promptrity

PROMPTRITY / PRODUCT GUIDES

คู่มือผู้ดูแลระบบ

ติดตั้ง สมาชิก นโยบายและการแก้ปัญหา

เอกสารภาษาไทย · ฉบับ 1.1
ข้อมูลผลิตภัณฑ์ ณ 9 พฤศจิกายน 2569

คู่มือสำหรับผู้ใช้งาน

USE WITH CONFIDENCE

ใช้ AI อย่างมั่นใจ
ด้วยนโยบายที่ทุกคนเข้าใจ

ขั้นตอนการใช้ • ขอบเขตสิทธิ์ • ข้อมูลและความปลอดภัย

CONTENTS

สารบัญ

เลือกหัวข้อที่ต้องการอ่าน สารบัญและลิงก์ท้ายเล่มกดเปิดได้ในโปรแกรมอ่าน PDF ที่รองรับ

เลือกคู่มือตามบทบาท	3
เข้าสู่ระบบและดูแลบัญชี	4
เชิญและดูแลสมาชิก	5
ติดตั้งและตรวจสถานะการป้องกัน	6
ตั้งนโยบายและทยอยเปิดใช้	7
ทำไมไม่บล็อกตั้งแต่วันแรก	8
ระดับการเปิดใช้งาน	9
เงื่อนไขก่อนปลดแต่ละขั้น	10
สร้างกฎเฉพาะและจดจำเอกสารลับ	13
ตั้งค่าการเก็บและความต่อเนื่อง	14
ส่งไฟล์แนบอย่างปลอดภัย	15
อ่านรายงานเพื่อปรับการใช้งาน	16
Promptrity เก็บข้อมูลอะไร	17
แก้ปัญหาและส่งเรื่องให้ผู้ดูแล	18

PROMPTRITY / 01

เลือกคู่มือตามบทบาท

บัญชีองค์กรมี 4 บทบาท การมองเห็นเมนูและสิทธิ์แก้ไขไม่เท่ากัน เจ้าของควรกำหนดสิทธิ์เท่าที่แต่ละคนจำเป็นต้องใช้

บทบาท	งานหลัก	ขอบเขตสำคัญ
เจ้าของ	เริ่มองค์กร ตั้งนโยบาย สมาชิก การเงิน และโอนเจ้าของ	เปิดการเรียกเก็บเงินได้ เริ่มคำขอเก็บข้อความและปิดการเก็บได้
ผู้ดูแลระบบ	ดูแลนโยบาย สมาชิก อุปกรณ์ และรายงาน	ไม่มีหน้าเรียกเก็บเงิน อนุมัติคำขอเก็บข้อความเป็นคนที่สองได้
ผู้ดูรายงาน	อ่านภาพรวม การใช้ AI ความเสี่ยง และรายงาน	แก้นโยบายหรือจัดการสมาชิกไม่ได้
พนักงาน	ใช้ส่วนขยายและดูประวัติของตนเอง	ไม่เห็นรายงานองค์กรหรือประวัติของคนอื่น

ทุกบัญชีมีพื้นที่ส่วนตัว

ทุกบทบาทเข้าหน้า “บัญชีของฉัน” เพื่อแก้ชื่อหรือรหัสผ่าน และเข้าหน้า “ประวัติของฉัน” ได้ องค์กรปิดสิทธิ์ดูประวัติของตนเองไม่ได้

แยกทีมงานบริการออกจากองค์กร

บัญชีทีมงาน Promptrity ใช้ระบบหลังบ้านแยกต่างหาก มีสิทธิ์ดูจำนวน การตั้งค่าและเอกสารการเงินตามหน้าที่ ไม่ใช่บัญชีสำหรับเปิดอ่านข้อความหรือประวัติพนักงานรายบุคคล

หาเมนูไม่พบ

ตรวจบทบาทกับเจ้าขององค์กรก่อน ไม่ใช้บัญชีร่วมกันเพื่อข้ามขอบเขตสิทธิ์ หากหน้าจอแจ้งสิทธิ์ไม่เพียงพอ ให้ผู้ที่มีสิทธิ์ดำเนินการจากบัญชีของตน

PROMPTRITY / 02

เข้าสู่ระบบและดูแลบัญชี

ใช้บัญชีที่องค์กรเชิญ ไม่ใช้รหัสผ่านร่วมกัน และออกจากระบบเมื่อใช้เครื่องส่วนกลาง

เริ่มจากคำเชิญ

1. เปิดลิงก์คำเชิญที่ส่งถึงอีเมลของตน ตรวจชื่อองค์กรหรือโรงเรียนก่อนตอบรับ
2. ตั้งรหัสผ่านตามเงื่อนไขบนหน้าเว็บ เก็บในเครื่องมือจัดการรหัสผ่านที่องค์กรอนุมัติ
3. เข้าสู่ระบบและตรวจชื่อบัญชี บทบาทและหน่วยงาน หากไม่ตรงให้หยุดใช้งานและติดต่อผู้ดูแล

เปลี่ยนข้อมูลบัญชี

เปิด “บัญชีของฉัน” แก้ชื่อหรือเปลี่ยนรหัสผ่านโดยกรอกรหัสผ่านปัจจุบัน เมื่อเปลี่ยนแล้วตรวจว่าเข้าใหม่ได้ ไม่ส่งรหัสผ่านให้ผู้ดูแลหรือทีมบริการ

ลืมรหัสผ่านหรือคำเชิญใช้ไม่ได้

ใช้ “ลืมรหัสผ่าน” ที่หน้าเข้าสู่ระบบ ตรวจกล่องอีเมลและจดหมายขยะ เปิดลิงก์ล่าสุดเพื่อตั้งใหม่ หากคำเชิญหมดอายุให้ผู้ดูแลตรวจและเชิญใหม่ ไม่เผยแพร่ลิงก์ตั้งรหัสหรือคำเชิญในกลุ่มสาธารณะ

เมื่อเข้าได้แต่เมนูไม่ตรง

ตรวจบทบาทกับผู้ดูแล การเข้าระบบสำเร็จไม่ได้ให้สิทธิ์ทุกหน้า หากเข้าลิงก์แล้วกลับหน้าแรกอาจเป็นการป้องกันตามสิทธิ์ ไม่ควรลองบัญชีของผู้อื่น

