REINHAUSEN

Guidelines for the Classification and Handling of Information of the REINHAUSEN Group

Version 1.2 (01.04.2012)

Area of application:

These guidelines are binding for all employees of the companies listed below (subsequently referred to as REINHAUSEN companies). These guidelines also apply to all suppliers, external service providers and partner companies of these companies to the extent that this is not specified otherwise in the individual sections.

Company	Valid as of
Maschinenfabrik Reinhausen GmbH	01.12.2009
Reinhausen Plasma GmbH	01.12.2009
Reinhausen Power Composites GmbH	01.12.2009
Highvolt Prüftechnik Dresden GmbH	14.06.2010
Messko GmbH	14.06.2010
MR China Ltd.	14.06.2010
MR do Brasil Ltd.	14.06.2010
MR Japan Corp.	14.06.2010
MR Manufacturing Inc.	14.06.2010
MR Russland (OOO MR)	14.06.2010
PT Reinhausen Indonesia (RID)	01.04.2012
Reinhausen 2e d.o.o. (RSI)	01.04.2012
Reinhausen Asia-Pacific Sdn Bhd.	14.06.2010
Reinhausen Australia Pty. Ltd.	14.06.2010
Reinhausen Canada Inc.	14.06.2010
Reinhausen Italia S.r.l.	14.06.2010
Reinhausen Korea Ltd.	14.06.2010
Reinhausen Luxembourg S.A.	14.06.2010
Reinhausen Manufacturing Inc.	14.06.2010
Reinhausen Middle East FZE	14.06.2010
Reinhausen South Africa (Pty) Ltd.	14.06.2010

Document history

Version	Date	Author	Comments
1.10	11.05.2010	FID Dr. Bauer	Translation of German guideline to English
1.20	28.03.2012	FID Dr. Bauer	Subsidiary JEPC deleted, RSI and RID included In the list in 4.2 added “data assigned to individual persons according to German Data Protection Act” Revision of chapter 6.

Release

Version 1.0 in German language has been released by General Management of Maschinenfabrik Reinhausen GmbH for the whole REINHAUSEN Group at Nov. 26th, 2009.

Contents

1. Fundamentals of Handling Information

- The REINHAUSEN Group is conscious of the significance of protecting information since its misuse can lead to great material and non-material damage. The classification and suitable handling of information is an important element in the avoidance of such damage.
- Information can be available in different forms (e.g., in electronic form as a file, in physical form as a printout, or also in the form of the spoken word). Information is classified by the confidentiality of its content. The degree of confidentiality reflects the degree of impact if information is misused. It also specifies how information is to be handled. The classification of information is not based on the medium used.
- In principle, only those persons should have access to critical company information who need this information to accomplish their jobs (i.e., principle of "need-to-know").

2. Area of Application

- These guidelines are directed to the employees of the REINHAUSEN Group corresponding to the areas of application stated on the cover sheet (subsequently referred to as REINHAUSEN companies). These guidelines are also directed to all suppliers, external service providers and partner companies to the extent that this is not specified otherwise in the individual sections.
- These guidelines are binding on every employee. They will be made accessible to every employee (on REINHAUSEN GroupNet, among others).
- When information is exchanged with an external party (e.g., business partner), every employee must influence this business partner to adhere also to the requirements of these guidelines.
- Violations of the guidelines may result in occupational, civil or criminal prosecution. The responsible company reserves the right to check the adherence to these guidelines at regular intervals.

3. Responsibilities and Roles

3.1. Information owner

- The information owner is responsible for the classification of information in his/her area of responsibility. Typically such persons belong to business unit, department or project management or have overlapping functions (e.g., information security, occupational safety, or data security). He/she specifies the circle of users (internal and, if applicable, external persons) by name or by their roles and rights. He/she can also delegate the responsibility of classifying information to other employees.
- Those information owners may deviate for certain functional reasons from the regulations of the guidelines for certain groups of information users, certain types of information exchange or in individual cases. Each deviation must be announced and documented.

