SECURING ASSETS AND FUTURE SUCCESSES.

Information Security at GEA

CONTENTS

SECURING YOUR ASSETS AND FUTURE SUCCESSES.

Dear Customers and Partners,

GEA is a leading technology group and one of the world's largest suppliers of systems and components to the food, beverage and pharmaceutical industries. We take pride in working with customers in so many critical industries, striving to be their partner of choice while making key contributions towards a sustainable future.

For more than 140 years, GEA has continued to innovate and set new standards to meet the needs of our markets and our customers. This includes safeguarding the quality and reliability of our systems and platforms. A prime example is the need for information security which is constantly growing – especially as digitalization increases.

At GEA, we are deeply committed to information security as one of our core strategic priorities. We ensure information is handled securely, making it a fundamental aspect of all our operations and each stage of our value creation processes. By protecting your company information, and our own, we pave the way for a secure and successful collaboration. This provides peace of mind and means we can focus on fulfilling our purpose of engineering for a better world.

In the following pages, we invite you to find out what we are doing at GEA to secure your information as well as our own.

We look forward to a secure and successful future together.

Yours sincerely,

Stefan Klebert, Chief Executive Officer
Bernd Brinker, Chief Financial Officer
Johannes Giloth, Chief Operations Officer

From left to right
Bernd Brinker, Chief Financial Officer
Stefan Klebert, Chief Executive Officer
Johannes Giloth, Chief Operations Officer

INFORMATION SECURITY MATTERS WORLDWIDE.

With advancing digitalization and globalization, the protection of information and sensitive company data is becoming increasingly important.

Security risks and the efforts of companies to protect their information are expanding worldwide.

Security Risks for Companies Worldwide.

Affected companies

84

Percent of companies in Germany were affected by data theft, industrial espionage, and sabotage in 2022*

Type of attacks

48

Percent of these attacks started with social engineering, mostly being contacted via telephone (27%) and email (24%)*

Stolen data

68

Percent of data stolen from German businesses in 2022 was communication data. Followed by intellectual property (45%)*

Data breach cost

4.35

Million dollars, is the average cost of a data breach in 2022**

Security Risks for Companies Worldwide.

Cybersecurity breaches

95

Percent of cybersecurity breaches are made possible by human error**

Cybersecurity expenses

1.75

Trillion dollars is spent on cybersecurity products and services is expected to reach between 2021-2025***

Working from home

59

Percent of IT security-related incidents attributed to working from home*

Ransomware attacks

3/4

Organizations worldwide faced ransomware attacks. 64% paid the ransom and only 40% of these recovered their data**

Source: *Bitkom **Mimecast ***Forbes

Dear customers and partners,

Everything we do comes down to information. Digital, physical, and verbal. In products, processes, and in people. Information security will have a significant impact on our joint success over the coming years. This is especially true since digitalization is advancing with information-based business models, digital production, and Industry 4.0 processes. GEA strives to be the world's leading technology group, providing innovative and sustainable solutions for sophisticated process industries. Accordingly, it is our goal to have a profound, secure, effective, and efficient Information Security Management System (ISMS) in place. We work hard every day to achieve this.

At GEA, we operate and continuously improve our global ISMS, which consists of preventive, detective, reactive, and corrective security measures against growing security threats. From top management to every employee, each member of the GEA Group worldwide is committed to protecting your and our information in the best possible way within their area of responsibility.

As Chief Information Security Officer (CISO) at GEA, I will be glad to answer your questions about this important topic at any time.

Please contact me at
security@gea.com

Looking forward to a secure and prosperous future,

Yours sincerely,

Iskro Mollov,
Chief Information Security Officer

INFORMATION SECURITY AT GEA.

Information security is one of our prime strategic priorities. We shape and design our value creation processes to ensure information is handled securely.

Our overall objective of information security at GEA is to protect all kinds of sensitive information: intellectual property, strategic, pricing, personal information and other knowledge processed by GEA, regardless of its format. Information security applies to physical, electronic, and verbal information alike.

