Corporate

Standard

Classification and Control of Information

Responsible Function	Corporate Security
Organizational Scope	All Organizational Units; Continental AG and subsidiaries under the management control of Continental
Reference (Superior Rule)	COR-M-6338916 Corporate Security
Further relevant Rules	COR-S-0600215 Utilization of used IT Equipment P 10.1 Global Communications COR-P-0000202 Governance, Risk & Compliance P 70.1 Record Retention
Key words	Information Security, Classification of Information, Control of Information
Functional contact	Corporate Information Security

Table of Contents

Annexes

1 Scope

This Corporate Standard “Classification and Control of Information” specifies the classification of corporate information to avoid unauthorized disclosure, alteration or destruction.

2 Information Classification

Information must include but is not limited to any information, whether disclosed orally, by written documents, drawings, pictures, audio or video recordings, computer software, e-mails, prototypes and every data transmission means or by visual inspection or in any other possible way.

Information must also include all analyses, compilations and fusions of the foregoing information whether made by Continental or a third party.

For the protection and handling of this information the following classification categories are defined[1] and described below. The chapters for each classification, starting with internal, build on each other, which means measures for internal information also apply to confidential information in addition to those defined in the respective chapters of confidential information.

The defined categories are:

- Public
- Internal
- Confidential
- Strictly Confidential

In compliance with this Corporate Standard, Continental expects the management and employees of its organizational units to ensure that its information is classified accordingly.

It is recommended to verify the classification and where appropriate change it accordingly during each review cycle.

All documents must include a visible classification label on each page, which states the category of the information as well as a copyright remark with the name of the respective legal entity.

[1] Aligned with the VDA white paper “Harmonization of Classification Levels”

All technical documents, like drawings, specifications, test reports, have to contain the standard proprietary terms:

“The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization is strictly prohibited. Infringements can result in civil and criminal penalties.”

The default classification for any information not specifically designated or labeled is “Internal”, unless public by its nature. It is not mandatory to label public information.

The *“COR-M-0000202 Governance, Risk & Compliance (GRC)”* is the baseline for identifying and evaluating risks.

The general idea is to assess two dimensions to define a “risk class” matrix:

1. Probability that a risk materializes
2. Expected impact of a risk if it materializes (e.g. information value)

The “risk classes” for information is based on the “Confidentiality labels” i.e. “Internal, Confidential”, or “Strictly Confidential” defined by this Corporate Standard.

The classification of information has to be done according to the following criteria:

- Financial or material value of the information
- Legal requirements which require a specific classification
- Customer / third party requirements which must be considered
- The potential resulting damage due to the loss of confidentiality of the information asset.

2.1 Public

Public information is intended to be or can be made available to the general public.

Non-exhaustive examples include:

- marketing brochures
- press releases
- freely accessible internet pages
- lectures

Any information considered for public dissemination has to be reviewed in coordination with the relevant departments such as respective Communications or Compliance, Law and Intellectual Property prior to dissemination according to the Global Communications Policy and supplementary internal rules (e.g. Antitrust Manual) and processes.

In order to avoid publications revealing protected technical, product specific, and/or otherwise qualified business information to the outside, responsible management of the organizational unit must ensure that a release process is implemented.

This process must be available in written form and has to be in compliance with Corporate Communications rules.

2.2 Internal

Internal information is not available to the public and its disclosure, alteration or destruction is expected to cause no more than a medium level of risk, according to the internal risk management rules of Continental.

“The potential for damage is low, of a short-term nature and limited to a single company.”[2]

This information is owned by Continental as a result of the creative and business efforts of its own employees and associated third parties.

Non-exhaustive examples include:

- personal employee data (e.g. name, business e-mail or telephone as published in the internal telephone book)
- internal guidelines and circulars
- internal product lists

Further examples are provided on the intranet page of corporate security.

If required Continental organizational units may add the name of their own organizational unit name to the classification “internal” to point out that this information is only to be handled within the respective organizational unit (e.g. internal-BU xy).

