engineering for a better world

INFORMATION SECURITY POLICY

Version:	03
Date:	01 September 2020
Last Amendment:	01 July 2022
Accountable Manager:	Chief Information Security Officer (CISO)
Owner:	Information & Cyber Security
Scope:	All companies and employees of GEA Group
Distribution:	GEA Internet and Intranet

1. SCOPE

This Information Security Policy applies to all companies and employees[1] of the GEA Group worldwide. The Group (hereinafter referred to as “GEA”) includes GEA Group Aktiengesellschaft and all companies affiliated with the GEA Group Aktiengesellschaft in accordance with corporate law.

2. INFORMATION SECURITY RESPONSIBILITY, STRATEGY AND OBJECTIVES

Engineering for a better world: This GEA claim represents the Group’s key value proposition. We shape and design our value creation processes and assist our partners in their endeavors to ensure the secure handling of their and our information regardless of the information environment – digitally, physically or verbally shared and processed information. Information security is thus one of the highest priorities of the GEA Executive Board.

The overall objective of information security is to protect the company-relevant information of our partners and our own information by ensuring the confidentiality, integrity and availability of that information and thereby offering more efficient and secure products and process solutions.

For this purpose, GEA operates an Information Security Management System (ISMS) with the following high-level information security objectives:

- Compliance with all applicable legal, regulatory and customer-based information security requirements
- Integration of information security in our business strategy and in daily processes involving business partners and other stakeholders
- Active involvement of employees in decision-making through cooperation, communication, training and awareness based on mutual trust
- Identification, analysis and effective control of all information security opportunities and risks in our business activities and definition of appropriate, sustainable, preventive, detective, reactive and corrective security measures
- Continuous monitoring and improvement of our ISMS performance and impact through assessing our objectives and adapting our security measures
- Continuous development of secure practices, processes, technologies, tools and procedures
- Mitigating the risks of cyber-attacks and handling ~~information~~ security incidents and ~~cyber~~ crisis situations
- Assure continuity of GEA operations by incorporating information security aspects in business continuity and crisis management
- Development and implementation of programs for the improvement of GEA’s information technology (IT) security, operational technology (OT) security, human resource (HR) security, physical security, ~~supplier~~ third parties' security, product security and digital media security.

[1] The term “employee” used in this and other GEA information security documents refers to all managers and employees