Our goal is to adequately protect all information assets against theft, loss, unauthorized disclosure, unlawful access, misuse, unauthorized modification, and destruction.

We achieve this by covering the core values of information security – confidentiality, integrity, and availability – also known as "CIA".

Confidentiality
prevents or minimizes unauthorized access to information

Integrity
ensures the reliability and correctness of information

Availability
ensures that authorized subjects are granted timely and uninterrupted access to information

Information Security Management System (ISMS)

For this purpose, GEA operates and runs a global Information Security Management System (ISMS). It supports the Executive Board, managers, and all GEA employees in protecting sensitive information.

The security measures put in place by our ISMS play a preventive role to avoid risks in the first place. But we have also defined detective, reactive and corrective measures to respond to successful attacks in a timely manner.

GEA's ISMS is based on the ISO/IEC 27001 standard, takes on board industry-specific regulations, is continuously further developed by our Chief Information Security Officer, and is reviewed and approved by the Executive Board.

At GEA, we approach security holistically.

Our ISMS and our team facilitate effective adaption to constantly evolving security requirements.

The CISO reports directly to the Chief Financial Officer and regularly to the Supervisory Board and its Audit and Cyber-security Committee.

Our ISMS spans across multiple levels.

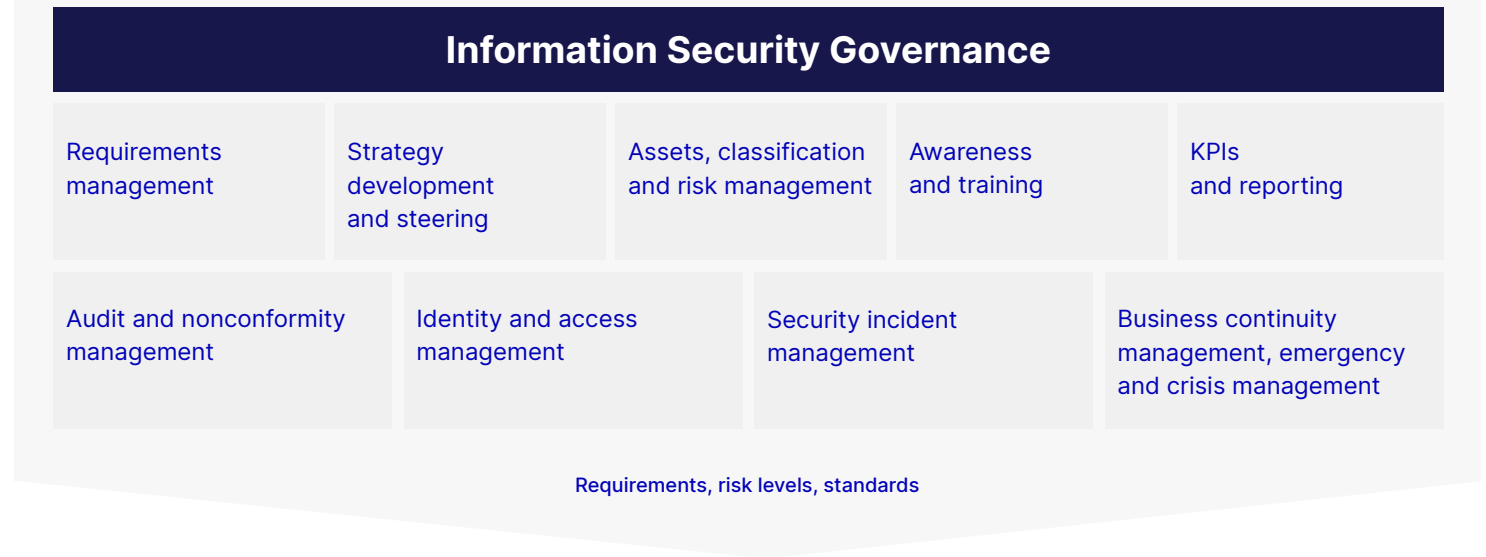|	
GEA Group	**Supervisory Board**
	Executive Board
	CISO Organization • Information Security Governance • Internet Security • IT-Security • Physical Security • Production Security • Supplier Security • Product Security • HR Security	**Global Process Owners**
Regions & Divisions	**Regional Information Security Organization** **Divisional Information Security Organization**
Site level	**Local Information SecurityResponsibilities**