ที่อยู่สำหรับเข้าใช้

app.promptrity.com/login สำหรับ dashboard; ปุ่ม Google/Microsoft มีเมื่อผู้ให้บริการเปิด SSO และยังต้องเป็นสมาชิกที่ได้รับเชิญ

PROMPTRITY / 03

เชิญและดูแลสมาชิก

เจ้าของและผู้ดูแลระบบใช้หน้า “สมาชิกและอุปกรณ์” เพื่อควบคุมว่าใครใช้งานในองค์กรและแต่ละคนมีสิทธิ์ใด

เชิญทีละคนและเป็นชุด

1. เลือก “เชิญพนักงาน” กรอกอีเมล แผนกและบทบาท ตรวจอีเมลก่อนยืนยัน
2. ส่งคำเชิญผ่านช่องทางของระบบ หากระบบแสดงลิงก์ให้คัดลอก ส่งให้ผู้รับโดยตรงและถือว่าลิงก์นั้นเป็นข้อมูลสำหรับเข้าบัญชี
3. สำหรับรายชื่อจำนวนมาก เลือกนำเข้าไฟล์ CSV, TSV หรือ XLSX ตรวจหัวคอลัมน์ อีเมล และผลพรีวิวจำนวนที่จะเพิ่มหรือข้ามก่อนยืนยัน
4. ให้ผู้รับเปิดลิงก์ ตอบรับและตั้งบัญชี จากนั้นตรวจสถานะในตาราง คำเชิญที่ยังรอตอบรับยังไม่เท่ากับผู้ใช้งานพร้อมเครื่องป้องกัน

เปลี่ยนบทบาทหรือแผนก

เปิดรายการสมาชิก เลือกบทบาทและแผนกให้ตรงงาน บันทึกแล้วตรวจค่าที่แสดงใหม่ การมีหลายอุปกรณ์ไม่ได้ทำให้เป็นหลายคน การนับ seat อิงผู้ใช้งานที่มีสถานะใช้งานอยู่

เมื่อย้ายงานหรือลาออก

เลือกระงับเมื่อจำเป็นต้องหยุดการใช้งานชั่วคราว หากนำออกจากองค์กร เหตุการณ์เดิมจะถูกเปลี่ยนให้ไม่ผูกกับตัวบุคคล การนำออกกับการลบข้อมูลตามคำขอเป็นคนละการกระทำ จึงต้องเลือกให้ตรงวัตถุประสงค์

คำขอลบข้อมูล

ตรวจตัวตนและขอบเขตคำขอกับผู้ประสานงานข้อมูลส่วนบุคคลก่อนดำเนินการผ่านเมนูของสมาชิก การลบมีหลักฐานในบันทึกการทำงาน หลีกเลี่ยงการส่งออกข้อมูลมากกว่าที่จำเป็นระหว่างตรวจคำขอ

PROMPTRITY / 04

ติดตั้งและตรวจสถานะการป้องกัน

ส่วนขยายต้องอยู่ในเบราว์เซอร์และโปรไฟล์ที่พนักงานใช้ AI จริง พร้อมลงทะเบียนเข้ากับองค์กร

พนักงานติดตั้งและเข้าใช้

1. เปิดลิงก์หน้า “สำหรับพนักงาน” ที่องค์กรส่งให้ แล้วกดติดตั้งจาก Chrome Web Store ใช้ได้กับ Google Chrome และ Microsoft Edge บน Edge ให้กด “อนุญาตส่วนขยายจากร้านค้าอื่น” ก่อน ถ้าฝ่าย IT ติดตั้งให้แล้วข้ามไปข้อถัดไป
2. คลิกไอคอน promptrity บนแถบเครื่องมือ ถ้าไม่เห็นให้กดรูปจิ๊กซอว์แล้วปักหมุด เข้าสู่ระบบด้วยอีเมลบริษัทที่ตอบรับคำเชิญแล้ว ไม่ใช้บัญชีหรือโทเคนของเพื่อนร่วมงาน
3. ตรวจสถานะในส่วนขยายและให้ผู้ดูแลตรวจเครื่องใน “สมาชิกและอุปกรณ์” ว่ามีการติดต่อระบบล่าสุด
4. เปิดเว็บ AI ที่องค์กรอนุญาต หากเพิ่งอัปเดตส่วนขยายและมีข้อความให้รีเฟรช ให้รีเฟรชแท็บก่อนส่งข้อความ
5. ทดลองด้วยข้อมูลสมมติ อ่านผลเทียบกับโหมดขององค์กร หากยังเป็นสังเกตการณ์ การไม่บล็อกเป็นพฤติกรรมที่ตั้งใจไว้

ฝ่าย IT ติดตั้งแบบบังคับ

ใน “สมาชิกและอุปกรณ์” กด “ส่งลิงก์ติดตั้ง” แผงนี้มีทั้งลิงก์ให้พนักงานติดตั้งเอง และขั้นตอนพร้อมค่าที่ต้องใส่สำหรับ Google Workspace (บังคับติดตั้งและปักหมุดที่แถบเครื่องมือ) Group Policy หรือ Intune ของ Chrome และ Edge ไฟล์ .reg สำหรับ Windows ที่ไม่มี Active Directory และ configuration profile ของ macOS ทดสอบเครื่องนำร่องและตรวจหน้า chrome://policy ก่อนกระจายทั้งองค์กร

การแจกส่วนขยาย

ส่วนขยาย Promptrity เผยแพร่บน Chrome Web Store แล้ว พนักงานพบลิงก์ติดตั้งในอีเมลเชิญ หน้า “สำหรับพนักงาน” และหน้า “ประวัติของฉัน” ขณะที่ยังไม่มีเครื่อง ไม่ติดตั้งจากไฟล์ที่ส่งต่อกันเอง วิธี Load unpacked ใช้เฉพาะการทดสอบของฝ่าย IT ตรวจคอลัมน์ “เครื่อง” ในตารางสมาชิก: ป้องกันอยู่ ยังไม่ติดตั้ง หรือเครื่องขาดการติดต่อ

เครื่องไม่มีการติดต่อ

ตรวจอินเทอร์เน็ต โปรไฟล์เบราว์เซอร์ ส่วนขยายและการเข้าสู่ระบบก่อน หากยังไม่พร้อม ให้หลีกเลี่ยงการส่งข้อมูลจริงที่เป็นความลับและแจ้งฝ่าย IT

