คู่มือเจ้าขององค์กร

เริ่มใช้ให้ครบใน 5 ขั้น การเปิดใช้งานทีละระดับ และงานดูแลประจำสัปดาห์ · ฉบับวันที่ 9 พฤศจิกายน 2569

promptrity ตรวจข้อความและไฟล์ที่พนักงานส่งเข้าเว็บ AI ก่อนออกจากบริษัท แล้วปล่อยผ่าน เตือน ปิดบัง หรือบล็อกตามนโยบายที่คุณตั้ง โดยไม่หยุดงานของพนักงานโดยไม่จำเป็น

เตรียมก่อนเริ่ม

- [ ] อีเมลบริษัทของคุณ และ**ผู้ดูแลระบบอีกอย่างน้อย 1 คน** (บางเรื่องต้องอนุมัติสองคน)
- [ ] รายชื่อพนักงานจาก HR เป็นไฟล์ .csv หรือ .xlsx มีอีเมล ชื่อ และแผนก หัวคอลัมน์ภาษาไทยหรืออังกฤษก็ได้
- [ ] ตัดสินใจว่าจะให้พนักงานติดตั้งส่วนขยายเอง หรือให้ฝ่าย IT ติดตั้งให้ทุกเครื่อง

เริ่มใช้ใน 5 ขั้น

1. **สมัครองค์กร**

   เข้า app.promptrity.com/signup กรอกอีเมล ชื่อองค์กร อุตสาหกรรม และรหัสผ่าน แล้วติ๊กยอมรับข้อกำหนด ระบบโหลดนโยบายเริ่มต้นตามอุตสาหกรรมให้ทันที หน้า **ภาพรวม** จะมีรายการขั้นตอนเริ่มต้นให้ทำตาม

2. **เชิญพนักงาน**

   เมนู **สมาชิกและอุปกรณ์** → **เชิญพนักงาน** เชิญทีละคน หรือ **อัปโหลดรายชื่อพนักงาน** แล้วดูผล **ตรวจสอบก่อนยืนยัน** (จำนวนที่จะเพิ่มและที่ข้าม) ก่อนยืนยัน

   เลือกบทบาทให้แต่ละคน: **พนักงาน** **ผู้ดูรายงาน** หรือ **ผู้ดูแลระบบ** พนักงานได้อีเมลพร้อมลิงก์ตั้งรหัสผ่าน ถ้าอีเมลไม่ถึง ใช้ **สร้างลิงก์เชิญ** แล้วส่งให้เอง

3. **ติดตั้งส่วนขยายให้ทุกเครื่อง**

   ในหน้า **สมาชิกและอุปกรณ์** กด **ส่งลิงก์ติดตั้ง** แล้วเลือกวิธี:

   - **ให้พนักงานติดตั้งเอง:** ส่งลิงก์หน้า "สำหรับพนักงาน" ทาง LINE หรืออีเมล หน้านั้นมีปุ่มติดตั้งจาก Chrome Web Store และอธิบายว่าระบบเห็นอะไร พร้อมแนบคู่มือพนักงานฉบับย่อ
   - **ให้ฝ่าย IT ติดตั้งให้ทุกเครื่อง:** แผงเดียวกันมีขั้นตอนและค่าที่ต้องใส่สำหรับ Google Workspace, Group Policy / Intune, ไฟล์ .reg สำหรับ Windows ที่ไม่มี Active Directory และ macOS

   ตรวจคอลัมน์ **เครื่อง** ในตารางสมาชิก: **ป้องกันอยู่** = พร้อม · **ยังไม่ติดตั้ง** · **เครื่องขาดการติดต่อ**