3.2. Authors

- The author works under the information owner and takes over the classification of the information from this person. He/she has no special rights with regard to revealing this information to others.

3.3. Users

- Users of a piece of information are all persons who are authorized to receive this information. The user acts in accordance with the rules of these guidelines to the extent that the information owner has not specified otherwise.

3.4. Core Users

- The information owner specifies the core users. Usually the range of core users is department overlapping and includes all employees who regularly process certain information within a process. Core users of a piece of information are entrusted with the handling of this information and are appropriately trained and sensitized by the person responsible for the information.
- Examples of core users of a piece of information are the employees of the personnel department regarding personnel files or of department-overlapping project teams – also with external advisors – regarding project data.
- The core user concept reduces the labeling effort. (See 5.2, Implicit Labeling.)

3.5. Technical staff

- Due to their special role, technical staff (e.g., administrators, archivists) handle classified information. They are not authorized to use this information outside the functions of their jobs (e.g., monitoring, evaluation for invoicing purposes).

3.6. Auditors and Investigators

- This circle of persons has explicit access to information for the purposes of investigation orauditing. This circle of persons includes, for example, public government officials (e.g., the police, district attorneys, etc.) or tax auditors and certified accountants.

4. Classification of Information – Levels of Confidentiality

4.1. Fundamentals

- The information that exists within the REINHAUSEN Group is classified by its confidentiality. The confidentiality is based on the significance for business processes or the potential damage when misused.
- Information is classified in the following levels of confidentiality:
    - Public
    - Internal
    - Confidential
    - Strictly confidential
- Examples of the classification of individual documents into levels of confidentiality can be found in GroupNet under security management.

4.2. Size of Damage

A knowledge of the potential damage that can be caused by undesired revelation of information or its transfer to third parties is important in the correct classification of information into the appropriate levels of confidentiality.

Size of Damage	Damage to the Company	Engl./Germ. Class	Examples
High up to existential endangerment	• The entire company is affected. • Very great damage to business and company • Serious legal consequences including prison sentences • Significant loss of standing and trust of several customers or suppliers	Strictly confidential/ Streng vertraulich	• Strategy documents • Data about severe product failures • Technical benchmarking • Passwords • Letter to supplier with data of new product development, …

Size of Damage	Damage to the Company	Engl./Germ. Class	Examples
Medium	• One business area is affected. • Significant financial damage • Legal consequences including administrative offenses and fines • Irritation and image loss of single customers or suppliers • Data assigned to individual persons according to German Data Protection Act	Confidential / Vertraulich	• Informations which have been acquired under a non-disclosure agreement • CRM-system data • Cost calculations • Documents of applicants • Labour contracts • Results of employee appraisal • Monthly report of a company, …
Minor	• No far-reaching consequences	Internal / Intern	• Orgcharts • Address change of an employee, …
None	• No damage since information is intended for the public	Public / Offen	• Product flyer • List of references, …

4.3. Levels of Confidentiality

The four levels of confidentiality will now be discussed together with the basic rules for identification, forwarding and security as well as the potential for damage when the information is misued.

"Public"

- This information does not need any labeling. Its unauthorized use cannot damage the company in any way. No restrictions apply to the handling of public information.
- The information owner decides whether a document will be made public or not.

"Internal"

- Implicit labeling (see 5) is sufficient for this information.
- Internal information can be passed on without restriction to employees of REINHAUSEN companies or to external offices when business requires (“need-to-know”).
- Damage to the company when the information is misused: minor.

"Confidential"

- Implicit labeling (see 5) is sufficient for this information if the information does not leave the circle of core users.
- If business requires, confidential information can be passed to certain users (i.e., those appointed by name or role by the information owner).
- If passed on to people other than core users, the information must be explicitly identified as "confidential" beforehand.
- Damage to the company when the information is misused: Medium

"Strictly confidential"

- This information always requires explicit labeling (see 5.1).
- The information may only be passed on to certain users named by the information owner . Recipients may not pass on the information to other users without the express permission of the information owner.

