



DOCUMENT TYPE

TITLE

DOCUMENT NO.

Corporate Policy

AI Tools and Systems Policy

ACEN-PH-ITDA-POL-027

EFFECTIVITY DATE

VERSION NUMBER

PAGE

22-Apr-2026

0

1 of 8

BUSINESS UNIT/
DEPARTMENT

INFORMATION TECHNOLOGY

DOCUMENT REVISION HISTORY

PAGE NO.	REVISION NO.	CHANGE DESCRIPTION	EFFECTIVITY DATE	PREPARED BY	REVIEWED BY	APPROVED BY
All	00	New Document	April 22, 2026	Charleen Tan	Legal and Governance	Board of Directors

1 OBJECTIVE

The purpose of ACEN Corporation's Artificial Intelligence (AI) Tools and Solutions Policy is to ensure legal and ethical use of AI tools and solutions technology. The guidance below defines acceptable and prohibited uses and outlines user obligations related to the use or development of AI tools and solutions models and applications.

This policy shall be read and interpreted in conjunction with all other ACEN policies, including but not limited to the Code of Conduct, Data Privacy Policy, Information Security Policy, and any applicable regulatory compliance guidelines. In case of any inconsistency, the provisions shall be harmonized to give effect to the intent of all applicable policies.

2 SCOPE

This policy applies to all relevant parties within the ACEN Corporation including but not limited to employees, contractors, directors, and third parties with access to critical or high-risk tools, systems, or AI applications. This policy covers the use of AI applications or development of AI models, including internal models, third-party models, or publicly available applications such as ChatGPT. This policy applies to the use of those applications on Company-owned devices and/or personal devices when used for work purposes.

This policy covers all AI use cases that involve the collection, processing, storage, or transfer of personal data, whether within the Philippines or across borders, and mandates compliance with National Privacy Commission (NPC) guidelines on cross-border data transfers.

Entities belonging to the ACEN Group which are situated outside of the Philippines are encouraged, at their discretion, to align with the structure and guiding principles of this policy. Any voluntary adoption must be undertaken in compliance with and subject to the applicable laws, rules, and regulations of the country in which the entity is located, particularly with respect to Data Privacy and the Responsible Use of AI. This ensures that local legal requirements always take precedence while still allowing international entities to benefit from the policy's framework.

Entities operated and managed by ACEN Corporation are also covered by this policy once they adopt it. Adoption shall occur through formal approval by the entity's board, management, or equivalent governing authority.

In all other aspects where no such conflict is present, the Philippine Data Privacy Act shall continue to apply and serve as the guiding framework.

3 DEFINITION OF TERMS

Artificial Intelligence (AI) – "a technical and scientific field devoted to the engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives." [ISO/IEC 22989:2022]

Generative AI - an artificial intelligence technology that synthesizes new versions of text, audio, or visual imagery from large bodies of data in response to user prompts. AI tools and solutions models can be used in stand-alone applications, such as Microsoft Copilot Chat, ChatGPT or Gemini, or incorporated into other applications such as internet search engines or word processing applications.

	DOCUMENT TYPE	TITLE	DOCUMENT NO.
	Corporate Policy	AI Tools and Systems Policy	ACEN-PH-ITDA-POL-027
	EFFECTIVITY DATE	VERSION NUMBER	PAGE
	22-Apr-2026	0	3 of 8

		Data User- An individual or organization that accesses and uses data for analysis, decision-making, or operational purposes. Data Subject - A person whose personal data is collected, stored, or processed by a data controller or processor. AI Hallucination - Error where AI generates false, misleading, or fabricated information that appears plausible but is not based on real data. Prompt - A command or question given to an AI system to guide its response or behavior.
--	--	---

4	GOVERNANCE	This document shall be reviewed every two (2) years, but an update may occur earlier if internal or external influences affect its suitability, adequacy, and effectiveness.
---	------------	--

5	CORPORATE POLICY	
---	------------------	--

5.1 PRINCIPLES

5.1.1 Transparency (Explainability)

Users and data subjects shall be informed when an AI system is used in decision-making. The reasoning behind an AI system's decision shall be understandable to the intended audience. Set up data protocols to govern who can access data, when it can be accessed, and for what purpose.

