to fulfilling these requirements. The scope of the certification includes:

- The scope of the ISO/IEC 27001:2022 certification applies to Wyssen Seilbahnen AG, Wyssen Avalanche Control AG, Wyssen Austria GmbH, Wyssen Norge AS, Wyssen Canada Inc., Wyssen USA Inc. and Wyssen Chile SpA (Wyssen Group).
- All employees
- All processes

2. Information security objectives

The Wyssen Group has set itself the following goals:

- IT has 99.9% availability.
- Ensuring the backup strategy for the data of the Wyssen Group and its customers (WAC.3®)
- Successful introduction and continuous improvement of ISO/IEC standard 27001:2022 as an everyday tool for information security.

3. The ISMS of the Wyssen Group

The Wyssen Group's Information Security Management System documents all procedures and rules that serve to ensure the information security of the Wyssen Group against its stakeholders. The ISMS is communicated on an ongoing basis and training is provided at the appropriate level. The application of these regulations is mandatory and binding. The ISMS policy is supplemented by specific guidelines that ensure the implementation of individual topics within the organization.

4. Continuous improvement

The Wyssen Group's ISMS is continuously reviewed and adapted to current circumstances. In the interests of continuous improvement, the skills of all departments involved are continuously developed.

5. Exceptions

If exceptions to or exemptions from applicable regulations are necessary, these are recorded transparently, accompanied by risk-mitigating measures, approved for a limited period, and their necessity is reviewed regularly.

6. Organization and responsibilities

6.1 Management

The management is the highest operational decision-making body of the company and delegates tasks, responsibilities, and competencies in information security to the CISO.

6.2 Internal employees / General

All employees of the Wyssen Group who perform activities within the scope of the ISMS are responsible for information security in their area of expertise. Supervisors at all hierarchical levels are obliged to provide the necessary resources and skills. They are obliged to implement all necessary security measures within their area of responsibility on a sustainable basis. They instruct and train their employees as required.

6.3 CISO

The CISO is responsible for developing, defining, monitoring, controlling, operating, and continuously improving the ISMS. He reports to the executive management.

6.4 Asset Owner

Asset owners establish rules for the permissible use of information and assets assigned to them, document these rules, and apply them.

6.5 Risk Owner

Risk owners lead the process of assessing and handling information security risks for their assigned risks. They analyze and evaluate the risks and define appropriate measures.

6.6 External employees / employees of third parties

The Wyssen Group's regulations in the context of information security also apply accordingly to persons who perform activities as external parties or employees of third parties within the scope of the ISMS and must be observed by them.

6.7 Controls

Wyssen Seilbahnen AG checks information security at planned and regular intervals with internal and external audits. The results of these checks are incorporated into the continuous improvement process.

6.8 Sanctions

The Wyssen Group agrees with third parties on contractual penalties that can be imposed in the event of repeated or individual serious violations of safety regulations and instructions. In such cases, sanctions under labor law apply to internal employees.

7. Definition of terms

7.1 Information security

Information security refers to all measures that are ordered, implemented, reviewed, and continuously improved to maintain the confidentiality, integrity, and availability of information. These measures may be organizational, technical, or structural in nature.

- Confidentiality: Ensuring that information is only accessible to authorized persons.
- Integrity: Ensuring the integrity and completeness of information and the methods used to process it.
- Availability: Ensuring that authorized users have access to information and related assets when they need it.

7.2 Information Security Management System (ISMS)

An ISMS is understood to mean:

- All rules, procedures, and processes within the scope of application that define, control, implement, review, maintain, and continuously improve information security.
- Documentation is provided by means of the ISMS framework, the SOA controls (statement of applicability), and corresponding policies, process overviews, and other supporting documents.
- The ISMS is integrated into the SynoTeams management system.

7.3 CISO (Chief Information Security Officer)

The CISO is responsible for information security within their assigned area of responsibility.