Any loss and/or unintended disclosure of internal information must be immediately reported to the information owner.

2.2.1 Disclosure, Alteration or Destruction of Internal information

Within Continental internal information may only be disclosed between regular, supplemental and part-time employees for whom this information is necessary to perform tasks associated with his or her job, scope of work or where a disclosure is beneficial for Continental.

Internal information must only be disclosed to third parties in line with applicable legal requirements, especially antitrust law, and if there is a business need for Continental to exchange this information with business partners, in which case a confidentiality agreement/obligation must be signed prior to such disclosure.

Employees and any associated third party should not make or keep any copy, photocopy, draft or any other kind of reproduction of internal information disclosed other than in the recognized course of the respective function or activities.

[2] VDA white paper “Harmonization of Classification Levels”

2.2.2 Protective Measures for Meetings

- Close doors and windows (for acoustic protection) / Ensure acoustic protection (e.g. close doors and windows).
- Prevent view from the public area into the meeting room (e.g. by using sun-blinds, curtains or milky glass).
- Media technology in the room has to be switched off if not in use.
- If video conferencing is used make sure the surroundings are free from any information, products, or people that are not to be shown.
- Whiteboards should be wiped clean after the meeting.
- All paper-based information must be properly disposed of.
- If printer is used, ensure the print is taken out and not left there. Ideally technical options such as follow-me print is used.

2.2.3 Mailing and Transmission of Internal Information

Internal information mailed or shipped externally by public mail or by courier must be placed in a nontransparent closed envelope or other nontransparent closed container.

It must be ensured by the respective employee that the recipient's address is correct.

2.2.4 Safekeeping, Storage and Archiving

Internal information must always be protected from unauthorized access. Access rights for internal information must follow the need-to-know principle.

Internal information must only be stored and processed on approved systems that comply with Continentals security rules. This applies to approved systems and services on-premise, approved mobile devices like laptops, in approved managed data centers and in approved cloud solutions.

Internal information in physical form including electronic media such as, but not limited to, USB sticks, external hard drives, memory cards, DVDs and CDs must not be left unattended unless it is secured behind a locked door or in locked office furniture.

Internal information must always be kept out of unauthorized view.

Internal information in computers including work stations must be protected by mechanisms which ensure that the information is accessed only by authorized individuals such as password protection or an authentication process.

Employees working remotely must ensure that internal information is secured at their work location to prevent unauthorized access.

Continental employees may only publish internal information on platforms (e.g. Sharepoint, ConNext, Intranet, etc.) in the internal network, if the need to know principle

is adhered to by setting appropriate access rights. Internal information must not be stored in external systems unless those systems are approved by Continental.

When internal information needs to be archived or backed up, it must be ensured, that the methods and processes defined in this standard are applied throughout the whole archiving period as well as to the disposal process after the archiving period ends.

2.2.5 Travel

If an employee needs to take internal information on a trip, it is strongly recommended to keep the internal information in his or her possession while in transit and to secure from unauthorized view.

2.2.6 Disposal of Internal Information

Internal information that is no longer needed must be destroyed in an adequate manner (e.g. torn up and disposed of in a waste container, shredded, erased) based on Continental's record retention rule and legal requirements.

The primary user of removable media is considered a custodian for the media, unless otherwise specified in the respective location disposal process, and is therefore responsible for the management and disposal of the media. The custodian must ensure that any internal information on that media is disposed of in the way as described above.

Any Continental owned removable media must be returned and all user accounts/ access that are owned on behalf of Continental must be transferred to the respective management prior to the end of employment.

2.3 Confidential

Confidential information is more sensitive than internal information which is not publicly available and is not generally available within Continental Group. All regulations defined for information classified as "internal" also apply to confidential information unless stated otherwise. Its disclosure, alteration or physical and electronical destruction is expected to cause a high level of risk, according to the internal risk management rules of Continental. This information is typically of high economic value. It is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question. The information has commercial value because it is secret.