CISO Organization

Within the ISMS, we operate and maintain two lines of defense against major security risks.

Second line of defense

Information Security Governance

Requirements management	Strategy development and steering	Assets, classification and risk management	Awareness and training	KPIs and reporting
Audit and nonconformity management	Identity and access management	Security incident management		Business continuity management, emergency and crisis management

Requirements, risk levels, standards

First line of defense

IT Security
Secure information in office IT network & systems

OT Security
Secure information in production & engineering network & systems

Product Security
Secure GEA's digital products and customer information

Internet Security
Secure web & social media presence

Physical Security
Secure information in sites, buildings, & offices

Supplier Security
Secure information in the procurement & supply chain

HR Security
Secure information in people's minds and prevent oversight & insider threats

FIRST LINE OF DEFENSE.

Operational management is responsible for maintaining effective controls and implementing risk and monitoring processes in their daily business. Seven focus areas address risks (threats and vulnerabilities) where they occur.

IT Security
We protect GEA's IT infrastructure, core IT services, and applications. Among others, this includes IT security architecture, network protection, perimeter and zoning, cloud security, and security of our Office IT applications.

OT (Operational Technology) Security
We protect GEA's production environments. Digital production and Industry 4.0 processes are increasingly important at GEA. OT Security ensures secure handling of all information within digitally driven production processes.

Product Security
We establish security as an integral part of products and product development at GEA. It ensures that all GEA products, applications, and cloud services are secure and protected, and that the same is true for the customer environments in which they are operated.

Internet Security
We protect GEA's online presence through web monitoring, domain management, web application security, and continuous process improvement. We further make sure that content production platforms are secure to use, that access is managed according to our guidelines, and that users are trained to use them securely.

Physical Security
We protect information in sites, buildings, and offices. To prevent unauthorized access and damage to GEA's information and information processing facilities, we manage, control, and audit physical access to sensitive areas, create security concepts for facilities, and roll out awareness training as well as related policies and processes.

Supplier Security
We protect all GEA information assets that are accessible to suppliers. The suppliers' security level must be compliant with our requirements, with those of our customers, and with applicable laws. This is integrated into the agreements and contracts with our suppliers.

HR Security
We control identities centrally and manage access rights on relevant IT services and applications. We conduct security-related training and campaigns among employees to raise awareness of the responsibility each and every one of us has in terms of protecting our information.

SECOND LINE OF DEFENSE.

As a second line of defense, the Chief Information Security Officer is responsible for Information Security Governance. He establishes the security levels at GEA by defining the security requirements, risk levels, and standards.

BENEFITS FOR OUR CUSTOMERS AND PARTNERS.

Thanks to GEA's Information Security Management System (ISMS) we protect all information assets through effective, efficient and modern methods.

As a GEA customer or partner, you benefit from:

Peace of mind
Your data is safe with us since we protect all information assets, including those of our customers and partners.

Competitiveness
Your competitiveness is preserved since we protect intellectual property (e.g., solutions tailored to you) against theft and espionage.

Security of supply
Your supply of GEA machinery, plants, or process technology is secure since we defend against sabotage and loss of production.

Protected infrastructure
Your infrastructure is protected since we defend against attacks targeting your systems through our GEA environment.

OUR ISMS IS CERTIFIED.*

You can view the existing certificates
by scanning this **QR code**.

As we continue to improve our approach to securing and protecting the information within our business and that of our customers and partners, we ensure that we follow international best practice.

