

# AI Governance At ETDA

Sak Segkhoonthod  
Advisor  
ETDA

# (ร่าง) นโยบายการใช้งานเทคโนโลยีปัญญาประดิษฐ์เชิงสร้างสรรค์ (Acceptable Use Policy: Generative AI)

## 1. ทั่วไป

การใช้งานเทคโนโลยีปัญญาประดิษฐ์เชิงสร้างสรรค์ (Generative Artificial Intelligent: Generative AI) สามารถช่วยลดเวลาและเพิ่มประสิทธิภาพในการทำงานได้ เนื่องจาก Generative AI มีความสามารถในการสร้างสรรค์เนื้อหาในรูปแบบที่หลากหลาย ตัวอย่างเช่น ข้อความ ภาพ วิดีโอ เพลง ซอร์สโค้ด เป็นต้น อีกทั้ง ยังสามารถสร้างเนื้อหาได้อย่างสมจริงและโต้ตอบกับผู้ใช้งานได้คล้ายคลึงกับมนุษย์

ซึ่งจากความสามารถดังกล่าวอาจทำให้ผู้ใช้งานเชื่อว่าเนื้อหาที่สร้างโดย Generative AI นั้น ถูกต้อง น่าเชื่อถือ และสามารถนำไปใช้งานได้ทันที โดยไม่จำเป็นต้องพิจารณาถึงความเหมาะสมและข้อจำกัดของเทคโนโลยี โดยเฉพาะอย่างยิ่งข้อจำกัดด้านภาษาไทยและความเข้าใจในบริบทหรือวัฒนธรรมของประเทศไทย

เมื่อผู้ใช้งานนำเนื้อหาดังกล่าวไปใช้ในงานต่างๆ เช่น การเขียนบทความ การเขียนข้อความ โฆษณา การเขียนโปรแกรม หรือการสร้างภาพศิลปะ เป็นต้น อาจก่อให้เกิดผลกระทบเชิงลบต่อบุคคล องค์กร และสังคมได้ ตัวอย่างเช่น



เมื่อผู้ใช้งานนำเนื้อหาดังกล่าวไปใช้ในงานต่างๆ เช่น การเขียนบทความ การเขียนข้อความ โฆษณา การเขียนโปรแกรม หรือการสร้างภาพศิลปะ เป็นต้น อาจก่อให้เกิดผลกระทบเชิงลบต่อบุคคล องค์กร และสังคมได้ ตัวอย่างเช่น

- เนื้อหาไม่ถูกต้องตามข้อเท็จจริง (Confabulation)
- เนื้อหาส่งผลกระทบต่อประเด็นที่มีความอ่อนไหว รวมถึงมีเนื้อหาที่ขัดต่อหลักการจริยธรรม (Sensitive and Ethics Context)
- เนื้อหาที่สร้างส่งเสริมให้เกิดอคติและการเลือกปฏิบัติ (Bias and Discrimination)
- ข้อมูลส่วนบุคคลรั่วไหล (Personal Data Leakage)
- การละเมิดทรัพย์สินทางปัญญา (Intellectual Property Infringement)
- ความมั่นคงปลอดภัย (Information Security)

## 5. หน้าที่และความรับผิดชอบ

การใช้งานเนื้อหาที่สร้างโดย Generative AI อาจส่งผลกระทบต่อบุคคล องค์กร และสังคม โดยที่ สพรอ. และผู้ใช้งาน (ซึ่งปฏิบัติหน้าที่ในนามของ สพรอ.) ไม่อาจปฏิเสธความรับผิดชอบต่อผลของการกระทำดังกล่าวได้ ด้วยเหตุนี้ ผู้ใช้งานและบุคคลที่เกี่ยวข้องกับการใช้งาน Generative AI จึงมีหน้าที่และความรับผิดชอบในการใช้งาน Generative AI ดังต่อไปนี้