PROMPTRITY / 05

ตั้งนโยบายและทยอยเปิดใช้

กฎตัดสินจากผู้ใช้ ประเภทข้อมูล ปลายทางและเงื่อนไขที่กำหนด เมื่อหลายกฎตรงกัน ลำดับกฎมีผลต่อคำตัดสิน

ผลของกฎ	สิ่งที่ผู้ใช้พบ
ปล่อยผ่าน	ข้อความส่งต่อได้ตามปกติ
เตือน	แสดงสิ่งที่พบและทางเลือกที่นโยบายอนุญาต
ปิดบัง	แทนส่วนข้อความที่ตรวจพบก่อนส่ง ผู้ใช้ควรอ่านผลอีกครั้ง
บล็อก	หยุดคำขอ ผู้ใช้แก้ข้อมูลหรือขอปรับนโยบายผ่านผู้ดูแล

เปลี่ยนกฎอย่างตรวจสอบได้

1. เข้า “นโยบาย” อ่านกฎที่ใช้อยู่และสถานะขั้นการเปิดใช้งาน
2. เลือกผลของกฎและสิทธิ์ส่งต่อพร้อมเหตุผลตามความจำเป็น แล้วบันทึกการเปลี่ยนแปลง
3. ทดสอบข้อความสมมติที่ควรพบและไม่ควรพบ ตรวจประเภทข้อมูล กฎที่ตรง และคำตัดสิน ไม่ดูแค่คะแนนความเสี่ยง
4. หลังครบ 14 วัน เลือก “เปิดขั้นถัดไป” ในส่วน “การเปิดใช้งาน” ทีละขั้น อ่านความหมายของแต่ละขั้นในหัวข้อ “ระดับการเปิดใช้งาน” และผ่านรายการตรวจในหัวข้อ “เงื่อนไขก่อนปลดแต่ละขั้น” ก่อนกดทุกครั้ง

รหัสลับและกุญแจเข้าระบบ

กฎ CREDENTIAL ไม่เปิดทางให้ส่งต่อด้วยเหตุผล และบล็อกตั้งแต่ขั้น 1 ของการเปิดใช้งานไปจนถึงขั้น 4 ช่วงสังเกตการณ์ยังไม่บล็อก จึงต้องทดสอบด้วยค่าเสมือนจริงที่ไม่มีสิทธิ์ใช้งาน

คะแนนไม่ใช่คำตัดสิน

การพบข้อมูลประเภทหนึ่งไม่ได้แปลว่าทุกอุตสาหกรรมต้องบล็อกเหมือนกัน ตรวจเงื่อนไขกฎและปลายทางเสมอ หากผลจากตัวทดสอบกับเครื่องจริงต่างกัน ให้ตรวจเวอร์ชันนโยบายและโหมดก่อน

PROMPTRITY / 06

ทำไมไม่บล็อกตั้งแต่วันแรก

เป้าหมายไม่ใช่การบล็อกให้ได้มากที่สุด แต่คือให้ข้อมูลลับไม่หลุด และพนักงานยังใช้ AI ทำงานในช่องทางที่องค์กรมองเห็น การเปิดบล็อกเต็มที่ตั้งแต่วันแรกมักให้ผลตรงข้าม

เหตุผล	ถ้าบล็อกตั้งแต่วันแรก
กฎเริ่มต้นยังไม่รู้จักองค์กร	นโยบายตามอุตสาหกรรมเป็นแค่จุดตั้งต้น คำศัพท์ภายใน ชื่อโครงการ หรือเลขเอกสารบางแบบอาจถูกมองว่าเป็นข้อมูลเสี่ยง งานปกติจะหยุดทั้งที่ไม่มีความลับ
การเตือนผิดทำลายความเชื่อใจเร็วที่สุด	พนักงานจะกดผ่านโดยไม่อ่าน หรือย้ายไปใช้ AI บนมือถือส่วนตัวซึ่งองค์กรมองไม่เห็นเลย ความเสี่ยงจึงสูงกว่าตอนไม่มีระบบ
พนักงานต้องรู้ก่อนว่าระบบคืออะไร	คนที่เจอกล่องบล็อกครั้งแรกโดยไม่เคยได้รับแจ้ง จะรู้สึกว่าถูกจับผิด ความร่วมมือหายไปตั้งแต่ต้น
การติดตั้งยังไม่ครบ	ช่วงแรกบางเครื่องยังไม่ได้ติดตั้ง ถ้าบางคนถูกบล็อกแต่บางคนไม่โดน จะไม่เป็นธรรมและสร้างความสับสน
ต้องมีตัวเลขฐานไว้เทียบ	ผลสังเกตการณ์ 14 วันบอกว่าก่อนเปิดใช้ ข้อมูลเสี่ยงถูกส่งเข้า AI กี่ครั้ง จากแผนกไหน ประเภทใด ใช้คุยกับผู้บริหาร วัดผลหลังเปิดใช้ และประกอบรายงาน PDPA

ทำไมต้องปรับทีละระดับ

แต่ละขั้นเพิ่มความเข้มเพียงเรื่องเดียว ถ้ามีเสียงบ่นหลังเลื่อนขั้นจึงรู้ทันทีว่ามาจากการเปลี่ยนแปลงไหน พนักงานเห็นกล่องเตือนก่อน แล้วจึงเจอการปิดบังและการบล็อก กฎถูกแก้จากข้อมูลจริงก่อนจะมีผลแรงขึ้น เพราะการเตือนผิดเสียเวลาไม่กี่วินาที แต่การบล็อกผิดทำให้งานหยุด และตัวเลขก่อนและหลังแต่ละขั้นใช้รายงานผู้บริหารและประกอบรายงาน PDPA ได้

ช่วงสังเกตการณ์ไม่ใช่ช่วงที่ระบบปิดตา

ระบบตรวจทุกข้อความตามนโยบายจริง เพียงยังไม่ขัดจังหวะใคร 14 วันนี้ข้ามไม่ได้ หากมีข้อมูลที่ต้องห้ามส่งทันที เช่น องค์กรเพิ่งมีเหตุข้อมูลรั่ว ให้ประกาศเป็นนโยบายกับพนักงานโดยตรงคู่กันไป

