INFORMATION CLASSIFICATION AND HANDLING POLICY REGARDING CONFIDENTIALITY

Doc ID:	PPC-2935
Version:	1
Last Review	01Jun2024
Date:	01Sep2020
Last Amendment:	01Jun2024
Accountable Manager:	Chief Information Security Officer (CISO)
Owner:	Information Security, Business Continuity and Crisis Management
Scope:	All companies and employees of GEA Group
Distribution:	GEA-Intranet and Emails

PUBLIC

Content

PUBLIC

1. Introduction

Summary
The subject of this Policy[1] is to provide rules for the classification of information regarding confidentiality into the information classification levels (also called information protection classes) "**PUBLIC**", "**GEA INTERNAL**", "**GEA CONFIDENTIAL**" and "**GEA STRICTLY CONFIDENTIAL**" and to define appropriate protective measures for each of these levels. This Policy supplements existing GEA policies[2] on information security. This Policy applies to all GEA employees and all concerned third parties.

As an innovative and globally active enterprise, GEA processes a large amount of information daily. To protect this information from unauthorized disclosure and loss – which may cause great **harm** to GEA – this Information Classification and Handling Policy regarding confidentiality ("**Policy**") sets out principles and rules for the classification and handling of **information** processed by GEA regarding its confidentiality. The Policy complements the GEA Information Security Regulations by specifying the classification of information and the related protective measures for each of the information protection classes "**PUBLIC**", "**GEA INTERNAL**", "**GEA CONFIDENTIAL**" and **GEA STRICTLY CONFIDENTIAL**".

Information
All types of information, including sensitive information of any kind - intellectual property (copyrights, trademarks, patents and trade secrets), strategic, partner, pricing, personal information and other know-how processed by GEA regardless of its format (physical, electronic or verbal).

This Policy applies to each of us equally – to management, all GEA Group entities and each individual **employee** of GEA, as well as all concerned **third parties**, working for or with GEA. Together, we are responsible for protecting Information.

Employee
Any employee of GEA (including management, department heads, apprentices, trainees and students etc.).

Third parties
Any staff contractually or otherwise commissioned to work for and/or with GEA (e.g., freelancers, agency workers, suppliers or customers), but not being employed by GEA. It is the duty of the employee who is responsible for the third party to ensure that the third party will be informed about regulation in this Policy.

GEA requires compliance with the Policy. Failure to comply could adversely affect GEA's business and reputation and may result in competitive disadvantages and financial or reputational harm. The GEA management of each legal entity and each Responsible Unit must therefore ensure that the content of this Policy is implemented and that its observance is appropriately monitored by means of the provided tools.

This Policy is binding with immediate effect.

1.1. Requirements and Background

The protection of business relevant, valuable and secret information ("**trade secrets**") is subject to various regulations worldwide. In particular, the Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS Agreement) of the World Trade Organization (WTO) contains respective provisions which are common international standards meanwhile. They have been implemented into various local laws, such as for example:

[1] The meaning of capitalized terms and acronyms used in this Policy is summarized again in the Glossary.
[2] GEA policies are available on the intranet in the Policies and Guidelines Center (→ GEA Insights → Policies and Guidelines).

State / Union	Reference	Title
European Union	Trade Secret DIRECTIVE (EU) 2016/943	The protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure
United States of America	PUBLIC LAW 114–153	Defend Trade Secrets Act of 2016
China	"AUCL 1993"	Anti-Unfair Competition Law of the People's Republic of China

Table 1: Legal texts on Trade Secret Protection

For GEA as a globally acting company, these legal obligations are not just applicable. Rather, compliance with the requirements of these laws is a mandatory prerequisite for the protection of trade secrets and their enforcement in case of misappropriation, such as theft, unauthorized copying, economic espionage or breach of confidentiality requirements. In this context, one major legal requirement must be highlighted:

Reasonable steps to protect trade secrets must be in place!

To benefit from trade secret protection under law, it is required that the trade secret has been subject to reasonable protection measures. If no evidence of this can be presented, the legal prerequisites for protection as a "trade secret" are not met and – as a result - no legal protection or legal actions (litigations etc.) will be possible. The implementation of a reasonable protection concept is therefore vitally important!

Note: Because this Policy covers all types of information, including those not necessarily identified as trade secrets, in the following only the broader term 'information' will be used which includes 'trade secrets'.

Furthermore, the classification and secure handling of information is subject of contractual customer requirements. Those requirements may be either customer-based or refer to compliance with international and industry standards, such as ISO 27001, IEC 62443, NIST SP 800-171, ISO 16016 and others.

1.2. Purpose of this Policy

Based on the above requirements and as a general GEA management requirement, this Policy therefore has two main objectives.

