

แนวทางการใช้ AI สำหรับพนักงาน

การใช้ AI อย่างปลอดภัยและรับผิดชอบ

จำไว้ 4 เรื่อง: ใช้ AI ที่บริษัทอนุญาต ไม่ใส่ข้อมูลที่ไม่ควรเปิดเผย ตรวจสอบคำตอบก่อนใช้ และคนต้องเป็นผู้ตัดสินใจ

ฉบับภาษาไทย

สารบัญ

เช็ก 5 ข้อก่อนใช้ AI	3
ก่อนใส่ข้อมูล ตรวจสอบชั้นข้อมูลทั้ง 4 ระดับ	4
สิ่งที่ควรทำและไม่ควรทำ.....	9
การใช้และติดตั้ง AI	10
งานที่ AI ช่วยได้ แต่คนต้องตัดสินใจ.....	12
เมื่อ AI แสดงข้อความหรือทำงานผิดปกติ.....	13
ถ้าใส่ข้อมูลผิดหรือ AI ทำสิ่งผิดปกติ.....	14
คำถามพบบ่อย	15
คำศัพท์ที่ควรรู้.....	18
สถานะและแหล่งอ้างอิง	20

เช็ก 5 ข้อก่อนใช้ AI

ถ้ายังตอบข้อใดไม่ได้ ให้หยุดและถามหัวหน้าหรือทีมที่ดูแลก่อน

บริษัทอนุญาตให้ใช้ AI ตัวนี้หรือไม่

เลือกเครื่องมือและบัญชีที่บริษัทจัดให้เป็นหลัก ส่วน AI อื่นใช้ได้เฉพาะงานทั่วไปและข้อมูลตามแนวทางนี้

ไม่แน่ใจ ให้หยุดและถาม

ข้อมูลนี้ใส่ใน AI ได้หรือไม่

ก่อนพิมพ์หรือแนบไฟล์ ให้ดูว่ามีข้อมูลลูกค้า พนักงาน ความลับ หรือรหัสเข้าระบบหรือไม่

มีข้อมูลที่ไม่ควรเปิดเผย ให้หยุด

ใช้ AI ช่วยตัดสินใจเรื่องสำคัญหรือไม่

เช่น คัดเลือกคน กำหนดราคา ให้เครดิต หรือแนะนำการทำงานที่มีผลต่อสุขภาพและความปลอดภัย

ถ้าใช่ ต้องขออนุมัติก่อน

คุณตรวจสอบคำตอบได้หรือไม่

อ่านทวน เช็กตัวเลข แหล่งข้อมูล ลิขสิทธิ์ ความลำเอียง และชุดคำสั่งโปรแกรมก่อนใช้

ตรวจไม่ได้ ห้ามนำไปใช้

คุณพร้อมรับผิดชอบงานนี้หรือไม่

คนที่ส่งหรืออนุมัติงานต้องรับผิดชอบ และควรบอกว่าใช้ AI ช่วยเมื่อผู้รับควรรู้

AI รับผิดชอบแทนคนไม่ได้

ห้ามเปิดเผยรหัสผ่านหรือรหัสลับให้ AI ทุกชนิด ส่วนข้อมูลลูกค้า พนักงาน และความลับของบริษัท
ใช้ได้เฉพาะเครื่องมือและงานที่ได้รับอนุญาต หากไม่แน่ใจให้หยุดและถามก่อน

ก่อนใส่ข้อมูล ตรวจสอบชั้นข้อมูลทั้ง 4 ระดับ

AI แบบเสียเงินหรือแบบองค์กรไม่ได้แปลว่าใส่ข้อมูลอะไรก็ได้
ต้องดูด้วยว่าบริษัทอนุญาตให้ใช้กับงานและข้อมูลชนิดนั้นหรือไม่

Restricted confidential

ข้อมูลลับที่จำกัดการเข้าถึงอย่างเข้มงวด

- ข้อมูลสุขภาพ เงินเดือน และผลประโยชน์พนักงาน
- ความลับทางการค้า กลยุทธ์ และแผนซื้อขายกิจการ

ใช้เฉพาะ AI ของบริษัทที่อนุญาตชัดเจนสำหรับข้อมูลและงานนั้น รหัสลับห้ามทุก AI

Confidential

ข้อมูลลับ

- ข้อมูลลูกค้า ข้อมูลการเงิน และข้อมูลคู่ค้า
- โค้ดโปรแกรม ผลทดสอบความปลอดภัย และแผนผังระบบ

ใช้เฉพาะ AI ของบริษัทที่อนุญาตสำหรับงานและข้อมูลนั้น ใส่เท่าที่จำเป็น

Internal

ข้อมูลภายในองค์กร

- ประกาศและการสื่อสารภายใน
- สมุดโทรศัพท์พนักงาน นโยบาย และกรอบการดำเนินงาน

ใช้กับ AI ของบริษัทภายในขอบเขตที่อนุญาต ห้ามใส่ใน AI สาธารณะหรือบัญชีส่วนตัว

Public

ข้อมูลสาธารณะของบริษัท

- ข้อมูลเว็บไซต์บริษัทและข่าวประชาสัมพันธ์
- รายงานการเงินและสื่อการตลาดที่อนุมัติและเผยแพร่แล้ว

ใช้กับ AI สาธารณะได้อย่างระมัดระวัง ตรวจสอบคำตอบ และไม่เพิ่มข้อมูลต้องห้าม

ห้ามเปิดเผยรหัสผ่าน PIN, OTP, API key, token, private key และ CVV ให้ AI ทุกชนิด รวมถึง AI ที่บริษัทจัดหาให้ โดยไม่มีข้อยกเว้น

ใส่ข้อมูลให้น้อยที่สุด: ลบชื่อ เลขประจำตัว อีเมล หมายเลขลูกค้า ชื่อโครงการ และรายละเอียดที่ไม่จำเป็นออกก่อน แต่ต้องลบให้มากพอจนเดาไม่ได้ว่าเป็นใครหรือเป็นเรื่องใด การลบชื่อไม่ได้ทำให้ยอดขาย ราคา หรือข้อมูลภายในกลายเป็นข้อมูลสาธารณะ

