Engineering progress
Enhancing lives

REHAU Group Informationssicherheitspolitik

Document Owner: REHAU Group CISO
Document Version: 2
Approved: 20.07.2023
Classification: PUBLIC

Präambel
Die REHAU Gruppe (hiernach auch REHAU) ist sich bewusst, dass ein wirksames Informationssicherheitsmanagement für den nachhaltigen Erfolg unseres Unternehmens von entscheidender Bedeutung ist. Es trägt bei zur Erfüllung gesetzlicher Anforderungen, der Einhaltung vertraglicher Verpflichtungen und zur Reduzierung geschäftlicher Risiken sowie Imageschäden.

Wir verpflichten uns, unserer Verantwortung in diesem Bereich nachzukommen. Dies erreichen wir durch:

- Einhaltung der gesetzlichen Regelungen und unternehmensweiten Richtlinien.
- Fachkundige Ressourcen zur Planung, Umsetzung, Überwachung, Messung und Überprüfung der operativen Wirksamkeit.
- Eine Managementstruktur mit klarer Definition der Verantwortlichkeiten für Informationssicherheit.
- Interne Kommunikation und Schulung, die angemessene Verhaltensweisen und Maßnahmen fördert.

Das Supervisory Board der Unternehmensgruppe fördert aktiv die Informationssicherheit und stellt erforderliche Ressourcen zur Umsetzung einer konsequenten Informationssicherheitspolitik bereit.

Geltungsbereich
Die hier enthaltenen Grundsätze zur Informationssicherheit gelten gruppenweit ohne Ausnahme. Eventuell einschränkendere lokale gesetzliche Regeln haben jedoch in jedem Fall Vorrang.

Sicherheitsziele
Der verantwortungsvolle Umgang mit Informationen von Geschäftspartnern und Mitarbeitenden wie auch mit unternehmenseigenen Informationen ist integraler Bestandteil unseres Handelns. Wir schützen alle Informationen angemessen unter Berücksichtigung ihres Wertes basierend auf den Informationssicherheitszielen Vertraulichkeit, Integrität und Verfügbarkeit

- REHAU erhält und sichert das in einem innovations- und technologiegetriebenen Umfeld aufgebaute Know-how und geistige Eigentum gegen Verlust der Vertraulichkeit.
- REHAU beachtet regulatorische, normative und kundenspezifische Forderungen in Bezug auf Informationssicherheit und schützt Informationen entsprechend.
- REHAU sorgt für hohe Integrität bei allen Informationssystemen in den Kern- und Managementprozessen, um unsere Qualitätsstandards sicher zu stellen.
- REHAU schützt die Informationssysteme, die zur Aufrechterhaltung der Wertschöpfungskette benötigt werden.
- REHAU trifft rechtzeitige Vorkehrungen für den Umgang mit Störungen und Einschränkungen im IT-Prozess, um Stör- und Notfälle innerhalb der definierten maximalen Wiederanlaufzeit zu beheben.
- REHAU sorgt für das Verantwortungsbewusstsein der Mitarbeitenden. Nachlässigkeit könnte dem Unternehmen schaden. Aus diesem Grund schult und sensibilisiert REHAU die Mitarbeitenden.

Engineering progress
Enhancing lives

Sicherheitsprozess

Grundlagen

Zur Erreichung der Sicherheitsziele lehnt REHAU das gruppenweite Regelwerk im Bereich Informationssicherheit an internationale Standards (z.B. ISO/IEC 27001) an und legt Verantwortlichkeiten sowohl auf globaler als auch auf lokaler Ebene fest. REHAU verfügt über Vorgaben zur systematischen Analyse und Erfüllung der Anforderungen sowie zur proaktiven Minderung von im Cyberraum entstehenden Risiken. Die Teilkonzerne setzen die erwähnten Vorgaben um. Dies umfasst insbesondere folgende Elemente:

Einführung und Betrieb eines Information Security Managementsystem (ISMS)

Die Teilkonzerne nutzen schriftlich festgelegte Prozesse zur Definition, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und kontinuierlichen Verbesserung eines ISMS.

Das ISMS verfolgt dabei einen risikoorientierten Ansatz. Hierzu ist eine Methode zur Identifikation und Bewertung von Informationssicherheits-Risiken inklusive der Schnittstelle zum strategischen Risikomanagement der Gruppe definiert. Die verantwortlichen Stellen melden identifizierte Risiken über die festgelegten Meldewege. Sie geben Maßnahmen zur Risikoreduktion frei, halten diese in einem Maßnahmenplan fest und veranlassen eine Umsetzung im definierten Zeitrahmen.

Überwachung/Managementbewertung

Die verantwortlichen Stellen überwachen die Erreichung der definierten Sicherheitsziele, die Einhaltung der Prozesse des ISMS sowie die Wirksamkeit von Schutzmaßnahmen. Dazu dient u.a. ein Kennzahlensystem. Sie initiieren die Beseitigung festgestellter Abweichungen und eskalieren bei erheblichen Störungen oder Verzögerungen an die exekutive Geschäftsleitung des jeweiligen Teilkonzerns.

Kontinuierliche Verbesserung

Die REHAU Gruppe überprüft und verbessert ihre Prozesse und Schutzmaßnahmen zur Informationssicherheit kontinuierlich und richtet diese an internationalen Standards und Best Practises aus. Dabei werden interne und externe Anforderungen berücksichtigt.

Sicherheitsorganisation

Der Director Group Information Security Management (Group CISO) verantwortet die Umsetzung und Weiterentwicklung der REHAU Informationssicherheitspolitik und des Informationssicherheits-Managementframeworks auf Gruppenebene.

Das CISO Council unterstützt die Standardisierung und kontinuierliche Verbesserung des Informationssicherheitsmanagements in der REHAU Gruppe und bereitet Entscheidungsvorlagen für die relevanten Gremien vor.

Die Teilkonzerne ernennen Chief Information Security Officer (CISO) zur Umsetzung des Informationssicherheits-Managementframeworks sowie zum Aufbau und Betrieb des ISMS. Die exekutive Geschäftsleitung des jeweiligen Teilkonzerns fördert aktiv den Informationssicherheits-Prozess und stellt angemessene Ressourcen zur Umsetzung der Informationssicherheitspolitik bereit.

REHAU erwartet von allen Mitarbeitenden ein stets vorhandenes Bewusstsein im Bereich Informationssicherheit bei allen täglich anfallenden Aktivitäten und fördert dies durch schriftlich definierte Vorschriften sowie zugehörige Schulungsmassnahmen. Alle Führungskräfte stellen die Einhaltung der Vorschriften zur Informationssicherheit durch ihre Mitarbeitenden sicher und prüfen dies angemessen. Die Nichteinhaltung der Vorschriften kann zu arbeitsrechtlichen Maßnahmen entsprechend den lokalen Bestimmungen führen.