HITAP
Health Intervention and Technology Assessment Program
FOUNDATION

AI Standard Practices

แนวปฏิบัติการใช้ปัญญาประดิษฐ์

October 2026

ฉบับที่ 1.0

วัตถุประสงค์และขอบเขต

วัตถุประสงค์

กำหนดแนวทางการปฏิบัติที่ชัดเจนสำหรับการใช้ปัญญาประดิษฐ์ (Artificial Intelligence: AI) ในการปฏิบัติงานของ HITAP เพื่อให้การใช้ AI เป็นไปอย่างเหมาะสม ปลอดภัย มีความรับผิดชอบ และสอดคล้องกับนโยบายการใช้ปัญญาประดิษฐ์ (AI Policy)

ขอบเขต

แนวทางปฏิบัตินี้ใช้กับบุคลากรของ HITAP รวมถึงนักศึกษาฝึกงาน ผู้ช่วยวิจัย ที่ปรึกษา ผู้รับจ้างและนักวิจัยร่วมจากสถาบันอื่นที่เข้าถึงข้อมูลหรือผลงานของ HITAP ที่ใช้ AI ในการปฏิบัติงานหรือในกิจกรรมที่เกี่ยวข้องกับ HITAP รวมถึงการใช้ AI ผ่านคอมพิวเตอร์ อุปกรณ์ หรือบัญชีผู้ใช้งานส่วนบุคคลหรือขององค์กร

AI Standard Practice อาจมีการปรับปรุงถี่กว่า AI Policy ตามพัฒนาการของ AI

บทบาทและความรับผิดชอบ

นโยบายการใช้ปัญญาประดิษฐ์ (AI Policy) กำหนดให้ทีมเทคโนโลยีสารสนเทศ (IT) ฝ่ายบริหารงานทั่วไป และผู้บริหาร ร่วมกันกำกับดูแลการใช้ AI รวมทั้งจัดทำและทบทวนแนวทางปฏิบัติในการใช้ AI (Standard Practices) ให้สอดคล้องกับนโยบายดังกล่าว

ผู้รับผิดชอบ	บทบาทและความรับผิดชอบ
ผู้บริหาร	กำหนดทิศทาง อนุมัติหลักการ และตัดสินใจเกี่ยวกับความเสี่ยงในระดับองค์กร
เจ้าหน้าที่เทคโนโลยีสารสนเทศ (IT)	ดูแลเครื่องมือ AI ความมั่นคงปลอดภัย การกำหนดสิทธิ์การเข้าถึง และมาตรการป้องกันทางเทคนิค
ฝ่ายบริหารงานทั่วไป	ประสานงานกลาง และจัดทำ รวบรวม และดูแลเอกสารแนวทางปฏิบัติ
ตัวแทนระดับฝ่าย	รวบรวมลักษณะการใช้งาน AI และขั้นตอนการทำงาน ระบุจุดเสี่ยง กำหนดเกณฑ์คุณภาพ และจัดทำตัวอย่างการใช้งานที่เหมาะสมกับบริบทของฝ่าย
บุคลากรทุกคน	ปฏิบัติตามแนวทางปฏิบัติในการใช้ AI ตรวจสอบผลลัพธ์ และรายงานเหตุการณ์ที่เกี่ยวข้องกับการใช้ AI

Central Standard + Unit Practice ใช้แนวทางปฏิบัติส่วนกลางร่วมกับแนวทางปฏิบัติเฉพาะของแต่ละฝ่าย เพื่อให้สามารถนำไปใช้ได้จริงและเหมาะสมกับบริบทการทำงาน ภายใต้นโยบายการใช้ AI เดียวกันขององค์กร

จากนโยบายการใช้ AI สู่แนวทางปฏิบัติส่วนกลาง AI Standard Practices

AI Policy
นโยบายการใช้ปัญญาประดิษฐ์

กำหนด “กรอบและหลักการ”

- การใช้ AI อย่างมีจริยธรรม โปร่งใส และเป็นธรรม
- ความรับผิดชอบและความเป็นเจ้าของ
- ความถูกต้องและความน่าเชื่อถือ
- การคุ้มครองข้อมูลและความลับ
- งานวิจัยและงานวิชาการ
- การรายงานเหตุการณ์และการกำกับดูแล

AI Standard Practices
แนวปฏิบัติการใช้ปัญญาประดิษฐ์

แปลงเป็น “วิธีปฏิบัติ”

- ใช้ AI กับงานประเภทใดได้
- ข้อมูลประเภทใดห้าม/ต้องขออนุมัติ
- ต้องตรวจอะไรบ้างก่อนใช้ผลลัพธ์
- ต้องเปิดเผยการใช้ AI เมื่อใด
- ใครเป็นผู้อนุมัติ/ให้คำปรึกษา
- ต้องรายงานเหตุการณ์กับใคร

Unit Practice
แนวทางปฏิบัติระดับฝ่าย

เติม “บริบทของงาน”

- Use Cases ที่เหมาะกับแต่ละฝ่าย
- Workflow และจุดควบคุม
- ข้อมูล/เอกสารที่ใช้บ่อย
- ตัวอย่าง Prompt ที่ปลอดภัย
- ความเสี่ยงเฉพาะของงาน
- เกณฑ์คุณภาพ/การตรวจสอบ

Policy = What / Why → Standard Practice = How → Unit Practice = How for my work

โครงสร้างแนวทางปฏิบัติส่วนกลางในการใช้ AI (AI Standard Practices)

กรอบและบทบาท

วัตถุประสงค์และขอบเขต บทบาทและความรับผิดชอบ และการเชื่อมโยงนโยบายสู่แนวทางปฏิบัติ

หลักการปฏิบัติร่วมกัน

หลักการ 7 ข้อที่ทุกคนต้องปฏิบัติ และเกณฑ์พิจารณาก่อนเริ่มใช้ AI

การใช้ AI ในงานประเภทต่าง ๆ

การใช้ AI ในงานทั่วไป งานบริหาร งานวิจัย และงานวิชาการ

ระดับความเสี่ยง

ความเสี่ยงจากการใช้ AI ทั้ง 4 ระดับ และแผนผังช่วยตัดสินใจ

การจัดการข้อมูลและการรักษาความลับ

ข้อมูลที่อนุญาตและห้ามนำเข้า AI ชั้นข้อมูล การทำข้อมูลให้ไม่สามารถระบุตัวบุคคลได้

เครื่องมือที่แนะนำ

เครื่องมือที่องค์กรแนะนำ ประเภทของ AI

คุณภาพและความโปร่งใส

การตรวจสอบคุณภาพและผลลัพธ์โดยผู้ใช้งาน การเปิดเผยการใช้ AI และการเขียนคำสั่ง (Prompt)

การรายงานเหตุการณ์และการขอความช่วยเหลือ

แจ้งเหตุการณ์หรือข้อกังวลที่เกี่ยวข้องกับการใช้ AI

หลักการปฏิบัติร่วมกันและเกณฑ์ก่อนใช้งาน

7 หลักการจาก AI Policy ที่ทุกคนปฏิบัติเหมือนกัน — และคำถามที่ต้องตอบได้ก่อนเริ่มใช้ทุกครั้ง (หลักการข้อ 7 อยู่ในหน้าถัดไป)

1. ใช้ AI เป็นเครื่องมือสนับสนุนการทำงาน

ใช้ AI เพื่อช่วยสืบค้น วิเคราะห์ สรุป แปลภาษา และร่างเอกสาร โดยมีวัตถุประสงค์ที่ชัดเจนและสนับสนุนภารกิจขององค์กร

ตรวจสอบก่อนเริ่ม: ใช้ AI เพื่อวัตถุประสงค์ใด และเกี่ยวข้องกับภารกิจขององค์กรอย่างไร

2. ใช้เครื่องมือ AI ที่องค์กรแนะนำ

เลือกเครื่องมือและแพ็กเกจการใช้งานให้เหมาะสมกับระดับชั้นของข้อมูลที่จะใช้

ตรวจสอบก่อนเริ่ม: เครื่องมือและบัญชีที่จะใช้องค์กรแนะนำหรือไม่

3. รักษาความลับและคุ้มครองข้อมูลส่วนบุคคล

ห้ามนำข้อมูลลับ ข้อมูลส่วนบุคคล หรือข้อมูลอ่อนไหวเข้าสู่เครื่องมือ AI ที่ไม่ได้แนะนำ

ตรวจสอบก่อนเริ่ม: ข้อมูลที่จะนำเข้าอยู่ในระดับชั้นใด สามารถลดปริมาณข้อมูลหรือขจัดข้อมูลที่ระบุตัวบุคคลได้หรือไม่

4. ตรวจสอบผลลัพธ์ก่อนใช้ และรับผิดชอบต่อการนำไปใช้

ผู้ใช้งานต้องตรวจสอบผลลัพธ์จาก AI ก่อนนำไปใช้ และรับผิดชอบต่อผลลัพธ์ การตัดสินใจ และผลกระทบที่ตามมา

ตรวจสอบก่อนเริ่ม: ใครเป็นผู้ตรวจสอบผลลัพธ์ก่อนนำไปใช้

5. ใช้ AI อย่างโปร่งใสและเคารพทรัพย์สินทางปัญญา

ไม่แอบอ้างผลงานที่ AI สร้างขึ้นว่าเป็นผลงานที่ตนจัดทำขึ้นเองทั้งหมด และเคารพสิทธิในผลงานของผู้อื่น

ตรวจสอบก่อนเริ่ม: งานนี้ต้องเปิดเผยการใช้ AI ตามนโยบายขององค์กร ข้อกำหนดของผู้ให้ทุน หรือวารสารหรือไม่

6. รายงานความเสี่ยงโดยเร็ว

แจ้งเหตุการณ์หรือข้อกังวลที่เกี่ยวข้องกับการใช้ AI ทันทีที่พบ

ตรวจสอบก่อนเริ่ม: ทราบช่องทางรายงานเหตุการณ์แล้วหรือไม่ โดยแจ้งหัวหน้าฝ่ายและสำเนาถึง IT

ก่อนใช้ AI ควรหยุดและขอคำปรึกษาเมื่อ : มีข้อมูลส่วนบุคคล ข้อมูลลับ หรือข้อมูลอ่อนไหวเกี่ยวข้อง • จะนำผลลัพธ์ไปใช้ประกอบการตัดสินใจสำคัญ • ไม่แน่ใจข้อกำหนดของผู้ให้ทุน • เป็นเครื่องมือที่องค์กรไม่แนะนำ

7.ความเป็นเจ้าของผลงานและลิขสิทธิ์

แนวปฏิบัติ

- งานที่ผู้ปฏิบัติงานสร้างขึ้นด้วยบัญชี AI ขององค์กรในระหว่างการปฏิบัติหน้าที่ ให้ถือเป็นผลงานของ HITAP และให้ HITAP เป็นผู้ถือลิขสิทธิ์ โดยต้องมีข้อตกลงเป็นหนังสือรองรับ
- ห้ามใช้บัญชี AI ขององค์กรกับงานส่วนตัว งานรับจ้างภายนอก หรืองานที่ไม่เกี่ยวกับภารกิจของ HITAP
- เมื่อสิ้นสุดการจ้างหรือสิ้นสุดโครงการ ให้ส่งมอบบทสนทนา ไฟล์ และ prompt ที่เกี่ยวกับงานให้ต้นสังกัด ก่อนองค์กรปิดบัญชี
- ผลลัพธ์ที่ AI สร้างขึ้นทั้งหมดโดยไม่มีการสร้างสรรค์ของมนุษย์ อาจไม่ได้รับความคุ้มครองลิขสิทธิ์ จึงต้องมีการเรียบเรียงและตรวจแก้อย่างมีนัยสำคัญโดยมนุษย์ ก่อนนำไปใช้เป็นผลงานขององค์กร
- ก่อนเผยแพร่ ต้องตรวจว่าผลลัพธ์ไม่ได้ทำซ้ำงานของผู้อื่นโดยไม่อ้างอิง เพราะ AI อาจใช้ข้อความที่ใกล้เคียงต้นฉบับ
- ผู้ที่ไม่ใช่พนักงาน (นักศึกษาฝึกงาน ที่ปรึกษา ผู้รับจ้าง นักวิจัยร่วม) ต้องมีข้อสัญญาโอนสิทธิ์ในผลงาน ที่สร้างด้วยบัญชีขององค์กร ผูกเข้ากับสัญญาหรือ TOR

ฐานทางกฎหมาย

พ.ร.บ. ลิขสิทธิ์ พ.ศ. 2537

- มาตรา 9 — งานที่ลูกจ้างสร้างสรรค์ลิขสิทธิ์ตกแก่ “ลูกจ้าง” เว้นแต่ตกลงกันไว้เป็นหนังสือเป็นอย่างอื่น (นายจ้างมีสิทธิเผยแพร่ตามวัตถุประสงค์ของการจ้าง)
- มาตรา 10 — งานที่เกิดจากการรับจ้างลิขสิทธิ์ตกแก่ “ผู้ว่าจ้าง” เว้นแต่ตกลงกันเป็นอย่างอื่น
- ผลคือ ถ้าไม่มีข้อตกลงเป็นหนังสือลิขสิทธิ์ในงานของพนักงานประจำจะไม่ได้เป็นขององค์กร

การใช้ AI ในงานประเภทต่าง ๆ
AI Use Across Work Functions

ลักษณะงาน	สิ่งที่ต้องตรวจสอบ
การสนทนาและสืบค้นข้อมูล	ข้อเท็จจริงและความเป็นปัจจุบัน ความเหมาะสมของเนื้อหา แหล่งอ้างอิง
ร่างหนังสือ อีเมล	ชื่อ วันเวลา ตัวเลข สาระและความครบถ้วน ภาษาและรูปแบบ เหมาะกับผู้รับ ระดับความเป็นทางการ
แปลภาษาและปรับสำนวน	ความหมายเดิม ศัพท์เฉพาะ ชื่อตำแหน่ง และน้ำหนักของข้อสรุป
ถอดเสียงและสรุปประชุม	ขอความยินยอมก่อนบันทึก ตรวจสอบมติ
สร้างสื่อ งานนำเสนอ	ความถูกต้อง และการสื่อสารที่ไม่ทำให้เข้าใจผิด

