



Guidelines and Instructions for the Use of AI at Ceragon

Introduction

Artificial Intelligence (AI) has become an integral part of our work environment, offering numerous benefits and possibilities. However, it is crucial to understand the associated risks and ensure responsible usage. These guidelines and instructions outline the potential risks and uses of AI at Ceragon and establish general principles and rules for its application.

Risks of AI Usage:

1. **Intellectual Property Ownership:** AI-generated output may raise concerns about the ownership of intellectual property. When utilizing AI, it's important to recognize that the output created by AI systems could potentially be subject to intellectual property rights. This means that we must be mindful of protecting our own rights and ensuring that we have the necessary permissions or licenses to use AI-generated content in our work.
2. **Confidentiality Risks:** When using AI systems, it's crucial to consider the confidentiality of the input data. We should refrain from entering sensitive or confidential information and queries into AI systems which are not approved in Ceragon and provided to you by Ceragon (such as Microsoft Copilot, for example) to minimize the risk of unauthorized access or accidental disclosure. Examples include customer or partner data, employee personal information, financial results or forecasts, source code, product roadmaps, security incidents, passwords or credentials, contracts, pricing, legal advice, and any non-public business information. Protecting the confidentiality of our data helps maintain trust with our customers, employees, and partners.
3. **Privacy and Data Security:** AI relies on data for training and operation, which introduces privacy and data security considerations. We must handle this data with utmost care, ensuring compliance with privacy regulations and implementing robust data security measures. Safeguarding personal and sensitive information is essential to maintain the privacy and trust of individuals whose data we control or process.
4. **Inaccuracy:** AI systems, including platform-based AI, may produce output that is inaccurate or misleading. It's crucial to recognize that AI is not foolproof, reliable, and can make errors. Therefore, verify and validate results generated by AI tools before relying on them. Human review and critical assessment of AI-generated output are necessary to ensure accuracy and reliability.
5. **Discrimination:** AI algorithms can inadvertently perpetuate biases and discrimination if not carefully designed, trained, and monitored. Biases in training data or the underlying algorithms can result in unfair or discriminatory outcomes. It's imperative to be vigilant and regularly assess AI tools to mitigate any potential bias or discrimination in their use. Ensuring fairness and inclusivity in AI systems is a priority.
6. **Overreliance on AI:** One risk is the tendency to overly rely on AI systems, neglecting human judgment and critical thinking. While AI can provide valuable insights and assistance, it should not



replace human decision-making entirely. It's important to maintain a balanced approach that combines AI-generated output with human expertise and judgment.

7. **Ethical Implications:** AI systems can introduce ethical concerns, especially when they involve sensitive areas such as data analysis, profiling, or decision-making. It's important to be mindful of the potential ethical implications of AI usage and ensure that our actions align with ethical standards and principles. Regular ethical reviews of AI systems and practices can help address these concerns.
8. **Dependency on External AI Services:** If we rely on external AI services or platforms, there is a risk of dependency on third-party providers. This dependency can raise concerns regarding service availability, data ownership, and potential changes in pricing or terms of service. It's important to carefully evaluate and monitor any external AI services we integrate into our workflow.
9. **Compliance with Contractual Undertakings:** Some of our customers may require that we refrain from or notify them when using AI in the provision of our services or products. In case of any doubt, please contact our Product Team for confirmation.
10. **Malware Penetration:** Unapproved AI tools, plugins, browser extensions, and content generated by them (such as code, scripts, macros, links, or files) may contain or introduce malware, malicious code, or security vulnerabilities into Ceragon's systems. Unapproved or compromised AI tools may also be exploited through prompt injection or used as a channel for phishing or data exfiltration. Only approved AI tools should be used. Files created by approved AI tools (such as Microsoft Copilot) are considered approved for use, while code or files generated by unapproved tools should not be opened, run, or deployed without appropriate security review, and any suspicious AI tool behavior should be reported to IT immediately.

By understanding and being mindful of these risks, we can take appropriate measures to mitigate them and utilize AI in a responsible and ethical manner.

Possible Uses of AI:

1. **Content Drafting and Summarization:** AI may assist with drafting, editing, translating, summarizing, and improving emails, presentations, procedures, social media posts, knowledge articles, and other business content, provided the output is reviewed before use.
2. **Software Development Support:** AI may help developers explain code, suggest improvements, identify possible bugs, generate test cases, or support documentation, subject to code review and security validation.
3. **Productivity and Knowledge Assistance:** AI may be used to search, summarize, and organize information from approved company sources, support meetings, prepare action items, and improve day-to-day productivity.
4. **Data Analysis and Business Insights:** AI may support analysis of approved business data, identify patterns, create summaries, support forecasting, and assist decision-making, as long as results are validated by business owners.
5. **Customer and Employee Support:** AI-powered assistants or chatbots may help answer routine questions, support service processes, and improve response times, when implemented through approved tools and with appropriate monitoring.



6. **Process Automation:** AI may help automate repetitive or rule-based tasks, such as document processing, workflow support, reporting, and quality checks, where automation is approved and human oversight remains in place.
7. **Security, Compliance, and Risk Support:** AI may assist with reviewing logs, identifying anomalies, summarizing incidents, supporting compliance checks, and highlighting potential risks, without replacing professional judgment or formal approval processes.

General Principles for AI Usage:

1. All AI Systems should be approved for use by Ceragon's IT department, prior to any use thereof. For example, Microsoft Copilot has been approved by Ceragon for use by employees.
2. Avoid Sensitive or Confidential Data: It is prohibited to enter sensitive or confidential information into AI systems not approved in Ceragon and provided to you by Ceragon (such as Microsoft Copilot) to safeguard the privacy and security of our data. No sensitive or confidential information is allowed to be entered into other AI systems such as private accounts in ChatGPT etc.
3. No Decision Making: AI should not be solely relied upon for decision-making purposes. Final decisions should always involve human judgment, considering AI-generated output as one of the factors.

Additional Measures:

To support responsible and secure AI use, Ceragon will maintain clear controls, guidance, and oversight for approved AI tools. Employees are expected to follow these measures when using AI in their work:

- **Use approved AI tools only:** Employees must use AI systems that have been reviewed and approved by Ceragon's authorized functions, including IT, Legal, Security, or other relevant owners and provided by Ceragon (such as Microsoft Copilot). No sensitive or confidential information is allowed to be entered into other AI systems such as private accounts in ChatGPT etc.
- **Protect company and personal data:** With the exception of AI systems which are approved in Ceragon and provided to you by Ceragon (such as Copilot), Employees must not enter confidential, sensitive, personal, customer, partner, financial, security, legal, or non-public business information into AI tools unless explicitly approved.
- **Apply human review:** AI-generated output must be reviewed and validated before it is used, shared, or relied upon for business purposes.
- **Maintain accountability:** Employees remain responsible for their use of AI, including the accuracy, appropriateness, confidentiality, and compliance of any AI-assisted work.
- **Complete training and follow guidance:** Ceragon will provide awareness, guidance, and annual training to help employees understand approved uses, risks, and required precautions.
- **Monitor and improve:** Ceragon will periodically (semi annually) review AI tools, vendors, usage practices, and these guidelines to address legal, security, ethical, and operational risks.



Conclusion:

By following these guidelines, we aim to harness the benefits of AI while mitigating its associated risks. Responsible AI usage is essential for maintaining the integrity, security, and fairness of our work environment.