**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. |  |

**Procedure for handling security incidents**

**1. Purpose**

The purpose of this procedure is to establish clear guidelines for the handling of security incidents.

**2. Scope**

This procedure is primarily intended for *[Insert relevant contact point/team responsible for assessing and handling security incidents]*, who are responsible for assessing and handling security incidents within *[insert company's name*.

| It is important to establish a fixed contact point within the company that is responsible for assessing and handling security incidents. This can be described in a general security incident handling policy.  Employees should know how to react and who to contact if they discover a security incident (or even suspect one).  Additionally, employees should receive ongoing training or education on this topic. |
| --- |

**3. Incident Response Process**

When *[Insert relevant contact point/team responsible for assessing and handling security incidents]* is notified of a security incident, there are several steps to consider:

3.1 Contain the Incident

If possible, the security incident should be contained as quickly as possible. This can be done in various ways depending on the nature of the incident. For example, it may involve disconnecting networks to prevent the spread of malware or unauthorized access, or shutting down systems to prevent further damage. It may also be necessary to block all access to the compromised system.

3.2 Assess for a Crisis Situation

It should always be assessed whether a crisis situation exists that requires the activation of the relevant emergency response. *[List examples of what a crisis situation might be, or what parameters should be considered. You can also refer to an existing crisis management plan or IT contingency plan for the assessment of whether a crisis situation exists and whether the emergency response should be activated.]*

3.3 Assess and Analyze the Incident

*[Insert relevant team/contact point responsible for assessing and handling security incidents]* is responsible for assessing and analyzing the security incident to determine how to handle the situation and how to prevent similar situations in the future. If a security incident involves personal data, this must be assessed by *[insert contact information for e.g., DPO or other relevant contact point]*. It is important that ongoing assessments are documented, see section 5.

3.4 Risk Assessment

Based on the handling of the security incident, it should always be assessed whether a risk assessment should be conducted or whether the existing and current risk assessment should be updated.

3.5 Implement Selected Measures

In connection with the assessment of the security incident, specific security measures to be implemented are identified. A plan for the specific implementation must be developed, including who is responsible for the implementation and the deadline. This should be included in the documentation of the security incident.

3.6 Notification/Reporting

As the security incident is assessed and handled, it must also be determined whether the security incident is of such a nature that a report must be made to, for example, (in Denmark the National Center for Cyber Security or the Danish Data Protection Agency).

| **Examples of Notification and Reporting Requirements**  *It is advisable to specify which regulations are relevant for your company.*  Major Security Incidents  If your organization has experienced a security incident, you may be required to notify relevant authorities. (in Denmark the Center for Cyber Security (CFCS). Since September 1, 2014, all government agencies have been obligated to notify the CFCS about major security incidents. Notifications of security incidents to the CFCS are made via virk.dk.)  Voluntary Notification  Companies may have the option to voluntarily notify relevant authorities of major security incidents. (In Denmark to the CFCS. Voluntary notifications are also made via virk.dk.)  Companies Covered by the NIS Directive  Specific notification requirements apply to authorities and companies covered by the current NIS Directive.  Such notifications of security incidents must be made to the authorities (in Denmark to CFCS, which is the national CSIRT, and to the relevant sectoral authorities).  Regarding the Upcoming NIS2 Legislation  In the draft law on measures to ensure a high level of cybersecurity, it is proposed that essential and important entities must, without undue delay, notify the relevant competent authority and the CSIRT of any significant incident, and that the requirements for the procedure and deadlines for notifications correspond in content to the requirements of the NIS2 Directive (Article 23).  Reporting to the relevant data protection authority  As a general rule, all personal data breaches must be reported to the relevant data protection authority (in Denmark to Datatilsynet). Only if it is unlikely that the personal data breach poses a risk to the rights and freedoms of natural persons is a notification not required. |
| --- |

3.7 Notification to Management and Other Stakeholders

| **Examples of notification and reporting requirements.**  *Please detail which specific regulations apply to your organization.*  Management involvement is crucial in assessing and responding to security incidents. They are ultimately accountable for ensuring proper handling and can provide necessary resources. |
| --- |

It should be assessed on an ongoing basis whether other stakeholders need to be informed about the specific security incident. This assessment should be documented.

**4. Documentation**

The assessment and handling of a security incident or breach should be documented on an ongoing basis. Documentation of the process is very important, especially as supporting documentation if the incident or breach results in a legal investigation.

Additionally, thorough documentation supports the considerations that have been made, for example, regarding mitigating measures.

**5. Evaluation**

After an incident is handled, an evaluation of the process should be conducted, including lessons learned and an assessment of whether additional preventive measures should be implemented.

A continuous assessment of the effectiveness of the incident handling process should also be conducted. The evaluation should also be documented.

**Document information**

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