The *first objective* of this Policy is the establishment of a global, uniform GEA standard for the secure handling of information regarding its confidentiality within GEA. Because of varying information sensitivity, information classification into different information protection classes and identification and implementation of corresponding protection measures is needed to ensure that information is appropriately protected.

Classification
Categorizing of information into different information classification levels with regard to the information properties and protection goals: Confidentiality, Integrity and Availability (CIA-triad)

Information Classification Levels
An information protection level. At GEA, there are 4 levels: "**PUBLIC**", "**GEA INTERNAL**", "**GEA CONFIDENTIAL**" and **GEA STRICTLY CONFIDENTIAL**".

Since organizational and technical safety measures alone may not adequately cover all security and risk aspects, a *second objective* of this Policy is to make each GEA legal entity, Responsible Unit, employee and any concerned third party aware of its role as a primary component in the security concept.

1.3. Scope

This Policy applies to all information processed by GEA (originated by the organization or entrusted to GEA by others). Examples are:

Technical information	Development information	Business, company and employee information
▪ design drawings, ▪ technical specifications, test parameters and test results, ▪ process descriptions and parameters ▪ spare part specifications	▪ development plans and documents ▪ intellectual property (IP) strategies, ideas, and drafts ▪ patent applications (unless publicly accessible)	▪ supplier and/or customer information ▪ price calculations / production details ▪ contracts (particularly commercial and technical specifications in contracts) ▪ risk and hazard assessments ▪ organizational charts, organizational sequences and employee data ▪ personal data ▪ business plans, strategies etc.

Table 2: Examples for Information

2. How does this Policy work?

Summary
This Policy sets out rules for the classification and handling of information, specifies the roles and responsibilities of involved stakeholders and provides for related guidance on how to comply. The rules of the Policy are basically conclusive. However, Responsible Units may define special classification advices.

2.1. Basic Concept

This Policy defines:

- ownership of information (chapter 4)
- roles and responsibilities (chapter 4)
- general rules, also concrete advice for the classification of information (chapter 5)
- concrete protection measures for each information classification level (chapter 5.4)

The rules laid down in this Policy are basically exhaustive, i.e. they apply equally within all GEA entities. However, there is one exception to this. Because GEA business is very diverse and there are many different types of information which cannot be enumerated conclusively in this Policy, each GEA Responsible Unit has the possibility to define further concrete classification advices for the classification of information within its area of responsibility or business line. This means that a Responsible Unit can, for example, define that an information XYZ shall be allocated by employees or concerned third parties to the information protection class *"Confidential"*. Such concretization is useful as it facilitates the classification of information (see *chapter 5*).

Responsible Unit
The unit within GEA responsible for a particular piece of information (because it was created or acquired there). Responsible Units are, for example: group process owners, legal entities, GEA divisions, GEA business units, the GEA country organization and its subunits, the GEA central organizational units such as the GEA Global Corporate Center (GCC), Shared Service Center (SCC) and the central units Production, Procurement and Technology and any subunits. The term "Responsible Unit" may but does not have to overlap with the so-called organizational units (see Glossary).

PUBLIC

2.2. Support and Contacts

GEA will provide its employees and concerned third parties with additional support, information and guidance on how to apply and comply with this Policy. This includes, for example, in-person and online training and supporting material that summarizes the classification and handling rules in a concise manner. In addition, further (market standard) technical means and software are to be implemented to support information protection.

In case of questions, suggestions, requests and enquiries, including requests for information, and complaints relating to information classification and handling issues, every GEA employee or concerned third party may contact the following in the order listed (and depending on the specific request):

- Group CISO
- IP ambassadors
- IP managers
- Legal department – compliance & principle legal matters

IP Ambassador
Local contact person and/or expert for IP issues on level of a GEA group company.

IP Manager
Member of the IP management team

3. General Information Protection Rules

Summary
In addition to classification, general rules regarding disclosure of information are to be observed. This includes the always applicable “need to know” principle and the general obligation to have non-disclosure agreements in place.

3.1. Protected Information

Information protection can only be achieved together. GEA thus expects all employees and concerned third parties to apply the rules of this Policy to their daily work activities; therefore, they shall:

- know how to identify the information classification levels of a document or email, for instance.
- know and apply the handling rules laid down in this Policy for specific information classification levels.

Information is considered to be protected if:

The author has:

- analyzed the confidentiality level of the information and has classified and labeled it,
- checked the distribution circuit for this information and, if necessary, defined it,
- taken the protective measures required for the confidentiality level of this information (see chapter 6);
- checked the confidentiality level when an information is transferred

The recipient:

- has taken protective measures within its sphere of influence that are required for the defined level of confidentiality.

