

JUN 09 2026

JOINT MEMORANDUM CIRCULAR NO. 003
Series of 2026

SUBJECT : PRINCIPLES FOR THE ETHICAL AND RESPONSIBLE DEVELOPMENT, DEPLOYMENT, AND USE OF ARTIFICIAL INTELLIGENCE (AI) IN THE GOVERNMENT

WHEREAS, Section 24, Article II of the 1987 Philippine Constitution expressly mandates that the State shall recognize the vital role of communication and information in nation-building;

WHEREAS, pursuant to Section 3, Article IX-B of the 1987 Philippine Constitution and Executive Order No. 292, otherwise known as the Administrative Code of 1987, the Civil Service Commission (CSC), as the central personnel agency of the Government, is constitutionally mandated to establish a career service and to adopt measures to promote morale, efficiency, integrity, responsiveness, progressiveness, and courtesy in the Civil Service;

WHEREAS, the CSC has the authority to prescribe, amend, and enforce rules and regulations necessary to carry out its mandate and to institutionalize a management climate conducive to public accountability and effective personnel administration;

WHEREAS, Section 6(I)(a) of Republic Act (R.A.) No. 10844 or the Department of Information and Communications Technology (DICT) Act of 2015 mandates the DICT to formulate, recommend, and implement national policies, plans, programs, and guidelines that will promote the development and use of ICT with due consideration to the advantages of convergence and emerging technologies;¹

WHEREAS, R.A. No. 10173 or the Data Privacy Act of 2012 declares the policy of the State to protect the fundamental human right of privacy of communication while ensuring a free flow of information to promote innovation and growth.² Further, the National Privacy Commission issued NPC Advisory No. 2024-04 to prescribe guidelines on the application of

¹ See An Act Creating the Department of Information and Communications Technology, defining its powers and functions appropriating funds therefor, and for other purposes [DICT Act of 2015], Republic Act No. 10844 § 6 (I) (a) (2016).

² See An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

R.A. No. 10173, its Implementing Rules and Regulations (IRR), and other issuances of NPC to AI systems processing personal information;³

WHEREAS, the rapid advancement of artificial intelligence (AI) offers significant opportunities across various sectors but also presents substantial risks that require responsible governance;

WHEREAS, the United Nations General Assembly adopted the Resolution on “Seizing the opportunities of safe, secure, and trustworthy artificial intelligence systems for sustainable development,” which establishes consensus on the responsible use and development of AI systems and recognizes its potential to accelerate progress towards sustainable development;⁴

WHEREAS, the Philippines, as a member-state of the United Nations Educational, Scientific and Cultural Organization (UNESCO), conforms with the Recommendation on the Ethics of Artificial Intelligence as adopted in November 2021 at the 41st UNESCO General Conference, in ensuring that AI is aligned with human rights, human well-being, and sustainable development;

WHEREAS, the Philippines, as an active member of the International Telecommunication Union (ITU), supports the implementation of AI for Good, which is the United Nations’ leading global and inclusive platform dedicated to identifying and scaling practical AI solutions that advance the Sustainable Development Goals for worldwide impact;⁵

WHEREAS, the Philippines is a signatory to the Bletchley Declaration, where the signatories affirm that AI should be designed, developed, deployed, and used in a safe human-centric, trustworthy, and responsible manner, for the benefit of all;⁶

WHEREAS, the Philippines, as a member-state of the Association of Southeast Asian Nations (ASEAN), adopted the ASEAN Guide on AI Governance and Ethics, which serves as a practical guide for regional organizations seeking to design, develop, and deploy traditional AI technologies in commercial, non-military, or dual-use applications, emphasizing alignment within ASEAN, fostering interoperability of AI frameworks across jurisdictions, and providing recommendations for national and regional initiatives to ensure the responsible development and deployment of AI systems;⁷

³ See National Privacy Commission, Advisory No. 2024-04 on Guidelines On The Application Of Republic Act No. 10173 or The Data Privacy Act Of 2012 (DPA), Its Implementing Rules And Regulations, And The Issuances Of The Commission To Artificial Intelligence Systems Processing Personal Data [NPC Advisory no. 2024-04], available at <https://privacy.gov.ph/wp-content/uploads/2025/02/Advisory-2024.12.19-Guidelines-on-Artificial-Intelligence-w-SGD.pdf>

⁴ See United Nations (UN) General Assembly, Resolution on “Seizing the opportunities of safe, secure, and trustworthy artificial intelligence systems for sustainable development”, available at <https://digitallibrary.un.org/record/4040897?ln=en&v=pdf>

⁵ See International Telecommunications Union (ITU), “AI for Good” (2023), available at <https://aiforgood.itu.int/about-ai-for-good/>

⁶ See Bletchley Declaration - AI Safety Summit (2023), available at <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>.