PROMPTRITY / 07

ระดับการเปิดใช้งาน

หลังสังเกตการณ์ ระบบเพิ่มความเข้มทีละขั้น เรียงจากกระทบงานน้อยไปมาก: บล็อกรหัสลับ เตือน ปิดบัง แล้วจึงบล็อกตามนโยบาย

ระดับ	ระยะ	ระบบทำอะไร และพนักงานเห็นอะไร
สังเกตการณ์	14 วัน ระบบบังคับ	ตรวจทุกข้อความตามนโยบายจริง แล้วปล่อยผ่านทั้งหมด นับไว้ว่าจะบล็อก จะปิดบัง หรือจะเตือน พนักงานไม่เห็นกล่องใด ๆ
ขั้น 1 บล็อกเฉพาะ API key และรหัสลับ	1 สัปดาห์	ส่ง API key รหัสผ่าน และ token ไม่ได้ แอป AI ที่ตั้งเป็น “ห้ามใช้” ถูกบล็อก ข้อมูลอื่นยังผ่านโดยไม่มีกล่อง
ขั้น 2 เตือนทุกประเภทข้อมูล	2 สัปดาห์	กฎทุกข้อขึ้นเป็นกล่องเตือน พนักงานเลือกเองว่าจะปิดบัง แก้ หรือส่งต่อ
ขั้น 3 ปิดบังข้อมูลตามกฎ	2 สัปดาห์	กฎที่ตั้งเป็นปิดบังหรือบล็อก จะปิดบังส่วนที่เสี่ยงให้ก่อนส่ง งานเดินต่อได้ ยังไม่บล็อกข้อมูลทั่วไป
ขั้น 4 บล็อกตามนโยบายเต็มรูปแบบ	ถาวร	กฎทุกข้อทำงานตามที่ตั้งไว้ กฎที่ตั้งเป็นบล็อกส่งไม่ได้จนกว่าจะเอาข้อมูลออก หรือส่งพร้อมเหตุผลถ้ากฎนั้นเปิดตัวเลือกไว้

กฎที่ตั้งไว้	สังเกตการณ์	ขั้น 1	ขั้น 2	ขั้น 3	ขั้น 4
API key / รหัสลับ	ผ่าน*	ส่งไม่ได้	ส่งไม่ได้	ส่งไม่ได้	ส่งไม่ได้
แอป AI ที่ตั้งเป็น “ห้ามใช้”	ผ่าน*	บล็อก	บล็อก	บล็อก	บล็อก
ข้อมูลที่ตั้งเป็น “บล็อก”	ผ่าน*	ผ่าน	เตือน	ปิดบัง	บล็อก
ข้อมูลที่ตั้งเป็น “ปิดบัง”	ผ่าน*	ผ่าน	เตือน	ปิดบัง	ปิดบัง
ข้อมูลที่ตั้งเป็น “เตือน”	ผ่าน*	ผ่าน	เตือน	เตือน	เตือน

อ่านตารางกฎ × ระดับ

* ผ่าน แต่นับไว้ในผลสังเกตการณ์ แต่ละขั้นเป็นเพดานของผล ไม่ใช่การบังคับเพิ่ม กฎที่ตั้งเป็นเตือนจะไม่กลายเป็นบล็อกในขั้นใดเลย ระยะของขั้น 1–4 เป็นค่าที่ระบบแนะนำ ระบบบังคับเฉพาะ 14 วันแรก ถ้าเงื่อนไขของขั้นถัดไปยังไม่ครบ ให้อยู่ขั้นเดิมนานกว่านี้ได้

PROMPTRITY / 08

เงื่อนไขก่อนปลดแต่ละขั้น

ก่อนกด “เปิดขั้นถัดไป” ทุกครั้ง ให้ผ่านรายการตรวจของขั้นนั้นและสื่อสารกับพนักงานให้ครบ เกณฑ์อัตราการเตือนผิดต่ำกว่า 10% ต่อกฎมาจากหน้าความเสี่ยงของระบบ ตัวเลขอื่นเป็นค่าแนะนำที่ปรับได้ตามองค์กร

ก่อนเปิดขั้น 1 · เมื่อสังเกตการณ์ครบ 14 วัน

1. ครบ 14 วันแล้ว ปุ่ม “เปิดขั้นถัดไป” จะกดได้เอง
2. เครื่องที่ “ป้องกันอยู่” ครอบคลุมพนักงานที่ใช้ AI อย่างน้อย 90% ตรวจการ์ด “เครื่องที่ไม่ได้รับการป้องกัน” ใน “ภาพรวม” และคอลัมน์ “เครื่อง” ใน “สมาชิกและอุปกรณ์”
3. อ่าน “ผลสังเกตการณ์” ใน “นโยบาย”: จะบล็อก จะปิดบัง จะเตือนกี่ครั้ง กฎที่ทำงานบ่อยสุด และแผนกที่กระทบมากสุด แล้วสุ่มดูเหตุการณ์ในหน้า “ความเสี่ยง” 10–20 รายการว่าตรงกับข้อมูลเสี่ยงจริง
4. ใช้ “ทดสอบข้อความ” กับข้อความที่ควรถูกจับ และข้อความงานปกติที่ไม่ควรถูกจับ แก้กฎที่ไม่ตรงก่อน
5. จัดหมวดแอปใน “การใช้ AI” เป็นอนุญาต เฝ้าระวัง หรือห้ามใช้ เพราะแอปที่ห้ามจะเริ่มถูกบล็อกตั้งแต่ขั้นนี้
6. สื่อสาร: แจ้งพนักงานล่วงหน้า 2–3 วันทำการ แนบคู่มือพนักงานและลิงก์ promptrity.com/employees กำหนดคนรับเรื่องเมื่อระบบเตือนผิด และถ้าผลสังเกตการณ์พบ API key ถูกส่งเข้า AI ให้ฝ่าย IT เปลี่ยนรหัสนั้น เพราะรหัสที่ส่งออกไปแล้วถือว่าหลุดแล้ว