- Regardless of all this, the circle of users must be kept as small as possible.
- Damage to the company when the information is misused: High up to existential endangerment.

4.4. Changes in the Classification / "Life History" of Information

- A piece of information can pass through various levels of confidentiality. This means that information intended for publication may still have to be classified and handled as confidential as long as it has not yet been publicized (e.g., draft of technical documents → publication of the technical documents).
- The classification can only be changed by the information owner.

4.5. Offers, Contracts

- Offers and contracts with companies concerning generally offered services for generally familiar return services without special side agreements are classified as "Internal." Other offers and contracts must be classified as "confidential" or "strictly confidential" depending on their content.
- Further requirements (e.g., public procurement law) are not affected by this.

4.6. Information Belonging to Third Parties

- The REINHAUSEN Group maintains the confidentiality of customer and supplier information and takes appropriate precautions. The legal and contractual regulations will be observed.
- Basically, information which is supplied to the REINHAUSEN Group and which is identified with a class of confidentiality will be handled according to the same rules as those which apply to the internal information of the REINHAUSEN Group

5. Labeling of Information

5.1. Explicit Labeling

- When information must be classified explicitly as "confidential" or "strictly confidential," the medium carrying the information (e.g., sheet of paper, DVD) must be clearly labeled as "confidential" or "strictly confidential."
- With multiple-page documents on paper or in electronic file format, each page must be labeled appropriately in bold letters in the middle of the header or footer line. The total number of pages must also be clearly readable.
- With "confidential" information, the circle of recipients must be given on the information carrier (e.g., "department ABC").
- With "strictly confidential" information, the circle of recipients must be indicated BY NAME (distribution list) on the information carrier.
- "Confidential" information on paper must be closed with adhesive tape when sent internally in the interoffice mail folder and a mark of the sender affixed. With external mail in a closed envelope, the recipient must be named and the comment "personal" added. When there is a risk of unauthorized third parties opening "confidential" information or "strictly confidential" information in general, the information must be placed in two envelopes (exceptions can be specified by the person responsible for the information). The inner envelope must indicate the class of confidentiality. The outer envelope may not contain any indication of confidentiality.

- Explicit labeling always takes precedence over implicit labeling.

5.2. Implicit Labeling

- Implicit labeling within a core user area (see 3.4) simplifies daily work. The information or the information carrier itself does not need to be identified. The user is aware of the classification based on the type of information and because the user has been appropriately trained and sensitized by the information owner.
- Implicit labeling can be used at the most for confidential information as long as this information does not leave the core user area. Confidential information which leaves the core user area and strictly confidential information in general both require explicit labeling with the class of confidentiality.
- When documents are created the newest templates for Microsoft Office files have to be used, as soon as they have been made available by OI department. If the template requires the labeling of a level of confidentiality, this has to be done according to chapter 4.

5.3. Documents in Draft Status

- Documents which are still in draft status must be labeled as such with the note "Entwurf" (German) or "Draft."
- However, this does not mean that the document does not have to be classified in its particular class of confidentiality.

6. Non Disclosure Agreements

- Every external service provider and supplier must commit to the nondisclosure of confidential information if he or she has potential access to data or information of the REINHAUSEN Group. This can be the case even before a contract is signed, for example during the negotiation phase. Then he or she has to sign a non disclosure agreement (NDA) before. Moreover it is necessary that a contract, which is signed afterwards, must also include a non disclosure clause.
- NDAs for suppliers or service providers are prepared by the Purchasing Department and for all other recipient groups by the Legal Services Department. The orderer has to classify the data with the right confidentiality level together with the responsible information owner and to inform afterwards the respective department which prepares the NDA.