"The potential for damage is considerable, or of a medium-term nature, or not limited to a single company."[3]

[3] VDA white paper "Harmonization of Classification Levels"

Non-exhaustive examples include:

- scientific and technical information such as product specifications, drawings, equipment and trade secrets
- invention disclosures (until patent application is filed)
- reports and correspondence relating to research and product development projects
- personal employee data (e.g. private address, private telephone number, private e-mail address, payroll results, employee dialogue data (e.g. targets / Target achievement /absence data etc.))

Further examples are provided on the intranet page of corporate security.

Any loss and/or unintended disclosure of confidential information must be immediately reported to the information owner and to information security department, as well as to the respective communication responsible.

2.3.1 Disclosure, Alternation or Destruction of Confidential Information

Confidential information must not be disclosed to anyone besides the defined authorized persons outside or inside of Continental and must not be used in any other way than to fulfill Continental's business obligations or to follow legal rules, contractual obligations respective contractual restrictions. And always needs to be in line with legal requirements, especially antitrust law.

Confidential information must only be exchanged or shared with third parties if in line with existing legal especially antitrust restrictions and if a Nondisclosure Agreement (respective templates are provided by the Law Department and Intellectual Property Department)[4] is signed prior to the information access of the third party. Any amendments and supplements to the respective agreement must be made in writing. Before either party passes on any kind of confidential information to an affiliated company or to a consultant it must ensure that the recipients, by reason of their contract of employment or by reason of any other written agreement, are bound by a non-disclosure obligation, which are at least equivalent to the respective non-disclosure agreement. The Parties undertake to treat confidential information in a manner at least equivalent to that applying under the respective agreement.

2.3.2 Protective Measures for Meetings

- protective measures descripted for “internal”. (see 2.2.2)
- If printer is used, ensure that technical options such as follow-me print is used.
- unauthorized audio-visual recording devices are prohibited and must be entirely switched off during the part of a meeting in which confidential content is discussed.

[4] for details see: http://ci-shortcode.conti.de/d55d

- Meeting initiator has to communicate the above

2.3.3 Mailing and Transmission of Confidential Information

Confidential information mailed or shipped externally and internally by public mail or by courier must be placed in a closed envelope or other closed container.

To secure electronic communications and exchange of information (e.g. data using electronic media, video conference systems) between persons and/or systems, the communication has to be encrypted by using Continental approved cryptographic methods including secure key management[5] and the email must be marked as confidential.

When printing confidential information, secure printing methods (e.g. secured by PIN, ID badge) must be implemented and used. This is to ensure that only the creator of the print job has access to the printout.

It is not allowed to scan confidential information to public storage media.

2.3.4 Safekeeping, Storage and Archiving of Confidential Information

Confidential information in physical form including removable media and prototypes/samples must always be kept under lock and key and out of view of those without a need to know.

Confidential information must always be stored encrypted (Continental approved cryptographic methods including secure key management[6]) and in a way that it is not accessible for unauthorized users. Administrators are allowed to access data only if necessary, to perform a specific approved task. The accesses are documented via logging data.

When confidential information needs to be archived or backed up, it must be ensured, that the methods and processes described in this Corporate Standard are applied throughout the whole archiving period as well as to the disposal process after the archiving period ends.

2.3.5 Travel

It must be avoided to take confidential Information on business trips unless absolutely necessary.

Confidential information in any form must not be left in luggage which is checked through at airports (instead it should be kept in hand luggage) and must be kept under lock, at least not to be left unprotected (e.g.in hotel rooms) or unattended in vehicles.

[5] for details see: https://links.conti.de/cybersecurity
[6] for details see: https://links.conti.de/cybersecurity

2.3.6 Disposal of Confidential Information

Confidential information that is no longer needed and is allowed to be disposed of according to Continental's record retention rules must be destroyed and handled in the following manner:

Paper containing confidential information must be shredded or incinerated. This can be done by an external provider with an appropriate certification and with which a non-disclosure agreement is in place.

