

แนวทางการปฏิบัติของคู่สัญญาเพื่อสอดคล้องกับหลักการใช้ งานปัญญาประดิษฐ์ (AI) อย่างมีความรับผิดชอบ (Guidelines for Third-Party Compliance with Responsible AI Principles)

กลุ่มเอไอเอส

เวอร์ชัน: 2.1

เจ้าของเอกสาร: AI Governance

วันที่ปรับปรุงแก้ไข: 06 กรกฎาคม 2569

ประวัติการปรับปรุง

เอกสารฉบับนี้มีการบันทึกการแก้ไขทั้งหมดตามตารางดังต่อไปนี้

เวอร์ชัน	วันที่	ผู้จัดทำ	รายละเอียด	ผู้สอบทาน	อนุมัติโดย
1.0	19 ธันวาคม 2568	AI Governance	เอกสารตั้งต้น	Intelligent Process Automation Manager	CoE
2.0	20 เมษายน 2569	AI Governance	เพิ่มเติม - สิทธิในทรัพย์สินทางปัญญาและ การใช้เทคโนโลยี AI	Intelligent Process Automation Manager	CoE
2.1	06 กรกฎาคม 2569	AI Governance	ปรับปรุงคำศัพท์และจัดตำแหน่งการ แสดงเนื้อหา	Intelligent Process Automation Manager	CoE

สารบัญ

1. บทนำ	4
1.1 วัตถุประสงค์	4
1.2 ขอบเขต	4
1.3 คำจำกัดความ	4
2. หลักการใช้งานปัญญาประดิษฐ์ (AI) อย่างมีความรับผิดชอบ (RESPONSIBLE AI PRINCIPLE)	4
2.1 ความเป็นธรรม (FAIRNESS)	5
2.2 การตัดสินใจของมนุษย์และการกำกับดูแล (HUMAN AGENCY AND OVERSIGHT)	5
2.3 ความเป็นส่วนตัวและความมั่นคงปลอดภัย (PRIVACY AND SECURITY)	5
2.4 ความปลอดภัย และความแข็งแกร่ง (SAFETY AND ROBUSTNESS)	5
2.5 ความโปร่งใสและความสามารถในการอธิบายได้ (TRANSPARENCY AND EXPLAINABILITY)	6
2.6 ความรับผิดชอบ (ACCOUNTABILITY)	6
2.7 ผลกระทบในด้านสิ่งแวดล้อม (ENVIRONMENT IMPACT)	6
3. ตัวอย่างรายการเอกสาร RESPONSIBLE AI สำหรับการพิจารณาผู้ให้บริการภายนอก (THIRD-PARTY VENDOR)	6
4. สิทธิในทรัพย์สินทางปัญญาและการใช้เทคโนโลยี AI	9
4.1 ความเป็นเจ้าของผลงานและสิทธิในทรัพย์สินทางปัญญา	9
4.2 การใช้ข้อมูลของผู้ว่าจ้างเฉพาะตามวัตถุประสงค์ของโครงการ	9
4.3 การไม่ละเมิดทรัพย์สินทางปัญญาของบุคคลภายนอกและความรับผิดชอบของผู้รับจ้าง	9

1. บทนำ

1.1 วัตถุประสงค์

เอกสารหลักจริยธรรมระบบปัญญาประดิษฐ์ (AI) นี้มีวัตถุประสงค์เพื่อให้เป็นมาตรฐานและแนวทางปฏิบัติที่ชัดเจนสำหรับ ผู้รับจ้าง/คู่สัญญา ในการออกแบบ พัฒนา และดำเนินการเกี่ยวกับระบบปัญญาประดิษฐ์ (AI) โดยมีเป้าหมายหลักคือการสร้างความมั่นใจ สอดคล้องกับหลักการจริยธรรม สังคม และกฎหมาย ของบริษัท พร้อมทั้งสร้างความเข้าใจในความคาดหวังหลักด้าน ความเป็นธรรม ความรับผิดชอบ ความปลอดภัย ความยั่งยืน (Sustainability) และความเป็นส่วนตัว การดำเนินการตามหลักการเหล่านี้จะทำหน้าที่เป็นกลไกในการลดความเสี่ยงที่อาจเกิดขึ้นจากการละเลย

