

OECD AI Transparency Report

Organization: NEC Corporation (JPN)

Reporting Period: Q3 2026

Published: October 2, 2026

Section 0 – Your role in the AI system lifecycle

Responding as (please select all that apply):

- Model developer (/provider)
- Application developer (/provider)
- Deployer

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

- Maintain an internal taxonomy, classification system, and/or set of risk area definitions
- 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): EU AI Act, OECD AI Principles, Hiroshima Process International Code of Conduct, Japan's Guidelines and NIST AI Risk Management Framework
- Consult with external stakeholders (e.g., from academia, industry groups, civil society, or standard development organisations) when developing or updating risk taxonomies

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.

We categorize the risks associated with the use of AI into two perspectives: "AI Safety," which ensures that AI operates safely and appropriately within the scope intended by humans and prevents harm to life, physical well-being, property, mental well-being, and the environment; and "AI Security," which protects AI from unauthorized access, tampering, damage, and data leaks from external sources. Furthermore, based on the "NEC Group AI and Human Rights Principles," we have established a framework for assessing human rights and privacy risks from the perspectives of fairness, privacy, transparency, accountability, and appropriate use.

We identify risks arising from AI that require attention and have established and implemented company-wide policies that define governance structures and compliance requirements, as well as guidelines, manuals, and checklists that outline operational workflows. At every phase of the lifecycle—from planning and proposal through design and development to operation and maintenance—the relevant departments collaborate to implement a risk mitigation process that involves taking measures commensurate with the severity of each risk.

In our enterprise-wide risk management, we refer to the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Integrated Framework and ISO 31000, and we utilize the "Risk Total Picture" framework, which classifies risks into three categories based on their nature. We update our risk map quarterly based on a five-level impact assessment and a three-level urgency assessment, and report it to the Risk Control and Compliance Committee, which is overseen by the Board of Directors. Within this framework, we have identified "Respect for Human Rights" as one of our risks. After continuously assessing both actual and potential negative impacts across the entire value chain, we have designated "New Technologies, such as AI, and Human Rights" as a significant human rights issue.

In accordance with Japan's AI Act (Act on Promotion of Research and Development, and Utilization of AI-related Technology), and taking into account global regulatory trends, guidelines, and social acceptance, we continuously review our risk assessments, internal policies, and the implementation of countermeasures. Furthermore, we regularly convene an advisory council comprising external experts to seek ongoing advice on AI and human rights risks posed by new

technologies and forms of application, such as generative AI, biometric authentication, and AI agents. We incorporate these insights into our deliberations on risk management strategies for new forms of application.

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 red teaming³
- Adversarial testing to detect technical vulnerabilities
- Publicly available benchmarks and measurement tools
- Internal benchmarks, standard metrics (e.g., frequency, severity scores)
- Structured techniques to explore the behavior or performance of a model and/or application, such as model elicitation or bottleneck assessments
- Qualitative assessments (e.g., expert judgment, narrative scoring)
- Impact assessments such as personal data protection assessment and fundamental rights impact assessments
- Internal model, system, or application-independent research initiatives
- External model, system, or application-independent research initiatives
- Vulnerability reports
- Incident reports, including reports shared by other organizations
- Automated monitoring / remote status reporting (e.g., telemetry pipelines, automated alerts when risk thresholds are breached)
- Specific risk identification practices for agentic AI capabilities, e.g., autonomous action-taking, tool use, multi-step planning (please specify): In the “cotomi Act”, we configure and operate AI agents in accordance with corporate governance rules and policies. We also examine risks specific to AI agents, such as autonomous selection of means to achieve a goal and the allocation of responsibility when multiple AI agents collaborate. Based on the OWASP AI Testing Guide, we conduct vulnerability testing that includes testing for excessive or unsafe autonomous behavior by AI agents.

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.

Prior to deploying AI systems, we implement the following measures from a multifaceted perspective, including AI governance, quality control, and security.

1. Risk Assessment Based on AI Governance and Human Rights Policies

In accordance with the “NEC Group AI and Human Rights Principles,” we conduct risk assessments using risk checklists and implement countermeasures at every phase of the lifecycle—from planning and proposal through design and development to operation and maintenance. Additionally, based on the “AI Guidelines for Business,” we apply and update these guidelines within our internal AI governance framework.

2. Development Management and Quantitative Standards Based on the AI Quality Guidelines

To ensure the quality of AI-powered systems, we have been applying the “NEC AI Quality Guidelines,” established in December 2019, to development projects since April 2020. These guidelines establish specific standards and checklists for each of the four development phases (1. System Planning and Proof of Concept (PoC), 2. Data Collection and Processing, 3. Model Creation, Evaluation, and Testing, and 4. System Operation). By conducting checks when transitioning between phases, we proactively prevent risks in the subsequent phase. In particular, by setting quantitative standards for the volume of training data, as well as for outliers and missing values, we ensure clarity in these standards and enable objective assessments by third parties.

3. Evaluation and Safety Measures for the Generative AI Core Technology “cotomi” and AI Agents

Regarding “cotomi,” our in-house generative AI core technology, we verify the model's safety and reliability under a comprehensive evaluation framework that utilizes multiple assessment tools—including general-purpose benchmarks, Japanese-language benchmarks, and RAG performance evaluations—while ensuring strict compliance with laws and regulations regarding training data. In addition, we have implemented high-precision AI guardrail functions, including technologies for detecting false and misleading information and proposing corrections. Furthermore, with our AI agent technology “cotomi Act,” we leverage our accumulated knowledge on risk mitigation to configure and operate agents in accordance with corporate rules and policies from a governance perspective, thereby enabling the safe and secure use of autonomous agents.

4. Security in Development and Operations

In accordance with the “Basic Information Security Rules (NEC Security Policy),” we conduct evaluations in a secure environment equipped with necessary security measures—such as isolation from external networks and authenticated access—as a prerequisite for deployment. Additionally, depending on the system's criticality (security level), we require or recommend that our in-house security team perform vulnerability self-assessments and penetration tests. Furthermore, regarding security risks—including those associated with AI systems—we implement risk management based on a cybersecurity checklist at every phase, from the planning and proposal stages through design and

implementation, to operation, maintenance, and lifecycle management. The project manager and organizational manager verify the status of these implementation efforts.

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.

To maintain the safety and reliability of our AI models and systems and to mitigate risks, we operate an integrated framework that encompasses the collection and analysis of incident and threat information, vulnerability management, industry and global collaboration, post-deployment operations and customer support, and quality improvement.

1. Deployment of AI Models and Systems

We have established a CSIRT (Computer Security Incident Response Team) under the CISO (Chief Information Security Officer) to monitor cyberattacks, analyze the characteristics of attacks and malware, preserve and analyze data in the event of an incident, investigate the causes, and resolve the situation.