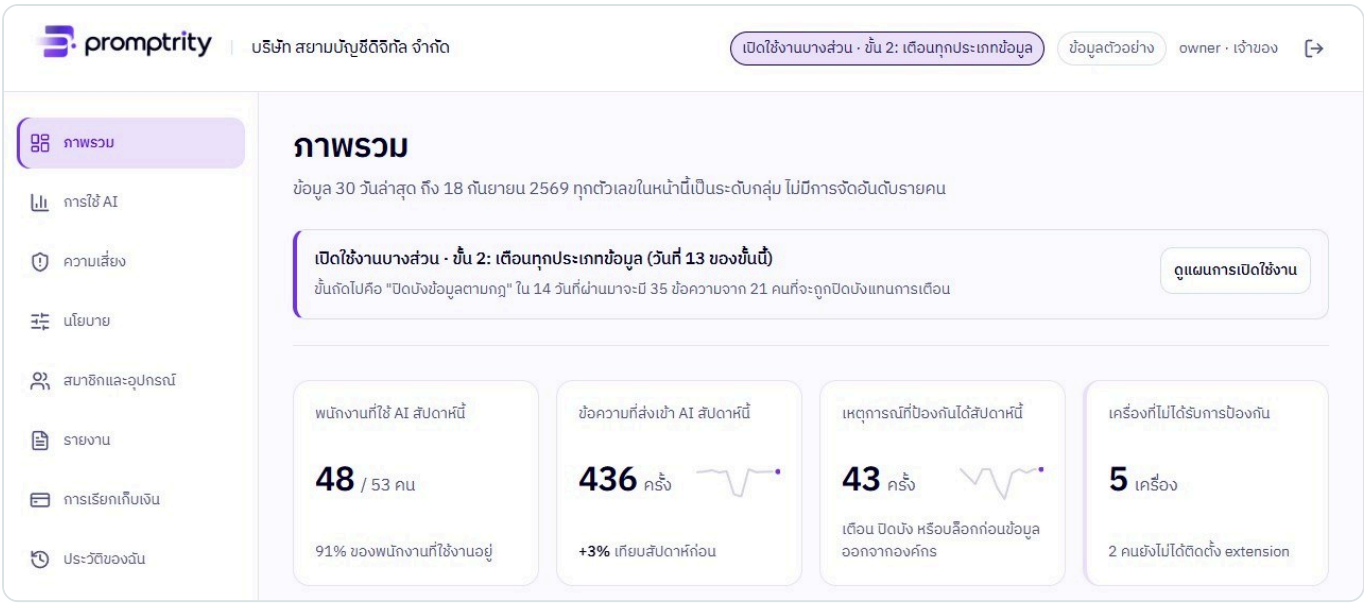
4. **สังเกตการณ์ 14 วัน**

   ช่วงนี้ระบบตรวจทุกข้อความแต่**ยังไม่เตือนหรือบล็อกใคร** ใช้เวลานี้ดูหน้า **ภาพรวม** **การใช้ AI** และ **ความเสี่ยง** คุณจะได้อีเมลสรุปในวันที่ 3, 7 และ 14 ปรับกฎใน **นโยบาย** และลองกับข้อความสมมติในตัวทดสอบได้ตลอด

5. **เปิดใช้จริงทีละขั้น**

   ครบ 14 วันแล้ว ไปที่ **นโยบาย** ส่วน **การเปิดใช้งาน** กด **เปิดขั้นถัดไป** แล้ว **ยืนยัน เปิดขั้นถัดไป** ระบบเปิดทีละขั้นจนครบ 4 ขั้น ก่อนกดทุกครั้ง อ่านเงื่อนไขของขั้นนั้นในหัวข้อ "การเปิดใช้งานทีละระดับ" ของคู่มือนี้

หน้าจอหลัก



หน้า "ภาพรวม" (ภาพจากข้อมูลสาธิต หน้าจอจริงอาจต่างเล็กน้อย): แถบด้านบนบอกขั้นการเปิดใช้ การ์ดบอกจำนวนคนที่ใช้ AI ข้อความที่ส่ง เหตุการณ์ที่ป้องกันได้ และเครื่องที่ยังไม่ได้รับการป้องกัน

เมนู	ใช้ทำอะไร
ภาพรวม	ตัวเลขสัปดาห์นี้ เครื่องที่ยังไม่ป้องกัน ขั้นการเปิดใช้ และปุ่ม "สรุปด้วย AI"
การใช้ AI	เว็บ AI และประเภทงานที่ทีมใช้ เทียบกับ subscription ที่บริษัทจ่ายอยู่
ความเสี่ยง	ข้อมูลประเภทไหน แผนกไหน กฎไหนทำงาน และอัตราการเตือนผิดต่อกฎ
นโยบาย	กฎ ตัวทดสอบข้อความ กฎเฉพาะบริษัท เอกสารลับ และขั้นการเปิดใช้
สมาชิกและอุปกรณ์	เชิญ เปลี่ยนบทบาท ระงับ นำออก ลิงก์ติดตั้ง และสถานะเครื่อง
รายงาน	รายงานรายเดือนและรายงาน PDPA ส่งออกเป็น CSV
การเรียกเก็บเงิน	แพ็กเกจ ข้อมูลภาษี และใบแจ้งหนี้ (เจ้าของเท่านั้น)
ตั้งค่า	ระยะเวลาเก็บข้อมูล การเก็บข้อความสั้นรอบจุดที่พบ สิ่งที่ทำเมื่อระบบตอบไม่ทัน และการโอนความเป็นเจ้าของ