1.2 ขอบเขต

เอกสารนี้มีผลบังคับใช้ครอบคลุมการทำงานทั้งหมดของผู้รับจ้าง/คู่สัญญาที่เกี่ยวข้องกับระบบปัญญาประดิษฐ์ (AI) ของหน่วยงาน โดยมีขอบเขตตั้งแต่ต้นจนจบของวงจรชีวิตโครงการ (Project Lifecycle) ซึ่งรวมถึงการออกแบบ การพัฒนา การทดสอบ การนำไปใช้ และการบำรุงรักษา

1.3 คำจำกัดความ

No	คำศัพท์	คำจำกัดความ
1.	Third-Party	บริษัทหรือผู้ให้บริการภายนอกที่เข้ามาพัฒนา จัดหา หรือให้บริการด้านระบบปัญญาประดิษฐ์ (AI) โดยต้องปฏิบัติตามหลักการ Responsible AI ขององค์กร
2.	Responsible AI	แนวทางการพัฒนาและใช้งานระบบปัญญาประดิษฐ์ (AI) อย่างมีจริยธรรม โปร่งใส ปลอดภัย เป็นธรรม และสามารถตรวจสอบได้
3.	Bias	อคติหรือความลำเอียงในข้อมูลหรืออัลกอริทึมที่อาจส่งผลต่อความเป็นธรรมของระบบปัญญาประดิษฐ์ (AI)
4.	Explainability	ความสามารถในการอธิบายเหตุผลของการตัดสินใจหรือผลลัพธ์ที่เกิดจากระบบปัญญาประดิษฐ์ (AI)
5.	Human-in-the-Loop (HITL)	การมีส่วนร่วมของมนุษย์ในกระบวนการตัดสินใจของระบบปัญญาประดิษฐ์ (AI) เพื่อควบคุมและลดความเสี่ยง
6.	Privacy	การคุ้มครองข้อมูลส่วนบุคคลและความลับของผู้ใช้งานในระบบปัญญาประดิษฐ์ (AI)
7.	Transparency	การเปิดเผยข้อมูล กระบวนการ และวิธีการทำงานของระบบปัญญาประดิษฐ์ (AI) ให้สามารถตรวจสอบได้

2. หลักการใช้งานปัญญาประดิษฐ์ (AI) อย่างมีความรับผิดชอบ (Responsible AI Principle)

เพื่อให้มั่นใจว่างานพัฒนาหรือใช้งานระบบปัญญาประดิษฐ์ (AI) ที่ท่านดำเนินการให้กับองค์กรเป็นไปตามมาตรฐานสูงสุดด้านจริยธรรม ความน่าเชื่อถือ และความรับผิดชอบต่อ คู่สัญญา (Third-party) จะต้องยึดมั่นและปฏิบัติโดยสอดคล้องกับหลักการทั้ง 7 ข้อดังต่อไปนี้

2.1 ความเป็นธรรม (Fairness)

ระบบปัญญาประดิษฐ์ (AI) ที่ท่านพัฒนาหรือดำเนินการต้องรับรองความเป็นธรรมอย่างเคร่งครัด โดยมีกลไกป้องกันการเลือกปฏิบัติต่อบุคคลหรือกลุ่มบุคคลใดๆ อย่างชัดเจน เป้าหมายหลักคือการหลีกเลี่ยงการตัดสินใจหรือการอนุมานที่ก่อให้เกิดผลเสียหรืออคติ (bias) ต่อกับกลุ่มผู้ใช้บางกลุ่มโดยไม่เป็นธรรม ท่านจะต้องออกแบบและพัฒนาระบบโดยคำนึงถึงความเสมอภาคและการปฏิบัติต่อทุกคนอย่างเท่าเทียมกัน เพื่อให้ผู้ใช้ทุกกลุ่มสามารถเข้าถึงและได้รับประโยชน์จากเทคโนโลยี AI นี้อย่างเท่าเทียมและเป็นธรรม การสร้างระบบที่มีความเป็นธรรมนี้ไม่เพียงแต่ช่วยลดความไม่เท่าเทียมที่อาจเกิดขึ้น แต่ยังเป็นการสร้างความไว้วางใจและความเชื่อมั่นในการใช้งานเทคโนโลยีอย่างยั่งยืน