ข้อมูลทุกช่องทางใช้กฎเดียวกัน: รวมถึงข้อความ รูปภาพ เสียง หน้าจอ แท็บเว็บ และข้อมูลที่ AI อ่านผ่านระบบเชื่อมต่อ ตรวจสอบข้อมูลที่ติดตามในฉากหลัง ความเห็นในเอกสาร และซีตที่ซ่อนอยู่ก่อนส่ง

ความหมายและตัวอย่างข้อมูล

ชั้นข้อมูลของบริษัท (Data Classification)

ตารางนี้สรุปชั้นข้อมูลที่บริษัทควบคุม 4 ชั้น

โดยคงชื่อภาษาอังกฤษตามต้นฉบับและใช้คำอธิบายไทยเพื่อให้อ่านง่าย การ์ด 4 สีด้านบนใช้ชื่อและสีเดียวกับตารางนี้ พร้อมสรุปเงื่อนไขการใช้ AI

Restricted confidential

ข้อมูลลับที่จำกัดการเข้าถึงอย่างเข้มงวด

บริษัทควบคุมข้อมูล ผู้ใช้ภายในจำกัดเฉพาะผู้ได้รับสิทธิ

การเปิดเผยภายนอกเป็นข้อยกเว้นที่ต้องอนุมัติและมีข้อตกลงรักษาความลับ (NDA)

ตัวอย่าง: ข้อมูลสุขภาพและข้อมูลส่วนบุคคลอ่อนไหว รหัสลับและรหัสหลังบัตร (CVV) เงินเดือน ผลประเมินพนักงาน เรื่องวินัย เหตุด้านความปลอดภัย ความลับทางการค้า กลยุทธ์ แผนระยะยาว แผนการตลาด การตรวจสอบกิจการก่อนลงทุน และแผนซื้อขายหรือควบรวมกิจการ

ใช้กับ AI อย่างไร

ห้ามใส่ใน AI สาธารณะหรือบัญชีส่วนตัว สำหรับ AI ที่บริษัทจัดหาให้

ต้องมีการอนุญาตให้ใช้ข้อมูลชั้นนี้กับงานนั้นอย่างชัดเจน หากไม่แน่ใจ ให้ถามเจ้าของข้อมูลและ Cybersecurity ก่อน

รหัสผ่าน รหัสลับ และ CVV ห้ามเปิดเผยให้ AI ทุกชนิด การมี NDA หรือการอนุมัติเปิดเผยภายนอกไม่ใช่ข้อยกเว้น

Confidential

ข้อมูลลับ

บริษัทควบคุมข้อมูล ผู้ใช้ภายในจำกัดเฉพาะผู้ได้รับสิทธิ การเปิดเผยภายนอกต้องอนุมัติและมี NDA

ตัวอย่าง: ข้อมูลระบุตัวลูกค้าหรือพนักงาน ข้อมูลการเงินและบัตรชำระเงิน ทรัพย์สินทางปัญญา ข้อมูลที่คู่ค้าฝากไว้ มาตรฐานและขั้นตอนงาน อีเมลบางประเภท โค้ดโปรแกรม ผลทดสอบเจาะระบบ แผนผังเครือข่าย และข้อมูลช่องโหว่

ใช้กับ AI อย่างไร

ใช้เฉพาะ AI ที่บริษัทจัดทำให้และอนุญาตสำหรับงานกับข้อมูลนั้น ใส่เฉพาะส่วนที่จำเป็น ห้ามใส่ใน AI สาธารณะหรือบัญชีส่วนตัว

มีสิทธิเปิดไฟล์ไม่ได้หมายความว่าไม่มีสิทธินำไปใช้กับ AI ทุกงาน

Internal

ข้อมูลภายในองค์กร

บริษัทควบคุมข้อมูล ใช้ภายในองค์กรตามการจัดชั้นข้อมูล การเปิดเผยภายนอกต้องได้รับอนุมัติ

ตัวอย่าง: ประกาศภายใน การสื่อสารภายใน สมุดรายชื่อและเบอร์โทรศัพท์งาน เอกสารนโยบายและกรอบการดำเนินงาน

ใช้กับ AI อย่างไร

ใช้กับ AI ที่บริษัทจัดทำให้ภายในขอบเขตงานและข้อมูลที่อนุญาต ห้ามใส่ใน AI สาธารณะหรือบัญชีส่วนตัว คำว่าใช้ภายในได้ ไม่ได้แปลว่าเผยแพร่ภายนอกหรือส่งให้บริการ AI ใดก็ได้

Public

ข้อมูลสาธารณะของบริษัท

บริษัทควบคุมข้อมูลและขั้นตอนอนุมัติการเปิดเผย

ใช้ข้อมูลฉบับที่ได้รับอนุมัติและเผยแพร่อย่างเป็นทางการแล้ว

ตัวอย่าง: เนื้อหาเว็บไซต์บริษัทที่เปิดอ่านได้โดยไม่ต้องเข้าสู่ระบบ ข่าวประชาสัมพันธ์ รายงานการเงินที่เผยแพร่แล้ว และสื่อการตลาดที่เผยแพร่แล้ว

ใช้กับ AI อย่างไร

ใช้กับ AI สาธารณะได้อย่างระมัดระวังตามแนวทางนี้ ตรวจสอบคำตอบก่อนใช้ และไม่แนบข้อมูลภายในหรือข้อมูลส่วนบุคคลเพิ่ม

พนักงานไม่มีสิทธิเปลี่ยนชั้นข้อมูลหรือเผยแพร่ข้อมูลบริษัทเองเพื่อให้ถือเป็น Public

ข้อมูลจากอินเทอร์เน็ต: ตรวจสอบแหล่งที่มา ความถูกต้อง และสิทธิในการใช้ก่อนนำเข้า AI ห้ามใช้ข้อมูลรั่วไหลหรือข้อมูลส่วนบุคคลที่ไม่ได้รับอนุญาต

