# Key Document Information

| Approval by body<br>RT IT-Risk & Comp | Date of approval<br>3/16/2016 | Effective since<br>3/16/2016 |
|---|---|---|
| Competent central division<br>AS-IT-CS | Expiration of grace period<br>5/21/2018 (for parts) | Effective until |
| Responsible contact person<br>Dr. Volker Batroff | E-mail<br>volker.batroff@evonik.com | Phone<br>+49 201 177 2726 |

| Purpose / Short description |
|---|
| The maintenance of confidentiality of information serves to protect Evonik against its competitors, e.g. the retention of its technological advantages or other significant competitive advantages. It also serves to protect the rights of third parties, e.g. from contractual obligations or legal requirements (e.g. Section 241 BGB, the protection of personal data in accordance with the BDSG (Federal Data Protection Act)). This procedure regulates the classification, communication, and handling of information in the working environment at Evonik. To ensure adequate protection of important information, protection classes are defined and the handling of these classes is described. The primary goal is to identify strictly confidential information and to protect it from loss or unauthorized disclosure.<br>Grace Period:<br>For implementation of the specifications regarding minimum standards for office areas, in particular, shredding machines, security cabinets, and safes, and also for the existing contracts with waste disposal companies, a grace period will apply until May 20, 2018. |
| Scope of application and limitation |
| This procedure is valid worldwide for all employees of Evonik Industries AG and its affiliated companies in accordance with Sections 15 et seq. German Stock Corporation Act. In other companies, in which Evonik Industries AG holds a stake, efforts should be made to comply with the procedure. |

| Superior documents | Document ID of superior documents |
|---|---|
| | |
| **Supersedes** | **Document ID of supersedes** |
| | |

| Changes to the previous version |
| --- |
| Revised Sections 4.2.5 and 4.2.6 |

Document owner, signatures, valid date, scope in terms of organizational unit, comments on training, distribution list, time span for periodic document review and retention time for this document: see QSI document information.

# Table of Contents

Page No.

# 1 Purpose

The maintenance of confidentiality of information serves to protect Evonik against its competitors, e.g. the retention of its technological advantages or other significant competitive advantages. It also serves to protect the rights of third parties, e.g. from contractual obligations or legal requirements (e.g. Section 241 BGB, the protection of personal data in accordance with the BDSG (Federal Data Protection Act)).

This procedure regulates the classification, communication, and handling of information in the business environment. To ensure adequate protection of important information, protection classes are defined and the handling of these classes is described.

The primary goal is to identify strictly confidential information and to protect it from loss, unauthorized disclosure or other misuse.

# 2 Roles & Responsibilities

| Role | Responsibility |
|---|---|
| Line Manager | The line managers are the executive bodies of the segments that are directly subordinate to the Executive Board of Evonik Industries AG and the heads of the central and service areas, regions (Regional Presidents) and other units that are directly subordinate to the Executive Board of Evonik Industries AG (definition from the Compliance Policy). They are responsible for the implementation of and compliance with this procedure in their areas of responsibility. |
| Information Owner | Any Evonik employee who makes decisions on access to information assets (data, information, software, hardware or IT services) is an information owner. The responsible information owner must define the information assets to be protected and the protection requirement. As a rule, the creator of the information is also the information owner. |
| Head of Corporate Security | The head of Corporate Security controls Group-wide the protection of employees, sites, facilities and transports, and also of particularly sensitive information. |

# 3 Definition

(a) The "need-to-know-principle" describes the handling of information as follows: It should only be disclosed to those employees who need to know it, and only to the extent necessary to enable fulfillment of the tasks of the employees. Non-public operational information is only to be disclosed to external parties on the basis of legal requirements or in the scope of contractual relationships and only to the extent necessary, as long as the external parties have effectively undertaken to handle this information confidentially.

(b) External parties are natural persons who are not employees of Evonik and legal persons who do not work for Evonik.

(c) Publications and presentations include all publications, presentations, speeches, seminar contributions or similar publications of Evonik information to external parties.

