Report

Organization: **Fujitsu**

https://www.fujitsu.com/global/about/research/technology/ai/initiatives/index.html

Publication date: Apr 22, 2025, 03:17 PM PDT

Reporting period: 2025

Section 1 - Risk identification and evaluation

a. How does your organization define and/or classify different types of risks related to AI, such as unreasonable risks?

Fujitsu is focusing on ethical biases and vulnerability risks, and as it actively promotes research and technological development initiatives, it is advancing the definition and classification of AI-related risks.Specifically, Fujitsu's "AI Ethics Risk Comprehension Technology", which helps understand AI-caused incidents according to different scenarios, defines and classifies AI-related risks in accordance with the principles and requirements of the European Ethics Guidelines for Trustworthy AI.

"AI Ethics Risk Comprehension Technology"

https://www.fujitsu.com/global/about/research/article/202304-aiethics-risk-comprehension.html

b. What practices does your organization use to identify and evaluate risks such as vulnerabilities, incidents, emerging risks and misuse, throughout the AI lifecycle?

Fujitsu implements the following practices to identify and assess the aforementioned risks throughout the AI lifecycle.

First, we have "AI Ethics Risk Comprehension Technology," which helps us understand AI-caused incidents within the specific contexts in which they occur. This technology enables detailed analysis of AI usage and allows for the early detection of ethical biases and potential problems.

Next, we have the "LLM Vulnerability Scanner." This scanner is equipped with multi-AI agent security technology that supports proactive measures against vulnerabilities and emerging threats, enabling continuous risk monitoring not only before AI model deployment but also during the operational phase.

"AI Ethics Risk Comprehension Technology"

https://www.fujitsu.com/global/about/research/article/202304-aiethics-risk-comprehension.html

"LLM Vulnerability Scanner"

https://www.fujitsu.com/global/about/resources/news/press-releases/2024/1212-01.html

c. Describe how your organization conducts testing (e.g., red-teaming) to evaluate the model's/system's fitness for moving beyond the development stage?

Fujitsu aims to provide a safe and reliable AI system by rigorously evaluating the compatibility of models and systems through the following tests included in the Generated AI Security Enhancement Technology developed in collaboration with Ben Gurion University.

First, the LLM Vulnerability Scanner automatically checks security resistance with high completeness. It addresses more than 7,700 industry-leading, up-to-date vulnerabilities for a variety of vulnerabilities known to exist in Generative AI. This helps identify potential vulnerabilities that are often overlooked during development and improves the overall robustness of the system.

Next is the LLM Guardrail, which automatically defends and mitigates attacks. It validates that the model does not produce inappropriate responses or harmful content, based on attack scenarios that assume a real production environment. In this way, through attack simulations such as red teaming, the behavior of the model is analyzed in detail to ensure safety.

“Fujitsu develops world’s first multi-AI agent security technology to protect against vulnerabilities and new threats, Collaboration among AI agents specialized in security with skills and knowledges of attacks and protection”

https://www.fujitsu.com/global/about/resources/news/press-releases/2024/1212-01.html

d. Does your organization use incident reports, including reports shared by other organizations, to help identify risks?

Yes

e. Are quantitative and/or qualitative risk evaluation metrics used and if yes, with what caveats? Does your organization make vulnerability and incident reporting mechanisms accessible to a diverse set of stakeholders? Does your organization have incentive programs for the responsible disclosure of risks, incidents and vulnerabilities?

Fujitsu's internal rules for information security stipulate that employees must report risks and incidents. Fujitsu has also established group-wide risk management rules for reporting incidents. In addition, Fujitsu is open to receive voices from external security researchers and Security information provider about product vulnerabilities.

https://www.fujitsu.com/global/about/csr/security/

https://www.fujitsu.com/global/about/csr/riskmanagement/

f. Is external independent expertise leveraged for the identification, assessment, and evaluation of risks and if yes, how? Does your organization have mechanisms to receive reports of risks, incidents or vulnerabilities by third parties?

Fujitsu leverages the knowledge of external experts, such as AISI, to identify and assess risks.