PUBLIC

3.2. Disclosure Principles

Disclosure of information is a main threat, particularly for **GEA CONFIDENTIAL** or **GEA STRICTLY CONFIDENTIAL** information. In this context, the general principles below, which apply regardless of and in addition to the classification concept, must be observed:

- The disclosure of information to employees of GEA and to third parties inside and outside GEA must always be handled according to the need-to-know principle and least-privilege principle. This means that access is limited to persons, processes and IT systems that have a legitimate interest in the information and need it for the performance of their business tasks.
- These principles are always applicable for all types of information. Information shall not be disclosed to others, unless the receiver of information has a need to know about respective information. The extent of disclosed information shall be strictly limited to the actual information needed. Any disclosure of information must be in accordance with the handling rules set out below (see chapter 5.4). These rules provide guidance as to how specific classified information must be handled.
- It is useful to know the basic principle underlying the information handling (and classification). This is the business value of information and it specifies that any information must be handled in the best interest of GEA. Thus, before classifying, handling or disclosing information, one should consider the benefits of specific information for GEA compared to potential risks which might be incurred by its disclosure. In this connection, the following questions can be raised, and the basic principle below applies:
  - Identifiability: How easily can this information be used to identify the subject protected (e.g. individual, machine, process, product, strategy)?
  - Sensitivity: How severely would GEA be impacted if the information were to end up in the wrong hands?
    Would you disclose this information to competitors?

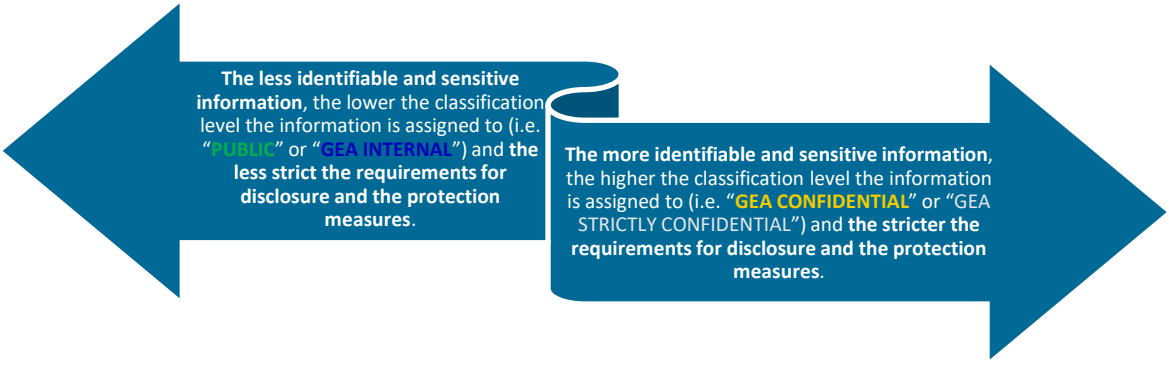

Figure 1: Basic principle for information classification and handling

- In case of doubt, information must be treated at least as GEA INTERNAL if its actual classification is unknown (no marking on a document, verbal information etc.). Therefore, in case of doubt, disclosure rules for confidential information as set out in chapter 5.4 below apply.

3.3. Confidentiality Agreements

A key element in protecting information from disclosure, particularly if shared with third parties, are non-disclosure agreements ("**NDA**"), also called confidentiality agreement (CA or CDA). The general rule is that an NDA must be in place **before** any access to information is possible. Exceptions may apply for third parties who are under a professional obligation of confidentiality, such as lawyers and patent attorneys.

Please contact Legal if an NDA is needed for sharing information or use the NDA Generator:

https://geacloud.sharepoint.com/sites/Intranet/Portal/Legal/guidelines/confidentiality-agreements-nda-generator

4. Roles & Responsibilities

Summary
Information Security, together with Legal & Compliance and IP Management, enable and ensure compliance with legal, regulatory and customer requirements and establish the organizational and technical framework for information protection. However, ultimate responsibility for compliance with this Policy and its classification and handling instructions remains with the Information Owners and Information Users.

4.1. Information Owner

Information Owners hold the main accountability for classification and protection within their business line.

Information Owner
The Information Owner is the Global Process Owner (GPO) of the respective GEA business process. An Information Owner may delegate his/her responsibility to an identified and appointed individual; however, accountability always remains with the Information Owner.

The Information Owner is responsible for:

- Defining global standard information naming conventions and the classification advice regarding confidentiality, integrity and availability. The standards information names and the classification advice are used as an orientation by the Information Users in their daily work with information.
- Information being collected, classified, and maintained by its Responsible Unit in accordance with the classification levels and the handling requirements defined in this Policy.
- Periodically revalidating the classification of their information.
- (Optionally) defining concrete classification advice for specific information typically processed within its Responsible Unit and informing employees as well as concerned third parties accordingly.