(d) A creator is any natural person who initially creates a document or who significantly changes or edits the document.

(e) Information carriers are media with which information is recorded, processed, saved or transferred. These include speech, paper documents in the broadest sense, telecommunications, data carriers (e.g. CD/DVDs, USB sticks, external drives, memory chips), IT systems, internet information exchange platforms, teamrooms, fileshares or file attachments, application systems and communication systems such as the internet, company intranets and extranets.

(f) Secure deletion refers to the overwriting of data to be deleted at least three times with random numbers or bit patterns using an appropriate software program.

(g) Information puzzling means that the information is broken down into small fragments and made accessible by different paths (e.g. via different communication media) and processed. This makes unauthorized access to the information more difficult. Each of the information fragments only contains meaningful content in combination with the remaining fragments of the whole.

(h) Breakpoint principle means that it is not possible to view an entire piece of information unless it is necessary. In line with the need-to-know principle, you can only view those parts, that is, fragments that are required in the particular case. In this way, the overall context can be obscured and potential damages through misuse of the information can be significantly reduced.

# 4 Description

## *4.1 Information Classification*

At Evonik, the information owners classify their information in one of four classes with regard to information protection:

- Public
- Internal
- Confidential
- Strictly confidential

The examples shown in this document are purely informational and suggestive unless indicated as mandatory. The information owner may reclassify information to a higher level at any time. In justified cases, the information may also be reclassified to a lower level. ***Appendix 1*** contains a list of examples of information classification. The ownership of information can also change. Reclassification of information can only take place in accordance with the specifications in Section 4.2.6.

## *4.2 Confidentiality Classes*

### 4.2.1 Confidentiality class "Public"

Information is to be classified as "public" if it is freely available and accessible or if, following a publication process within Evonik, it has explicitly been made public. Any user and any person outside the company is entitled to gain knowledge of the content of the information. This information is not subject to any further restrictions.

No access restrictions are required for public information.

Information / Examples:

- Internet content
- Corporate responsibility reports
- Press releases, TV and radio reports
- Public discussion contributions (e.g. at symposia)

- Public product presentations

### 4.2.2 Confidentiality class “Internal”

Information is to be classified as “internal” if it is not to be disclosed or passed to third parties outside Evonik, as the possibility cannot be ruled out that publication of the information could result in damage to Evonik.

Internal information is only intended for employees and external business partners who have a legitimate right to knowledge of the information.

Information / Examples:

- Publications in the intranet
- Internal regulations (policies, newsletters, instructions)
- Internal communication that is neither confidential nor strictly confidential
- Organizational charts at management level
- General marketing information

### 4.2.3 Confidentiality class “Confidential”

Information is to be classified as “confidential” if its disclosure or passing to third parties could result in financial damage, negative legal consequences, or damage to the company's reputation. In general, this class contains all information that is important for the economic success of individual business units. In particular, this includes all information which, if known, would be of value to competitors and would weaken the position of Evonik in the market.

Information that is designated as “confidential” is intended for a group of recipients determined by the information owner. These recipients require the information in order to perform their tasks (need-to-know principle). Any forwarding of the information beyond the group of defined recipients may only be carried out in line with the need-to-know principle. In case of doubt, the information owner should be consulted.

Information / Examples:

- Marketing strategies

- License contracts
- Specific supplier data
- Not yet published product modifications
- Individual prices (protected by confidentiality agreement)
- Information relating to pant availability
- Organizational charts
- Personal data that arises in the context of an employment relationship
- Personal data that arises in the context of customer/supplier contacts
- Information relating to the internal network topologies or security architectures
- Medium-term planning of a company unit
- Copies, data backups, and archiving of confidential information
- Confidential information of third parties

Obligatory classification:

- Filing a patent application between the date of filing and publication or withdrawal before publication

### 4.2.4 Confidentiality class "Strictly Confidential"

Information is to be classified as "strictly confidential" if its disclosure or passing to third parties could result in substantial damage to the business purposes and objectives of the company, serious negative legal consequences, an impact on the share price, or serious damage to the company's reputation or the company's representatives.