2. Provision of AI Models and Systems

Through the "Cyber Intelligence Sharing Platform," we rapidly share threat intelligence—including cyberattack methods, incident cases, vulnerability risk metrics, and security countermeasure indicators—with each business division, where it is utilized as a basis for assessing business risks.

In addition, we have established the NEC Group Information Security Incident Response Desk, which receives and manages reports of security incidents. The desk includes experts in security, legal affairs, and public relations, who provide response advice from various perspectives. By operating a system that collects vulnerability information regarding products and customer deliverables and distributes patch information, we ensure a rapid response to newly identified vulnerabilities and incorporate these findings into the revision of our guidelines.

For post-deployment maintenance and operational support, we maintain and operate programs that monitor logs and implement countermeasures appropriate to the level of risk. Furthermore, we have established it as standard company practice to report and explain issues to each customer using our AI systems and to implement improvements when problems are confirmed. We participate in the "AI Safety Evaluation Environment Task Force" operated by Japan AISI, sharing insights and providing feedback within the industry based on our trial use of AI safety evaluation tools, including automated red-team functions.

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"

The reporting mechanism is determined based on legal and regulatory requirements, internal policies, and the severity of the risk.

Regarding vulnerability information, in accordance with our "Vulnerability Disclosure Policy," we have established the NEC Group PSIRT Vulnerability Report Contact (psirt-info[at]mlsig.jp.nec.com; PGP encryption recommended), which accepts reports from external discoverers (such as researchers) on an ongoing basis. Information on the status of our response and corrective measures is published on the "NEC Group Product Security Information Portal" and the domestic vulnerability response portal "JVN" on the disclosure dates agreed upon with the coordinating body (JPCERT/CC).

We have established standard internal procedures requiring those involved in, or who discover, incidents (or potential incidents or accidents) involving the leakage of personal information to report them to the heads of their respective departments and the NEC Group Information Security Incident Response Desk. In accordance with relevant laws, regulations, and government agency guidelines, and after taking into account the risk of infringement on the rights and interests of the individuals concerned, the designated department coordinates with the Personal Information Protection Promotion Office and relevant departments to notify the individuals concerned, make public announcements, and report to supervisory authorities (such as the Personal Information Protection Commission and the Ministry of Economy, Trade and Industry).

We require third parties with whom we share data or to whom we outsource services (such as supply chain partners) to maintain personal information protection management and operational standards equivalent to those of the NEC Group, and to follow established escalation procedures in the event of a data breach or other incident, as stipulated in our contracts.

Reference URLs:

- Vulnerability Disclosure Policy: https://jpn.nec.com/security-info/policy_en.html
- NEC Group Product Security Information Portal: <https://jpn.nec.com/security-info/index.html> ☐Japanese☐
- Personal Information Protection and Privacy (Incident Response):
<https://www.nec.com/en/global/sustainability/social/privacy.html>

How does your organization share relevant information as appropriate?

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

Please describe what type of information is shared.

For example:

1. Vulnerability Information

We share the following information via our Product Security Information Portal and JVN: the names of products containing vulnerabilities, the affected product versions, the type of vulnerability (buffer overflow, RCE, etc.), the CVE number (NEC assigns CVEs to its own products as CNA), the potential impact of the vulnerability, and the correction procedures, patches, or workarounds.

2. Personal Information Leaks, etc.

We report the following details—an overview of the incident, the cause, the types and number of personal data records involved, whether secondary damage occurred and its nature, the status of our response to the individuals concerned, the status of public disclosure, and measures to prevent recurrence—to the supervisory authorities (such as the Personal Information Protection Commission) in accordance with applicable laws and regulations, and notify the individuals concerned and make a public announcement as necessary.

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)
- Industry-led best practices or codes of conduct
- General Purpose AI Code of Practice

- Other international or regional standards (please specify): Board member of ETSI (European Telecommunications Standards Institute); Vice Chair of the OSG AI Committee, ISO/IEC JTC1/SC42, ITU-T Advisory Committee and member of AI-related committees at Japanese government ministries and agencies

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.)	☐		
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.

To address the wide-ranging and cascading risks that AI poses to society, we continue to participate in cross-sectoral collaborations and partnerships with a wide range of stakeholders.

1. Collaboration with external experts and the academic community (advisory council, joint research, etc.)

2. Collaboration with Public Agencies and Government Policies

We participate in various activities at the Japan AISI, where we test AI safety assessment tools and share insights and feedback. We also participate in government committees and other bodies involved in AI policy, contributing to the formulation of policy recommendations and guidelines.

3. Contributions to standard-setting by international standardization organizations and overseas agencies

- **ISO/IEC JTC1/SC42 (AI):** we serve as a member of the national technical committee.
- **U.S. NIST:** We submitted feedback (such as public comments) on the development process for the AI Risk Management Framework (AI RMF).
- **U.S. IEEE:** We led the AI ethics project "P7001."
- **European ETSI:** As a member of the Board of Directors and Vice Chair of the AI Coordination Group (OCG-AI), we are directly involved in and contributing to the development of international standards for AI safety and risk management.
- **ITU-T:** As Vice Chair of the Advisory Committee, we are monitoring trends in the development of international recommendations, including those related to AI.

Any further comments and implementation documentation.

No answer provided

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).

Since there was no space to list "specific practices" in Question 7 above, we did not answer that question this time. Throughout the entire lifecycle of AI systems, we implement comprehensive risk management by combining cross-functional governance at the executive level, multi-layered risk checks based on policies and guidelines, regular review and update processes, and management measures specific to generative AI and agentic AI.

1. Cross-functional Governance, Risk Management Throughout the Entire Lifecycle, and a Review and Evaluation Framework

- The risk management framework, centered on the Risk Control and Compliance Committee and the CRCO (Chief Risk & Compliance Officer), updates the risk map quarterly based on a five-level impact assessment and a three-level urgency assessment, and provides oversight at the executive level.
- We apply the "NEC AI Quality Guidelines" (which are updated regularly to accommodate generative AI) and have established specific criteria for each of the four distinct phases of development: planning and PoC, data collection and processing, model creation, evaluation, and testing, and system operation. By conducting checks when transitioning between phases, we proactively prevent risks that could arise in the next phase.
- Throughout all phases of the lifecycle—planning and proposal, design and development, and operation and maintenance—we utilize risk checklists based on the "NEC Group AI and Human Rights Principles" to identify human rights and privacy risks and incorporate cross-functional measures to address them.
- With regard to security risks involving AI systems, we implement risk management based on cybersecurity checklists at every phase—from planning and proposal through operation, maintenance, and lifecycle management—and identify risks, evaluate countermeasures, and conduct reviews at each phase.