4.2. Information User

Information Users are those who process information in their work activities. Unlike many Information Owners, they regularly come into direct contact with information (e.g. by creating it) and are therefore co-responsible particularly for the initial classification of information.

Information User
Any employee (as defined) and any third party (as defined) authorized to create, access, store, modify, use, transmit or delete information.

The Information User is responsible for protecting the information entrusted to him, including:

- Classifying information in accordance with this Policy or the classification advices of a relevant Responsible Unit. In case of doubt, they shall seek the assistance of the Information Owner.
- Handling and protecting information as described in chapter 5.4.

PUBLIC

5. Information Classification

Summary
This chapter defines the general rules for classification and outlines the 4 information protection classes "**PUBLIC**", "**GEA INTERNAL**", "**GEA CONFIDENTIAL**" and "**GEA STRICTLY CONFIDENTIAL**". In addition, this chapter provides examples of information classification.

5.1. Classification Rules

Following are the basic classification rules provided under this Policy:

- Information shall be classified into one of the 4 information protection classes "PUBLIC", "GEA INTERNAL", "GEA CONFIDENTIAL" and "GEA STRICTLY CONFIDENTIAL" as set out in the matrix below (chapter 5.2).
- Information received from third parties is treated and classified in the same way. If such information has already been labeled by the third party with a specific class, no lower class shall be chosen.
- When choosing the appropriate information protection class for information of heterogeneous nature, the level shall be selected based on the most sensitive piece of information.
- Since it is not possible to define the appropriate information classification level abstractly for all types of information and, in particular, in order to simplify classification for Information Owner and Information User, this Policy uses classification advices that provide a default classification for a particular type of information (unless special circumstances exist which may lead to a higher of lower classification). The list of examples is not exhaustive. Note that Responsible Units can define additional classification advices for information typically processed within their area of responsibility or business line.

Classification Advice
Indicative, non-binding recommendation of a default information protection class for a type of information (rule of thumb).

Note: There are two conditions for classification advices to be valid. First, they must be communicated by the Responsible Unit to the relevant stakeholders. Second, additional classification advices of a Responsible Unit must not conflict with the general definitions of the information protection classes as defined in table 5 (below). For example, this means that information whose unintended disclosure could significantly harm a GEA project, activity or entity must be classified at least as **"GEA CONFIDENTIAL"**.

Examples of classification advices defined by the Group Process Owner:

- The Group Process Owner defines classification advices within its area of responsibility, e.g. specific tax relevant information must be classified as "Confidential".
- The business unit Pharma & Healthcare may define classification advices for its business line, e.g. specific unpublished strategic information for regulatory approval procedures must be classified as "**GEA STRICTLY CONFIDENTIAL**".

The main accountability for ensuring the classification of information lies with the Information Owner (s). Information handlers are co-responsible for classification (see chapter 4). Guidance for classification is given to them by the concrete classification advices defined by Responsible Units (highest priority) and, if certain information is not covered therein, the general classification advices defined in this Policy (second highest priority). In the absence of any relevant classification advice(s), the general rules for classification as set out in Figure 5 of this Policy apply. Thus, when classifying specific information, Information Owner and Information User should follow this order:

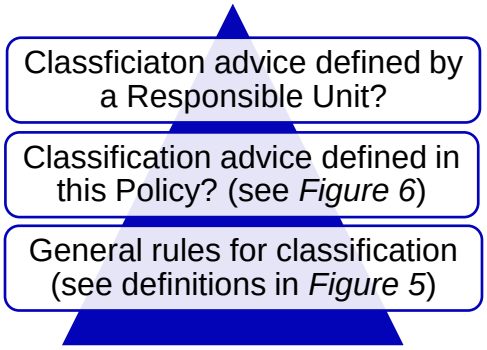

Figure 2: Workflow for classifying information

In general, information classification as described in this Policy shall apply throughout the entire information lifecycle (creating, labeling, replication and distribution, transmission and transport, downgrading, destruction). However, Information Owners must regularly review information classifications and re-classify information if the information protection class has changed. Re-classification can result in a higher or lower information protection class.

Users who identify information classified at a level too low (e.g., labelled "**GEA INTERNAL**" but the content matches the "**GEA CONFIDENTIAL**" description in this Policy) shall handle and re-classify it according to the higher level and notify the Information Owner (s). If the Information Owner cannot be determined, users shall consult their line managers.