อ้างอิงชื่อชั้นข้อมูลและตัวอย่างจากตาราง Data Classification ที่ให้มา ส่วน “ใช้กับ AI อย่างไร” เป็นการเชื่อมกับแนวทาง AI ฉบับนี้ บันทึกการประชุมต้องพิจารณาชั้นของเนื้อหาที่บันทึกไว้ด้วย หากเอกสารไม่มีป้ายกำกับ มีข้อมูลหลายชั้น หรือไม่แน่ใจ ให้ถามเจ้าของข้อมูลก่อนใช้ ห้ามถือว่าเป็น Public เอง

คำอธิบายประเภทข้อมูลเพิ่มเติม

ประเภทข้อมูลด้านล่างอาจอยู่ได้หลายชั้น ให้ดูป้ายกำกับและเนื้อหาประกอบกัน

ข้อมูลส่วนบุคคลไม่ใช่ชั้นข้อมูลแยกต่างหาก ส่วนข้อมูลส่วนบุคคลอ่อนไหวตาม PDPA เป็นประเภทที่กฎหมายกำหนด

ข้อมูลที่ไม่ควรเปิดเผยคืออะไร

ข้อมูลที่ถ้ารั่ว ถูกนำไปใช้ผิด หรือไปอยู่กับคนที่ไม่ควรเห็น อาจทำให้คน บริษัท ลูกค้า คู่ค้า หรือระบบเสียหาย

ตัวอย่าง: รายชื่อลูกค้า ยอดขายที่ยังไม่ประกาศ สัญญาคู่ค้า ชุดคำสั่งโปรแกรม จุดอ่อนของระบบ เอกสารคดี และกฎแฉเข้าระบบ

ข้อมูลส่วนบุคคลคืออะไร

ข้อมูลที่บอกได้ว่าเป็นใคร ทั้งจากข้อมูลชิ้นเดียวหรือเมื่อนำไปรวมกับข้อมูลอื่น

ตัวอย่าง: ชื่อ เบอร์โทร อีเมลส่วนตัว ที่อยู่ รหัสพนักงาน รหัสลูกค้า รูปถ่าย ตำแหน่งที่อยู่ ประวัติการซื้อ และประวัติการทำงาน

ข้อมูลส่วนบุคคลที่มีความอ่อนไหวตาม PDPA คืออะไร

ข้อมูลตามมาตรา 26 ได้แก่ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม และข้อมูลชีวภาพ รวมถึงข้อมูลอื่นที่กฎหมายกำหนดในลักษณะเดียวกัน

ตัวอย่าง: ใบรับรองแพทย์ ผลตรวจสุขภาพ ข้อมูลความพิการ ลายนิ้วมือ แบบจำลองใบหน้า ม่านตา DNA และประวัติอาชญากรรม ข้อมูลกลุ่มนี้ต้องใช้ฐานกฎหมายและระบบที่ได้รับอนุมัติ ห้ามใส่ใน AI สาธารณะ

ข้อมูลลับของบริษัทคืออะไร

ข้อมูลที่บริษัทยังไม่เปิดเผยต่อคนทั่วไป หรือให้เฉพาะคนที่ต้องใช้งานเห็น แม้ข้อมูลนั้นจะไม่เกี่ยวกับบุคคลก็ตาม

ตัวอย่าง: กลยุทธ์ แผนเปิดสาขา ราคา กำไร ประสิทธิภาพ งบประมาณ สัญญา แผนซื้อขายกิจการ ข้อมูลคู่ค้า รายงานสอบสวน ชุดคำสั่งโปรแกรม แบบระบบ จุดอ่อนด้านความปลอดภัย และเอกสารกฎหมาย

รหัสลับหรือกฎแฉเข้าระบบคืออะไร

ข้อมูลที่ใช้ยืนยันว่าเป็นคุณ ใช้เปิดระบบ ถอดรหัส หรือเชื่อมต่อบบบอื่น ห้ามพิมพ์ลงคำถาม แชต บันทึกการทำงาน หรือไฟล์ที่ส่งขึ้นระบบ แม้ใช้ AI แบบองค์กร

ตัวอย่าง: รหัสผ่าน PIN, OTP, API key, token, private key, certificate, รหัสเชื่อมฐานข้อมูล และรหัสกุ้คั่น สำหรับงานเขียนโปรแกรม ให้ระบบส่งรหัสตรงไปยังโปรแกรมโดยไม่แสดงค่าให้ AI เห็น

ตัวอย่างใกล้ตัว

พนักงานบัญชี

ทำได้: ถามหลักบัญชีทั่วไป หรือให้ช่วยร่างรูปแบบรายงานโดยใช้ตัวเลขสมมติ

อย่าใส่ใน AI สาธารณะ: ใบแจ้งหนี้จริง เงินเดือน เลขบัญชีธนาคาร เลขประจำตัวผู้เสียภาษี หรืองบที่ยังไม่ประกาศ

ช่างซ่อม

ทำได้: ถามวิธีตรวจอาการจากคู่มือที่เปิดเผยต่อสาธารณะ โดยไม่บอกข้อมูลสถานที่หรือระบบจริง

อย่าใส่ใน AI สาธารณะ: รหัสเครื่อง แผนผังเครือข่าย บันทึกแจ้งเตือน รหัสผ่าน ภาพพื้นที่หวงห้าม หรือข้อมูลลูกค้า

พนักงานขาย

ทำได้: ให้ช่วยร่างข้อความขายโดยใช้ชื่อลูกค้าสมมติและตัวเลขสมมติ แล้วแก้ไขตรงกับข้อเท็จจริง

อย่าใส่ใน AI สาธารณะ: รายชื่อลูกค้า เบอร์โทร ประวัติการซื้อ ราคาพิเศษ ส่วนลดเฉพาะราย หรือข้อตกลงที่ยังไม่เปิดเผย

