|  |
| --- |
| **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.

|  |
| --- |
| Text boxes in the document contain focus points and good advice for you as a data controller or data processor. 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 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.

**Security Measures in [Insert Organization Name]**

**1. Purpose**

The security measures in [Insert Organization Name] are designed to ensure that the security level in [Insert Organization Name] reflects the objectives of [Insert Organization Name]'s information security policy.

**2. Organizational Security Measures**

**2.1. Regulation of Employee Conduct**

[Insert Organization Name] has implemented [insert relevant document name for example: Guidelines for Employees on Information Security and Data Protection], which set out guidelines that relate to the work on information security in the company; including what specific security measures each employee must take.

**2.2. Awareness Activities**

Employees in [Insert Organization Name] are kept up to date on relevant topics in data protection and information security.

2.2.1. Induction Day

When employed in [Insert Organization Name], an induction day is held where employees are trained in data protection and information security.

2.2.2. Knowledge Sharing

Employees are regularly informed about relevant news and current focus areas within data protection and information security in the company's [insert relevant channels].

Employees can also find information on topics within data protection and information security on the company's intranet.

[Insert Organization Name] continuously shares knowledge on relevant topics within data protection and information security in connection with employees' tasks, including knowledge sharing in connection with regular knowledge-sharing meetings.

2.2.3 Content

[Insert Organization Name]'s awareness activities include information on relevant guidelines, procedures, and policies that arise from [Insert Organization Name]'s information security policy.

The awareness activities also include information on relevant rules in the field of data protection legislation and the consequences of violating these provisions.

The awareness activities must be adapted to the specific target audience so that the best possible effect is achieved.

2.2.4 Responsibility

The awareness activities are carried out by [Insert Organization Name]'s compliance team.

2.2.5. Evaluation

The awareness activities are evaluated annually. It is also assessed which awareness measures are needed.

2.2.6. Documentation

The awareness activities are documented in [Insert Organization Name]'s awareness folder.

**2.3. Administration of User Rights**

2.3.1 Access Restriction

* Access to systems, etc., used by [Insert Organization Name] must be restricted so that it is a prerequisite for access that there is a work-related need.
* The management of [Insert Organization Name] administers the granting and withdrawal of user rights.
* When an employee no longer needs to have access to a system, access must be terminated.
* When an employee's employment ceases, the "termination procedure" is reviewed to ensure that the employee's access and user rights are terminated.

A review of all accesses to the relevant systems is carried out semi-annually to ensure that the accesses to the systems are relevant.

2.3.2. Responsibility

The management of [Insert Organization Name] is responsible for ensuring that employees have the correct user rights.

2.3.3. Evaluation

Granted user rights are followed up annually.

**2.4. Addition of New Systems/Suppliers**

Employees are instructed that a system must be approved before it is taken into use.

The following guidelines must also be followed when adding systems where personal data is not processed.

2.4.1. Approval of New Systems/Suppliers

The company's compliance team initially assesses:

* Whether the information about the use of the system is sufficient; including whether the use of the system has been approved by the manager and whether the use of the system is necessary.
* Whether personal data is processed in the system in question and whether the processing of personal data will be in accordance with data protection legislation.
* Whether the commissioning of the system/supplier in question will be in accordance with the data processing agreements that have been entered into with customers.
* Whether the system/supplier in question is covered by a sufficient level of security.

The company's IT department assesses whether the system is subject to sufficient technical security measures.

Then the system is approved by the company's management.

The approval must take the following elements into account:

* The use/addition of new systems should be limited to what is necessary.
* The use/addition of new systems should take place on as informed a basis as possible by investigating the supplier's processing of personal data and its security measures.
* Suppliers from third countries should be avoided as far as possible.

When a new system has been approved, the compliance team must ensure that:

* The information obligation is complied with in relation to the processing in question.
* The system and the supplier contain sufficient information on the [Insert Organization Name] site in Wired Relations: including information on data processing relationships, etc.

**2.5 Guidelines for the Use of Systems and Devices**

[Insert Organization Name] has established guidelines for the use of systems and devices.

The specific regulation of the use of systems and devices, etc., is set out in the [insert relevant document name for example: Guidelines for Employees on Information Security and Data Protection].

**2.6. Confidentiality**

Employees of [Insert Organization Name] are subject to confidentiality in relation to the processing that is carried out as part of their employment. This is stated in the employees' employment contracts.

Management-approved external consultants may, after signing a confidentiality agreement, gain access to data on the same principles as the company's other employees. External consultants are also subject to [Insert Organization Name]'s information security policy and the policies, guidelines, and procedures that flow from it.

**3. Technical Security Measures**

The implementation of [Insert Organization Name]'s technical security measures is carried out by [Insert Organization Name]'s IT department.

**3.1. General Technical Security Measures**

The following is a non-exhaustive list of technical security measures used in [Insert Organization Name]:

* All workstations use a VPN connection and are protected by a firewall and endpoint protection.
* [Insert Organization Name] uses two-factor authentication on selected systems.
* Data stored on electronic removable media outside the company must be stored in encrypted form.
* Data may only be exchanged with partners via a secure connection or by encrypting data.

**3.2. IT Contingency Plan**

[Insert Organization Name] has an IT contingency plan that is continuously tested.

**3.3. Follow-up**

The established technical measures are continuously tested by vulnerability scans and penetration tests.

**4. Physical Access Control**

Security measures relating to the company's premises, etc.; including physical access control and alarms, are handled by [insert by who].

### **Document Information**

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