If shredded, the shredder must have at least security level 4 and cross-cut. The particle size must not be larger than ≤ 160 mm² with width ≤ 6 mm.

Storage media may either be physically destroyed onsite or offsite by an external provider with an appropriate certification and with which a non-disclosure agreement is in place. The regular local electronic disposal process is to be applied and documented for any onsite case.

Alternatively, the storage media may also be deleted using certified software deletion method.

If the disposal is carried out by an external service provider, the respective media must be kept under lock and key until they are handed over to the service provider.

The disposal must be adequately documented to ensure traceability of the performed actions by the party performing the removal or destruction.

The primary user of removable media is considered a custodian for the media, unless otherwise specified in the respective location disposal process, and is therefore responsible for the management and disposal of the media. The custodian must ensure compliance with the methods and processes defined in this Corporate Standard.

If the storage media or the information itself is fully encrypted, using the Continental standards, the secure deletion process (mentioned in this Corporate Standard) is not necessary and media may just be simply formatted or erased.

Any prototypes or samples which can be disposed of according to internal rules need to be disposed of in compliance with the respective project agreement or technical specification.

2.3.6.1 External disposal contractor

If removable media must be transported to a specific place for data deletion or destruction the custodian is responsible for the appropriate documentation (chain of custody). It must be ensured that no access to confidential data stored on removable media is possible for non-authorized persons (e.g. transport in locked container).

Locked destruction bins, for the disposal of removable media, may be provided by the location as long as it is ensured that access is only possible to authorized personnel,

e.g. a service provider with an appropriate contract with which a non-disclosure agreement is in place.

The custodian is responsible for the chronological documentation of all persons and items involved in the transport or disposal process (chain of custody). Records of this must be kept.

A corresponding non-disclosure agreement has to be concluded with any external service providers involved in the transport, deletion or destruction of removable media.

2.3.6.2 Analysis of removable media

If removable media needs to be sent to a specific place for data analysis (e.g. compliance issues, warranty) the custodian is responsible for the chronological documentation of all persons involved in the transport (chain of custody). It must be ensured that no access to confidential data stored on removable media is possible for non-authorized persons (e.g. by encrypting the removable media).

The respective media must be kept under lock and key until transfer of perils to the third party is consummated.

2.3.7 Reuse

Before removable and rewritable data carriers that contain confidential information can be transferred to a different user inside or outside of Continental the data must be deleted via software according to the standards described in the chapter “Disposal” of this Corporate Standard. When the new primary user has a need to know (e.g. a successor of a certain job) the confidential information on the media may be - with proper management approval - transferred without deletion.

2.4 Strictly Confidential

Strictly confidential information is more sensitive than confidential information. All regulations defined for information classified as “confidential” also apply to strictly confidential information unless stated otherwise.

Strictly Confidential information is sensitive information defined by laws, regulations or contractual clauses and requires a specific level of protection. This information is only available to defined recipients. Its disclosure, alteration or destruction is expected to cause a very high level of risk, according to the internal risk management rules of Continental.

“The potential for damage threatens the company’s existence, or is of long-term nature, or is not limited to a single company.”[7]

[7] VDA white paper “Harmonization of Classification Levels”

Information of such nature often includes data and information with elevated security requirements that needs to be exchanged in course of specific projects.

This kind of information needs to be treated with extreme care, especially considering existing confidentiality obligations.

Strictly confidential information must only be classified as such if there is an explicit need as described above.

Non-exhaustive examples may include but are not limited to:

- Technological specifications (e.g. immobilizer codes)
- Strategy documents (M&A, business models, etc.)
- special categories of personal data according to Article 9 EU General Data Protection Regulation (e.g. health data), personal data relating to criminal convictions and offenses

Further examples are provided on the intranet page of corporate security.