ลักษณะงาน	สิ่งที่ต้องตรวจสอบ
ค้นคว้าและทบทวนวรรณกรรม	อ่านต้นฉบับ ยืนยันแหล่งอ้างอิง และตรวจว่าประเด็นสำคัญไม่ตกหล่น
วิเคราะห์ข้อมูลและเขียนโค้ด	ทดสอบกับข้อมูลสมมติก่อน ตรวจตรรกะ สมมติฐาน และผลคำนวณด้วยวิธีที่เชื่อถือได้
AI Agent / เชื่อมระบบ	ใช้เฉพาะการเชื่อมต่อที่ได้รับอนุมัติ จำกัดสิทธิ์ และให้คนยืนยันก่อนส่ง ลบ หรือแก้ไขข้อมูลสำคัญ

ลักษณะงาน	สิ่งที่ต้องตรวจสอบ
การสร้างและแก้ไขรูปภาพ	สิทธิ์ในสื่อต้นทาง การใช้ภาพบุคคลต้องได้รับอนุญาตตามขอบเขต ความถูกต้องของเนื้อหา ความเหมาะสม อคติ การไม่ทำให้เข้าใจผิด ไม่ใช้ภาพสร้างหรือภาพดัดแปลงเสมือนเป็นหลักฐานจริง คุณภาพของชิ้นงาน การเปิดเผยการใช้ AI
การสร้างภาพเคลื่อนไหวและวิดีโอ	
การสร้างเสียงสังเคราะห์และดนตรี	สิทธิ์ในเสียงและดนตรีต้นทาง การเลียนเสียงบุคคล ความถูกต้องและคุณภาพ ความเหมาะสมและการไม่ทำให้เข้าใจผิด การเปิดเผยการใช้ AI

การใช้ AI กับข้อมูลวิจัย

ก่อนนำข้อมูลวิจัยเข้าสู่ AI ต้องตรวจสอบให้ครบทั้ง 4 ด้าน

1

โครงร่างการวิจัย

ตรวจสอบว่าโครงร่างการวิจัย (Research Protocol) ที่ได้รับอนุมัติครอบคลุมวัตถุประสงค์ วิธีใช้ AI และประเภทข้อมูลที่จะนำเข้า

2

การให้ความยินยอม

ใช้ข้อมูลภายในขอบเขต informed consent ที่ผู้เข้าร่วมวิจัยได้รับทราบและยินยอมไว้

3

การรับรองจริยธรรม

ตรวจสอบเงื่อนไขที่คณะกรรมการจริยธรรมการวิจัย (IRB/EC) อนุมัติ รวมถึงข้อจำกัดในการใช้และเปิดเผยข้อมูล

4

ข้อตกลงและข้อกำหนดขององค์กร

ปฏิบัติตามข้อตกลงการแบ่งปันหรือใช้ข้อมูล (Data-sharing / Data-use Agreement) ข้อกำหนดของเจ้าของข้อมูล และแนวทางการใช้ AI ของ HITAP

ครบทั้ง 4 ด้าน → ใช้ตามขอบเขตของวัตถุประสงค์ • บันทึกการใช้ AI • ตรวจสอบผลลัพธ์ก่อนนำไปใช้

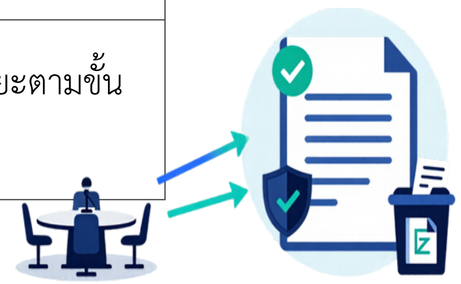
หากยังไม่ครบ หรือไม่ชัดเจน



หยุดการนำข้อมูลเข้าสู่ AI และขอคำปรึกษาจากผู้เกี่ยวข้อง หัวหน้า หรือผู้บริหาร ก่อนดำเนินการ

การถอดเสียงประชุม

ก่อนบันทึก	แจ้งผู้เข้าร่วมถึงการบันทึกและใช้ AI วัตถุประสงค์ ผู้มีสิทธิ์เข้าถึง และระยะเวลาเก็บข้อมูล พร้อมดำเนินการเรื่องการอนุญาตหรือความยินยอมตามข้อกำหนดที่เกี่ยวข้อง
เลือกเครื่องมือและบัญชี	ใช้เฉพาะเครื่องมือและบัญชีที่ HITAP อนุญาตสำหรับชั้นข้อมูลของการประชุมนั้น และขออนุมัติเมื่อเข้าข่ายข้อมูลลับ
ตรวจข้อมูลก่อนอัปโหลด	ห้ามนำข้อมูลต้องห้ามเข้า AI หากไฟล์เสียงมีข้อมูลดังกล่าว ให้ตัดช่วงนั้นออกก่อนอัปโหลด การลบข้อมูลจาก transcript ภายหลังไม่ถือเป็นการปกปิดก่อนส่ง
ตรวจผลลัพธ์	ตรวจชื่อผู้พูด ตัวเลข มติ และงานที่มอบหมายก่อนนำ transcript หรือสรุปประชุมไปใช้
การจัดเก็บไฟล์	เมื่อถอดเสียงเสร็จ ให้ดาวน์โหลดบทถอดเสียง (transcript) ไปเก็บบน SharePoint หรือคอมพิวเตอร์ โดยจำกัดการเข้าถึงเฉพาะผู้เกี่ยวข้อง และกำหนดระยะเวลาเก็บรักษาที่เหมาะสม
ลบไฟล์ออกจาก AI	เมื่อเก็บไฟล์ครบ ถอดเสียงเสร็จ ให้ลบไฟล์เสียง transcript และสรุปออกจากบริการ AI รวมถึงถังขยะตามขั้นตอนของบริการ โดยเฉพาะเมื่อเป็นบัญชีร่วมของทีมหรือฝ่าย ให้ลบทันทีเมื่อใช้งานเสร็จ



ความเสี่ยงในการใช้ AI

ตัวอย่างการใช้งานและเครื่องมือ	ถ้าใช้โดยไม่ระวัง จะเกิดอะไรขึ้น
1 ผู้ช่วยสนทนาทั่วไป ChatGPT · Claude · Gemini	• ตัวเลขหรือข้อเท็จจริงที่ AI แต่งขึ้น หลุดเข้าไปในรายงาน • ข้อความที่ paste เข้า prompt ควบคุมไม่ได้ถ้าใช้บัญชีส่วนตัว
2 ค้น/สังเคราะห์ข้อมูล NotebookLM · Perplexity · Elicit	• ได้อ้างอิงที่ไม่มีอยู่จริง หรือมีจริงแต่เนื้อหาไม่ตรงที่อ้าง • อัปโหลด full-text ที่ไม่มีสิทธิ์ ผิดเงื่อนไขลิขสิทธิ์
3 วิเคราะห์ข้อมูลและโค้ด Code Interpreter · GitHub Copilot	• โค้ดรันผ่าน แต่ตัวเลขผิดแบบไม่มี error ให้จับ • เผลออัปโหลดไฟล์ข้อมูลรายบุคคลทั้งชุดให้ AI วิเคราะห์
4 ถอดเทปและสรุปประชุม Teams · Zoom · Otter · Whisper	• บันทึกเสียงโดยผู้เข้าประชุมบางคนไม่ได้ยินยอม • ข้อมูลที่ยังไม่เผยแพร่ถูกเก็บไว้บนบริการภายนอก
5 แปลและขัดเกลาภาษา DeepL · Grammarly · Gemini	• ศัพท์เฉพาะ HTA และชื่อตำแหน่งราชการถูกแปลผิดความหมาย • AI แก้ประโยคจนเปลี่ยนน้ำหนักของข้อสรุปโดยไม่ทันสังเกต
6 สร้างภาพ สื่อ สไลด์ Canva · Gamma · ตัวสร้างภาพ	• ภาพคล้ายงานมีลิขสิทธิ์ หรือสิทธิ์เชิงพาณิชย์ไม่ครอบคลุม • สร้างภาพคนที่เหมือนบุคคลจริงโดยไม่ได้รับความยินยอม
7 AI Agent / เชื่อมระบบ Agent ที่เข้าถึงอีเมล ไฟล์ ปฏิทิน	• Agent เปิดไฟล์หรือส่งอีเมลเองโดยไม่มีคนยืนยันทีละขั้น • ดึงข้อมูลข้ามโครงการโดยไม่ตั้งใจ เมื่อเชื่อมเข้าระบบองค์กร

ไม่แนะนำให้ทำ (Red Lines)

งานวิจัยและวิชาการ

- ✗ ให้ AI คัดกรองวรรณกรรมลำพัง
  งานวิจัยพบว่าพลาดงานที่เข้าเกณฑ์ราว 1 ใน 5
- ✗ ใช้ citation ที่ AI สร้างโดยไม่เปิดต้นฉบับ
- ✗ ให้ AI ตีความผลหรือสรุปข้อค้นพบแทนผู้วิจัย
- ✗ ใส่ AI เป็นผู้แต่ง หรือปิดบังการใช้ AI

ระบบและการตัดสินใจ

- ✗ เปิด AI notetaker ก่อนได้ความยินยอมทุกคน
- ✗ ติดตั้ง extension AI นอกบัญชีที่อนุมัติ
- ✗ เชื่อม AI เข้าอีเมลหรือไฟล์องค์กรเอง
- ✗ ให้ AI ตัดสินใจเรื่องคนหรือเรื่องเงิน

ความเสี่ยงเหล่านี้ป้องกันได้ด้วย 3 อย่าง: เลือกเครื่องมือที่ HITAP แนะนำ · ไม่ใส่ข้อมูลเกินชั้นที่อนุญาต · ให้คนตรวจผลก่อนนำไปใช้เสมอ

ระดับความเสี่ยง
AI Risk Levels

ระดับความเสี่ยง

ยิ่งข้อมูลอ่อนไหว / ผลกระทบสูง / ต้องใช้เพื่อการตัดสินใจสำคัญ → ยิ่งต้องมีการอนุมัติและการตรวจสอบเข้มงวดขึ้น

ความเสี่ยงต่ำ

งานที่ใช้ AI ช่วยคิด ร่าง แปล หรือสรุปจากข้อมูลที่เปิดเผยต่อสาธารณะ หรือข้อมูลที่ได้รับอนุญาตให้ใช้ และไม่มีผลกระทบอย่างมีนัยสำคัญต่อบุคคล องค์กร หรือการตัดสินใจสำคัญ

ตัวอย่าง: Brainstorm, ปรับภาษา, ร่างอีเมล, สรุปเอกสารทั่วไป, ทำโครงร่าง PPT

แนวทาง: AI tools ส่วนตัวปิดการนำข้อมูลไปเทรน+ ตรวจผลลัพธ์ก่อนใช้ และ ต้องมี human review ก่อนเสมอ

ความเสี่ยงปานกลาง

งานที่ผลลัพธ์จาก AI อาจมีผลต่อคุณภาพงานหรือการสื่อสาร แต่ยังมีผู้รับผิดชอบตรวจสอบ แก้ไข และตัดสินใจก่อนนำไปใช้

ตัวอย่าง: วิเคราะห์ข้อมูลภายในที่ไม่ใช่ข้อมูลอ่อนไหว, สรุปรายงาน, ช่วยจัดทำ Presentation

แนวทาง: ตรวจแหล่งข้อมูล/บริบท + ระบุข้อจำกัดเมื่อเหมาะสม และ ต้องมี human review ก่อนเสมอ

ความเสี่ยงสูง

ผลลัพธ์จาก AI อาจส่งผลกระทบอย่างมีนัยสำคัญต่อสิทธิ ความเป็นส่วนตัว ความปลอดภัย ความน่าเชื่อถือของงานวิจัยหรือองค์กร หรือการตัดสินใจที่สำคัญ และต้องอยู่ภายใต้การกำกับดูแลและการทบทวนโดยมนุษย์อย่างเหมาะสม

ตัวอย่าง: วิเคราะห์ข้อมูลวิจัย, ช่วยตีความผล, เนื้อหาที่ใช้ประกอบการตัดสินใจสำคัญ

แนวทาง: Approval Required + ใช้เฉพาะ AI tools ที่ HITAP แนะนำ + ปรึกษาผู้รับผิดชอบ/หัวหน้าฝ่ายตามความเหมาะสม

ห้ามใช้

การใช้งานที่ขัด AI Policy กฎหมาย จริยธรรม

ตัวอย่าง: ป้อนข้อมูลลับ/ข้อมูลส่วนบุคคล/ข้อมูลอ่อนไหวเข้า AI ที่ไม่ได้รับอนุมัติ; สร้างหรือเผยแพร่ข้อมูลเท็จ/หลอกลวง; ใช้ AI ในลักษณะที่ละเมิดสิทธิหรือข้อกำหนด Automated decision ที่กระทบสิทธิบุคคลโดยไม่มี human review

แนวทาง: ห้ามใช้งาน และรายงานเหตุการณ์/ข้อกังวลตามช่องทางองค์กร

แผนผังการตัดสินใจเพื่อประเมินระดับความเสี่ยงในการใช้ AI

1. การใช้ AI นี้เกี่ยวข้องกับการตัดสินใจโดยอัตโนมัติ การใช้ข้อมูลลับโดยไม่ได้รับอนุญาต หรือการจงใจสร้างหรือเผยแพร่ข้อมูลเท็จ บิดเบือน หลอกลวง หรือก่อให้เกิดอันตรายหรือไม่
   - ใช่ → **ห้ามใช้**
     ห้ามใช้งานในลักษณะดังกล่าว และแจ้งหัวหน้าฝ่ายโดยสำเนาถึง IT
   - ไม่ → ข้อ 2

2. การใช้ AI นี้อาจส่งผลกระทบอย่างมีนัยสำคัญต่อสิทธิ ความเป็นส่วนตัว ความปลอดภัย การจ้างงาน หรือผลประโยชน์สำคัญอื่น ๆ ของบุคคลหรือไม่
   - ใช่ → **มีผู้ตรวจสอบ?**
     - ใช่ → **ความเสี่ยงสูง** — Approval Required
       ต้องขออนุมัติ · เฉพาะเครื่องมือที่แนะนำ
     - ไม่ → **ห้ามใช้**
   - ไม่ → ข้อ 3