⁷ See Association of Southeast Asian Nations (ASEAN), “AI Guide on Governance and Ethics” [ASEAN AI Guide], available at https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf (2024)

WHEREAS, in 2024, the Philippines, together with other participating nations, signed the AI Seoul Ministerial Statement and affirmed its commitment to collaboratively develop policies that guide the design, development, deployment, and application of artificial intelligence to ensure safe, inclusive, innovative, and trustworthy AI systems that maximize societal benefits;⁸

WHEREAS, it is essential to establish guiding principles that ensure the ethical, justified, and proportionate use of AI systems, consistent with applicable laws and societal values, to promote accountability and safeguard positive outcomes; and

WHEREAS, the DICT and the CSC, in line with their respective mandates and in recognition of the need for ethical and responsible governance of artificial intelligence, hereby adopt the following principles to guide the ethical and responsible development, including its training and testing, deployment, and use of AI systems in government;

NOW, THEREFORE, pursuant to the foregoing, the DICT and the CSC hereby promulgate the following:

SECTION 1. TITLE. — This Joint Memorandum Circular (JMC) shall be known as the *“Principles for the Ethical and Responsible Development, Deployment and Use of Artificial Intelligence (AI) in the Government”*.

SECTION 2. PURPOSE. — This JMC is being issued to adopt the fundamental principles that shall establish a stable policy environment for an ethical and responsible development, deployment, and use of AI in the government.

SECTION 3. SCOPE. — This JMC shall apply to all government officials and employees in all government agencies and instrumentalities, namely: Constitutional Bodies; departments, bureaus, and agencies of the National Government; Government-Owned or -Controlled Corporations (GOCCs) with original charters; Local Government Units (LGUs); and State Universities and Colleges (SUCs), regardless of status of appointment (permanent, temporary, provisional, substitute, coterminous, casual, contractual, or fixed term).

Heads of offices and supervisors engaging individuals under job orders or contracts of service whose duties and functions may involve the use of artificial intelligence shall ensure that said individuals observe the principles set forth in this JMC. Compliance of such individuals shall be governed by the terms and conditions of their contracts, consistent with applicable rules.

⁸ See AI Seoul Summit Ministerial Statement - AI Seoul Summit (2024), available at <https://www.gov.uk/government/publications/seoul-ministerial-statement-for-advancing-ai-safety-innovation-and-inclusivity-ai-seoul-summit-2024/seoul-ministerial-statement-for-advancing-ai-safety-innovation-and-inclusivity-ai-seoul-summit-2024>

SECTION 4. DEFINITION OF TERMS. — For purposes of this JMC, the following terms are defined:

- a. **Artificial Intelligence (AI)** refers to the branch of computer science devoted to developing data processing systems that perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement.⁹
- b. **AI System** refers to the engineered system that generates outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives.¹⁰

For the purpose of this policy, AI systems include, but are not limited to:

- i. Machine Learning and Deep Learning
 - ii. Generative AI Models
 - iii. Autonomous and adaptive systems
 - iv. Logic- and knowledge-based approaches; and
 - v. Emerging AI technologies or any future systems that meet the functional criteria of an AI system, regardless of the underlying architectural method
- c. **AI developer** refers to a unit within the government office that is concerned with the development, including training and testing of AI services and products.¹¹

For this policy, an AI developer shall also refer to the government office that outsourced the development of an AI system.