This is usually information that is very important for the success and continued existence of company units or the entire Group.

Information that is designated as "strictly confidential" is intended exclusively for defined persons to be nominated by the information owner. These recipients require the information in order to perform their tasks.

Any forwarding or making available of strictly confidential information to other persons requires the express permission of the information owner.

Information / Examples:

- Sales figures, contribution margins and manufacturing costs of many products of Evonik
- Unpublished new product plans or development plans
- Formulations of key products
- Product simulations
- Confidential information on the control and application of procedures
- Start-up documentation of plants
- Information that could impact the Evonik share price, e.g. information on company disposals
- Copies, data backups, and archiving of strictly confidential information
- Strictly confidential information of third parties

Obligatory classification:

- Reported inventions prior to filing a patent application
- Medical documentation (including patient data, health data, data on sexual activity)
- Information on personal relationships (including income, garnishments, family relationships, racial/ethnic origin, political opinions, religious and philosophical convictions)
- Information that has already been classified by third parties as strictly confidential (e.g. correspondence with public prosecutors, lawyers)
- Bank details of employees
- Documents relating to social counseling and operational integration management
- Personal information relating to company pension schemes

### 4.2.5 Excerpts of classified information

In practice, it is necessary from time to time to make use of excerpts from documents, documentation and presentations for specific operational purposes. In particular, in cases where the underlying information or documents contain (strictly) confidential content, you must ensure that

(a) the withdrawal of partial information is appropriate for other purposes, and that Evonik suffers no damage as a result and
(b) the newly created partial information or partial document is classified.

In each of these cases, the "withdrawal" and any reclassification must take place in consultation with the information owner of the original information or document if the underlying information is strictly confidential.

### 4.2.6 Reclassification of information

If the specific classification of information or of a document no longer appears appropriate (downgrade or upgrade), the information owner should be notified of this and given relevant reasons. The information owner is responsible for reviewing the current classification.

If it is determined that information is not classified at all, the information owner must be notified immediately. The information owner should carry out the classification immediately.

When classifying information as either "confidential" or "strictly confidential", you should check whether

- legal requirements correspond to such a decision (e.g. professional discretion),
- the classification can be time-limited (e.g. by a date or event).

If information from different classifications is to be distributed together, then the regulation for the highest existing classification applies.

Information can be reclassified to a lower level by the information owner if the protection class is no longer applicable, e.g. after a long period of archiving.

In each of these cases, the reclassification must take place in consultation with the information owner of the original information or document if the underlying information is strictly confidential.

## *4.3 Minimum Requirements for Equipment and Use of Areas in which (Strictly) Confidential Information Is Processed or Stored*

### 4.3.1 Business office

Employees must configure their work environment in such a way that access to (strictly) confidential information by unauthorized persons is prevented. This means in detail:

(a) Offices or access to open-plan offices must always be locked in the absence of the office user(s).

(b) Even if the employee's workplace is left unattended only briefly, the computer should be locked (e.g. Windows key + "L" or by removing the Smart-Card).

(c) If the employee leaves the office for a longer period (e.g. for several hours or after work), the computer/laptop should at least be hibernated. In addition, the devices must be physically secured against removal, that is, the laptop must be secured with a Kensington lock, for example, or mobile telecommunications devices / data carriers must be locked in suitable cabinets.

(d) During working hours, as far as possible, only those documents required for the transaction currently being processed should be on the desk.

(e) Confidential documents must be stored in cabinets which are locked in the absence of the user.

(f) Strictly confidential documents must be stored in office security cabinets or safes and the security class of these cabinets/safes is to be determined following individual risk assessment (environment/criticality of the documents) in consultation with the security organization. In the absence of the user, the security cabinets or safes must be locked. You can find examples of permitted security cabinets or safes in the Evonik procurement tool *Hubwoo.*

(g) All keys for safes and security cabinets for storage of (strictly) confidential documents must always be handled securely. The following options are possible:

- Employee takes keys (adds them to private key ring) and handles with care
- They are stored in a key safe, possibly with PIN code lock (for permitted examples, see Evonik procurement tool *Hubwoo)*

Key safes must be of at least the same security class or have the same burglary protection as the security cabinets/safes whose keys are to be stored in the key cabinet / key safe.