2. Review Frequency and Update Triggers

- Internal rules, such as the "NEC AI Quality Guidelines," are updated regularly (e.g., to enhance the checklist for generative AI), and we have established "recognition of new threats arising from technological advancements" and "changes in the social environment" as triggers for these updates (e.g., we have updated our policies in response to the increased risk of copyright infringement in image-generation services).
- In accordance with directives from the high-level information security strategy council, we periodically review our company-wide measures.

3. Management Measures Specific to Generative AI (cotomi) and Model Evaluation

- For the generative AI core technology "cotomi," we implement a multi-layered management system that combines strict compliance with laws and regulations regarding training data, a comprehensive evaluation framework utilizing multiple evaluation tools—including general-purpose and Japanese-language benchmarks as well as RAG performance metrics—and AI guardrail functions.
- Based on Japan AISI's "Guide to Evaluation Perspectives on AI Safety," we are developing an AI guardrail that covers all of the evaluation items outlined in the guide.
- We operate a system that combines vulnerability assessments using AI red teaming and penetration testing with continuous verification of outputs through anti-hallucination features.

4. Management Measures Specific to Agentic AI (e.g., cotomi Act)

- Based on the insights gained so far regarding risk mitigation, configuring and operating agents in a manner that takes corporate governance rules and policies into account constitutes a unique management measure that distinguishes this approach from conventional generative AI.

- In “cotomi v3”, we are working to ensure compliance with the Model Context Protocol (MCP) and improve task decomposition and tool selection capabilities. At the same time, we have developed Agentic AI for system risk assessment and internal information security audits, which supports the entire process from threat and vulnerability detection to the formulation of countermeasures.

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).

In the “Data Collection and Processing” phase of the “NEC AI Quality Guidelines,” we have established quantitative standards for factors such as the volume of training data, outliers, and missing values. By conducting rigorous checks in accordance with these standards during phase transitions, we have established and operate a system that enables the early identification and detection of risks stemming from data.

We regard the principles of “responsible AI” (fairness, privacy, transparency, accountability, control, and safety) as fundamental considerations throughout the entire AI development process, and we incorporate these principles even during the data collection and curation stages to ensure quality and fairness.

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

- Isolated and secure test environments
- Network isolation from external access
- Locally hosted testing environments
- Restrictions on outbound Internet or API access, including a list of permitted domains or APIs
- Isolation of staging environments (from production / operational environments)
- Controlled environments for red-teaming and adversarial testing
- Containment measures for prompt-injection and jailbreak attempts
- Controlled security vulnerability testing
- Rate limits and resource caps
- Human-in-the-loop controls for higher-risk test cases
- Access controls, including roles-based permissions
- Disabling, restricting or simulating high-impact capabilities during testing
- Audit logging and monitoring
- Use of “AI-safe” test-data, as appropriate
- Use of synthetic, anonymized, or dummy data, as appropriate

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.

To ensure the secure testing of AI systems, vulnerability assessments are conducted for each project in accordance with the rules established by the cybersecurity department. When more advanced testing is required, security experts conduct tests such as penetration tests.

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
- Refrain from the unlawful circumvention of technological protection measures in data sourcing
- 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.
- Filtering results using keyword or image-based restrictions to reduce risks of misuse
- Other(s) (specify): Our internal generative AI usage policy requires employees to check the quality of generated content and use the AI after considering the risks, and mandates that inputs and outputs be logged in a manner that

allows for auditing.

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)
- Other(s) (specify): Privacy Mark certification (obtained in October 2005), Personal Information Protection Management System compliant with JIS Q 15001

Describe key privacy measures and data-protection standards applied.

We have established and published the “NEC Privacy Policy,” which complies with the Act on the Protection of Personal Information and “JIS Q 15001: Personal Information Protection Management Systems—Requirements,” and we have implemented management systems and technical measures throughout our entire group, both in Japan and overseas.

1. Basic Policy, Applicable Standards, and Company-wide Implementation Framework

- We obtained Privacy Mark certification in October 2005 and have been continuously maintaining and renewing it (we completed our ninth certification renewal in October 2021).
- We designate a person responsible for managing personal information in each department that handles personal information, take measures to ensure that personal information is not handled beyond the scope necessary to achieve the specified purposes of use, and strive to prevent leaks, loss, and damage through necessary and appropriate security measures.
- Based on our cybersecurity checklist, we protect privacy and data throughout the entire development lifecycle of our products, systems, and services. Key measures include identifying and assessing risks to protected assets such as personal information, trade secrets, and authentication credentials; clarifying the division of responsibilities with customers and defining SLAs; implementing access control based on the principle of least privilege; encrypting stored data, backups, and communication channels; ensuring secure cryptographic key management; preventing the output of confidential information in logs and applying masking; restricting the use of confidential information in test data; monitoring access during operations; deleting unnecessary accounts and access rights; and performing irreversible data erasure when disposing of media. This checklist incorporates the principles of ISO/IEC 15408 and draws on the privacy and security management measures outlined in NIST SP 800-53.
- We also require third parties with whom we share or outsource data to comply with security measures equivalent to those of our Group.

2. Technical Safety Management Measures

- We implement access control based on identification and authentication, measures to prevent unauthorized external access, and encryption during transmission (such as TLS), tailored to the risks associated with each operational phase.
- We prevent information leaks in the event of theft, loss, or accidental transmission by applying storage device and file encryption (encryption at rest) as the default security level across the entire NEC Group and by appropriately configuring access rights and usage expiration dates.
- To meet customers' security requirements and data sovereignty demands, we offer multiple deployment options—including on-premises, the domestically developed and operated cloud “NEC Cloud Storage (St)” (limited to domestic data centers), and hybrid models—providing choices that help avoid the risks associated with the cross-border transfer of highly confidential data.
- We provide a filtering function for sensitive information and personal information when entering prompts into generative AI systems, and have established a mechanism that allows users to proactively protect their data according to their risk level.

3. Privacy-Enhancing Technologies (PETs) and Advanced Research and Development

- We are conducting research and development on “highly secure federated learning,” which combines federated learning—a technique that utilizes training data from various organizations in a distributed manner rather than aggregating it in a single location—with secure computation, which enables computational processing while the data remains encrypted. We are advancing research on this technology to prevent the inference of training data from model parameters while also avoiding a decline in AI accuracy.
- At our lab, we are conducting research on a technology that combines differential privacy with federated learning to provide a theoretical guarantee that training data cannot be inferred from model outputs.
- We are working on synthetic data generation technology that can be used for training and validating AI models without using real data (creating synthetic data that reproduces statistical characteristics using generative AI).

- We are conducting research and development on technologies that enable training without disclosing confidential data during additional training (fine-tuning), and have successfully demonstrated the ability to run “cotomi” for inference in a confidential computing environment.

