

OECD AI Transparency Report

Organization: KDDI Corporation (JPN) Reporting Period: Q2 2026 Published: October 2, 2026

Section 0 – Your role in the AI system lifecycle

Responding as (please select all that apply):

- Deployer
- Application developer (/provider)

If any of the fields above are selected, please indicate your organization size:

Large enterprise: 250 or more employees

Section 1 – Risk Identification and Evaluation

1. How does your organization define and/or classify different types of risks related to AI?¹

- Align with specific external frameworks, standards, reports, and/or guidance documents such as taxonomies, classification systems, and/or sets of definitions for risk areas (e.g. the NIST AI Risk Management Framework, the ISO/IEC 42001, the OECD AI Principles, the EU General-Purpose AI Code of Practice, the International AI Safety Report). (please specify): Japan AI Guidelines for Business☐OECD AI Principle☐EU General Purpose AI Code of Practice
- Maintain an internal taxonomy, classification system, and/or set of risk area definitions

How does your organization define thresholds at which severe risks, unless adequately mitigated, may be considered "unreasonable"? Please describe the framework(s) most relevant to your organization's role and context. If your organisation does not use formal thresholds, you may describe instead the policies, decision criteria, or governance processes you apply when assessing severe AI risks. You may also describe: • Specific examples of contexts in which your models or systems could, in your assessment, pose unreasonable or intolerable risk; • How mitigations are graduated by capability or propensity level; • How your organisation considers the specificities of different AI technologies, such as generative AI and agentic AI, including any specific risk assessment or governance mechanisms applied to agentic AI capabilities.

Rather than relying on predefined capability thresholds, KDDI applies a risk-based approach to AI risk assessment. KDDI evaluates risks by considering factors including impact severity, likelihood, scale, and reversibility, and determines appropriate mitigation measures based on the results of that assessment.

2. Both before and after deployment, what practices does your organization use to identify and evaluate vulnerabilities, incidents, emerging risks and misuse throughout the AI system lifecycle?

- Internal benchmarks, standard metrics (e.g., frequency, severity scores)
- Internal model, system, or application-independent research initiatives
- Incident reports, including reports shared by other organizations
- Other(s) (please specify): Conducting pilot testing for the introduction of an internal red teaming
- Qualitative assessments (e.g., expert judgment, narrative scoring)
- Impact assessments such as personal data protection assessment and fundamental rights impact assessments
- Vulnerability reports
- Publicly available benchmarks and measurement tools

Please briefly describe your organization's decision-making process for deploying an AI model or system including: who has decision authority; what evidence and criteria are required (e.g., performance, safety/security, robustness, fairness, privacy, compliance, independent external testing, evaluation, validation and verification (TEVV) or assurance); contextual caveats or limitations required in interpreting risk evaluation metric results; what approvals/sign-offs are needed; and what safeguards (e.g., mitigations, monitoring, or phased release) must be in place to move into deployment.

- **Evidence and criteria:**

In addition to performance-related considerations, KDDI assesses AI systems against criteria derived from the KDDI Group AI Development and Utilization Principles, including human oversight, safety and security, privacy, fairness, transparency, accountability, and compliance.

- **Approvals and sign-off:**

In accordance with KDDI's internal AI Guidelines, AI projects are subject to a second-line review process. Deployment decisions are made by the relevant first-line business organization, taking into account the scale, scope, and risk profile of the model or system.

- **Safeguards required for deployment:**

Prior to deployment, applicable mitigation measures identified through the AI Impact Assessment (AIA) process and specified in the AI Development Guidelines must be implemented.

Following deployment, how do you use incident reports — including those shared by other organizations — to identify emerging issues, update risk assessments, and trigger corrective actions.

Findings from incident reports and newly identified issues are incorporated into KDDI's internal AI Guidelines as appropriate, taking into account their significance and recurrence.

3. Does your organization have mechanisms to receive and/or share reports of risks, incidents or vulnerabilities by/with third parties?

Yes, both receiving and sharing

If yes, please indicate which stakeholders reporting mechanisms may be accessible to, recognising specifics will depend on the nature of the report and risk level. For each, indicate whether access is on a standing basis (Always), activated based on context (Ad hoc/as relevant), or not currently accessible.