(h) Particular care must be taken with the storage of technical items which enable access to Evonik sites, premises, networks and information (e.g. company ID, tokens, dongles, etc.).

(i) (Strictly) confidential information must be removed from walls and flipcharts after use, boards must be cleaned immediately (clean-wall, clean-flipchart and clean-board policy).

(j) (Strictly) confidential documents must be destroyed with a document shredder of at least security level 4 (cross-cut, DIN 66399-2) or equivalent (that is, cross-cut, max. 4mm by 40mm, particle size max. 160 $mm^2$). For this purpose, appropriate devices should be deployed (e.g. in the copy rooms). For appropriate devices, see Evonik procurement tool *Hubwoo*.

(k) Printout and transfer of strictly confidential information must be carried out securely, e.g. with a PIN code procedure for multi-function printers.

(l) The loss of (strictly) confidential information (e.g. documents, data carriers with (strictly) confidential information, the company computer or laptop, or other mobile devices) must be reported immediately to the Global Service Desk.

### 4.3.2 Working outside the office

(a) Each employee who carries out company work at a different location to his/her office must ensure adequate protection of (strictly) confidential information.

(b) Such (strictly) confidential documents should only be removed from the office if required for business purposes. (Strictly) confidential documents and Evonik IT devices must be carried in hand baggage. The hand baggage must be monitored. If documents or IT devices are left in the car, they should not be visible from the outside and should not be left unattended for lengthy periods.

(c) The screen of a company device is to be aligned in such a way that it cannot be seen by unauthorized persons. When traveling, you must equip your laptop with a privacy filter. The processing of strictly confidential information in the presence of unauthorized persons is generally prohibited.

## *4.4 Procedure and Labeling*

### 4.4.1 Labeling

The responsible information owner must ensure that information is labeled clearly according to its classification and that labeling takes place promptly.

There is no labeling requirement for public and internal information. In some situations, it can be appropriate to label internal information as “for internal purposes only,” for example, for training documents that are not intended for external persons.

Confidential information is to be labeled appropriately e.g. with a note on the cover sheet.

Strictly confidential information must be labeled on each individual page with “strictly confidential” and the name and, if required, the company ID of the information owner.

### 4.4.2 Handling by information recipient

The information recipient must use the information in accordance with the classification made by the information owner.

## *4.5 Storage and Saving*

Internal, confidential and strictly confidential information may only be saved in Evonik systems or in systems that have been commissioned by Evonik.

Access by unauthorized persons to (strictly) confidential information must be prevented both inside and outside Evonik:

(a) Mobile devices (e.g. laptops, smartphones) must be equipped and used with encryption functions.

(b) Paper documents may not be left unattended and accessible.

(c) Saving information in the intranet is only permitted in protected areas (user authentication) – storing of strictly confidential information in the intranet is forbidden.

(d) Data security or archives used for strictly confidential information must meet the requirements for handling strictly confidential information.

## *4.6 Information Exchange*

The rules relating to the exchange of company information are listed here.

(a) The transmission of (strictly) confidential information to external persons generally requires a prior agreement relating to non-disclosure.

(b) During a conversation, you should ensure at all times that you do not rashly or unwillingly reveal any (strictly) confidential information. You must at all times be aware of the possibility that the conversation partner may attempt, using manipulative conversational techniques ("social engineering" or "piecing together of conversations") to obtain information from an employee.

(c) Conversations with strictly confidential content should only be held in an environment in which eavesdropping or overhearing by unauthorized persons is difficult or unlikely (e.g. not in hotel rooms or bars).

### 4.6.1 E-mail / internet

Information that is classified as public or internal does not have to be encrypted for electronic transmission.

Confidential information *should* be encrypted when sent either internally and externally.