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

- Conduct regular cybersecurity risk and vulnerability assessments tailored to AI models or systems
- Perform threat modeling that includes AI-specific risks (e.g., data poisoning, prompt injection)
- Maintain or update security policies aligned with recognized standards (e.g., NIST CSF, ISO/IEC 27001, SOC 2, CIS Critical Security Controls), and review them regularly in response to emerging risks or regulatory guidance
- Maintain vulnerability management processes (scanning, channels for external reporting, patching, remediation)
- Implement incident response, disaster recovery, or business continuity plans, including escalation procedures for high-severity incidents
- Train staff on cybersecurity best practices and AI-specific threats, including how to recognize and respond to misuse or unintended outcomes of advanced AI systems
- Integrate cybersecurity AI risks into broader cybersecurity risk management activities
- Regularly review security measures and update them in response to emerging risks, incidents, or major releases

11.B. Technical and operational controls

- Apply multi-factor authentication (MFA) and role-based access controls for advanced AI systems
- Encrypt AI assets (datasets, models, configurations) in storage and in transit as appropriate
- Restrict physical access to servers, GPUs, or devices hosting AI models, systems, and/or applications
- Monitor system activity and log access to detect anomalies or misuse
- Conduct secure AI development and/or deployment practices
- Conduct security testing focused on AI-specific risks (e.g., red-teaming, adversarial testing, stress tests)

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

- Limit access to proprietary AI assets based on role or need-to-know
- Store model weights, datasets, and algorithms in secure, access-controlled environments
- Use hardware security modules (HSMs) or trusted execution environments (TEEs) where feasible
- Track and log access to sensitive AI resources
- Require NDAs or confidentiality agreements for staff and contractors with access

11.D. Insider risk protection detections

- Monitor for unauthorized internal access or suspicious activity
- Provide staff training on cybersecurity best practices and AI-specific threats
- Implement insider-risk escalation or response procedures

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

Based on a company-wide cybersecurity governance framework overseen by the CISO (Chief Information Security Officer) and compliance with international standards and specifications, we implement the following security measures for AI (Security for AI) and multi-layered protection measures for high-value and highly confidential AI assets:

1. Company-wide Cybersecurity Governance Framework, Standards, and Shared Infrastructure

- Based on the “NEC Group Information Security Statement,” the “Basic Information Security Rules,” and the “Cybersecurity Management Rules,” we have clarified our accountability structure to establish and maintain the ISMS (ISO/IEC 27001), and we implement security measures for customer-facing systems, products, and services. Under the oversight of the CISO, the CSIRT (comprising four teams: Threat Intelligence, Incident Response, SOC, and Development) is responsible for monitoring, analyzing, and investigating cyberattacks to determine their causes. PSIRT operates a vulnerability information management system and a permanently open reporting channel (psirt-info[at]mlsig.jp.nec.com), and publishes response information under an early warning partnership with JPCERT/CC and other organizations. We have also established a framework for collaboration between the cybersecurity department and the information security administrators in each business division.
- We comply with the NIST Cybersecurity Framework 2.0, ISO/IEC 27001, and the “Cybersecurity Management Guidelines Ver. 3.0.” We conduct quarterly (four times a year) vulnerability assessments, review countermeasures twice a year at information security strategy meetings, and perform regular cyber risk assessments by a Red Team.
- We have implemented multi-factor authentication, passwordless authentication, EDR/NDR, DLP, and file encryption company-wide based on the Zero Trust Model (CISA Maturity Model).

2. Security Measures for AI (Security for AI)

- We are systematically advancing our efforts along three pillars: “Governance (Establishing Policies and Rules),” “Management (Reviewing and visualizing compliance requirements),” and “Security Infrastructure (AI Asset Detection = Shadow AI Detection, AI Vulnerability Assessments and Audits, AI Guardrails).”
- Referencing Japan AISI’s “Guide to Red Teaming Methodology on AI Safety” and the OWASP AI Testing Guide, we conduct verification of attack scenarios—such as prompt injection (direct and indirect) and jailbreak—in a controlled, isolated environment, while also performing penetration testing on systems, including large language models (LLMs). Additionally, we have set the automation of attack diagnostics by the AI Red Team as one of our key objectives.
- For “NEC Generative AI Service,” used internally, we have implemented prompt input restrictions based on information confidentiality classifications, as well as a system that logs all input and output in a manner that allows for continuous auditing.
- The mandatory cybersecurity checklist includes items specific to AI systems, and we are implementing the necessary measures for each project.

3. Special Protective Measures for Highly Confidential and Valuable AI Assets (Training Data, Models, Inference Environments, etc.)

- Sensitive AI assets (such as data, model weights, and inference environments) are managed using secure storage (access control, encryption, and audit trail management) and are provided in on-premises or dedicated cloud environments within a dedicated data center. This ensures that access to high-value AI assets is restricted to a controlled environment, including through secure, private connections to public clouds.
- We are working to ensure confidentiality at the hardware level by running “cotomi” inference on a confidential computing environment (using a Trusted Execution Environment, or TEE).

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
- Other(s) (please specify): Assigns CVE numbers as a CNA (CVE Numbering Authority)
- Defined escalation criteria and follow-on actions for identified vulnerabilities (e.g., for external reporting or information sharing)
- Recognition of external finders of confirmed risks or vulnerabilities

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
- Monitoring and emergency controls specific to agentic AI systems (e.g., ability to interrupt autonomous action sequences, override tool-use permissions, or revoke delegated authority)
- Other(s) (please specify): We regularly review logs to verify that there has been no unauthorized access or unauthorized activity. If an incident occurs that is suspected to be a security incident, we report it to the NEC Group Information Security Incident Response Desk. We also share case studies of security incidents with the information security administrators in each business division, and by sharing details regarding the causes and countermeasures, we strive to prevent similar incidents from occurring.

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

- Other (specify): We refer to the OWASP Top 10 for Agentic Applications and organize and implement practical measures within the company's AI-driven development team to address risks such as agent goal hijacking and tool misuse.

Please provide any further comments and implementation documentation.

No answer provided

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.

1. AI and Human Rights Principles, and ESG-Related Public Documents

These are our publicly available documents regarding our policy on respecting human rights in the use of AI, our governance framework, and our overall ESG (Environmental, Social, and Governance) initiatives.