5.2. Classification Levels

Information is subject to various confidentiality levels depending on its identifiability and sensitivity (see *chapter 3)*. The individual classes and their definitions are set out below:

	Information Classification Levels			
	PUBLIC	**GEA INTERNAL**	**GEA CONFIDENTIAL**	**GEA STRICTLY CONFIDENTIAL**
Definition	▪ All publicly available information authorized and published by GEA or a third party. ▪ No damage expected for GEA in case of information leakage.	▪ Any information that is intended to circulate only within GEA and with authorized third parties, but which is not intended for public disclosure. ▪ Damage expected for GEA in case of information leakage.	▪ Any information which may be communicated only to the persons directly concerned. ▪ Serious damage expected for GEA in case of information leakage.	▪ This kind of information is only shared between very few named individuals (a named distribution list). ▪ Exceptionally grave damage expected for GEA in case of information leakage.
➲ **Value for GEA**	▪ The value corresponds to the respective purpose of the publication (e.g., marketing)	▪ Internal information about GEA, required to run the business in the most efficient and effective manner.	▪ Information provides an advantage over competition or has the potential for such an advantage in the future	▪ Information provides an outstanding advantage over competition or has the potential for such advantage in the future

	Information Classification Levels			
	PUBLIC	**GEA INTERNAL**	**GEA CONFIDENTIAL**	**GEA STRICTLY CONFIDENTIAL**
➲ **Damage for GEA, if disclosed**	▪ No damage expected when disclosed	▪ Damage ▪ Disclosure to unauthorized recipients could cause damage – competitive disadvantage, financial or reputational loss or other minor undesirable effects	▪ Serious damage ▪ Competitive disadvantage, financial or reputational harm, loss of trustworthiness, when disclosed ▪ It will not affect GEA in general, but might affect a respective GEA division, business unit or group function.	▪ Exceptionally grave damage ▪ Tremendous competitive disadvantage, financial or reputational harm when disclosed ▪ It may affect GEA as a whole or may cause exceptionally grave damage to a GEA division, business unit or group function.

Table 3: Definition of the 4 Information Protection Classes

5.3. Advices for Classification

The list of classification advices below outlines how specific types of information should be classified **by default**, unless there is more concrete classification advice from an organization unit.

Information Owner and information handler are generally on the “safe side” when they choose the information protection class provided in the classification advices of Responsible Units (which have priority) or, in the absence of such, the classification advices in this Policy. However, Information Owners and Information Users are also encouraged to consider the circumstances of the individual case that may justify a higher or lower classification. In case of doubt, the stakeholders defined in *chapter 2.2* should be contacted for support.

Information Classification Levels				
	PUBLIC	**GEA INTERNAL**	**GEA CONFIDENTIAL**	**GEA STRICTLY CONFIDENTIAL**
	▪ GEA public website ▪ Published press releases ▪ Published job offers ▪ Published marketing materials for GEA products and services ▪ Commercial register extracts ▪ Published annual financial reports Published patents and applications	▪ Information published on the GEA Intranet. ▪ General documentation, manuals, user guides ▪ Organization charts, directives, policies, standards, operating procedures, job specifications. Majority of internal emails	▪ Technical information, such as know-how ▪ Development-related information, including projects, strategies, reported inventions and unpublished patent applications ▪ Personnel documents such as applications, payrolls, social security documents ▪ Information about pending litigation and legal cases. ▪ Financial information, such	▪ Unpublished management reports and strategic documents ▪ Unpublished annual financial reports, ad-hoc-notifications and other investor relation-documents ▪ Sensitive development documents, drawings, strategies, projects ▪ Information about upcoming litigation Information about M&A projects (usually)

Information Classification Levels				
	PUBLIC	**GEA INTERNAL**	**GEA CONFIDENTIAL**	**GEA STRICTLY CONFIDENTIAL**
			as announcements, reports and forecasts prior to publication. ▪ Commercial information such as procurement details, supplier and/or customer information, contracts, invoices, etc. ▪ Information security-related information, such as secret keys and vulnerability lists, detailed network topography, security logs, etc. ▪ Internal/external audit reports.	

Table 3: Classification Advices

* The list of classification advices is not exhaustive. There are many more types of information and documents that require a suitable information protection class. In particular, there are document types that need to be assigned individually to either one of the classes based on actual document content. Such assignments can vary from document to document. For instance, a CAD drawing containing specifications for a spare part in a device already out of production requires a lower classification than a CAD drawing of a new invention.

5.4. Special Requirements for Classification

Trade secrets (e.g. under Article 2, paragraph 1 of Directive EU 2016/943) are to be classified at least **GEA CONFIDENTIAL** and are subject to the protective measures to be applied for that purpose. Trade secrets that are not marked as such or not yet marked as **GEA CONFIDENTIAL** must nevertheless be treated at least as **GEA CONFIDENTIAL**.