Strictly confidential information *must* be encrypted with the recommended encryption functions when sent either internally and externally.

Transmission of (strictly) confidential information to public services in the internet (such as translation machines, communication services) is forbidden.

### 4.6.2 Telephony and telephone conferences

There are no restrictions on the transmission of public or internal information.

During transmission of (strictly) confidential information via telephone, you should always ensure that unauthorized third parties who may be present cannot overhear the content of the conversation. The same applies for the public environment and the office.

Telephone conferences using teleconferencing solutions which are not operated in accordance with Evonik's specifications on encryption are permitted for the exchange of information up to and including the class “confidential.”

Transmission of strictly confidential information by means of unencrypted or not fully encrypted telephony is forbidden.

For telephone exchange of strictly confidential information, the communication solution prescribed by Evonik is to be used. During a conversation, electronic devices should be kept out of range or technically isolated (e.g. Faraday cage).

Please note that hotel rooms can be subject to conspiratorial audio-visual monitoring, and also that hotel bars and restaurants are not appropriate places for holding strictly confidential conversations.

If the secure communication path for strictly confidential telephony as described above is not available, the following procedure is recommended:

- Maintenance of strict communication discipline (e.g. avoiding revelation of commercial, technical, or personal details, paraphrasing of issues from which outside third parties cannot

glean any information), transmission of the strictly confidential details via a different secured channel if applicable (e.g. via encrypted e-mail).

### 4.6.3 Short messages

Sending (strictly) confidential information as a short message – such as SMS or WhatsApp – is forbidden unless the medium of SMS is used for "information puzzling" – that is, critical information is split into fragments and sent via different communication media. In this case, each information fragment only contains meaningful content in combination with the remaining fragments of the whole.

### 4.6.4 Video communication and conferences

There are no restrictions on the exchange of public or internal information.

During exchange of (strictly) confidential information via the Evonik video communication system, you should always ensure that no unauthorized third parties can overhear or see the content of the conversation. The same applies for the public environment and the office.

The exchange of strictly confidential information requires complete encryption of the communication and the composition of the group should be in line with the "need-to-know" principle. In the pubic environment, you should avoid the exchange of strictly confidential information.

### 4.6.5 Social media

Evonik employees may use social networks (e.g. XING, Facebook) privately. There are restrictions, however, with regard to professional and company-related information (see the Social Media Guidelines):

(a) In social networks, you may specify no more than the company name and your job title.

(b) A detailed job description is not permitted.

(c) It is not permitted to specify the name of your department.

(d) It is also not permitted to specify names or other information relating to your managers, colleagues or employees.

(e) You must not reveal your project-related knowledge, project names, product prices, etc.

(f) In social networks, you are not permitted to exchange either internal or (strictly) confidential Evonik information.

#### 4.6.6 Sending by surface mail

When sending confidential documents internally or externally, you must use a sealed, opaque envelope noted “personal.”

When sending strictly confidential documents internally, you must use two sealed, opaque envelopes. The external envelope must bear the note “personal” and the internal envelope must bear the note “strictly confidential” plus the signature of the sender.

When sending strictly confidential documents externally, you must use a courier or mail service if it is not possible to personally deliver the items. An acknowledgement of receipt must be requested.

#### 4.6.7 Fax

The transmission of strictly confidential information via fax is forbidden.

### *4.7 Publications and Presentations*

When publishing company information, the following points must be observed:

(a) Publication must not infringe any laws or internal regulations and must serve the business interest of Evonik. The publication should be designed so that a competitor cannot obtain excessive benefit from it.

(b) A publication requires – depending on its type and scope – approval by the responsible head of department or responsible area manager and Group communication (see the valid version of the *Group Communication Policy*).

(c) Organizational charts below the level of area management may not be published in the internet or in external presentations.

(d) Information, which could be related to as yet unregistered inventions or developments, must be checked before publication jointly with the patent department of Intellectual Property Management (IPM-PAT) or an external patent lawyer with regard to prejudice to novelty and inventiveness. In cases of doubt, the information must be classified as strictly confidential at least until the patent application has been filed.

