|  |
| --- |
| **Guide to using Wired Relations' templates** |

Wired Relations' templates\* can be used directly in your work with data protection and information security - but can also be used as inspiration for your own material. You can modify them as needed to make them exactly as you want them.

NOTE! There may be sections that are not relevant to all organizations. If this is the case, it will be clearly indicated in the text.

There will be places in the text where you are prompted to insert the organization's name or other information. In these cases, it will be marked as follows: [insert organization's name].

At the bottom of each document, there will be a table that provides an overview of the document's version, the latest update, and who is responsible for the document.

Here are some additional tips for using Wired Relations' templates:

* Read the instructions carefully before you start using the templates. This will help you understand how to use them effectively.
* Customize the templates to fit your organization's needs. You can add or remove sections, change the wording, and add your own logo and branding.
* Keep your templates up to date. Data protection and information security regulations are constantly changing, so it's important to make sure your templates are always up to date.

We hope you find Wired Relations' templates helpful. If you have any questions, please don't hesitate to contact us.

Here are some links to additional resources that you may find helpful:

* The Danish Data Protection Agency: [https://datatilsynet.dk/](https://datatilsynet.dk/" \t "_blank)
* The Danish Centre for Cybersecurity:  [Center for Cybersikkerhed (cfcs.dk)](https://www.cfcs.dk/da/)

**Information security policy**

**1. Purpose**

The purpose of this information security policy is to establish the framework for the work with information security within [insert organization’s name here]. The policy creates the foundation upon which the work with information security is established.

The purpose of the policy is also to create a common consensus of what information security is as a whole and define both goals and the division of responsibilities for the work with information security within [insert organization’s name here].

**2. Definitions**

Information security policy means the protection of all resources that are part of, or contribute to, the processing of data, both electronically and physically. The protection includes all relevant measures, including measures related to technology as well as organizational processes.

Data encapsulates all information related to the business conduct of [insert organization’s name here], including development, delivery and servicing of solutions and products to customers and potential customers, as well as information related to employees of [insert organization’s name here].

**3. Scope**

The policy is applicable to all [insert organization’s name here] business practices; including all employees as well as for use of all systems used by [insert organization’s name here].

**4. Objectives**

[insert organization’s name here] considers the work with information security as a quality element that supports the credibility of the product that [insert organization’s name here] offers. This is reflected in the fact that [insert organization’s name here] constantly strives to ensure a high level of security that reflects its contextual development.

[insert organization’s name here] works towards obtaining the following certifications:

* [insert relevant certifications/declarations (e.g., ISAE-3000)]

[insert organization’s name here] strives to promote a good information security culture based on the mindset that a high level of information security is a crucial competitive parameter in a digitalised world. [insert organization’s name here] wants to convey this message to customers as well as employees, which must be communicated through awareness campaigns and general communication.

The work with information security in [insert organization’s name here] must be based on the current legislation as well as recognised standards within information security. This should be reflected in the level of information security in [insert organization’s name here], which should be consistent with the requirements that can be deduced from it.

The level of security within [insert organization’s name here] must at all times reflect that [insert organization’s name here] complies with the agreements that [insert organization’s name here] has entered into with its customers regarding the security of the processing of their data.

The level of security in [insert organization’s name here] must be determined on the basis of risk assessments that include the current level of threat.

The level of security in [insert organization’s name here] must also ensure a high degree of confidentiality, integrity and accessibility:

* **Confidentiality:** Data may only be available in the relevant systems and for those persons who, for reasons of necessity, have been granted access. The data must be treated in a confidential manner within this framework.
* **Integrity:** Systems, including IT systems used in the course of business operations, must be reliable and function properly. It must also be ensured that the data basis is both reliable and credible.
* **Accessibility:** [insert organization’s name here]’s systems must be available 24/7 to the extent possible when taking maintenance etc. of the system into question. The system must be subject to the necessary security measures to ensure accessibility (as well as confidentiality and integrity). In addition, an IT contingency plan must be maintained that can ensure that normal operation of the business systems can be re-established within 24 hours if availability is temporarily lost.

**5. Responsibility**

It is the management within [insert organization’s name here] which has the overall responsibility for ensuring that [insert organization’s name here] lives up to the objectives of this policy.

The day-to-day management of working with information security is handled by the company’s internal compliance team in collaboration with the company’s IT department.

For each system used in [insert organization’s name here], one or more system administrators have been appointed to assist the internal compliance team in the work with information security in relation to the individual system.

The individual employee is responsible for carrying out her/his work in accordance with this policy, as well as for following the guidelines that should arise from this policy. The individual employee is also obliged to notify management of breaches of information security or suspicions thereof.

**6. Follow-up**

This policy, as well as the guidelines, policies and procedures arising therefrom are reviewed and approved once a year by the management team of [insert organization’s name here] in collaboration with the compliance team.

Any change to this policy or the guidelines, policies and procedures arising therefrom, must be made in compliance with the obligations of [insert organization’s name here] on the basis of concluded data processing agreements, etc.

The level of security is assessed on an ongoing basis by the compliance team in collaboration with the company's IT department to the extent necessary to comply with the objectives of this policy.

**7. Violation**

Violations of this information security policy or supporting guidelines, policies or procedures may have employment consequences.

**8. Exceptions**

This policy can be deviated from, if it is assessed by the management that this will be a necessary part of the business. Deviations from this policy must be specifically justified and must be documented. Management must strive to avoid deviations to the greatest possible extent.

**9. Supportive guidelines, policies and procedures**

[insert organization’s name here] maintains a list of applicable policies, policies and procedures arising out of this policy.

**10. Documentation**

[insert organization’s name here] documents the work with information security as well as compliance with the data protection law rules on [insert organization’s name here]'s site in [insert organization’s name here].

**11. Contact**

Questions regarding [insert organization’s name here]'s work with information security and data protection can be directed to the company's internal compliance team.

Contact: [insert email address of contact person in the organization]

### **Document Information**

|  |  |
| --- | --- |
| Document Version |  |
| Date of Issue for This Version |  |
| Responsible Person |  |
| Status |  |