3. การใช้ AI นี้เกี่ยวข้องกับข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ข้อมูลลับ ข้อมูลวิจัยที่ยังไม่เผยแพร่หรือมีข้อจำกัดในการใช้งาน หรือข้อมูลอื่นที่มีข้อจำกัดในการเข้าถึงหรือใช้งานหรือไม่
   - ใช่ → **ความเสี่ยงสูง** — Approval Required
     ต้องขออนุมัติ · เฉพาะเครื่องมือที่แนะนำ
   - ไม่ → ข้อ 4

4. หากผลลัพธ์จาก AI ไม่ถูกต้อง อาจส่งผลกระทบอย่างมีนัยสำคัญต่อคุณภาพงานหรือการสื่อสารขององค์กรหรือไม่
   - ใช่ → **ความเสี่ยงปานกลาง** — Human Review Required
     ต้องมีผู้ตรวจสอบผลลัพธ์ · ตรวจสอบแหล่งข้อมูล
   - ไม่ → ข้อ 5

5. การใช้ AI นี้เป็นงานทั่วไปที่ใช้ข้อมูลสาธารณะ และไม่มีข้อมูลส่วนบุคคลเกี่ยวข้องใช่หรือไม่
   - ใช่ → **ความเสี่ยงต่ำ** — Human Review Required
     ใช้เครื่องมือที่องค์กรแนะนำ · มีผู้ตรวจสอบผลลัพธ์
   - ไม่ → **ความเสี่ยงปานกลาง** — Human Review Required
     ต้องมีผู้ตรวจสอบผลลัพธ์ · ตรวจสอบแหล่งข้อมูล

การจัดการข้อมูลและการรักษาความลับ
Data & Confidentiality

Data & Confidentiality: ชั้นข้อมูลที่อนุญาตและห้ามนำเข้าสู่ AI

ชั้นข้อมูลแต่ละชั้นเชื่อมโยงกับระดับความเสี่ยง และแผนผังการตัดสินใจ เมื่อทราบชั้นข้อมูล จึงระบุแนวทางปฏิบัติที่ต้องดำเนินการได้

ชั้นที่ 1 — Low Risk

ข้อมูลสาธารณะ (Public data)

ใช้ได้ตามปกติ

รายงานที่ตีพิมพ์แล้ว · ข่าวประชาสัมพันธ์ · เอกสารบนเว็บไซต์องค์กร

ใช้กับเครื่องมือ AI ทั่วไปได้ โดยตรวจสอบผลลัพธ์ก่อนนำไปใช้

ชั้นที่ 2 — Moderate Risk

ข้อมูลภายใน (Internal Only data)

เฉพาะเครื่องมือที่ HITAP แนะนำ

ร่างเอกสารทั่วไป · บันทึกประชุมภายใน · คู่มือปฏิบัติงาน · แผนงาน
ไม่มีข้อมูลส่วนบุคคลหรือเนื้อหาที่เป็นข้อมูลลับ

ใช้เฉพาะเครื่องมือ AI ที่ HITAP แนะนำ

ชั้นที่ 3 — High Risk

ข้อมูลลับ (Confidential data)

ต้องขออนุมัติก่อน

ข้อมูลวิจัยที่ยังไม่เผยแพร่ · งบประมาณ · ข้อมูลบุคลากร · ข้อมูลส่วนบุคคลทั่วไป · MOU / NDA ที่มีเนื้อหาเป็นความลับ

ต้องได้รับอนุมัติก่อนนำเข้า และใช้เฉพาะเครื่องมือ AI ระดับองค์กร (Enterprise GenAI) ที่ HITAP แนะนำ

ชั้นที่ 4 — Prohibited

ข้อมูลที่ถูกจำกัด (Restricted data)

ห้ามทุกกรณี

ข้อมูลสุขภาพที่ระบุตัวตนได้ · พันธุกรรม · ชีวภาพ · เชื้อชาติ · ศาสนา · ข้อมูลอ่อนไหวอื่นที่ระบุตัวบุคคลได้โดยตรงหรือโดยอ้อม · รหัสผ่าน API key · ข้อมูลที่เจ้าของข้อมูลหรือ IRB/EC กำหนดห้ามนำเข้า AI

หมายเหตุ: หากมีข้อมูลหลายชั้น ให้ใช้ข้อกำหนดของชั้นสูงสุดที่อยู่ในไฟล์

ตัวอย่างชั้นข้อมูล

ชั้นที่ 1ข้อมูลสาธารณะ (Public data)

- ข้อมูลองค์กร: เนื้อหาบนเว็บไซต์และสื่อสังคมออนไลน์ ข้อมูลภาคีและโครงการร่วม รวมถึงโครงการของ HITAP และ GEAR
- งานการเงินและบัญชี: งบการเงิน รายรับ–รายจ่ายที่เผยแพร่แล้ว และหลักเกณฑ์ด้านการเงิน บัญชี และภาษีจากหน่วยงานภาครัฐ
- งานจัดซื้อจัดจ้างและ HR: ประกาศจัดซื้อจัดจ้าง ประกาศรับสมัครงาน และข้อมูลสวัสดิการที่เปิดเผยแล้ว
- แหล่งทุนและแนวทางวิจัย: ประกาศรับทุน ประเด็นวิจัย คู่มือและผลการประเมินฉบับสาธารณะ
- เอกสารสรุปเชิงนโยบาย (Policy Brief) อินโฟกราฟิก โปสเตอร์ และสไลด์นำเสนอที่ได้รับอนุญาตให้เผยแพร่ต่อสาธารณะแล้ว

- บทความวิชาการแบบเปิด (Open Access) และรายงานวิจัยฉบับเผยแพร่
- บทคัดย่อ ข้อมูลบรรณานุกรมและข้อมูลกำกับบทความ (Metadata) ที่เปิดเผยต่อสาธารณะ
- ชุดข้อมูลเปิดที่ไม่มีข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหวที่เชื่อมโยงถึงบุคคลได้ รวมถึงพจนานุกรมข้อมูลและข้อมูลตัวอย่างที่เจ้าของเผยแพร่ให้ใช้
- ข้อมูลสุขภาพและสถิติระดับรวมที่เผยแพร่แล้ว เช่น สถิติประชากร จำนวนผู้รับบริการ อัตราการเกิดโรค และตัวชี้วัดสุขภาพ โดยไม่สามารถระบุตัวบุคคลได้
- โค้ดและแบบจำลองที่เผยแพร่ต่อสาธารณะและอนุญาตให้นำไปใช้ตามเงื่อนไข

ข้อพิจารณาก่อนนำเข้า AI

- เข้าถึงหรือดาวน์โหลดได้ ไม่ได้หมายความว่านำเข้า AI ได้เสมอ ต้องตรวจสอบสิทธิ์การใช้งานและเงื่อนไขของแหล่งข้อมูล โดยเฉพาะบทความที่เข้าถึงผ่านสิทธิ์สมาชิกขององค์กร
- ใช้เฉพาะฉบับเผยแพร่ โดยไม่แนบความเห็นภายใน บันทึกส่วนตัว ผลวิเคราะห์ที่ยังไม่เผยแพร่ หรือข้อมูลจากโครงการเพิ่มเติม
- ข้อมูลสาธารณะที่มีข้อมูลส่วนบุคคลต้องพิจารณาตามเกณฑ์ข้อมูลส่วนบุคคล ไม่จัดเป็นชั้นที่ 1 เพียงเพราะค้นพบได้บนอินเทอร์เน็ต
- แม้เป็นข้อมูลชั้นที่ 1 ต้องตรวจสอบความถูกต้อง แหล่งอ้างอิง และความเหมาะสมของผลลัพธ์จาก AI ก่อนนำไปใช้
- บัญชี AI แบบฟรี: ปิดการนำข้อมูลไปใช้ฝึกโมเดล AI (AI Training)

ชั้นที่ 2 ข้อมูลภายใน (Internal Only data)

- ระเบียบภายใน คู่มือปฏิบัติงาน แบบฟอร์มเปล่า ร่างหนังสือโต้ตอบ และตารางงาน
- วาระและบันทึกประชุมทั่วไป รายการงานที่ต้องดำเนินการต่อ แผนกิจกรรม และร่างสไลด์ภายใน
- ขั้นตอนยื่นโครงการ แบบรายงาน ร่างแผนดำเนินงาน และ ToR เฉพาะส่วนที่ไม่มีรายละเอียดลับ
- ขั้นตอนเบิกจ่าย แบบฟอร์มเปล่า รายการตรวจสอบเอกสาร ปฏิทินปิดบัญชี และแบบงบประมาณที่ไม่มีข้อมูลจริง
- คู่มือพนักงาน แผนอบรม เอกสารปฐมนิเทศ และแบบประเมินเปล่า

- คู่มือดำเนินงานวิจัยทั่วไป ตารางดำเนินงาน คู่มือเตรียมต้นฉบับ แบบฟอร์ม Peer Review เปล่า และรายการตรวจสอบก่อนส่งบทความ
- แผนผลิตสื่อ แบบประชาสัมพันธ์ และร่างสื่อถ่ายทอดองค์ความรู้ที่ใช้ข้อมูลสาธารณะหรือผลงานที่เผยแพร่แล้ว

ข้อพิจารณาก่อนนำเข้า AI

- ใช้เฉพาะเครื่องมือ AI ที่ HITAP แนะนำ

ชั้นที่ 3 ข้อมูลลับ (Confidential data)

- บันทึกประชุมที่มีประเด็นลับ แผนกลยุทธ์ที่ยังไม่เปิดเผย ร่างข้อเสนอโครงการ ร่างสัญญา และรายละเอียดการเจรจากับภาคี
- งบประมาณและรายงานการเงินที่ยังไม่เผยแพร่ กระแสเงินสด รายละเอียดธุรกรรม และเอกสารเบิกจ่ายที่ระบุผู้รับเงินหรือเลขบัญชี
- ใบเสนอราคาที่มีเงื่อนไขเฉพาะ ผลเปรียบเทียบราคา คะแนนประเมินผู้เสนอราคา และข้อมูลการต่อรองที่ยังไม่เปิดเผย
- ประวัติผู้สมัครงาน สัญญาจ้าง เงินเดือน ผลประเมินการปฏิบัติงาน
- ข้อมูลหรือเอกสารที่มีข้อผูกพันในการรักษาความลับหรือข้อจำกัดในการใช้งาน
- ข้อมูลบุคลากรรายบุคคล เงินเดือน ผลประเมินการปฏิบัติงาน และข้อมูลผู้สมัครงาน
- ไฟล์ที่มีความคิดเห็น (Comments) หรือประวัติการแก้ไข (Track Changes): ตรวจทานและลบข้อมูลที่ไม่ควรเปิดเผย รวมถึงข้อความเดิมที่ยังคงอยู่ในประวัติการแก้ไข
- สัญญา MOU, NDA, DSA และเอกสารงบประมาณที่เป็นความลับ โดยต้องไม่ขัดต่อข้อกำหนดของคู่สัญญาหรือเจ้าของข้อมูล

- Manuscripts ของเราเองที่ยังไม่เผยแพร่ ปฏิบัติตามข้อกำหนดของวารสารหรือแหล่งทุน หากมีข้อมูลชั้นที่ 4 ให้ใช้ข้อกำหนดของชั้นที่ 4
- ข้อมูลผู้เข้าร่วมวิจัยรายชื่อและข้อมูลติดต่อ
- ชุดข้อมูลที่ผ่านการลดทอนข้อมูลระบุตัวตนแล้วแต่ยังไม่เผยแพร่ต่อสาธารณะ
- ร่างข้อเสนอแนะเชิงนโยบาย ผลวิจัยที่อยู่ระหว่างรอเผยแพร่ ความเห็นภาคีที่ให้เป็นความลับ

ข้อพิจารณาก่อนนำเข้า AI

- ต้องได้รับอนุมัติก่อนนำเข้า และใช้เฉพาะเครื่องมือ AI ระดับองค์กร (Enterprise GenAI) ที่ HITAP แนะนำ

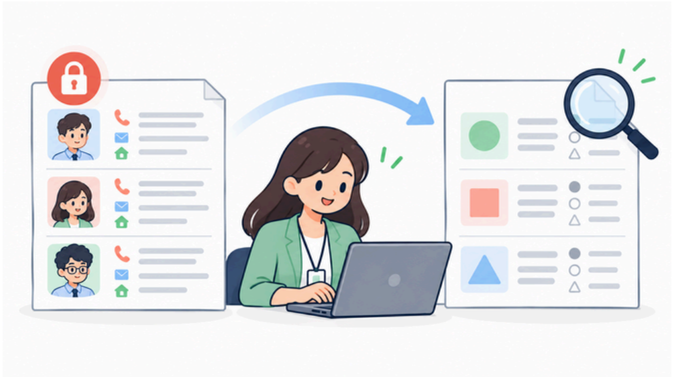
ชั้นที่ 4 ข้อมูลที่ถูกจำกัดการใช้งาน (Restricted data)

- ข้อมูลส่วนบุคคลหรือข้อมูลผู้เข้าร่วมวิจัยที่ระบุตัวตนได้โดยตรงหรือเชื่อมโยงกลับถึงบุคคลได้
- ข้อมูลระบุตัวตนที่มีความเสี่ยงต่อการสวมสิทธิ์ เลขบัตรประชาชน เลขหนังสือเดินทาง และสำเนาเอกสารยืนยันตัวตน
- เชื้อชาติ ศาสนา ความคิดเห็นทางการเมือง พฤติกรรมทางเพศ และประวัติอาชญากรรมที่เชื่อมโยงถึงบุคคลได้
- รหัสผ่านระบบธนาคาร รหัส PIN รหัส OTP และข้อมูลยืนยันตัวตนสำหรับทำธุรกรรม
- ใบรับรองแพทย์ ประวัติสุขภาพ ข้อมูลความพิการ ประวัติอาชญากรรม และข้อมูลลายนิ้วมือหรือใบหน้าที่ใช้ยืนยันตัวตน
- เอกสารประกอบที่มีข้อมูลสุขภาพหรือข้อมูลอ่อนไหวซึ่งระบุตัวบุคคลได้
- ข้อมูลอ่อนไหวสูงที่มีข้อจำกัดทางกฎหมาย จริยธรรม หรือสัญญากำกับไว้

- ข้อมูลสุขภาพที่ระบุตัวบุคคลได้
- แบบสอบถามหรือบทสัมภาษณ์ที่มีข้อมูลสุขภาพหรือข้อมูลอ่อนไหวและระบุตัวบุคคลได้
- กรณีศึกษาหรือคำสัมภาษณ์ที่เปิดเผยข้อมูลอ่อนไหวและระบุตัวบุคคลได้
- เวชระเบียนรายบุคคล ข้อมูลพันธุกรรมที่เชื่อมโยงถึงบุคคลได้
- รหัสผ่านหรือคีย์สำหรับเข้าถึงฐานข้อมูล
- ข้อมูลที่เจ้าของข้อมูล คณะกรรมการจริยธรรมการวิจัย (IRB/EC) กำหนดห้ามเปิดเผย และ/หรือ ห้ามนำเข้า AI
- Manuscripts under Peer Review ห้ามนำเข้าสู่ AI ทุกกรณี เพื่อรักษาความลับของกระบวนการพิจารณาบทความ
- บทความที่จำกัดการเข้าถึง (Restricted-access Articles)

หากงานมีข้อมูลที่ห้ามนำเข้าสู่ AI ต้องทำอย่างไร?