- **NEC Group AI and Human Rights Principles** <https://www.nec.com/en/press/201904/images/0201-01-01.pdf>
- **NEC ESG Databook 2026:** https://www.nec.com/en/press/202609/global_20260914_01.html

2. Technical documentation for NEC Generative AI Cloud (SaaS)

Publicly available technical documentation for NEC Generative AI Cloud (SaaS) is published in Japanese at:

<https://docs.genai-api.nec-cloud.com/> (Japanese)

The documentation includes:

- **Notes and Limitations** — describes service performance and functional limitations, operational considerations, and usage restrictions:
<https://docs.genai-api.nec-cloud.com/user-guide/common/%E6%B3%A8%E6%84%8F%E5%88%B6%E9%99%90%E4%BA%8B%E9%A0%85.pdf>
- **Generative AI Cloud (SaaS) Service Specification** — describes the service scope, functions, and service conditions:
[https://docs.genai-api.nec-cloud.com/contract/Generative%20AI%20Cloud%20\(SaaS\)%20%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9%E4%BB%95%E6%A7%95.pdf](https://docs.genai-api.nec-cloud.com/contract/Generative%20AI%20Cloud%20(SaaS)%20%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9%E4%BB%95%E6%A7%95.pdf)
- **Available LLMs** — identifies supported LLMs and relevant model information:
<https://docs.genai-api.nec-cloud.com/user-guide/management/%E5%88%A9%E7%94%A8%E5%8F%AF%E8%83%BD%E3%81%AALLM.pdf>
- **Generative AI Cloud (SaaS) API and OpenAI-Compatible API** — provide API specifications, technical instructions, and error information:
<https://docs.genai-api.nec-cloud.com/user-guide/development/api/genai-api.html>
<https://docs.genai-api.nec-cloud.com/user-guide/development/api/genai-oai-api.html>

The documents provide technical documentation and instructions for use, including information on service capabilities, usage limitations, available models, guardrail configuration, and answer-grounding verification. They do not constitute public summaries of safety, security, societal-risk evaluations, or red-teaming results.

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.

We share and disclose information through channels and in formats appropriate to the nature and needs of the relevant stakeholders.

1. Sharing and explaining information to individual customers and providing easy-to-understand summaries

- It is our standard practice to report and explain the evaluation results and risks associated with our AI systems to individual customers, and we implement improvements when issues are identified. However, the specific content, scope, and frequency of this information sharing constitute confidential business information and are therefore not disclosed to the general public.
- We prepare explanatory brochures for non-technical personnel and a broad audience for each relevant project to ensure that policies and practices can be smoothly shared and confirmed with our customers.

2. Presentation of various reports to general shareholders, investors, and the general public

3. Sharing Insights with the Government, Industry Associations, and the Academic and Expert Communities

- Through our participation as members of study groups and committees established by various government ministries and agencies, we share and provide insights on risk management and governance.
- We participate in activities organized by industry associations and share the results of pilot tests of assessment tools as well as feedback.
- Through joint research with various universities and research institutions, as well as participation in academic conferences, we share specialized expertise on advanced risk management and governance.

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.

1. Company-wide Privacy Policy and Detailed Guidelines for Handling Personal Information

This is a publicly available policy that sets forth the company-wide principles for handling personal information, as well as specific procedures and security measures at each stage—including collection, use, storage, disclosure, and deletion.

- **About our privacy practices:** <https://jpn.nec.com/site/privacy/en/privacy.html>
- **Global Privacy Notice:** <https://group.nec/global/en/site/privacy/>

2. Additional Notes Regarding the Documentation for the Generative AI “cotomi”

The API service specifications for the generative AI “cotomi” are a document designated exclusively for contract holders and explicitly labeled as a “Confidential Document” within the document itself; therefore, they are not included in this draft response as part of the publicly available 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?

- Protected information sharing
- Other (specify): A system for providing information on a case-by-case basis in response to requests from customers or other parties

Please provide links to any publicly available information.

As a general rule, our company does not publicly disclose information regarding the data sources used to train our AI systems; instead, we provide appropriate information on a case-by-case basis in response to requests from customers or other stakeholders.

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

Yes

If yes, describe additional method(s), including where relevant transparency measures related to AI agents

We ensure transparency through the following methods.

1. Commitment to Accountability and Sharing with Customers

- In the “NEC Group AI and Human Rights Principles,” we are committed to establishing a system that enables explanations of decision outcomes.

2. The ability to verify output in real time using technical means

- We offer a feature designed to combat hallucinations by comparing and identifying the output of generative AI with the source data on which it is based, on a sentence-by-sentence basis, and displaying the results in real time along with their sources. This enables users to independently verify the validity of AI-generated content.

3. Objective verification and dialogue through academic publication and external advisory bodies

- We publish research findings—such as technologies for analyzing disinformation and misinformation—as papers at peer-reviewed international conferences, such as the AAAI (Association for the Advancement of Artificial Intelligence), thereby making the technical details publicly available for verification by external experts.

4. Future Transparency Measures Regarding Customer Service Operations and AI Agents

- For each customer to whom we provide AI systems, we incorporate an operational process that involves providing regular reports and explanations as part of our standard customer support and contract management procedures, and implementing improvements when issues arise.
- We are currently exploring ways to collaborate with external stakeholders on transparency mechanisms specifically designed for AI systems (particularly AI agents), and we plan to move forward with this initiative in the future.

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?

Yes

If yes, please provide links or describe the scope of insights published, including where relevant contributions to understanding AI adoption in specific sectors (e.g. public administration, education systems).

We have been publishing the “Survey on the Latest Trends and Changes in Digital Transformation” annually since 2023. The most recent 2026 edition provides statistical insights into the adoption status, areas of application, and concerns regarding AI agents, broken down by the manufacturing and non-manufacturing sectors.
<https://jpn.nec.com/dx/dx-report/2026.html> (Japanese)

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
- Independent advisory body
- Other (e.g., distributed / multi-institutional governance arrangement) (please specify): Specialized Organization for AI Governance

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).

We have integrated AI governance into our internal control framework. Under the direction of the Risk Control and Compliance Committee, the AI Governance Officer is responsible for implementing AI governance.

Under this framework, the dedicated AI governance department is responsible for implementing internal rules and guidelines to ensure that business activities related to the use and application of AI respect human rights. The corporate department, which handles risk management, collaborates with the business units responsible for products, services, and delivery.

1. Decision-Making Authority (Routine Matters)

The AI Governance Officer bears primary responsibility for the day-to-day implementation of AI governance.

2. Decision-making Authority (Important Matters)

The Risk Control and Compliance Committee deliberates on and decides key policy matters regarding AI risks.

3. Advisory Authority (Advisory)

An advisory council composed of external experts with specialized knowledge in legal systems, human rights, privacy, and ethics will provide advice to the AI Governance Officer. The council itself has no decision-making authority.

4. Frequency of Policy Reviews

The company-wide risk map, which includes AI risks, is updated quarterly following deliberation by the Risk Control and Compliance Committee and is regularly reported to the Board of Directors. In addition, as necessary, changes to regulations and other policies overseen by the corporate functions, as well as significant updates to internal systems, are implemented and reported to the appropriate senior management.

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).

We conduct the following training for executives and employees (including temporary and contract workers) on AI governance policies and AI risk management practices.

1. Regular Training

We conduct an annual online training program for all employees to learn about the importance of AI technology and AI ethics, trends in relevant laws and regulations, human rights and privacy considerations associated with the use of AI, and the content and implementation of the "NEC Group AI and Human Rights Principles." The completion rate in fiscal year 2026 was 95.6%.