A **company secret** is a type of trade secret and is treated as its equivalent.

Personal data that does not belong exclusively to internal communication data shall be classified at least **GEA CONFIDENTIAL**.

Inventions and invention disclosures must be classified at least **GEA CONFIDENTIAL** at the time of creation and may be reclassified by the responsible employee or manager in the patent department.

The information classification **GEA STRICTLY CONFIDENTIAL** must be coordinated with the responsible Group Process Owner (GPO). The classification **GEA STRICTLY CONFIDENTIAL** by a member of the Executive Board does not have to be coordinated with the GPO.

6. Protection Measures for Information

Summary
This chapter defines the appropriate protective measures for each of the 4 information classification levels "**PUBLIC**", "**GEA INTERNAL**", "**GEA CONFIDENTIAL**" and "**GEA STRICTLY CONFIDENTIAL**".

Classification alone is not enough to protect information. What matters is how information is handled. Therefore, in addition to classification, this Policy also defines appropriate protective measures for each information protection class. In this respect, it is essential to observe the rules for the 4 different levels.

The following requirements must be observed regardless of the detailed regulations listed below:

- When creating information, it must be treated immediately at least as GEA INTERNAL, even if not labeled as such. All information which does not yet belong to a level of confidentiality shall be treated as if it were classified GEA INTERNAL.
- The forwarding of information classified as GEA INTERNAL or above to private email addresses is prohibited.

6.1. Information Protection Handling Matrix

The following table details the handling of information by outlining the protective measures for each information protection class:

<table>
<tr><th colspan="5">Information Classification Levels</th></tr>
<tr><th></th><th>PUBLIC</th><th>GEA INTERNAL</th><th>GEA CONFIDENTIAL</th><th>GEA STRICTLY CONFIDENTIAL</th></tr>
<tr><td colspan="5">General</td></tr>
<tr><td rowspan="2">Access & Distribution List
(see also "Trans-mission" below)</td><td rowspan="2">No access restrictions</td><td rowspan="2">Only to be shared internally or with entrusted third parties (with need to know)</td><td>▪ Access only to authorized personnel and dedicated third parties and only under a confidentiality agreement / NDA:
▪ For GEA employees: Confidentiality agreement must be part of work contract.
▪ For external third parties: NDA required with party or its organization (exceptions may apply with third parties who are under a professional obligation of confidentiality (see chapter 2.2)).
▪ In public locations, a privacy screen filter shall be used</td><td></td></tr>
<tr><td></td><td>▪ Access to be restricted to a named distribution list of highly trusted individuals.
NDA must identify disclosed information and the individual(s) to which this</td></tr>
</table>

<table>
<tr><th colspan="5">Information Classification Levels</th></tr>
<tr><th></th><th>PUBLIC</th><th>GEA INTERNAL</th><th>GEA CONFIDENTIAL</th><th>GEA STRICTLY CONFIDENTIAL</th></tr>
<tr><td></td><td></td><td></td><td></td><td>information is disclosed.</td></tr>
<tr><td rowspan="2">Labelling</td><td>To be labelled as PUBLIC (on every page in case of documents)</td><td>To be labelled as “GEA INTERNAL” (on every page in case of documents)
Per default every information is at least GEA INTERNAL (also not yet labeled) and all measures apply</td><td>To be labelled as “GEA CONFIDENTIAL” (on every page in case of documents)</td><td>To be labelled as “GEA STRICTLY CONFIDENTIAL” (on every page in case of documents)</td></tr>
<tr><td colspan="4">Where possible, the Responsible Unit(s) associated with the information shall be provided on the first page of a document.
* Labeling is not necessary for GEA PUBLIC information, if not reasonable (e. g. marketing materials or internet pages)
* Labeling is not necessary for information carriers where labeling is not technically possible (e.g. information in not yet configured databases or handwritten notes)</td></tr>
<tr><td>Printing/ Copying</td><td colspan="2">No restrictions</td><td colspan="2">User or entrusted person must be present during printout.
A secure printing mode (incl. authentication) is preferred.</td></tr>
<tr><td colspan="5">Storage</td></tr>
<tr><td>Location of electronic information</td><td>No restrictions</td><td>Company desktop/laptop with encrypted hard drives and corporate registered and managed mobile devices, corporate databases, and authorized cloud applications.</td><td>Only encrypted storage is permitted independent of the storage place (desktop/laptop, corporate registered and managed mobile devices, file servers, IT system, email accounts, corporate databases, and authorized cloud applications, etc.).</td><td>Only encrypted storage combined with digital rights management (DRM) is permitted.</td></tr>
<tr><td>Access Control of electronic information</td><td>No restrictions</td><td colspan="3">Access rights are to be granted and monitored by a corresponding means (in line with the respective Information Security Policies and Procedures).</td></tr>
<tr><td>Electronic information protection</td><td>No restrictions</td><td>User authentication required.</td><td>User authentication and authorization.</td><td>User authentication and authorization and data-level encryption required.</td></tr>
<tr><td rowspan="2">Physical Information</td><td rowspan="2">No restrictions</td><td rowspan="2">Reasonable precautions to restrict display and access.</td><td colspan="2">Do not keep unattended in your work area and store with appropriate physical security with access only by authorized personnel.</td></tr>
<tr><td>The information shall be locked (e.g., in cabinet or drawer).
The office rooms shall be locked outside of the working hours.</td><td>The information shall be locked in a safe.
The office rooms shall be locked outside of the working hours.</td></tr>
</table>