- 1) ผู้ใช้งานต้องสื่อสารกับผู้บริหารตามสายบังคับบัญชาอย่างชัดเจน เมื่อใช้ Generative AI ในการปฏิบัติงาน
- 2) ผู้ใช้งานต้องตรวจสอบเนื้อหาที่สร้างโดย Generative AI ก่อนนำไปใช้งานหรือเผยแพร่ต่อสาธารณะ โดยในการตรวจสอบผู้ใช้งานจำเป็นต้องพิจารณาในประเด็น ดังต่อไปนี้
  - ความถูกต้องของเนื้อหา
  - ผลของการใช้งานหรือเผยแพร่เนื้อหาที่นำไปสู่การกระทำผิดทางกฎหมาย รวมถึงการละเมิดทรัพย์สินทางปัญญา
  - ความเท่าเทียมและการไม่เลือกปฏิบัติต่อบุคคลหรือกลุ่มบุคคล
  - การรักษาความลับและคุ้มครองข้อมูลส่วนบุคคล
  - ผลกระทบต่อความมั่นคงปลอดภัย
  - ผลกระทบเชิงลบอื่นๆ ที่อาจเกิดขึ้นต่อบุคคล องค์กร และสังคม
- 3) ผู้ใช้งานต้องรายงานให้ผู้บริหารตามสายการบังคับบัญชารับทราบโดยทันที ในกรณีที่การใช้งาน Generative AI เกิดความผิดพลาด และอาจส่งผลกระทบต่อบุคคล องค์กร และสังคม
- 4) ผู้บริหารตามสายบังคับบัญชาและผู้ใช้งานต้องมีการทบทวนประเด็นปัญหา ประเมินประสิทธิภาพและประสิทธิผลของการใช้งาน Generative AI เพื่อปรับปรุงวิธีการทำงานและเลือกใช้แอปพลิเคชันหรือบริการที่เหมาะสมกับการปฏิบัติงาน
- 5) คณะกรรมการบริหารเทคโนโลยีสารสนเทศ (IT Steering) มีหน้าที่ในการพิจารณาและอนุมัติรายการแอปพลิเคชันหรือบริการ Generative AI ที่เหมาะสมกับการใช้งานภายใน สพรอ.

## ระเบียบวาระที่ 4 เรื่องเพื่อพิจารณา

### 4.X หลักเกณฑ์ในการจัดหาแอปพลิเคชันหรือระบบ Generative AI ให้สอดคล้องกับ Acceptable Use Policy: Generative AI

#### 2.2. ขออนุมัติรายการแอปพลิเคชันหรือบริการ Generative AI ที่มีการใช้งานภายในสำนักงาน เพื่อจัดทำรายการ Generative AI ที่เหมาะสมกับการใช้งานภายในสำนักงาน

|   | หลักเกณฑ์   | MS Copilot | Copilot for Microsoft 365 | ChatGPT Enterprise/Team | Gemini Advance   | Claude    |
|---|---|------------|---------------------------|-------------------------|--|-----------|
| 1 | ไม่นำข้อมูลจากผู้ใช้ไปสอน AI (Training AI)                                      | ✓<br>[1]   | ✓<br>[2]                  | ✓<br>[4]                | ?<br>มีการ review prompt โดยคนและนำไป improve<br>[8]     | ✓<br>[11] |
| 2 | มีมาตรการในการคุ้มครองข้อมูลองค์กรและข้อมูลส่วนบุคคล                            | ✓<br>[1]   | ✓<br>[2]                  | ✓<br>[4]                | ?<br>มีการนำข้อมูลไป Review แต่ user สามารถปิดได้<br>[8] | ✓<br>[11] |
| 3 | มีมาตรการในการควบคุมการสร้างเนื้อหาที่ไม่เหมาะสม                                | ✓<br>[2]   | ✓<br>[2]                  | ✓<br>[5]                | ✓<br>[9]   |           |
| 4 | มีมาตรการลดหรือหลีกเลี่ยงการเกิดอคติ (Bias) และการเลือกปฏิบัติ (Discrimination) | ✓<br>[2]   | ✓<br>[2]                  | ✓<br>[6]                | ✓<br>[9]   |           |
| 5 | ผลลัพธ์จาก Generative AI สามารถนำไปใช้ได้ โดยไม่ละเมิดทรัพย์สินทางปัญญา         | ✓<br>[3]   | ✓<br>[3]                  | ✓<br>[7]                | ✓<br>[10]  |           |

## ระเบียบวาระที่ 4 เรื่องเพื่อพิจารณา

### 4.X หลักเกณฑ์ในการจัดหาแอปพลิเคชันหรือระบบ Generative AI ให้สอดคล้องกับ Acceptable Use Policy: Generative AI

#### 2.2. ขออนุมัติรายการแอปพลิเคชันหรือบริการ Generative AI ที่มีการใช้งานภายในสำนักงาน เพื่อจัดทำรายการ Generative AI ที่เหมาะสมกับการใช้งานภายในสำนักงาน