บทบาทในองค์กร

บทบาท	ทำอะไรได้
เจ้าของ	ทุกอย่าง รวมถึงการเรียกเก็บเงินและโอนความเป็นเจ้าของ
ผู้ดูแลระบบ	นโยบาย สมาชิก อุปกรณ์ และรายงาน ไม่เห็นหน้าการเงิน อนุมัติคำขอเก็บข้อความเต็มเป็นคนที่สองได้
ผู้ดูรายงาน	อ่านภาพรวมและรายงานอย่างเดียว
พนักงาน	ใช้ส่วนขยายและดูประวัติของตัวเอง

ทุกบทบาทมีเมนู "ประวัติของฉัน" และ "บัญชีของฉัน" ของตัวเอง

ทำไมไม่บล็อกตั้งแต่วันแรก

เป้าหมายของ promptrity ไม่ใช่การบล็อกให้ได้มากที่สุด แต่คือ**ให้ข้อมูลลับไม่หลุด และพนักงานยังใช้ AI ทำงานในช่องทางที่บริษัทมองเห็น** การเปิดบล็อกเต็มที่ตั้งแต่วันแรกมักได้ผลตรงข้าม ด้วยเหตุผล 5 ข้อ

1 กฎเริ่มต้นยังไม่รู้จักบริษัทคุณ

นโยบายตามอุตสาหกรรมเป็นแค่จุดตั้งต้น คำศัพท์ภายใน ชื่อโครงการ หรือเลขเอกสารบางแบบอาจถูกมองว่าเป็นข้อมูลเสี่ยง ถ้าบล็อกทันที งานปกติจะหยุดทั้งที่ไม่มีความลับ

2 การเตือนผิดทำลายความเชื่อใจเร็วที่สุด

ถ้าระบบขวางงานปกติบ่อย พนักงานจะกดผ่านโดยไม่อ่าน หรือย้ายไปใช้ AI บนมือถือส่วนตัวซึ่งบริษัทมองไม่เห็นเลย ความเสี่ยงจะสูงกว่าตอนไม่มีระบบ

3 พนักงานต้องรู้ก่อนว่าระบบคืออะไร

คนที่เจอกล่องบล็อกครั้งแรกโดยไม่เคยได้รับแจ้ง จะรู้สึกว่าถูกจับผิด ความร่วมมือหายไปตั้งแต่ต้น

4 การติดตั้งยังไม่ครบ

ช่วงแรกบางเครื่องยังไม่ได้ติดตั้ง ถ้าบางคนถูกบล็อกแต่บางคนไม่โดน จะไม่เป็นธรรมและสร้างความสับสน

5 คุณต้องมีตัวเลขฐานไว้เทียบ

ผลสังเกตการณ์ 14 วันบอกว่าก่อนเปิดใช้ ข้อมูลเสี่ยงถูกส่งเข้า AI กี่ครั้ง จากแผนกไหน ประเภทใด ใช้คุยกับผู้บริหาร ใช้วัดผลหลังเปิดใช้ และประกอบรายงาน PDPA

> **ช่วงสังเกตการณ์ไม่ใช่ช่วงที่ระบบปิดตา** ระบบตรวจทุกข้อความตามนโยบายจริง เพียงยังไม่ขัดจังหวะใคร 14 วันนี้ข้ามไม่ได้ ถ้ามีข้อมูลที่ต้องห้ามส่งทันที เช่น บริษัทเพิ่งมีเหตุข้อมูลรั่ว ให้ประกาศเป็นนโยบายกับพนักงานโดยตรงคู่กันไป

ทำไมต้องปรับทีละระดับ

- **รู้ต้นเหตุเมื่อมีปัญหา:** แต่ละขั้นเพิ่มความเข้มเพียงเรื่องเดียว ถ้ามีเสียงบ่นหลังเลื่อนขั้น คุณรู้ทันทีว่ามาจากการเปลี่ยนแปลงไหน
- **ทีมปรับตัวทัน:** พนักงานเห็นกล่องเตือนก่อน แล้วจึงเจอการปิดบังและการบล็อก ไม่มีใครเจอการบล็อกโดยไม่ทันตั้งตัว
- **แก้กฎจากข้อมูลจริงก่อนจะมีผลแรงขึ้น:** เตือนผิดในขั้น 2 ทำให้เสียเวลาไม่กี่วินาที แต่ถ้าบล็อกผิด งานจะหยุด
- **ได้หลักฐานทุกขั้น:** ตัวเลขก่อนและหลังแต่ละขั้น ใช้รายงานผู้บริหารและประกอบรายงาน PDPA ได้