5.1.2 Accountability

Designers, developers, architects, engineers, and users shall be accountable for the development and use of AI. AI shall be aligned with all relevant laws, rules, and regulations, as well as relevant responsible and ethical AI frameworks.

Third parties engaged for the development and use of AI shall be bound by the requirement.

5.1.3 Safety (Risk, Security, Privacy)

AI shall not be used in a manner that would lead to a state where human life, health, or property is threatened, nor result in negative environmental or societal impact. AI shall be secured against malicious attacks. AI shall cope with errors during execution and unexpected or erroneous input, and cope with stressful environmental conditions. AI shall perform consistently, work reliably, and have consistent results for a range of inputs and situations.

5.1.4 Fairness (Equity, Bias, Non-discrimination)

AI shall not result in unfair bias or discrimination. Algorithmic decisions shall not lead to discriminatory or unjust results that impact different demographics. The design and development of AI shall be done with consideration that the training datasets and the resulting models are reasonably representative of all groups involved.

5.1.5 Human Centricity (Human Autonomy, Sustainability)



AI systems shall respect human autonomy and human-centric values and pursue benefits for the community, including our customers' and employees' overall well-being, productivity, and efficiency, while being protected from potential harms.

5.2 DATA PRIVACY AND CONFIDENTIALITY CONSIDERATIONS

When using AI tools and solutions, information is typically shared through user prompts, instructions, or questions. By default, this constitutes data sharing with the tool. It is important to understand the implications of this sharing, particularly in relation to data privacy and confidentiality.

5.2.1 Data Privacy

Information is shared with AI tools and solutions through user prompts, instructions or questions. By default, providing access to information in this manner constitutes sharing data with the tool. This sharing of data potentially makes confidential, sensitive or personal information public as the tool may train its model on the data shared. In some cases, data that has been anonymized could be linked to personal information and become exposed. Any customer or employee personal information, Company proprietary information or intellectual property, or otherwise confidential information entered into the prompt may appear in other users' output.

To prevent any exposure of personal information, the following "privacy by design" rules shall always be observed when using AI tools and AI for solutioning:

- Proactive not Reactive; Preventative not Remedial: Anticipate privacy issues and prevent them before they occur.
- Privacy as the Default Setting: Ensure maximum privacy protection by default.
- Privacy Embedded into Design: Integrate privacy into the design of systems and processes from the outset.
- Full Functionality: Positive-Sum, not Zero-Sum: Seek solutions that balance privacy with other functionalities.
- End-to-End Security: Full Lifecycle Protection: Protect data throughout its entire lifecycle.
- Visibility and Transparency: Keep it Open: Be transparent about data processing practices.
- Respect for User Privacy: Keep it User-Centric: Prioritize the privacy rights and freedoms of users and data subjects.

The mechanisms to be adopted and implemented to ensure responsible and ethical AI use of tools and systems shall be in accordance with applicable law, government stipulations, and industry best practices.

5.2.2. Confidentiality

In addition to privacy concerns, the use of AI tools also raises issues related to confidentiality. Any Company proprietary information, intellectual property, or other confidential data entered into AI prompts may inadvertently be exposed or reproduced in outputs accessible to other users.

This may cover, but is not limited to, the following:

- Trade secrets
- Internal business strategies
- Financial data
- Legal documents
- Employee or customer records





DOCUMENT TYPE

TITLE

DOCUMENT NO.

Corporate Policy

AI Tools and Systems Policy

ACEN-PH-ITDA-POL-027

EFFECTIVITY DATE

VERSION NUMBER

PAGE

22-Apr-2026

0

5 of 8

To ensure proper handling of such information, employees must refer to and comply with the Employee Code of Conduct, which outlines the standards for safeguarding confidential and proprietary data.

5.3 VERIFICATION OF GENERATIVE AI OUTPUT

Outputs created by AI tools and solutions tools may provide false answers, sometimes referred to as "AI hallucinations". Furthermore, many open-source AI tools and solutions models are often trained on large, publicly available datasets (e.g., through data extraction of public webpages). The outputs may therefore contain copyrighted information, or intellectual property belonging to others.