1. เลือกส่วนงานที่ให้ AI ช่วยได้
    - พิจารณาว่าต้องการให้ AI ช่วยอะไร และใช้เฉพาะข้อมูลส่วนที่จำเป็นต่องานนั้น ไม่ส่งเอกสารทั้งฉบับ
2. เตรียมข้อมูลก่อนนำเข้า AI
    - ลบ ปกปิด ตัดออก หรือแทนที่ข้อมูลต้องห้าม (Data Masking/Anonymization)
    - ตัดข้อมูลที่ไม่จำเป็น ปกปิดหรือแทนที่ข้อมูลระบุตัวตน และลดรายละเอียดที่อาจเชื่อมโยงกลับถึงบุคคล เช่น [บุคคล A] [องค์กร B]
    - ตรวจไฟล์ที่จะส่ง รวมถึง Comments, Track Changes และชีตที่ซ่อน
3. ให้ผู้อื่นช่วยตรวจสอบ
    - ให้เพื่อนร่วมทีมหรือหัวหน้าที่มีสิทธิ์เข้าถึงข้อมูลตรวจสอบว่าไม่มีข้อมูลต้องห้ามหลงเหลือ โดยเฉพาะชุดข้อมูลที่ซับซ้อน
4. ประเมินข้อมูลอีกครั้งหลังเตรียมข้อมูล/ไฟล์ และตรวจว่าเครื่องมือ บัญชี และวัตถุประสงค์การใช้เป็นไปตามข้อกำหนด ก่อนนำเข้า AI
    - หากครบถ้วนแล้ว ไม่ต้องส่งขออนุมัติ
5. หากยังจำเป็นต้องใช้ข้อมูลที่มีข้อจำกัด ให้ปรึกษาและขออนุมัติหัวหน้าฝ่ายเพื่อให้คำแนะนำ ร่วมกับ IT



Data Masking/Anonymization: ปกปิดและแทนที่ข้อมูลก่อนนำเข้าสู่ AI

ปกปิดหรือนำข้อมูลจริงที่ไม่ควรเปิดเผยออก และแทนด้วยข้อความหรือค่าสมมติ โดยคงเฉพาะรายละเอียดที่จำเป็นต่อการทำงาน

1. ข้อมูลต้นฉบับ
ตั้งต้นจากไฟล์จริงที่อยู่ในระบบขององค์กร

2. แทนที่ด้วยรหัสแทน
เปลี่ยนชื่อ ตัวเลข และสิ่งที่ระบุตัวตนเป็น placeholder

3. ให้ AI ทำงานจากบริบท
AI วิเคราะห์โครงสร้างและเหตุผล ไม่ต้องรู้ว่าใครเป็นใคร

4. คนใส่ข้อมูลจริงกลับ
ผู้รับผิดชอบงานนำค่าจริงกลับเข้าผลลัพธ์ในไฟล์ขององค์กร

ห้ามป้อนแบบนี้ เสี่ยงละเมิด PDPA และความลับ

“สรุปประวัติการรักษาของนายสมชาย เลขประจำตัวประชาชน 1-xxxx-xxxxx-xx-x ผู้ติดเชื้อ HIV และค้างชำระโรงพยาบาล A จำนวน 45,000 บาท”

มีทั้งชื่อจริง เลขบัตรประชาชน ข้อมูลสุขภาพที่อ่อนไหว และชื่อหน่วยงาน

ข้อความที่ผ่านการทำ Data Masking

“สรุปเคสของ [ผู้ป่วย-A] กลุ่มโรค [เรื้อรัง-01] มียอดค้างชำระ [จำนวน-X] บาท ควรมีแนวทางบริหารจัดการอย่างไร”

AI ยังตอบได้ตรงเหมือนเดิม เพราะสิ่งที่ต้องใช้คือโครงสร้างของปัญหา ไม่ใช่ตัวตนของผู้ป่วย

ตารางแทนค่าที่ใช้บ่อย เก็บตารางนี้ไว้ในไฟล์ของตนเองบนระบบขององค์กร ห้ามวางลงใน AI

ชื่อ-นามสกุล	**เลขประจำตัวประชาชน**	**วันเกิด**	**โรคหรือภาวะสุขภาพ**	**จำนวนเงินและงบประมาณ**	**ชื่อหน่วยงานและสถานพยาบาล**
→ [ผู้ป่วย-A] · [ผู้ให้ข้อมูล-1]	→ ตัดทิ้ง ไม่ต้องแทนค่า	→ ช่วงอายุ เช่น 45–49 ปี	→ [กลุ่มโรค-01]	→ [จำนวน-X] หรือสัดส่วนร้อยละ	→ [หน่วยงาน-1]

Data Masking/Anonymization: ปกปิดและแทนที่ข้อมูลก่อนนำเข้าสู่ AI

ปกปิดแล้ว ต้องตรวจสอบอะไรอีก?



รายละเอียดที่อาจเชื่อมโยงถึงบุคคล:

- ตรวจสอบอายุ เพศ อาชีพ พื้นที่ วันที่เข้ารับบริการ และเหตุการณ์เฉพาะ เมื่อพิจารณาร่วมกันแล้ว อาจบ่งชี้ว่าเป็นใครได้

บุคคลหรือกลุ่มที่มีลักษณะเฉพาะ

- ระวังข้อมูลโรคหายาก เหตุการณ์ที่เป็นข่าว หรือกลุ่มที่มีจำนวนน้อย แม้ไม่มีชื่อก็อาจระบุตัวบุคคลหรืออนุมานข้อมูลอ่อนไหวได้

ลดรายละเอียดให้เหมาะกับงาน

- เปลี่ยนอายุเป็นช่วงอายุ ขยายพื้นที่จากหมู่บ้านเป็นจังหวัด ลดความละเอียดของวันที่ หรือตัดรายการที่มีความเสี่ยงสูงออก

ตรวจสอบความเสี่ยงหลังปรับข้อมูล

- ประเมินว่ายังเชื่อมโยงกลับถึงบุคคลได้หรือไม่ และข้อมูลที่ปรับแล้วยังเหมาะกับวัตถุประสงค์ของงานหรือไม่

ให้มีผู้ร่วมตรวจสอบ

- ควรให้มีผู้ร่วมตรวจสอบประเมินเพิ่มเติม เช่น เพื่อนร่วมทีม PI หัวหน้าฝ่าย

Data Masking/Anonymization: ปกปิดและแทนที่ข้อมูลก่อนนำเข้าสู่ AI

แทนชื่อด้วยรหัสแล้ว อาจยังระบุตัวบุคคลได้

- แม้เปลี่ยนชื่อเป็น “ผู้เข้าร่วม A” แต่รายละเอียดอื่นอาจทำให้รู้ว่าเป็นใคร เช่น “ผู้หญิงอายุ 47 ปี เป็นผู้อำนวยการโรงเรียนแห่งเดียวในตำบลและเข้ารักษาในวันที่ระบุ” คนที่รู้จักหรือมีข้อมูลอื่นอาจเชื่อมโยงได้
- ห้ามส่งตารางจับคู่รหัสกับข้อมูลจริงเข้า AI รายการที่บอกว่า “ผู้เข้าร่วม A = ใคร” หากส่งตารางนี้เข้า AI ด้วย การแทนชื่อก็ไม่ช่วยปกปิดตัวตน จึงต้องเก็บตารางแยกไว้ และจำกัดผู้เข้าถึง

จึงควร

- สร้างไฟล์ใหม่เฉพาะข้อมูลที่จำเป็น ไม่ใช้ไฟล์เดิมที่เพียงซ่อนคอลัมน์หรือซ่อนชีตตารางจับคู่ไว้
- ตัดรายละเอียดที่เชื่อมโยงถึงบุคคลได้ เช่น ชื่อโรงเรียน ตำแหน่งเฉพาะ ที่อยู่ละเอียด และวันที่เข้ารับบริการ หากไม่จำเป็นต่องาน
- เก็บตารางจับคู่แยกจากไฟล์ที่จะส่ง ไว้ในพื้นที่ขององค์กรที่จำกัดสิทธิ์เฉพาะผู้เกี่ยวข้อง ไม่แนบ ไม่คัดลอกลงบทสนทนา และไม่เชื่อม AI เข้าถึงพื้นที่นั้น



Data Masking/Anonymization: ปกปิดและแทนที่ข้อมูลก่อนนำเข้าสู่ AI

การวางกล่องสีทับข้อความหรือซ่อนแถวในตารางไม่ใช่การลบข้อมูล

วางกล่องสีทับหรือซ่อนแถวแล้ว เป็นเพียงการซ่อนจากสายตา ข้อมูลต้นฉบับอาจยังอยู่ในไฟล์ เช่น

- Word หรือ PDF: วางสี่เหลี่ยมสีดำทับชื่อ แต่ข้อความด้านล่างอาจยังเลือก คัดลอก หรือดึงออกมาได้
- Excel: ซ่อนแถว คอลัมน์ หรือชีต แต่ผู้รับสามารถเปิดให้แสดงอีกครั้ง และโปรแกรมอาจอ่านข้อมูลที่ซ่อนไว้ได้

จึงควร

- ลบข้อมูลออกจากสำเนาที่จะส่งจริง ๆ หรือใช้วิธีปกปิดถาวร (Redaction) ที่ลบเนื้อหาต้นฉบับ แล้วตรวจไฟล์อีกครั้ง สำหรับตาราง อาจสร้างไฟล์ใหม่ที่มีเฉพาะข้อมูลที่อนุญาตให้นำเข้า AI ค่ะ
- สร้างเอกสารใหม่ที่มีเฉพาะเนื้อหาที่จำเป็น ลบหรือแทนที่ข้อมูลต้องห้าม และให้ผู้ช่วยตรวจสอบก่อนนำเข้า AI หากไม่สามารถเตรียมไฟล์ได้อย่างมั่นใจ ให้ปรึกษา IT



การขออนุมัติการใช้ข้อมูลกับ AI ภายในองค์กร

ใช้เมื่อจะนำข้อมูลชั้นที่ 3 เข้า AI หรือจะใช้เครื่องมือ AI นอกรายการที่แนะนำ ทุกขั้นต้องเป็นลายลักษณ์อักษร เพื่อให้ตรวจย้อนหลังได้ว่าใครอนุมัติอะไร เมื่อใด

เมื่อใดต้องขออนุมัติใช้ AI

ใช้ได้โดยไม่ต้องขออนุมัติเป็นรายครั้ง

- ข้อมูลชั้นที่ 1 มีคนตรวจสอบเสมอ
- ข้อมูลชั้นที่ 2 ใช้เฉพาะเครื่องมือและบัญชีที่ HITAP แนะนำ

ต้องขออนุมัติก่อนเสมอ

- นำข้อมูลชั้นที่ 3 มาใช้กับ AI (ข้อมูลลับ)
- นำข้อมูลชั้นที่ 2 (ข้อมูลภายใน) มาใช้เครื่องมือ AI ที่ HITAP ไม่ได้แนะนำ
- เชื่อมต่อ AI กับอีเมล แหล่งเก็บไฟล์ หรือระบบขององค์กร
- ใช้ AI ประเมิน จัดอันดับ หรือเสนอแนะเพื่อประกอบการตัดสินใจที่กระทบสิทธิของบุคคล การจ้างงาน หรือการอนุมัติทางการเงิน

ขออนุมัติไม่ได้ ห้ามนำเข้า AI

- ข้อมูลชั้นที่ 4
- ข้อมูลหรือเอกสารที่มีข้อกำหนดห้ามใช้กับ AI

ยื่นคำขออย่างไร

- ช่องทาง: ส่งอีเมลถึงหัวหน้าฝ่าย และสำเนาถึง IT
- หัวเรื่อง: [ขออนุมัติใช้ข้อมูลกับ AI] ชื่องานหรือโครงการ
- รายละเอียดคำขอ: ระบุว่าจะนำข้อมูลอะไรเข้า AI ชั้นข้อมูลใด ใช้เพื่ออะไร เหตุใดจึงจำเป็นต้องใช้ข้อมูลดังกล่าว เครื่องมือ ประเภทบัญชี ผู้ใช้งาน ผู้ตรวจสอบผลลัพธ์ และระยะเวลาที่ต้องการใช้
- ข้อมูลประกอบ: อธิบายลักษณะข้อมูลและรายการข้อมูลที่จะใช้ โดยไม่แนบไฟล์ข้อมูลจริงทั้งชุด
- ระหว่างรอผล: ห้ามนำข้อมูลที่ขออนุมัติเข้า AI จนกว่าจะได้รับอนุมัติเป็นลายลักษณ์อักษร
- หลักฐาน: เก็บอีเมลอนุมัติพร้อมขอบเขตและเงื่อนไขไว้ใช้อ้างอิง