2.2 การตัดสินใจของมนุษย์และการกำกับดูแล (Human Agency and Oversight)

ระบบปัญญาประดิษฐ์ (AI) ควรถูกออกแบบและนำไปใช้ในลักษณะที่สนับสนุนการตัดสินใจของมนุษย์ โดยที่มนุษย์สามารถควบคุมและกำกับดูแลระบบได้อย่างเหมาะสม เพื่อป้องกันผลกระทบเชิงลบต่อบุคคลและสังคม รวมถึงส่งเสริมคุณค่าพื้นฐานและสิทธิมนุษยชน ทั้งนี้ควรลดความเสี่ยงจากการพึ่งพาระบบปัญญาประดิษฐ์ (AI) มากเกินไป โดยเฉพาะในบริบทที่เกี่ยวข้องกับชีวิต ความปลอดภัยและศักดิ์ศรีของความเป็นมนุษย์

ข้อกำหนดเพิ่มเติมด้านการกำกับดูแล: ท่านต้องกำหนดระดับการมีส่วนร่วมของมนุษย์ที่เหมาะสมกับความเสี่ยงของระบบ

Human-in-the-Loop (HITL): ใช้สำหรับระบบที่มีความเสี่ยงสูงหรือมีผลกระทบร้ายแรงต่อบุคคล โดยกำหนดให้มนุษย์ต้องเข้าแทรกแซงหรือทำการตัดสินใจขั้นสุดท้ายในทุกๆ ครั้งที่ระบบให้ข้อเสนอแนะหรือการตัดสินใจ

Human-on-the-Loop (HOTL): ใช้สำหรับระบบที่มีความเสี่ยงปานกลางถึงต่ำ โดยกำหนดให้มนุษย์ตรวจสอบและกำกับดูแลการทำงานของระบบเป็นระยะ และมีกลไกการแจ้งเตือนที่ชัดเจนเพื่อให้มนุษย์สามารถเข้าแทรกแซงหรือแก้ไขเมื่อเกิดความผิดพลาดหรือผลลัพธ์ที่ไม่คาดคิด

2.3 ความเป็นส่วนตัวและความมั่นคงปลอดภัย (Privacy and Security)

ระบบปัญญาประดิษฐ์ (AI) ควรถูกออกแบบและพัฒนาโดยคำนึงถึงความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูลผู้ใช้งานเป็นสำคัญ เพื่อป้องกันการละเมิดสิทธิส่วนบุคคลและปกป้องข้อมูลจากการเข้าถึงที่ไม่ได้รับอนุญาต อีกทั้งต้องสอดคล้องกับวัตถุประสงค์ที่ชัดเจนและเป็นประโยชน์ต่อผู้ใช้งานและสังคม โดยคำนึงถึงผลกระทบทางจริยธรรม สังคม และกฎหมาย เพื่อให้ระบบปัญญาประดิษฐ์ (AI) สร้างประโยชน์สูงสุดแก่มนุษย์และสังคม ขณะเดียวกันก็ลดความเสี่ยงและผลกระทบเชิงลบที่อาจเกิดขึ้น

2.4 ความปลอดภัย และความแข็งแกร่ง (Safety and Robustness)