ก่อนเปิดขั้น 2 · อยู่ขั้น 1 อย่างน้อย 1 สัปดาห์

1. ไม่มีเครื่อง “ขาดการติดต่อ” ค้าง และส่วนขยายเป็นเวอร์ชันล่าสุดในคอลัมน์ “เบราว์เซอร์ · เวอร์ชัน extension”
2. การบล็อกรหัสลับไม่ไปโดนข้อความงานปกติ เช่น เลขอ้างอิงยาวที่หน้าตาคล้าย key
3. ไม่มีเรื่องร้องเรียนจากพนักงานที่ยังไม่ได้ตอบ
4. สื่อสาร: บอกพนักงานว่าจะเริ่มเห็นกล่องเตือน แต่ละปุ่มหมายถึงอะไร และการกด “ไม่ใช่ข้อมูลลับ ส่งได้เลย” เมื่อระบบเตือนผิดช่วยให้ระบบดีขึ้น โดยไม่มีผลเสียกับพนักงาน

PROMPTRITY / 08

เงื่อนไขก่อนปลดแต่ละขั้น (ต่อ)

ก่อนเปิดขั้น 3 · อยู่ขั้น 2 อย่างน้อย 2 สัปดาห์

1. “อัตราการเตือนผิด” ในหน้า “ความเสี่ยง” ต่ำกว่า 10% ทุกกฎ กฎที่เกินจะถูกไฮไลต์
2. กฎที่เกิน 10% แก้แล้ว: ปรับเงื่อนไข จำกัดแผนกหรือแอป หรือลดผลเป็นเตือน
3. ใช้ “ทดสอบข้อความ” กับตัวอย่างงานจริงของแต่ละแผนก ดูว่าข้อความหลังปิดบังยังใช้ทำงานกับ AI ต่อได้ และถามหัวหน้าทีมที่ใช้ AI มากที่สุดว่ากฎข้อใดขวางงาน
4. สื่อสาร: แจ้งพนักงานว่าระบบจะเริ่มปิดบังข้อมูลเสี่ยงให้ก่อนส่ง งานยังเดินต่อได้ แต่ควรอ่านข้อความหลังปิดบังก่อนกดส่ง

ก่อนเปิดขั้น 4 · อยู่ขั้น 3 อย่างน้อย 2 สัปดาห์

1. อัตราการเตือนผิดยังต่ำกว่า 10% ทุกกฎ
2. ทบทวนกฎที่ตั้งเป็น “บล็อก” ทีละข้อ ว่าต้องบล็อกจริงหรือปิดบังก็พอ เพราะการปิดบังให้งานเดินต่อได้ และตัดสินใจว่ากฎใดเปิดให้ส่งต่อพร้อมเหตุผล เหมาะกับงานที่บางตำแหน่งต้องใช้ข้อมูลนั้นจริง กฎเรื่อง API key เปิดไม่ได้
3. ผู้บริหารรับทราบว่าจะมีข้อความถูกบล็อกประมาณเท่าใด จากผลสังเกตการณ์และหน้าความเสี่ยง
4. เลือกสิ่งที่ทำเมื่อระบบตอบไม่ทันใน “ตั้งค่า”: ปล่อยผ่าน (ค่าเริ่มต้น) ใช้เฉพาะการตรวจในเครื่อง หรือบล็อกทุกข้อความจนกว่าระบบจะกลับมา
5. สื่อสาร: ผู้บริหารแจ้งพนักงานเป็นทางการว่าข้อมูลประเภทใดส่งเข้า AI ไม่ได้ และถ้างานติดต้องทำอย่างไร พร้อมเปิดช่องทางขอข้อยกเว้นที่ตอบได้ภายใน 1 วันทำการ เพื่อไม่ให้พนักงานหันไปใช้มือถือส่วนตัว

PROMPTRITY / 08

เงื่อนไขก่อนปลดแต่ละขั้น (ต่อ)

หลังขั้น 4: ดูแลต่อเนื่องทุกสัปดาห์

1. ตรวจ “สมาชิกและอุปกรณ์” ว่ามีใคร “ยังไม่ติดตั้ง” หรือเครื่องที่ “ขาดการติดต่อ”
2. ดู “ความเสี่ยง” ระดับกลุ่มว่าข้อมูลประเภทใดเพิ่มขึ้น และกฎใดมีอัตราการเตือนผิดเกิน 10% แล้วปรับใน “นโยบาย”
3. อ่านอีเมลสรุปประจำสัปดาห์ที่ส่งถึงเจ้าของและผู้ดูแลทุกวันจันทร์ 08:00
4. กฎใหม่เริ่มที่ “เตือน” 1–2 สัปดาห์ ดูอัตราการเตือนผิด แล้วจึงเปลี่ยนเป็นปิดบังหรือบล็อก กฎเฉพาะบริษัทที่สร้างใหม่เริ่มต้นเป็นเตือนอยู่แล้ว
5. ทบทวนกฎทั้งหมดทุกไตรมาส หรือเมื่อทีมเริ่มใช้แอป AI ใหม่ เมื่อระบบนิ่งแล้วพิจารณาตั้งสิ่งที่ทำเมื่อระบบตอบไม่ทันเป็น “ใช้เฉพาะการตรวจในเครื่อง”

เลื่อนขั้นได้ทางเดียว

ระบบไม่มีปุ่มถอยขั้น เจ้าของและผู้ดูแลระบบเป็นผู้กด “เปิดขั้นถัดไป” ได้ และทุกครั้งมีหลักฐานว่าใครดำเนินการเมื่อใด ถ้าเลื่อนแล้วพบปัญหา ให้แก้ที่กฎข้อนั้นใน “นโยบาย” ส่วน “กฎทั้งหมด” โดยลดผลเป็นเตือน เปิดให้ส่งต่อพร้อมเหตุผล หรือปิดกฎชั่วคราว กฎเรื่อง API key ปิดไม่ได้ เครื่องพนักงานได้รับค่าใหม่ภายในประมาณ 5 นาที หรือทันทีเมื่อกด “ตรวจสอบตอนนี้” ในส่วนขยาย

PROMPTRITY / 09

สร้างกฎเฉพาะและจดจำเอกสารลับ

ใช้เมื่อกฎมาตรฐานไม่ครอบคลุมศัพท์ภายใน ราคาต้นทุน หรือข้อความจากเอกสารที่องค์กรมีสิทธิ์นำมาใช้