As a mechanism for receiving reports of risks, incidents, or vulnerabilities from third parties, we have an inquiry form for products and services on our website. We also respond to inquiries from the media, investors, and the general public through our reporting hotline.

https://www.fujitsu.com/global/about/csr/compliance/

g. Does your organization contribute to the development of and/or use international technical standards or best practices for the identification, assessment, and evaluation of risks?

Fujitsu contributes to the establishment of international standards and best practices, with notable contributions including:

i. Two members appointed to the AI4People Institute Scientific Committee (from FY23 to the present), where they contributed to the drafting and publication of white papers.

ii. Three members acting as members of *CEN* and CENELEC's JTC 21 (Artificial Intelligence) committee. One member also serving as an editor for ISO/IEC JTC1 SC42, contributing to the development of key standards such as ISO 24030 (AI Use Cases), ISO 42001 (AI Risk Management Systems), and others.

iii.Fujitsu has provided the Italy-based startup with AI Trust technologies, consisting of five core tools from its Fujitsu Kozuchi AI service. These technologies will enable AKOS's AI governance platform AKOS HUB, to offer EU AI Act compliance, risk management and general AI governance services and solutions to enterprise customers.

https://www.fujitsu.com/global/about/resources/news/press-releases/2025/0418-01.html

h. How does your organization collaborate with relevant stakeholders across sectors to assess and adopt risk mitigation measures to address risks, in particular systemic risks?

Fujitsu is incorporating controls, including AI risk assessments, into its global-group-wide quality assurance processes described in the next section as part of its AI risk mitigation measures, and cooperate with relevant parties across divisions.

Section 2 - Risk management and information security

a. What steps does your organization take to address risks and vulnerabilities across the AI lifecycle?

Fujitsu has established rules at both the group-wide level and the country/product/service level, and we are committed to following procedures in accordance with these rules.

Specifically, we have formulated the "Fujitsu Global Quality Guideline" for all products, including all systems, services, and software, including AI that we develop and provide.

Under this guideline, Fujitsu employees are required to develop regulations and standards tailored to the characteristics of countries, products, and services, customer requirements, and laws and regulations.

Furthermore, we recognize risks related to AI as quality issues for Fujitsu, and we evaluate risks and thoroughly implement countermeasures by deploying a common platform for evaluating quality risks and a quality assurance process that supports service delivery throughout the Fujitsu Group.

"Fujitsu Global Quality Guideline"

https://www.fujitsu.com/global/about/csr/society/quality/

b. How do testing measures inform actions to address identified risks?

Fujitsu conducts "AI Risk Assessments" to identify potential risks in projects and consider countermeasures. The information obtained from this assessment process is directly used to formulate concrete action plans for risk mitigation.

Specifically, in the "AI Risk Assessment", projects are recommended to implement measures using "Fujitsu AI Ethics for Fairness" for systems or datasets where fairness risks exist. This allows for easy verification and improvement of the fairness of AI models.

"Fujitsu AI Ethics for Fairness"

https://en-documents.research.global.fujitsu.com/ai-ethics-fairness/

c. When does testing take place in secure environments, if at all, and if it does, how?

Fujitsu emphasizes testing in a secure environment before delivery to ensure the safety and reliability of its AI systems.

In particular, for fairness verification of AI models, we provide a customer-dedicated environment on our AI technology publishing product service, “Fujitsu Kozuchi”, and conduct verification using "Fujitsu AI Ethics for Fairness", which facilitates the verification and improvement of AI model fairness. This allows customers to analyze their data in a secure environment and evaluate the fairness of their AI models.

“Fujitsu Kozuchi”

https://www.fujitsu.com/global/services/kozuchi/

"Fujitsu AI Ethics for Fairness"

https://en-documents.research.global.fujitsu.com/ai-ethics-fairness/

d. How does your organization promote data quality and mitigate risks of harmful bias, including in training and data collection processes?