ระบบปัญญาประดิษฐ์ (AI) ควรถูกออกแบบและนำไปใช้อย่างมั่นใจในความปลอดภัย โดยสามารถป้องกันและลดความเสี่ยงที่อาจเกิดขึ้นจากการนำไปใช้งานในสถานการณ์ต่าง ๆ

ระบบปัญญาประดิษฐ์ (AI) ควรมีความทนทาน กล่าวคือ ในการนำไปใช้งานนั้นสามารถหลีกเลี่ยงปัญหาหรือข้อโหว่ ซึ่งมีความสำคัญอย่างยิ่งต่อการพัฒนาระบบปัญญาประดิษฐ์ (AI) ที่ไว้วางใจได้ ระบบปัญญาประดิษฐ์ (AI) ควร

ความสามารถในการทนทานต่อการโจมตีและสามารถทำงานได้ตามที่คาดหวังในสถานการณ์ต่าง ๆ โดยไม่มีการหยุดชะงักหรือข้อบกพร่อง นอกจากนี้ระบบปัญญาประดิษฐ์ (AI) ควรมีประสิทธิภาพสามารถทำงานได้ภายในเวลาที่กำหนดและใช้ทรัพยากรอย่างคุ้มค่า

2.5 ความโปร่งใสและความสามารถในการอธิบายได้ (Transparency and Explainability)

ระบบปัญญาประดิษฐ์ (AI) ควรได้รับการออกแบบโดยให้ข้อมูลที่ชัดเจน ถูกต้อง และสามารถเข้าถึงได้เกี่ยวกับกระบวนการทำงาน การตัดสินใจ และการกระทำของระบบ รวมถึงการแจ้งให้ทราบถึงแหล่งข้อมูล อัลกอริทึม และวิธีการที่ใช้ ให้ผู้ใช้สามารถเข้าใจว่าปัญญาประดิษฐ์ (AI) ทำงานอย่างไร ระบบปัญญาประดิษฐ์ (AI) ต้องสามารถอธิบายความคิด ผลลัพธ์และกระบวนการตัดสินใจของระบบในลักษณะที่เข้าใจได้ง่าย ทั้งนี้รวมถึงการให้ข้อมูลเกี่ยวกับวิธีที่ได้มาซึ่งข้อสรุป ทำให้ผู้ใช้สามารถเข้าใจและเชื่อถือในผลลัพธ์ของระบบปัญญาประดิษฐ์ (AI)

2.6 ความรับผิดชอบ (Accountability)

ผู้พัฒนาระบบปัญญาประดิษฐ์ (AI) และผู้ใช้งานต้องมีความรับผิดชอบต่อผลที่เกิดขึ้นจากการนำระบบไปใช้

ความรับผิดชอบนี้รวมถึงการให้ข้อมูลที่ชัดเจน ถูกต้อง และสามารถเข้าถึงได้เกี่ยวกับกระบวนการ การตัดสินใจ การดำเนินการ และการกำกับดูแล

ระบบปัญญาประดิษฐ์ (AI) ควรมีการกำกับดูแลที่ชัดเจน มีการกำหนดโครงสร้างและหน้าที่ที่รับผิดชอบที่ช่วยส่งเสริมการใช้งานปัญญาประดิษฐ์ (AI) ให้ตรงตามหลักความยุติธรรมและประสิทธิภาพ การกำกับดูแลนี้รวมถึงการตรวจสอบ การติดตาม และการปรับปรุง เพื่อให้ปัญญาประดิษฐ์ (AI) ทำงานได้ตามที่คาดหวัง

2.7 ผลกระทบในด้านสิ่งแวดล้อม (Environment Impact)

ระบบปัญญาประดิษฐ์ (AI) ควรถูกออกแบบและพัฒนาโดยให้ความสำคัญกับการลดผลกระทบต่อสิ่งแวดล้อมในทุกขั้นตอนของการพัฒนาระบบตั้งแต่ การออกแบบ การเลือกแบบจำลองและอัลกอริทึม การใช้งานและการบริหารจัดการตารางแนวทางการประเมิน