	Always	Ad hoc / as relevant	Not currently accessible
Relevant employees (security, legal/compliance, etc.)	☐		
Public authorities (e.g., public reporting offices for security incidents or data breaches)	☐		
Supervisory authorities (e.g., data protection authorities)	☐		
Industry partners or industry fora	☐		
Users (end users, enterprise customers, developers using APIs)	☐		
Business customers / deploying organizations (if different from “users”)	☐		
Supply-chain partners (cloud, data providers, etc.)			☐
Academia / researchers	☐		
Independent auditors		☐	
Standards bodies / multi-stakeholder initiatives (OECD.AI, ISO/IEC, IEEE, etc.)	☐		
Specific civil society organizations	☐		
Media / general public (people or communities indirectly impacted)	☐		
Other:			☐

Please describe how your organisation determines when and how reporting mechanisms are made accessible to different stakeholders (e.g. based on legal or regulatory requirements, internal policies, or risk level). Please also provide public URLs or details on how to submit reports. If none, write “Not applicable”

KDDI determines the appropriate reporting channels and response processes based on applicable legal and regulatory requirements, internal compliance and security policies, and the severity and risk level of the matter being reported.

Employees may report concerns through the KDDI Group Business Ethics Helpline (whistleblowing system). Customers, business partners, and other external stakeholders may submit inquiries, concerns, or reports through the Helpline for Suppliers and publicly available contact channels. Reported matters are handled and escalated in accordance with established governance processes, and, where required, are reported to relevant authorities or regulators.

Public information regarding these channels is available at:

- [Compliance \(including the Business Ethics Helpline\): KDDI Compliance](#)

- [Helpline for Suppliers](#)
- [Corporate contact channels: KDDI Contact](#)
- [Security-related governance information: KDDI Security Portal](#)

How does your organization share relevant information as appropriate?

- Information-sharing partnerships (with confidentiality agreements as appropriate)
- Reporting to regulatory authorities as relevant
- Publicly

Please describe what type of information is shared.

KDDI publicly discloses information regarding significant incidents that exceed a certain severity threshold, including, where appropriate, the nature of the incident, its impact, root causes, and measures implemented to prevent recurrence. In addition, information on other incidents is shared through relevant information-sharing partnerships and industry coordination mechanisms. However, the scope of disclosure is subject to contractual, confidentiality, legal, and security obligations, and certain information may therefore be restricted to authorized stakeholders.

4. If your organization has programs to incentivize risk(s) disclosure, incidents and systemic vulnerabilities, please share what type of programs you use?

- Not applicable

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

Contributes and uses

If contributes or uses, please select all that apply:

- ISO/IEC standards (e.g., ISO/IEC 27001, ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 42005)
- NIST AI Risk Management Framework (AI RMF)
- General Purpose AI Code of Practice
- Other international or regional standards (please specify): Japan AI Guidelines for Business

6. Does your organization collaborate with relevant stakeholders across sectors to assess and adopt risk mitigation measures to address risks that could have broad and potentially cascading socio-economic impacts? Please indicate which stakeholders you collaborate with, and whether collaboration is on a standing basis (Always-on), activated based on context (Ad hoc/as relevant), or there is no current collaboration.

	Always-on	Ad hoc / as relevant	No current collaboration
Relevant employees (security, legal/compliance, etc.)	☐		

	Always-on	Ad hoc / as relevant	No current collaboration
Public authorities / regulators / AI safety institutes / other public sector bodies and inter-governmental coordination structures	☐		
Industry partners or industry fora	☐		
Users (end users, enterprise customers, developers using APIs)	☐		
Business customers / deploying organizations (if different from “users”)	☐		
Supply-chain partners (cloud, data providers, etc.)			☐
Academia / researchers		☐	
Independent auditors		☐	
Standards bodies / multi-stakeholder initiatives (OECD.AI; ISO/IEC; IEEE; AIID etc.)		☐	
Independent civil society organizations (e.g., for evaluations, audits, or policy review)			☐
Media / general public (people or communities indirectly impacted)		☐	
Other(s) (please add any other relevant stakeholder groups):			☐
Not applicable			☐

Please describe examples of how your organization collaborates. Examples may include: participating in multi-stakeholder or industry initiatives; partnering with academia, civil society, or the public sector; establishing internal or joint governance structures with external experts or in partnership with other efforts to share knowledge and jointly address risks.

Examples include:

- Convening an advisory board with external experts to obtain independent perspectives and discuss AI-related risks and mitigation strategies.
- Participating in the AI Governance Association (AIGA), which promotes the adoption of AI governance practices in Japan. Through AIGA, KDDI collaborates with industry, academia, and other stakeholders to exchange information and advance approaches to AI risk mitigation.

Any further comments and implementation documentation.

No answer provided

Section 2 – Risk Management and Information Security

7. Across the AI system lifecycle, what steps does your organization take to manage risks and vulnerabilities? Please indicate which specific practices, tools or metrics your organization uses at each lifecycle stage. You may refer to tools or metrics present in the OECD.AI Catalogue of Tools and Metrics or suggest additions. Respondents may complete only the lifecycle stages relevant to their organisation's role. Stages that do not apply may be left blank.