- d. **AI deployer** refers to a unit within the government office that implements, including training and testing, an AI system, which could either be developed by their in-house team or a third-party developer.¹²
- e. **AI user** refers to all government officials and employees covered by this JMC who “interact with an AI system or an AI-enabled service and can be affected by its decisions”¹³ in the course of delivering public services.
- f. **AI vendor** (or AI provider) refers to an organization or entity that provides products or services that use one or more AI systems. This encompasses AI platform providers, suppliers, manufacturers, distributors, consultants, and service providers of AI products or services.¹⁴

⁹ See . PNS ISO/IEC 2382:2018 - Information technology — Vocabulary available at [https://standardsph.dti.gov.ph/portal/catalogue/forms/3bece8a83efc5fe734c6e667acbfc495f488d65b2a1c23f88dbdafayoOuYnmzEZDTR034ColNPzW~3j2Rzff3~Z4gvKK1mlSl6GspPysabIF~1IcWZJMFUIb3thm1mF9WnNUpf7iLLsfEOhogqSDAZIsEZPSGEI2TjDWz6DiGlccSjuZvgpobW2eSozi7yzY8EZbtrgIfjd0AGnG9T69IGQCX4QGoFRgwn44RUiHmsU.XuEFH0PNQvXacwYtMBeCxUVecLLRVdMv2x.cFJKCXI5jZJlfrAVBScDUpzqq.sDnJGkC6KwRqTrlqAd3e4zT4ywqhCDxM81gJELi3eYA6TTed~44G8n600n545lh5Pe6iZ2IXrIs97tJAAkTEAgxNdryoUxWDA~/-](https://standardsph.dti.gov.ph/portal/catalogue/forms/3bece8a83efc5fe734c6e667acbfc495f488d65b2a1c23f88dbdafayoOuYnmzEZDTR034ColNPzW~3j2Rzff3~Z4gvKK1mlSl6GspPysabIF~1IcWZJMFUIb3thm1mF9WnNUpf7iLLsfEOhogqSDAZIsEZPSGEI2TjDWz6DiGlccSjuZvgpobW2eSozi7yzY8EZbtrgIfjd0AGnG9T69IGQCX4QGoFRgwn44RUiHmsU.XuEFH0PNQvXacwYtMBeCxUVecLLRVdMv2x.cFJKCXI5jZJlfrAVBScDUpzqq.sDnJGkC6KwRqTrlqAd3e4zT4ywqhCDxM81gJELi3eYA6TTed~44G8n600n545lh5Pe6iZ2IXrIs97tJAAkTEAgxNdryoUxWDA~/)

¹⁰ See PNS ISO/IEC 22989:2023 - Information technology — Artificial intelligence — Artificial intelligence concepts and terminology [PNS ISO/IEC 22989] 3.1.4, available at <https://standardsph.dti.gov.ph/>

¹¹ See *Id.* 5.19.3.2.

¹² See ASEAN AI Guide, p. 9.

¹³ See ASEAN AI Guide, p. 9.

¹⁴ See PNS ISO/IEC 22989 5.19.2.1.

- g. **Deceptive Design Patterns** refer to design techniques embedded in an analog or digital interface that aim to manipulate or deceive a data subject to perform a specific act relating to the processing of their personal data.¹⁵

SECTION 5. GENERAL AI PRINCIPLES. — The following general AI principles, as issued by the Organisation for Economic Co-operation and Development (OECD), UNESCO, and ASEAN, provide guidance on the development, including its training and testing, deployment, and use of AI systems in the government:

- a. **Proportionality and Do No Harm**¹⁶ – This principle, based on the UNESCO Recommendation on the Ethics of Artificial Intelligence, states that all AI systems shall neither cause nor exacerbate harm nor adversely affect human beings. AI developers, deployers, and users have the fundamental responsibility to develop, deploy, and use AI in ways that do not cause harm. In cases where potential harm cannot be fully ruled out, appropriate risk assessments shall be conducted, and proportionate safeguards shall be adopted by the concerned government offices to prevent or mitigate such harm.

In developing, deploying, or using AI systems for public service delivery, the following shall be observed:

1. The AI system shall be suitable for its intended purpose without exceeding the mandate and function of the concerned agency;
2. Under no circumstances shall it be used to violate or abuse human rights; and
3. The approach shall be grounded in sound scientific principles and evidence.

Further, the use of AI systems is strictly prohibited for activities that could infringe on privacy rights, abuse of power, or undermine citizens' freedom.

