Carmen Stan

Ethical technology policies do not replace general compliance or business ethics, but they should all connect in some way. Just as your approach to cybersecurity hasn't taken the place of your company's more general privacy policies, your ethical technology approach should complement your overall approach to ethics and serve as its logical extension in the digital realm. Some companies are expanding the mission of existing ethics, learning, and inclusion to include ethical technology, while maintaining separate technology ethics programs. Doing so helps keep technology ethics top of mind across the organization and encourages executives to consider the distinctions between technology-related ethical issues and broader corporate and professional ethics concerns.

In pursuit of trust

In the digital era, trust is a complex issue fraught with myriad existential threats to the enterprise. And while disruptive technologies are often viewed as vehicles for exponential growth, tech alone can't build long-term trust. For this reason, leading organizations are taking a 360-degree approach to maintain the high level of trust their stakeholders expect.

In technology we trust

Artificial intelligence (AI), machine learning, blockchain, digital reality, and other emerging technologies are integrating into our everyday lives more quickly and deeply than ever. How can businesses create trust with the technologies their customers, partners, and employees are using?

Encode your company's values. With technology ingrained in the business and machine learning driving business decisions and actions, an organization's values should be encoded and measured within its technology solutions. Digital systems can be designed to reduce bias and enable organizations to operate in line with their principles.6 For instance, a city government worked with policy institutes to develop an algorithm toolkit intended to identify ways to minimize unintended harm to constituents by limiting biases in the criminal justice system and other institutions.

Safeguards can promote stakeholder welfare by helping prevent users from engaging with technology in unhealthy or irresponsible ways. Examples include a company that imposes time and spending limits on habit-forming games, a content aggregator that prompts users to be skeptical about the veracity of crowdsourced information, and cloud computing providers that automatically issue alerts before customers go over budget.

Build a strong data foundation. Without methodically and consistently tracking what data you have, where it lives, and who can access it, you cannot create an environment of trust. A strong data foundation unifies stakeholders around a single vision of data accountability and delivers on secure technology that supports effective data management. Leaders should aim to give stakeholders some control over how their data will be used and delete data on demand unless it's necessary to keep it for legal or regulatory purposes. Cyber defenses represent your commitment to protect your customers, employees, and business partners from those who do not share their

values—or yours. Cyber risk strategy should be built and managed from the ground up, embedded in the business mindset, strategy, and policies, not only within IT. Business leaders can collaborate with IT to create a comprehensive cyber risk strategy—encompassing security, privacy, integrity, and confidentiality—to help build stakeholder trust and drive competitive advantage. This requires considering the organization's risk tolerance, identifying the most vulnerable gaps as well as the most valuable data and systems, then devising plans for mitigation and recovery.

What's in a process

A strong foundation for ethical technology and trust will be shaped by the principles of an organization's leaders and realized in business processes.

Respect stakeholder privacy. One of technology disruption's most overarching effects has been to accelerate the collection, analysis, and dissemination of information. Not so long ago, the transactional details of our lives were kept in physical file cabinets, pulled out and referenced for specific needs. Today, systems routinely collect these details and combine them with our purchase histories, posts on social media, online searches, and even the route we drive to work each day. If consumers have reason to believe their data is being used in ways they don't approve of, reactions can include calls for boycotts, public inquiries, and even severe penalties under strict regulations, such as the European Union's General Data Protection Regulation.

Companies should create data privacy policies that build, rather than erode, public trust.