CyberEd in a Box Use of AI Policy

**Policy for Using AI in CyberEd in a Box**

This policy outlines the ethical and practical principles for the integration and use of AI within the CyberEd in a Box program. By adhering to these guidelines, educators, students, and institutions can ensure that AI systems are employed responsibly, transparently, and effectively, engendering trust and advancing the core values of cybersecurity education.

Stakeholders: CyberEd in a Box – Cyber 12 – Certificate in Risk Management, Faculty, Learning Management Team.

Core Values: Fairness, Accountability, Non-Maleficence, Transparency, and Trust

Issued: 1/29/2025

**1. Responsible AI Use**

AI technologies can enhance productivity and innovation, but their responsible use is essential to maintain integrity and trust.

**Policy Guidelines:**

* Advocate for transparency and accountability in all AI applications.
* Require full disclosure of AI involvement, verification of accuracy, and strict adherence to privacy laws such as GDPR.
* Expand awareness to include global frameworks like CCPA, China’s Cybersecurity Law, and the EU AI Act.

**Implementation:**

* Always disclose the use of AI tools in academic work, including text generation, coding assistance, or content analysis. Cite the AI system and its contributions.
* Verify AI-generated outputs for accuracy, bias, and errors. Human oversight is mandatory.
* Avoid uploading sensitive or personally identifiable information to AI systems. Follow all institutional and legal data protection guidelines.

**Example:** [AI Tool] partially generated this summary, and I have verified its accuracy and relevance.

**2. Enhancing Cybersecurity Learning**

AI enhances cybersecurity training, but it must complement—not replace—human judgment.

**Policy Guidelines:**

* Use AI as an assistant to human analysis, ensuring ethical oversight at every stage.
* Promote AI-driven hands-on simulations for ethical hacking, threat detection, and incident analysis.

**Implementation:**

* Design AI tools to support human-led analysis while leaving final decisions to trained professionals, and students training to be professionals.
* Integrate AI into simulations for ethical hacking and vulnerability assessments, documenting processes to demonstrate understanding.
* Use critical thinking to validate AI findings, ensuring adherence to ethical standards.

**Example:** I used an AI-based scanner to detect potential weaknesses but manually reviewed logs to confirm and understand each vulnerability.

**3. Academic Integrity**

Maintaining the highest standards of transparency and originality is essential when using AI in academic contexts.

**Policy Guidelines:**

* Explicitly prohibit plagiarism and mandate proper attribution of AI contributions.
* Enforce adherence to institutional conduct codes to ensure fair use of AI in education.

**Implementation:**

* Require proper citation of AI contributions in all academic work.
* Prohibit unauthorized assistance or uncredited AI-generated content.
* Emphasize originality by verifying and editing AI outputs.

**Example:** Sections of this policy draft were generated using [AI Tool]. The final document was edited for originality and accuracy by me.

**4. Ethical Decision-Making**

Incorporate ethical considerations into AI decision-making processes to prevent bias and ensure fairness.

**Policy Guidelines:**

* Regularly perform bias detection and audits to evaluate and audit your core, societal, cultural, and personal values as their pertain to your AI outputs.
* Employ algorithmic fairness tools like IBM AI Fairness 360 or SHAP to ensure inclusive and just outcomes. Examine industry tools from Google, Apple, Amazon, Microsoft that perform similar functions.

**Implementation:**

* Evaluate AI decisions critically, identifying and mitigating biases at every stage.
* Reflect on the broader impact of AI decisions on individuals, communities, and societal values.
* Develop ethical codes for AI systems that align with principles of autonomy, justice, accountability, and empathy.

**Example:** When developing an AI-based intrusion detection system, I ensured performance testing across diverse environments to address potential biases.

**5. Continuous Learning and Adaptation**

AI evolves rapidly, demanding ongoing education and ethical reflection.

**Policy Guidelines:**

* Encourage continuous learning on AI advancements, ethical frameworks, and emerging risks.
* Adapt ethical guidelines as AI capabilities expand, addressing challenges like deepfakes or automated decision-making.

**Implementation:**

* Participate in workshops, research, or study groups to stay informed about AI advancements.
* Reassess ethical policies regularly to align with industry standards and new developments.
* Seek mentorship or resources to fill knowledge gaps and strengthen accountability.

**Example:** Participated in a cybersecurity competition using new AI frameworks and reflected on how my ethical decision-making adapted to emerging challenges.

**6. Policy and Regulation Awareness**

Understand and adhere to legal and institutional frameworks for both essential and responsible AI use. If you find no policy, recommend the institution create one.

**Policy Guidelines:**

* Align AI applications with institutional and global standards.
* Use measurable metrics, such as transparency indices and trust ratings, to evaluate adherence to guidelines.

**Implementation:**

* Follow institutional policies on AI usage, including restrictions and citation requirements.
* Familiarize yourself with laws such as GDPR and regional equivalents to ensure compliance.
* Respect intellectual property by using and sharing AI-generated content responsibly.

**Example:** For a project processing real-world user data, I consulted GDPR regulations to ensure legal and ethical compliance. I uploaded the website and asked the AI to review my work.

**7. Role Definitions**

Clear roles ensure accountability and effective implementation of ethical AI principles.

**Policy Guidelines:**

* Define responsibilities for educators, students, policymakers, and institutions in AI governance.

**Roles:**

* **Educators:** Integrate ethical and technical AI training into curricula and develop hands-on learning opportunities.
* **Students:** Uphold academic integrity and critically evaluate AI-generated outputs.
* **Policymakers:** Develop and enforce ethical AI standards and establish oversight mechanisms.
* **Institutions:** Provide infrastructure for ethical AI use and support research into emerging challenges.

**Conclusion**

By adhering to these policies, stakeholders in CyberEd in a Box can ensure the ethical and responsible integration of AI in cybersecurity education. These guidelines empower students and educators to apply AI technologies effectively while maintaining trust, accountability, and a commitment to continuous learning.