**AI Security Policy Template**

**1. Purpose**

The purpose of this AI policy is to establish guidelines and principles for the usage of AI technologies within [Organisation Name]. This policy aims to ensure that AI systems are utilised in a manner that prioritises ethical considerations, safeguards privacy and security, and aligns with the organisation's values and objectives.  
  
**2. Scope**

This policy governs the utilization of third-party or publicly available AI tools, encompassing platforms such as ChatGPT, Google Gemini, DALL-E, Midjourney, and analogous applications designed to simulate human intelligence for generating responses, producing work outputs, or executing specific tasks. **3. Dos/Don'ts**

**3.1 Dos:**

**🗸** Prioritise ethical considerations and fairness in AI deployment.

**🗸** Acknowledge that AI tools can offer utility but should not replace human judgment and creativity.

**🗸** Recognise the potential for inaccuracies, including "hallucinations," false information, or incomplete information, in AI outputs, and always verify responses meticulously.

**🗸** Treat all information provided to an AI tool as potentially public, regardless of tool settings  
or assurances from creators.

**🗸** Inform your supervisor when utilising an AI tool to aid in task completion.

**🗸** Ensure that any response from an AI tool intended for reliance is accurate, unbiased,   
compliant with intellectual property and privacy laws, and aligns with company policies.

**🗸** Obtain explicit written permission from your supervisor and the IT Department before integrating any AI tool with internal company software.

**3.2 Don'ts:**

* Do not rely solely on AI algorithms without human oversight and intervention in critical   
  decision-making processes.
* Avoid using AI tools in making employment decisions concerning applicants or employees, spanning recruitment, hiring, performance monitoring, and termination.
* Refrain from inputting confidential, proprietary, or sensitive company data into any AI tool, such as passwords, health information, or personnel material.
* Do not upload personal information about any individual, including names, addresses, or likenesses, into  
  AI tools.
* Do not misrepresent AI-generated work as your original creation.
* Do not use AI tools not included in the approved list from the IT Department, as malicious chatbots could potentially compromise information security.

**4. Violations**

Violations of this AI policy may result in disciplinary action, including but not limited to reprimands, training requirements, suspension of AI system usage privileges, or termination of employment, depending on the severity and recurrence of the violation.  
  
**5. Disclaimer**

This AI policy is intended to provide general guidance and principles for the ethical and responsible use of AI within [Organisation Name]. It does not constitute legal advice, and [Organisation Name] reserves the right to modify or amend this policy as necessary to address evolving regulatory requirements, technological advancements, or organisational needs.  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Please Note:** The above policy document serves as an illustrative example and does not constitute legal advice or a comprehensive AI security policy for any specific organisation. It is imperative to consult with appropriate legal counsel, compliance officers, and relevant stakeholders within your organisation to develop a tailored AI security policy that meets your specific needs, regulatory requirements, and risk tolerance. Implementation of any AI security policy should be subject to thorough review and approval by authorised personnel and regulatory authorities within your organisation. Additionally, ongoing monitoring and updates may be necessary to ensure continued compliance and effectiveness in addressing evolving security concerns associated with AI technologies.