Policy on handling information

1 General

Ordina stands for scrupulous and reliable. And that also characterises the way in which Ordina handles information. We protect information, whether this is Ordina's own information or information with which its clients, employees, suppliers or partners have entrusted the company. We adhere to legal and contractual obligations that exist to protect and maintain the confidentiality of information and to the relevant internal policies. This policy on Handling Information is such an internal policy.

In the context of data security, reference is often made to the ***B**eschikbaarheid* (availability)*, data -**I**ntegriteit* (integrity) and ***V**ertrouwelijkheid* (confidentiality) of information and information systems (BIV). See also the data security policy and associated guidelines in this context.

There are a number of possible approaches to the concept of information. The internal Classification guidelines, for instance, outline the various types of information.

This policy on Handling Information specifically addresses the **confidentiality aspect** of information; in other words, the question of who you are allowed to share information with and how you can ensure that information only reaches people who are entitled to have that information.

This policy document has been drawn up to help you deal with information. Protecting information insufficiently or sharing information with people who lack the required authorisation can have grave consequences. It can lead to damage, high fines and it can harm Ordina's reputation.

Chapter 2 describes which kinds of information Ordina distinguishes (classification) and/or how it should be labelled. Chapter 3 discusses measures to protect the various types of information. Chapter 4 addresses the question of who you may share which information with.
A number of specific situations – such as being seconded - is discussed in chapter 5. Finally, in chapter 6, you can find who to contact if you have any questions. The Quick Reference Card (Annex 1) contains a brief summary of this policy.

2. Types of information

At Ordina, we distinguish three types of information: non-sensitive, sensitive and (business) critical information. We call these three distinct types of information classifications. The more sensitive the information, the smaller the group of people you can share the information with and the greater the need to protect the information. The classification level also determines whether or not you need to label the information.

You label information by:
- Stating the classification level on the physical document: think front page and/or watermark;
- Stating the classification level in (digital) storage / registration: for instance, mapping different types of information within (parts of) information systems

Classification table*

Level of sensitivity ↓	Confidentiality	Ordina classification	Is labelling necessary?	Share with
High	**(Business) interests[1] will be severely harmed if unauthorised people have access.**	**Critical / Strictly confidential**	**Necessary**	**Only specifically named people**
Medium	**(Business) interests are harmed if unauthorised people gain access**	**Sensitive / confidential**	**Preferred**	**Based on need to know principle[2]**
Low	**(Business) interests will not be harmed if the information is made public**	**non-sensitive/ non-classified**	**Not necessary**	**Everyone**

*The table above is a partial representation of the classification table that is included in the Classification guidelines; see the Classification guidelines for the full table.

2.1 Non-sensitive information

The key feature of non-sensitive information is that no (business) interests will be harmed if the information becomes public knowledge. Public sources such as newspapers and internet by definition contain non-sensitive information.

- If you create non-sensitive information, you do not need to label it.

Examples of non-sensitive information:
- *annual reports*
- *information on (external) website of companies*
- *press releases (**NB**: press releases often cover important topics; a press release is only non-sensitive **after** it has been sent to the media. Before that time, a press release is frequently (business) critical)*

Question: Is all non-labelled Ordina information non-sensitive?

Answer: No. You should never assume that it is in fact non-sensitive information. Check the content of the information before you use it or share it. If necessary, consult the creator of the information or your superior for advice.

Question: What about non-labelled information of clients and other business partners?

Answer: You should consider such information as at least 'sensitive'. You can consider such information only as non-sensitive once you have determined that this involves information that is available in the public domain. If necessary, ask the client/business partner for advice.

[1] (Business) interests are also taken to refer to the interests of our business partners and employees, for instance in the case of personal data.
[2] Need to know principle: Ordina's information may be shared only with those colleagues who need access to that information for the execution of their tasks; information from clients / business partners may be shared only with those colleagues who need access to that information to execute the tasks contractually agreed with those clients / business partners.

2.2 Sensitive information

The key feature of sensitive information is that (business) interests will be harmed if unauthorised people gain access to that information.

Information may also be sensitive solely on the basis of the law. This applies, for instance, to personal data (with the exception of delicate personal data, such as medical data, which is critical).

- If you create sensitive information, it is **preferable** that you label it (as *confidential* for instance, or '*for internal use only*')

.

Examples of sensitive Ordina information:

- *commercial documents such as market studies, quotes for contracts, OCS*
- *contracts, and the financial information relating to contracts*
- *project data such as PID, steering group reports, test results, risk, issue and quality registers*
- *files with personal data (without extraordinary data)*
- *management data such as SLA, DAP, SLR, release approach, impact analyses*

Information is always sensitive if it is labelled as such.

Question: Can non-labelled Ordina information be 'sensitive'?

Answer: Yes. Always check the content of the information before you use it or share it. If necessary, consult the creator of the information or your superior for advice.

