



THINKTOFINISH / FREE RESOURCE

นโยบายการใช้

Generative AI

อย่างรับผิดชอบ

แม่แบบสำหรับองค์กรในประเทศไทย

ใช้งานได้ทันที

ปรับข้อความใน [วงเล็บ] ให้ตรงกับองค์กรก่อนประกาศใช้

เวอร์ชัน 1.0 • 17 กันยายน 2569 • เอกสารเผยแพร่ฟรี

จัดทำใหม่เพื่อบริบทองค์กรไทย โดยสังเคราะห์ประเด็นจากตัวอย่างนโยบายของ Fisher Phillips แนวทางของ ETDA และกฎหมายไทยที่เกี่ยวข้อง เอกสารนี้ไม่ใช่คำแปลอย่างเป็นทางการและไม่ใช่อำนาจกฎหมาย

ก่อนนำแม่แบบนี้ไปประกาศใช้

เอกสารนี้ตั้งใจให้ฝ่ายบริหาร HR, IT, Security, Privacy และ Legal ใช้เป็นจุดเริ่มต้นร่วมกัน

01

แทนที่ข้อความใน [วงเล็บ]

ระบุชื่อองค์กร เจ้าของนโยบาย เครื่องมือที่อนุมัติ ช่องทางขออนุมัติและรายงานเหตุ

02

ผูกกับนโยบายเดิม

ตรวจให้สอดคล้องกับนโยบายความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล จรรยาบรรณ การใช้ IT และวินัยพนักงาน

03

สื่อสารด้วยตัวอย่างงานจริง

อบรมจากข้อมูลและเครื่องมือที่ทีมใช้จริง กำหนดผู้อนุมัติ และทบทวนหลังเริ่มใช้งาน

หลักคิดขั้นที่สุด

ถ้าไม่แน่ใจ ให้หยุดก่อนส่ง

อย่าป้อนข้อมูลจนกว่าจะตอบได้ว่าเครื่องมือนี้ได้รับอนุมัติหรือไม่ ข้อมูลอยู่ระดับใด เรามีสิทธิใช้ข้อมูลนั้นหรือไม่ ผลลัพธ์จะกระทบใคร และใครเป็นผู้ตรวจทาน

ข้อสงวนสิทธิและการใช้งาน

- เผยแพร่ให้ใช้ฟรีและนำไปปรับใช้ภายในองค์กรได้ โดยควรคงเครดิตแหล่งที่มา
- ไม่รับรองว่าแม่แบบนี้เพียงอย่างเดียวทำให้องค์กรปฏิบัติตามกฎหมายหรือข้อกำหนดเฉพาะอุตสาหกรรมครบถ้วน
- ควรให้ผู้เชี่ยวชาญด้านกฎหมาย ความเป็นส่วนตัว ความมั่นคงปลอดภัย และแรงงานตรวจทานก่อนประกาศใช้
- แยกนโยบายนี้ออกจากคู่มือการใช้เครื่องมือรายผลิตภัณฑ์ เพื่อให้อัปเดตเครื่องมือได้โดยไม่ต้องแก้นโยบายหลักทุกครั้ง



01 / POLICY

แม่แบบนโยบาย

ข้อความตั้งแต่หน้านี้สามารถคัดลอกไปปรับใช้เป็นนโยบายขององค์กรได้

ชื่อองค์กร	[ชื่อองค์กร]
เจ้าของนโยบาย	[ตำแหน่ง/หน่วยงาน]
เวอร์ชัน / วันที่มีผล	[เวอร์ชัน] / [วัน เดือน ปี]
รอบทบทวน	อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนเครื่องมือ/กฎหมาย/ความเสี่ยงสำคัญ
ช่องทางขออนุมัติหรือรายงานเหตุ	[อีเมล / Service Desk / ผู้รับผิดชอบ]

1. วัตถุประสงค์

[ชื่อองค์กร] สนับสนุนการใช้ Generative AI เพื่อเพิ่มคุณภาพ ความรวดเร็ว และการเรียนรู้ในการทำงาน โดยต้องไม่ลดทอนความรับผิดชอบของมนุษย์ ความมั่นคงปลอดภัย สิทธิในข้อมูลส่วนบุคคล ทรัพย์สินทางปัญญา ความเป็นธรรม หรือความน่าเชื่อถือขององค์กร