3. ตัวอย่างรายการเอกสาร Responsible AI สำหรับการพิจารณาผู้ให้บริการ

ภายนอก (Third-Party Vendor)

รายการเอกสารนี้เป็นแนวทางเพื่อใช้ประกอบการประเมิน Vendor และไม่ใช่ข้อกำหนดที่ต้องส่งตามรายการทั้งหมด โดย Vendor สามารถใช้เอกสารในรูปแบบอื่นที่เทียบเท่าได้ หากสามารถแสดงให้เห็นถึงการปฏิบัติตามหลักการ Responsible AI ขององค์กร

หลักการ	รายการเอกสาร
1. ความเป็นธรรม (Fairness)	Fairness Metric & Thresholds: ระบุมาตรวัด (Metrics) และเกณฑ์ (Thresholds) ที่ใช้ในการประเมินความเป็นธรรมของโมเดลอย่างชัดเจน รวมถึงเหตุผลในการเลือกใช้มาตรวัดดังกล่าว Dataset Card: ข้อมูลรายละเอียดของชุดข้อมูลที่ใช้ในการฝึกฝนและทดสอบโมเดล เช่น แหล่งที่มา สถิติประชากร ข้อจำกัด วิธีการรวบรวม และการจัดการข้อมูลกลุ่มอ่อนไหว Bias Mitigation Strategy: วิธีการและผลลัพธ์ของการปรับปรุงแก้ไข (Mitigation) ออกคิตที่ตรวจพบพร้อมระบุคิตที่ยังคงเหลืออยู่หลังการแก้ไข Post-Deployment Fairness Monitoring Plan: แผนการติดตามและประเมินอคติหลังการนำระบบไปใช้งานจริง โดยรวมถึงวิธีตรวจสอบ drift ความถี่การประเมิน และเกณฑ์ที่ต้องดำเนินการแก้ไขเมื่อพบความไม่เป็นธรรม
2. การตัดสินใจของมนุษย์และการกำกับดูแล	Risk Classification & HITL/HOTL Plan: การจัดประเภทความเสี่ยงของระบบปัญญาประดิษฐ์ (AI) และแผนการระบุจุดที่ต้องให้มนุษย์เข้าแทรกแซง (Human-in-the-Loop) หรือตรวจสอบและควบคุมผลลัพธ์ (Human-on-the-Loop) รวมถึงเหตุผลประกอบการออกแบบ oversight Formal Oversight Sign-off: บันทึกการอนุมัติ การตรวจสอบ หรือการตัดสินใจขั้นสุดท้ายโดยผู้ควบคุมที่เป็นมนุษย์ สำหรับกรณีที่มีความเสี่ยงสูงหรือมีผลกระทบสำคัญต่อผู้ใช้หรือองค์กร Oversight Runbook: คู่มือปฏิบัติงานที่ระบุขั้นตอน วิธีการตรวจสอบ สัญญาณเตือนที่ต้องจับตา และแนวทางการตัดสินใจเมื่อระบบปัญญาประดิษฐ์ (AI) แสดงพฤติกรรมผิดปกติหรือมีความไม่แน่นอนในผลลัพธ์ Escalation Path & Criteria: เกณฑ์และเส้นทางการส่งต่อปัญหาเมื่อผู้ตรวจสอบพบสถานการณ์ที่เสี่ยงสูงหรือมีความไม่แน่นอน รวมถึงการกำหนดจุดที่ต้องส่งต่อให้ผู้เชี่ยวชาญ ผู้บริหารหรือดำเนินการหยุดระบบชั่วคราว
3. ความเป็นส่วนตัวและความมั่นคงปลอดภัย	Access Control Matrix: ตารางที่ระบุสิทธิ์การเข้าถึงข้อมูลทั้ง Training Data, Validation Data และ Live Data รวมถึงสิทธิ์ในการเข้าถึงโมเดล เวอร์ชันโมเดล และระบบที่เกี่ยวข้อง พร้อมอธิบายหลักการควบคุมสิทธิ์และบทบาทของผู้ใช้งานแต่ละกลุ่ม AI-Specific Security Test Report: รายงานผลการทดสอบความปลอดภัยที่ออกแบบเฉพาะสำหรับระบบปัญญาประดิษฐ์ (AI) เช่น การประเมินความเสี่ยงต่อ Model Inversion, Membership Inference, Model Extraction, Data Poisoning และการโจมตี adversarial พร้อมสรุปช่องโหว่ที่ตรวจพบและมาตรการปิดช่องโหว่ Data Quality Assessment: รายงานการประเมินความสมบูรณ์ ความถูกต้อง ความสอดคล้อง ความทันสมัย และความสะอาดของข้อมูลที่ใช้ในทุกขั้นตอนของกระบวนการพัฒนาโมเดล รวมถึงข้อจำกัดและผลกระทบที่ข้อมูลอาจมีต่อประสิทธิภาพหรือความเสี่ยงของระบบ
4. ความปลอดภัยและความแข็งแกร่ง	Performance Testing Report: ผลการทดสอบความแม่นยำ/ประสิทธิภาพ (Accuracy, F1-Score, AUC) ภายใต้สภาวะปกติและสภาวะที่ท้าทาย รวมถึงการประเมินผลกระทบเมื่อข้อมูลมีความคลาดเคลื่อนหรือไม่สมบูรณ์