Plan and design

Collect and process data

Build, integrate and interpret model

Verify and validate

Deploy

Operate and monitor

Please provide a consolidated description of your organisation's approach to risk management across the AI system lifecycle, including how the practices identified above operate together and any cross-cutting governance, review or escalation processes. Please also indicate how often these practices are reviewed and what types of events trigger reviews and updates. Where relevant, please distinguish between different types of AI systems (e.g. generative or agentic AI).

KDDI operates a risk management framework centered on the KDDI Group AI Development and Utilization Principles, the AI Guidelines (internal), and the AI Impact Assessment (AIA) process. AI-related risks are managed through a cross-functional governance structure based on the Three Lines Model under executive oversight. Business units (first line), the AIA Office and governance functions (second line), and independent oversight functions (third line) work together to identify, assess, mitigate, and monitor AI risks throughout the AI lifecycle.

Risk assessments are conducted during the planning phase using a risk-based approach, and appropriate mitigation measures are identified before deployment. Following deployment, KDDI continuously monitors AI system performance, output quality, fairness, and other relevant risk indicators, and implements improvements where necessary.

As part of KDDI's enterprise-wide PDCA-based risk management cycle, AI governance policies and practices are reviewed at least twice a year. Additional reviews may be triggered by factors such as incidents, emerging risks, significant technological developments, or revisions to external laws, regulations, standards, and guidelines.

KDDI also adopts differentiated risk management approaches depending on the type of AI system. For general generative AI systems, assessments focus primarily on risks related to information leakage, privacy protection, and the reliability and appropriateness of outputs. For agentic AI systems, additional emphasis is placed on controllability, human oversight, and Human-in-the-Loop (HITL) mechanisms to ensure that human operators can appropriately supervise and intervene when necessary.

Reviews and oversight are supported through the AI Expert Advisory Meeting, the AIA Office, the Data & AI Governance Subcommittee, and the Risk Management Committee as part of KDDI's agile

governance approach.

Please describe any measures used to ensure data quality and fairness across the data collection and curation stage (e.g., dataset audits, filtering training data to remove harmful content or personal information, fine-tuning on curated data, use of moderation tools, assessment of limitations to model generalisability).

KDDI uses multiple measures to support data quality, fairness, and privacy protection throughout the data collection and curation process. Privacy risks are assessed through impact assessment processes, and data governance is supported through dedicated governance structures, including advisory mechanisms involving internal and external expertise.

To protect privacy and confidential information, KDDI applies data handling controls in accordance with its internal policies and privacy requirements. Where appropriate, data is anonymized or de-identified before use, and multi-layer filtering processes are applied to reduce the risk of inappropriate, sensitive, or low-quality data being incorporated into AI systems.

KDDI also evaluates fairness and bias risks as part of its AI governance framework. Depending on the use case, AI-based techniques may be utilized to help identify personal or sensitive information within datasets and support appropriate data management practices.

These measures operate in conjunction with the AI Guidelines (internal) and the AI Impact Assessment (AIA) process, which require consideration of privacy, fairness, non-discrimination, and responsible data handling throughout the AI lifecycle.

8. What security measures are used in testing AI systems?

- Other(s) (please specify): KDDI conducts AI system testing in environments that are isolated from production environments and applies multiple layers of security controls. Several of the measures referenced in the checklist are implemented in practice, including controls for which detailed information has not been publicly disclosed. However, KDDI does not publicly disclose detailed technical and operational security configurations. In line with our security governance practices, certain operational details of security controls are not publicly disclosed. These controls are governed through internal security policies and risk management processes.

8.A. Please indicate, if relevant, the team or role responsible for overseeing secure testing and whether this responsibility is shared across multiple teams and/or functions.

The team responsible for AI governance acts as the central point of coordination and works in collaboration with the information security function and relevant first-line business organizations. This cross-functional approach enables the identification, assessment, mitigation, and monitoring of AI-related risks while ensuring alignment with KDDI's broader risk management and governance framework.

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

9.A. Safeguards that promote lawful data use and transparency in AI training:

- Maintain a copyright policy that addresses data sourcing, content provenance, safeguards, and organizational roles and responsibilities
- Apply provenance controls to guard against training data being sourced from websites or repositories that have been determined to engage in large-scale piracy
- Maintain policies or practices to respect copyright holders' preferences through, where appropriate/applicable, mechanisms like Robots.txt "do not train" tags or other machine-readable protocols developed through voluntary, industry-led standards processes
- Conduct data cleaning, qualification, and/or tokenization activities as part of a transformative data preparation process
- Engage in AI training that comprises a non-consumptive use of any underlying data
- Consult and/or retain an intellectual property attorney to protect, enforce, and comply with, intellectual property rights.