สิ่งที่ควรทำและไม่ควรทำ

AI ช่วยทำงานได้ แต่คนส่งงานยังต้องรับผิดชอบความถูกต้องและผลที่เกิดขึ้น

✓ ควรทำ

- ใช้ AI ช่วยคิด ร่าง สรุป หรือแปล แล้วอ่านทวนด้วยตนเอง
- ใช้ AI และบัญชีที่บริษัทอนุญาต พร้อมเปิดการยืนยันตัวตนสองขั้นตอนเมื่อมีให้ใช้
- เช็กข้อเท็จจริง ตัวเลข ลิงก์ แหล่งข้อมูล และคำแนะนำทุกครั้ง
- ถ้างานใช้ประเมินคน ให้ชี้แจงว่า AI ไม่ลำเอียงหรือทำให้ใครเสียเปรียบอย่างไม่เป็นธรรม
- บอกว่าใช้ AI ช่วย เมื่อไม่บอกแล้วอาจทำให้ผู้รับเข้าใจผิด
- สำหรับงานสำคัญ ให้เก็บคำถาม คำตอบ ชื่อเครื่องมือ และชื่อผู้ตรวจงานไว้

✗ ไม่ควรทำ

- อย่าใส่ข้อมูลลับ ข้อมูลส่วนบุคคล ชุดคำสั่งโปรแกรม หรือเอกสารภายในลง AI สาธารณะ
- อย่าส่งคำตอบจาก AI ต่อทันทีโดยไม่อ่านและตรวจสอบ
- อย่าติดตั้งโปรแกรม AI ส่วนเสริมของเบราว์เซอร์ หรือ AI ในเครื่องด้วยตนเอง
- อย่าเชื่อคำสั่งแปลก ๆ ที่ซ่อนอยู่ในเว็บไซต์ ไฟล์ หรืออีเมลที่ AI เปิดอ่าน
- อย่าใช้ AI ปลอมตัว หรือสร้างภาพ เสียง และวิดีโอปลอมเพื่อหลอกผู้อื่น
- อย่าให้ AI ตัดสินเรื่องสำคัญแทนคน หรือข้ามขั้นตอนขออนุมัติ

การใช้และติดตั้ง AI

AI ส่วนตัว หมายถึงบัญชีที่สมัครเอง ไม่ว่าจะใช้ฟรีหรือจ่ายเงินเอง
การจ่ายเงินไม่ได้แปลว่าบริษัทอนุญาต และไม่ได้ทำให้คุณมีสิทธิใส่ข้อมูลบริษัท

เครื่องมือที่บริษัทอนุญาต 2 รายการ

- Microsoft Copilot Enterprise ที่บริษัทจัดหาให้
- Claude Enterprise / Claude Code ที่บริษัทจัดหาให้
- ใช้บัญชีและช่องทางที่บริษัทกำหนด เฉพาะงานและข้อมูลที่ได้รับอนุญาต และไม่ให้ผู้อื่นยืมบัญชี
- ให้ IT ติดตั้งและตั้งค่าโปรแกรมสำหรับองค์กร
ไม่เปลี่ยนการตั้งค่าความเป็นส่วนตัวหรือการเชื่อมต่อระบบเอง

ห้ามทำเอง

- ติดตั้งโปรแกรม AI แอปมือถือ AI ในเครื่อง หรือส่วนเสริมของเบราว์เซอร์เพื่อใช้ทำงาน
- เชื่อม AI กับอีเมล ไดรฟ์ แชต ฐานข้อมูล ที่เก็บชุดคำสั่งโปรแกรม หรือระบบงาน
- ให้สิทธิ AI จัดการระบบหรือเข้าถึงข้อมูลเพิ่มโดยไม่ได้รับอนุมัติ
- ซื้อบริการหรือกดยอมรับเงื่อนไขแทนบริษัท

AI อื่น: ใช้ด้วยความระมัดระวัง

AI สาธารณะหรือบัญชีส่วนตัว ทั้งฟรีและเสียเงิน

ใช้ช่วยงานทั่วไปได้อย่างระมัดระวังโดยไม่ต้องขออนุมัติเป็นรายครั้ง

ใช้เฉพาะข้อมูลสาธารณะหรือข้อมูลสมมติที่ไม่มีข้อมูลส่วนบุคคล ความลับ หรือเรื่องภายในบริษัท
และตรวจคำตอบก่อนใช้

ห้ามใส่ข้อมูลภายใน ข้อมูลส่วนบุคคล ความลับ หรือรหัสลับ หากจะติดตั้งเพื่อใช้ทำงาน
เชื่อมกับระบบบริษัท เพิ่มสิทธิการเข้าถึง หรือใช้กับงานที่มีผลกระทบสูง
ต้องขออนุมัติหัวหน้างานและปรึกษา Cybersecurity ก่อนดำเนินการ

สำหรับกรณีที่ต้องขออนุมัติ: เก็บหลักฐานชื่อเครื่องมือ บัญชี งาน ประเภทข้อมูล และสิทธิที่อนุญาต
งานเดิมทำต่อได้ภายในเงื่อนไขและระยะเวลาที่อนุมัติ หากเปลี่ยนเครื่องมือ บัญชี วัตถุประสงค์
ประเภทข้อมูล หรือเพิ่มการเข้าถึง ให้ขอทบทวนก่อน หากขอบเขตยังไม่ชัดเจน ให้ถามก่อนเริ่มใช้

AI สำหรับองค์กรที่บริหารจัดการให้

บริษัทจัดหาให้และอนุญาตให้ใช้งาน

Microsoft Copilot Enterprise

ใช้เฉพาะงานและข้อมูลที่บริษัทอนุญาตให้นำมาใช้กับ AI การเปิดไฟล์ได้ไม่ได้หมายความว่าใช้ข้อมูลนั้นกับ AI ได้ทุกงาน ระบบจะทำตามสิทธิและชั้นข้อมูลที่บริษัทตั้งไว้ Microsoft ระบุว่าจะไม่นำคำถาม คำตอบ และข้อมูลงานไปฝึกโมเดล AI หลัก