สร้างกฎเฉพาะบริษัท

1. ใน “นโยบาย” อธิบายข้อมูลที่ต้องการป้องกันให้ชัด เช่น ราคาต้นทุนต่อชิ้น แทนคำกว้าง ๆ ว่า “ข้อมูลสำคัญ”
2. เลือก “สร้างตัวอย่างให้ยืนยัน” แล้วอ่านนิยาม ตัวอย่างที่ควรเตือน ตัวอย่างที่ควรผ่าน และคำสำคัญที่เสนอ
3. แก้ตัวอย่างและคำสำคัญให้ตรงภาษาที่ใช้จริง จากนั้น “ยืนยันและเปิดใช้”
4. ตรวจผลของกฎในรายการกฎหลัก ค่าเริ่มต้นของกฎเฉพาะเป็นการเตือน หากจะเปลี่ยนเป็นบล็อก ต้องทดสอบผลกระทบก่อน

ลงทะเบียนเอกสารลับ

1. เปิดส่วน “เอกสารลับ” อัปโหลดเอกสารที่มีสิทธิ์ใช้งาน รอให้ปรากฏในรายการพร้อมจำนวนส่วนที่จดจำ
2. ใช้ข้อความสมมติหรือส่วนที่อนุญาตให้ทดสอบในช่องทดสอบ ตรวจว่าระบุเอกสารที่ตรงถูกต้อง
3. ทดสอบข้อความที่ไม่เกี่ยวข้องด้วย และลบรายการเมื่อเอกสารเลิกใช้หรือไม่ต้องการให้เป็นฐานตรวจอีกต่อไป

ข้อจำกัดที่สำคัญ

การตรวจเอกสารใช้ลายนิ้วมือข้อความ และอาจใช้เวกเตอร์ความหมายเมื่อเปิดบริการเสริม การคัดลอกช่วงยาวตรวจได้ดีกว่าข้อความสั้น การเรียบเรียงใหม่ทั้งหมดอาจไม่ตรง กฎเฉพาะยังพึ่งการคัดกรองและคำสำคัญ จึงไม่รับประกันการตรวจทุกถ้อยคำ

แยกสองช่องทางให้ชัด

เอกสารที่ลงทะเบียนไว้เพื่อจดจำไม่ใช่ไฟล์แนบของพนักงานที่ส่งเข้า AI การเปิดเทียบความหมายอาจส่งชิ้นส่วนเอกสารไปผู้ให้บริการ embedding ตามประกาศข้อมูล

PROMPTRITY / 10

ตั้งค่าการเก็บและความต่อเนื่อง

เจ้าของและผู้ดูแลควรบันทึกเหตุผลของการตั้งค่า และทบทวนเมื่อเปลี่ยนวัตถุประสงค์การใช้งาน

ระยะเวลาเก็บและข้อความตัดตอน

หน้า “ตั้งค่า” เลือกอายุข้อมูล 30, 90, 180 หรือ 365 วัน ค่าเริ่มต้น 90 วัน และเลือกว่าจะเก็บข้อความสั้นรอบจุดตรวจพบที่ปิดบังแล้วหรือไม่ กำหนดเท่าที่จำเป็นต่อวัตถุประสงค์ การลดระยะเวลาไม่ควรถูกตีความว่าไฟล์ส่งออกหรือสำรองเดิมหายทันที

เปิดเก็บข้อความเต็มเมื่อจำเป็น

1. เจ้าของระบุเหตุผลและยืนยันตัวตนซ้ำใน “ตั้งค่า” เพื่อเริ่มคำขอ
2. ผู้ดูแลอีกคนเข้าบัญชีของตน อ่านเหตุผลและยืนยันตัวตนก่อนอนุมัติ ผู้เริ่มคำขออนุมัติเองไม่ได้
3. ตรวจแถบแจ้งการเก็บข้อความเต็มที่ผู้ใช้เห็น และตรวจบันทึกการอนุมัติ
4. เมื่อหมดความจำเป็น เจ้าของปิดการเก็บได้โดยไม่ต้องรออนุมัติอีกคน การปิดไม่เท่ากับลบข้อมูลที่เก็บไปแล้ว

เมื่อระบบกลางตอบไม่ทัน

ค่าเริ่มต้นคือ fail-open เพื่อไม่หยุดงาน องค์กรอาจเลือกโหมดที่มีในหน้าตั้งค่า เช่น ใช้เฉพาะการตรวจในเครื่อง ต้องสื่อสารผลของแต่ละแบบกับผู้ใช้ การหมดเวลารอไม่ได้หมายถึงตรวจแล้วปลอดภัย

ส่งมอบหน้าที่เจ้าของ

เตรียมผู้ดูแลที่ตอบรับคำเชิญแล้ว ใช้กระบวนการโอนความเป็นเจ้าของในหน้าตั้งค่า ตรวจผู้รับและผลหลังดำเนินการ ไม่ส่งรหัสผ่านบัญชีเดิมให้เจ้าของคนใหม่

ก่อนเก็บเพิ่ม

ต้องแจ้งพนักงานและทบทวนฐานการประมวลผลขององค์กร การมีปุ่มเปิดในระบบไม่ได้แทนการประเมินความจำเป็นหรืออำนาจทางกฎหมาย

PROMPTRITY / 11

ส่งไฟล์แนบอย่างปลอดภัย

ไฟล์ที่รองรับจะถูกพักคำขอไว้เพื่ออ่านและตรวจข้อความก่อนอัปโหลดไปยัง AI แต่ไม่มีการรับประกันว่าอ่านได้ทุกไฟล์

ชนิด	สิ่งที่ต้องทราบ
TXT MD CSV JSON	ตรวจข้อความที่อ่านได้จากไฟล์
DOCX PDF XLSX PPTX	แยกข้อความจากโครงสร้างไฟล์ก่อนตรวจ
ภาพ สแกน หรือไฟล์อ่านไม่ได้	ยังไม่มี OCR สำหรับไฟล์ภาพหรือสแกน อาจถูกปล่อยผ่านพร้อมสถานะข้ามการตรวจ

ขั้นตอนของพนักงาน

1. เลือกไฟล์จากหน้า AI ที่รองรับ รอระบบตรวจ ไม่ปิดแท็บหรือกดส่งซ้ำระหว่างกำลังประมวลผล
2. ถ้ามีข้อความเตือน อ่านตัวอย่างบริเวณที่พบข้อมูล โดยจำไว้ว่าตัวอย่างไม่ใช่การสรุปทั้งไฟล์
3. หากต้องแก้ ให้ยกเลิกการส่ง แก้ไฟล์ต้นฉบับหรือนำข้อมูลออก แล้วแนบใหม่
4. ถ้าผลระบุว่าข้ามการตรวจ อย่าตีความว่าไฟล์ปลอดภัย ให้ตรวจด้วยคนหรือใช้ช่องทางภายในที่องค์กรอนุมัติ

