**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.

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. |  |

**AI Policy**

*Effective Date: xx.xx.202x*

**1. Purpose**

The purpose of this policy is to provide guidelines for the appropriate and secure use of generative artificial intelligence (AI) models, such as ChatGPT, Bard, Copilot etc., within *[insert company name]*. This policy aims to ensure the protection of sensitive information, maintain ethical standards, and mitigate potential risks associated with the use of generative AI.

**2. Scope**

This policy applies to all employees, contractors, and third parties who utilize generative AI models, including ChatGPT, on behalf of *[insert company name]*.

**3. Policy Statements**

**3.1. Authorization and Access**

1. Access to generative AI models shall be granted only to authorized personnel who have received proper training and have a legitimate business need.
2. *[Insert relevant title, for example CTO]* or their designated representative shall approve and oversee access to generative AI models.
3. Unauthorized distribution, sharing, or replication of generative AI models is strictly prohibited.

**3.2. Data Usage and Privacy**

1. Generative AI models shall not be used to generate, process, or manipulate personal data or sensitive personal data, customer data or critical business information unless explicit approval is obtained from the appropriate data privacy and legal teams.
2. Generative AI models may only be used as a supporting system and shall be reviewed for its accuracy and you have to check the quality and correctness of the output.
3. Users of generative AI models are not allowed to enter personal data or sensitive personal data, customer data or critical business information in to this model at any time.

**3.3. Ethical Use**

1. Users of generative AI models are prohibited from engaging in any activities that may result in harm, misinformation, or deception.
2. The generated content must adhere to ethical standards, and users must avoid generating offensive, discriminatory, or harmful content.

**3.4. Intellectual Property**

1. Users shall respect intellectual property rights and not use generative AI models to infringe upon copyrights, trademarks, or other intellectual property rights.
2. Content generated using generative AI models may only be used within *[insert company name]* for authorized purposes. See point 3.2.2

**3.5. Security and Compliance**

1. Users shall adhere to all applicable laws, regulations, and compliance requirements when using generative AI models.
2. All generated content shall be subject to regular security assessments and reviews to identify and mitigate potential vulnerabilities.
3. The *[insert relevant title, for example CTO]* shall ensure that generative AI models are regularly updated with the latest security patches and updates.

**4. Responsibilities**

**4.1. *[Insert relevant title, for example CTO]***

The *[insert relevant title, for example CTO]* or their designated representative shall:

1. Approve access to generative AI models.
2. Oversee the implementation of this policy.
3. Ensure that security measures are in place to protect against potential risks.
4. Provide guidance on ethical usage and best practices.

**4.2. Authorized Users**

Authorized users shall:

1. Complete training on the appropriate use of generative AI models.
2. Comply with this policy and adhere to ethical standards.
3. Report any security incidents or concerns related to the use of generative AI models to the *[insert relevant title, for example CTO].*

**5. Non-Compliance**

Violations of this AI usage Policy or supporting guidelines, policies or procedures may have employment consequences.

**6. Policy Review**

This policy will be reviewed and updated as necessary to ensure its effectiveness and relevance. Changes to the policy will be communicated to all relevant parties.

**7. Approval**

This policy, as well as the guidelines, policies and procedures arising therefrom are reviewed and approved once a year by the management team of *[insert company name]* in collaboration with the compliance team.

This policy has been approved and authorized by:

*[insert name of the responsible person, for example the CTO]*

*[insert relevant title, for example CTO]*

*[insert company name]*

**Document information**

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