- เช็กสิทธิใน SharePoint, Teams และ OneDrive เพราะ Copilot อาจเจอไฟล์ที่เคยแชร์กว้างเกินไป
- ห้ามใส่รหัสผ่านหรือกุญแจเชื่อมระบบ เช่น API key และ token
- อ่านและตรวจคำตอบก่อนใช้ เพราะ Copilot ยังตอบผิดหรือแต่งข้อมูลได้
- การต่อกับระบบอื่นหรือเพิ่มส่วนเสริมต้องขออนุมัติแยก

สำหรับผู้ที่ยังไม่พร้อมจะจัดตั้งบัญชีและกำหนดขอบเขตงานให้

Claude Enterprise และ Claude Code

Claude Enterprise ใช้ได้ตามขอบเขตงานที่บริษัทกำหนดให้ผู้ใช้แต่ละราย หากยังไม่ชัดเจน

ให้ถามหัวหน้างานและ Cybersecurity ก่อนใช้ ส่วน Claude Code

ใช้กับงานเขียนโปรแกรมและไฟล์โครงการในขอบเขตที่ได้รับอนุญาต เปิดให้เห็นเฉพาะไฟล์ ระบบ และเว็บไซต์ที่จำเป็น

- ตรวจสอบสิ่งที่ AI แก่ คำสั่งที่ AI จะรัน โปรแกรมเสริม และผลทดสอบก่อนยอมรับ
- อย่าปิดระบบที่ถามก่อนแก้ไฟล์หรือรันคำสั่ง นอกจากทำงานในพื้นที่ทดสอบที่บริษัทอนุมัติ
- ใช้บัญชีและรหัสสำหรับทดสอบที่มีสิทธิน้อยที่สุด และแยกระบบจริงออกจากระบบทดสอบ
- ห้ามให้คำสั่งแสดงรหัสลับในหน้าจอ บันทึกข้อผิดพลาด แชต หรือไฟล์ที่ส่งขึ้นระบบ
- การเชื่อม Claude กับเครื่องมือหรือเว็บไซต์อื่นต้องได้รับอนุมัติ

ห้ามเปิดเผยรหัสลับให้ AI ทุกชนิด รวมถึงรหัสระบบทดสอบ โดยไม่มีข้อยกเว้น: รวมถึง Claude Enterprise และ Claude Code ห้ามให้ AI อ่านรหัสผ่านหรือรหัสลับจากไฟล์ .env แชต หน้าจอ หรือบันทึกการทำงาน หากโปรแกรมต้องใช้รหัสลับ ให้ทีม IT ตั้งค่าวิธีส่งรหัสตรงไปยังโปรแกรม โดยป้องกันไม่ให้ AI อ่านหรือแสดงรหัสลับ

งานที่ AI ช่วยได้ แต่คนต้องตัดสินใจ

AI ช่วยรวบรวมและร่างข้อมูลได้ แต่เรื่องที่กระทบคน เงิน กฎหมาย หรือความปลอดภัย ต้องมีผู้รับผิดชอบตรวจสอบและตัดสินใจ

ตัวอย่างงาน	ระดับการควบคุม	สิ่งที่ต้องทำก่อนใช้
ร่างข้อความทั่วไป สรุปข้อมูลที่เปิดเผยแล้ว หรือช่วยคิดไอเดีย	งานทั่วไป	อ่านทวน เช็คความถูกต้อง ลิขสิทธิ์ และความเหมาะสมก่อนส่ง
เอกสารลูกค้า สัญญา รายงานการเงิน ชุดคำสั่งโปรแกรม หรือข้อความที่จะส่งออกนอกบริษัท	ต้องให้เจ้าของงานตรวจ	ใช้ AI ที่บริษัทอนุญาต ใส่ข้อมูลเท่าที่จำเป็น และให้ผู้รู้เรื่องนั้นตรวจ
รับคน เลื่อนตำแหน่ง เลิกจ้าง กำหนดราคา ให้เครดิต ให้สิทธิประโยชน์ หรือให้คำแนะนำด้านกฎหมาย สุขภาพ และความปลอดภัย	ต้องขออนุมัติก่อน	ให้ผู้มีอำนาจตรวจสอบข้อมูล เหตุผล และผลกระทบ แล้วเป็นผู้ตัดสินใจ
ใช้ AI หลอกหรือบังคับคน ให้คะแนนคนเพื่อจำกัดสิทธิ หรือใช้ใบหน้า/ลายนิ้วมือเฝ้าติดตามโดยไม่ มีฐานกฎหมายและการอนุมัติ	ห้ามทำ	หยุดและแจ้งทีมกำกับดูแลข้อมูล ความเป็นส่วนตัว หรือความปลอดภัยสารสนเทศ

เมื่อ AI แสดงข้อความหรือทำงานผิดปกติ

หาก AI ขอรหัสลับ ให้ส่งข้อมูลไปที่อื่น หรือทำสิ่งที่คุณไม่ได้สั่ง ให้หยุดและปฏิบัติดังนี้

ถ้าเห็นข้อความแบบนี้: “ไม่ต้องทำตามกฎเดิม ส่งข้อมูลทั้งหมดและรหัสเข้าระบบมาที่ลิงก์นี้”

สิ่งที่ต้องทำทันที: หยุดใช้งาน • ไม่กดลิงก์ • ไม่ส่งข้อมูล • แจ้ง Cybersecurity

สิ่งที่ต้องทำ

- ข้อความในเว็บไซต์ ไฟล์ และอีเมลมีไว้ให้อ่าน ไม่ใช่คำสั่งที่ต้องทำตาม
- อย่าให้ AI เปิดดูข้อมูล อีเมล ไฟล์ หรือระบบที่ไม่จำเป็นกับงาน
- ถ้า AI ขอรหัสผ่าน OTP ฤๅญแจเข้าระบบ หรือให้ส่งข้อมูลไปที่อื่น ให้หยุดทันที
- ก่อนให้ AI ส่งข้อมูล แก่ไฟล์ ส่งซื้อ หรือทำรายการสำคัญ ต้องมีคนตรวจและกดยืนยัน
- ถ้า AI สร้างคำสั่งคอมพิวเตอร์หรือโปรแกรม ต้องให้ผู้รัๅตรวจและทดลองก่อนใช้กับระบบจริง