2. ขอบเขต

นโยบายนี้ใช้กับกรรมการ ผู้บริหาร พนักงาน ลูกจ้างชั่วคราว ผู้รับจ้าง ที่ปรึกษา และบุคคลอื่นที่ใช้ Generative AI เพื่อทำงานให้ [ชื่อองค์กร] ไม่ว่าจะเป็นใช้อุปกรณ์ บัญชี หรือเครือข่ายขององค์กรหรือส่วนตัว

ครอบคลุมเครื่องมือสาธารณะ เครื่องมือของบุคคลที่สาม API ส่วนเสริม เบราว์เซอร์ ระบบสร้างข้อความ ภาพเสียง วิดีโอ โค้ด และระบบอัตโนมัติที่มี Generative AI เป็นส่วนประกอบ

3. หลักการบังคับใช้

- มนุษย์รับผิดชอบผลลัพธ์สุดท้ายเสมอ
- ใช้ข้อมูลให้น้อยที่สุดและอยู่ในขอบเขตที่ได้รับอนุญาต
- ตรวจสอบข้อเท็จจริง ที่มา อคติ ความเหมาะสม และสิทธิในการใช้งานก่อนนำผลลัพธ์ไปใช้
- เปิดเผยการใช้ AI เมื่อจำเป็นต่อความโปร่งใส ความไว้วางใจ หรือข้อกำหนดของงาน
- ยกระดับการอนุมัติตามความเสี่ยง ไม่ใช่ตามความสะดวกของเครื่องมือ



02 / OWNERSHIP

คำสำคัญและผู้รับผิดชอบ

4. คำสำคัญ

- **Generative AI** — ระบบที่สร้างหรือแปลงเนื้อหา เช่น ข้อความ ภาพ เสียง วิดีโอ โค้ด หรือคำตอบ จากคำสั่งและข้อมูลที่ได้รับ
- **เครื่องมือที่อนุมัติ** — ผลิตภัณฑ์ รุ่น บัญชี หรือสภาพแวดล้อมที่ [ชื่อองค์กร] ประเมินและอนุญาตให้ใช้ตามเงื่อนไขที่กำหนด
- **ข้อมูลภายใน** — ข้อมูลที่ยังไม่เปิดเผยต่อสาธารณะ แม้อาจไม่ถูกจัดชั้นเป็นความลับ
- **ผลกระทบสูง** — การใช้ AI ที่อาจกระทบสิทธิ การจ้างงาน สุขภาพ ความปลอดภัย เครดิต การเงิน กฎหมาย ชื่อเสียง หรือการเข้าถึงบริการของบุคคล
- **ผู้ตรวจทานที่เหมาะสม** — บุคคลที่มีความรู้และอำนาจเพียงพอจะตรวจความถูกต้อง ความเสี่ยง และอนุมัติการใช้ผลลัพธ์

5. บทบาท

ผู้บริหาร	อนุมัติทิศทาง ระดับความเสี่ยง ทรัพยากร และข้อยกเว้นสำคัญ
เจ้าของนโยบาย	ดูแลรายการเครื่องมือ กติกา แบบฟอร์มอนุมัติ การสื่อสาร และรอบทบทวน
IT / Security	ประเมินผู้ให้บริการ สิทธิเข้าถึง การเชื่อมระบบ การบันทึกเหตุการณ์ และการตอบสนองเหตุ
Privacy / DPO / Legal	ให้คำแนะนำเรื่อง PDPA สัญญา ทรัพย์สินทางปัญญา การส่งข้อมูล และการใช้งานผลกระทบสูง
HR และหัวหน้างาน	กำหนดการใช้กับบุคลากร อบรม กำกับดูแล และดำเนินการอย่างเป็นธรรมตามนโยบายองค์กร
ผู้ใช้งาน	เลือกเครื่องมือและข้อมูลให้ถูก ตรวจทานผลลัพธ์ เก็บหลักฐาน และรายงานเหตุหรือข้อสงสัยทันที