7. Rules for Handling Information

The rules for handling information are summarized in appendix 1.

8. Connection of MR Subsidiaries via e-mail

Appendix 2

What is labeled?	Public	Internal	Confidential	Strictly Confidential
Labeling of information in paper format	None	Implicit (i.e., the user is familiar with the type of information and can deduce the class of confidentiality from this, without this having been identified on the information carrier)	Implicit among the core users Explicit when the information leaves the circle of core users: – With "confidential" in the subject line and header or footer of each page. – Distribution circle on first page – Page numbers indicated as "page x of y"	Explicit: – With "strictly confidential" in the subject line and header or footer of each page. – Distribution circle by name on first page – Page numbers indicated as "page x of y"
Labeling of electronic information	None	Implicit	Implicit among the core users Explicit with "confidential" when the information leaves the circle of core users.	Explicit: – With "strictly confidential"

What do I do for …?		Public	Internal	Confidential	Strictly Confidential
Duplication via copy machine, printer		No restrictions	No restrictions	Supervision of the duplication procedure	Only after release by the information owner, supervision of the duplication procedure
Forwarding		No restrictions	To all employees of the REINHAUSEN companies or authorized service providers or customers – to the extent required for business purposes.	Passing on to core user or to user defined (by name or role) by the information owner if required for business purposes. For external service providers, an agreement of non-disclosure must exist.	Passing on only to users defined by name by the information owner. Recipients may pass on strictly confidential information only after explicit permission from the information owner. For external service providers, an agreement of non-disclosure must exist.
Transmission via post office	**Internal**	No restrictions	Office mail folder	Close office mail folder with adhesive strips and affix user's mark. Use double envelopes if there is a risk of being opened by an unauthorized third party exists.	Use double envelopes. Mark the inner envelope with the class of confidentiality. The outer envelope may not contain any indication of confidentiality.
	External	No restrictions	Normal letter	Closed envelope, add "personal" to recipient's name. Use double envelopes if a risk of being opened by an unauthorized third party exists.	Use registered letter, courier delivery. Add "personal" to recipient's name. Use double envelopes. Mark the inner envelope with the class of confidentiality. The outer envelope may not contain any indication of confidentiality.
Transmission via e-mail (Table for internal or external link of the subsidiaries to GroupNet under security management)	**Internal**	No restrictions	No restrictions	Send with message option "confidential"	Send with message option "confidential"
	External	No restrictions Attachments usually as PDF document	No restrictions Attachments usually as PDF document	Contents as attachment encrypted with WINZIP (instructions in GroupNet), attachments usually as PDF document	Contents as attachment encrypted with WINZIP (instructions in GroupNet), attachments usually as PDF document
Transmission via fax	**Internal**	No restrictions	No restrictions	Only after previous announcement	Only after previous announcement
	External	No restrictions	Cover sheet with number of pages	Only after previous announcement Cover sheet with number of pages	Prohibited
Verbal transmission		No restrictions	Only permitted when no unauthorized persons are listening in.	Only permitted when no unauthorized persons are listening in.	Only permitted when no unauthorized persons are listening in. No messages left on answering machines /in mailboxes. Secure identity of the person talked with.
Destruction of information in paper format		No restrictions	Waste paper baskets at the office, not for personal data	Secure destruction (e.g., in the data protection container)	Shred