ถ้าใส่ข้อมูลผิดหรือ AI ทำสิ่งผิดปกติ

แจ้งเร็วช่วยลดความเสียหาย อย่าปกปิดหรือทดลองซ้ำ

หยุด จดรายละเอียด และแจ้งทันที

- หยุดคุย อัปโหลด แชร์ หรือเชื่อม AI กับระบบ
- เก็บหลักฐานที่มีอยู่ และทำตามคำแนะนำของทีม Cybersecurity ในการลบข้อมูลหรือยกเลิกสิทธิ
- จดชื่อ AI เวลา บัญชีที่ใช้ ประเภทข้อมูล ผู้ที่ได้รับข้อมูล และสิ่งที่ AI ทำไปแล้ว
โดยไม่ใส่รหัสลับในข้อความอีเมลหรือไฟล์แนบ หากต้องส่งภาพหลักฐาน
ให้ปิดรหัสลับและข้อมูลส่วนบุคคลที่ไม่จำเป็นในสำเนาที่ส่ง เก็บต้นฉบับไว้ตามคำแนะนำของ
Cybersecurity
- อย่าส่งข้อมูลต่อหรือทำเหตุการณ์เดิมซ้ำเพื่อทดลอง
- แจ้งทีม Cybersecurity ทันทีที่ bit_cyber@cpaxtra.co.th พร้อมแจ้งหัวหน้างาน
ไม่ต้องรออนุมัติก่อนแจ้งเหตุ

แจ้งเหตุ: bit_cyber@cpaxtra.co.th

แจ้งหัวหน้างานด้วย

คำถามพบบ่อย

ถ้ายังไม่แน่ใจ อย่าเพิ่งใส่ข้อมูล ให้ถามก่อน

ใช้บัญชี AI ส่วนตัวทำงานได้หรือไม่

ใช้ช่วยงานทั่วไปได้อย่างระมัดระวัง ทั้งบัญชีฟรีและเสียเงิน โดยไม่ต้องขออนุมัติเป็นรายครั้ง
ใช้เฉพาะข้อมูลสาธารณะหรือข้อมูลสมมติที่ไม่มีข้อมูลส่วนบุคคลหรือเรื่องภายในบริษัท
และตรวจสอบก่อนใช้ ห้ามใส่ข้อมูลภายใน ความลับ หรือรหัสลับ หากจะติดตั้งเพื่อทำงาน เชื่อมระบบ
เพิ่มสิทธิ หรือใช้กับงานที่มีผลกระทบสูง ต้องขออนุมัติหัวหน้างานและปรึกษา Cybersecurity ก่อน

ใช้ AI แปลหรือสรุปเอกสารภายในได้หรือไม่

ทำได้เฉพาะในเครื่องมือและกรณีใช้งานที่ได้รับอนุมัติ ต้องลดข้อมูลตามความจำเป็น
และต้องไม่ใส่ข้อมูลลับหรือข้อมูลส่วนบุคคลใน AI สาธารณะ

ถ้าลบชื่อออกแล้ว ข้อมูลปลอดภัยหรือไม่

ยังไม่แน่มื่อไป เพราะตำแหน่ง สาขา วันที่ หรือรายละเอียดอื่นอาจทำให้เดาได้ว่าเป็นใคร
และแม้ระบุตัวบุคคลไม่ได้ ยอดขาย ราคา กำไร หรือเนื้อหาที่เหลืออาจยังเป็นข้อมูลภายในหรือความลับ
การลบชื่อไม่ได้อนุญาตให้ส่งข้อมูลนั้นเข้า AI สาธารณะ

ต้องบอกว่าใช้ AI ช่วยทุกครั้งหรือไม่

ควรบอกเมื่อไม่บอกแล้วอาจทำให้ผู้รับเข้าใจผิด โดยเฉพาะภาพ เสียง หรือวิดีโอที่ดูเหมือนจริง
รวมถึงกรณีที่กฎหมายหรือขั้นตอนงานกำหนด สำหรับงานภายในทั่วไป ให้บันทึกไว้ตามความสำคัญของงาน

หัวหน้าอนุมัติแล้ว แต่ Cybersecurity ยังไม่ตอบ เริ่มใช้ได้หรือไม่

หากเป็นกรณีที่ต้องขออนุมัติ เช่น ติดตั้ง เชื่อมระบบ เพิ่มสิทธิ หรืองานที่มีผลกระทบสูง
ต้องรอคำแนะนำงานขอบเขตชัดเจนก่อนดำเนินการ งานเร่งด่วนไม่ยกเว้นขั้นตอนนี้
ส่วนการถามความรู้ทั่วไปหรือร่างข้อความสมมติโดยไม่มีข้อมูลต้องห้าม
ใช้ได้ตามแนวทางโดยไม่ต้องขออนุมัติเป็นรายครั้ง

อนุมัติครั้งเดียว ใช้ได้ทุกงานตลอดไปหรือไม่

สำหรับงานที่ต้องขออนุมัติ การอนุมัติไม่ครอบคลุมทุกงาน ให้เก็บหลักฐานว่าครอบคลุมเครื่องมือ บัญชี งาน
ประเภทข้อมูล และการเข้าถึงใด งานเดิมที่อยู่ในขอบเขตยังใช้ได้ตามเงื่อนไขและระยะเวลาที่อนุมัติ
เมื่อเปลี่ยนเครื่องมือ บัญชี วัตถุประสงค์ ประเภทข้อมูล หรือเพิ่มการเข้าถึง ต้องขอทบทวนก่อน
หากไม่ได้รับขอบเขตชัดเจน ให้ถามก่อน

จ่ายเงินเองหรือใช้อีเมลบริษัทสมัคร ถือว่าเป็น AI ที่บริษัทอนุญาตหรือไม่

ไม่ถือว่าได้รับอนุญาตโดยอัตโนมัติ ต้องเป็นเครื่องมือ บัญชี และช่องทางที่บริษัทกำหนด
แม้ค่าบริการจะเหมือนกับเครื่องมือของบริษัทก็ตาม