อะไรใช้ได้ อะไรต้องอนุมัติ อะไรห้าม

ระดับ	ใช้ได้เมื่อ	ตัวอย่าง	การควบคุมขั้นต่ำ
ใช้ได้	ข้อมูลเป็นสาธารณะหรือสร้างขึ้นใหม่	ระดมไอเดีย ปรับภาษา สรุปข้อมูลสาธารณะ	ตรวจทานความถูกต้อง ก่อนใช้
ต้องอนุมัติ	มีข้อมูลภายใน ผลกระทบ ภายนอก หรือเชื่อมระบบ	เอกสารลูกค้า โค้ดภายใน งานเผยแพร่ การทำงาน อัตโนมัติ	ใช้เครื่องมือองค์กร + เจ้าของงาน/IT/กฎหมาย อนุมัติตามความเสี่ยง
ห้าม	มีข้อมูลต้องห้าม หรือ วัตถุประสงค์ผิด กฎหมาย/หลอกลวง	รหัสผ่าน ข้อมูลอ่อนไหว deepfake หลอกลวง การ ตัดสินใจแบบ อัตโนมัติ	หยุด ไม่ป้อนข้อมูล และ รายงานหากเกิดเหตุ

6. ตัวอย่างการใช้ที่ยอมรับได้

- ระดมความคิด จัดโครงสร้าง หรือสร้างคำถาม โดยไม่ป้อนข้อมูลลับหรือข้อมูลส่วนบุคคล
- ปรับภาษา แปล หรือสรุปเนื้อหาที่องค์กรมีสิทธิใช้และอยู่ในระดับข้อมูลที่เครื่องมือรองรับ
- สร้างตัวอย่าง แบบฟอร์ม หรือข้อมูลจำลองที่ไม่สามารถย้อนกลับไปสู่ตัวบุคคลหรือความลับจริง
- ค้นหาแนวทางเบื้องต้นจากข้อมูลสาธารณะ โดยผู้ใช้ต้องตรวจสอบแหล่งที่มาและข้อมูลล่าสุดด้วยตนเอง
- ช่วยเขียนหรือทบทวนโค้ดในสภาพแวดล้อมที่อนุมัติ โดยไม่ส่ง source code, key หรือช่องโหว่ที่เป็นความลับออกนอกขอบเขต

7. การใช้ที่ต้องได้รับอนุมัติก่อน

- นำข้อมูลภายใน ข้อมูลลูกค้า หรือเอกสารตามสัญญาไปประมวลผล
- เผยแพร่ผลลัพธ์ต่อสาธารณะ ส่งให้ลูกค้า ใช้ในคำแนะนำวิชาชีพ หรือสื่อสารในนามองค์กร
- เชื่อม AI กับอีเมล ฐานข้อมูล ระบบงาน หรือให้ AI ส่งการแทนผู้ใช้
- ใช้กับการสรรหา ประเมินผลงาน วินัย ค่าตอบแทน เลื่อนตำแหน่ง หรือการตัดสินใจที่กระทบบุคคล
- ใช้ในงานกฎหมาย การเงิน สุขภาพ ความปลอดภัย วิศวกรรม หรือบริบทที่ความผิดพลาดสร้างความเสียหายสูง

8. การใช้ที่ห้าม

- ป้อนรหัสผ่าน token API key private key หรือข้อมูลรับรองทุกชนิด
- สร้างเนื้อหาหลอกลวง ปลอมตัว ละเมิดสิทธิ คุกคาม เลี่ยงปฏิบัติ หรือช่วยกระทำการผิดกฎหมาย
- หลีกเลียงมาตรการรักษาความปลอดภัย การอนุมัติ หรือข้อจำกัดการเข้าถึงขององค์กร
- นำผลลัพธ์ AI ไปใช้เป็นข้อเท็จจริงหรือคำตัดสินสุดท้ายโดยไม่มีการตรวจทานที่เหมาะสม