Information Classification Levels				
	PUBLIC	**GEA INTERNAL**	**GEA CONFIDENTIAL**	**GEA STRICTLY CONFIDENTIAL**
Removable / External media	No restrictions		Allowed on encrypted media.	Allowed on encrypted media not to be transferred to third parties even after deletion of stored information.
Transmission (see also "Confidentiality" and "Access" above)				
General			For external recipient's confidentiality agreement / NDA required (see "Confidentiality" and "Access" above). The transmission must be **documented** (e.g., by email, minutes of meetings or correspondence).	
Email	No restrictions		Encrypted emails and protected attachment are required.	
File sharing	No restrictions	No internal restrictions.	Up-to-date secure transport encryption required. Up-to-date secure data level encryption required. Sharing via fax not allowed.	
		For external recipients sharing only via authorized up-to-date secure encrypted content collaboration platform (e.g., SharePoint Online).		
Postal mail (including courier)	No restrictions	Regular mail allowed.	Registered mail and opaque envelope with the label "Personal".	If possible, no external sharing. If required, only personal handover against signature in a double envelope, each glued together. The closure of the inner envelope must be signed or enclosed.
	No restrictions	Shall not be exchanged verbal in public locations.		

Information Classification Levels				
	PUBLIC	**GEA INTERNAL**	**GEA CONFIDENTIAL**	**GEA STRICTLY CONFIDENTIAL**
Verbally, including using technical equipment (e. g, web video conference tools or mobile phones)		All methods of internal approved communication systems may be used.	The confidentiality level of the information shall be recognizable at the start of the communication. Ensure that no third parties listen to your conversation.es containing confidential or strictly confidential information shall not be left on answering machines, voice boxes etc.	The confidentiality level of the information shall be recognizable at the start of the communication. Ensure that no third parties listen to your conversation. Messages containing confidential or strictly confidential information shall not be left on answering machines, voice boxes etc. Record (e.g., in a memo or email) which information was transmitted to whom – for documentation purposes.
			The communication system used shall be internally approved (e. g. Skype, MS Teams, GEA mobile phones).	If possible, no use of any communication systems – only direct conversation in secure environment without any mobile devices in the room.
Destruction method				
Disposal of removable / external devices	No specific requirement	Return device to IT where it will be at least securely overwritten prior disposal with the intent that original data is non-retrievable.	Return device to IT where it will be at least securely purged prior disposal with the intent that original data is non-retrievable.	Return device to IT where it will be securely physical destroyed.
Disposal of hard copies	No specific requirements.	Shredder or confidential waste bins.	Shredder sized not larger than 160mm^2 or confidential waste bins.	Shredder with orders of magnitude not bigger than 30mm^2.

Information Classification Levels				
	PUBLIC	**GEA INTERNAL**	**GEA CONFIDENTIAL**	**GEA STRICTLY CONFIDENTIAL**
Downgrading	No specific requirements.	Downgrading to PUBLIC shall be approved by the communication department or the acceptance of the downgrading rules shall be performed and documented.	Downgrading to GEA INTERNAL shall be approved by the Information Owner or by the direct manager. The downgrading shall be documented. Downgrading to PUBLIC shall be additionally approved by the communication department or the acceptance of the downgrading rules shall be performed and documented.	Downgrading shall be approved by the Information Owner and the GEA CISO shall be informed. The downgrading shall be documented. Downgrading to PUBLIC shall be additionally approved by the communication department or the acceptance of the downgrading rules shall be performed and documented.

Figure 4: Information handling matrix

Note: All of the above measures, in particular technical means, are subject to availability.

Additional technical means and software to protect information are to be introduced gradually by IT. This includes, for example, additional encryption options, SharePoint solutions or digital data rooms, logging software or live monitoring to allow digital tracking and alarms in case of unusual activities.

