**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. |  |

# **Policy for reporting and handling security incidents**

**1. Purpose**

The purpose of this policy is to establish a consistent and effective method for managing cyber and information security incidents to minimize the risk of breaches to the confidentiality, integrity, and availability of information.

Additionally, this policy aims to ensure relevant and up-to-date communication regarding threats and vulnerabilities.

**2. Scope**

This policy applies to the entire company. All employees of *[insert company name]* are expected to be familiar with the contents of this policy and know how to respond if they suspect or detect a cyber or information security incident.

|  | If relevant, consider adding: This policy also applies to external stakeholders such as consultants and partners who have access to the company's systems or data. |
| --- | --- |

**3. Definitions**

A security incident can be characterized as a state, activity, or event that negatively impacts (or has the potential to impact) the confidentiality, integrity, and availability of the information we hold at *[insert company name]*.

|  | There are various definitions of security incidents. Below are some examples that can be used as a starting point. In the ISO27000 standard, an information security incident is described as*:* *“An identified occurrence of a system, service, or network state which compromises the security policy of an information system or a security control, or a security-relevant event.”*CFCS defines an IT security incident as:*“An event that negatively affects or is assessed as likely to affect the availability, integrity, or confidentiality of data, information systems, digital networks, or digital services.”*The NIS2 Directive provides the following definitions of incidents, according to Article 6(1)(5-7): *“Near miss*: *an event which could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of services offered by or accessible through information and communication systems but which was prevented from materializing or did not materialize.”* *“Incident: an event which compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of services offered by or accessible through information and communication systems.”* *“Large-scale cybersecurity incident: an incident causing a disruption at a level that exceeds a Member State’s capacity to respond to it or having a significant impact on at least two Member States.”* |
| --- | --- |

Examples of an incident that could potentially lead to a security breach:

* Multiple failed login attempts by unauthorized individuals
* Suspicious traffic on the company network
* Computers stolen from the company premises

Examples of confirmed security breaches:

* **DDoS attack:** An attack that overwhelms a system with traffic to make it unavailable to legitimate users.
* **Ransomware**: An attack where malicious actors encrypt a company's data and demand payment to decrypt it.
* **Malware:** Malware (malicious software) is installed on a system without the user's knowledge and can steal data or take over control of the system.
* **Loss of physical devices:** A laptop or mobile phone containing sensitive data is stolen or lost.

If personal data is involved in an information security breach, this must also be handled in accordance with the personal data breach policy.

**4. Reporting Security Incidents**

If an employee discovers or suspects a security incident or if a specific security breach is detected, they must immediately contact: *[insert relevant contact point - and describe specifically how the security incident should be reported (also outside of normal business hours)]*.

The sooner a response is made, the sooner the security breach can be stopped or perhaps even prevented. A quick response can help minimize the potential consequences associated with a security incident.

|  | It varies from company to company how much the individual employee should do in relation to a specific security incident. If it is expected that the employee should handle it themselves, it can be useful to describe what is expected of the employee, for example:* Stop the information security breach (if possible)
* Get an overview of the situation (and document the individual steps)
* Assess the information security breach, including describing any mitigating measures, notification, etc. (a specific procedure can be developed for this)
* Report to the relevant contact point
 |
| --- | --- |

**5. Handling and Assessment of Security Incidents**

Reporting of security incidents is made to *[insert relevant contact point]*, who will then immediately assess the security incident, in accordance with *the procedure for handling and assessing security incidents*.

Handling and assessment of the security incident includes, among other things, an assessment of whether a crisis response should be initiated, how the security incident should be handled in relation to any mitigating measures, management reporting, reporting to relevant authorities, documentation, evaluation, and awareness.

*[Insert relevant contact point]* handles and assesses security incidents according to the procedure for handling security incidents.

**6. Communication and Awareness**

The learning associated with handling security incidents must be communicated widely throughout the company to ensure that the risk of it happening again is minimized. This can be done in connection with ongoing awareness of information and cybersecurity.

The same applies if new threats or vulnerabilities are identified that could affect information security at *[insert company name]*.

**Document information**

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

###