1. Ausgangslage und Geltungsbereich

Die Wyssen Seilbahnen AG, zertifiziert sich nach der ISO/IEC Norm 27001:2022 und verpflichtet sich zur Erfüllung dieser Anforderungen. Dabei umfasst der Geltungsbereich der Zertifizierung:

- Der Scope für die ISO/IEC Norm 27001:2022 Zertifizierung gilt für die Wyssen Seilbahnen AG, Wyssen Avalanche Control AG, Wyssen Austria GmbH, Wyssen Norge AS, Wyssen Canada Inc., Wyssen USA Inc. und Wyssen Chile SpA (Wyssen Gruppe).
- Alle Mitarbeiter
- Alle Prozesse

2. Ziele der Informationssicherheit

Die Wyssen Gruppe hat sich folgende Ziele gesetzt:

- Die IT hat eine Verfügbarkeit von 99.9%.
- Sicherstellen der Backup Strategie für die Daten der Wyssen Gruppe sowie deren ihrer Kunden (WAC.3®)
- Erfolgreiche Einführung und Kontinuierliche Verbesserung von ISO/IEC Norm 27001:2022 als Alltagswerkzeug zur Informationssicherung.

3. Das ISMS der Wyssen Gruppe

Im Informationssicherheits-Managementsystem der Wyssen Gruppe werden alle Verfahren und Regeln dokumentiert, welche dazu dienen, die Informationssicherheit der Wyssen Gruppe gegenüber ihren Anspruchsgruppen zu gewährleisten. Das ISMS wird laufend kommuniziert und stufengerecht geschult. Die Anwendung dieser Regelungen ist zwingend und verbindlich. Die ISMS Politik wird mit spezifischen Richtlinien ergänzt, welche die Umsetzung einzelner Themen in der Organisation sicherstellen.

4. Kontinuierliche Verbesserung

Das ISMS der Wyssen Gruppe wird laufend überprüft und den aktuellen Gegebenheiten angepasst. Im Sinn einer kontinuierlichen Verbesserung werden die Kompetenzen aller beteiligten Stellen laufend weiterentwickelt.

5. Ausnahmen

Besteht die Notwendigkeit von Ausnahmen zu oder Befreiungen von geltenden Regelungen, werden diese transparent erfasst und mit risikovermindernden Massnahmen versehen, befristet bewilligt und deren Notwendigkeit wird regelmässig überprüft.

6. Organisation und Verantwortlichkeiten

6.1 Geschäftsleitung

Die Geschäftsleitung ist das oberste operative Entscheidungsorgan der Firma und delegiert Aufgaben, Verantwortung und Kompetenzen in der Informationssicherheit an den CISO.

6.2 Interne Mitarbeitende / Generell

Alle Mitarbeitenden der Wyssen Gruppe, welche Tätigkeiten im Geltungsbereich des ISMS verrichten sind für die Informationssicherheit in ihrem Fachbereich verantwortlich. Die Vorgesetzten aller Hierarchiestufen sind verpflichtet, die dafür nötigen Ressourcen und Skills zur Verfügung zu stellen. Sie sind verpflichtet, sämtliche notwendigen Sicherheitsmassnahmen im Rahmen ihres Verantwortungsbereiches nachhaltig umzusetzen. Sie leiten ihre Mitarbeitenden an und schulen sie bedarfsgerecht.

6.3 CISO
Der CISO ist verantwortlich für die Erarbeitung und Definition, Überwachung, Steuerung und Betrieb und kontinuierliche Verbesserung des ISMS. Er rapportiert an die Geschäftsleitung.

6.4 Asset Owner
Asset Owner legen Regeln für den zulässigen Gebrauch von ihnen zugeteilten Informationen und Werten fest, dokumentieren diese und wenden sie an.

6.5 Risk Owner
Risk Owner führen den Prozess zur Informationssicherheitsrisikobeurteilung und –Behandlung für ihre zugeteilten Risiken. Sie analysieren und bewerten die Risiken und legen entsprechende Massnahmen fest.

6.6 Externe Mitarbeitende / Mitarbeitende von Dritten
Die Regelungen der Wyssen Gruppe im Kontext Informationssicherheit gelten entsprechend auch für Personen, welche als Externe oder Mitarbeitende von Dritten im Geltungsbereich des ISMS Tätigkeiten verrichten und sind durch diese einzuhalten.

6.7 Kontrollen
Die Wyssen Seilbahnen AG überprüft die Informationssicherheit in geplanten und regelmässigen Abständen mit internen und externen Audits. Die Ergebnisse dieser Kontrollen fliessen in die kontinuierliche Verbesserung ein.

6.8 Sanktionen
Die Wyssen Gruppe vereinbart mit Dritten Konventionalstrafen, welche bei wiederholten oder einzelnen schwerwiegenden Verstössen gegen die Sicherheitsvorschriften und –Weisungen eingefordert werden können. Bei den internen Mitarbeitenden kommen in solchen Fällen die arbeitsrechtlichen Sanktionen zur Anwendung.

7. Begriffsdefinitionen

7.1 Informationssicherheit
Unter der Informationssicherheit werden alle Massnahmen verstanden, die zur Aufrechterhaltung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen angeordnet, durchgeführt, überprüft und kontinuierlich verbessert werden. Diese Massnahmen können u. a. organisatorischer, technischer oder baulicher Natur sein.

- Vertraulichkeit: Gewährleistung des Zugangs zu Informationen nur für die Zugangsberechtigten.
- Integrität: Sicherstellen der Unversehrtheit und Vollständigkeit von Informationen und deren Verarbeitungsmethoden.
- Verfügbarkeit: Gewährleistung des bedarfsorientierten Zugangs zu Informationen und den zugehörigen Werten für berechtigte Benutzer.

7.2 Informationssicherheits-Managementsystem (ISMS)
Unter einem ISMS wird verstanden:

- Sämtliche Regeln, Verfahren und Prozesse innerhalb des Anwendungsbereichs, welche die Informationssicherheit definieren, steuern, durchführen, überprüfen, aufrechterhalten und kontinuierlich verbessern.
- Die Dokumentation erfolgt mittels ISMS Framework, den Controls der SOA (Anwendbarkeitserklärung) und mit entsprechenden Policies, Prozessübersichten und weiteren Nachweisdokumenten.
- Das ISMS ist in das Managementsystem SynoTeams integriert.

7.3 CISO (Chief Information Security Officer)

Der CISO ist verantwortlich für die Informationssicherheit in seinem zugewiesenen Geltungsbereich.