Fujitsu is actively working to promote data quality and mitigate the risk of harmful biases, including training and data collection processes, to ensure the quality of AI systems. As a specific measure, we recommend that projects implement countermeasures using "Fujitsu AI Ethics for Fairness" in "AI Risk Assessment," which facilitates the verification and improvement of AI model fairness.

"Fujitsu AI Ethics for Fairness"

https://en-documents.research.global.fujitsu.com/ai-ethics-fairness/

e. How does your organization protect intellectual property, including copyright-protected content?

Fujitsu currently instructs AI system development project members to clarify the scope and rights of intellectual property and reach agreement among stakeholders through "AI Risk Assessments." This ensures that awareness of intellectual property is shared from the project's initial stages, reducing the risk of infringement. We are promoting literacy improvement by formulating and publicly releasing AI Ethics education materials including e-learning and guidelines on AI ethics and intellectual property, both internally and externally.

f. How does your organization protect privacy? How does your organization guard against systems divulging confidential or sensitive data?

Fujitsu recognizes privacy protection as one of its highest priorities and takes strict measures to meet the trust of our customers and society.

Currently, Fujitsu has implemented the following initiatives:

Clarification and Agreement on Personal Information Protection in "AI Risk Assessments": At the start of projects, we instruct employees to clarify the scope of responsibility and compliance matters related to personal information protection and reach an agreement. This raises awareness of personal information protection and ensures proper handling.

Analysis and Countermeasures for the Risk of Training Data Leakage due to AI Security Attacks in "AI Risk Assessments": We recognize the risk of training data leakage due to AI security attacks and instruct projects to analyze and implement countermeasures. This allows us to assess the risk of data leakage and strive to protect confidential data by taking appropriate security measures.

g. How does your organization implement AI-specific information security practices pertaining to operational and cyber/physical security?

- **i. How does your organization assess cybersecurity risks and implement policies to enhance the cybersecurity of advanced AI systems?**
- **ii. How does your organization protect against security risks the most valuable IP and trade secrets, for example by limiting access to proprietary and unreleased model weights? What measures are in place to ensure the storage of and work with model weights, algorithms, servers, datasets, or other relevant elements are managed in an appropriately secure environment, with limited access controls in place?**
- **iii. What is your organization's vulnerability management process? Does your organization take actions to address identified risks and vulnerabilities, including in collaboration with other stakeholders?**
- **iv. How often are security measures reviewed?**
- **v. Does your organization have an insider threat detection program?**

Fujitsu implements information security practices through a multi-layered approach, including establishing standards based on external organizations' standards. By taking comprehensive measures, we ensure the security of information systems, including AI systems.

i) We have established the "Fujitsu Group Information Security Countermeasures Standards" based on external organizations' standards such as "NIST CSF" and "ISO/IEC 27000 series," and use them in risk assessments conducted during system development and operation.

ii) We classify all confidential information handled within Fujitsu according to its importance and scope of disclosure. Based on this classification, we designate storage locations and implement access controls and encryption measures.

Furthermore, the development of information systems, including AI systems, is conducted on the Fujitsu Developers Platform, a secure development platform common to the Fujitsu Group, with enhanced authentication, access control, and monitoring capabilities."

iii) Through xSIRT activities we collect vulnerability information from related organizations At the same time, IT asset information of information systems, including AI systems, is managed in a database. The collected vulnerability information and IT asset information are compared to identify items that need to be addressed, and the completion of the countermeasures is managed through a ticketing system.

iv) We require a review of the security measures status of information systems, including AI systems, at least once a year, and manage its implementation.

v) We require and manage the implementation of monitoring for privileged use and suspicious behavior, etc., for information systems, including AI systems.

"Fujitsu Group Information Security Countermeasures Standards"

https://www.fujitsu.com/global/about/csr/security/

h. How does your organization address vulnerabilities, incidents, emerging risks?

Fujitsu recognizes the potential risks of AI as part of information security and is implementing the following initiatives:

Regular Security Risk Assessments and Vulnerability Scans: We conduct regular security risk assessments for information systems, including AI systems, to identify potential vulnerabilities. We also continuously monitor the status of countermeasures against known vulnerabilities through regular system vulnerability scans.