Security measures and methods in addition to the above mentioned are to be defined by the respective organizational unit and Corporate IT Cybersecurity as well as Corporate Information Security need to approve.

Any loss and/or unintended disclosure of strictly confidential information must be immediately reported to the information owner and to information security department, as well as to the respective communication responsible.

2.4.1 Disclosure, Alteration or Destruction of strictly confidential information

Strictly confidential information must not be disclosed to anyone besides the defined authorized persons, whose authorization must be properly documented, outside or inside of Continental or be used in any other way than Continental's business or as required by law. With third parties, strictly confidential information must only be exchanged or shared with if in line with existing legal especially antitrust restrictions.

A confidentiality agreement/obligation has to be signed before access to information is granted. Any amendments and supplements to the respective agreement must be made in writing. Before either party passes on any kind of strictly confidential information to an affiliated company or to a consultant it must ensure that the recipients, by reason of their contract of employment or by reason of any other written agreement, are bound by a non-disclosure obligation, which are at least equivalent to the respective nondisclosure agreement.

2.4.2 Protective Measures for Meetings

- protective measures as 2.2.2 and 2.3.2
- The room must be tap-protected

- Unauthorized Audio-visual recording devices have to be kept outside of the room
- Media technology in the room has to be switched off if not in use and seals must be intact
- Video conferencing should not be used
- All printouts must be properly disposed of immediately after the meeting and must not remain in the room after the meeting is over.
- Documents are shown but not handed over

2.4.3 Mailing and Transmission of strictly confidential information

Strictly confidential information mailed or shipped externally and internally by public mail or by courier must be placed in a closed envelope or another sealed container.

To secure electronic communications and exchange of information (e.g. data using electronic media, video conference systems, email) between persons and/or systems, Continental approved cryptographic methods including secure key management[8] must be used.

When printing strictly confidential information, secure printing methods (e.g. secured by PIN, ID badge) must be implemented and used. This is to ensure that only the creator of the print job has access to the printout.

It is not allowed to scan confidential information to public storage media.

2.4.4 Safekeeping, Storage and Archiving of strictly confidential information

Strictly confidential information must always be kept under lock and key and out of view of those without a need to know.

Prior to gaining access to information of strictly confidential needs, users must be authenticated at least by means of strong authentication (e.g. two-factor authentication) according to the state of the art.

Strictly confidential information must always be stored encrypted and in a way that it is not accessible for unauthorized users. Administrators are allowed to access data only if necessary, to perform a specific approved task. The accesses are documented via logging data.

Strong Cryptographic key material and state of art encryption procedures must be used and the key management (e.g. custom generated keys) must be fully under Continentals control. Both the definition of the strong cryptographic keys as well as the key management control method must be approved by Cybersecurity.

[8] for details see: https://links.conti.de/cybersecurity

2.4.5 Travel

It must be avoided to take strictly confidential Information on business trips unless absolutely necessary.

Strictly confidential Information in which form whatsoever must not be left in luggage which is checked through at airports (instead it should be kept in hand luggage) and must be kept under lock.

2.4.6 Disposal of strictly confidential information

Strictly confidential information that is no longer needed and is allowed to be disposed of according to Continental's record retention rule must be destroyed and handled in the following manner:

Paper containing strictly confidential information must be shredded or incinerated. This can be done by an external provider with an appropriate certification and with which a confidentiality agreement is in place.

If shredded, the shredder must have at least security level 5 and cross-cut. The particle size must not be larger than ≤ 30 mm² with width ≤ 2 mm.

Strictly confidential information on hard disk drives (HDD) must be either deleted or the HDD must be physically destroyed (shredded or drilled several times at various places of the disk), both in a way that does not allow the data to be recovered.

Rewriteable media, e.g. HDDs must be physically destroyed onsite, unless it is fully encrypted using the Continental standards.