Information in IT Systems	*Public*	*Internal*	*Confidential*	*Strictly Confidential*
Storage in IT systems / applications of the REINHAUSEN companies	No restrictions	Storage under consideration of access rights. If necessary, explicit allocation of access rights.	Storage under consideration of access rights. If necessary, explicit allocation of access rights.	Storage under consideration of access rights. Check current access rights regularly. If necessary, explicit allocation of access rights.
Mobile devices (Notebooks, MDAs)	No restrictions	No restrictions	Encryption required for notebooks. Avoid storage of confidential data on other mobile devices.	Encryption required for notebooks. Storage of strictly confidential data prohibited on other mobile devices.
Mobile data carriers (CDs, DVDs, USB sticks)	No restrictions	No restrictions	Encryption required (e.g., with WINZIP). See instructions in GroupNet.	Encryption required (e.g., with WINZIP). See instructions in GroupNet.
Placement on the Internet (blogs, forums)	No restrictions	Prohibited	Prohibited	Prohibited
Deletion of electronic information	Deletion from file system	Deletion from file system	Deletion from file system	Deletion from file system
Disposal /destruction of hardware and mobile data carriers (CDs, DVDs, USB sticks)	No restrictions	Hardware: return to Local Security Manager Mobile data carriers: Physical destruction	Return to Local Security Manager for disposal and destruction	Return to Local Security Manager for disposal and destruction

Physical Storage and Filing of Information	*Public*	*Internal*	*Confidential*	*Strictly Confidential*
General	No restrictions	Prevent unauthorized access by third parties with simple measures. A suitable technical implementation must be provided by the person responsible for the information, based on the degree of danger in individual cases.	Prevent access by unauthorized third parties. A suitable technical implementation must be provided by the person responsible for the information, based on the degree of danger in individual cases.	Prevent access by unauthorized third parties. A suitable technical implementation must be provided by the person responsible for the information, based on the degree of danger in individual cases.
In company buildings of the REINHAUSEN companies	No restrictions	Lock the office when possible. Special regulations are possible for areas that are physically secured in addition.	Lock the office when possible. This measure is sufficient if it is ensured that no one except the person with the key can enter the office. Otherwise: When you are away for longer periods of time (more than 30 minutes), lock the information away. Special regulations are possible for areas that are physically secured in addition.	Lock the office when possible. This measure is sufficient if it is ensured that no one except the person with the key can enter the office. Otherwise: When you are away from physically secured areas for longer periods of time (more than 30 minutes), lock the information away. In areas which are not separately physically secured, lock the information away for periods of absence longer than 10 minutes.
While traveling (e.g., hotel) or at home	No restrictions	Locked room (e.g., hotel room, home office)	Store safe from access (e.g., lock up in hotel safe).	Store safe from access (e.g., lock up in hotel safe).

Connection of MR-subsidiaries
Anbindung der MR-Tochtergesellschaften

	Name	Land / Country	Anbindungsart (Mailverkehr) Connection Type (Mail traffic)
MR-PQ	Erfurt / Berlin	Germany	intern / internal
RP	Reinhausen Plasma GmbH	Germany	intern / internal
MRT	MR China	China	intern / internal
MRM	MR Manufacturing	China	intern / internal
RA	Reinhausen Australia	Australia	intern / internal
RAP	Reinhausen Asia-Pacific	Malaysia	intern / internal
RI	Reinhausen Italia	Italy	intern / internal
RKR	Reinhausen Korea	South Korea	intern / internal
RME	Reinhausen Middle East	U.E.A	intern / internal
RPC	Reinhausen Power Composites GmbH	Germany	intern / internal
MS	Messko GmbH	Germany	intern / internal
RSI	Reinhausen 2e d.o.o.	Slovenia	intern / internal
RLU	Reinhausen Luxemburg	Luxembourg	intern / internal
RZA	Reinhausen South Africa	South Africa	intern / internal
RM	Reinhausen Manufacuring	USA	intern / internal
MRB	MR do Brasil	Brazil	intern / internal
RID	Reinhausen Indonesia	Indonesia	intern / internal
HV	Highvolt Prüftechnik Dresden GmbH	Germany	extern / external
EMR	Easun-MR Tap Changers	India	extern / external
MRJ	MR Japan	Japan	extern / external
MRR	MR Russland	Russia	extern / external
ITASS	Iran Transfo After Sales Services Co.	Iran	extern / external
RCA	Reinhausen Canada	Canada	intern / internal