|   | หลักเกณฑ์   | MS Copilot | DALL-E<br>(ที่มากับ ChatGPT<br>Enterprise/Team) | Gemini Advance  | Midjourney |
|---|---|------------|---|---|------------|
| 1 | ไม่นำข้อมูลจากผู้ใช้ไปสอน AI (Training AI)                                      | ✓<br>[1]   | ✓<br>[4]  | ?<br>บอกเพียงว่าจะมีการ review โดยคนและนำไป improve [8] | N/A        |
| 2 | มีมาตรการในการเก็บรักษาข้อมูลองค์กร และข้อมูลส่วนบุคคลที่เหมาะสม                | ✓<br>[1]   | ✓<br>[4]  | ?<br>มีการนำข้อมูลไป Review แต่ user สามารถปิดได้ [8]   | ?<br>[X]   |
| 3 | มีมาตรการในการควบคุมการสร้างเนื้อหาที่ไม่เหมาะสม                                | ✓<br>[2]   | ✓<br>[5]  | ✓<br>[9]  | N/A        |
| 4 | มีมาตรการลดหรือหลีกเลี่ยงการเกิดอคติ (Bias) และการเลือกปฏิบัติ (Discrimination) | ✓<br>[2]   | ✓<br>[6]  | ✓<br>[9]  | N/A        |
| 5 | ผลลัพธ์จาก Generative AI สามารถนำไปใช้ได้ โดยไม่ละเมิดทรัพย์สินทางปัญญา         | ✓<br>[3]   | ✓<br>[7]  | ✓<br>[10]   | ✓<br>[X]   |



# ChatGPT Enterprise & Team

- ✓ (1) ไม่นำข้อมูลจากผู้ใช้งานไปสอน AI
- ✓ (2) มีมาตรการในการคุ้มครองข้อมูลองค์กรและข้อมูลส่วนบุคคล

## Enterprise privacy at OpenAI

Ownership: You own and control your data

✓ We do not train on your business data (data from ChatGPT Team, ChatGPT Enterprise, or our API Platform)  
✓ You own your inputs and outputs (where allowed by law)  
✓ You control how long your data is retained (ChatGPT Enterprise)

Control: You decide who has access

✓ Enterprise-level authentication through SAML SSO (ChatGPT Enterprise and API)  
✓ Fine-grained control over access and available features  
✓ Custom models are yours alone to use and are not shared with anyone else

Security: Comprehensive compliance

✓ We've been audited for SOC 2 compliance (ChatGPT Enterprise and API)  
✓ Data encryption at rest (AES-256) and in transit (TLS 1.2+)  
✓ Visit our Security Portal to understand more about our security measures

Reference: <https://openai.com/enterprise-privacy/>

### General FAQ

Does OpenAI train its models on my business data?

No. We do not use your ChatGPT Team, ChatGPT Enterprise, or API data, inputs, and outputs for training our models.

Does OpenAI review my business data?

We may run any business data submitted to OpenAI's services through automated content classifiers and safety tools, including to better understand how our services are used. The classifications created are metadata about the business data but do not contain any of the business data itself. Business data is only subject to human review as described below on a service-by-service basis.

### ChatGPT Team FAQ

Who can view conversations and chat history in ChatGPT Team?

Within your organization, only end users can view their conversations. Workspace admins have control over workspaces and access. Our access to conversations stored on our systems is limited to (1) authorized employees that require access for engineering support, investigating potential platform abuse, and legal compliance and (2) specialized third-party contractors who are bound by confidentiality and security obligations, solely to review for abuse and misuse.

# Midjourney

- ✓ (5) ผลลัพธ์จาก Generative AI สามารถนำไปใช้ได้ โดยไม่ละเมิดทรัพย์สินทางปัญญา

## 4. Content Rights

Your Rights and Obligations

You own all Assets You create with the Services to the fullest extent possible under applicable law. There are some exceptions:

- Your ownership is subject to any obligations imposed by this Agreement and the rights of any third-parties.
- If you are a company or any employee of a company with more than \$1,000,000 USD a year in revenue, you must be subscribed to a "Pro" or "Mega" plan to own Your Assets.
- If you upscale the images of others, these images remain owned by the original creators.

Please consult Your own lawyer if You want more information about the state of current intellectual property law in Your jurisdiction. Your ownership of the Assets you created persists even if in subsequent months You downgrade or cancel Your membership.

Inputs, Assets, and other content such as messages, photos, videos, and documents that you may provide to the Services (such as through uploading, posting, sharing, or chat messages) are collectively, "Content". You are responsible for all Content that you provide or generate, including ensuring that it does not violate any applicable laws or this Agreement, and that you have all necessary rights and permissions to provide the Content.

Reference: <https://docs.midjourney.com/docs/terms-of-service>

## 10. Limitation of Liability and Indemnity

We provide the service as is, and we make no promises or guarantees about it.

You understand and agree that we will not be liable to You or any third party for any loss of profits, use, goodwill, or data, or for any incidental, indirect, special, consequential or exemplary damages, however they arise. Our aggregate liability under this Agreement will not exceed the amount You paid for the Services that gave rise to the claim during the 12 months before the claim.

You are responsible for Your use of the service. If You harm someone else or get into a dispute with someone else, we will not be involved.

To the extent permitted by law, you will indemnify and hold us harmless, our affiliates, and our personnel, from and against any costs, losses, liabilities, and expenses (including attorneys' fees) from third party claims arising out of or relating to your use of the Services and Assets or any violation of these Terms.