04 / DATA

ข้อมูล ความเป็นส่วนตัว และความลับ

ประเภทข้อมูล	ตัวอย่าง	กติกา
สาธารณะ	ข้อมูลที่องค์กรเผยแพร่แล้วโดยชอบ	ใช้ได้ แต่ยังต้องตรวจสอบสิทธิและความถูกต้อง
ใช้ภายใน	แนวทางทำงานทั่วไป บันทึกภายในที่ไม่เป็นความลับ	ใช้เฉพาะเครื่องมือที่องค์กรอนุมัติและตามสิทธิ์เข้าถึง
ลับ/จำกัด	กลยุทธ์ ราคา สัญญา โค้ด รายงานเหตุ รายชื่อลูกค้า ข้อมูลยังไม่เปิดเผย	ห้ามใส่ในเครื่องมือสาธารณะ; ต้องมีอนุมัติและมาตรการเฉพาะ
ข้อมูลส่วนบุคคล	ชื่อ อีเมล ภาพ เสียง รหัสพนักงาน ประวัติการทำงาน	ใช้เท่าที่จำเป็น มีฐานกฎหมาย/คำแจ้ง และอยู่ในขอบเขตที่อนุมัติ
ข้อมูลส่วนบุคคลที่มีความอ่อนไหว	สุขภาพ ชีวภาพ ความพิการ ศาสนา ความเห็นทางการเมือง ประวัติอาชญากรรม ฯลฯ	โดยหลักไม่ป้อน; ใช้ได้เฉพาะกรณีจำเป็น มีฐานกฎหมายและอนุมัติจาก Privacy/Legal
ข้อมูลรับรอง/ความลับระบบ	รหัสผ่าน API key token private key	ห้ามป้อนทุกกรณี; หากเผลอป้อนให้เพิกถอน/เปลี่ยนและรายงานทันที

9. กติกาก่อนป้อนข้อมูล

- ใช้ข้อมูลเท่าที่จำเป็นต่อวัตถุประสงค์ ตัดรายละเอียดที่ไม่เกี่ยวข้อง และแทนที่ข้อมูลจริงด้วยข้อมูลจำลองเมื่อทำได้
- ตรวจสอบกฎหมาย คำแจ้งความเป็นส่วนตัว ความยินยอม (หากใช้) สัญญา และข้อกำหนดการส่งข้อมูลไปต่างประเทศก่อนประมวลผลข้อมูลส่วนบุคคล
- อย่าเชื่อว่าการปิดประวัติสนทนา โหมดส่วนตัว หรือคำรับรองของผู้ให้บริการทำให้ข้อมูลปลอดภัยโดยอัตโนมัติ
- ใช้บัญชีองค์กรและสิทธิ์เข้าถึงที่ได้รับมอบหมาย ห้ามแชร์บัญชีหรือคัดลอกข้อมูลไปยังบัญชีส่วนตัว
- ห้ามนำข้อมูลที่ติดข้อจำกัดของลูกค้า คู่ค้า NDA สิทธิพิเศษทางกฎหมาย หรือข้อกำหนดเฉพาะอุตสาหกรรมไปใช้โดยไม่ได้รับอนุมัติ

PDPA ไม่ได้เริ่มที่คำว่า ‘ยินยอม’

การประมวลผลข้อมูลส่วนบุคคลต้องมีวัตถุประสงค์และฐานกฎหมายที่เหมาะสม แจ้งรายละเอียดตามที่กฎหมายกำหนด ใช้ข้อมูลเท่าที่จำเป็น ดูแลสิทธิของเจ้าของข้อมูล และมีมาตรการรักษาความมั่นคงปลอดภัย ความยินยอมเป็นเพียงหนึ่งในฐานกฎหมาย



05 / OUTPUT

ตรวจสอบผลลัพธ์ก่อนใช้ทุกครั้ง

10. ความถูกต้องและอคติ

- ตรวจสอบข้อเท็จจริง ตัวเลข วันที่ ชื่อบุคคล กฎหมาย ข้อกำหนด และแหล่งอ้างอิงจากแหล่งต้นทางที่เชื่อถือได้
- ทดสอบผลลัพธ์กับกรณีที่หลากหลายเพื่อหาความลำเอียง การเหมารวม หรือผลกระทบที่ไม่เป็นธรรม
- ห้ามอ้างอิง คำพิพากษา งานวิจัย มาตรฐาน หรือบุคคลที่ยังไม่ได้เปิดและตรวจสอบจริง
- งานที่มีผลกระทบสูงต้องมีผู้ตรวจทานที่มีความเชี่ยวชาญและบันทึกเหตุการณ์การตัดสินใจ