เหตุใดไฟล์ไม่ถูกปิดบังอัตโนมัติ

ผลปิดบังจากนโยบายเปลี่ยนเป็นการเตือนสำหรับการอัปโหลด เพราะระบบไม่สร้างไฟล์ใหม่ที่แก้ไขเนื้อหาให้ ผู้ใช้ต้องแก้ต้นฉบับเอง ไฟล์ที่ตรวจไม่ได้หรือเกินเวลารออาจผ่านตามพฤติกรรม fail-open ของช่องไฟล์

ข้อมูลออกจากเครื่องไปที่ใด

ไบต์ของไฟล์ที่รองรับถูกส่งไปเซิร์ฟเวอร์เพื่อแยกข้อความและตรวจในหน่วยความจำ ไม่เก็บตัวไฟล์ แต่เหตุการณ์อาจมีชื่อไฟล์ ชนิด ขนาด ผลตรวจ และข้อความตัดตอนตามการตั้งค่า ชื่อไฟล์จึงไม่ควรมีข้อมูลลับ

ชื่อไฟล์ไม่ใช่ผลตรวจ

การเปลี่ยนนามสกุลหรือชื่อไฟล์ไม่ทำให้เนื้อหาปลอดภัย การตรวจพบหรือไม่พบขึ้นกับข้อมูลที่อ่านได้และรูปแบบคำขอของเว็บ AI

PROMPTRITY / 12

อ่านรายงานเพื่อปรับการใช้งาน

เจ้าของ ผู้ดูแลระบบ และผู้ดูรายงานใช้ข้อมูลระดับกลุ่มเพื่อเข้าใจประโยชน์และความเสี่ยง ไม่ใช้รายงานจัดอันดับพนักงาน

หน้า	คำถามที่ตอบได้
ภาพรวม	การใช้งานและความเสี่ยงขององค์กรเป็นอย่างไร เครื่องเริ่มใช้พร้อมหรือยัง
การใช้ AI	แอปและประเภทงานใดถูกใช้ เทียบกับรายการ subscription ที่องค์กรบันทึก
ความเสี่ยง	ข้อมูลประเภทใดถูกพบ กฎใดทำงาน และแนวโน้มเปลี่ยนอย่างไร
รายงาน และ PDPA	ส่งออกรายงานและหลักฐานการตั้งค่าที่ใช้ประกอบงานกำกับดูแล

อ่านและส่งออกอย่างมีบริบท

1. เลือกช่วงเวลาและกลุ่มที่ต้องการ เปรียบเทียบช่วงที่มีขนาดใกล้เคียงกัน
2. ตรวจโหมดการเปิดใช้งานของช่วงนั้น เพราะผลจำลองไม่เท่ากับจำนวนที่ถูกบล็อกจริง
3. เลือกส่งออก CSV จากหน้าที่รองรับ เก็บไฟล์ในพื้นที่ที่องค์กรอนุมัติและกำหนดผู้รับ
4. ถ้าใช้ “สรุปด้วย AI” ให้อ่านเทียบกับตัวเลขต้นทาง สรุปเป็นคำอธิบายช่วยอ่าน ไม่ใช่ข้อสรุปยืนยันเหตุการณ์

ข้อควรระวังในการตีความ

การพบความเสี่ยงมากอาจเกิดจากใช้งานมากขึ้น เปลี่ยนนโยบาย หรือครอบคลุมอุปกรณ์มากขึ้น ไม่ได้แปลว่าพนักงานประมาทกว่าเดิม รายงานใช้งานไม่ได้วัดความถูกต้องของคำตอบ AI หรือผลิตภาพรายบุคคล

ผู้ดูรายงาน

บทบาทนี้เปิดรายงานและประวัติของตนเองได้ แต่ปรับนโยบาย สมาชิกหรือการเงินไม่ได้ ส่งข้อเสนอพร้อมช่วงเวลาที่อ้างอิงให้ผู้ดูแลพิจารณา

PROMPTRITY / 13

Promptrity เก็บข้อมูลอะไร

แยกการตรวจชั่วคราวออกจากการเก็บเป็นเหตุการณ์ การไม่เก็บตัวไฟล์ไม่ได้แปลว่าไม่มีข้อมูลเกี่ยวกับไฟล์หรือผลตรวจอยู่ในระบบ

ชุดข้อมูล	วัตถุประสงค์และขอบเขต
บัญชีและองค์กร	ชื่อ อีเมล บทบาท แผนก รหัสผ่านแบบแฮช และข้อมูลองค์กร ใช้ยืนยันตัวตนและกำหนดสิทธิ์
หลักฐานการสมัคร	เวลาและเวอร์ชันข้อกำหนด/นโยบายที่ผู้สมัครใหม่ยอมรับหรือรับทราบ
อุปกรณ์และกิจกรรม	รหัสอุปกรณ์ เวอร์ชัน เวลาติดต่อ แอป ประเภทงาน หมวดความเสี่ยง ผลตรวจและค่าแฮชข้อความ
ข้อความตัดตอนและเหตุผล	ข้อความสั้นรอบจุดพบที่ปิดบังแล้วเมื่อเปิดตัวเลือก และเหตุผลส่งต่อที่เข้ารหัส
ข้อความเต็ม	ปิดเป็นค่าเริ่มต้น เปิดได้เมื่อผ่านการอนุมัติสองคนและมีแถบแจ้ง เก็บแบบเข้ารหัส
ไฟล์และเอกสารลับ	ไม่เก็บไฟล์ต้นฉบับ เก็บข้อมูลประกอบไฟล์ ลายนิ้วมือและเวกเตอร์เมื่อเปิดใช้ สำหรับเอกสารลับมีตัวอย่างข้อความสั้นเพื่อระบุส่วนที่ตรง
การเงินและบันทึก	ข้อมูลภาษี ใบแจ้งหนี้ เลขอ้างอิงการชำระและประวัติการแก้ไขระบบ