Incident Response and Deployment of Risk Countermeasures: We have established a system to respond quickly to the occurrence of security incidents or the detection of new risks. In the event of an incident, we promptly investigate the cause, identify the scope of impact, and perform recovery work, as well as implement measures to prevent recurrence. For new risks, we plan measures to address them and deploy them throughout the company, thereby improving the security level of the entire organization.

In addition to the above information security measures, Fujitsu is taking the following initiatives to address AI-specific issues:

Review of all AI Business Negotiation: We have established and implemented a review process to reduce risks from an ethical perspective, as well as a risk assessment from the perspectives of AI quality, security, and ethics, and are reducing risks from multiple perspectives.

Awareness on AI Ethics: We raise knowledge and awareness of AI for AI developers, providers, and users and promote their appropriate use.

Section 3 - Transparency reporting on advanced AI systems

a. Does your organization publish clear and understandable reports and/or technical documentation related to the capabilities, limitations, and domains of appropriate and inappropriate use of advanced AI systems?

- **i. How often are such reports usually updated?**
- **ii. How are new significant releases reflected in such reports?**
- **iii. Which of the following information is included in your organization's publicly available documentation: details and results of the evaluations conducted for potential safety, security, and societal risks including risks to the enjoyment of human rights; assessments of the model's or system's effects and risks to safety and society (such as those related to harmful bias, discrimination, threats to protection of privacy or personal data, fairness); results of red-teaming or other testing conducted to evaluate the model's/system's fitness for moving beyond the development stage; capacities of a model/system and significant limitations in performance with implications for appropriate use domains; other technical documentation and instructions for use if relevant.**

Fujitsu's IT systems and services are primarily offered on a B-to-B basis to companies and administrative organizations. In the contract process with our customers, we ensure transparency and accountability by clarifying the following elements according to the customer's required level:

Data Information:

Description of the datasets used for training (type, size, collection method, etc.)

Evaluation of data quality and biases

Efforts related to data privacy protection (anonymization, differential privacy, etc.)

Model Information:

Type of AI model, learning method, evaluation metrics, and model performance evaluation results (accuracy, precision, recall, etc.)

Information on the interpretability of the model (importance of features, etc.)

Evaluation of model vulnerabilities

Ethical Considerations:

Potential ethical issues that the AI solution may bring (e.g., discrimination, bias, privacy infringement)

Measures to mitigate ethical risks (fairness evaluation, improvement of explainability, etc.)

Compliance with internal regulations and guidelines on AI ethics

Operation and Monitoring System:

Operation and monitoring system of the AI solution

Response process in case of errors

Efforts for continuous improvement

Responsibility System:

Clear indication of the person responsible for the development and operation of the AI solution

Contact point for inquiries from customers

b. How does your organization share information with a diverse set of stakeholders (other organizations, governments, civil society and academia, etc.) regarding the outcome of evaluations of risks and impacts related to an advanced AI system?

Fujitsu has the following initiatives to share information with diverse stakeholders (other organizations, governments, civil society, academia, etc.) regarding the results of assessments of risks and impacts associated with advanced AI systems:

Formulation and publication of the Fujitsu Group AI Commitment (March 2019) , holding of the External Advisory Committee on AI Ethics based on it, and sharing of its discussions with the Board of Directors to ensure transparency for shareholders.

Holding shareholder IR, media briefings, and technology strategy briefings twice a year

Actively participating in academia and industry organizations related to AI (e.g., AI4People Institute, GPAI, SC42, etc.) and contributing to the development of best practices and the resolution of ethical issues for the industry as a whole.

“Fujitsu Group AI Commitment”

https://global.fujitsu/en-global/technology/key-technologies/ai/aiethics/governance

c. Does your organization disclose privacy policies addressing the use of personal data, user prompts, and/or the outputs of advanced AI systems?

At Fujitsu, in order to appropriately protect confidential information of other companies, including personal information, as well as our own confidential information, we are implementing initiatives to protect information by operating an information protection management system that includes the use of personal data in AI systems. This involves setting up appropriate management tailored to the circumstances of our customers and business partners.