Question: What about non-labelled information of clients and other business partners?

Answer: You should initially consider such information as ***at least*** *sensitive, unless you have determined that the information is available in the public domain. If necessary, ask the client/business partner for advice.*

2.3 Critical information

The key feature of critical information is that (business) interests will be severely harmed if unauthorised persons gain access to that information. Information may also be critical solely on the basis of the law; this applies, for instance, to delicate personal data such as medical data.

Sometimes, the classification 'critical' depends on the moment at which you have the information at your disposal. Ordina's annual results (and interim and quarterly results), for instance, are critical until the moment they are published. After publication, that information becomes non-sensitive (because it is in the public domain).

- If you create critical information, you must label it *'critical'* or *'strictly confidential'*. You also have to determine for which specifically named people the information is intended.

Examples of critical information:

- *Personnel files*
- *Medical information*
- *Plans for takeovers or reorganisations*
- *Management reports*

Information labelled as *'critical'* or *'strictly confidential'* should always be considered 'critical'.

Question: Can non-labelled Ordina information be critical?

Answer: Yes. It is possible that someone has forgotten to label the information as critical. Check the content of

Question: Can the non-labelled information of clients and other business partners be critical?

Answer: Yes. You should initially consider such information as ***at least*** *sensitive, but it may be critical. If the information proves critical, label it as such as ask the client/business partner for advice on how to deal with this.*

2.4 Do you have doubts about the correct classification?

If you have doubts about the correct level of classification, you should treat the information as **at least** sensitive, until you have had a chance to verify its status with your superior or the client/business partner.

3. Code of conduct for the protection of data

There are various ways in which data is protected within Ordina. We have put technical and organisational safeguards in place to protect data, such as firewalls, access passes and screening. You can find these safeguards on Connect (section 'beleid' (policy)/ 'beveiliging' (security).

Moreover, we have certain rules of conduct aimed at protecting data. Sections 3.1 through 3.3 deal with these rules of conduct.

3.1 Protecting Ordina's data

Always observe the following **basic rules** for the protection of data (from non-sensitive to critical).

- clean-desk: do not leave important information (paper/usb) unattended in your workspace;
- clear-screen: lock your computer when you leave your workspace;
- avoid having a lot of information on your personal computer / laptop. Use the facilities Ordina provides, such as working with Scope, workspaces, web applications, Lync, etc.
- lock mobile equipment physically (with a laptop lock, for instance);
- only use the USB hard disk to secure the data from your Ordina laptop; do not use it for other purposes;
- when using your own device (BYOD), make sure it meets the same requirements as Ordina devices. See the guideline mobile equipment and data storage devices (or ask the Information Management department for advice);
- report any loss or theft of a mobile device to your superior and the Security Officer as soon as possible.

The following additional measures apply to **sensitive Ordina information:**

- be careful with authorisations for access to sensitive data, see authorisations policy;
- ensure that sensitive (printed) information is stored safely, both at home and in the office, at the very least in a closed/locked cabinet;
- When disposing of sensitive (printed) information, ensure that it is only placed in the closed paper container.

In addition to the basic rules and additional measures, the following rules also apply to **critical Ordina information**:

- avoid storing critical information on mobile devices where possible; ensure that critical information is only stored on a mobile device if the encryption meets the latest Ordina encryption standards;
- when consulting or sharing critical information, avoid information channels that do not guarantee confidentiality, such as internet email and public wifi networks (or even client networks).
- ensure that (printed) critical information is shredded after use.

3.2 Protecting the information of clients and other business partners

In the event that Ordina has contractual data protection agreements with the client/business partner

When dealing with the information of clients and other business partners, you adhere strictly to the measures Ordina has agreed with the business partners. If you work with a client or business partner's information, you request information on those agreements proactively.

Explanation: Ordina often reaches agreements on security measures with clients (and some other business partners). These measures may relate to sending information via email, for instance, or printing and storage on storage devices, or the storage and/or disposal of information. The public sector, the financial sector and the healthcare sector in particular have their own security requirements related to the execution of contracts.

Examples of specific security requirements

- *Algemene Beveiligingseisen voor Defensieopdrachten (ABDO)(General Security Requirements for Defence Contracts)*
- *Baseline Informatiebeveiliging Rijksdienst (BIR) (Baseline Government Department Data Security)*
- *Voorschrift Informatiebeveiliging Rijksdienst (VIR)(Government Department Data Security Directive)*

You should comply with the contractual agreements with the client / business partner if those agreements exceed the rules that apply to Ordina's own sensitive information. If the agreements with the client / business partner are less stringent than those governing Ordina's own sensitive information, you should nonetheless comply at the very least with the rules that Ordina applies to its own sensitive information, as outlined in section 3.1 (unless it has been determined that the information in question is available in the public domain).