2. In-House Seminar

We conduct in-house seminars for business personnel involved in advancing our AI initiatives. We invite external experts to serve as instructors and, using examples of cases that have faced public criticism and other case studies, provide concrete guidance on key considerations and appropriate responses when deploying AI. Additionally, starting in fiscal year 2021, we have been holding seminars led by external experts for senior management to deepen their understanding of international trends regarding AI and human rights, enabling them to make business decisions that respect human rights.

3. AI Literacy Education

We are offering the "BluStellar Academy for AI"—a program that teaches participants about how data and AI are being used across a growing range of areas in society, the proper handling of data, and key considerations for utilizing AI—to both employees and external participants.

4. Channels for Reporting Concerns

Concerns regarding AI governance and AI-related risks can be reported through a general compliance hotline available to all executives and employees, and confidentiality and whistleblower protection are guaranteed.

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.

We have made our Security Incident Response Manual available company-wide and are implementing response measures in accordance with this manual. We have established the NEC Group Information Security Incident Response Desk, which receives and manages reports of security incidents. The desk includes experts from the Security, Legal, and Public Relations departments, among others, who provide advice on response measures from a variety of perspectives.

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).

We share research findings and best practices regarding the response to and management of AI risks widely with society and the industry.

1. Public dissemination of practical insights through technical publications and blogs

- We regularly publish information on the latest trends in AI governance, AI standardization, and rule-making; measures to address hallucinations in generative AI and guardrail technologies; technical insights aimed at developing safer large language models (LLMs); and know-how regarding training data management and quality assurance.
- Through media channels operated by NEC, we continuously publish and share practical best practices from a practitioner's perspective, including AI red teaming methodologies and verification results; practitioner-led explanations of the "Guide to Red Teaming Methodology on AI Safety"; prompt injection testing and countermeasures; challenges related to AI jailbreaking and multilingual attacks; and security risks specific to AI agents—based on the OWASP "Top 10 for Agentic Applications"—along with our company's practical countermeasures.

2. Presentation of Research Findings at Academic Conferences and International Conferences

- Our research findings on technologies for analyzing disinformation and misinformation were accepted by the AAAI Conference on Artificial Intelligence (AAAI 2025), and we have published the results following a rigorous peer-review process.
- We share our expert insights on AI risk management through participation in various academic conferences and presentations at the “AI Conference” organized by the European standards body ETSI.

3. Contributions to international standardization organizations and leadership in standard-setting

- **ISO/IEC JTC1/SC42 (AI)**: we serve as a member of the national technical committee.
- **IEEE (U.S.)**: We led the AI Ethics Project “P7001.”
- **European ETSI**: Through our work as a member of the Board of Directors and Vice Chair of the AI Coordination Group (OCG-AI), we are engaged in collaboration with the international standardization community and in the development of standards.
- **ITU-T**: Telecommunication Standardization Advisory Group (TSAG) Vice-chair

4. Collaboration with other sectors, industry-academia consortia, etc.

- We participated in Japan AISI's “AI Safety Evaluation Environment Task Force” and shared the results of pilot testing of evaluation tools. We also joined the “Business Demonstration Working Group” alongside major domestic and international companies to share our initiatives related to AI safety and security.
- We participated in an industry-academia consortium comprising a total of nine organizations, including the National Institute of Informatics (NII), and promoted the joint development of a platform to combat disinformation and misinformation.
- We participate in the Information Security Early Warning Partnership and contribute to the cross-industry sharing of vulnerability-related information.

5. Joint Research with Academic Institutions and Universities

- Through joint research with the Keio University Global Research Institute (KGRI) and the Institute for Future Initiatives, The University of Tokyo, as well as through interdisciplinary industry-academia collaboration projects, we are advancing studies on the ethics, legal frameworks, and risk management related to AI, and we widely share the results of this research at symposia and other events.

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:

- ISO/IEC standards (e.g., ISO/IEC 27001, ISO/IEC 42001)
- NIST AI Risk Management Framework (AI RMF)
- OECD AI Principles
- Industry-led best practices or codes of conduct
- Other international or regional standards (please specify): Hiroshima Process International Code of Conduct, EU AI Act, OWASP Top 10 for Agentic Applications, Japanese Guidelines

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

In our AI Risk Management and Governance Policy, we utilize the following international technical standards and best practices.

1. ISO/IEC

Several divisions and group companies within the NEC Group have obtained and maintained ISO/IEC 27001 certification and utilize it as a risk assessment and management process for information assets, including AI systems. In addition, NEC serves as a member of the domestic technical committee within the ISO/IEC JTC1/SC42 (AI) committee.

2. NIST AI Risk Management Framework□AI RMF□

As part of the “Security for AI” initiative, we are utilizing the NIST AI RMF as our core framework and mapping compliance requirements under the EU AI Act and the AI Guidelines for Business to the NIST AI RMF to advance the scrutiny and visualization of AI governance compliance.

3. OECD AI Principles

The “NEC Group AI and Human Rights Principles,” formulated in 2019, was developed with reference to the OECD AI Principles, the Trustworthy AI Guidelines of the EU High-Level Expert Group, and Japan's “Social Principles of Human-Centric AI.”

4. Hiroshima Process International Code of Conduct

Taking into account the Hiroshima Process International Code of Conduct, we have incorporated its principles on AI risk management and governance, including participation in this reporting framework.

5. EU AI Act

As part of the “Security for AI” initiative, we are compiling the compliance requirements under the EU AI Act and mapping them to our AI governance framework, in conjunction with the NIST AI RMF and the AI Guidelines for Business.

6. OWASP Top 10 for Agentic Applications

When addressing security risks associated with AI agents, we refer to the “Top 10 for Agentic Applications” published by OWASP and incorporate these guidelines into our company’s development practices, such as restricting the execution of destructive or irreversible commands and implementing human verification and approval processes.

7. AI Guidelines for Business

Based on the principles of the “AI Guidelines for Business,” we are continuously reviewing our risk assessments, internal policies, and the implementation of countermeasures.

8. Machine Learning Quality Management Guidelines (AIQM)

We are utilizing these guidelines in the development of our internal “NEC AI Quality Guidelines” and have incorporated them as a framework for quality and risk management throughout the entire lifecycle of AI systems.

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?

- User disclosure (e.g., text notice, verbal statement, or system label)
- Documentation or FAQs explaining when and how AI is used in the system
- Other (specify): End User License Agreements (EULAs) provided for each AI system

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).

We implement various approaches, such as explicitly stating the service name, providing notification through the EULA (End User License Agreement), and offering advance explanations in B2B transactions.

For the automated response services we provide, such as AI chatbots, we explicitly include “AI” in the service name itself. This ensures that when users interact with the service, they can intuitively recognize and understand that they are communicating with an automated response system.

We have developed and made available an End User License Agreement (EULA) for each AI system, and we provide the necessary notifications to users and obtain their consent through these agreements and terms of use.