การขออนุมัติการใช้ข้อมูลกับ AI ภายในองค์กร

1 ผู้ใช้งาน: เตรียมคำขอก่อนส่ง

- ระบุชั้นข้อมูล และประเมินความเสี่ยงของการใช้งานตาม Decision Tree
- ใช้ข้อมูลเท่าที่จำเป็น โดยลบหรือปกปิดรายละเอียดที่ไม่จำเป็นก่อนเสนอขออนุมัติ
- ระบุวัตถุประสงค์ ชุดข้อมูลและชั้นข้อมูล เครื่องมือและประเภทบัญชี ผู้ใช้งาน ผู้ตรวจสอบผลลัพธ์ และระยะเวลาที่ต้องการใช้

2 หัวหน้าฝ่าย: กลั่นกรองความจำเป็นและขอบเขตงาน

- พิจารณาว่าจำเป็นต้องใช้ข้อมูลจริงหรือไม่ และใช้ข้อมูลสมมติหรือข้อมูลที่ลดรายละเอียดแทนได้หรือไม่
- ตรวจสอบความสอดคล้องกับขอบเขตโครงการ เงื่อนไข IRB/EC และข้อตกลงที่เกี่ยวข้อง เช่น MOU / NDA / DSA
- หากเห็นชอบ ให้ส่งต่อฝ่าย IT หากไม่เห็นชอบ ให้ส่งคืนผู้ขอพร้อมเหตุผลเป็นลายลักษณ์อักษร

3 IT: ตรวจสอบความเหมาะสมของเครื่องมือและมาตรการคุ้มครองข้อมูล

- ตรวจสอบว่าเครื่องมือและประเภทบัญชีได้รับอนุมัติให้รองรับข้อมูลชั้นที่ขอใช้หรือไม่
- ตรวจสอบเงื่อนไขการนำข้อมูลไปฝึกโมเดล ระยะเวลาจัดเก็บ และวิธีลบข้อมูล
- ตรวจสอบเงื่อนไขผู้ให้บริการ สถานที่จัดเก็บและประมวลผลข้อมูล การเชื่อมต่อระบบและสิทธิ์การเข้าถึง
- สรุปผลการตรวจสอบ ความเสี่ยง และเงื่อนไขที่เสนอ เพื่อประกอบการพิจารณาอนุมัติ

4 ผู้บริหารร่วมกับฝ่าย IT พิจารณาและอนุมัติ

- แจ้งผลการพิจารณาเป็น อนุมัติ / อนุมัติแบบมีเงื่อนไข / ไม่อนุมัติ พร้อมเหตุผลและเงื่อนไขที่เกี่ยวข้อง
- ระบุขอบเขตให้ชัดเจน ได้แก่ ผู้มีสิทธิ์ใช้งาน ชุดข้อมูล เครื่องมือและบัญชี วัตถุประสงค์ และระยะเวลาที่อนุมัติ
- แจ้งผลให้ผู้ขอทราบเป็นลายลักษณ์อักษร และบันทึกผลพร้อมเงื่อนไขไว้ในทะเบียนการอนุมัติ

5 หลังได้รับอนุมัติ — ใช้งาน ทบทวน และปิดสิทธิ์

- ใช้เฉพาะเครื่องมือ บัญชี ชุดข้อมูล และวัตถุประสงค์ที่ได้รับอนุมัติ
- หากเปลี่ยนเครื่องมือ ชุดข้อมูล หรือขยายขอบเขตการใช้งาน ต้องขออนุมัติใหม่ก่อนดำเนินการ
- ตรวจสอบผลลัพธ์โดยผู้รับผิดชอบก่อนนำไปใช้ทุกครั้ง (Human Review) และให้หัวหน้าพิจารณาเพิ่มเติมตามระดับความเสี่ยงหรือเงื่อนไขการอนุมัติ
- เมื่อสิ้นสุดโครงการหรือครบกำหนดการอนุมัติ ให้หยุดใช้งานในขอบเขตนั้น และแจ้งฝ่าย IT เพื่อปิดสิทธิ์ที่เกี่ยวข้อง

การอนุมัติผูกกับข้อมูลชุดนั้น + เครื่องมือตัวนั้น + ช่วงเวลานั้น เท่านั้น · อนุมัติแล้วผู้ใช้งานยังรับผิดชอบผลลัพธ์เสมอ · ไม่แน่ใจ = หยุดก่อน ปรึกษาหัวหน้าฝ่าย , IT

เครื่องมือที่แนะนำ
Recommended AI Tools

ทะเบียนบัญชี AI (1): การใช้เครื่องมือ AI ฟรีผ่านบัญชีส่วนบุคคล

ใช้ได้เฉพาะข้อมูลชั้นที่ 1 ตามแนวทางของ HITAP โดยต้องตรวจสอบเงื่อนไขการใช้ข้อมูลและการตั้งค่าของแต่ละบริการก่อนเริ่มใช้งาน

เครื่องมือ	ตัวอย่างการใช้งาน	ข้อควรตรวจสอบก่อนใช้
ChatGPT	ผู้ช่วยทั่วไป เขียน สรุป วิเคราะห์	ปิด training ในตั้งค่า
Claude	อ่านเอกสารยาว วิเคราะห์ และเรียบเรียง	ไม่ใช้ฝึกโมเดลโดยค่าเริ่มต้น
Gemini	ผู้ช่วยทั่วไป สรุปและถาม-ตอบจากเอกสารของเราเอง	ปิด Gemini Apps Activity
Canva · CapCut	กราฟิก สไลด์ อินโฟกราฟิก และตัดต่อวิดีโอ	ตรวจสิทธิ์ภาพก่อนเผยแพร่
V2md	แปลงเอกสารเป็นข้อความสำหรับใช้งานต่อ	ตรวจว่าประมวลผลที่ใด
AISysRev	คัดกรอง title และ abstract ในการทบทวนวรรณกรรม	ส่งต่อ API ภายนอก
Grammarly	ขัดเกลาภาษาอังกฤษเชิงวิชาการ	ปิดการเก็บข้อความ
DeepL	แปลไทย–อังกฤษ	ห้ามวางเอกสารทั้งฉบับ
Perplexity	ค้นข้อมูลพร้อมลิงก์ — ใช้เป็นตัวช่วยหาแหล่ง	ต้องเปิดลิงก์ตรวจทุกครั้ง

ข้อปฏิบัติในการใช้บัญชี AI ส่วนตัว

ใช้ได้แค่ไหน

- ใช้ได้กับข้อมูลชั้นที่ 1 เท่านั้น คือข้อมูลที่เผยแพร่ต่อสาธารณะแล้ว
- ห้ามใช้กับข้อมูลชั้นที่ 2 ขึ้นไปโดยเด็ดขาด แม้จะรู้สึกว่าไม่เป็นความลับก็ตาม

ต้องทำก่อนใช้ทุกครั้ง

- ปิดการนำข้อมูลไปฝึกโมเดลในหน้าตั้งค่าของเครื่องมือนั้น และตรวจซ้ำเมื่อผู้ให้บริการอัปเดต
- ไม่แชร์ลิงก์บทสนทนาที่มีเนื้อหาเกี่ยวกับงานขององค์กร

ความเข้าใจผิดที่พบบ่อย

- สมัครบัญชีฟรีด้วยอีเมลขององค์กร ไม่ได้ทำให้กลายเป็นบัญชีองค์กร สิทธิ์และสัญญายังเป็นแบบบัญชีส่วนตัว
- ผลงานที่สร้างด้วยบัญชีส่วนตัวในระหว่างปฏิบัติหน้าที่ยังถือเป็นผลงานขององค์กร

ทะเบียนบัญชี AI (2): เครื่องมือที่ HITAP แนะนำ

ใช้ได้เฉพาะข้อมูลชั้นที่ 1-2

กลุ่มหลัก (Core) — บัญชีระดับองค์กร

เครื่องมือ	ตัวอย่างการใช้งาน	ชั้นข้อมูล
Microsoft 365 Copilot	ทำงานบนไฟล์ อีเมล และการประชุมในระบบเดิมขององค์กร	1-2
ChatGPT Team	ผู้ช่วยทั่วไป เขียน สรุป วิเคราะห์	1-2
Claude Team	เอกสารยาว วิเคราะห์ และช่วยเขียนโค้ด	1-2
Canva Pro · CapCut Pro	กราฟิก สไลด์ อินโฟกราฟิก และวิดีโอ	1-2
ChatPDF	อ่าน ถาม-ตอบ และสรุปจากเอกสาร PDF	1-2
Mentimeter	สร้างงานนำเสนอแบบมีส่วนร่วม โพล และแบบทดสอบ	1
Zotero · EndNote	จัดการและยืนยันรายการอ้างอิง	1-2

กลุ่มถอดเสียงและสรุปการประชุม (Transcript)

เครื่องมือ	ตัวอย่างการใช้งาน	ชั้นข้อมูล
Otter.ai	ถอดเสียงประชุม สร้าง transcript และสรุปการประชุม	1-2
Transkriptor	ถอดเสียงประชุม สร้าง transcript และสรุปการประชุม	1-2

แนวทางการใช้งาน

บัญชีองค์กรต่างจากบัญชีฟรีอย่างไร

- ผู้ให้บริการมีสัญญากับองค์กรว่าไม่นำข้อมูลไปฝึกโมเดล จึงใช้กับชั้นที่ 2 ได้ แต่ข้อมูลยังออกไปอยู่บนระบบของผู้ให้บริการ

การถอดเสียงประชุม

- หลีกเลี่ยงการอัปโหลดข้อมูลส่วนบุคคลที่อ่อนไหว หรือข้อมูลวิจัยที่เป็นความลับ
- หากจำเป็นต้องใช้ ให้ปกปิดข้อมูลระบุตัวตนก่อนอัปโหลด
- เมื่อถอดเสียงเสร็จ ให้ดาวน์โหลด transcript ไปเก็บบน SharePoint แล้วลบไฟล์ออกจากระบบ AI
- บัญชีที่ใช้ร่วมกันหลายคน ต้องลบทั้งไฟล์เสียงและ transcript ทุกครั้งหลังใช้เสร็จ

รอพิจารณาขึ้นทะเบียน

- NotebookLM · V2md · AISysRev — ฝ่ายแจ้งว่าใช้อยู่ แต่ยังไม่อยู่ในทะเบียน ต้องตรวจก่อนว่าส่งข้อมูลออกนอกองค์กรหรือไม่
- ฟีเจอร์ AI ที่เพิ่มเข้ามาใหม่ในซอฟต์แวร์ที่ HITAP แนะนำ ยังไม่ถือว่าผ่านการตรวจสอบความปลอดภัย ให้แจ้งฝ่าย IT เพื่อประเมินก่อนใช้กับข้อมูลชั้นที่ 2 ขึ้นไป

การตั้งค่า ปิดการใช้ข้อมูลเพื่อฝึกโมเดล

- **ChatGPT:** Settings → Data controls → ปิด “Improve the model for everyone”
- **Claude:** Settings → Privacy → ปิด “Help Improve our AI models”
- **Gemini:** Gemini Apps Activity → ปิด “Keep Activity” (เหลือเก็บ 72 ชั่วโมง)
- **Copilot แบบฟรี:** ไม่มีการรับประกันระดับองค์กร — ห้ามใช้กับข้อมูลชั้นที่ 2 ขึ้นไป
- **ปิดแล้วยังไม่พอ:** ข้อมูลชั้นที่ 2 ขึ้นไป ต้องใช้บัญชีอีเมลองค์กรเท่านั้น

ทำครั้งเดียวต่อบัญชี — เมนูอาจเปลี่ยนตามเวอร์ชัน

ตั้งค่าก่อนเริ่มใช้งาน และตรวจสอบเป็นระยะ หากไม่พบเมนูหรือไม่แน่ใจ ให้สอบถาม IT

การตั้งค่าบัญชีช่วยลดความเสี่ยง แต่ไม่ได้ทำให้ข้อมูลชั้นสูงกลายเป็นข้อมูลที่ใส่ได้ — ผู้ใช้งานรับผิดชอบข้อมูลที่ป้อนเข้า AI เสมอ

ปิดการฝึกโมเดล ≠ ไม่เก็บข้อมูล และไม่เปลี่ยนชั้นความลับของข้อมูล

การใช้งานเครื่องมือ AI อย่างปลอดภัย

ห้ามอนุญาตให้เครื่องมือ AI เข้าถึงข้อมูลภายในเครื่องทั้งหมด



จำกัดสิทธิ์เฉพาะโฟลเดอร์ที่ใช้งานเท่านั้น

เพื่อความปลอดภัยของข้อมูลโปรดปฏิบัติตาม AI Policy

1 แยกพื้นที่ทำงาน AI ออกจากโฟลเดอร์ที่ซิงค์ OneDrive



สร้างโฟลเดอร์เฉพาะแยกออกจากโฟล์เดอร์ที่ซิงค์กับ OneDrive
เช่น D:\ai-workspace
หากไม่แน่ใจให้ปรึกษา IT

2 คัดลอกไฟล์ที่ต้องใช้เข้า workspace และนำผลลัพธ์ออก

ปกปิดข้อมูลที่เป็นความลับก่อนนำเข้า AI



3 ระบุโฟลเดอร์เป้าหมายให้ชัดเจนทุกครั้งเมื่อสั่ง AI ค้นหาหรือเข้าถึงไฟล์

หลีกเลี่ยงคำสั่ง“ค้นทั้งเครื่อง , ค้นหาทั้งหมดให้เจอ”



ระบุโฟลเดอร์เป้าหมายให้ชัดเจน



ค้นทั้งเครื่อง / อนุญาตทั้งหมด

ขอความร่วมมือทุกท่าน ปฏิบัติตามอย่างเคร่งครัด

คุณภาพและความโปร่งใส
Quality & Transparency

การตรวจสอบคุณภาพและการทบทวนโดยผู้รับผิดชอบ
Quality & Human Review

ผลลัพธ์จาก AI ถือเป็น “ร่าง” จนกว่าจะผ่านการตรวจสอบความถูกต้องและความเหมาะสมโดยผู้รับผิดชอบ ก่อนนำไปใช้หรือเผยแพร่