9.B. Safeguards that reduce the risk of dissemination of outputs that may infringe copyright:

- Restricting outputs that raise ethical, human rights, or legal concerns—such as non-consensual intimate imagery, unauthorized deepfakes, or outputs that are substantially similar to copyrighted works.
- Designating clear points of contact so creators or rights holders can raise concerns about infringing outputs
- Filtering results using keyword or image-based restrictions to reduce risks of misuse
- Other(s) (specify): KDDI provides AI service "Buffmee," which enables copyright holders and content creators to share and manage content in a trusted manner. By providing an environment that supports the appropriate handling of rights-related information, the service helps promote the responsible use of copyrighted content and reduce the risk of unauthorized use.

10. How do you protect privacy and prevent your systems from disclosing confidential or sensitive data across the AI lifecycle?

- Make information about data privacy, practices, and controls accessible to a diverse set of stakeholders
- Use security controls, including encryption at rest and in transit
- Provide organizational customers with controls to configure and implement privacy choices (e.g., data retention, logging, access, or processing settings)
- Apply Privacy-Enhancing Technologies (PETs) where applicable (e.g. differential privacy, federated learning, synthetic data generation, homomorphic encryption)

Describe key privacy measures and data-protection standards applied.

KDDI applies a multi-layered approach to privacy protection and data governance across the AI lifecycle.

KDDI maintains and continuously publishes a dedicated [Privacy Portal](#) that provides comprehensive information on its privacy governance framework, including the KDDI Privacy Policy, principles for personal data protection, data subject rights, and measures for the appropriate handling of personal information. This enables stakeholders to access up-to-date information regarding KDDI's privacy practices and commitments.

To strengthen data protection, KDDI continuously evaluates and develops advanced cryptographic technologies. This includes research activities related to Post-Quantum Cryptography (PQC) and other next-generation security technologies.

KDDI also provides security-focused services for enterprise customers operating in sectors with stringent security and compliance requirements, including financial services, healthcare, and the public sector. Examples include the "[KDDI Encryption Key Management Service for Google Cloud](#)," provided in collaboration with KDDI IRET, a KDDI Group company.

As part of its Privacy-Enhancing Technology (PET) initiatives, KDDI is studying and evaluating technologies such as Fully Homomorphic Encryption (FHE) through research activities and Secure Multi-Party Computation (MPC) in collaboration with external partners. These efforts are intended to support privacy-preserving data utilization while maintaining a high level of security and trust.

These technical and organizational measures are complemented by AI governance processes, including the AI Guidelines (internal) and AI Impact Assessment (AIA) framework, which require consideration of privacy, security, and responsible data handling throughout the AI lifecycle.

11. How does your organization assess cybersecurity risks and implement policies to enhance the cybersecurity of advanced AI systems across the AI system lifecycle? Respondents may complete the checkbox subsections in 11.A–11.D or describe their overall approach under 11.E.

11.A. Governance, policy and assessments

- Other(s) (specify): In line with the questionnaire guidance allowing respondents to describe their overall approach under "Other," KDDI provides a consolidated response in Q11.E. Detailed technical and operational security measures are not publicly disclosed for security reasons.

11.B. Technical and operational controls

- Other(s) (please specify): In line with the questionnaire guidance allowing respondents to describe their overall approach under "Other," KDDI provides a consolidated response in Q11.E. Detailed technical and operational security measures are not publicly disclosed for security reasons.

11.C. Protection of sensitive or high value AI assets

- Other (please specify): In line with the questionnaire guidance allowing respondents to describe their overall approach under "Other," KDDI provides a consolidated response in Q11.E. Detailed technical and operational security measures are not publicly disclosed for security reasons.

11.D. Insider risk protection detections

- Other (please specify): In line with the questionnaire guidance allowing respondents to describe their overall approach under "Other," KDDI provides a consolidated response in Q11.E. Detailed technical and operational security measures are not publicly disclosed for security reasons.

11.E. Please describe the main security measures your organization applies and indicate which are specific to particularly sensitive AI assets, where relevant.

Consistent with the questionnaire guidance that respondents may describe their overall approach rather than complete each individual subsection, KDDI provides a consolidated description of its cybersecurity

governance and security management approach below.

KDDI assesses cybersecurity risks and implements security controls in accordance with internal rules and guidelines established based on its corporate Security Policy. To enhance the security of advanced AI systems, KDDI has established internal development standards and operational guidelines that address AI-related risks as part of its broader governance and security framework. These measures operate in conjunction with the AI Guidelines (internal), the AI Impact Assessment (AIA) process, and enterprise-wide risk management activities.

KDDI maintains an Information Security Management System (ISMS) certified under ISO/IEC 27001 and operates its security management framework in accordance with the requirements of that standard.