หลักการ	รายการเอกสาร
	Operational Design Domain (ODD): เอกสารที่ระบุขอบเขตและเงื่อนไขการใช้งานที่ระบบปัญญาประดิษฐ์ (AI) ได้รับการออกแบบและทดสอบให้ทำงานได้อย่างปลอดภัย เช่น ชนิดข้อมูลที่รองรับ สภาพแวดล้อมการทำงาน ข้อจำกัดที่ต้องระวัง และเงื่อนไขที่ไม่ควรใช้งาน Adversarial Testing Report: รายงานผลการทดสอบเพื่อประเมินความสามารถของระบบในการต้านทานการโจมตีที่ทำให้เกิดความผิดพลาด ทั้งการโจมตีด้วยข้อมูล (Adversarial Inputs) การหลอกโมเดล การดัดแปลงสัญญาณ และผลการแก้ไขช่องโหว่ที่ตรวจพบ Stress & Load Robustness Test: ผลการทดสอบความแข็งแรงของระบบเมื่อรับภาระการประมวลผลสูงหรือปริมาณคำขอมากกว่าปกติ รวมถึงพฤติกรรมของโมเดลเมื่ออยู่ในภาวะทรัพยากรจำกัดหรือมี latency สูง
5. ความโปร่งใสและการอธิบายได้	Model Card: รายละเอียดทางเทคนิคของโมเดลที่ประกอบด้วยวัตถุประสงค์ ข้อจำกัด เมตริกประสิทธิภาพ เงื่อนไขการใช้งานที่เหมาะสมและปัจจัยที่อาจทำให้โมเดลให้ผลลัพธ์ที่คลาดเคลื่อน User Disclosure Statement: ข้อความแจ้งผู้ใช้อย่างชัดเจนว่ากำลังมีปฏิสัมพันธ์กับระบบปัญญาประดิษฐ์ (AI) รวมถึงระดับการพึ่งพาอัตโนมัติของผลลัพธ์ และข้อควรระวังที่ผู้ใช้ควรรับทราบ Explainability Report: รายงานที่อธิบายหลักการตัดสินใจของโมเดลโดยแสดงเหตุผล ปัจจัยสำคัญ (Feature Importance/Explainable AI (XAI) Methods) และตัวอย่างการอธิบายผลลัพธ์สำหรับกรณีที่มีความเสี่ยงสูงหรือมีผลกระทบต่อบุคคล
6. ความรับผิดชอบ (Accountability)	Responsible AI Governance Policy: นโยบายการกำกับดูแล AI อย่างมีความรับผิดชอบของ Vendor หรือเอกสารยืนยันการปฏิบัติตามนโยบาย Responsible AI ขององค์กรผู้ว่าจ้าง รวมถึงกรอบการกำกับดูแล บทบาท และกระบวนการตัดสินใจที่เกี่ยวข้องกับระบบปัญญาประดิษฐ์ (AI) RACI Matrix (สำหรับฝ่าย AI): ตารางที่ระบุความรับผิดชอบในแต่ละขั้นตอนของวงจรชีวิตระบบปัญญาประดิษฐ์ (AI) โดยกำหนดชัดเจนว่าใครเป็นผู้รับผิดชอบ (Responsible) ผู้ตัดสินใจ (Accountable) ผู้ให้คำปรึกษา (Consulted) และผู้ที่ต้องรับทราบข้อมูล (Informed) Audit Trail & Evidence Index: บันทึกหลักฐานและเหตุการณ์สำคัญที่เกิดขึ้นในกระบวนการพัฒนา ทดสอบ ปรับปรุง และใช้งานระบบปัญญาประดิษฐ์ (AI) โดยจัดทำดัชนีเพื่อให้สามารถตรวจสอบย้อนหลังได้อย่างโปร่งใสและครบถ้วน Incident Response Plan: แผนรับมือเหตุการณ์ด้านความเสี่ยงหรือความผิดพลาดของระบบปัญญาประดิษฐ์ (AI) ซึ่งครอบคลุมวิธีการตรวจจับ การประเมินความรุนแรง การแจ้งเหตุ การแก้ไขปัญหา และการป้องกันไม่ให้เกิดซ้ำ
7. ผลกระทบต่อสิ่งแวดล้อม	Energy & Carbon Report: รายงานปริมาณการใช้พลังงานและการปล่อยคาร์บอนที่เกิดจากการฝึก การทดสอบ และการใช้งานโมเดล โดยระบุวิธีคำนวณปริมาณทรัพยากรที่ใช้และผลกระทบต่อสิ่งแวดล้อมโดยรวม Efficiency Optimization Plan: แผนการเพิ่มประสิทธิภาพทรัพยากรของโมเดล เช่น การลดขนาดโมเดล การปรับโครงสร้างสถาปัตยกรรม หรือการใช้เทคนิคเพิ่มประสิทธิภาพเพื่อช่วยลดการใช้พลังงานและค่าใช้จ่ายในการประมวลผล