# Gemini

- ✓ (3) มีมาตรการในการควบคุมการสร้างเนื้อหาที่ไม่เหมาะสม
- ✓ (4) มีมาตรการลดหรือหลีกเลี่ยงการเกิดอคติ (Bias) และการเลือกปฏิบัติ (Discrimination)

Back

## Policy guidelines for the Gemini app

Our goal for the Gemini app is to be maximally helpful to users, while avoiding outputs that could cause real-world harm or offense. Drawing upon the expertise and processes developed over the years through research, user feedback, and expert consultation on various Google products, we aspire to have Gemini avoid certain types of problematic outputs, such as:

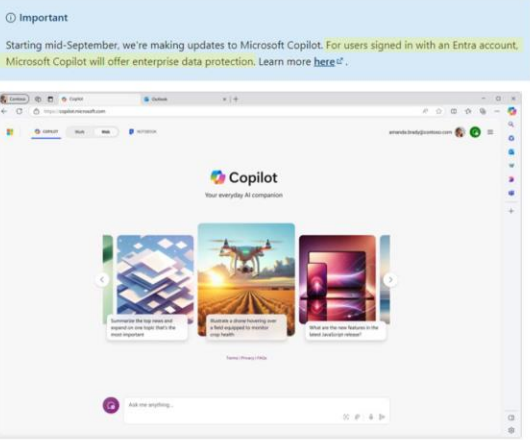
- **Threats to Child Safety:** Gemini should not generate outputs, including Child Sexual Abuse Material, that exploit or sexualize children.
- **Dangerous Activities:** Gemini should not generate outputs that encourage or enable dangerous activities that would cause real-world harm. These include:
  - Instructions for suicide and other self-harm activities, including eating disorders.
  - Facilitation of activities that might cause real-world harm, such as instructions on how to purchase illegal drugs or guides for building weapons.
- **Violence and Gore:** Gemini should not generate outputs that describe or depict sensational, shocking, or gratuitous violence, whether real or fictional. These include:
  - Excessive blood, gore, or injuries.
  - Gratuitous violence against animals.

- **Harmful Factual Inaccuracies:** Gemini should not generate factually inaccurate outputs that could cause significant, real-world harm to someone's health, safety, or finances. These include:
  - Medical information that conflicts with established scientific or medical consensus or evidence-based medical practices.
  - Incorrect information that poses a risk to physical safety, such as erroneous disaster alerts or inaccurate news about ongoing violence.
- **Harassment, Incitement and Discrimination:** Gemini should not generate outputs that incite violence, make malicious attacks, or constitute bullying or threats against individuals or groups. These include:
  - Calls to attack, injure, or kill individuals or a group.
  - Statements that dehumanize or advocate for the discrimination of individuals or groups based on a legally protected characteristic.
  - Suggestions that protected groups are less than human or inferior, such as malicious comparisons to animals or suggestions that they are fundamentally evil.
- **Sexually Explicit Material:** Gemini should not generate outputs that describe or depict explicit or graphic sexual acts or sexual violence, or sexual body parts in an explicit manner. These include:
  - Pornography or erotic content.
  - Depictions of rape, sexual assault, or sexual abuse.

# Microsoft Copilot

- ✓ (1) ไม่นำข้อมูลจากผู้ใช้งานไปสอน AI
- ✓ (2) มีมาตรการในการคุ้มครองข้อมูลองค์กรและข้อมูลส่วนบุคคล

Back



## Commercial data protection explained

To help business and educational organizations protect corporate data, Copilot adds commercial data protection when eligible users sign in with their work or school accounts (Entra ID).

Commercial data protection means both user and organizational data are protected:

- Prompts and responses aren't saved
- Microsoft has no eyes-on access
- Chat data isn't used to train the underlying large language models

Unlike Copilot for Microsoft 365, Copilot has no access to organizational data in the Microsoft 365 Graph. Commercial data protection applies to users with eligible work or school accounts wherever Copilot is available.

## Generated search queries

Microsoft Copilot parses a user's prompt and identifies terms where web grounding would improve the quality of the response. Based on these terms, Copilot generates a search query that it sends to the Bing Search service asking for more information.

This generated search query is different from the user's original prompt—it consists of a few words informed by the user's prompt. A few terms from uploaded files or content actively viewed in Edge may also be sent to the Bing search service to ground responses if Copilot needs them to understand the user's prompt.

