Executive One-Page Brief

Ten commitments for responsible AI adoption.

By David H. Wever

Artificial intelligence is reshaping how organizations operate, compete, hire, manage, communicate, and make decisions. It offers real promise, but it also introduces risks to trust, privacy, workforce stability, child safety, accountability, and public legitimacy.

Organizations that adopt AI responsibly should commit to the following ten standards.

1. Assign clear accountability

AI governance must have an accountable owner at the board or executive level. Responsibility should not disappear into technical teams, vendors, or vague committee language.

2. Know where AI is operating

Maintain an inventory of material AI systems across the organization, including what each system does, who owns it, what data it uses, and who may be affected.

3. Classify systems by risk

Not all AI carries the same stakes. Low-risk tools require lighter oversight. Systems affecting jobs, pay, education, health, access, or legal standing require stricter governance.

4. Review before deploying

No high-risk AI system should be deployed without documented review of purpose, benefits, risks, affected populations, privacy issues, workforce impact, failure modes, and human oversight.

5. Keep humans responsible for consequential decisions

AI may assist decisions, but final responsibility for major employment, access, financial, health, educational, or legal outcomes must remain with accountable human beings.

6. Communicate honestly with workers and users

People should know when AI materially affects how they are evaluated, monitored, ranked, served, or decided upon. Disclosure should be clear, not buried in legal fog.

7. Prepare for workforce impact

Before major automation, assess job redesign, possible displacement, retraining, redeployment, and transition support. Responsible adoption includes carrying people through change, not merely extracting labor savings.

8. Protect privacy and sensitive data

Use only data reasonably necessary for legitimate purposes. Apply heightened protection to health, mental health, education, finance, biometric, location, and child-related data.

9. Protect children and vulnerable users

Do not design AI systems that exploit emotional dependency, distress, developmental immaturity, loneliness, or crisis states for engagement, spending, or influence.

10. Report, review, and improve

Maintain incident response procedures, periodically reassess material systems, and publish a basic annual transparency statement describing major AI uses, governance, harms observed, and corrective actions taken.

Bottom line

The question is not whether an organization can adopt AI. The real question is whether it can do so without degrading trust, dignity, accountability, and human judgment. Organizations that deserve long-term trust in the AI age will be those that govern before harm, not apologize after it.