**Cybersecurity Policy for AI and LLM Usage**

**Purpose**

This policy outlines guidelines for employees to ensure the secure and ethical use of Artificial Intelligence (AI) technologies, including Large Language Models (LLMs) like ChatGPT (Shadow AI). The goal is to protect sensitive information, maintain data privacy, and mitigate potential risks associated with AI usage.

**Scope**

This policy applies to all employees who use AI technologies, including LLMs, in their work.

**Policy Statement**

Employees are expected to use AI technologies responsibly and ethically, adhering to the following principles:

1. **Data Privacy and Security:**
	* **Data Protection:** Handle sensitive data with care and do not share confidential or sensitive information with AI systems.
	* **Data Minimization:** Only input necessary data into AI systems.
	* **Secure Data Transfer:** Use secure methods to transfer data to and from AI systems.
	* **Data Storage:** Often LLMs will save previous chat history and are reviewed by human’s as part of the AI development. Employees should disable all recall and storage functionality within LLM’s such as ChatGPT and Gemini to ensure that sensitive data is not exposed.
2. **Ethical Use:**
	* **Bias Awareness:** Be aware of potential biases in AI outputs and interpret results critically. You should manually verify responses for accuracy.
	* **Misinformation Prevention:** Avoid sharing or generating misleading or harmful content.
	* **Intellectual Property:** Respect copyright laws and avoid using AI to infringe on intellectual property rights.
3. **Security Best Practices:**
	* **Strong Passwords:** Use strong, unique passwords for AI accounts and avoid sharing them.
	* **Phishing Awareness:** Be cautious of phishing attacks targeting AI users.
	* **Software Updates:** Keep AI software and systems up-to-date with the latest security patches where applicable.
4. **Responsible AI Usage:**
	* **Human Oversight:** Use AI as a tool to assist, not replace, human judgment.
	* **Validation:** Verify AI-generated outputs, especially for critical tasks.
	* **Transparency:** Be transparent about the use of AI in work processes.

**Violation of this policy may result in disciplinary action.**

**Additional Guidelines:**

* **Prompt Engineering:** Craft clear and specific prompts to guide AI systems.
* **Output Verification:** Always verify the accuracy and relevance of AI-generated content.
* **Training Data Quality:** Ensure the quality and relevance of data used to train AI models.
* **Regular Security Assessments:** Conduct regular security assessments of AI systems and infrastructure.

By following these guidelines, employees can harness the power of AI while mitigating potential risks and ensuring the security of the organisation.

**[Organization Name]** reserves the right to update this policy as needed to reflect changes in technology or regulatory requirements.