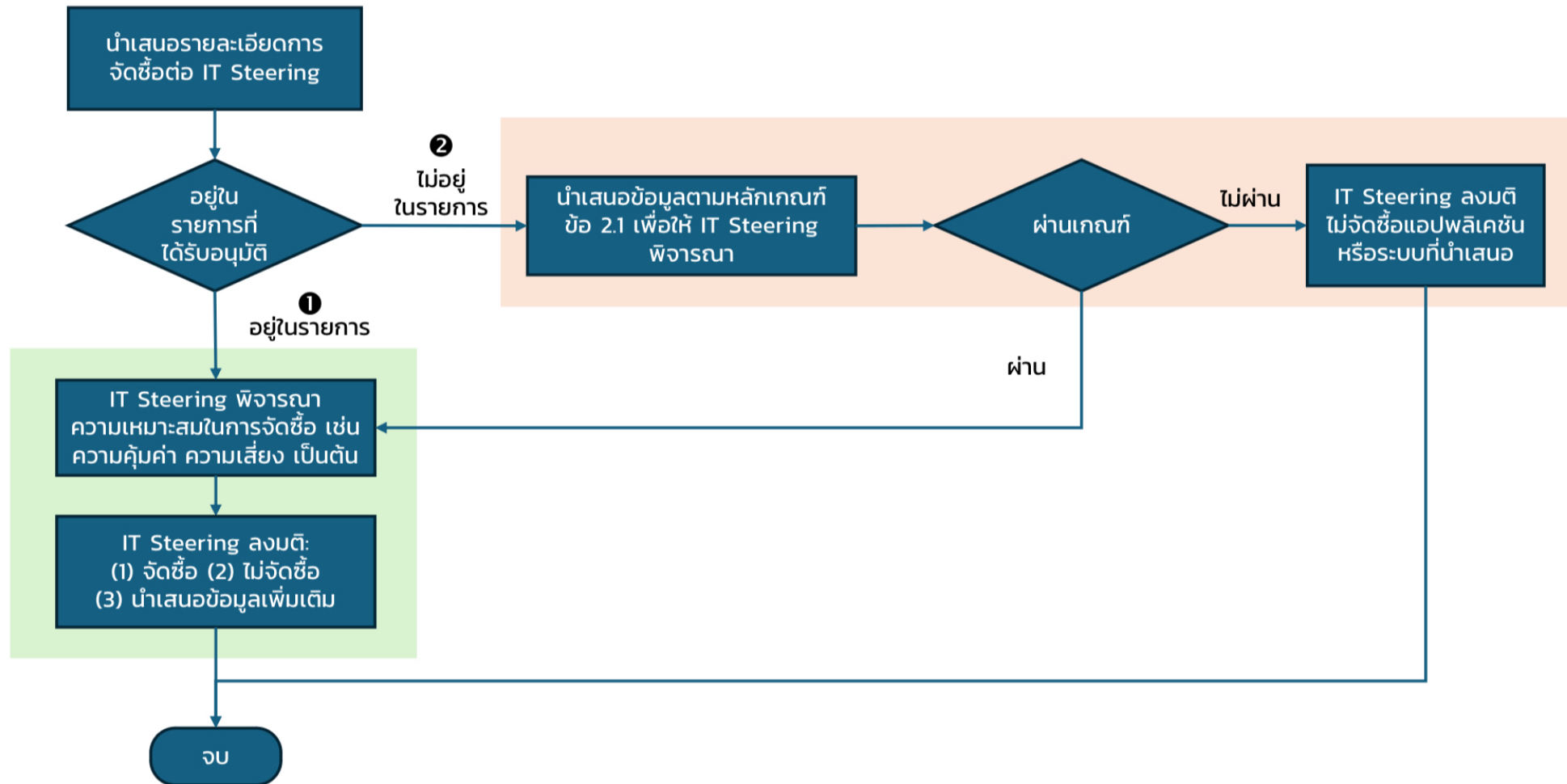
The following information is not included in the generated query sent to the Bing search service:

- The user's entire prompt, unless the prompt is very short (for example, "local weather")
- Entire files uploaded into Copilot
- Entire web pages or PDFs summarized by Copilot in Edge
- Any identifying information based on the user's Entra ID (for example: username, domain, or tenant ID)

Generated search queries sent to the Bing search service are dissociated from the user ID and tenant ID. They aren't shared with advertisers. Also, web grounding queries sent to Bing don't impact any of the following:

- Search Ranking

## 2.3. แนวทางการขออนุมัติซื้อ License สำหรับใช้งานแอปพลิเคชันหรือบริการ Generative AI





## THAILAND'S AI STRATEGY PLAN



## 5 developed areas in Thailand AI

S1: ELSI

S2: Infrastructure

S3: Human Capability

S4: Technology & Innovation

S5: Promotion

*\*ELSI is Ethics Legal and Social Implication*

## THAILAND'S AI ETHICS GUIDELINE (AI ETHICS PRINCIPLES & MODEL)



## 6 Principles of Thailand AI Ethics

Competitiveness &  
Sustainability Development

Laws Ethics &  
International Standards

Transparency &  
Accountability

Security &  
Privacy

Fairness

Reliability

## AI GOVERNANCE GUIDELINE & TOOLKITS



## 3 Pillars of AI Governance Guideline:

3 Pillars for preparing trust, safe, responsible use of AI in Organization



AI Structure



AI Strategy



AI Operation

**Promote**

- Responsible AI
- Trust
- Risk Mitigation

# AI Governance Center : AIGC

## OUR MISSIONS

### Research and Development

Conduct research and development on AI governance, including the creation of guidelines, standards, white papers, toolkits, and regulations.