- b. **Human-centricity**¹⁷ – This principle, based on the ASEAN Guide on AI Governance and Ethics, states that AI systems shall respect human-centered values and pursue benefits for human society. It shall be developed for the common good and the benefit of society and humanity as a whole. Human-centricity shall be incorporated throughout the AI system lifecycle—from design to development to deployment and use. Actions shall be taken to understand the way AI users interact with the AI system, how it is perceived, and if there are any negative outcomes arising from its outputs. These actions may include, but are not limited to, user testing, feedback mechanisms, and post-deployment monitoring. AI shall not be used for malicious purposes or to sway or deceive users into making decisions that are not beneficial to them or society. With this, AI developers and AI deployers shall also ensure that deceptive design patterns are avoided.

¹⁵ See National Privacy Commission, Guidelines on Deceptive Design Patterns, Advisory No. 2023-01, series of 2023 [NPC Advisory No. 2023-01], § 2 (a) (07 November 2023).

¹⁶ See UNESCO, "Recommendation on the Ethics of Artificial Intelligence" [UNESCO Recommendation on AI Ethics] (2021), III.2 (25-26), p. 20, available at <https://unesdoc.unesco.org/ark:/48223/pf0000381137>

¹⁷ See ASEAN AI Guide, B (4), at 14

In situations where decisions may endanger human lives or pose irreversible damage or damage that is difficult to reverse, AI systems may be used to gather insights and obtain recommendations, but the final decision shall always be made by a human.

When the deployment and use of AI precipitate significant and demonstrable alterations to existing workflows, job functions, or conditions of employment, a formal consultation with all affected government personnel is important in order to come up with options for consideration by management and affected personnel.

- c. **Fairness and Non-Discrimination**¹⁸ – This principle, based on the UNESCO Recommendation on the Ethics of Artificial Intelligence, states that AI systems shall be developed and used in ways that are fair, transparent, and consistent, ensuring that the processes and outcomes do not discriminate against individuals or groups. Developers, deployers, and users of AI systems shall ensure that data is processed responsibly, avoiding manipulative or oppressive practices, and shall actively protect individuals from algorithmic discrimination and biases.

Moreover, appropriate safeguards and accountability measures, such as conducting bias audits and implementing mitigation strategies, as well as compliance with relevant laws and regulations, shall be in place. This is to ensure that the system's decisions are not discriminatory against or for particular groups or individuals based on sexual orientation, gender identity and expression, race, nationality, disability, political or religious beliefs, and others. This includes implementing mechanisms to detect, monitor, and eliminate bias throughout the lifecycle of the AI system.

Further, systemic bias, human bias, and statistical bias shall be considered when assessing or auditing the AI systems. AI systems shall respect multilingualism and cultural diversity, and are encouraged to feature locally relevant content.

- d. **Transparency and Explainability**¹⁹ – This principle, based on the UNESCO Recommendation on the Ethics of Artificial Intelligence, states that decisions generated by an AI system shall be explainable to the extent applicable, so that stakeholders may understand the factors that contributed to the AI systems' output and their corresponding accuracies and influences.

A clear and concise explanation regarding the purpose of such processing, the factors and inputs considered by the AI System, the risks and limitations identified, expected output and impact, and any applicable dispute mechanisms shall be available to the public relevant to the AI System.²⁰

Further, in accordance with the same advisory, all information communicated to stakeholders concerning the data processing activities of the AI system shall be readily accessible. Such information shall be concrete, definitive, and specifically adapted to be understood by the intended user, utilizing clear and plain language, with necessary

¹⁸ See UNESCO Recommendation on AI Ethics, III.2 (28-30), pp. 20-21.

¹⁹ See UNESCO Recommendation on AI Ethics, III.2 (37-40), p. 22.

²⁰ See NPC Advisory No. 2024-04, § 2 (a).

technical terminology retained only where essential for precision and accompanied by appropriate explanations where feasible.

- e. **Data Governance, Privacy, and Protection** – This principle, in accordance with the Data Privacy Act of 2012, its Implementing Rules and Regulations, and other pertinent issuances of the NPC, provides that all AI systems shall have built-in protections against abusive data practices, including conduct of privacy impact assessment prior to deployment and periodically thereafter.