11. ทรัพย์สินทางปัญญาและสิทธิของบุคคลอื่น

- ผู้ใช้ต้องมีสิทธิใช้ข้อมูลนำเข้า ภาพ เสียง เนื้อหา ซอฟต์แวร์ และเครื่องหมายการค้าที่นำไปให้ AI ประมวลผล
- ตรวจสอบว่าผลลัพธ์มีความคล้ายคลึงกับงานของผู้อื่นหรือมีเจตนาไขว่คว้าในอนุญาตที่ต้องปฏิบัติตามหรือไม่
- ห้ามสั่งให้เลียนแบบบุคคลที่ระบุตัวได้ สร้างภาพ/เสียงบุคคลโดยไม่มีสิทธิ หรือปกปิดที่มาของเนื้อหาเพื่อหลีกเลี่ยงลิขสิทธิ์
- ปรีกษา Legal ก่อนใช้ผลลัพธ์ AI เป็นทรัพย์สินหลัก เครื่องหมายการค้า งานโฆษณาสำคัญ หรือสิ่งที่จะขอความคุ้มครองทางกฎหมาย

12. ความโปร่งใส

เปิดเผยการใช้ AI เมื่อผู้รับอาจเข้าใจผิดว่าเนื้อหาถูกสร้าง ตรวจสอบ หรือรับรองโดยมนุษย์ทั้งหมด เมื่อสัญญาหรือกฎหมายกำหนด หรือเมื่อผลลัพธ์มีผลกระทบต่อบุคคล

ข้อความเปิดเผยตัวอย่าง

“เอกสารนี้จัดทำโดยใช้ Generative AI ช่วยร่าง/สรุป และได้รับการตรวจทานโดย [ชื่อ/ตำแหน่ง] ก่อนเผยแพร่”



บุคลากรและการตัดสินใจที่มีผลกระทบสูง

13. ห้ามให้ AI เป็นผู้ตัดสินใจสุดท้าย

AI อาจช่วยจัดโครงสร้างข้อมูลหรือเสนอประเด็นให้พิจารณาได้เฉพาะเมื่อได้รับอนุมัติ แต่ห้ามใช้เป็นผู้ตัดสินใจสุดท้ายในเรื่องการสรรหา คัดออก เลื่อนตำแหน่ง ประเมินผลงาน ค่าตอบแทน โยกย้าย วินัย เลิกจ้าง หรือการตัดสินใจอื่นที่มีผลอย่างมีนัยสำคัญต่อบุคคล

14. เงื่อนไขขั้นต่ำสำหรับการใช้กับบุคลากร

- กำหนดวัตถุประสงค์ เจ้าของงาน เกณฑ์ และข้อมูลที่ใช้ให้ชัดเจนก่อนเริ่ม
- ให้ HR, Privacy/Legal และ IT/Security ประเมินความจำเป็น ความเป็นธรรม ความเป็นส่วนตัว และผู้ให้บริการ
- แจ้งบุคคลที่เกี่ยวข้องตามที่กฎหมายและความเหมาะสมกำหนด พร้อมช่องทางให้สอบถามหรือโต้แย้ง
- ให้นำมาพิจารณาหลักฐานทั้งหมดอย่างมีความหมาย ไม่ใช่เพียงกดยืนยันคำแนะนำของ AI
- บันทึกข้อมูลที่ใช้ รุ่น/เครื่องมือ ผลลัพธ์ ผู้ทบทวน เหตุผล และการตัดสินใจสุดท้ายเท่าที่จำเป็น
- ติดตามผลลัพธ์ระหว่างกลุ่ม หาความคลาดเคลื่อนหรือการเลือกปฏิบัติ และหยุดใช้เมื่อควบคุมความเสี่ยงไม่ได้

15. งานวิชาชีพและงานสำคัญ

ผลลัพธ์ AI ไม่ใช่คำแนะนำทางกฎหมาย การแพทย์ การเงิน ภาษี ความปลอดภัย หรือวิศวกรรมโดยตัวมันเอง งานดังกล่าวต้องผ่านผู้มีคุณสมบัติและอำนาจตามวิชาชีพ รวมถึงกระบวนการอนุมัติขององค์กรก่อนนำไปใช้

หลักฐานสำคัญกว่าคำว่า human-in-the-loop

องค์กรควรกำหนดว่าใครจะตรวจสอบ ใช้หลักฐานใด มีอำนาจหยุดหรือแก้ผลลัพธ์หรือไม่ และเก็บร่องรอยการทบทวนอย่างไร



