

Informationssicherheitspolitik

Der Schutz von Informationen ist für die Wertheim Unternehmensgruppe von geschäftskritischer Bedeutung. Als Hersteller sicherheitsrelevanter Produkte (u. a. Tresore, Sicherheitssysteme, Schweißzeugnisse) hat der Schutz sensibler Daten höchste Priorität. Diese Politik legt die Grundsätze für Aufbau, Pflege und kontinuierliche Verbesserung unseres Informationssicherheitsmanagementsystems (ISMS) nach ISO/IEC 27001 fest.

Schutzziele der Informationssicherheit (CIA)



- Integrität: Korrektheit und Verlässlichkeit von Informationen sicherstellen.
- Vertraulichkeit: Schutz sensibler Informationen vor unbefugtem Zugriff.
- Verfügbarkeit: Sicherstellung des bedarfsgerechten Zugriffs für autorisierte Personen und Systeme.



Verantwortung & Rollen

Informationssicherheit ist gemeinsame Verantwortung aller Mitarbeitenden.

- Die Geschäftsleitung stellt die nötigen Ressourcen für Einführung und Weiterentwicklung bereit.
- Der Informationssicherheitsbeauftragte (CISO) verantwortet Umsetzung und Weiterentwicklung des ISMS sowie die Sensibilisierung der Mitarbeitenden.
- Führungskräfte stellen die Einhaltung der Sicherheitsvorgaben in ihren Bereichen sicher.

Umsetzung & kontinuierliche Verbesserung



Ein offener Dialog über sicherheitsrelevanten Themen mit unseren Stakeholdern ist für uns essenziell. Wir kommunizieren unsere Ziele und -maßnahmen transparent und arbeiten eng mit Partnern zusammen, um gemeinsam nachhaltige Lösungen zu entwickeln und umzusetzen.



Kommunikation & Bewusstsein

Diese Politik wird verbindlich kommuniziert, ist intern verfügbar und wird im Rahmen der Leitungstätigkeit regelmäßig auf Eignung und Wirksamkeit geprüft. Schulungen und Informationsangebote fördern unser Sicherheitsbewusstsein.



Martina Lunzer



Roman Foramitti



Andreas Weissenbacher



Roman Rod

Politika informačnej bezpečnosti

Ochrana informácií je pre podnikanie skupiny spoločností Wertheim kriticky dôležitá. Ako výrobca bezpečnostne relevantných výrobkov (napr. trezorov, bezpečnostných dverí a zvarovaných výrobkov) je ochrana citlivých údajov našou najvyššou bezpečnostnou prioritou. Táto politika stanovuje zásady pre zavedenie, udržiavanie a neustále zlepšovanie nášho systému manažérstva informačnej bezpečnosti (ISMS) v súlade s normou ISO/IEC 27001.

Ciele ochrany informačnej bezpečnosti (CIA)



- **Dôvernosť:** Chrániť citlivé informácie pred neoprávneným prístupom.
- **Integrita:** Zabezpečiť správnosť a spoľahlivosť informácií.
- **Dostupnosť:** Zabezpečiť prístup podľa potrieb pre autorizované osoby a systémy.



Zodpovednosti a úlohy

Informačná bezpečnosť je spoločnou zodpovednosťou všetkých zamestnancov.

- Vedenie spoločnosti poskytuje potrebné zdroje na jej zavedenie a ďalší rozvoj.
- Poverený pracovník pre informačnú bezpečnosť (CISO) zodpovedá za implementáciu a ďalší rozvoj ISMS, ako aj za zvyšovanie povedomia zamestnancov.
- Vedúci pracovníci zabezpečujú dodržiavanie bezpečnostných požiadaviek v oblastiach, za ktoré nesú zodpovednosť.

Implementácia a neustále zlepšovanie



Otvorený dialóg o témach týkajúcich sa informačnej bezpečnosti so všetkými zainteresovanými stranami považujeme za nevyhnutný. Naše ciele a opatrenia komunikujeme transparentne a s partnermi úzko spolupracujeme na spoločnom rozvoji a realizácii udržateľných riešení.



Komunikácia a povedomie

Táto politika je dôsledne komunikovaná, interne dostupná a pravidelne preskúmaná z hľadiska vhodnosti a aktuálnosti. Povedomie o informačnej bezpečnosti zabezpečujeme prostredníctvom školení a cieľených informačných aktivít.



Martina Lunzer



Roman Foramitti



Andreas Weissenbacher



Roman Rod

Information Security Policy

The protection of information is business-critical to the Wertheim Group.

As a manufacturer of safety-relevant products (including safes, security doors, and welded components), the protection of sensitive data is a top priority. This policy sets out the principles for establishing, maintaining, and continually improving our Information Security Management System (ISMS) in accordance with ISO/IEC 27001.

Information Security Protection Objectives (CIA)



- Confidentiality: Protect sensitive information from unauthorized access.
- Integrity: Ensure the accuracy and reliability of information.
- Availability: Ensure access as needed for authorized individuals and systems.



Responsibilities & Roles

Information security is a shared responsibility of all employees.

- Management provides the necessary resources for implementation and further development.
- The Chief Information Security Officer (CISO) is responsible for implementing and further developing the ISMS as well as raising employee awareness.
- Managers ensure compliance with security requirements within their areas.

Implementation & Continual Improvement



We consider open dialogue on information security issues with all stakeholders to be essential. We communicate our goals and measures transparently and work closely with our partners to jointly develop and implement sustainable solutions.



Communication & Awareness

This policy is consistently communicated, internally available, and regularly reviewed for appropriateness and relevance. We ensure awareness of information security through training and targeted information activities.



Martina Lunzer



Roman Foramitti



Andreas Weissenbacher



Roman Rod