(e) The names of critical experts within the company should not be published unless it is necessary.

(f) Technical information that is published should, unless national laws stipulate otherwise, be formulated as unspecifically as possible. Details, solutions or descriptions should only be published piecemeal in accordance with the breakpoint principle.

(g) Commercial or strategic information may only be published to the extent that competitors or potential cooperation partners cannot obtain special benefit from it (e.g. internal schedules, concrete business plans, outlooks and internal deadlines).

(h) Personal details of third parties and/or their business tasks/functions and company information in internet platforms (social networks, web 2.0, e.g. Facebook, XING, StudiVZ, MeinVZ, LinkedIn) are not permitted.

## *4.8 Disposal, Destruction and Deletion*

Information and data carriers, once they are no longer needed, must be deleted, destroyed or disposed of in accordance with the requirements of their protection class. Alternative disposal through an internal or external service provider may only be carried out if this service provider (and the provider's disposal processes) have been certified by C-SC of the IT Security Organization.

It must be ensured that (strictly) confidential information is disposed of securely or deleted and that this information is not accessible to third parties or does not reach third parties.

Before final disposal of company documents, it must be checked which of these documents must be made available to the Group archive for long-term archiving and whether the legal requirements for storage of business documents are met (see the valid version of *Policy on Global Retention of Documents in the Evonik Group*).

### 4.8.1 Handling of information in paper form

Documents that are classified as public or internal can be disposed of in the normal paper waste without any special security precautions.

(Strictly) confidential documents must be destroyed with a document shredder of at least security level 4, cross-cut, (DIN 66399-2 or equivalent). The documents must be destroyed without storage or delay - and in the case of strictly confidential documents - they must be destroyed personally.

### 4.8.2 Handling of information in electronic form

Electronically stored information is deleted in server systems in accordance with a standardized procedure. If data carriers are scrapped or transferred to third parties, they must be securely deleted or securely disposed of via an appropriate destruction method.

Data carriers may only be returned to manufacturers or sellers if confidential handling of the information has been contractually guaranteed. Data carriers with strictly confidential information must not be returned to manufacturers, but must be securely deleted or destroyed.

Data carriers with confidential information must be destroyed analagous to DIN 66399-2 level 3, as follows: Microfilm material particle size ≤ 10 mm², CD/DVD material particle size ≤ 160 mm², disks, ID cards, magnetic tape cassettes material particle size ≤ 320 mm², memory sticks, chip cards, solid state drives (SSD), mobile communication devices: Medium split and material particle size ≤ 160 mm², hard disks with magnetic data storage are deformed.

Data carriers with strictly confidential information must be destroyed analagous to DIN 66399-2 level 4, as follows: Microfilm material particle size ≤ 2.5 mm², CD/DVD material particle size ≤ 30 mm², disks, ID cards, magnetic tape cassettes material particle size ≤ 160 mm², memory sticks, chip cards, solid state drives (SSD), mobile communication devices: Medium split and material particle size ≤ 30 mm², hard disks with magnetic data storage are split multiple times and deformed and material particle size ≤ 2000 mm².

## *4.9 Local Legislation*

Local legislation may require stricter classification than that prescribed by Evonik. In this case, the local law applies. The representative of the relevant region or country must report any such stricter classification to the CSIO, to data protection, or to the head of Corporate Security, in order to agree on the further procedure. This must also be reported if the local legislation is in conflict with the Evonik classification.

## *4.10 Exceptional Regulations / Escalation*

If it is not possible to carry out individual regulations exactly, appropriate methods must be used, in consultation with the responsible SIO, to achieve the relevant level of security. Any escalation must be carried out via the CSIO, the data protection officer at Evonik, or the head of Corporate Security.