การอนุมัติเครื่องมือและการเชื่อมระบบ

16. รายการเครื่องมือที่อนุมัติ

ใช้เฉพาะเครื่องมือ รุ่น แผนบริการ และบัญชีที่อยู่ใน [รายการเครื่องมือที่อนุมัติ] ตามประเภทข้อมูลและกรณีใช้งานที่ระบุ การอนุมัติข้อผลิตภัณฑ์หนึ่งไม่ได้หมายถึงอนุมัติทุกฟีเจอร์ ส่วนเสริม หรือการเชื่อมต่อของผลิตภัณฑ์นั้น

17. การประเมินผู้ให้บริการขั้นต่ำ

- ☐ ข้อมูลถูกใช้ฝึกโมเดลหรือไม่ ปิดได้จริงหรือไม่ และเงื่อนไขต่างกันตามแผนบริการอย่างไร
- ☐ ระยะเวลาเก็บข้อมูล วิธีลบข้อมูล สำเนาสำรอง และข้อมูลที่ถูกให้บริการบันทึก
- ☐ สถานที่ประมวลผล ผู้รับช่วงประมวลผล และกลไกการส่งข้อมูลไปต่างประเทศ
- ☐ การเข้ารหัส SSO/MFA การกำหนดสิทธิ์ audit log การแจ้งเหตุ และการรับรองด้านความปลอดภัย
- ☐ กรรมสิทธิ์ input/output ใบอนุญาต ข้อจำกัดการใช้งาน การชดเชยความเสียหาย และข้อจำกัดความรับผิดชอบ
- ☐ ความพร้อมใช้งาน การเปลี่ยนรุ่นโมเดล ความสามารถในการย้ายข้อมูลออก และแผนยุติการใช้

18. การเชื่อมระบบและ Agent

- ห้ามเชื่อม AI กับอีเมล ไฟล์ ฐานข้อมูล ระบบลูกค้า ระบบการเงิน หรือระบบปฏิบัติการโดยไม่ได้รับอนุมัติเป็นลายลักษณ์อักษร
- กำหนดสิทธิ์ต่ำสุด ขอบเขตคำสั่ง วงเงิน/ผลกระทบ จุดอนุมัติของมนุษย์ การบันทึก log และวิธีหยุดระบบฉุกเฉิน
- ทดสอบในสภาพแวดล้อมแยกก่อนใช้งานจริง และไม่ใช้ข้อมูลจริงหากข้อมูลจำลองเพียงพอ
- ทบทวนสิทธิ์และ integration เมื่อเปลี่ยนเจ้าของงาน ผู้ให้บริการ โมเดล หรือวัตถุประสงค์



08 / INCIDENTS

เมื่อเกิดเหตุให้หยุดและรายงานเร็ว

19. เหตุที่ต้องรายงาน

- บ่อนข้อมูลผิดระดับ ข้อมูลส่วนบุคคล ความลับ รหัสผ่าน หรือข้อมูลของบุคคลที่สามโดยไม่ได้รับอนุญาต
- พบผลลัพธ์ที่อาจเลือกปฏิบัติ หมิ่นประมาท ละเมิดสิทธิ ไม่ปลอดภัย หรือทำให้ผู้รับเข้าใจผิด
- AI ดำเนินการนอกขอบเขต ส่งข้อความ แก้อัปเดต หรือเรียกใช้ระบบโดยไม่คาดหมาย
- สงสัยว่าบัญชีถูกเข้าถึงโดยไม่ชอบ มีข้อมูลรั่วไหล หรือผู้ให้บริการเปลี่ยนเงื่อนไขสำคัญ

20. ขั้นตอนทันที

01

หยุด

หยุดการใช้ การเผยแพร่ หรือการเชื่อมระบบที่เกี่ยวข้อง และอย่าพยายามแก้เหตุด้วยการลบหลักฐาน

02

จำกัดผลกระทบ

หากเป็น credential ให้เพิกถอนหรือเปลี่ยนตามขั้นตอนฉุกเฉิน; หากเป็นงานเผยแพร่ให้ระงับหรือเรียกคืนเมื่อทำได้

03

รายงาน

แจ้ง [ช่องทางรายงานเหตุ] พร้อมเวลา เครื่องมือ บัญชี ประเภทข้อมูล ผู้รับ และสิ่งที่เกิดขึ้น