For specific guidelines relevant to this principle, refer to Section 2 of NPC Advisory 2024-04.²¹

- f. **Responsibility and Accountability**²² – This principle, based on the UNESCO Recommendation on the Ethics of Artificial Intelligence, states that a responsible AI system must operate in accordance with clearly defined policies that specify accountability and assign responsibility for its outcomes. The AI developers and AI deployers shall be accountable for the development and deployment of AI systems and for the outcomes and consequences of such implementation. This accountability is imposed on the specific unit undertaking the development or deployment of the AI system, including its training and testing. When such processing is outsourced, the government agency that initiated the outsourcing shall remain accountable for the actions of its third-party developers.

AI systems shall not displace ultimate human responsibility and accountability.

- g. **Multistakeholder and adaptive governance and collaboration**²³ – This principle, adopted from the UNESCO Recommendation on the Ethics of Artificial Intelligence, states that participation of different stakeholders throughout the AI system life cycle is necessary for inclusive approaches to AI governance, enabling the benefits to be shared by all, and to contribute to sustainable development.

Stakeholders include, but are not limited to, government agencies, intergovernmental organizations, the technical community, civil society, researchers and academia, media, education, policymakers, private sector companies, human rights institutions and equality bodies, anti-discrimination monitoring bodies, and groups for youth and children.

The adoption of open standards and interoperability to facilitate collaboration shall be in place. Measures shall be adopted to consider shifts in technologies, the emergence of new groups of stakeholders, and to allow meaningful participation by marginalized groups, communities, and individuals.

²¹ See NPC Advisory No. 2024-04, § 2.

²² See UNESCO Recommendation on AI Ethics, III.2 (42-43), pp. 22-23.

²³ See UNESCO Recommendation on AI Ethics, III.2 (28-30), pp. 20-21.

- h. **Cyber Safety and Security** – Aligned with the National Cybersecurity Plan,²⁴ AI systems shall be protected from cybersecurity threats and risks that cause physical and digital harm.

AI systems shall demonstrate safety and effectiveness through adequate safeguards, such as, pre-deployment vulnerability assessment and penetration testing, risk identification and mitigation, privacy impact assessment, periodic cybersecurity audits, and other cybersecurity protocols. These measures are designed to align intended use cases, mitigate unsafe outcomes, and ensure adherence to internationally established standards.

- i. **Robustness and Reliability**²⁵ – This principle, based on the ASEAN Guide on AI Governance and Ethics, states that AI systems shall be sufficiently robust to cope with errors during execution and unexpected or erroneous input, or cope with stressful environmental conditions. It shall also perform consistently. AI systems shall, where possible, work reliably and have consistent results for a range of inputs and situations. It shall operate reliably and follow its intended purpose. The AI system needs to be resilient and secure to ensure that unintentional harm can be prevented. Measures such as proper documentation of data sources, testing, validation, and continuous monitoring are essential to uphold the reliability of AI technologies and systems.
- j. **Sustainability**²⁶ – This principle from the UNESCO Recommendation on the Ethics of Artificial Intelligence states that AI developers and deployers shall consider the environmental, social, and economic implications of their AI system since it can contribute to the overall growth and prosperity of all individuals, society, and the planet, and advance global development objectives. The AI technologies shall be assessed against their impacts on sustainability.

SECTION 6. ROLES AND RESPONSIBILITIES OF AI STAKEHOLDERS. – The following are the roles and responsibilities of AI stakeholders:

- a. **AI developers** shall ensure that the AI is designed, trained, and tested responsibly without inherent biases, and with safety measures to prevent misuse or errors. As an accountability measure, they shall document the nature, purpose, and extent of the processing of data when such processing is involved in the development of AI systems, including its training and testing.
- b. **AI deployers** shall be responsible for regularly monitoring the proper implementation and effectiveness of governance mechanisms in place, with clearly defined lines of accountability to determine who is responsible for the deployed systems.

Moreover, referring to Section 5(d) on the principle of Transparency and Explainability, AI deployers shall ensure and maintain the accuracy, relevance, and

²⁴ See DICT, National Cybersecurity Plan 2023-2028, available at <https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf>

²⁵ See ASEAN AI Guide, p. 16.

²⁶ See UNESCO Recommendation on AI Ethics, III.2 (31), p. 21.

integrity of the data utilized by these systems. This obligation is crucial for producing fair, unbiased, and reliable AI outputs. Appropriate technical and organizational measures shall be implemented and maintained to verify that personal data processed by AI systems is correct, current where necessary, and handled in a manner that minimizes the risk of biased outcomes.