1	**ความถูกต้องตามข้อเท็จจริง**	ข้อเท็จจริงเชิงตัวเลข แหล่งอ้างอิงมีอยู่จริง ข้อมูลเป็นปัจจุบัน
2	**หลักฐานและแหล่งอ้างอิง**	แหล่งอ้างอิงมีอยู่จริง สนับสนุนข้อความที่อ้าง และเพียงพอต่อข้อสรุป
3	**ความเป็นกลางและตรรกะ**	ไม่มีอคติหรือการเหมารวมด้านเพศ วัฒนธรรม และค่านิยม นำเสนอประเด็นขัดแย้งตามหลักฐาน ไม่เข้าข้างโดยไม่มีเหตุผลรองรับ แยกข้อเท็จจริงออกจากความคิดเห็นอย่างชัดเจน
4	**ความครบถ้วน**	ครอบคลุมเงื่อนไข ข้อยกเว้น และข้อจำกัดที่เกี่ยวข้อง มีรายละเอียดเพียงพอต่อการนำไปใช้หรือตัดสินใจ ไม่สรุปจนขาดสาระสำคัญ
5	**ความพร้อมก่อนส่งต่อ**	ไม่มีข้อมูลที่ไม่อนุญาตให้เปิดเผย ตรวจสิทธิ์การใช้เนื้อหา และเปิดเผยการใช้ AI ตามข้อกำหนด

การตรวจสอบคุณภาพและการทบทวนโดยผู้รับผิดชอบ
Quality & Human Review

ความถูกต้องตามข้อเท็จจริง

- ตัวเลขทุกตัวตรงกับแหล่งต้นทาง — เปิดไฟล์ต้นฉบับเทียบทุกครั้ง
- ชื่อคน หน่วยงาน ยา และโรค สะกดถูกและมีอยู่จริง
- หน่วยและสกุลเงินถูกต้อง (บาท / USD, ต่อปี / ต่อครั้ง)
- ผลลัพธ์สอดคล้องกับบริบทของไทยและขององค์กรหรือไม่
- ตรวจความครบถ้วน — มีอะไรที่ AI ตัดออกโดยไม่บอกหรือไม่
- ระวังคำตอบที่ฟังดูมั่นใจแต่ไม่มีหลักฐานรองรับ
- ถามซ้ำแล้วได้คำตอบต่างกัน = ยังเชื่อไม่ได้

แหล่งอ้างอิง

- เปิดเอกสารต้นฉบับทุกรายการ — ห้ามเชื่อรายการที่ AI สร้าง
- ตรวจว่า DOI / PMID เปิดได้จริง และตรงกับเรื่องที่อ้าง
- ตรวจว่าผู้แต่ง ปี และวารสาร ตรงกับตัวจริง
- ตรวจว่าข้อความที่อ้างมีอยู่ในเอกสารนั้นจริง ไม่ใช่ถูกสรุปเกิน
- ระวัง citation ที่ดูสมเหตุสมผลแต่ไม่มีอยู่จริง (hallucination)
- ใช้โปรแกรมที่เชื่อถือได้หรือฐานข้อมูลจริงยืนยันทุกรายการ
- รายงานกลยุทธ์การสืบค้นฉบับที่ใช้จริง ไม่ใช่ฉบับที่ AI ร่างให้

การตรวจสอบข้อมูลและแหล่งอ้างอิงที่ AI อาจสร้างขึ้น (Hallucination)

AI อาจให้ข้อมูลที่ดูน่าเชื่อถือแต่ไม่ถูกต้อง รวมถึงสร้างชื่อผู้แต่ง ชื่อบทความ ปีที่พิมพ์ วารสาร DOI หรือ URL ที่ไม่มีอยู่จริง ผู้ใช้งานจึงต้องตรวจสอบกับแหล่งต้นทางก่อนนำไปใช้



สัญญาณที่ต้องตรวจสอบเพิ่มเติม

1. ตัวเลขที่ไม่มีหลักฐานรองรับ: เช่น ร้อยละของประสิทธิภาพหรืองบประมาณที่ประหยัดได้ โดยไม่ระบุแหล่งข้อมูล วิธีคำนวณ หรือเงื่อนไข
2. การอ้างกฎหมายหรือข้อบังคับไม่ครบถ้วน: ไม่ระบุชื่อกฎหมาย ฉบับ ปี หรือมาตราให้ตรวจสอบได้
3. แหล่งอ้างอิงตรวจสอบไม่ได้: เปิดลิงก์ไม่ได้ ค้นไม่พบเอกสาร หรือ DOI เชื่อมไปยังบทความคนละเรื่อง
4. ข้อมูลปัจจุบันที่ไม่ระบุแหล่งและวันที่: เช่น ข่าว นโยบาย หรือสถานการณ์ล่าสุดที่ยังไม่ได้ตรวจสอบกับแหล่งข้อมูลปัจจุบัน
5. ข้อความอ้างอิงอย่างกว้าง ๆ: เช่น “งานวิจัยพบว่า” หรือ “ผู้เชี่ยวชาญเห็นตรงกัน” โดยไม่ระบุว่าเป็นงานวิจัยใดหรือใครเป็นผู้ให้ความเห็น



แนวทางปฏิบัติ

- ตรวจข้อเท็จจริงและตัวเลขกับเอกสารต้นฉบับหรือแหล่งข้อมูลที่เชื่อถือได้
- ตรวจว่าแหล่งอ้างอิงมีอยู่จริง รายละเอียดตรงกัน และเนื้อหาสนับสนุนข้อความที่อ้างอิง
- ตรวจข้อมูลที่เปลี่ยนแปลงได้กับแหล่งทางการฉบับปัจจุบัน แม้ AI จะใช้ระบบค้นหาเว็บแล้วก็ตาม
- หากยังยืนยันไม่ได้ ให้นำข้อมูลนั้นจากชิ้นงาน และส่งให้ผู้รับผิดชอบหรือผู้เชี่ยวชาญตรวจสอบก่อนใช้
- หากนำข้อมูลผิดไปใช้แล้ว ให้ดำเนินการตามแนวทางรายงานเหตุการณ์ของ HITAP

การถามค้านและตรวจสอบซ้ำ (Cross-Examination Prompting)

ใช้ AI ช่วยทบทวนจากมุมมองผู้ตรวจสอบ แทนการถามเพียงว่า “คำตอบนี้ถูกต้องหรือไม่” ให้ขอ AI ตรวจหาข้อผิดพลาด ข้อสันนิษฐานที่ไม่มีหลักฐาน ข้อมูลที่ตกหล่น และข้อโต้แย้งที่ควรพิจารณา อาจเปิดบทสนทนาใหม่เพื่อแยกการทบทวนออกจากการร่างเดิม

Ex 1:

สวมบทบาทผู้ตรวจสอบบัญชีและตรรกะ (The Strict Auditor Role)

[Role]: คุณคือผู้ตรวจสอบภายใน (Internal Auditor) ที่มีความเข้มงวดสูงมาก และยึดมั่นในความถูกต้อง ของข้อมูล 100% [Task]: จงตรวจสอบร่างรายงานต่อไปนี้อย่างละเอียด:

[วางข้อความ/รายงานที่ได้จาก AI]

[Instructions]:

1. ค้นหาจุดบกพร่อง ช่องโหว่ทางตรรกะ หรือจุดที่มีการอ้างอิงเลื่อนลอยมาอย่างน้อย 3 จุด

2. ชี้จุดที่อาจมีตัวเลขหรือการคำนวณที่ผิดพลาด 3. ระบุประเด็นที่รายงานฉบับนี้มองโลกในแง่ดีเกินไป (Overly Optimistic) พร้อมเสนอฉากทัศน์ความเสี่ยง (Worst-Case Scenario)

Ex 2:

สวมบทบาทนักวิพากษ์วิชาการ (Devil's Advocate Reviewer)

[Role]: คุณคือนักวิชาการอาศรมความคิด (Devil's Advocate) มีหน้าที่จับผิดและตั้งคำถามค้านกับทุกข้อเสนอแนะ

[Task]: อ่านข้อเสนอแนะนโยบายด้านล่างนี้ แล้วตอบคำถาม 3 ข้อ:

1. หากมีผู้เชี่ยวชาญในสายงานนี้มาอ่าน ข้อเสนอตรงจุดใดจะถูกโต้แย้งหนักที่สุด?

2. มีข้อสมมติฐาน (Assumptions) ใดบ้างในข้อความนี้ที่ไม่เป็นจริงในบริบทสังคมไทย?

3. จงเขียนข้อโต้แย้ง 3 ข้อพร้อมเหตุผลสนับสนุน เพื่อคัดค้านรายงานฉบับนี้

[แนบ : ข้อเสนอแนะนโยบาย]

ข้อความจาก AI Literacy Handbook โดย ศ.ดร.สุเทพ สวนใต้

วิธีสามเส้า (Triangulation Method) กับแหล่งข้อมูลปฐมภูมิ



คำตอบที่ดูน่าเชื่อถืออาจมีข้อผิดพลาด แม้ AI จะยืนยันซ้ำหรือหลายเครื่องมือให้คำตอบตรงกัน จึงควรตรวจสอบแบบสามเส้า (Triangulation) โดยเปรียบเทียบคำตอบกับหลักฐานจากแหล่งต้นทาง และใช้แหล่งข้อมูลอิสระหรือผู้เชี่ยวชาญร่วมตรวจสอบ เพื่อให้มั่นใจก่อนนำไปใช้

ขั้นตอนที่ 1: แยกแยะ "หน่วยข้อมูลที่ต้องพิสูจน์" (Extract Claim Units)

สั่งให้ AI แยกคำตอบดิบออกเป็น Atomized Claims หรือหน่วยข้อเท็จจริงย่อย เพื่อเตรียมนำไปตรวจกับแหล่งข้อมูลจริง

- [Prompt สกัดข้อเท็จจริงเพื่อการตรวจสอบ]: "จงสกัดข้อเท็จจริง ตัวเลข ชื่อบุคคล ชื่อกฎหมาย และสถิติ จากข้อความด้านล่างนี้ ออกมาเป็นรายการข้อๆ (Bullet Points) โดยไม่ต้องสรุปเนื้อหา เพื่อใช้สำหรับนำไป Fact-Check กับแหล่งข้อมูลทางการ"

ขั้นตอนที่ 2: เทียบเคียงกับแหล่งข้อมูลปฐมภูมิ (Primary Source Cross-Check)

นำข้อเท็จจริงแต่ละข้อไปตรวจสอบกับแหล่งข้อมูลที่เป็นทางการ (Primary Official Sources) เช่น:

- ข้อกฎหมาย/มาตรา: ตรวจสอบกับ ราชกิจจานุเบกษา หรือ กฤษฎีกา
- ตัวเลขทางเศรษฐกิจ/สาธารณสุข: ตรวจสอบกับ สำนักงานสถิติแห่งชาติ, กระทรวงสาธารณสุข หรือ องค์การอนามัยโลก (WHO)
- ระเบียบปฏิบัติองค์กร: ตรวจสอบกับ คู่มือปฏิบัติงานทางการ (SOP) ของหน่วยงาน

ขั้นตอนที่ 3: การประเมินความขัดแย้ง (Conflict Resolution)

หากผลลัพธ์จาก AI ไม่ตรงกับแหล่งข้อมูลปฐมภูมิ ให้ยึดแหล่งข้อมูลปฐมภูมิเป็นความจริงสูงสุด (Ground Truth) เสมอ และตัดส่วนที่ AI แต่งเติมออกทันที

Human Review

ต้องมีผู้รับผิดชอบตรวจสอบก่อนใช้เสมอ

- ผลลัพธ์จาก AI ถือเป็น “ร่าง” จนกว่าจะผ่านการตรวจสอบโดยผู้รับผิดชอบ
- ต้องระบุได้ว่า “ใคร” เป็นผู้ตรวจและรับผิดชอบผลงานนั้น
- ตรวจทุกชิ้นก่อนใช้หรือส่งต่อ: ตรวจความถูกต้อง ความครบถ้วน แหล่งอ้างอิง อคติ และความเหมาะสมกับงาน
- ตรวจด้วยหลักฐานและความรู้: ไม่ยึดเพียงความมั่นใจของคำตอบ หรือการให้ AI ยืนยันซ้ำ หากเกินความเชี่ยวชาญ ให้ผู้มีความรู้ในเรื่องนั้นร่วมตรวจ
- เพิ่มการทบทวนตามความเสี่ยง: งานที่กระทบข้อสรุปวิจัย ข้อเสนอเชิงนโยบาย สิทธิของบุคคล หรืองบประมาณ ต้องมีผู้ทบทวนตามขั้นตอนของงาน
- แก้ไขหรือหยุดใช้ได้: หากยังยืนยันประเด็นสำคัญไม่ได้ ต้องแก้ไขหรือชะลอการใช้ ไม่รับรองผลลัพธ์เพียงเพราะ AI สร้างมา
- ห้ามให้ AI ตัดสินใจเรื่องบุคลากร การเงิน หรือสิทธิของบุคคลโดยลำพัง ต้องมีผู้มีอำนาจตรวจสอบและยืนยันก่อนดำเนินการ
- เก็บหลักฐานการตรวจสอบตามความเสี่ยงของงาน โดยระบุผู้ตรวจ ประเด็นที่ตรวจ และผลการตรวจ เพื่อให้ตรวจสอบย้อนหลังได้

AI ช่วยประกอบการตัดสินใจ แต่ไม่ใช้ AI ในการตัดสินใจแทนมนุษย์
มนุษย์ต้องตรวจสอบ ใช้วิจารณญาณ และรับผิดชอบต่อการตัดสินใจทุกครั้ง

ความโปร่งใสและการเปิดเผยการใช้ AI
Transparency and Disclosure

เปิดเผยเมื่อ AI มีบทบาทสำคัญต่อเนื้อหา — ไม่ต้องเปิดเผยสำหรับงาน routine ที่ไม่กระทบสาระ

เมื่อใดต้องเปิดเผย

ต้อง disclose

- AI มีส่วนสำคัญต่อการสร้างเนื้อหา
- AI ถูกใช้เป็นส่วนสำคัญของกระบวนการ เช่น คัดกรองวรรณกรรม สกัดข้อมูล
- **ผู้ให้ทุน วารสาร ที่ประชุม คณะกรรมการจริยธรรมการวิจัย ข้อตกลงของโครงการกำหนดไว้ หรือหน่วยงานภายนอกกำหนดให้เปิดเผย**
- AI มีบทบาทที่อาจกระทบความน่าเชื่อถือหรือความโปร่งใสของผลงาน
- สร้างภาพ สื่อ หรือวิดีโอเพื่อเผยแพร่ต่อสาธารณะ