Under the principle of respecting the personality of individuals, Fujitsu deeply recognizes that appropriately handling personal information is a social responsibility as a company, and we promise to protect and respect personal information based on the following items.

“Fujitsu Integrated Report 2024” p.86 Information management

https://global.fujitsu/en-global/about/integrated-report

d. Does your organization provide information about the sources of data used for the training of advanced AI systems, as appropriate, including information related to the sourcing of data annotation and enrichment?

To enhance the transparency and reliability of AI systems, Fujitsu provides data source information as appropriate and fulfills accountability regarding AI-specific risks through the following initiatives within the contractual relationship with customers:

Data Source Recording: We record the types of data, collection methods, and purposes of use for the data used to train AI systems and establish a management system to disclose this information as needed.

Transparency of Data Annotation and Enrichment: When performing data annotation or enrichment, we record the process, personnel in charge, and tools used to ensure transparency.

Data Privacy Protection: When handling data containing personal information, we comply with relevant laws and regulations (such as the Personal Information Protection Act) and take appropriate security measures.

Data Bias Reduction: We recognize biases in datasets and strive to reduce them. We consider using diverse data sources and technical methods for bias removal as needed.

e. Does your organization demonstrate transparency related to advanced AI systems through any other methods?

Fujitsu strives to improve transparency by sharing information on the development and operation of AI systems with stakeholders (customers, society, researchers, etc.) and collecting feedback.

Section 4 - Organizational governance, incident management and transparency

a. How has AI risk management been embedded in your organization governance framework? When and under what circumstances are policies updated?

Fujitsu recognizes AI risks as important management issues for the entire organization and promotes the responsible development and use of AI as part of corporate governance and sustainability initiatives. Considering the rapid pace of new advancements in AI technology and the corresponding changes in benefits and potential risks, we appropriately review our approach as needed, taking into account AI policies and rule-making both overseas and in Japan, as well as customer industry trends.

b. Are relevant staff trained on your organization’s governance policies and risk management practices? If so, how?

At Fujitsu, AI-related staff receive training on Fujitsu's AI governance policies and risk management practices as follows:

AI Ethics Initiatives: We formulated and published the "Fujitsu Group AI Commitment," clearly outlining our basic philosophy on AI ethics. We also released the "AI Ethics Course" for employees to promote knowledge and raise awareness of AI ethics.

Integration into Company-Wide Quality Assurance Processes: We defined criteria from the perspective of AI ethics ("AI Ethics Check") and AI risk assessment ("AI Risk Assessment") within our quality assurance processes and deployed them in Japan. This enables us to determine the feasibility of business promotion from an ethical perspective and extract and hedge AI-specific risks from the perspectives of quality, security, and ethics from the early stages of AI development and implementation.

Awareness and Response to Laws, Regulations, and Guidelines: We established an AI Governance HQ (Headquarters) within the company and, for example, disseminated information on responses to prohibited AI under the EU AI Act to the entire company through internal information sharing tools. This enables us to quickly grasp global regulatory trends and build a compliance system.

“Fujitsu AI Ethics Governance”

https://global.fujitsu/en-global/technology/key-technologies/ai/aiethics/governance

c. Does your organization communicate its risk management policies and practices with users and/or the public? If so, how?

Fujitsu discloses its initiatives on its official website.

d. Are steps taken to address reported incidents documented and maintained internally? If so, how?

Fujitsu's IT system quality governance, including AI systems, is working to prevent the recurrence of serious incidents and strengthen the quality of products and services under the CQO (Chief Quality Officer). Furthermore, as an AI governance measure, we are utilizing the current group-wide risk management framework and implementing an appropriate escalation mechanism that incorporates the characteristics of AI.

“Fujitsu Quality Initiatives”

https://www.fujitsu.com/global/about/csr/society/quality/

e. How does your organization share relevant information about vulnerabilities, incidents, emerging risks, and misuse with others?