ISO/IEC 27001: global certifications
GEA's ISMS is based on the globally recognized ISO/IEC 27001 standard. Taking industry-specific requirements into account, it is continuously updated by the CISO and approved by the Executive Board. These legal entities are already certified:
- **GEA Group AG**, Düsseldorf, Germany
- **GEA Group Services GmbH**, Düsseldorf, Germany
- **GEA Westfalia Separator Group GmbH**, Oelde, Germany
- **GEA Germany GmbH**, Oelde, Germany
- **GEA Mechanical Equipment GmbH**, Oelde, Germany
- **GEA Westfalia Separator Group GmbH**, Hamburg, Germany
- **GEA Westfalia Separator Group GmbH**, Niederahr, Germany
- **GEA Process Engineering S.A.**, Alcobendas, Spain
- **GEA Westfalia Separator Ibérica S.A.**, Alcobendas, Spain
- **GEA Farm Technologies Ibérica S.L.**, Alcobendas, Spain
- **GEA Food Solutions International**, Alcobendas, Spain
- **GEA North America Inc.**, Columbia, USA
- **GEA Mechanical Equipment US Inc. Northvale**, New Jersey, USA
- **GEA Westfalia Separator (S.E.A.) Pte. Ltd**, Singapore, Singapore
- **GEA Process Engineering Pte. Ltd**, Singapore, Singapore
- **GEA Process Engineering (India) Pvt. Ltd**, Vadodara Gujarat, India
- **GEA Avapac Limited Avalon**, Hamilton, New Zealand
- **GEA Process Engineering Pty. Ltd**, Melbourne, Australia
- **GEA Farm Technologies Australia Pty.**, Melbourne, Australia
- **GEA Westfalia Separator Australia Melbourne Airport**, Melbourne, Australia
- **GEA Process Engineering Pty. Ltd**, Kirawee, Australia

IEC 62443-2-1 and IEC 62443 4 -1: certifications in Oelde and Niederahr, Germany
The GEA productions at the Oelde and Niederahr locations are certified according to the IEC 62444-2-1 standard, Security Level 3. Furthermore, secure production development at the Alcobendas location in Spain was prepared for certification under the IEC 62443 4-1 standard and will soon be on a par with the already certified Oelde location.

Cyber Essentials Plus certification in the UK
In 2023, the information security processes of GEA Mechanical Equipment UK Limited in Milton Keynes, UK, were again reviewed according to the "Cyber Essentials" certification, which is required by the British government and overseen by the National Cyber Security Centre (NCSC). The successful recertification, together with the additional Cyber Essentials Plus certification received this year, demonstrates to customers that GEA is able to adequately protect its own data and that of others. UK Cyber Essentials certification is relevant across industries, but especially to the shipping industry, which has strong ties to the UK's Royal Navy.

MLP 2.0 compliance China
The Chinese government is reinforcing cyber security in the country through numerous cyber security laws. In 2023, GEA reviewed the maturity of the security measures at its own Chinese sites and companies in accordance with the Multi-Level Protection Scheme (MLP) 2.0 and implemented any necessary measures. Corresponding assessments submitted to the relevant Chinese authorities ensured compliance.

ITAR compliance in the United States of America
The International Traffic in Arms Regulations (ITAR) provide the framework for direct suppliers or contractors to ensure secure execution of orders for the US Department of Defense. ITAR compliance makes it possible for GEA to securely and reliably process the corresponding customer orders for marine separators.

We will continue to add to the certificates for all GEA locations and services, in alignment with our long-term goal to make GEA as secure as possible worldwide.

* Status May 2024

OUR VALUES.

Responsibility	Integrity	Diversity	Passion	Excellence
We care for people and planet.	We walk our talk.	We value our differences.	We love what we do.	We deliver outstanding work.

GEA values provide the foundation for all our business activities. They are an important red thread connecting our global workforce across geography and cultures.

GEA.com