สิ่งที่ไม่ใช่หน้าที่ของระบบ

ไม่เก็บประวัติท่องเว็บทั่วไปนอกขอบเขต AI ไม่บันทึกภาพหน้าจอเป็นเครื่องมือเฝ้าดู ไม่เก็บคำตอบ AI ของพนักงานเป็นประวัติสนทนา และไม่มีตารางจัดอันดับพนักงาน

ข้อมูลตัวอย่างจากเอกสารลับ

ตัวอย่างข้อความของส่วนเอกสารที่ใช้เทียบมีอยู่ในแบบข้อมูล จึงต้องจำกัดสิทธิ์และทบทวนความจำเป็น ไม่ควรประกาศว่าเก็บเพียงค่าแฮชที่ไม่มีเนื้อหาใด ๆ

PROMPTRITY / 14

แก้ปัญหาและส่งเรื่องให้ผู้ดูแล

เริ่มจากตรวจบัญชี เครื่อง โหมดและนโยบายก่อนสรุปว่าเครื่องมือตรวจผิด

อาการ	ตรวจและดำเนินการ
ไม่เห็นการบล็อก	ดูแถบด้านบนของ “ภาพรวม” ว่ายังอยู่ในสังเกตการณ์ 14 วัน หรือขั้น 1–3 ที่บล็อกเฉพาะรหัสลับและแอปที่ห้ามใช้ ใช้ข้อความสมมติทดสอบกฎ
หน้าส่วนขยายให้รีเฟรช	คัดลอกงานที่พิมพ์ค้างไว้ แล้วกด “รีเฟรชตอนนี้” เพื่อโหลดตัวตรวจรุ่นปัจจุบัน
ขึ้น “ผูกครบจำนวนเครื่องแล้ว”	เลือกเครื่องเก่าที่ไม่ใช้แล้วเพื่อถอดออก จำนวนเครื่องต่อคนขึ้นกับแพ็กเกจ เมื่อคืนเครื่องให้กด “ออกจากเครื่องนี้” ในส่วนขยาย
เตือนข้อมูลไม่ลับ	ใช้ตัวเลือกแจ้งเตือนผิดเมื่อมีให้ หรือส่งเวลาและประเภทกฎให้ผู้ดูแล
เอกสารลับไม่ตรง	ตรวจว่าข้อความยาวพอและคัดลอกตรงหรือไม่ ข้อความสั้นหรือเรียบเรียงใหม่อาจไม่พบ
ไฟล์ไม่มีผลตรวจ	ดูว่ารูปแบบอ่านได้หรือเป็นภาพสแกน ตรวจสถานะข้ามการตรวจ ไม่ถือว่าปลอดภัย
กฎใหม่ยังไม่ทำงาน	ตรวจว่าบันทึกสำเร็จ เครื่องรับนโยบายใหม่ภายในประมาณ 5 นาที หรือทันทีเมื่อกด “ตรวจสอบตอนนี้” ในส่วนขยาย
หน้าแก้ไขถูกปิด	ตรวจบทบาทและแถบสถานะการเรียกเก็บเงินกับเจ้าของ

ข้อมูลที่ช่วยตรวจปัญหา

แจ้งชื่อองค์กร บทบาท วันเวลา เว็บ AI รุ่นเบราว์เซอร์ รุ่นส่วนขยาย ขั้นตอนสั้น ๆ ผลที่คาดและผลที่พบ แนบภาพเฉพาะบริเวณที่ลบข้อมูลจริงแล้ว ไม่ส่ง prompt จริง เอกสารลับ โทเคน รหัสผ่านหรือคุกกี้

หากสงสัยว่าข้อมูลออกไปแล้ว

หยุดส่งข้อมูลชุดนั้น แจ้งผู้รับผิดชอบความปลอดภัยขององค์กร ระบุเวลา แอปและชนิดข้อมูล หากเกี่ยวกับรหัสลับให้ผู้มีอำนาจเพิกถอนหรือหมุนรหัสทันทีตามแผนองค์กร การลบข้อความในหน้า AI ไม่รับประกันว่าผู้ให้บริการปลายทางลบสำเนาทั้งหมด

ติดต่อผู้ให้บริการ

official@promptrity.com โดยประสานผ่านผู้ดูแลองค์กรสำหรับเรื่องบัญชีและนโยบายขององค์กร

REFERENCE & SUPPORT

แหล่งข้อมูลและการติดต่อ

ตรวจคู่มือให้ตรงรุ่นและเงื่อนไขของบริการที่องค์กรหรือโรงเรียนเปิดใช้

ข้อมูลผลิตภัณฑ์

https://promptrity.com

นโยบายความเป็นส่วนตัว · ข้อกำหนดการใช้บริการและ DPA

ติดต่อผู้ให้บริการ

promptrity · official@promptrity.com

ผู้ใช้งานติดต่อผู้ดูแลองค์กรหรือโรงเรียนก่อนสำหรับสิทธิ์ นโยบายและข้อมูลของตนเอง

เอกสารประกอบและกฎหมาย

คู่มือนี้เรียบเรียงจากสเปกผลิตภัณฑ์ คู่มือทดสอบตามบทบาท และขอบเขตสิทธิ์ของระบบ ณ วันที่จัดทำ ความสามารถที่ต้องเปิดบริการเสริมหรือยังพัฒนาระบุไว้ในหัวข้อที่เกี่ยวข้อง

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ราชกิจจานุเบกษา 27 พฤษภาคม 2562

ราชกิจจานุเบกษา เล่ม 136 ตอน 69 ก หน้า 52

สำเนาเผยแพร่โดยกรมทรัพยากรน้ำบาดาล

การใช้เอกสาร

คู่มือเป็นคำอธิบายการใช้งานและมาตรการ ไม่แทนสัญญาที่มีผลหรือการตรวจทางกฎหมาย องค์กรควรทบทวนก่อนแจกให้ผู้ใช้และเมื่อระบบเปลี่ยนแปลง ไม่อ้างว่าผ่านการรับรองมาตรฐานหรือมีความแม่นยำสมบูรณ์

ชื่อและโลโก้ใช้เพื่อระบุผลิตภัณฑ์ตามอัตลักษณ์ของเว็บไซต์ ไม่มีการกล่าวอ้างสถานะจดทะเบียนเครื่องหมายการค้าเพิ่มเติม