Fujitsu strives to ensure accountability to customers by disseminating relevant information internally regarding AI risks through employee websites and other channels. Our company also discloses vulnerabilities in our products based on the company's established response processes and disclosure policies.

・Information and alerts regarding AI legal compliance (e.g., addressing prohibited AI under the EU AI Act) and AI-specific risks are communicated to all internal organizations through a dedicated company-wide website.

f. Does your organization share information, as appropriate, with relevant other stakeholders regarding advanced AI system incidents? If so, how? Does your organization share and report incident-related information publicly?

Fujitsu has already established a mechanism within the group to share incident information not only for AI but also for IT systems in general and provides explanations and reports to government authorities as necessary. In addition, we implement appropriate information sharing by publishing related information such as incident responses on our website.

https://www.fujitsu.com/jp/support/security/psirtpolicy/

https://www.fujitsu.com/global/about/csr/security/

g. How does your organization share research and best practices on addressing or managing risk?

Fujitsu shares research and best practices on addressing and managing AI risks internally and externally through the following methods:

<External>

For the purpose of promoting the appropriate adoption of AI, we provide best practices through collaboration with industry organizations, governments, technology strategy meetings, and other multi-stakeholders.

<Internal>

Regular Reporting and Sharing Between Departments: The control department regularly reports and shares information on addressing and managing risks and practices in "AI Risk Assessments" with related departments, including the research and development department. This ensures that the entire organization shares the latest information on risk response and enhances knowledge.

Sharing with Business Departments and Each Region: Following the above reporting and sharing, information is also shared with business groups (BGs) and regions (Rs). This supports the construction of risk management systems that take into account business strategies and regional characteristics.

h. Does your organization use international technical standards or best practices for AI risk management and governance policies?

Fujitsu utilizes the following international technical standards or best practices in its AI risk management and governance policies:

Use of International Standards: In "AI Risk Assessments," we refer to international standards such as ISO and ALTAI (AI High-Level Expert Group's Assessment List for Trustworthy AI) to conduct AI risk analysis. This enables us to achieve risk assessments that align with international standards.

Enhancement with Guidelines: Based on ALTAI, we strengthen risk assessments using the Machine Learning Quality Management Guidelines for quality and the Machine Learning System Security Guidelines for security. This allows us to take concrete measures to further improve the quality and security of AI systems.

Continuous Monitoring of International Standards: We plan to respond to AI governance measures while monitoring trends in international standards. To respond to rapidly changing AI technologies and social conditions, we continuously collect the latest information and incorporate optimal standards to continuously improve our AI risk management and governance policies.

Section 5 - Content authentication & provenance mechanisms

a. What mechanisms, if any, does your organization put in place to allow users, where possible and appropriate, to know when they are interacting with an advanced AI system developed by your organization?

Fujitsu's IT systems and services are primarily offered on a B-to-B basis to companies and administrative organizations. In the contract process with our customers, we fulfill our accountability to them regarding the use of advanced AI systems in our IT systems and services.

---

b. Does your organization use content provenance detection, labeling or watermarking mechanisms that enable users to identify content generated by advanced AI systems? If yes, how? Does your organization use international technical standards or best practices when developing or implementing content provenance?

Currently, Fujitsu is not using these.

Furthermore, Fujitsu is promoting research and development and implementation of technologies to enable users to identify content generated by advanced AI systems. For example, we are undertaking a Japanese government project, in collaboration with industry and academia, aimed at developing and implementing technologies to combat disinformation, and we are promoting activities aimed at standardization.

In the first place, while the distribution of disinformation via Generative AI and synthetic content on the internet has become a major social problem, technologies to detect intentional disinformation (text, images, audio, and video) using deepfakes have been individually considered. However, these are only partial solutions to the problem of disinformation and do not provide a fundamental solution. In order to accurately detect disinformation, it is essential to have a mechanism that not only detects it using these individual technologies, but also collects and integrates various related peripheral information for comprehensive verification. To address this challenge, Fujitsu is collaborating with industry-academia organizations to begin research and development of various technologies and is also working to build the world's first disinformation countermeasures platform that comprehensively integrates everything from disinformation detection to evidence gathering, analysis, and evaluation.