04

เก็บหลักฐาน

เก็บ prompt, output, ลิงก์, screenshot, log และการดำเนินการที่ทำแล้วตามคำแนะนำของทีมรับเหตุ

21. การประเมินและแจ้งเหตุ

IT/Security, Privacy/DPO, Legal และเจ้าของข้อมูลร่วมประเมินผลกระทบ การแจ้งเจ้าของข้อมูล/คู่สัญญา/หน่วยงานกำกับ การแก้ไข และบทเรียนตามกฎหมาย สัญญา และแผนตอบสนองเหตุขององค์กร



การบันทึก ข้อยกเว้น วินัย และการทบทวน

22. การเก็บบันทึก

เก็บบันทึกเท่าที่จำเป็นเกี่ยวกับความเสี่ยง เช่น วัตถุประสงค์ เจ้าของงาน เครื่องมือ/รุ่น ประเภทข้อมูล การอนุมัติ prompt/output ที่จำเป็น ผู้ตรวจทาน การตัดสินใจ และเหตุการณ์ผิดปกติ โดยเป็นไปตามตารางเก็บรักษาข้อมูลขององค์กร

23. ข้อยกเว้น

ข้อยกเว้นต้องขอเป็นลายลักษณ์อักษร ระบุเหตุผล ขอบเขต ระยะเวลา ผู้รับผิดชอบ และมาตรการทดแทน และได้รับอนุมัติจาก [ผู้มีอำนาจ] ก่อนเริ่มใช้งาน ข้อยกเว้นหมดอายุโดยอัตโนมัติเมื่อครบกำหนด

24. การไม่ปฏิบัติตาม

การไม่ปฏิบัติตามอาจทำให้องค์กรระดับสิทธิ์ใช้เครื่องมือ สั่งแก้ไข อบรมเพิ่มเติม หรือดำเนินการทางวินัยตามข้อบังคับการทำงาน สัญญา และกฎหมาย โดยพิจารณาความร้ายแรง เจตนา ผลกระทบ และการรายงานโดยสุจริตอย่างเป็นธรรม

ห้ามตอบโต้ผู้ที่รายงานข้อกังวลโดยสุจริตหรือให้ความร่วมมือในการตรวจสอบ

25. การทบทวน

เจ้าของนโยบายทบทวนอย่างน้อยปีละ 1 ครั้ง และเมื่อเกิดเหตุสำคัญ มีการเพิ่มเครื่องมือ/การเชื่อมระบบ เปลี่ยนข้อกำหนดของผู้ให้บริการ หรือกฎหมาย/แนวทางกำกับเปลี่ยนแปลง

การรับทราบ

ผู้อนุมัติ	ชื่อ / ตำแหน่ง
ลายมือชื่อ / วันที่	_____
ประกาศใช้ผ่าน	[ช่องทาง / ระบบนโยบาย]



คู่มือ 60 วินาทีก่อนส่งข้อมูลให้ AI

01

เครื่องมือนี้ได้รับอนุมัติหรือยัง?

ชื่อเดียวกันแต่คนละแผนบริการ ฟीเจอร์ หรือบัญชี อาจมีกติกาต่างกัน

02

ข้อมูลอยู่ระดับใด?

ถ้ามีข้อมูลลับ ข้อมูลส่วนบุคคล ข้อมูลลูกค้า หรือ credential ให้หยุดและตรวจเงื่อนไขก่อน

03

เรามีสิทธิใช้ข้อมูลนี้หรือไม่?

ตรวจ NDA สัญญา ลิขสิทธิ์ สิทธิในภาพ/เสียง และวัตถุประสงค์ที่เจ้าของข้อมูลได้รับแจ้ง

04

ผลลัพธ์จะกระทบใคร?

ถ้ากระทบบุคลากร ลูกค้า เงิน สุขภาพ ความปลอดภัย หรือสิทธิ ต้องยกระดับการอนุมัติ

05

ใครจะตรวจและรับผิดชอบ?