ปิดการนำข้อมูลไปฝึก AI หรือใช้โหมดเขตชั่วคราวแล้ว ใส่ข้อมูลลับได้หรือไม่

ไม่ได้ การตั้งค่าเหล่านี้ไม่เปลี่ยนขอบเขตข้อมูลที่บริษัทอนุญาต และไม่ยกเว้นข้อห้ามเรื่องรหัสลับ

เปิดไฟล์ได้อยู่แล้ว ให้ Copilot อ่านได้ทุกไฟล์หรือไม่

ไม่ได้ ต้องมีเหตุผลในการใช้ข้อมูลกับงานที่ได้รับอนุญาตด้วย หาก AI แสดงข้อมูลที่ไม่เกี่ยวข้องกับงานหรือสงสัยว่าไม่ควรเห็น ให้หยุดใช้ข้อมูลนั้น ไม่เผยแพร่ต่อ และแจ้ง Cybersecurity

พนักงานบัญชีหรือฝ่ายขายใช้ Claude Enterprise ได้หรือไม่

ใช้ได้เมื่อบริษัทจัดบัญชีและกำหนดให้ใช้กับงานนั้นแล้ว ไม่ได้หมายความว่าพนักงานทุกคนได้รับสิทธิอัตโนมัติ หากไม่ทราบขอบเขต ให้ถามหัวหน้างานและ Cybersecurity ส่วน Claude Code ต้องใช้ในขอบเขตงานเขียนโปรแกรมที่ได้รับอนุญาต

แค่ให้ AI อ่านหน้าจอหรือฟังเสียง ไม่ได้แนบไฟล์ ถือว่าใช้ข้อมูลหรือไม่

ถือว่าใช้ข้อมูลเช่นกัน กฎครอบคลุมข้อความ รูปภาพ เสียง หน้าจอ แท็บเว็บ และข้อมูลที่ AI อ่านผ่านระบบเชื่อมต่อ แม้เป็นพีเจอร์ที่มีอยู่แล้วในเบราว์เซอร์หรือมือถือ ก็ต้องตรวจสอบเครื่องมือ บัญชี และข้อมูลก่อนใช้

ถ่ายรูปปะไหล่ แต่มีใบหน้าลูกค้ำหรือรหัสผ่านติดมูมภาพ ใช้ได้หรือไม่

ต้องตรวจข้อมูลทั้งภาพ ไม่ใช่เฉพาะอะไหล่ที่ต้องการถาม ตัดหรือปิดข้อมูลที่ไม่จำเป็นก่อนส่ง และห้ามให้ AI เห็นรหัสลับ สำหรับไฟล์เอกสาร ให้ตรวจหน้าที่แนบ ความเห็น และซีตที่ซ่อนอยู่ด้วย

รหัสระบบทดสอบหรือรหัสที่กำลังจะหมดอายุ ให้ AI อ่านได้หรือไม่

ไม่ได้ หากยังใช้เข้าถึงระบบได้จริงถือเป็นรหัสลับ แม้เป็นระบบทดสอบหรือรหัสชั่วคราว หากต้องสาธิตให้ใช้ข้อความสมมติที่ใช้เข้าระบบไม่ได้ เช่น YOUR_API_KEY

ไฟล์ .env ไม่มีรหัสลับ ให้ AI อ่านได้หรือไม่

พิจารณาเนื้อหาและขอบเขตงาน ไม่ใช่ชื่อไฟล์เพียงอย่างเดียว ค่าตั้งค่าที่ไม่มีรหัสลับอาจใช้ได้ในงานที่อนุญาต แต่ชื่อระบบ ที่อยู่ระบบ หรือค่าอื่นอาจยังเป็นข้อมูลภายใน ห้ามส่งค่ารหัสลับที่ใช้จริงให้ AI

ร่างอีเมลแจ้งราคาที่อนุมัติแล้ว ต้องขออนุมัติการกำหนดราคาใหม่หรือไม่

การช่วยเรียบเรียงโดยคงราคาที่อนุมัติแล้ว ไม่ใช่การให้ AI กำหนดราคาใหม่ แต่ต้องอยู่ในขอบเขตการใช้ AI ที่อนุญาตและตรวจราคาก่อนส่ง หากให้ AI เสนอราคา ส่วนลด หรือเงื่อนไขใหม่ ต้องผ่านขั้นตอนอนุมัติที่เกี่ยวข้อง

ช่างให้ AI สรุปรุ่นมือซ่อมได้หรือไม่

สรุปรุ่นมือสาธารณะเพื่อเรียนรู้ได้ในเครื่องมือและขอบเขตที่อนุญาต แต่ก่อนนำไปซ่อมหรือปรับเครื่องจริง ต้องตรวจสอบรุ่นผู้ผลิต ขั้นตอนความปลอดภัย และให้ผู้รับผิดชอบพิจารณา ห้ามใช้คำตอบ AI แทนขั้นตอนอนุมัติงานที่มีผลต่อความปลอดภัย

ใช้มือถือส่วนตัวนอกเวลางาน หรือถามแค่ประโยคช่วยพรให้ลูกค้า ต้องทำตามรุ่นมือหรือไม่

กฎเรื่องข้อมูลและการตรวจคำตอบยังใช้เหมือนเดิม ไม่ว่าจะใช้อุปกรณ์ใดหรือเวลาใด รวบรวมช่วยพรทั่วไปด้วยข้อมูลสมมติได้โดยไม่ต้องขออนุมัติเป็นรายครั้ง แต่ห้ามใส่รายชื่อกู้ค้า ข้อมูลส่วนบุคคล หรือข้อมูลภายในลงบัญชี AI ส่วนตัว

เผลอส่งข้อมูลแล้วลบแชตทันที ยังต้องแจ้งหรือไม่

ต้องแจ้งทันที การลบแชตไม่ได้ยืนยันว่าข้อมูลถูกลบจากทุกระบบ แจ้ง bit_cyber@cpaxtra.co.th และหัวหน้างาน ไม่ต้องรอหัวหน้าอนุมัติ ไม่ส่งรหัสลับซ้ำในอีเมลหรือภาพแนบ และทำตามคำแนะนำของ Cybersecurity