“Fujitsu to combat fake news in collaboration with leading Japanese organizations Fujitsu-led industry-academia consortium commences development of world’s first disinformation countermeasure platform”

https://www.fujitsu.com/global/about/resources/news/press-releases/2024/1016-01.html

---

Section 6 - Research & investment to advance AI safety & mitigate societal risks

a. How does your organization advance research and investment related to the following: security, safety, bias and disinformation, fairness, explainability and interpretability, transparency, robustness, and/or trustworthiness of advanced AI systems?

Fujitsu has invested greatly in research and development of technologies that can promote fairness and security while removing bias and misinformation in AI systems. As a result of R&D activities, Fujitsu:

•contributed to the scientific community by participating in scientific conferences and publishing academic articles

•partnered with the Linux Foundation to make a fairness technological solution developed by Fujitsu Research open source

https://www.fujitsu.com/global/about/resources/news/press-releases/2023/0915-01.html

•published freely available white papers, including a white paper on the ethics impact assessment approach developed by Fujitsu

https://global.fujitsu/en-global/technology/key-technologies/ai/aiethics/technology

https://www.fujitsu.com/global/about/resources/news/press-releases/2022/0221-01.html

•successfully applied to include Fujitsu AI ethics technologies into the OCED GPAI Catalogue of Tools & Metrics for Trustworthy AI

https://oecd.ai/en/catalogue/tools?terms=fujitsu&page=1

---

b. How does your organization collaborate on and invest in research to advance the state of content authentication and provenance?

In 2024 Fujitsu was selected by Japan's New Energy and Industrial Technology Development Organization ("NEDO"), through NEDO's public request for proposals to develop technologies to analyze disinformation. Fujitsu is conducting R&D to determine the authenticity of information and detect and evaluate disinformation.

"Fujitsu chosen to help solving social issues caused by fake news Chosen in the Key and Advanced Technology R&D through Cross Community Collaboration Program"

https://www.fujitsu.com/global/about/resources/news/press-releases/2024/0719-01.html

---

c. Does your organization participate in projects, collaborations, and investments in research that support the advancement of AI safety, security, and trustworthiness, as well as risk evaluation and mitigation tools?

Fujitsu has invested and participated in international projects and collaborations that support the advancement of AI safety, security and trustworthiness, and the development of risk evaluation and mitigation tools. In particular:

•In 2018 Fujitsu was one of the founding members of AI4People Institute, the first multi-stakeholder network to prompt European institutions to stem future AI risks. From 2018 to 2025 Fujitsu has published 4 reports as part of AI4People Institute, sharing best practice and contributing to the development of an Ethical Framework for a Good AI Society. In 2024, Fujitsu acted as a co-chair of the Scientific Committee meeting of AI4People Institute.

https://ai4people.org/ai4people-institute/

•Fujitsu was a member of the High-Level Expert Group on AI, the expert group created in 2018 by the European Commission to support the ethical implementation of the European initiative on AI.

•Fujitsu invested and participated in AI ethics research projects with international universities, including the University of Oxford (United Kingdom), the Technical University of Munich (Germany)..

https://www.tum.de/en/news-and-events/all-news/press-releases/details/neue-zusammenarbeit-von-tum-und-fujitsu

•Fujitsu collaborated with Ochanomizu University(Japan) to establish a new AI ethics research lab, leveraging AI technologies to promote gender equality

https://www.fujitsu.com/global/about/resources/news/press-releases/2023/0317-02.html.

•Fujitsu actively collaborate to setting technical standards for AI safety, security and trustworthiness by participating in international standardization institutes in Japan, UK and Europe.

https://phawm.org/

・Fujitsu has provided the Italy-based startup with AI Trust technologies, consisting of five core tools from its Fujitsu Kozuchi AI service. These technologies will enable AKOS's AI governance platform AKOS HUB, to offer EU AI Act compliance, risk management and general AI governance services and solutions to enterprise customers.

https://www.fujitsu.com/global/about/resources/news/press-releases/2025/0418-01.html

d. What research or investment is your organization pursuing to minimize socio-economic and/or environmental risks from AI?