เมื่อใดไม่จำเป็น

routine support

- ตรวจ spelling / grammar หรือปรับ wording เล็กน้อย
- แปลข้อความสั้น ๆ และช่วยจัด format
- brainstorm เบื้องต้น
- สรุปข้อมูลเพื่อใช้เป็น working notes ภายใน
- ลบพื้นหลังภาพ
- แต่ถ้าผลจาก AI กลายเป็นเนื้อหาหลักของงาน ต้อง disclose แม้เริ่มจากงาน routine

ตัวอย่างข้อความเปิดเผยการใช้ AI

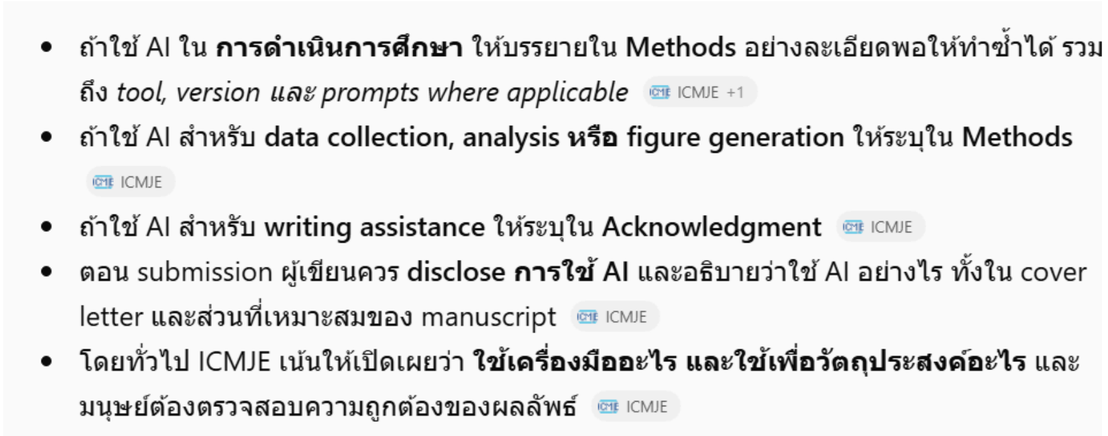
- ใต้ภาพหรือวิดีโอ: “AI-generated image” · “This video contains AI-generated content” · “Created with AI assistance”
- ในกิตติกรรมประกาศ: “AI was used to assist with language editing. The content was reviewed and verified by the authors.”
- ในวิธีการศึกษา: ระบุชื่อเครื่องมือ ผู้พัฒนา เวอร์ชัน ช่วงเวลาที่ใช้ ขอบเขตการใช้ และวิธีตรวจสอบผลลัพธ์
- ปฏิบัติตามข้อกำหนดของผู้ให้ทุนหรือวารสารเป็นลำดับแรกเสมอ

ถ้า AI มีผลต่อ “สาระสำคัญ” ของงาน ให้เปิดเผย · ถ้ามีผลแค่ “รูปแบบ” ไม่ต้อง — ไม่แน่ใจให้เปิดเผยไว้ก่อน และห้ามปิดบังเมื่อถูกถาม

การเปิดเผยการใช้ AI (Disclosure)

ในกรณีที่ AI **มีส่วนสำคัญ**ในการดำเนินงานวิจัย ผู้วิจัยควรจัดทำบันทึกการใช้ AI ในระดับที่เหมาะสม เพื่อให้สามารถตรวจสอบที่มาของกระบวนการ วิเคราะห์วิธีการใช้งาน และสนับสนุนความโปร่งใส ได้ตามความเหมาะสม

- ชื่อเครื่องมือ
- และรุ่นหรือโมเดล (หากสามารถระบุได้)
- วัตถุประสงค์
- AI prompt หรือคำสั่งที่สำคัญในกรณีที่เกี่ยวข้อง
- วิธีการที่ผู้วิจัยใช้ในการตรวจสอบหรือทวนสอบผลลัพธ์จาก AI
- บันทึกวันที่หรือช่วงเวลาที่ใช้งาน



- ถ้าใช้ AI ใน **การดำเนินการศึกษา** ให้บรรยายใน Methods อย่างละเอียดพอให้ทำซ้ำได้ รวมถึง *tool, version และ prompts where applicable* ICMJE +1
- ถ้าใช้ AI สำหรับ **data collection, analysis หรือ figure generation** ให้ระบุใน Methods ICMJE
- ถ้าใช้ AI สำหรับ **writing assistance** ให้ระบุใน **Acknowledgment** ICMJE
- ตอน submission ผู้เขียนควร **disclose การใช้ AI** และอธิบายว่าใช้ AI อย่างไร ทั้งใน cover letter และส่วนที่เหมาะสมของ manuscript ICMJE
- โดยทั่วไป ICMJE เน้นให้เปิดเผยว่า **ใช้เครื่องมืออะไร และใช้เพื่อวัตถุประสงค์อะไร** และมนุษย์ต้องตรวจสอบความถูกต้องของผลลัพธ์ ICMJE

ผู้ใช้งาน/ผู้วิจัย ต้องสามารถอธิบายได้ว่าผลลัพธ์จาก AI ได้รับการตรวจสอบหรือทวนสอบอย่างไร ก่อนนำไปใช้ในการวิเคราะห์ ตีความ รายงาน หรือเผยแพร่ผลการวิจัย

*ปฏิบัติตามข้อกำหนดของวารสาร ผู้ให้ทุน หรือผู้รับผลงานเสมอ

แบบข้อความเปิดเผยการใช้ AI (Disclosure Template)

"During the preparation of this work, the author(s) used [Specify tool name, e.g., ChatGPT-4o] in order to [Specify reason, e.g., improve readability and language editing of the manuscript]. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication."

"ในการจัดทำผลงานชิ้นนี้ ผู้เขียนได้ใช้ [ระบุชื่อเครื่องมือและรุ่น] เพื่อ [ระบุวัตถุประสงค์ เช่น ปรับปรุงความชัดเจนของภาษาและตรวจแก้ต้นฉบับ] หลังใช้เครื่องมือดังกล่าว ผู้เขียนได้ตรวจสอบและแก้ไข เนื้อหาตามความจำเป็น และรับผิดชอบต่อเนื้อหาของผลงานนี้ทั้งหมด"

เปิดเผยไว้ที่ใด: กิตติกรรมประกาศ (Acknowledgements): สำหรับการช่วยร่างเนื้อหาและตรวจภาษา วิธีการศึกษา (Methods): เมื่อใช้ AI ช่วยคัดกรองวรรณกรรม สกัดข้อมูล หรือวิเคราะห์ คำบรรยายใต้ภาพ: เมื่อใช้ AI สร้างหรือช่วยสร้างภาพ

5 องค์ประกอบที่ต้องมีครบ

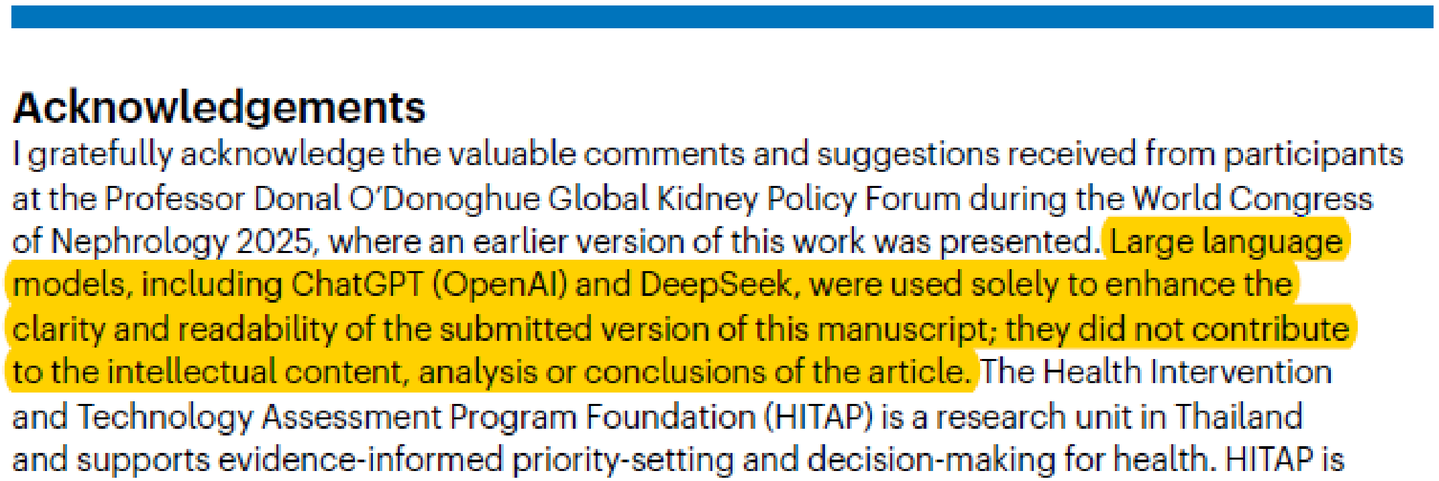
- ชื่อเครื่องมือและรุ่นที่ใช้ เช่น ChatGPT-4o ไม่ใช่เขียนกว้าง ๆ ว่า AI
- ช่วงเวลาที่ใช้ เช่น เดือนและปี
- ขั้นตอนที่ใช้ AI ช่วย ระบุให้ตรงว่าใช้ตรงไหนของงาน
- สิ่งที่ผู้เขียนตรวจสอบเองหลังได้ผลลัพธ์
- คำยืนยันว่าผู้เขียนรับผิดชอบเนื้อหาทั้งหมด

ข้อควรระวัง

- ตรวจข้อกำหนดของวารสารเป้าหมายก่อนเสมอ เพราะแต่ละฉบับกำหนดถ้อยคำและตำแหน่งที่ต้องวางต่างกัน
- ห้ามระบุ AI เป็นผู้แต่งร่วม (author) ในทุกกรณี — วารสารส่วนใหญ่ไม่ยอมรับ เพราะ AI รับผิดชอบต่อผลงานไม่ได้
- ก่อนใช้ AI ช่วยตรวจทานต้นฉบับบทความวิชาการของผู้อื่น ควรตรวจสอบนโยบายของวารสารที่เกี่ยวข้องก่อน เนื่องจากวารสารหลายแห่งไม่อนุญาตให้ใช้ AI ในลักษณะดังกล่าว ทั้งนี้ ต้องปฏิบัติตามข้อกำหนดและข้อจำกัดในการใช้ AI ของ HITAP ด้วย

แบบข้อความเปิดเผยการใช้ AI (Disclosure Template)

- AI-generated image/This video contains AI-generated content/ Created with AI assistance
- AI was used to assist with language editing. The content was reviewed and verified by the authors.



Acknowledgements

I gratefully acknowledge the valuable comments and suggestions received from participants at the Professor Donal O'Donoghue Global Kidney Policy Forum during the World Congress of Nephrology 2025, where an earlier version of this work was presented. Large language models, including ChatGPT (OpenAI) and DeepSeek, were used solely to enhance the clarity and readability of the submitted version of this manuscript; they did not contribute to the intellectual content, analysis or conclusions of the article. The Health Intervention and Technology Assessment Program Foundation (HITAP) is a research unit in Thailand and supports evidence-informed priority-setting and decision-making for health. HITAP is

- **Acknowledgements ช่วยร่าง แก้ไข แปล จัดรูปแบบต้นฉบับ**
  - “The authors acknowledge the use of Microsoft Copilot (accessed August 2024) to generate a first draft of the Acknowledgments section and translate the Methods section from Spanish to English. All AI-assisted text was reviewed and revised by the authors to ensure accuracy and clarity of meaning.”

- **Methods ช่วยระเบียบวิธี วิเคราะห์ข้อมูล ทบทวนวรรณกรรม**
  - “Literature screening was assisted by GPT-4 (accessed March 2024) to categorize 500+ abstracts by predefined relevance criteria. AI-assisted outputs were reviewed and validated by the authors, who confirmed the final inclusion and exclusion decisions.”

- **Figure caption สร้างหรือแก้ภาพ กราฟ แผนภาพ**
  - “Figure 1. Conceptual diagram of treatment pathway. Diagram created using DALL·E 3 (accessed March 2024) to generate an initial draft, with subsequent modifications by the authors in Canva. All content was reviewed for accuracy by the clinical team.”

- **Peer review ผู้ประเมินใช้ AI ช่วยเรียบเรียงความเห็น**
  - “GPT-5 was used to prioritize and polish review feedback. All original review feedback was provided by the peer reviewer, and all AI-generated content was reviewed, revised, and approved by the peer reviewer prior to sending this review.”