6.2. Specific Information Protection Labels

6.2.1. « Protection » Notice (mandatory)

Regardless of the classification in the four levels of confidentiality described in this Policy, a protective notice shall be used in the following form for all documents with technical content:

"*The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization is prohibited. Offenders will be held liable and the assertion of damages and/or other claims are reserved. All rights reserved in the event of the grant of a patent, utility model, design or other intellectual property rights*."

6.2.2. «Copyright» Notice (mandatory)

Information that represents a personal, intellectual creation and is therefore independent creative achievement is also protected by copyright against unauthorized use. The holder of the exclusive rights of use and exploitation may assert this protection. For all information that GEA employees have created, the holder is the GEA company where the employee is employed.

A copyright notice states that the GEA company mentioned in the note is entitled to assert the legal protection. Documents must therefore be accompanied by a copyright notice as follows:

"Copyright © <GEA Group company> <Year>All Rights Reserved",

Or

"Copyright © <GEA Group companies> <Year> All rights reserved"

e.g. "Copyright © GEA Group AG 2021 – All rights reserved". The copyright notice shall indicate the year in which the document was created or, if it was earlier, the first publication of the content of the document.

6.2.3. «Personal» Notice (optional)

Any information intended only for a specific person may be accompanied by the "Personal" shipping notice, irrespective of the classification. This defines that this information is intended only for a specific person.

The "Personal or Representative" shipping note may be used to allow an officially appointed representative of the addressee to open the incoming mail.

7. Special handling policies

Summary
This Policy governs the handling of information not conclusively. Other existing legal regulations, policies, guidelines and procedures must be observed.

Legal regulations regarding information classification (e. g. national security or export control regulations) are unaffected by the directions in this document.

Within GEA, there are further Policies that may concern and complement the protection and handling of information. For example, the following functions/topics:

- Protection of patents and inventions
- Protection of intellectual property (IP)
- Data protection in accordance with legal requirements
- Archiving
- Document control (labeling, verification, release, etc.)

These other policies exist independently of this document and their rules must be observed in addition to this Policy. Further information can be found on the GEA intranet GEA Insights Guidelines & Policies.

Note: In particular, this applies to policies on data protection and compliance. Among other things, this means:

- Personal data must only be processed in compliance with the established principles as set out in the GEA Data Protection Policy. Contact details and further information can be found on the GEA intranet Portals Global Initiatives Program Digital Security.
- The exchange of competitive information to competitors is only permissible with involvement of the GEA legal department as set out in the GEA Competition Policies.

Summary
The management of the Responsible Units and line managers are expected to support the implementation of this Policy.

7.1. Responsibility of GEA Management and Line Manager

The management of GEA, particularly of the Responsible Units, is expected to lead by example (“tone at the top”). Our managers are the first contacts to ensure that the employees and concerned third parties in their area of responsibility know, understand and follow the rules and instructions set out in this Policy. This

means that personal talks between line managers and employees as well as concerned third parties regarding awareness of information protection are just as necessary as organizational measures. If the Responsible Units and/or line managers need support, they can reach out to the contacts specified in *chapter 2.2.*

7.2. Training

The content of this Policy is to be conveyed to all employees and concerned third parties and training is to be documented. Responsibility for providing training material and execution of trainings rests with the IP management and the information security teams. Responsible Units and their line managers are responsible for the involvement of their employees and concerned third parties. Regarding new employees, the HR department shall ensure that they are assigned to an obligatory training at the start of their work for GEA. For clarification: Training is also to be provided to external staff as part of their security training.

8. Reporting

Summary
Incidents must be reported in a timely manner! This enables mitigation actions to keep potential damages to a minimum.

Due to the far-reaching importance of information protection, adherence to this Policy is a collective task. If there are indications of a violation of these Policy rules, a loss of information or unusual activities (hereafter "**Incidents**"), GEA expects all employees and concerned third parties to notify line managers or the contacts specified in *chapter 2.2* accordingly (i.e. IP Ambassadors, IP Managers, IT Security). GEA managers shall ensure that incidents, such as potential information loss or unusual activities, are reported to the contacts.

If an employee or third party is involved in an incident, a timely reporting is expected and will be considered in his favour. In particular, timely reporting enables prompt initiation of mitigation actions and thus minimization of potential damage.

9. Sanctions for Policy Violations

Violations of this Policy may lead to disciplinary and/or legal consequences for GEA managers, employees or third parties. Employees may be affected by labour law measures. GEA reserves the right to initiate additional measures against individuals who disregard the directives set forth in this Policy.

10. Glossary

The information security glossary is available at the Information Security Portal of GEA's intranet where it is continuously updated.

Date	Review and Revision
2021	Review without changes
2022	Review without changes
2023	Review without changes (layout change with new branding)
2024	Review without changes

PUBLIC