We primarily operate a B2B (business-to-business) business, and we provide advance explanations to client companies that implement and use our services, with the expectation that they will understand and grasp the extent of AI involvement and the terms of operation.

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?

- Detection tool(s) for hidden provenance signals (e.g., watermark or metadata checks)
- Other (specify): Advance explanations to client companies in B2B businesses (disclosure on a contract- or project-by-project basis)

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

Not applicable

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.

We are implementing this as follows:

1. Measures for B2B businesses

- Since our AI-related businesses are primarily B2B (business-to-business), our operations and contracts regarding content generated by generative AI are based on the premise that we provide advance explanations to the customer companies using such content.

2. Investment in research and development of content authenticity verification and misinformation detection technologies

- We are continuously investing in research and development at research institutes both in Japan and abroad, focusing on technologies such as the detection of fake and misleading information, fact-checking support, the detection of AI-generated content, and the multifaceted analysis of the authenticity of information spreading on social media and other platforms.
- We have independently developed technology that compares the output of generative AI with the source data to detect and highlight in real time any passages that may contain unfounded content (hallucinations), and we began offering this service at the end of October 2024.
- To determine whether content created by third parties has been generated or modified by AI, we are developing technology to assess and analyze text, images, videos, and audio to identify whether they have been generated or modified.

3. Government Demonstration Projects and Collaboration with External Organizations and Industry-Academia Consortia

- Following our selection for the Ministry of Internal Affairs and Communications' "Project for the Development and Demonstration of Technologies to Counter Fake and Misinformation on the Internet," we are promoting the development and demonstration of technologies for verifying content authenticity and analyzing fake and misinformation.
- We are collaborating with the Japan Fact-Check Center, broadcasters, and other mass media organizations to verify the effectiveness and validity of the detection and analysis technologies we have developed.
- We participated in an industry-academia consortium comprising a total of nine organizations, including the National Institute of Informatics (NII), and promoted the joint development of a platform to combat disinformation and misinformation.

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.

We are promoting research and investment in a multifaceted manner across our domestic and international R&D divisions, as well as our cybersecurity division.

1. Security

- In the cybersecurity division, we assess our compliance with international security frameworks, such as the NIST Cybersecurity Framework (CSF), and implement policies and measures accordingly.

2. Safety

- We are participating in Japan AISI's "AI Safety Evaluation Environment Task Force" and are conducting pilot tests of assessment tools and providing feedback on our findings (the results are shared as part of our collaboration with Japan AISI).

3. Data quality, fairness & representativeness

- Regarding the training data for the generative AI "cotomi," we have independently developed a multi-stage data cleansing technology that utilizes both rule-based and learning-based filtering, and have published the technical details in the NEC Technical Journal.

<https://www.nec.com/en/global/techrep/journal/g23/n02/230212.html>

- We are advancing research on test data and experimental programs for bias detection and ensuring fairness, and we utilize an in-house bias detection dataset in our AI quality inspections prior to shipment. In addition, through collaboration with partner companies, we are working to implement mechanisms to check for harmful biases in AI and guardrails to detect biases in AI outputs.

4. Information integrity

- Under a demonstration project selected by the Ministry of Internal Affairs and Communications, we developed technology for analyzing fake and misleading information, presented a paper on the topic at the international conference “AAAI 2025” (publicly available), and engaged in joint development and information sharing (among partners) through an industry-academia consortium that included the National Institute of Informatics (NII) and others.
<https://www.nec.com/en/global/rd/technologies/202511/index.html>
https://www.nec.com/en/press/202410/global_20241016_01.html
- We are continuously investing in fact-checking support technologies that analyze the accuracy of information shared on social media and other platforms, as well as technologies for detecting misinformation in AI-generated outputs.
https://www.nec.com/en/press/202409/global_20240913_01.html

5. System performance & outcomes

- Regarding “cotomi”’s Japanese conversational capabilities, we have demonstrated through comparative evaluations (Rakuda, etc.) that it outperforms top-tier LLMs both in Japan and internationally, and we have made these results publicly available in a press release and technical documentation.
<https://www.nec.com/en/global/techrep/journal/g23/n02/230212.html>

6. Explainability or interpretability

- We have developed technologies such as the “LLM Explainer,” which cross-checks and compares generative AI outputs with source data sentence by sentence and presents the results with supporting evidence in real time. We publish our research findings on the NEC Research and Development website and other platforms.
<https://www.nec.com/en/global/techrep/journal/g25/n01/250108.html>

7. Transparency

- We have published our technology related to methods for collecting and cleaning training data in the NEC Technical Journal.
<https://www.nec.com/en/global/techrep/journal/g23/n02/230212.html>
- We are conducting ongoing research on a global scale—primarily through our in-house global research institute—into technologies such as the detection of misinformation, fact-checking, and the detection of AI-generated content.

8. Robustness, reliability

- We have conducted verification tests on “highly secure federated learning” technology—which combines secure computation and federated learning—as well as guardrail technologies for LLM-embedded systems (such as NeMo Guardrails), and have published the results on our technical blog.
<https://jpn.nec.com/cybersecurity/blog/250805/index.html> (Japanese)
<https://www.nec.com/en/global/techrep/journal/g23/n02/230215.html>
- We conduct red teaming as part of the suitability assessment when model systems transition beyond the development phase. In addition to requiring or recommending that the in-house security team perform vulnerability assessments and penetration tests (self-assessments) on developers, we also conduct third-party penetration tests performed by a group company’s specialized security team that is independent of the development project.

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.

We are promoting ongoing research and investment initiatives in the development, implementation, and utilization of AI.

1. Initiatives Related to Socioeconomic Considerations

- We run the “Tiger’s Den” program, which is designed for selected employees—including those with no prior experience in AI—to acquire AI skills and achieve tangible results over the course of one month.
<https://www.nec-businessintelligence.co.jp/initiative/digital-transformation.html> (Japanese)
- In addition to fostering digital transformation (DX) skills among all employees through our hands-on AI training program, “Reskilling Camp,” we continue to provide training to improve AI and large language model (LLM) literacy.
<https://www.persol-innovation.co.jp/news/2025-1128-1> (Japanese)
- Within the “Corporate AI & Workforce Division,” established in August 2026, we are operating an autonomous organization in which AI handles every role—from division head to staff—and are advancing our own pilot projects and research on the optimal allocation of human capital and AI capital. We plan to share the insights gained from this

initiative with external parties and other organizations.

https://jpn.nec.com/press/202608/20260810_01.html (Japanese)