Fujitsu is pioneering the convergence of digital technologies with insights from the humanities to address pressing social and environmental challenges. This capability is particularly valuable in addressing challenges such as:

•Urban planning and development: Social digital twins can inform the planning of sustainable and resilient cities, optimizing infrastructure, transportation, and public services.

•Climate change mitigation and adaptation: By modeling the impact of climate change on cities and regions, social digital twins can inform adaptation strategies and resource allocation.

•Public health and safety: Social digital twins can facilitate the tracking and prediction of epidemics, enabling targeted interventions and public health measures.

•Social inclusion: Social digital twins can identify and address social inequalities, ensuring that opportunities and resources are distributed equitably across communities.

https://www.fujitsu.com/uk/emerging-technologies/key-technologies/converging/

Section 7 - Advancing human and global interests

a. What research or investment is your organization pursuing to maximize socio-economic and environmental benefits from AI? Please provide examples.

Fujitsu is making extensive research and development investments to maximize the socio-economic and environmental benefits of AI. Based on publicly available information, here are some specific examples of initiatives:

AI-powered Drug Discovery: Utilizing AI to explore new drug candidates and streamline clinical trials, contributing to the advancement of medicine. For example, Fujitsu is collaborating with AI-powered drug discovery startups to accelerate the development of treatments for intractable diseases.

https://global.fujitsu/en-global/uvance/healthy-living

Contributing to Climate Change Adaptation Measures: Fujitsu will leverage advanced forecasting technologies, incorporating sensing, high-performance computing (HPC) simulations, AI, advanced ICT and other digital technologies to effectively reduce greenhouse gas emissions. These technologies will be used to develop solutions for building resilient social infrastructure, ensuring a stable supply of agricultural products, and mitigating food loss. Through these efforts, we aim to minimize the harm caused by climate change to society and our customers.

“Fujitsu Climate and Energy Vision”

https://www.fujitsu.com/global/about/environment/climate-energy-vision/

---

b. Does your organization support any digital literacy, education or training initiatives to improve user awareness and/or help people understand the nature, capabilities, limitations and impacts of advanced AI systems? Please provide examples.

As a company that develops and provides AI, Fujitsu has committed to AI governance. Since stakeholder collaboration is essential to ensure the reliability on AI, we share our knowledge throughout education on AI technology and its risks with our clients and the broader community. This will help to improve overall AI literacy.

c. Does your organization prioritize AI projects for responsible stewardship of trustworthy and human-centric AI in support of the UN Sustainable Development Goals? Please provide examples.

Fujitsu is actively engaged in initiatives towards achieving the SDGs. These efforts are showcased on the official website. Specifically, as examples of contributing to the SDGs through digital technology and services, there are initiatives such as "Precise Prediction of Meteorological Disasters" and "Realizing a Resilient Society" supported by the supercomputer Fugaku technology.

https://www.fujitsu.com/global/about/csr/sdgs/

d. Does your organization collaborate with civil society and community groups to identify and develop AI solutions in support of the UN Sustainable Development Goals and to address the world's greatest challenges? Please provide examples.

Fujitsu has launched Uvance, a high-value-added business model focused on creating markets addressing social issues. To address global challenges, we believe that partnerships with civil society and community groups are essential. These collaborations bring diverse perspectives and expertise, bridging the crucial knowledge gap in both technical understanding and data literacy between AI providers and the broader community. These are important to build trust in the AI industry.

https://www.fujitsu.com/global/about/csr/sdgs/

https://www.fujitsu.com/global/about/csr/vision/ungc/

As an important element of this partnership, we actively engage in industry-academic partnerships with educational and research institutions, focusing on AI ethics research and development, and human capital development. These include developing courses, giving lectures, and hosting interns.

The insights gained from these collaborations inform the development of our AI solutions across the value chain, from AI research and development to responsible technologies' deployment and user literacy.