1

### AI Governance Testing

Develop criteria and systems for AI governance testing and LLM benchmarking (AI sandbox).

2

### Consultation

Provide recommendations for AI policy and AI governance development through in-house consultations and workshops.

3

4

### Collaboration

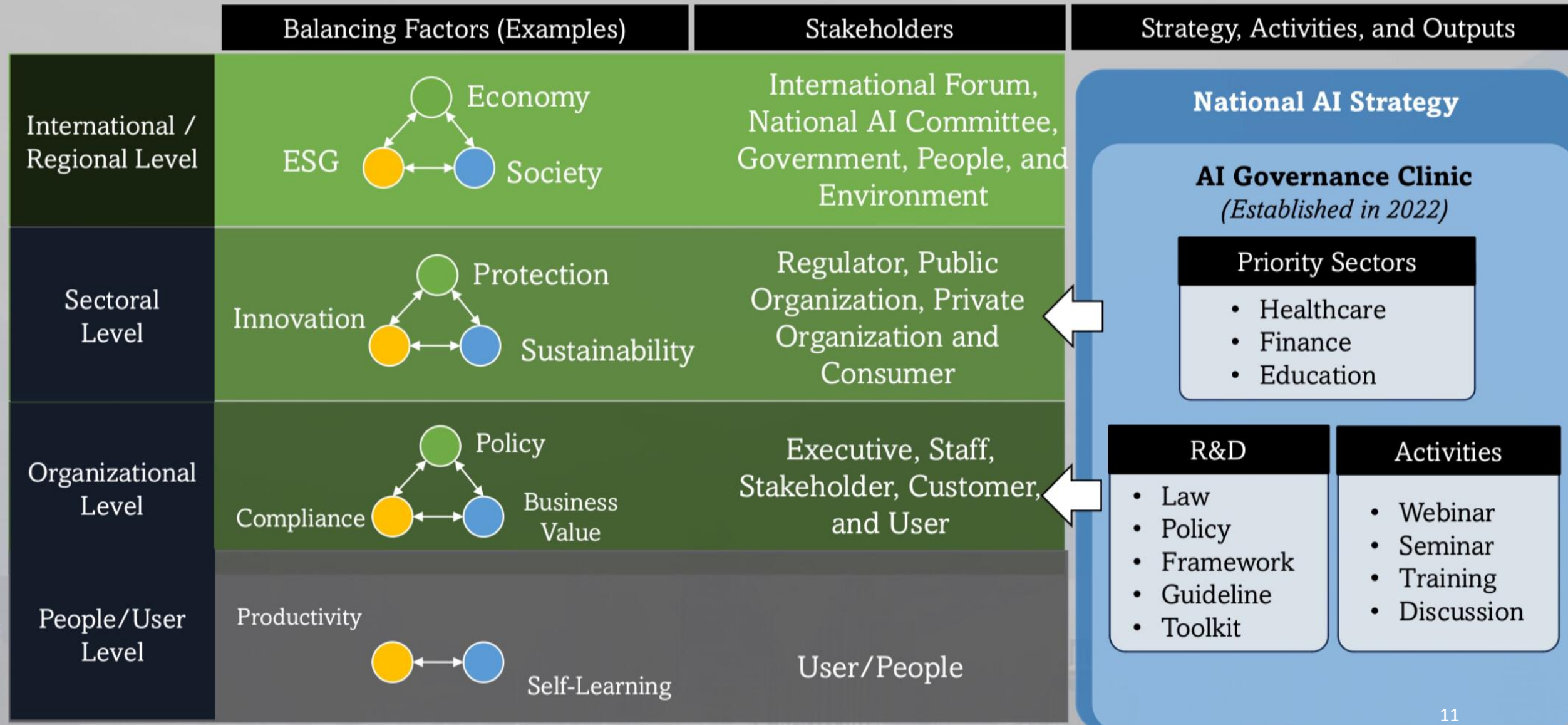
Establish regional and global positions on AI governance in collaboration with organizations such as UNESCO, OECD, and ASEAN.

# 14

**AIGC Fellows**  
(4 new in 2024)

**3**    Microsoft  
**Industry Collaborators**

# Thailand's AI Governance Approach





# AI Governance Guidelines and Toolkits Blueprint

## Align AI Frameworks & Guidelines

### Conceptual Guidelines

- ✓ AI Governance Framework  
(align with AI principles of global, OECD)



AI Governance Structure

AI Strategy

AI Operation

### Practical Guidelines

Practical Guidelines by **Technology**

May

Generative AI

Etc.