As described in KDDI's "[Initiatives for Safe and Secure Service Delivery](#)," and its [publicly available Security Policy](#), KDDI classifies information assets according to their importance and sensitivity and defines handling requirements accordingly. Appropriate technical and organizational controls are applied based on the classification and criticality of those assets, including AI systems and associated data, to ensure the protection of sensitive information and the secure operation of services.

While KDDI does not publicly disclose detailed technical or operational security controls at the level of granularity reflected in Sections 11.A–11.D, relevant controls are implemented and managed through KDDI's security governance framework, internal security policies, and risk management processes.

12. 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?

- Internal vulnerability disclosure receipt and tracking processes
- Investigation of reported or identified risks and vulnerabilities
- Development of patches or other mitigations for confirmed risks or vulnerabilities
- Testing of patches or other mitigations
- Scanning for and mitigation of similar risks or vulnerabilities
- Collaborative vulnerability sharing (e.g., with partners, industry groups)
- Vulnerability disclosure program that is aligned with internationally recognized standards, e.g. ISO/IEC 30111 and 29147.
- Reporting to regulators / authorities when relevant
- Defined escalation criteria and follow-on actions for identified vulnerabilities (e.g., for external reporting or information sharing)

13. What post-deployment practices does your organization use to monitor and respond to vulnerabilities, incidents, emerging risks and misuse of advanced AI systems?

- Conduct post-deployment monitoring
- Perform root-cause analysis and apply lessons learned to improve future development and/or deployment practices

14. Do you develop or deploy agentic AI systems (systems that can autonomously plan/act or use tools)?⁴

Yes

14.A. If yes, please indicate which categories of controls your organization applies. Please select all.

- Constraints on the agent's action space (e.g., tool-use permissions, environment sandboxing, allowlists/blocklists of resources, scope limits per task)
- Human oversight or interruptibility mechanisms (approval requirements for sensitive actions, escalation paths, interruption interfaces)
- Monitoring (anomaly detection, multi-agent interaction monitoring)
- Logging of agent actions

Please provide any further comments and implementation documentation.

Regarding our response to the opening question of Question 7.

KDDI manages AI-related risks and vulnerabilities throughout the AI system lifecycle through the KDDI Group AI Development and Utilization Principles, the AI Guidelines (internal), and the AI Impact Assessment (AIA) process, including the identification, assessment, mitigation, and monitoring of such risks and vulnerabilities. In responding to this question, KDDI has taken steps to register the KDDI Group AI Development and Utilization Principles as a tool, but has not yet received a response regarding its registration.

As a result, although KDDI implements these risk management practices throughout the AI system lifecycle, we have not been able to fully reflect these practices in the prescribed lifecycle-stage-specific response fields.

Section 3 – Transparency Reporting on Advanced AI Systems

15. Does your organization publish public reports and/or technical documentation related to the capabilities, limitations, and domains of appropriate and inappropriate use of advanced AI systems? Are these clear and understandable by non-technical audiences?

Yes

15.A. If yes, which of the following information is included in your organization's publicly available documentation for any of your AI products?

- Risk management policies
- Capabilities, behaviours, and limitations, including domains of appropriate and inappropriate use or indicative thresholds associated with systemic risks.
- Technical documentation and instructions for use if relevant.
- Plain-language or non-technical summaries

Please provide links or references showing where this information is made public.

KDDI publicly discloses its AI governance framework, including AI risk management policies, through its [AI Governance website](#). These disclosures include the KDDI Group AI Development and Utilization

Principles, which describe KDDI's approach to responsible AI, including human oversight, safety and security, privacy, fairness, transparency, accountability, and collaboration.

In addition, KDDI provides service-specific information, including [terms of use and operational guidance, to customers and users of AI-enabled services \(in Japanese\)](#). Depending on the service, this information may include descriptions of service functionality, limitations, appropriate use conditions, and user responsibilities.

15.B. If yes, how often are such reports usually updated?

At or before major product releases

16. 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?

- Public documentation
- Protected information sharing
- Regulatory reporting as relevant
- Direct engagement with AI safety institutes, civil society or academic partners

Describe how evaluation results are shared and with which stakeholders (e.g. other organizations, governments, civil society and academia, etc). You may also indicate whether non-technical or plain-language summaries are provided for broader audiences.

KDDI shares information regarding AI governance and risk management through AI Security Portal, etc. KDDI also engages with external experts, academic stakeholders, industry organizations, and multi-stakeholder initiatives to discuss AI governance and emerging risks. Publicly available information is generally provided in a manner intended to be understandable by a broad audience.

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

Yes

If yes, provide links to privacy policies or notices covering personal data, user inputs, and AI-generated outputs.