They shall also put in place a reporting and feedback mechanism for the AI systems they will be deploying for public use or internal tasks.

Further, they shall provide proper disclosure to the public or concerned stakeholders on whether AI models and systems, including machine learning and learning language models, were used for all deliverables and services provided.

Each agency deploying AI systems, whether public-facing or for internal operations, shall properly define the method of disclosure in its respective internal policies.

- c. **AI users** shall be responsible and accountable for their AI utilization, ensuring employment of proper, appropriate, and effective governance mechanisms, reviewing the system output, and adhering to AI principles, including physical, technical, and organizational data security measures, and respecting intellectual property rights.

Referring to Section 5(d) on the principle of Transparency and Explainability, AI users who are suspected to be affected by AI decisions have the right to contest or challenge the outcomes, outputs, and/or actions of AI systems and request a human review from the concerned agency. If an AI decision is deemed incorrect or unfair, affected individuals are entitled to effective redress.

- d. **AI vendors** shall ensure AI solutions are reliable, secure, and ethical. They shall be held accountable for delivering flawed products and failing to disclose potential AI risks and limitations.

SECTION 7. AWARENESS AND LITERACY.²⁷ — In line with the UNESCO Recommendation on the Ethics of Artificial Intelligence, public awareness and understanding of AI systems and the value of data shall be actively promoted through inclusive, accessible education and civic engagement initiatives such as digital skills development, AI ethics training, and media and information literacy, among others. These initiatives require collaborative leadership by the government agencies, academia, and the private sector.

Moreover, social and cultural diversity shall be considered in implementing the abovementioned initiatives, ensuring a meaningful public participation, enabling all individuals to make informed decisions regarding the use of AI, and to be safeguarded against undue influence.

²⁷ See UNESCO Recommendation on AI Ethics, III.2 (44-45), p. 23.

AI deployers shall be responsible for advancing AI awareness and literacy by supporting and participating in these initiatives, enabling all members of society to make informed decisions about the use of AI systems and to be protected from undue influence.

This shall include structured training programs that shall cover, at least, the enhancement of technical competencies, focusing on AI ethics, cybersecurity, and governance.

SECTION 8. OVERSIGHT MECHANISM.— Referring to Section 5(f) on Responsibility and Accountability, government agencies that use AI systems are mandated to ensure that oversight and review mechanisms are in place to guide the use and deployment of AI systems and to adopt measures to ensure accountability, responsibility, and legal liability for any unlawful harm or damage to human rights and fundamental freedoms resulting from the application of AI systems. Government agencies shall be able to demonstrate that effective policies and procedures and the necessary documentation are in place.

Relevant to this, all government agencies and instrumentalities shall institute an internal committee that shall provide oversight and guidance on the development and deployment of AI systems. At a minimum, the internal committee shall be composed of the head or designated representatives from the IT and Legal units, with representatives from the AI developer and AI deployer. Should the developer be outsourced by the agency, the end-user who initiated the outsourcing shall be designated as the representative in the committee.

The internal committee shall provide recommendations to the Head of Agency, or its authorized executive officer, on the allowable extent of development, deployment, and use of AI systems within the agency. The Head of Agency, or its authorized executive officer, shall be held accountable for the approval and adoption of AI systems despite evident risks or those risks.

SECTION 9. HANDLING OF GOVERNMENT DATA IN AI SYSTEMS. — All covered entities shall classify and process all government data to be integrated into AI systems with respect to the level of classification of the data involved consistent with the R.A. No. 6713 or the Code of Conduct and Ethical Standards for Public Officials and Employees;²⁸ R.A. No. 10173 or the Data Privacy Act of 2012, including applicable issuances of the NPC; Executive Order (E.O.) No. 02, s. 2016, on Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies to Full Public Disclosure and Transparency in the Public Service and providing Guidelines therefor;²⁹ Memorandum Circular (MC) No. 78, series of 1964, entitled "Security of Classified Matter in Government Departments and Instrumentalities,"³⁰ as amended by MC No. 196, series of 1968; E.O. No.

²⁸ See An Act Establishing a Code of Conduct and Ethical Standards for Public Officials and Employees, to Uphold the Time-Honored Principle of Public Office being a Public Trust, Granting Incentives and Rewards for Exemplary Service, Enumerating Prohibited Acts and Transactions and Providing Penalties for Violations Thereof and for other Purposes [Code of Conduct and Ethical Standards for Public Officials and Employees], Republic Act No. 6713, § 7 (c) (1989).