All CD/DVD-types, magnetic tapes and flash disk (including USB) drives that contain strictly confidential data or where it has to be assumed or is unclear, must be physically destroyed, by applying at least security level 5 standards. This can be done by an external provider with an appropriate certification and with which a confidentiality agreement is in place. CDs and DVDs can be destroyed internally by using a common commercial shredder, which must have at least security level 5.

The disposal must be adequately documented to ensure traceability of the performed actions by the party performing the removal or destruction (see annex 1).

Any prototypes or samples which are allowed to be disposed of according to internal rules need to be disposed of in compliance with the respective project agreement or technical specification.

The disposal of electronics must be clearly regulated by a process at the location. The electronic disposal process is to be applied for any onsite case.

2.4.6.1 External disposal contractor

Removable media must be disposed of onsite. The custodian is responsible for the appropriate documentation (chain of custody). It must be ensured that no access to data

stored on removable media is possible for non-authorized persons (e.g. storage in locked container).

Locked destruction bins, for the disposal of removable data carriers, may be provided by the location as long as it is ensured that only authorized personnel have access, e.g. a service provider with an appropriate contract including confidentiality agreement.

3 Proper Documentation

The obligation to produce supporting documents lies with the custodian. The custodian is responsible for the chronological documentation of all persons and items involved in the transport or disposal process (chain of custody).

A corresponding confidentiality agreement has to be concluded with any external service providers involved in the transport, deletion or destruction of removable media.

4 Obligations of employees and project communication rules

Corporate information has to be treated in an appropriate way. Employees and associated third parties who have access to corporate Information have to make every reasonable effort to preserve and fully protect it.

4.1 Responsibilities of the employees and associated third parties

Employees and associated third parties who leave Continental continue to be obliged not to disclose or use corporate Information. All patent rights copy rights and property rights in corporate Information arising from an employee's work for Continental continue to be owned by Continental after the employee leaves. Employees who leave Continental are required to immediately return access rights, devices and Continental property, including corporate Information.

These responsibilities are to be communicated to the leaving employee during the debriefing process.

HR is obliged to ensure the compliance with, and implementation of, the debriefing and return process mentioned above.

The responsible management must ensure that any Continental owned removable information/data carrier must be returned to the respective management prior to the end of the respective employment contract.

4.2 Project Communication Rules

Appropriate communication rules with external project parties need to be defined and implemented by the responsible project management (Project Manager, Sponsor and Steering, etc.).

Such communication rules must stipulate that sharing information with third parties must follow contractual agreements (e.g. confidentiality agreement) and the “Need to Know” principle.

Communication rules must be part of the mandatory project approval and must comply with applicable Continental rules.

4.3 Classification of IT services

The service provider/owner must specify what classification-level the respective service is suitable for. Classification by the IT service provider must be in accordance with this Corporate Standard.

5 Application

This Corporate Standard applies to all business environments in which Continental’s staff is working. This includes mobile work scenarios.

Further relevant rules will be aligned within the application time frame described hereafter.

The rules described in this Corporate Standard have to be implemented in the organizational units within a time frame of two years after effective date.

The implementation of this version (2) is monitored by Corporate Information Security.

All affected companies will be informed about the update of this policy via Intranet and a communication campaign.

6 List of Abbreviation

Abbreviation	Description
HDD	Hard disk drives
ID-badge	Identification badge
M&A	Mergers & Acquisitions
PIN	Personal identification number
USB	Universal Serial Bus

7 Approval

S-list ID:9634551

Director Corporate Security, Frank Busch

S-list ID:9634551

Head of Corporate Information Security, Markus Schlitt

Document History

Version	Responsible Function	Details	Effective
1	Corporate Information Security	Update of content. New classification level (third-party confidential). Replaces Corporate Manual Classification and Control of Information (M.60.02.07).	August 1st, 2016
2	Corporate Information Security	Update content: Meetings Change of “third party confidential” to “strictly confidential” Document structure	Nov 1st, 2019