

**AI Principles Outline**  
**WASHI**  
**26 March 2021**

**Our Approach**

Artificial Intelligence (AI) is a transformative tool with the potential to unlock new commercial opportunities and higher levels of human potential. As a global leader in this rapidly evolving field, Hitachi is committed to ensuring that AI systems are developed and deployed responsibly.

AI systems should be trustworthy, explainable and free from algorithmic bias. And while the Federal Government can accelerate the widespread adoption of responsible AI by creating an open research environment and increasing R&D investment, it is also incumbent on cutting-edge technology companies like Hitachi to provide policymakers with industry insight into areas that may warrant closer oversight.

**Recommendations for an Innovative AI Ecosystem**

The nation's AI policy framework should remain flexible and drive innovation, promote transparency and trustworthiness, and encourage greater inclusivity and accessibility.

**Prioritize Open and Accessible Government Data:** Robust and reliable data sets are needed to train trustworthy AI systems at scale. As such, the Federal Government should prioritize the development and expeditious release of public datasets in machine-readable formats that are commonly structured and tagged, easily discoverable, and protect personally identifiable information (PII). These open and annotated datasets should prize usability by clearly stating the characteristics of the data included (e.g. source, demographics, etc.).

**Encourage International Standards:** The Federal Government should encourage the development of global AI standards that are consensus-based, voluntary, and industry-led. U.S. public and private sector representation is needed on recognized international standards-setting bodies to ensure that AI standards are drafted in a fair and open manner, promote innovation, and reward ethical deployment. Federal Agencies should also cooperate with counterparts from like-minded democracies to determine IT standards integral to the advancement of AI (e.g. cloud computing, cyber security, Internet of Things (IoT), etc.).

**Increase Research and Development Investment:** Increased investment in basic and foundational research is needed to advance AI and better understand how AI can be utilized to revolutionize other fields. Towards that end, the Federal Government should expand the number of grants from the National Science Foundation (NSF) and Defense Advanced Research Projects Agency (DARPA) and allow for multi-year competitive grants. Research into high-risk initiatives and areas where the market is undefined should also be encouraged.

**Expand Federal AI Adoption:** The U.S. Government should accelerate AI adoption across Federal Agencies and update related IT systems. Agency advisory boards should be established to effectively identify governmental processes that can be automated or made more accurate and efficient through AI. Additionally, these advisory boards should monitor AI implementation to promote accountability in the system's use, and publicly report any barriers to widespread adoption.

**Promote Trustworthiness and Foster Public Trust:** The widespread development and deployment of responsible AI is contingent upon public trust in its creation and application, as well as the adoption of

internationally recognized definitions and standards for “Trustworthy AI”’s characteristics: accuracy, reliability, robustness, security, explainability, safety, privacy, and ethics. Given the rapid pace of technological advancement, we urge the Federal Government to continue collaborating with industry to better understand how “trustworthiness” is evolving and ensure that decisions taken by global standards setting bodies reflect that evolution. Finally, given the general public’s concerns around disinformation, algorithmic bias, and job displacement, the U.S Government should partner with industry, academia and other private sector stakeholders to articulate how AI can be utilized for the public good.

**Invest In and Incentivize A Workforce for the Future:** AI promises to significantly transform the labor market, and the Federal Government and industry leaders should work together to ensure the nation’s transition to an AI economy benefits America’s workforce. The U.S. Government should pursue legislative action to create new pathways for vocational and technical skills training, increase tax credits for employee reskilling initiatives (indexed to inflation), and expand R&D tax credits so that advanced computing training programs are covered. Furthermore, the U.S. should develop enhanced STEM education programs to give young Americans of all backgrounds the technical tools to compete in a global, digital economy.

**Utilize Test Beds:** The U.S. Government should encourage the development of AI test beds in which stakeholders from the public and private sectors can jointly evaluate, tune, and validate novel algorithms and AI solutions.

**Recognize Existing Regulatory Frameworks:** AI-enabled solutions span sectors already subject to laws and regulatory frameworks. As such, the U.S. Government should maintain a sector-specific approach and seek industry’s help in identifying regulatory gaps or frameworks that need updating or require greater scrutiny.

**Maintain a Risk-Based Approach:** The U.S. Government should continue cultivating an innovative AI ecosystem by maintaining a flexible, risk-based approach to AI policy formulation. Towards that end, the Administration should issue guidance on acceptable risk-mitigation, safe harbors, and protocols for developing and deploying AI algorithms, solutions, and technologies responsibly. The U.S. Government should also encourage the development of regulatory and non-regulatory standards that offer greater transparency around AI risk, detailing the scope of the industrial problem domain, source datasets, the target solution, and the appropriate level of human judgement or supervision required to safely and effectively utilize the solution.

**Privacy and Data Protection:** The collection, retention, and processing of data is central to training AI algorithms, but AI advancement should not come at the expense of consumer privacy violations or personal data exploitation. To promote data-driven innovation and best protect against evolving privacy vulnerabilities, policymakers should avoid rigid regulations and work in concert with private sector stakeholders to advise on industry-set guidelines.

### **An Industrial AI Leader**

Industrial AI is the application of Artificial Intelligence and Machine Learning (AI & ML) to exploit opportunities and tackle challenges presented by Industry 4.0. Hitachi has successfully developed AI-based methods in the following areas (Maintenance and Repair Analytics; Operation Optimization; Quality Enhancement) and applied them in various verticals: manufacturing, mining, mobility, energy, and healthcare.

### **Recommendations for the Industrial AI Space**

As a global Industrial AI leader, Hitachi possesses unique insight into less-explored AI areas (automation, data and video analytics, robotics, etc.) and emerging applications that warrant greater attention and engagement from U.S policymakers.

**Cobotics:** The advent of collaborative robotics, or “cobotics,” promises to transfer dirty, dull, and even dangerous tasks carried out by humans to AI-enabled robots working in close proximity to and in collaboration with human co-workers on the connected factory or warehouse floor. Cobots, with the ability to learn and adapt to new tasks while safely operating alongside humans, can measurably improve workers’ efficiency, safety, and longevity. But, as cobots are increasingly introduced across the supply chain, policymakers need to consider workplace safety regulations and data privacy concerns in a new light.

**Data Model Security:** Future security threats will likely include cyber attacks that corrupt Machine Learning data models for forecasting. If, for example, a malign actor fed an energy consumption forecasting model bad data, that actor could wreak financial havoc on the energy futures market. Data model security deserves urgent attention by policymakers and industry leaders, alike.

**Liability Insurance:** The existing legal framework is designed to regulate human behavior—not algorithms—even as increasingly sophisticated AI-enabled products and systems are making decisions without human input. Policymakers should review regulatory options for emerging AI liability insurance models.