[KDDI's Privacy Policy](#)

18. How 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?

- Not applicable

Please provide links to any publicly available information.

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

Not applicable

20. Does your organization publish statistical insights derived from anonymised, aggregated usage data to advance understanding of AI adoption and its economic impacts in areas including occupations and tasks by region, sector and country? To this end, do you contribute to international cooperation efforts?

No

Please estimate the total staff time and annual expenses associated with conducting compliance activities and include any further comments and implementation documentation (optional).

No answer provided

Section 4 – Organizational Governance, Incident Management, and Transparency

21. How has AI risk management been embedded in your organization's governance framework?

- Board of Directors oversight
- Executive oversight
- Senior management oversight
- Governance council or committee

Please describe how AI risk management is integrated into governance structures, including: which roles or bodies have advisory versus decision-making authority; which roles or bodies have final accountability for AI risk-related decisions; and how often policies are reviewed or updated (e.g., following major incidents, regulatory changes, or material updates to systems).

KDDI has established a multi-layer governance framework for AI risk management. Executive oversight is provided through the Risk Management Committee, which brings together the President, Directors, and CxO-level leadership to address significant enterprise risks. Under this framework, the Data & AI Governance Subcommittee, supervised by the Chief Digital Officer (CDO), oversees AI governance policies, plans, and responses to material AI-related risks.

The AIA Office serves as the central coordination function for AI governance and conducts AI Impact Assessments (AIA) in collaboration with security, legal, and intellectual-property functions. Regular advice and external perspectives are provided through the AI Expert Advisory Meeting.

Policies and operating rules are reviewed on a regular basis, including through expert meetings held at least twice annually. Reviews may also be triggered by technological developments, regulatory

changes, emerging risks, or incidents.

22. Are relevant staff trained on your organization's governance policies and risk management practices?

Yes

If yes, describe training methods (e.g., onboarding modules, regular sessions, and confidential channels to report concerns).

KDDI offers specialized education through [KDDI DX University](#), including training programs focused on responsible AI for employees who develop or provide AI-enabled services and systems.

23. Are steps taken to address reported incidents documented and maintained internally?

Yes

If yes, describe how incident records are kept and used for follow-up (e.g., incident logs, root-cause analysis reports, internal tracking systems). You may indicate whether and how you define escalation thresholds for when incidents must be surfaced to senior leadership or external parties.

Incident records are centrally managed and documented by dedicated security and risk management functions through internal management systems.

Following an incident, KDDI conducts follow-up reviews, including the preparation of post-incident reports and root-cause analyses. Corrective and preventive measures are tracked through internal management systems to ensure implementation and effectiveness. Lessons learned are also reflected in internal rules, operational guidelines, and employee training programs.

KDDI maintains escalation thresholds based on the severity and potential impact of incidents. Where predefined thresholds are exceeded, incidents are promptly escalated to senior management. In addition, reporting to relevant regulatory authorities is conducted where required by applicable laws and regulations.

24. Does your organization share research and best practices on addressing or managing risk?

Yes

If yes, describe how research or good practices are shared (e.g., publications, conferences, collaborations with other sectors).

KDDI shares knowledge and best practices related to AI governance, cybersecurity, and risk management through publicly available resources.

KDDI publishes [annual reports](#) and other public materials covering cybersecurity initiatives, risk management activities, and efforts to provide secure and trustworthy digital services. These publications are intended to promote transparency and contribute to broader understanding of cybersecurity and AI-related risks.

In addition, KDDI operates [the AI Security Portal](#), which provides information on emerging AI security

risks, threat trends, and recommended mitigation measures to support the safe and secure use of AI technologies. Through this portal, KDDI seeks to share practical knowledge and contribute to improving AI security awareness across society.

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

Yes

If yes, please indicate which standards or frameworks apply:

- Other international or regional standards (please specify): Japan, AI Guidelines for Business
- ISO/IEC standards (e.g., ISO/IEC 27001, ISO/IEC 42001)
- NIST AI Risk Management Framework (AI RMF)
- OECD AI Principles

If yes, describe which international technical standards or best practices your organization uses.

Described above.

Any further comments and implementation documentation.

No answer provided

Section 5 – Content Authentication & Provenance Mechanisms

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

- Disclosure to end-users when an AI system is acting autonomously or executing actions on their behalf (e.g., making purchases, sending communications, modifying files)
- Documentation or FAQs explaining when and how AI is used in the system
- Distinct branding or labeling for AI-generated content (e.g., “AI-generated” tag, metadata label)
- Persistent visual or audio indicators (e.g., watermark, icon, chime, banner) during AI interaction
- User disclosure (e.g., text notice, verbal statement, or system label)

Provide any additional details or context on how or when users are informed they are interacting with advanced AI systems (e.g. if such mechanisms are planned, in testing, or applied only to certain products).