หลักการ	รายการเอกสาร
	Hardware Efficiency Disclosure: ข้อมูลเกี่ยวกับฮาร์ดแวร์ที่ใช้ เช่น ประเภท GPU/TPU ประสิทธิภาพต่อวัตต์ และปัจจัยที่มีผลต่อการใช้พลังงาน เพื่อให้สามารถประเมินประสิทธิภาพด้านสิ่งแวดล้อมของตัวเลือกโครงสร้างพื้นฐานได้

4. สิทธิในทรัพย์สินทางปัญญาและการใช้เทคโนโลยี AI

เพื่อคุ้มครองสิทธิประโยชน์ทรัพย์สินทางปัญญา และความสามารถในการใช้ประโยชน์จากผลงานของผู้ว่าจ้าง อย่างเต็มที่ การจัดทำ พัฒนา และส่งมอบผลงานภายใต้โครงการที่มีการใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) ต้องอยู่ภายใต้หลักการด้านทรัพย์สินทางปัญญาและการใช้ระบบปัญญาประดิษฐ์ (AI) อย่างถูกต้องตามกฎหมาย หลักการดังต่อไปนี้ใช้เป็นกรอบอ้างอิงในการกำหนดข้อกำหนดในสัญญา รวมถึงใช้ประกอบการพิจารณา ตีความ และกำกับดูแล การดำเนินโครงการตลอดอายุสัญญา