In the event that Ordina has no contractual agreements with the client / business partner on data protection

If there are no contractual agreements in place with the client / business partners regarding data protection, you should comply at least with the rules Ordina applies to its own sensitive information, as outlined in section 3.1 (unless it has been determined that the information in question is available in the public domain).

4 Sharing information

4.1 Sharing Ordina's information

You can share **non-sensitive** Ordina information with anyone, both internally and externally.

With respect to **sensitive** Ordina information, you can share this internally only on the basis of the need-to-know principle. This means that you may only share that information with colleagues who need the information to carry out their tasks.
You should, in principle, not share sensitive Ordina information externally. You should therefore also refrain from discussing this kind of information with your partner or family and friends.

If it is in Ordina's interest to share sensitive information (in the context of cooperation, for instance), you should ensure that the recipient of the information is obliged to maintain the confidentiality of that information and/or protect same, by having them sign a confidentiality agreement for example. You can use the standard confidentiality agreement for this purpose, or contact the Legal department.

When **critical** Ordina information is involved, you should only share this with people who have been specifically designated as authorised by the person who created the information. If it is unclear who has been specifically authorised, you should ask the person who created the information.

You should, in principle, not share critical Ordina information externally. You should therefore also refrain from discussing such information with your partners or with your family and friends.

If you need to share critical information externally, you need to request permission in advance from the person who created the information. To ensure that the recipient of the critical information maintains the confidentiality of that information, you must have the recipient sign a confidentiality agreement. You can use the standard confidentiality agreement for this purpose, or contact the Legal department.

4.2 Sharing the information of clients and other business partners

Non-sensitive information of clients / business partners
Please note that the information of clients / business partners should initially be considered at least sensitive. You can consider such information non-sensitive and share same internally (and externally) only after you determine that the information is available in the public domain. If necessary, ask the client / business partners for advice.

Sensitive information of clients / business partners
Within Ordina, you should share sensitive information of clients/ business partners only on a need-to-know basis. This means you share such information only with colleagues who need access to that information to carry out the tasks contractually agreed with the client / business partner. You should request information about such agreements proactively if you wish to share information.

If you wish to share this information outside this circle of Ordina colleagues, you need permission from the client.
NB. Irrespective of the permission from the client, there are instances in which it may be illegal to share the client's information: for instance, in a tender process in which Ordina is not permitted to use information to which other competitors may not have access. You can find more information on this subject in the policy on Fair Competition.

Should it be in the interest of the client / business partner to share sensitive information with third parties (in the context of cooperation, for instance), you should ensure that the recipient of the information is obliged to maintain the confidentiality of said information and or protect same. Before sharing such information externally, you should agree on same with the client / business partner concerned.

Critical information of clients / business partners
You should exercise extreme caution when sharing critical information of clients / business partners. You should only share such information with colleagues if this is absolutely necessary for the execution of the contractually agreed tasks. Please be aware that is it infinitely preferable to check more than once with the client / business partner as to whether information can be shared, than to share the information with someone for whom it is not intended.

You should not share any critical information of clients / business partners with external parties. You should therefore also refrain from discussing such information with your partner or with family and friends.

5. Specific situations

Below you will find a number of specific situations described which you may be confronted with. You will find the policy on handling information in each of these situations.

5.1 You are asked to sign a personal confidentiality agreement

It is possible that a client will ask you to sign a confidentiality agreement in a personal capacity. This is supplementary to the duty of confidentiality that exists contractually between Ordina and the client. (And supplementary to the duty of confidentiality in your employment contract with Ordina.) There is a risk that the agreements contradict each other or that agreements are reached which are unworkable. The following therefore applies:

- Ask advice from the Legal department before you sign a confidentiality agreement with clients in a personal capacity.

When you have signed a confidentiality agreement in a personal capacity, you should obviously comply with the provisions of said agreement.

5.2 Ordina has seconded you to a client

If Ordina seconds you to client, your position changes vis-a-vis both Ordina and the client. You should then consider Ordina as a third party. In this situation, the following rules apply:

- You adhere to the duty of confidentiality the client applies internally and to the obligations Ordina has agreed for you in the secondment contract with the client, or – if you have signed a confidentiality agreement yourself – to individual agreements contained therein.

- If you are not (sufficiently) familiar with those agreements, you should ask your secondment coordinator about the content of those agreements.

  If you wish to share any client information with colleagues at Ordina, you should ask the client for permission in advance (unless it has been determined that said information is available in the public domain). To avoid any discussions after the fact, you should make sure that you have some evidence of that permission. You can ask the client to confirm the agreement, but you yourself can also confirm what you have agreed with the client in this respect.

Example: You are working at the client location. During a team meeting, you find out that a number of IT services will soon be outsourced. The next day, you talk to your secondment coordinator at Ordina, who asks whether you have any news.

Question: What do you do?