ต้องมีผู้ตรวจทานที่เข้าใจเนื้อหา มีอำนาจแก้หรือหยุด และรับผิดชอบผลลัพธ์สุดท้าย

กติกาจำง่าย

PUBLIC + APPROVED + REVIEWED = เริ่มได้ | INTERNAL/PERSONAL = ขออนุมัติ | SECRET/CREDENTIAL = ห้ามป้อน



11 / IMPLEMENT

เช็กลิสต์ก่อนเปิดใช้ในองค์กร

	หัวข้อ	พร้อมเมื่อ
☐	เจ้าของ	แต่งตั้งเจ้าของนโยบาย ผู้อนุมัติ เครื่องมือ ผู้รับเหตุ และผู้ตัดสินใจ ยกเว้น
☐	เครื่องมือ	เผยแพร่รายการเครื่องมือ/บัญชี/ ฟังก์ชันที่อนุมัติ พร้อมประเภท ข้อมูลและกรณีใช้งาน
☐	ข้อมูล	ผูกกับ data classification, PDPA, NDA, retention และการส่งข้อมูลไปต่างประเทศ
☐	บุคลากร	กำหนดขั้นตอนพิเศษสำหรับงาน HR และการตัดสินใจที่มีผลกระทบ สูง
☐	ผู้ให้บริการ	ประเมิน security, privacy, training use, retention, IP, subprocessors และ exit plan
☐	การเชื่อมระบบ	กำหนดสิทธิ์ต่ำสุด approval gate, log, limit และ kill switch สำหรับ automation/agent
☐	การอบรม	ใช้ตัวอย่าง prompt และข้อมูลจาก งานจริงของแต่ละทีม ไม่สอนเพียง ฟังก์ชันของเครื่องมือ
☐	การวัดผล	กำหนด baseline, quality, adoption, incident และ value ก่อนขยายผล
☐	การทบทวน	กำหนดรอบตรวจรายการเครื่องมือ เหตุการณ์ แจ้งไขผู้ให้บริการ และ กฎหมาย/แนวทางใหม่

สิ่งที่ควรแยกเป็นเอกสารประกอบ

- รายการเครื่องมือที่อนุมัติและเงื่อนไขรายเครื่องมือ
- แบบฟอร์มขออนุมัติ use case / integration / exception
- คู่มือจัดชั้นข้อมูลและตัวอย่าง prompt ที่ปลอดภัย
- ขั้นตอนรายงานเหตุและผู้ติดต่อฉุกเฉิน
- แบบบันทึก human review สำหรับงานผลกระทบสูง



เกี่ยวกับ ThinkToFinish

ThinkToFinish ช่วยให้องค์กรเริ่มใช้ AI จากโจทย์ธุรกิจจริง ไม่ใช่จากชื่อเครื่องมือ เราประเมินความพร้อม คัดเลือก use case วางขอบเขตข้อมูลและธรรมาภิบาล ออกแบบ pilot และวิธีวัดผล เพื่อให้ผู้บริหาร IT และทีมปฏิบัติการเห็นภาพเดียวกันและดำเนินงานต่อไปได้

แนวทางของเราเน้นการสร้างคุณค่าควบคู่กับความรับผิดชอบต่อ: เริ่มเล็กในขอบเขตที่ชัด มีเจ้าของ มี human review และขยายเมื่อหลักฐานชี้ว่าคุ้มค่าและควบคุมความเสี่ยงได้

เริ่มจากคำถามเดียว

งานอะไรควรดีขึ้น ใครเป็นเจ้าของ และเราจะรู้ได้อย่างไรว่าดีขึ้นจริง

ThinkToFinish Co., Ltd. • thinktofinish.com • chawit@thinktofinish.com

ที่มาและแหล่งอ้างอิง

- [Fisher Phillips — Acceptable Use of Generative AI Tools \[Sample Policy\]](#)
- [ETDA — แนวทางการประยุกต์ใช้ Generative AI อย่างมีธรรมาภิบาลสำหรับองค์กร](#)
- [พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562](#)
- [กรมทรัพย์สินทางปัญญา — พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 และที่แก้ไขเพิ่มเติม](#)
- [กรมทรัพย์สินทางปัญญา — พระราชบัญญัติความลับทางการค้า พ.ศ. 2545](#)
- [กระทรวงแรงงาน — กฎหมายคุ้มครองแรงงาน](#)

เข้าถึงแหล่งอ้างอิงล่าสุดเมื่อ 17 กันยายน 2569 • ควรตรวจสอบกฎหมาย ข้อยกเว้น และเงื่อนไขผู้ให้บริการอีกครั้งก่อนประกาศใช้