KDDI promotes transparency regarding AI use through its AI Governance framework. As part of the AI Impact Assessment (AIA) process and AI Guidelines (internal), KDDI encourages clear disclosure when

users are interacting with AI-enabled services, such as chatbots, where appropriate. KDDI also provides public information regarding its AI governance policies and responsible AI practices.

27. Does your organization use content provenance detection, labeling or watermarking mechanisms that enable users to identify content generated by advanced AI systems?

Yes

27.A. If yes, how?

- Manifest disclosure (e.g., visible label)

27.B. If yes, does your organization use international technical standards or best practices when developing or implementing content provenance?

No

27.C. Does your organization collaborate on or invest in research to advance content authentication and provenance?

Yes

Describe how provenance mechanisms are implemented and which standards or tools are used, and any collaborations or investments to improve content authentication (e.g., C2PA credentials, joint R&D projects, open-source initiatives, standard-setting groups). You may also indicate whether these mechanisms are tested for robustness against removal, tampering, or circumvention.

KDDI supports content authenticity and provenance through a combination of detection technologies, transparency measures, and research initiatives.

- KDDI has invested in Resemble AI through its corporate venture fund. Resemble AI develops technologies to detect AI-generated and manipulated content, including multimodal threat detection capabilities that help identify synthetic audio, video, and image content that may be used for impersonation, fraud, or other harmful purposes, thereby supporting efforts to enhance trust and safety in the AI ecosystem.
- In addition, KDDI Research has conducted research and development related to digital watermarking technologies. For example, KDDI Research developed high-speed video watermarking technologies capable of embedding unique identifiers into streaming content, supporting traceability and the detection of unauthorized redistribution.

Any further comments and implementation documentation.

No answer provided

Section 6 – Research & Investment to Advance AI Safety & Mitigate Societal Risks

28. Does your organization advance research and investment in the following areas?

- Security

- Safety
- Data quality and representativeness
- Information integrity
- System performance and outcomes (e.g. accuracy, consistency)
- Explainability or interpretability
- Transparency
- Robustness or reliability

If yes, please describe key research or investment initiatives in the areas selected above (e.g., dedicated safety teams, funding of research programs, contributions to open-source safety tools, publishing research, partnerships and collaborative research initiatives). You may also indicate whether related outputs are publicly shared, shared with partners or within consortia or not publicly disclosed.

KDDI advances AI safety, security, transparency, and reliability through research, technology development, and public knowledge sharing activities.

KDDI and KDDI Research publish research papers and technical findings related to AI, cybersecurity, trust, and digital infrastructure. These activities contribute to the broader understanding of the opportunities and risks associated with advanced AI technologies.

In addition, KDDI operates the AI Security Portal, which provides publicly accessible information regarding emerging AI security risks, threat trends, and recommended mitigation measures. Through this portal, KDDI shares practical knowledge and best practices to support the safe and trustworthy deployment of AI technologies.

29. Does your organization pursue research or investment related to socio-economic or environmental considerations in the development and deployment of AI?

- Socio-economic considerations (e.g., AI adoption and productivity, workforce transitions, skills development, access to AI tools)
- Environmental considerations (e.g., energy use, computational efficiency, resource use)

If yes, please provide examples of relevant research or investment initiatives for the areas selected above.

- Socio-economic considerations ☐
 - **Partner Upskilling:**
KDDI invests in co-creating AI-driven solutions with corporate clients to address severe domestic labor shortages, optimize supply chains, and enhance productivity in sectors such as logistics and retail, thereby easing structural transitions in the workforce.
- Environmental considerations ☐
 - **100% Renewable Energy in Data Centers:**
By March 2026, KDDI successfully transitioned 100% of the electricity used at its data centers globally (including Telehouse and domestic facilities like the Osaka Sakai Data Center) to renewable energy. This was achieved through a combination of solar generation under au Renewable Energy and long-term Virtual Power Purchase Agreements (vPPAs).

- **High-Efficiency Cooling Technology for AI Infrastructure:**

AI and high-performance GPU clusters generate immense heat. At the Osaka Sakai and Telehouse Tokyo data centers, KDDI has deployed liquid cooling (immersion/water-cooling) systems to scale computing capabilities while slashing air-conditioning energy consumption by up to 70%.

- **AI-Controlled Green Mobile Network Infrastructure:**

Mobile base stations consume significant energy. KDDI co-developed and deployed AI-controlled energy-saving software for its base stations (in partnership with Nokia). This deep-learning software dynamically predicts traffic patterns and powers down inactive network hardware in real-time, reducing base station energy consumption by up to 50% without degrading user connection quality.