# 5 Revision History

| Version | Date (MM YYYY)[1] | Change | Change by whom |
|---|---|---|---|
| | | | |
| | | | |

[1] For the exact date of each version, please refer to QSI

# 6 Appendix

## 6.1 Appendix 1 List of Examples of Information Classification

| Category | Internal | Confidential | Strictly confidential |
|---|---|---|---|
| **Marketing** | General marketing information | Marketing strategy | Marketing strategy that fundamentally changes something, marketing strategies with deliberately incorrect information |
| | General information on one or two suppliers | Some specific supplier data | |
| | General information on the products of the company,<br><br>General product modifications | Sales figures, contribution margin, manufacturing costs of a product,<br><br>Not yet published product modification,<br>Not yet published development modification,<br>Information on business initiations | Sales figures, contribution margin, and manufacturing costs of many products of the company<br>Not yet published (new) product plans<br>Not yet published (new) development plans |
| | | New product information before official announcement | Formulations for products of particular economic or strategic importance |
| **Offers** | General offers | Specific offer for a procedure optimization | |
| **Prices** | Normal commercial prices, catalog prices, office furniture | Product prices, prices relating to third parties, individual prices (NDA protected) | A list of many confidential prices, particularly sensitive price structure, contribution margins, industry cost curve |
| | Invoice for magazine subscription | Product invoices, invoices relating to third parties, individual invoices, invoices relating to consultancy services | |

| Category | Internal | Confidential | Strictly confidential |
|---|---|---|---|
| **Organization** | High-level organizational charts | Organizational charts | |
| | General planning | Strategic planning | Information or planning relating to fundamental changes in the company,<br>Technological planning |
| | | Development and design documents | Information on procedural tricks |
| | Work results | | Information that influences the share price,<br>Detailed information on production procedures |
| | Plans | Company policy | Company strategy |
| | | Medium-term planning of a company unit | Special circumstances in medium-term planning (limited period) |
| | | Budget plan of a company unit | |
| | | | Information on crisis situations |
| **M&A** | Information, reports, when the contract has been signed | Information on sale of company units | Information on company sales that influences the share price |
| | | Details on company spin-offs | |
| | | Information on company acquisitions, takeovers | Information on company sales that has a significant influence on the share price |
| | | Information on joint ventures | |
| | | Details on mergers and purchases | |
| **Contracts** | | Contracts and agreements with confidential content, license contracts | License contracts with particular sensitivity |
| | | Business-related contract drafts with confidential content | |
| **Audit** | | Audit reports | |

| Category | Internal | Confidential | Strictly confidential |
|---|---|---|---|
| **Miscellaneous** | Publications in the intranet | Information on executives, employees | Personal information on the executive board, travel destinations and routes |
| | Internal regulations (policies, newsletters, instructions) | Information on employment relationships | |
| | Internal communication or correspondence that is neither confidential nor strictly confidential | | |
| **Innovation** | | Patent applications between filing and publication | Reported inventions prior to filing a patent application |
| **Information of third parties** | | Confidential information of third parties (NDA) | Information that could be the reason for an information attack against Evonik |
| | | Information on existing (IT) weak points | |
| | | Information on (IT) security measures | |
| | | Copies, data backups of confidential information | Copies, data backups of strictly confidential information |
| | | Archiving of confidential information | Archiving of strictly confidential information |
| | | Publications in the intranet with closed user group | |
| | | Documents relating to customized searches | |
| | | Documents relating to contract analyses | |
| **Information relating to Evonik (insider knowledge)** | Contributions in the intranet | Information relating to pant availability | Information relating to a quarterly report / annual report before publication<br>Information that could influence the share price |
| **Production** | | Start-up plan | Start-up documentation, procedure, shutdown |
| **Data protection** | | Personal data<br>(data protection) | Personal data (data protection), if this data contains details of the person's racial and ethnic |

| Category | Internal | Confidential | Strictly confidential |
|---|---|---|---|
| | | | origin, political opinions, religious and philosophical convictions, union membership, health or sexual activity. |
| | | | Information that is covered by the legal obligation to secrecy (e.g. in Germany, Section 203 of the German Penal Code). |
| | | | Documents relating to social counseling and operational integration management (BEM) |
| | | Bank details of employees or social security number | |
| | | | |