²⁹ See Executive Order No. 02, series of 2016, Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies to Full Public Disclosure and Transparency in the Public Service and providing Guidelines therefor [E.O. No. 02, s. 20216] (23 July 2016).

³⁰ See Office of the President, Memorandum Circular No. 78, s. 1964, "Promulgating Rules Governing Security of Classified Matter in Government Offices." [M.C. No. 78, s. 1964] (14 August 1964).

608, series of 2007, on Establishing a National Security Clearance System for Government Personnel with Access to Classified Matters and for other purposes,³¹ and relevant issuances from the National Security Council, National Archives of the Philippines (NAP) General Circular No. 1 on Rules and Regulations Governing the Management of Public Records and Archives Administration,³² and other relevant and applicable issuances.

For handling of data with different classification levels, the application shall be based on the highest classification level of any individual data within that collection.

Agencies shall ensure transparency, accountability, security, and human review in the implementation of an AI system, with violations subject to penalties under existing laws.

SECTION 10. MONITORING AND EVALUATION MECHANISM. — Referring to Section 5(f) of this JMC, AI developers and deployers shall monitor on a regular basis the compliance of their respective AI systems with this JMC.

Moreover, all covered agencies shall issue their internal policy as aligned with the principles adopted by this JMC. Agencies that have already promulgated their respective internal policies consistent with their mandates shall ensure that such policies are reviewed and, where necessary, harmonized with the principles and standards set forth in this Joint Memorandum Circular. Nothing herein shall be construed to diminish the agencies' statutory or regulatory authority.

Further, the applicability of this JMC shall be integrated into their respective Information System Strategic Plan (ISSP), as well as into their procurement process and procedures, technical specifications, terms of references, service agreements, and contracts, among others.

SECTION 11. IMPLEMENTING GUIDELINES AND OTHER SUPPLEMENTAL ISSUANCES. — The DICT and the CSC shall jointly develop and issue the implementing guidelines operationalizing the provision of this JMC, within ninety (90) days upon effectivity of this JMC.

Further, the DICT and the CSC may issue orders and circulars to supplement the adoption and implementation of any particular provision or group of provisions under this JMC.

SECTION 12. RESERVATION CLAUSE. — Nothing in this JMC shall be construed to limit, decrease, or restrain the DICT's and the CSC's authority and mandate under relevant laws and issuances.

³¹ See Executive Order No. 608, series of 2007, Establishing a National Security Clearance System for Government Personnel with Access to Classified Matters and for other purposes [E.O. No. 608, s. 2007] (30 March 2007).

³² See National Archives of the Philippines, Rules and Regulations Governing the Management of Public Records and Archives Administration, General Circular No. 1, series of 2009 [NAP Gen. Circ. 1, s. 2009] (20 January 2009).

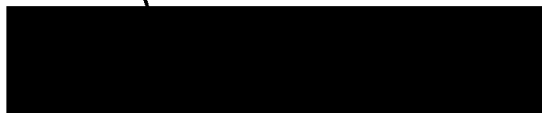
SECTION 13. SEPARABILITY CLAUSE. — If any provision of this JMC is declared invalid or unconstitutional, the other provisions not affected thereby shall remain valid and subsisting.

SECTION 14. REPEALING CLAUSE. — All issuances, orders, rules, and regulations that are inconsistent with the provisions of this JMC are hereby repealed or modified accordingly.

SECTION 15. EFFECTIVITY CLAUSE. — This JMC shall take effect immediately upon filing three (3) certified true copies with the Office of the National Administrative Register, University of the Philippines Law Center, and publication in a newspaper of general circulation.

Let copies of this JMC be posted and published on the official DICT and CSC websites and bulletin boards.

SECTION 16. APPROVING AUTHORITY.



HENRY R. AGUDA
*Secretary, Department of Information and
Communications Technology*



ATTY. MARILYN B. YAP, CPA
Chairperson, Civil Service Commission

**PRINCIPLES FOR THE ETHICAL AND RESPONSIBLE USE AND DEVELOPMENT OF ARTIFICIAL INTELLIGENCE
(AI) IN THE GOVERNMENT**