**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 for all companies. If this is the case, it will be clearly indicated in the text.

|  | Text boxes in the document contain focus points and good advice. Please note that the text boxes should be removed from the final version of the specific policy or procedure. |  |
| --- | --- | --- |

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

At the end 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: |  |
| --- | --- | --- |
|  | * You can add or remove sections, change the wording, and add your own logo and branding.
 |  |
|  | * Stay up-to-date with your templates. Data protection and information security regulations are evolving rapidly, so it's crucial to keep your templates current.
 |  |
|  | Should you have any inquiries concerning the templates, please feel free to contact us. |  |

**Information Security Policy**

**1. Purpose**

The purpose of this information security policy is to establish the framework for information security work in *[insert company's name]*. Furthermore, the policy aims to create a common understanding of what information security entails, including defining objectives and responsibilities for information security work in *[insert company's name]*.

**2. Definitions**

Information security is understood as the protection of all assets involved in or contributing to the processing of data, both electronically and physically. Protection encompasses all relevant measures; including measures related to organizational processes, individual behavior, physical environments, and technology. Data refers to all information related to *[insert company's name]*'s business operations; including the development, delivery, and servicing of solutions/products to customers and potential customers, as well as information related to employees, etc. in *[insert company's name]*.

**3. Scope**

The policy applies to all of *[insert company's name]*'s business operations; including all employees, etc., and all use of systems, etc. used by *[insert company's name]*.

**4. Objectives**

*[insert company's name]* considers information security work a quality element that supports the credibility of the product offered by *[insert company's name]*. This is reflected in *[insert company's name]*'s efforts to ensure a high level of security that continuously reflects its contextual development. *[insert company's name]* strives to achieve the following certifications/declarations:

*[Insert relevant certifications/auditor's statements (e.g., ISAE-3000 or ISO27001 certification)]*

*[insert company's name]* strives to promote a good information security culture based on a mindset that a high level of information security is a crucial competitive parameter in a digitalized world.

*[insert company's name]* wishes to communicate this message to both employees and customers, which should be expressed through a strong awareness campaign and through general communication. Information security work in *[insert company's name]* must be based on applicable legislation and recognized standards in information security. This must be reflected in the level of information security in *[insert company's name]*, which must comply with the requirements that can be derived therefrom. The level of security in *[insert company's name]* must at all times reflect the fact that *[insert company's name]* complies with the agreements that *[insert company's name]* has entered into with its customers regarding the security of the processing of their data. The level of security in *[insert company's name]* must be determined on the basis of risk assessments that take into account the current threat landscape. The level of security in *[insert company's name]* must also ensure a high degree of confidentiality, integrity, and availability:

* **Confidentiality:** Data may only be accessible in relevant systems and to those persons who, based on a necessity assessment, have been granted access. The data must be handled confidentially within these frameworks.
* **Integrity:** Systems, including IT systems used as part of business operations, must be reliable and function correctly. It must also be ensured that the data basis is both reliable and trustworthy.
* **Availability:** *[insert company's name]* systems must be available 24/7 to the extent that this is possible, taking into account the maintenance of the systems in question, etc. The systems must be subject to the necessary security measures to ensure availability (as well as confidentiality and integrity). An IT contingency plan must also be maintained to ensure that normal operation of business systems can be re-established within 24 hours if availability is temporarily lost.

**5. Responsibility**

Management in *[insert company's name]* has overall responsibility for ensuring that *[insert company's name]* complies with the objectives of this policy. The day-to-day management of information security work is carried out by *[e.g., the internal compliance team]* For each system used in *[insert company's name]*, one or more system administrators have been designated who are responsible for information security in relation to the individual system. Each employee is responsible for performing their work in accordance with this policy and for following the guidelines, etc., that arise from this policy. Each employee is also obliged to notify management of any breaches of information security or suspicion thereof.

**6. Follow-up**

This policy, as well as the guidelines, policies, and procedures that arise from it, is reviewed and approved once a year by the management of *[insert company's name]* in cooperation with the company's internal compliance team.

Any changes to this policy or the guidelines, policies, and procedures that arise from it must be made in compliance with the obligations that *[insert company's name]* has based on concluded contracts, data processor agreements, etc.

The level of security is continuously assessed by the company's internal compliance team in cooperation with the company's IT department to the extent necessary to comply with the objectives of this policy.

**7. Violation**

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

**8. Exceptions**

This policy may be deviated from if management deems it necessary for business operations. Deviations from this policy must be specifically justified and documented. Management must strive to avoid deviations as much as possible.

**9. Supporting Guidelines, Policies, and Procedures**

*[insert company's name]* maintains a register of current guidelines, policies, and procedures that arise from this policy.

**10. Documentation**

*[insert company's name]* documents its work on information security and compliance with data protection regulations on the [insert company's name] site in Wired Relations.

**11. Contact**

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

Contact: *[Insert email address of contact person in the company].*

**Document information**

| Document version |  |
| --- | --- |
| Date of Issue for this version |  |
| Responsible Person |  |
| Status |  |