คำศัพท์ที่ควรรู้

ความหมายของคำที่ใช้ในคู่มือนี้ ชื่อบริการหรือการเสียเงินไม่ได้บอกว่าบริษัทอนุญาตให้ใช้ข้อมูลใด

AI สาธารณะ

บริการ AI ที่บุคคลทั่วไปสมัครใช้งานได้ เช่น ChatGPT, Claude และ Gemini ในบริการสำหรับผู้ทั่วไป มีทั้งแบบฟรีและเสียเงิน การใช้บริการดังกล่าวด้วยบัญชีส่วนตัวไม่ถือว่าได้รับอนุญาตให้ใส่ข้อมูลภายในบริษัท

ตัวอย่าง: สมัครบัญชีเองเพื่อถามความรู้ทั่วไปหรือร่างข้อความด้วยข้อมูลสมมติ

ตามขอบเขตที่แนวทางนี้ออนุญาต

บัญชี AI ส่วนตัว

บัญชีที่พนักงานสมัครและดูแลเอง มีทั้งแบบฟรีและจ่ายเงินเอง การซื้อแพ็คเกจหรือใช้อีเมลบริษัทสมัคร ไม่ได้ทำให้บัญชีนั้นเป็นบัญชีที่บริษัทอนุญาตโดยอัตโนมัติ

Web AI หรือ AI ที่ใช้ผ่านเว็บไซต์

หมายถึงช่องทางการใช้งานผ่านเว็บเบราว์เซอร์ ไม่ได้ระบุว่าเป็นบัญชีส่วนตัวหรือบัญชีองค์กร และไม่ได้ยืนยันว่าบริษัทอนุญาต AI สาธารณะและ AI ที่บริษัทจัดหาให้ต่างก็อาจใช้งานผ่านเว็บไซต์ได้

AI Desktop หรือแอป AI ที่ติดตั้งบนคอมพิวเตอร์

โปรแกรม AI ที่เปิดใช้งานจากแอปบนคอมพิวเตอร์ แทนการเปิดผ่านเว็บไซต์

แอปอาจส่งคำถามและไฟล์ไปประมวลผลออนไลน์

การติดตั้งบนเครื่องจึงไม่ได้หมายความว่าข้อมูลจะอยู่ในเครื่องเสมอ

สิ่งที่ต้องทำ: ก่อนติดตั้งเพื่อใช้งาน ให้ขออนุมัติหัวหน้างานและปรึกษาทeam Cybersecurity โดยให้ IT ดำเนินการตามขั้นตอนของบริษัท การเข้าถึงไฟล์ หน้าจอ หรือระบบอื่นต้องอยู่ในขอบเขตที่ได้รับอนุญาต และห้ามเปิดเผยรหัสลับให้ AI

AI ที่บริษัทอนุญาต

เครื่องมือ บัญชี และช่องทางที่บริษัทระบุว่าจะใช้ได้สำหรับงานและข้อมูลที่กำหนด ต้องตรวจสอบให้ครบ ไม่พิจารณาจากชื่อบริการเพียงอย่างเดียว

ตัวอย่าง: Claude ที่สมัครเองกับ Claude Enterprise ที่บริษัทจัดหาให้ใช้ชื่อเดียวกัน

แต่มีขอบเขตการใช้งานต่างกัน ห้ามเปิดเผยรหัสลับให้ AI ทั้งสองกรณี

AI สำหรับองค์กร หรือ Enterprise AI

บริการ AI สำหรับใช้งานในองค์กร คำว่า Enterprise เพียงอย่างเดียวไม่ได้แปลว่าบริษัทอนุญาต หรือสามารถใส่ข้อมูลได้ทุกประเภท ต้องใช้ตามขอบเขตที่บริษัทกำหนด

รหัสลับ และไฟล์ .env

รหัสลับ เช่น รหัสผ่าน รหัสใช้ครั้งเดียว (OTP) และรหัสเชื่อมต่อระบบ (API key หรือ token)

ใช้เข้าถึงบัญชีหรือระบบ ส่วน .env เป็นไฟล์ตั้งค่าโปรแกรมที่อาจมีรหัสเหล่านี้ ห้ามให้ AI อ่านค่ารหัสลับ
แม้เป็น AI ที่บริษัทอนุญาต

สถานะและแหล่งอ้างอิง

ฉบับนี้สังเคราะห์จากร่าง AI Governance Policy เอกสารเสนอคณะกรรมการ และสื่อ Cyber Security Communication ที่ให้มา ใช้เป็นแนวทางการใช้งาน AI สำหรับพนักงาน ควบคู่กับนโยบาย IM, IS, PDPA, Code of Conduct และคำสั่งที่มีผลอยู่ โดยไม่ได้แทนที่เอกสารเหล่านั้น

- [ISO/IEC 42001:2023](#) ระบบการจัดการ AI
- [ISO/IEC 27090](#) แนวทางความมั่นคงปลอดภัยของระบบ AI ซึ่งยังอยู่ระหว่างการจัดพิมพ์ ณ วันที่ทบทวนฉบับนี้
- [Thailand's AI Governance Guideline](#) ของ ETDA
- [EU AI Act](#) ใช้เป็นแหล่งอ้างอิงด้านการจัดการตามความเสี่ยงและข้อห้าม
- [พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562](#) มาตรา 6 และมาตรา 26
- [Microsoft Copilot Enterprise Data Protection](#)
- [Claude Code Security](#) และ [Anthropic commercial data usage](#)

เมื่อไม่แน่ใจ ให้หยุดและถาม

ติดต่อหัวหน้างาน ฝ่ายช่วยเหลือด้าน IT ทีมความปลอดภัยสารสนเทศ ทีมคุ้มครองข้อมูลส่วนบุคคล หรือทีมกำกับดูแล ผ่านช่องทางของบริษัท

ทบทวนล่าสุด 28 กันยายน 2569