Ethical Framework for AI usages and models

Establishing clear and transparent usage guidelines		Continuous scrutinizing and reviewing		Ensuring cyber-defenses and offenses work and comply with regulations

Users, Developers, Organizations

Ethical Framework Model:

This model will help showcase how certain principles can create a standardized ethical framework for AI models used by users, developers, and organizations. While there can be obviously more principles used to create an even stronger, better, and useful framework, there are many commonalities and overlaps each principle may have when they contribute to the final product.

Analysis of Ethical Framework Model:

This diagram represents an ethical framework for AI usages and models, structured like a stable building. At the very top, the roof symbolizes the goal of creating ethical, safe, and

responsible AI systems. This structured framework depends on several key pillars that uphold it, ensuring AI remains secure, transparent, and beneficial to everyone involved.

The first pillar, "Establishing clear and transparent usage guidelines", represents the principle of transparency. This means that developers and organizations should openly communicate how AI systems are designed, trained, and used [42]. Transparent usage guidelines prevent misuse, reduce misinformation, and make it easier for regulators, users, and even other developers to understand what the system is doing. Just as a building's first column provides crucial stability, transparency forms the beginning of public trust.

The second pillar, "Continuous scrutinizing and reviewing", is mostly about human oversight and accountability in action. AI systems cannot simply be set loose without constant evaluation. Regular auditing, monitoring, and testing ensure that these systems continue to act ethically and safely over time [26]. This principle reinforces that humans must stay in the loop, assessing biases, unintended outcomes, and security flaws. It's not just about fixing problems when they appear, but about creating a cycle of reflection and improvement that keeps AI aligned with equally important values.

The third pillar, "Ensuring cyber-defenses and offenses work and comply with regulations", highlights accountability and security. Ethical AI development doesn't stop at creating powerful tools; it includes protecting them [4]. By making sure that both defensive and offensive capabilities follow strict cybersecurity standards and legal frameworks, organizations demonstrate responsibility for how their AI is used. Safety isn't just technical; it's also moral. Following the regulations shows respect for user rights, data protection, and broader impacts.

All of these pillars rest upon the foundation of Users, Developers, and Organizations. Without the ones who design, use, and regulate these systems, even the strongest framework would collapse. This foundation emphasizes collaboration and shared responsibility: developers must design ethically, users must employ AI responsibly, and organizations must enforce standards that keep systems trustworthy. Transparency ensures clarity, human oversight maintains control, accountability guarantees compliance, and the human foundation keeps the system grounded in the real-world. When all these parts work together, they create not just an ethical framework, but a safe and secure AI ecosystem that serves society ethically and responsibly.