4.1 ความเป็นเจ้าของผลงานและสิทธิในทรัพย์สินทางปัญญา

ผลงานทั้งหมดที่เกิดขึ้นจากการดำเนินโครงการ ไม่ว่าจะเป็นผลจากการพัฒนาโดยมนุษย์ การใช้ระบบอัตโนมัติ หรือเทคโนโลยีปัญญาประดิษฐ์ (AI) ในทุกขั้นตอน ให้ถือเป็นผลงานที่จัดทำขึ้นเพื่อผู้ว่าจ้างโดยเฉพาะ และเป็นทรัพย์สินทางปัญญาของผู้ว่าจ้างแต่เพียงผู้เดียว หลักการนี้มีวัตถุประสงค์เพื่อให้ผู้ว่าจ้างสามารถใช้ ทำซ้ำ ดัดแปลง ต่อยอด เผยแพร่ หรือใช้ประโยชน์เชิงพาณิชย์จากผลงานได้อย่างเต็มที่ โดยไม่ถูกจำกัดด้วยสิทธิหรือข้อผูกพันของบุคคลอื่น ทั้งนี้ การนำทรัพย์สินที่มีอยู่ก่อนมาใช้ต้องไม่กระทบต่อความสมบูรณ์ของสิทธิของผู้ว่าจ้างในผลงานที่ส่งมอบ

4.2 การใช้ข้อมูลของผู้ว่าจ้างเฉพาะตามวัตถุประสงค์ของโครงการ

ข้อมูล คำสั่ง (Prompts) และผลลัพธ์ที่เกิดจากการดำเนินโครงการ ถือเป็นสินทรัพย์ที่อยู่ภายใต้การควบคุมของผู้ว่าจ้าง หลักการนี้กำหนดให้การใช้ข้อมูลดังกล่าวต้องจำกัดอยู่ภายในวัตถุประสงค์ของโครงการเท่านั้น เพื่อคุ้มครองข้อมูลความลับทางธุรกิจ และสิทธิในทรัพย์สินทางปัญญาของผู้ว่าจ้าง การนำข้อมูลหรือผลลัพธ์ไปใช้ในการฝึกฝน ปรับปรุง หรือพัฒนาโมเดลระบบปัญญาประดิษฐ์ (AI) อื่น ไม่ว่าจะเป็นของผู้รับจ้างหรือบุคคลที่สามจะไม่สามารถกระทำได้ เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ว่าจ้าง ทั้งนี้ หลักการนี้มีเป้าหมายเพื่อป้องกันการ ใช้ข้อมูลนอกขอบเขตและลดความเสี่ยงเชิงกฎหมายในระยะยาว

4.3 การไม่ละเมิดทรัพย์สินทางปัญญาของบุคคลภายนอกและความรับผิดชอบของผู้รับจ้าง

การดำเนินโครงการต้องไม่เกี่ยวข้องกับการนำผลงาน ข้อมูล โมเดล ซอฟต์แวร์ เนื้อหา หรือทรัพย์สินทางปัญญาของบุคคลอื่นมาใช้โดยไม่ได้รับอนุญาตตามกฎหมาย หลักการนี้กำหนดให้ผู้รับจ้างมีหน้าที่ตรวจสอบความชอบด้วยกฎหมายของทรัพยากร เทคโนโลยี และเนื้อหาที่นำมาใช้อย่างรอบคอบ และต้องสามารถแสดงหลักฐานสิทธิการใช้งานได้เมื่อมีการร้องขอ ในกรณีที่มีการตรวจพบหรือมีเหตุอันควรสงสัยว่าผลงานภายใต้โครงการละเมิดสิทธิของบุคคลอื่น ผู้รับจ้างต้องรับผิดชอบต่อความเสียหาย ผลกระทบ และภาระทางกฎหมายทั้งหมดที่เกิดขึ้นเพื่อคุ้มครองผู้ว่าจ้างจากข้อพิพาทและความเสี่ยงที่อาจเกิดขึ้น