- In addition to training AI professionals capable of solving social issues through the “BluStellar Academy for AI,” we offer advanced specialized training programs for external participants. We also implement initiatives to improve AI literacy through industry-academia collaboration programs.
<https://jpn.nec.com/nec-academy/index.html> (Japanese)
- We publish an annual report titled “Survey on the Latest Trends and Changes in Digital Transformation,” which examines corporate trends in the adoption of AI and AI agents, their use across various industries, and related concerns, providing statistical insights into their social impact.
<https://group.nec.jp/ja/solutions/nec-blustellar/thoughtleadership/dx-report202604> (Japanese)
- At the IISE FORUM 2026, an event organized by our group company, the Institute for International Socio-Economic Studies (IISE), the central theme was “A Future Society Co-created with AI—A Day Where Global Knowledge Converges.” In addition to keynote speeches on the cutting edge of AI investment, the forum featured discussions on the implications of an AI-native society for the economy, business management, and humanity. The environmental session, titled “AI-Driven Environmental Digitalization: Transforming Decision-Making and Markets,” featured participation from our company’s supply chain and sustainability staff.
https://www.i-ise.com/jp/information/symposium/2026/sym_iise-forum2026_abstracts.html (Japanese)

2. Initiatives Related to Environmental Considerations

- With a focus on decarbonization and reducing environmental impact, we develop and provide AI models with lightweight configurations that minimize the consumption of computational resources.
- For our in-house generative AI, “cotomi,” we have developed technology that maximizes performance while improving GPU computational efficiency, thereby helping to reduce power consumption during AI use and lower our customers’ Scope 3 emissions.
<https://group.nec/assets/global/en/about/ir/library/pdf/250217/250217-01.pdf>
- We operate the “NEC Kanagawa Data Center Phase 2” and the “NEC Kobe Data Center Phase 3,” both of which run on 100% renewable energy, thereby reducing the environmental impact of our infrastructure.
<https://www.nec.com/en/global/techrep/journal/g24/n01/240113.html>
- We are participating in the “Green Innovation Fund Project/Construction of Next Generation Digital Infrastructure” run by the New Energy and Industrial Technology Development Organization (NEDO) and aim to achieve dramatic energy savings across the entire data center by developing technology for the dynamic, optimal allocation of computing resources using AI inference.
https://jpn.nec.com/press/202202/20220225_04.html (Japanese)

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.

We are implementing a wide range of initiatives to improve digital literacy.

1. User Education and Public AI Education Programs

- In addition to cultivating AI professionals capable of addressing social issues through the “BluStellar Academy for AI,” we provide advanced specialized training to a wide range of organizations, including the general public, corporations, local governments, and universities.

2. Collaboration with Schools, Universities, and Higher Education Institutions

- In March 2026, we signed an industry-academia collaboration agreement with the University of Tokyo and established the “NEC-UTokyo Lab,” where we are promoting dialogue, social collaboration programs, and the development of next-generation leaders with the aim of realizing a trustworthy society that coexists with AI.
https://www.nec.com/en/press/202603/global_20260317_01.html
- We have established the “World Model and Simulator Endowed Chair” (July 2021–June 2026) at the Graduate School of Engineering, The University of Tokyo, and are working to cultivate the next generation of AI talent through the study of deep learning technologies.
https://www.u-tokyo.ac.jp/adm/uci/en/projects/ai/project_00051.html

- Through the “Data Science Endowed Chair” (established in April 2021) at the University of Toyama, we are promoting the development of professionals who will contribute to solving regional challenges and fostering new industries.
<https://www.eco.u-toyama.ac.jp/en/education/data-science.html>
- Since July 2020, we have been offering a “PBL (Project-Based Learning) Implementation Program” for faculty members and teaching assistants at universities and technical colleges, and we are providing educational support with the goal of expanding the program to 70 institutions in Japan over the next three years.
<https://group.nec.jp/ja/solutions/cybersecurity/topics/250702> (Japanese)
- In addition to hosting free seminars for university staff to introduce AI literacy education curricula, we are promoting the development of AI talent and collaboration with data science departments through industry-academia partnerships with the University of Tokyo, Keio University, Osaka University, and others.
<https://jpn.nec.com/nec-academy/service-university/> (Japanese)

3. Local and Community Workshops and Social Contributions

- In collaboration with the Waseda University Career Research Society, we held a hands-on problem-solving workshop for college students that utilized generative AI (September 2025). Conducted as part of the “NEC Pro Bono Initiative,” in which our Group employees work to solve social issues faced by local governments, NPOs, social entrepreneurs, educational institutions, and others, this program contributes to improving digital literacy throughout the community.
https://www.nec.com/en/global/community/resources/business_supporter.html

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.

We are promoting projects that utilize AI technology to achieve social and public benefits through collaboration with international organizations, local governments, universities, NPOs, and other entities.

1. Collaboration with International Organizations

- In collaboration with the Cambodian Mine Action Center, we successfully used AI to predict the locations of remaining landmine-contaminated areas.
https://www.nec.com/en/press/202510/global_20251029_04.html
- We are strengthening our partnership with the United Nations World Food Programme (WFP) to promote collaboration in the fields of humanitarian aid and food assistance.
https://www.nec.com/en/press/202508/global_20250820_01.html
- We signed a memorandum of understanding with the United Nations Industrial Development Organization (UNIDO) on inclusive and sustainable industrial development through the use of advanced ICTs in developing countries (TICAD 7, 2019).
<https://www.nec.com/en/global/sdgs/innovators/partnership/index.html>
- Together with Gavi and Simprints, we verified the effectiveness of fingerprint recognition technology for young children as a means of promoting vaccine uptake.
https://www.nec.com/en/press/201906/global_20190606_01.html
- In collaboration with Nagasaki University, we supported efforts to improve maternal and child health care information in Kenya.
https://www.nec.com/en/press/201904/global_20190418_01.html

2. Collaboration with Local Governments and Community Groups

- Starting in February 2024, we began offering an “Evacuation Action Support Service” aimed at ensuring that no “disaster-vulnerable individuals”—such as the elderly and people with disabilities who have difficulty evacuating on their own—are left behind, and we are promoting collaboration between local governments and community groups.
<https://www.nec.com/en/global/corporateblog/202402/01.html>

3. Collaboration with NPOs and Social Entrepreneurs

- In fiscal year 2025, we carried out various initiatives, including providing planning and operational support for a local project to assist families with children in collaboration with Fukushima Prefecture; hosting the inaugural “Kawasaki Pro Bono Summit” in partnership with Kawasaki City, Senshu University, and others; supporting a workshop on solving social issues through the use of generative AI in collaboration with the Waseda University Career Research Society; and providing STEAM education support (including hosting children’s programming classes) in partnership with Minato Children’s Cafeteria.
<https://jpn.nec.com/community/ja/report/007.html> (Japanese)
<https://jpn.nec.com/corporateblog/202609/03.html> (Japanese)
https://www.nec.com/en/global/community/resources/business_supporter.html
<https://jpn.nec.com/corporateblog/202412/03.html> (Japanese)

Any further comments and implementation documentation.

No answer provided