**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. |  |

# **Supplier Management Policy**

**1. Purpose**

|  | It is essential to establish security requirements for suppliers before entering into an agreement and to continuously monitor compliance with these requirements after the agreement has been entered into. Security requirements must be proportionate and appropriate to the risk associated with using the supplier's services and deliveries. |
| --- | --- |

The purpose of this policy is to establish clear guidelines for entering into partnerships with the company's suppliers, including ongoing supplier management.

**2. Scope**

The term supplier management encompasses all phases of *[insert company name]*'s collaboration with suppliers, including (i) the procurement of a system or service, (ii) ongoing contract management, including monitoring and evaluation of the supplier's performance, to (iii) termination of the partnership.

**3. Roles and Responsibilities**

The management of *[insert company name]* is ultimately responsible for the company's management of cyber and information security, including the internal organization and setting of the company's security level. Management is also responsible for ensuring that there are the right resources and competencies to carry out the task of supplier management within the company.

The day-to-day responsibility for supplier management is placed with *[insert person responsible for supplier management]*.

With regard to data protection matters, responsibility lies with *[insert relevant contact point, team or DPO]*.

|  | Describe any delegated responsibilities for technical advice, risk identification, ongoing monitoring, etc. to, for example, the IT manager or system and data owner.In addition, the responsibility for ongoing contract management and legal advice should be described.  |
| --- | --- |

**4. Supplier Selection - Procurement of a System or Service**

When entering into an agreement with a new supplier, it is important to simultaneously set requirements for the supplier's information security.

An assessment of which requirements should be set is made based on a risk assessment of the specific delivery and supplier. At the same time, it is assessed how critical the supplier's performance is to *[insert company name]*.

In connection with the setting of requirements, it must also be determined how *[insert company name]* can subsequently follow up on the requirements set for the supplier.

For example, it may be agreed that the supplier must be able to demonstrate compliance with the security requirements (ISO27001 certification, audit reports, etc.), quarterly meetings, physical inspections, or other means by which information security and the supplier's services can be discussed.

|  | Here are some general security requirements that can be included in company contracts, regardless of the specific delivery:* It is beneficial to create a list of general security requirements that can be included in all company contracts, regardless of the specific delivery.
* Different sets of requirements can be created to accommodate varying risk profiles, criticality assessments, or classifications.
* The severity of the security requirements should be directly proportional to the risk posed by the supplier and the criticality of their services to the company's operations.
* When specifying cybersecurity requirements, emphasis should be placed on achieving the desired security outcomes rather than dictating the exact technical measures to be implemented by the supplier.

\*\*\*\*\*The Danish Center for Cyber Security (CFCS) has developed a guideline for outsourcing IT systems. It can be found [here (in Danish)](https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/Vejledning-cybersikkerhed-i-leverandorforhold_cfsc_digst-2022.pdf) . For public authorities that have outsourced critical IT systems, there are specific requirements for contract and supplier management, as outlined in the Digitalization Agency's guidelines, available [here (in Danish)](https://www.sikkerdigital.dk/Media/638137953663038929/Katalog%20over%20krav%20til%20kontrakt-%20og%20leverand%C3%B8rstyring%20for%20samfundskritiske%20it-systemer%202023.pdf). |
| --- | --- |

4.1. Documentation

A maintained list of all relevant suppliers is kept in *[Insert e.g. Wired Relations and also describe how contract management takes place].*

The assessments made during the process, including risk assessments, are documented in *[e.g. Wired Relations or other].*

**5. Ongoing Supplier Management During the Contract Period**

Ongoing risk assessments of the supplier and its services are carried out to address potential risks to *[insert company name]*. This helps ensure that we continuously adjust and set the right requirements for our suppliers.

In addition, ongoing monitoring and supervision of suppliers is carried out in accordance with the agreed contract, ensuring that suppliers comply with their obligations.

*[Insert relevant function, team, or department]* is responsible for ongoing supplier management.

All risk assessments and inspections are documented in *[insert e.g. GRC platform, Wired Relations or other].*

|  | It is a resource-intensive task to carry out ongoing supervision of suppliers, and it is important to use the available resources in the company in the best possible way.Therefore, it is also important that the ongoing supervision of suppliers is commensurate with the risk assessment and assessment of criticality that has been carried out of the supplier and its services.Describe your considerations on this matter. |
| --- | --- |

**6. Termination of a Supplier Relationship**

When a partnership with a supplier ceases or is terminated, it is essential that cyber and information security is maintained. This is addressed already at the conclusion of the agreement, where the focus should be on:

* The supplier's obligations and continued service objectives during the termination period, if the agreement is terminated voluntarily or due to disputes between the parties.
* Our requirements for cyber and information security in the customer-supplier relationship while the task is transferred to another supplier or taken over by ourselves.
* A complete list of the information and assets (including backup) stored with the supplier that must be returned, transferred to a new supplier, or disposed of. There should be a plan or procedure for how this is ensured.

The supplier must be obligated to a smooth transition and operation if there is a re-tendering, if the task is brought in-house, or if the task is to be transferred to a new supplier.

A plan must be developed for how the agreed security level is maintained throughout the entire termination process, including which security measures must be in place during the process.

**7. Evaluation of Supplier Management**

The practical aspects of supplier management in *[insert company name]* are evaluated continuously and at least once a year to ensure effectiveness and relevance. Based on this, this policy is updated.

Changes to the policy will be communicated to all relevant parties.

**Document information**

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