Practical Guidelines by **Topic**

JUN

AI Job Redesign Guideline

May

AI Roadmap Guideline

JUN

AI Procurement Guideline

AI Training Data Guideline

Recommendation on Data Governance for AI

Etc.

## Inspire AI Action

### Toolkit

Toolkits for AI Governance Structure

- ✓ AI Readiness Assessment Toolkit

JUN

AI Job Redesign Toolkit

Etc.

Toolkits for AI Strategy

- ✓ AI Use Case Canvas Toolkit

- ✓ AI Risk Assessment Toolkit

JUN

AI Value Assessment Toolkit

AI Project Management Toolkit

Etc.

Toolkits for AI Operations

AI Procurement Toolkit

Etc.

## Guide AI Execution

### Stakeholder Empowerment

Who to Empower

Government Agencies

Healthcare entities

Financial Institutions

Educational institutions

Etc.

How to Empower

Knowledge Sharing

Workshop

Focus Group

Meeting

Consultation Clinic

Training

Etc.

## Co-Create AI Policies

### Policy & Regulatory Recommendations

Policy & Regulatory Recommendations

AI National Governance

AI Adoption Policy

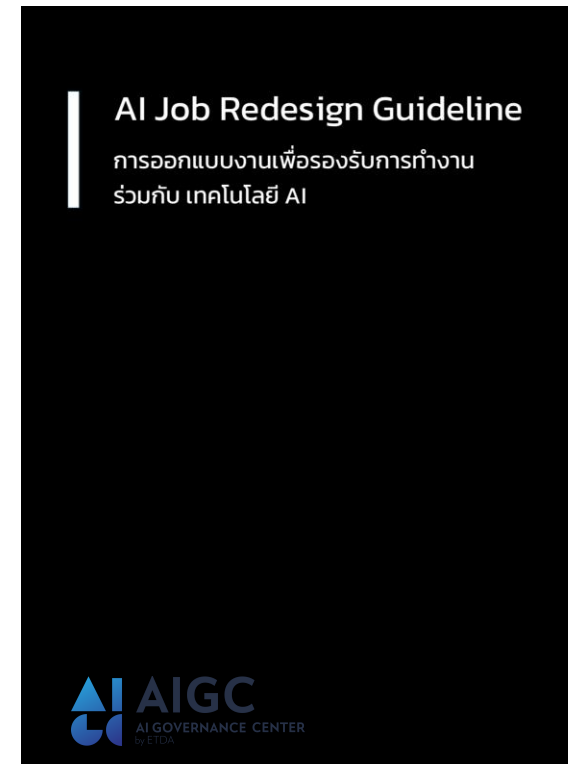
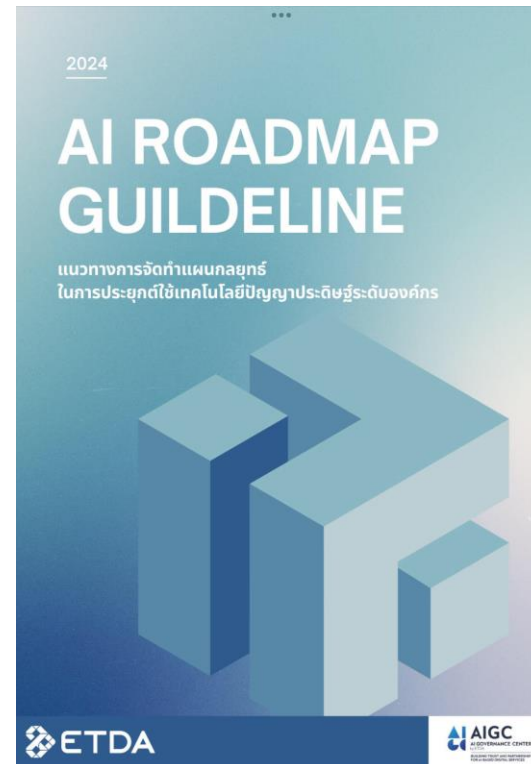
AI Regulations

AI Skill Transition

Etc.

# Research and Development

- Guidelines & toolkits to support AI Governance Guideline for Executives implementation:
- Online AI readiness scan tool (to release soon)
- Fellow publications (to publish Aug-Sep 2024)
- Future R&D in finance, education, AI sandbox, etc



# AI Tools

- AI Value Assessment Tool;
- Online AI readiness scan tool (to release soon)
- AI Use Case Canvas
- AI Risk Mitigation

## AI Value Assessment Toolkits



ersion : 1.0

ทำไมองค์กรถึงควรทำ **AI Value Assessment Toolkits** ?