Any further comments and implementation documentation.

No answer provided

Section 7 – Advancing Human and Global Interests

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

Yes

If yes, describe any digital literacy or training initiatives your organization supports (e.g., user education, public AI-education programs, school or university partnerships, community workshops). You may also indicate whether these efforts include or prioritise underserved or underrepresented communities.

KDDI supports a range of digital literacy, AI education, and workforce development initiatives designed to help individuals understand the capabilities, limitations, and responsible use of AI technologies.

- **School Education and Youth Partnerships**

KDDI collaborates with educational institutions to provide practical learning opportunities related to AI and digital technologies.

- **University Co-Creation Projects:** KDDI and KDDI Agile Development Center (KAG) work with universities to provide hands-on AI education. Students learn how AI systems can address real-world challenges while also developing an understanding of AI limitations, governance considerations, and responsible deployment practices.
- **AI and Frontier Technology Classrooms:** In collaboration with local boards of education, KDDI provides educational programs that introduce students to AI-enabled technologies, including autonomous systems and drones, while explaining operational constraints and safety considerations.

- **School DX and Teacher Training:** Through KDDI Biz Edge and related initiatives, KDDI supports teachers and school administrators in understanding the safe and responsible use of generative AI, including privacy protection, hallucination risks, and ethical considerations.

- **Regional Revitalization and Digital Inclusion**

KDDI promotes digital inclusion and works to reduce the digital divide, particularly in regional communities and among elderly populations.

- **Marugoto Digital Association:** Through collaboration with local governments and regional stakeholders, KDDI supports digital literacy programs and community workshops that help citizens understand digital services, privacy considerations, and the appropriate use of AI-enabled tools.
- **Regional AI Development Programs:** KDDI has collaborated with organizations such as Aidemy to support AI and DX training programs for regional businesses, municipal governments, and small-to-medium enterprises, helping broaden access to AI capabilities outside major metropolitan areas.

- **Professional and Community Training**

KDDI Group companies also provide advanced training programs for engineers and organizations adopting AI technologies.

- **KAGAI Learning Hub:** KDDI Agile Development Center operates programs designed to support practical AI application development and responsible AI deployment.
- **Advanced AI Operations and Governance Training:** These programs include topics such as Retrieval-Augmented Generation (RAG), Model Context Protocol (MCP), LLMOps, observability, evaluation, AI monitoring, and risk mitigation approaches that help participants understand both the capabilities and limitations of advanced AI systems.

Through these initiatives, KDDI seeks to promote responsible AI adoption while ensuring that AI literacy opportunities are available to students, educators, businesses, regional communities, and other stakeholders.

31. Does your organization pursue AI projects that aim to deliver societal or public benefits, including through partnerships with civil society and community groups?

Yes

If yes, please provide examples, including any collaborations with civil society, community groups, or efforts to address broader societal challenges.

KDDI positions sustainability management as a core pillar of its corporate strategy, aiming to achieve both business growth and the creation of social value. As one of the key enablers of this vision, KDDI leverages AI to generate societal and public benefits through collaboration with local governments, academic institutions, industry partners, and civil society organizations.

- **Disaster Prevention, Public Safety, and Infrastructure Resilience**

KDDI works with local governments and public-sector stakeholders to strengthen disaster preparedness and emergency response capabilities. Examples include AI-enabled autonomous drone solutions for search-and-rescue operations, disaster monitoring, and emergency connectivity

support, as well as the deployment of AI-based fault recovery technologies to help maintain critical communications infrastructure during emergencies.

- **Regional Revitalization, Agriculture, and Fisheries**

KDDI collaborates with regional communities to address challenges such as population decline, labor shortages, and the aging workforce. Examples include AI-enabled smart fisheries that support sustainable aquaculture through image analysis and feeding optimization, as well as AI-based wildlife monitoring systems that help local communities protect agricultural resources and ecosystems.

- **Municipal Digital Transformation and Public Services**

KDDI supports local governments and regional organizations in deploying AI and digital transformation solutions. Examples include generative AI initiatives that improve administrative efficiency and AI-enabled mobility services that enhance transportation access for elderly and underserved populations.

- **Support for Academia, Non-Profit Organizations, and Civil Society**

Through the KDDI Foundation, KDDI provides research grants, funding, and support for initiatives led by universities, NPOs, and NGOs that utilize ICT and AI technologies to address societal challenges, promote digital inclusion, and support regional development.

Through these activities, KDDI seeks to advance the realization of an AI-Native Society that delivers societal value while ensuring that the benefits of AI are broadly shared across communities. KDDI is committed to promoting the responsible and trustworthy deployment of AI in support of this vision.

Any further comments and implementation documentation.

No answer provided