engineering for a better world

INFORMATION SECURITY POLICY

Version:	03
Datum:	1. September 2020
Letzte Änderung:	01. Juli 2022
Verantwortlicher Manager:	Chief Information Security Officer (CISO)
Dokumentverantwortliche/r:	Informations- und Cybersicherheit
Geltungsbereich:	Alle Firmen und Mitarbeiter der GEA Group
Verteiler:	GEA-Intranet

1. GELTUNGSBEREICH

Die vorliegende Information Security Policy gilt weltweit für alle Unternehmen und Mitarbeiter[1] der GEA Group. Die Gruppe (im weiteren Verlauf als „GEA“ bezeichnet) umfasst die GEA Group Aktiengesellschaft und alle mit dieser nach dem Gesellschaftsrecht verbundenen Unternehmen.

2. INFORMATIONSSICHERHEITSVERANTWORTUNG, STRATEGIE UND ZIELE

Engineering for a better world: Dieses GEA-Motto repräsentiert das wesentliche Leistungsversprechen der Gruppe. Wir formen und gestalten unsere Wertschöpfungsprozesse und unterstützen unsere Partner bei ihren Anstrengungen, den sicheren Umgang mit ihren und unseren Informationen unabhängig von der Informationsumgebung zu gewährleisten – seien es digital, physisch oder mündlich übermittelte und verarbeitete Informationen. Informationssicherheit ist daher eine der höchsten Prioritäten des GEA Vorstands.

Die oberste Zielsetzung von Informationssicherheit ist es, die unternehmensrelevanten Informationen unserer Partner sowie unsere eigenen Informationen zu schützen, indem wir die Vertraulichkeit, Integrität und Verfügbarkeit dieser Informationen sicherstellen und damit effizientere und sicherere Produkte und Prozesslösungen anbieten können.

Zu diesem Zweck unterhält GEA ein Information Security Management System (ISMS) mit den folgenden übergeordneten Informationssicherheitszielen:

- Einhaltung aller geltenden rechtlichen, gesetzlichen und kundenbasierten Informationssicherheitsanforderungen
- Integration von Informationssicherheit in unsere Unternehmensstrategie und in tägliche Abläufe unter Einbindung unserer Geschäftspartner und anderer Interessensvertreter
- Aktive Einbeziehung von Mitarbeitern in die Entscheidungsfindung durch Zusammenarbeit, Kommunikation, Schulungen und Sensibilisierung basierend auf gegenseitigem Vertrauen
- Identifizierung, Analyse und effektive Steuerung aller Chancen und Risiken hinsichtlich Informationssicherheit in unseren Unternehmensaktivitäten und Definition geeigneter, nachhaltiger, präventiver, detektiver, reaktiver und korrektiver Sicherheitsmaßnahmen
- Kontinuierliche Überwachung und Verbesserung der Leistung unseres ISMS und seinen Auswirkungen durch die Bewertung unserer Ziele sowie die Anpassung unserer Sicherheitsmaßnahmen
- Ständige Entwicklung von sicheren Praktiken, Prozessen, Technologien, Instrumenten und Verfahren
- Minderung der Risiken von Cyberangriffen und Umgang mit ~~Informations-~~ Sicherheitsvorfällen und ~~Cyber-~~Krisensituationen
- Sicherstellung der Kontinuität des GEA-Geschäftsbetriebs durch die Aufnahme von Informationssicherheitsaspekten in das betriebliche Kontinuitäts- und Krisenmanagement
- Entwicklung und Umsetzung von Programmen zur Verbesserung der Sicherheit der Informationstechnologie (IT), der Betriebstechnologie (OT), der Humanressourcen (HR), der physischen Sicherheit, der Sicherheit von~~Zulieferern und~~ Drittparteien, der Produktsicherheit und der Sicherheit digitaler Medien bei GEA.

[1]Der in diesem und in anderen GEA-Informationssicherheitsdokumenten verwendete Begriff „Mitarbeiter“ bezieht sich auf alle Manager und Mitarbeiter.