Users must also be aware that AI tools and solutions tools may incorporate biases of the data sets that were used to train them. This modeling bias may not always align with ACEN's core values and its commitment to diversity, equity and inclusion. Therefore, model output may make systematic errors or favor certain groups, leading to unfair or discriminatory outcomes. Users of AI tools and solutions must therefore adhere to existing review processes where AI tools and solutions are used to make decisions or provide analysis of information that may be subject to bias.

ACEN shall put in place, as part of governance mechanisms, a system, procedure, and/or a reviewing body to ensure the accuracy of the output of AI systems before allowing their actual use in the workplace.

5.4 TRANSPARENCY

Consistent with our Code of Conduct and other policies, we aim to provide our employees, third parties, and customers with transparency regarding how we use AI tools and solutions to support our work. All content generated using AI tools and solutions must be clearly identified on both internal-facing content and any external-facing content.

5.5 THIRD PARTY RISK

Data shared by ACEN Corporation to third parties may be used by those third party in their AI tools and solutions tools, including, without limitation, for training new AI models, updating existing AI models, and improving the user experience. Any sensitive information entered into unapproved AI tools and solutions applications may be disclosed or generated as output accessible to individuals outside the Company. Failure to use AI tools and solutions in accordance with this policy may result in a breach of ACEN's contractual obligations with customers or vendors, and in certain cases, may also constitute a violation of applicable law.

5.6 ACCEPTABLE USE

Use of AI tools whether accessed through platforms, software, or other solutions must comply with the Company's Code of Conduct, internal policies, and applicable laws. Company-owned devices must be used only for business purposes. Use of personal devices or accounts within Company premises is permitted only for work-related purposes and must not be used to bypass or violate Company safeguards or policies. Such Company policies on the use of personal devices shall provide the rules on acceptable use (i.e., applications and assets employees are allowed to access using personal devices), minimum required security controls, and Company rights over the device (e.g., remote wiping for lost or stolen devices), among others.

For any use of AI tools and solutions applications, employees must adhere to the following:

5.6.1 To maintain the security of our data and IT systems, employees are prohibited from attempting to gain access to unapproved AI tools and solutions applications when using Company systems or networks, conducting business on behalf of the Company, or when using the Company's data. To avoid potential data leaks or security incidents:

- Do not use Company credentials, email addresses, or telephone numbers as a login to publicly available AI tools and solutions applications.
- Do not install non-approved Application Programming Interfaces (APIs), plug-ins, connectors, or software related to AI tools and solutions systems.
- Code generated by AI tools and solutions may be used on Company systems provided it undergoes the same rigorous code review and quality assurance processes as human-written code. AI-generated code must not be exempt from human oversight. For transparency, teams are strongly encouraged to indicate in commit logs or other forms of documentation when AI tools have been substantially used to generate code.

5.6.2 To maintain the confidentiality of sensitive information, including but not limited to employee and customer personal information, our intellectual property, and copyrighted material, employees and contractors must only share information with approved personnel and only input sensitive information into approved AI tools and solutions systems. To maintain confidentiality:

- Do only use approved generative AI applications for work purposes.
- Do not input Company intellectual property into generative AI applications without an enterprise account.
- Do not enter personally identifiable information (PII) of employees, customers, or other third parties into any generative AI applications without an enterprise account and without the consent of the said data subjects unless a different legal ground is relied upon the use and processing thereof. Treat the application as you would an employee of another company with whom we have no formal relationship.
- Do contact your manager, or email dataprivacy@acenrenewables.com if you are unsure whether information you are planning to input falls into any of the above categories.
- Do review the Company's data handling policies.

5.6.3 To maintain transparency with customers and employees and protect the Company from claims against copyright infringement and/or theft of intellectual property, all AI tools and solutions generated content must be cited and reviewed if used for work purposes. To protect the Company:

- Do clearly attribute any output used for work purposes to the AI tools and solutions that generated it, either through a footnote or another visible method. This is important if the output will directly impact or be used by external customers.
- Do maintain an updated record of AI tools and solutions used for work purposes and be able to share those records with your manager or other authorized Company personnel upon request.