Reply: You do not tell your secondment coordinator about the plans until after you have spoken to your manager on the client side and they have informed you that you have permission to share this information with Ordina. You send an email to the manager on the client side to confirm this.

NB: Irrespective of the permission from the client, there are instances in which it may be illegal to share the client's information: for instance, in a tender process in which Ordina is not permitted to use information to which other competitors may not have access. You can find more information on this subject in the policy on Fair Competition.

5.3 You are part of an Ordina project team that works for the client, be it on location or not (you are not seconded to the client's business).

When you are working on a contract for a client, you probably hear and see a lot of information of that client. You may have access to the intranet, for instance, or certain of the client's systems, or because

you take part in meetings.

Obviously, you will use the information you see and her to execute the contract. You can also share that information with your project team on a need-to-know basis (in other words, with colleagues who need access to that information for the execution of the contractually agreed tasks). But if you share that information within Ordina outside the project team, you need permission from the client. .

NB: Irrespective of the permission from the client, there are instances in which it may be illegal to share the client's information: for instance, in a tender process in which Ordina is not permitted to use information to which other competitors may not have access. You can find more information on this subject in the policy on Fair Competition.

6. Do you have any questions or doubts?

Do you still have questions or doubts about how to act in a specific situation? Always contact your manager or the Compliance Officer.

In the event of non-compliance with this 'handling information' policy, Ordina may take disciplinary action.

This policy applies in conjunction with:

- General employment terms and conditions
- Data protection policy and associated guidelines
- Privacy regulations (processing personal data)
- Classification guidelines
- Record retention policy
- Mobile equipment and data storage devices policy
- Insider trading policy
- Policy on Fair Competition

Annex 1. – Quick reference card

Types of information – Chapter 2

Classification table*

Level of sensitivity ↓	Confidentiality	Ordina Classification	Is labelling necessary?	Share with
High	**(Business) interests[3] are harmed severely if unauthorised persons gain access.**	**Critical / strictly confidential**	**Necessary**	**Only specifically named parties**
Medium	**(Business) interests are harmed if unauthorised parties gain access**	**Sensitive / Confidential**	**Preferred**	**On a need-to-know basis[4]**
Low	**(Business) interests are not harmed in the event of disclosure**	**Non-sensitive / Unclassified**	**Not necessary**	**Everyone**

*This table is a partial representation of the classification table as included in the Classification guidelines; see for the complete table the Classification guidelines.

How to protect data – chapter 3

	Ordina information		Information of business partners
always	• clear desk • clean screen • lock mobile devices • limit amount of data on your laptop • use USB hard drive only for your own data on your laptop • ensure that your own devices (BYOD) meet the same requirements as Ordina devices; • report loss or theft immediately		• You comply with the contractual agreements with the business partner; • If the agreements with the business partners are less stringent than the rules governing **sensitive** Ordina information – or if no contractual agreements are in place – you should comply at
sensitive information	**additional** • be careful with authorisations; • store sensitive (printed) information safely or dispose of it in a closed paper container		
Critical	**additional**		

[3] (Business) interests are also taken to refer to the interests of our business associates and employees, in the case of personal data for instance.
[4] Need-to-know principle: Ordina's information may be shared only with those colleagues who need access to that information for the execution of their tasks; the information of clients / business partners may be shared only with those colleagues who need access to that information to execute the tasks contractually agreed with those clients / business partners.

information	• can be stored on a mobile device only if the encryption (data encryption) meets Ordina's latest encryption standards; • avoid all unsecured communication channels (such as public Wifi); • shred printed critical information after use		least with the rules governing **sensitive** Ordina information (unless it has been determined that the information in question is available in the public domain).

Sharing Ordina's information – chapter 4.1

type of information	sharing internally	sharing externally
non-sensitive	allowed	allowed
sensitive	only on a need-to-know basis	not allowed, unless in Ordina's interest and protected by confidentiality agreement
critical / strictly confidential	internally only with specifically authorised employees	not allowed, unless with permission in advance from the person who created the information and subject to the protection of a confidentiality agreement

Sharing information of clients and other business partners – chapter 4.2

type of information	sharing internally	sharing externally
non-sensitive NB: information is only non-sensitive if you have determined that it is available in the public domain	allowed	allowed
sensitive in principle, all client information falls at least into this category	only with employees who need the information to carry out tasks contractually agreed with the client **OR** with permission from the client[5]	not allowed, unless with permission from the client and protected by a confidentiality agreement
critical /strictly confidential	only with employees who need access to the information to carry out the work contractually agreed with the client **OR** with permission from the client[6]	not allowed

[5] Irrespective of the permission from the client, there are instances in which it may be illegal to share the client's information: for instance, in a tender process in which Ordina is not permitted to use information to which other competitors may not have access. You can find more information on this subject in the Fair competition policy.

[6] idem