AI Value Assessment Toolkits เป็นเครื่องมือที่ช่วยให้คุณสามารถคำนวณได้ว่า Use Case สำหรับนำ AI มาใช้งานในองค์กรมีประโยชน์อย่างไรโดยประกอบไปด้วยกัน 2 ด้าน

ด้านที่ 1 : ประโยชน์ทางตรง (Tangible Benefit)

AI Value Assesment Toolkits จะช่วยท่านคำนวณประโยชน์ในด้านต่างๆที่ออกมาเป็นหน่วย บาท/ปี เพื่อใช้ประเมินถึงความคุ้มค่าในการลงทุน

ด้านที่ 2 : ประโยชน์ทางอ้อม (Intangible Benefit)

AI Value Assessment Toolkits จะช่วยให้ท่านหาประโยชน์ทางอ้อมที่ไม่ได้เป็นตัวเงิน เพื่อส่งเสริมการตัดสินใจในการลงทุน

🗨️ กลุ่มเป้าหมายของ **AI Value Assessment Toolkits**

ผู้บริหารหรือพนักงานที่เกี่ยวข้องกับ AI ในองค์กร

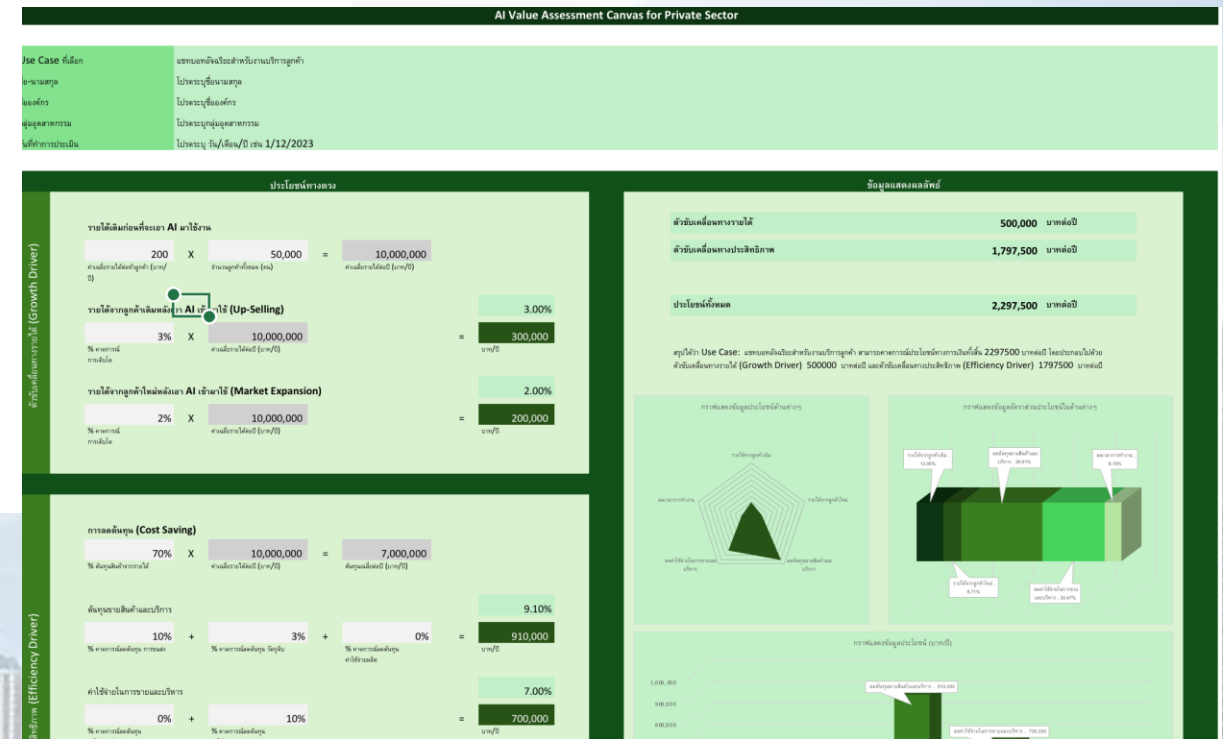
ขั้นตอนการใช้งาน **AI Value Assessment Toolkits**

AI Value Assessment Toolkits จะแบ่งออกเป็น 2 ส่วน คือ

## ส่วนที่ 1 : AI Value Assessment Toolkits สำหรับภาครัฐ

## ส่วนที่ 2 : AI Value Assesment Toolkits สำหรับภาคเอกชนและรัฐวิสาหกิจ

ให้เลือกทำส่วนใดส่วนหนึ่งตามรูปแบบของบัตรของท่าน







# Thank you



# AIGC

**AI GOVERNANCE CENTER**

by ETDA