5.6.4 To protect our employees and clients from harm, and to protect the Company from reputational damage, employees must use AI tools and solutions in accordance with ACEN Corporation's Code of Conduct and non-discrimination policies. AI tools and solutions-created content that are inappropriate, discriminatory or otherwise harmful to our employees or clients/customers must not be used for work purposes. Such use will result in disciplinary action, up to and including termination. To protect our employees, customers, and the Company:

- Do review output of AI tools and solutions applications to make sure it meets Company's standards for principles of equity, ethics, and appropriateness.





DOCUMENT TYPE

TITLE

DOCUMENT NO.

Corporate Policy

AI Tools and Systems Policy

ACEN-PH-ITDA-POL-027

EFFECTIVITY DATE

VERSION NUMBER

PAGE

22-Apr-2026

0

7 of 8

- Do not use any output that discriminates against individuals on the basis of race, color, religion, sex, national origin, age, disability, marital status, political affiliation or sexual orientation.
- Do not use AI tools and solutions applications to create text, audio, or visual content for purposes of committing fraud or to misrepresent an individual's identity.

5.6.5 All employees and contractors are expected to comply with applicable laws, regulations, or Company policies regarding the use or development of AI tools and solutions content or tools.

5.6.6 All employees are expected to report any instances of non-compliance with this policy to whistleblower@acenrenewables.com. Employees are encouraged to speak up if they witness misconduct. Employees who report misconduct or concerns in good faith will not be retaliated against.

5.6.7. All employees shall undergo mandatory training on the responsible and ethical use of AI and this Policy. The IT Business Unit, together with Human Resources Corporate Functional Unit, shall be responsible for providing the training.

5.7 MONITORING

ACEN Corporation and its subsidiaries reserve the right to access and monitor the use of AI tools and solutions applications on any Company-issued devices or that appears on Company-managed networks to ensure compliant use of these systems.

AI audits shall be conducted on regular basis to determine that AI systems and their supporting algorithms comply with legal and ethical standards.

The IT Steering Committee shall be responsible for monitoring the Corporation's compliance with this Policy.

5.8 NON-COMPLIANCE

Any violation of this policy will be handled and investigated in accordance with the procedure provided in the Company's Code of Conduct.

Any violation may lead to serious consequences, including disciplinary action, termination of employment in accordance with ACEN's Code of Conduct, without prejudice to the possible filing of civil and/or criminal penalties.

Any AI tools and solutions-related activities which violate applicable laws will be reported to external law enforcement.

If monitoring systems and processes detect a possible policy violation or if a User reports a possible policy violation, the suspect event shall be processed using appropriate security incident response processes.



DOCUMENT TYPE

TITLE

DOCUMENT NO.

Corporate Policy

AI Tools and Systems Policy

ACEN-PH-ITDA-POL-027

EFFECTIVITY DATE

VERSION NUMBER

PAGE

22-Apr-2026

0

8 of 8

6

**RELATED GUIDELINES /
REFERENCES**

This document shall take effect immediately upon approval. Memoranda, guidelines, or issuance inconsistent with this document is hereby repealed or shall be aligned within a reasonable timeline. Unaffected portions of the aforementioned memoranda, guidelines or issuances will still remain in force.

- ISO/IEC 22989:2022 IT — Artificial intelligence — Artificial intelligence concepts and terminology
- ISO/IEC 42001:2023 IT – Artificial Intelligence – Management System
- NIST Risk Management Framework
- OECD Framework for the Classification of AI Systems
- EU AI Act
- ASEAN Guide on AI Governance and Ethics
- Singapore Government Approach to AI Governance

7

ANNEXES

- Information Technology Data Management Guidelines
- Information Technology Incident Management Policy
- Employee Code of Conduct and Ethics
- Whistleblower Policy
- Data Privacy Manual

8

APPROVALS

Document Prepared by


CHARLEEN TAN

Head, Enterprise Innovation Group

Document Reviewed By

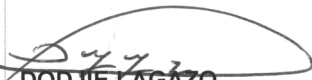

ALAN ASCALONSenior Vice President
Legal, Governance and Compliance
MICO BARNES

Legal and Compliance Counsel

Document Approved By


ZEESHAN PERVEZ

President, ACEN Shared Services Inc.


DODYE LAGAZO

Group General Counsel and Compliance Officer


MARIA LOURDES HERAS DE-LEONChairperson
Corporate Governance Committee