ศึกษาเพิ่มเติม : Wiley — Using AI tools in your research www.wiley.com/en-us/publish/article/ai-guidelines

การรายงานเหตุการณ์และการขอความช่วยเหลือ
Incident & Support

7 เหตุการณ์ที่ต้องรายงาน

1 **พบหรือสงสัยว่าเครื่องมือหรือบัญชี AI ไม่ปลอดภัย ไม่น่าเชื่อถือ**
ใช้แล้วพบว่าไฟล์ที่อัปโหลดเปิดให้บุคคลอื่นดูได้โดยไม่ตั้งใจ ถูกขอให้กรอกรหัสผ่านอีเมลลงในแชท หรือมีการดาวน์โหลดไฟล์หรือติดตั้งส่วนขยายโดยไม่ได้สั่ง
ทำทันที: หยุดใช้งาน · เก็บหลักฐานและรายละเอียดข้อมูลหรือสิทธิ์ที่ให้ไว้ · แจ้งหัวหน้าฝ่ายและ IT ทันที

2 **นำข้อมูลลับหรือข้อมูลส่วนบุคคลเข้า AI**
นำข้อมูลผู้ป่วยหรือเอกสารลับในเครื่องมือหรือบัญชี AI ที่ไม่ได้รับอนุญาตให้ใช้กับข้อมูลนั้น
ทำทันที: หยุดใช้ทันที · เก็บภาพหน้าจอไว้เป็นหลักฐาน · แจ้งหัวหน้าฝ่ายและ IT ทันที

3 **สงสัยว่าข้อมูลรั่วไหลจาก AI (AI Data Leakage)**
ข้อมูลภายในหรือข้อมูลลับปรากฏแก่ผู้ไม่มีสิทธิ์ หรือมีการแชร์ลิงก์แชทนอกขอบเขตที่อนุญาต
ทำทันที: หยุดใช้งานที่เกี่ยวข้อง · ปิดลิงก์แชร์หรือจำกัดการเข้าถึง · เก็บหลักฐานอย่างปลอดภัย · แจ้งหัวหน้าฝ่ายและ IT

4 **ข้อมูลผิดพลาดจาก AI ถูกนำไปใช้แล้ว (AI-Generated Misinformation Distributed)**
ตัวเลข ข้อเท็จจริง หรือเอกสารอ้างอิงที่ AI สร้างขึ้นผิดพลาดในสาระสำคัญ ถูกส่งต่อ เผยแพร่ หรือใช้ประกอบการตัดสินใจแล้ว
ทำทันที: หยุดส่งต่อ · แจ้งหัวหน้าฝ่ายและ IT ทันที · ประสานผู้รับหรือผู้เกี่ยวข้องเพื่อแก้ไขหรือถอนข้อมูล

5 **พฤติกรรมผิดปกติของ AI (Suspicious AI Behaviour)**
AI แสดงข้อมูลที่สงสัยว่าอยู่นอกสิทธิ์เข้าถึง หรือ Agent ส่งข้อความ แก้ไข ลบข้อมูล หรือดำเนินการเกินคำสั่งหรือสิทธิ์ที่อนุญาต
ทำทันที: หยุดการทำงานของ Agent หรือการใช้งานที่เกี่ยวข้อง · เก็บหลักฐานและคำสั่งที่ใช้ · แจ้งหัวหน้าฝ่ายและ IT ทันที

6 **สงสัยว่าบัญชีถูกเข้าถึงโดยไม่ได้รับอนุญาต**
พบการเข้าสู่ระบบหรือกิจกรรมที่ไม่รู้จักและอธิบายไม่ได้ เช่น แชทที่ไม่มีผู้ใช้งานที่ได้รับอนุญาตเป็นผู้สร้าง
ทำทันที: แจ้งหัวหน้าฝ่ายและ IT · เปลี่ยนรหัสผ่านผ่านช่องทางทางการ · ออกจากระบบทุกอุปกรณ์และเปิด MFA หากทำได้ โดยประสาน IT

7 **ข้อกังวลด้านลิขสิทธิ์ (Copyright Concern)**
พบเหตุให้สงสัยว่าภาพหรือข้อความจาก AI ทำซ้ำหรือดัดแปลงผลงานของผู้อื่นโดยไม่มีสิทธิ์ใช้งาน
ทำทันที: ระงับการใช้หรือเผยแพร่ชิ้นงานนั้น · แจ้งหัวหน้าฝ่ายและ IT เพื่อตรวจสอบสิทธิ์ · หากเผยแพร่แล้ว ให้ประสานแก้ไขหรือนำออกตามความเหมาะสม

การรายงานเหตุการณ์และการขอความช่วยเหลือ

วิธีรายงานเหตุ

ส่งอีเมลถึง หัวหน้าฝ่าย และ CC ฝ่าย IT

- แจ้งทันทีที่ทราบเหตุ และไม่เกิน 24 ชั่วโมง
- ระบุ: เกิดอะไรขึ้น เมื่อใด เครื่องมือหรือบัญชีที่ใช้ ชั้นข้อมูลที่เกี่ยวข้อง · สิ่งที่ดำเนินการไปแล้ว
- หากเกี่ยวข้องกับข้อมูลส่วนบุคคล ให้ CC ผู้บริหารด้วย



หลังแจ้งเหตุ ดำเนินการอย่างไร

ดำเนินการควบคู่ตั้งแต่เริ่มประเมิน
ผู้บริหาร หัวหน้าฝ่าย และ IT ประเมินการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตาม PDPA กับหน่วยงานที่เกี่ยวข้อง หรือเจ้าของข้อมูล และดำเนินการภายในกรอบกฎหมาย

ทันทีที่พบ ไม่เกิน 24 ชั่วโมง
ผู้พบเหตุ: หยุดการใช้งานที่เกี่ยวข้อง แจ้งหัวหน้าฝ่าย และ IT พร้อมเก็บหลักฐานอย่างปลอดภัย

ภายใน 1 วันทำการ
หัวหน้าฝ่ายและ IT: ประเมินเบื้องต้น ระงับหรือลดผลกระทบ และประสานผู้บริหารหรือผู้รับผิดชอบที่เกี่ยวข้อง

ภายใน 5 วันทำการ
ผู้ได้รับมอบหมาย สอบทานสาเหตุและจัดทำมาตรการแก้ไขเบื้องต้น

ภายใน 30 วัน
ผู้ได้รับมอบหมาย สรุปบทเรียนและแผนป้องกันเหตุซ้ำ สื่อสารโดยไม่เปิดเผยตัวบุคคล

แจ้งเร็ว ช่วยลดผลกระทบ HITAP สนับสนุนให้บุคลากรแจ้งข้อผิดพลาด เหตุการณ์ ความเสี่ยง หรือข้อกังวลเกี่ยวกับการใช้ AI ทันทีที่พบ เพื่อให้ร่วมกันแก้ไขและลดผลกระทบ ผู้ที่รายงานโดยสุจริตจะได้รับการปฏิบัติอย่างเป็นธรรม และบทเรียนที่ได้จะนำมาแบ่งปันโดยไม่เปิดเผยตัวบุคคล เพื่อป้องกันการเกิดเหตุซ้ำ

การขอคำแนะนำและความช่วยเหลือ (Support) หากมีข้อสงสัยหรือต้องการความช่วยเหลือในการใช้ AI ให้ติดต่อหัวหน้าฝ่ายและ/หรือ IT ตามความเหมาะสมกับเรื่องที่ต้องการคำแนะนำ

ประเภทของเหตุ และเกณฑ์ว่าเหตุใดต้องรายงาน

แยกเหตุออกเป็นสองประเภท เพราะแก้ด้วยวิธีคนละอย่าง — และระบุให้ชัดว่าเหตุแบบใดต้องรายงาน แบบใดแค่บันทึก

ประเภท 1 เหตุจากผู้ใช้งาน

แก้ด้วยการอบรมและการควบคุมบัญชี

- นำข้อมูลชั้นที่ 3 หรือ 4 เข้าเครื่องมือ
- ใช้บัญชีส่วนตัวกับงานขององค์กร
- แชร์ลิงก์บทสนทนาที่มีข้อมูลขององค์กร
- ใช้เครื่องมือที่ไม่แนะนำ โดยไม่ได้ขออนุมัติ

ประเภท 2 เหตุจากตัวระบบ AI

แก้ด้วยการตรวจสอบโดยมนุษย์และการเลือกเครื่องมือ

- สร้างข้อมูลหรือแหล่งอ้างอิงที่ไม่มีอยู่จริง
- ผลลัพธ์ที่มีอคติหรือเลือกปฏิบัติ
- AI ตัวแทน (agent) ดำเนินการเกินคำสั่ง
- ผลลัพธ์ที่ละเมิดลิขสิทธิ์ของผู้อื่น
- ข้อมูลรั่วข้ามผู้ใช้จากตัวบริการ

กรณีใดต้องรายงาน กรณีใดบันทึกไว้

แจ้งหัวหน้าฝ่ายและฝ่าย IT ทันทีที่ทราบเหตุ และไม่เกิน 24 ชั่วโมง

- ข้อมูลชั้นที่ 3–4 ถูกส่งเข้า AI หรือเปิดเผยนอกขอบเขตที่อนุญาต รวมถึงกรณีสงสัยว่าข้อมูลรั่วไหล ไม่ว่าจะนำผลลัพธ์ไปใช้หรือไม่
- ผลลัพธ์ที่ผิดพลาดในสาระสำคัญถูกเผยแพร่ ส่งต่อ หรือใช้ประกอบการตัดสินใจแล้ว และอาจกระทบความถูกต้องของงาน บุคคลอื่น หรือองค์กร
- AI ดำเนินการเกินคำสั่งหรือสิทธิ์ที่อนุญาต เช่น ส่งข้อความ เปิดเผย แก้ไข หรือลบข้อมูลโดยไม่ได้รับอนุญาต

บันทึกไว้ โดยไม่ต้องรายงานเป็นเหตุการณ์

- ผู้ใช้ตรวจพบข้อมูลหรือแหล่งอ้างอิงที่ไม่ถูกต้องก่อนนำไปใช้ และแก้ไขหรือยกเลิกการใช้แล้ว โดยไม่มีข้อมูลรั่วไหล การดำเนินการเกินสิทธิ์ หรือผลกระทบต่อผู้อื่น ให้บันทึกข้อผิดพลาดที่สำคัญหรือเกิดซ้ำ เพื่อใช้ปรับปรุงการทำงาน

ข้อมูลออกนอกขอบเขตที่อนุญาต หรือ AI ทำเกินสิทธิ์ = รายงานเสมอ ผลลัพธ์ผิดในสาระสำคัญและนำไปใช้แล้ว = รายงาน

ผลลัพธ์ผิด แต่ตรวจพบและแก้ไขก่อนใช้ โดยไม่มีผลกระทบ = บันทึก

ตัวอย่างปัญหาจากการทำงานของระบบ AI

- ให้เอกสารอ้างอิงที่ไม่ถูกต้องหรือไม่มีอยู่จริง
- ให้คำตอบที่ดูมั่นใจ แต่ข้อเท็จจริงคลาดเคลื่อน
- ตีความบริบทหรือความต้องการของผู้ใช้ผิดไป

ทั้งสามข้อเป็นประเภท 2

แนวทางรับมือ: เน้นการฝึกทักษะตรวจสอบข้อเท็จจริงและแหล่งอ้างอิง โดยใช้รายการตรวจสอบก่อน การพบข้อผิดพลาดจาก AI ไม่ได้หมายความว่าผู้ใช้งานทำผิด

ทำไมต้องแยกประเภทเหตุการณ์

เพื่อวิเคราะห์สาเหตุและแก้ไขให้ตรงจุด ทั้งด้านเครื่องมือ การใช้งาน และขั้นตอนตรวจสอบ โดยเหตุหนึ่งอาจเกี่ยวข้องกับหลายปัจจัย

AI Do’s and Don’ts

Do’s & Don’ts: ตัวอย่างพฤติกรรมที่ควรทำและไม่ควรทำ

Quick Reference

DO’s – ควรทำ

- ตรวจชั้นข้อมูล เลือกเครื่องมือและบัญชีให้เหมาะสม
- ใช้ข้อมูลเท่าที่จำเป็น ตรวจไฟล์ก่อนอัปโหลด
- ตรวจข้อเท็จจริง ตัวเลข และแหล่งอ้างอิงก่อนใช้
- ให้ผู้อื่นตรวจทานก่อนนำข้อมูลเข้า AI ตัดสินใจ หรือส่งงาน
- หากพบเหตุผิดปกติหรือสงสัยว่าเกิดเหตุจากการใช้ AI ให้แจ้งหัวหน้าฝ่ายและ IT ทันที
- ตรวจสอบ Prompt ไฟล์แนบ และสิทธิ์การเข้าถึงข้อมูลทุกครั้งก่อนใช้ AI และไม่เชื่อมต่อเครื่องมือ AI กับแหล่งข้อมูลขององค์กร เช่น SharePoint

DON’Ts – ไม่ควรทำ

- นำข้อมูลลับ ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหวเข้า AI
- เชื่อผลลัพธ์ AI โดยไม่ตรวจสอบ
- ปกปิดการใช้ AI ในกรณีที่ต้องเปิดเผย
- ใช้ AI เพื่อสร้างหรือเผยแพร่ข้อมูลเท็จ บิดเบือน หลอกลวง
- ให้ AI ตัดสินใจแทนมนุษย์ในเรื่องที่มีผลกระทบสำคัญ
- ละเลยข้อกำหนดของกฎหมาย ผู้ให้ทุน วารสาร หรือหน่วยงานกำกับดูแล
- รอให้เกิดความเสียหายหรือแก้ไขเสร็จแล้วจึงแจ้ง
- ส่งเอกสารทั้งฉบับโดยไม่ตรวจข้อมูลที่อยู่ภายใน

AI ใช้ได้ แต่ต้อง “THINK” ก่อนใช้

T

Trust but Verify
ตรวจสอบคำตอบก่อนใช้

- เปิดต้นฉบับเทียบตัวเลขและอ้างอิง
- ถามซ้ำได้คำตอบต่าง = ยังเชื่อไม่ได้

H

Handle Data Carefully
อย่าใส่ข้อมูลลับหรือข้อมูลส่วนบุคคล

- ข้อมูลผู้ป่วยและข้อมูลอ่อนไหว = ห้าม
- ข้อมูลชั้น 2 ขึ้นไป ใช้บัญชีองค์กรเท่านั้น

I

Intellectual Property
เคารพลิขสิทธิ์และทรัพย์สินทางปัญญา

- เช็คลิขสิทธิ์ก่อนอัปโหลด full-text
- ไม่แอบอ้างผลงาน AI เป็นของตนเอง

N

No Sensitive Decisions Alone
อย่าให้ AI ตัดสินใจเรื่องสำคัญแทนคน

- เรื่องคน เงิน สิทธิ ต้องมีคนตัดสิน
- การตีความผลวิจัย เป็นของผู้วิจัย

K

Keep Responsibility
คนใช้ยังคงเป็นผู้รับผิดชอบ

- ผลลัพธ์จาก AI คือ “ร่าง” เสมอ
- ระบุได้ว่าใครตรวจและรับผิดชอบ

ไม่แน่ใจข้อไหน = หยุดก่อน แล้วปรึกษาหัวหน้าฝ่าย หรือฝ่าย IT — ถ้าส่งข้อมูลชุดนั้นให้คนนอกองค์กรทางอีเมลไม่ได้ ก็ไม่ควรป้อนเข้า AI เช่นกัน