ระดับการเปิดใช้งาน

หลังสังเกตการณ์ ระบบเพิ่มความเข้มทีละขั้น เรียงจากกระทบงานน้อยไปมาก: บล็อกรหัสลับ → เตือน → ปิดบัง → บล็อกตามนโยบาย

ระดับ	ระยะ	ระบบทำอะไร และพนักงานเห็นอะไร	เป้าหมายของระดับนี้
สังเกตการณ์	14 วัน ระบบบังคับ	ตรวจทุกข้อความตามนโยบายจริง แล้วปล่อยผ่านทั้งหมด นับไว้ว่า "จะบล็อก จะปิดบัง จะเตือน" พนักงานไม่เห็นกล่องใดๆ	ได้ตัวเลขฐาน ปรับกฎ และติดตั้งให้ครบ
ขั้น 1 บล็อกเฉพาะ API key และรหัสลับ	1 สัปดาห์	ส่ง API key รหัสผ่าน และ token ไม่ได้ แอป AI ที่ตั้งเป็น "ห้ามใช้" ถูกบล็อก ข้อมูลอื่นยังผ่านโดยไม่มีกล่อง	พนักงานเห็นระบบทำงานครั้งแรกในเรื่องที่ไม่มีใครเถียง และยืนยันว่าทุกเครื่องรับนโยบายแล้ว
ขั้น 2 เตือนทุกประเภทข้อมูล	2 สัปดาห์	กฎทุกข้อขึ้นเป็นกล่องเตือน พนักงานเลือกเองว่าจะปิดบัง แก้ หรือส่งต่อ	วัดการเตือนผิดจากการใช้งานจริง แล้วแก้กฎก่อนเพิ่มความเข้ม
ขั้น 3 ปิดบังข้อมูลตามกฎ	2 สัปดาห์	กฎที่ตั้งเป็นปิดบังหรือบล็อก จะปิดบังส่วนที่เสี่ยงให้ก่อนส่ง งานเดินต่อได้ ยังไม่มีการบล็อกข้อมูลทั่วไป	ยืนยันว่าข้อความที่ปิดบังแล้วยังใช้งานกับ AI ได้
ขั้น 4 บล็อกตามนโยบายเต็มรูปแบบ	ถาวร	กฎทุกข้อทำงานตามที่ตั้งไว้ กฎที่ตั้งเป็นบล็อกส่งไม่ได้จนกว่าจะเอาข้อมูลออก หรือส่งพร้อมเหตุผลถ้ากฎนั้นเปิดตัวเลือกไว้	ป้องกันเต็มที่ และดูแลต่อเนื่อง

ระยะของขั้น 1–4 เป็นค่าที่ระบบแนะนำ ระบบบังคับเฉพาะ 14 วันแรก ถ้าเงื่อนไขของขั้นถัดไปยังไม่ครบ ให้อยู่ขั้นเดิมนานกว่านี้ได้

กฎแต่ละแบบทำงานอย่างไรในแต่ละระดับ

กฎที่คุณตั้งไว้	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

* ผ่าน แต่นับไว้ในผลสังเกตการณ์ · แต่ละขั้นเป็น "เพดาน" ไม่ใช่การบังคับเพิ่ม กฎที่คุณตั้งเป็นเตือนจะไม่กลายเป็นบล็อกในขั้นใดเลย

> **เลื่อนขั้นได้ทางเดียว** ระบบไม่มีปุ่มถอยขั้น เจ้าของและผู้ดูแลระบบเป็นผู้กดได้ และทุกครั้งมีหลักฐานว่าใครกดเมื่อไหร่ ถ้าเลื่อนแล้วพบปัญหา ให้แก้ที่กฎข้อนั้นใน `นโยบาย` → `กฎทั้งหมด` : ลดผลเป็นเตือน เปิดให้ส่งต่อพร้อมเหตุผล หรือปิดกฎชั่วคราว (กฎเรื่อง API key ปิดไม่ได้) เครื่องพนักงานได้รับค่าใหม่ภายในประมาณ 5 นาที หรือทันทีเมื่อพนักงานกด "ตรวจสอบตอนนี้" ในส่วนขยาย

เงื่อนไขก่อนปลดแต่ละขั้น

ก่อนกด **เปิดขั้นถัดไป** ทุกครั้ง ให้ผ่านเช็กลิสต์ของขั้นนั้นและทำมาตรการกับพนักงานให้ครบ เกณฑ์อัตราการเตือนผิด 10% มาจากหน้าความเสี่ยงของระบบ ส่วนตัวเลขอื่นเป็นค่าแนะนำ ปรับได้ตามบริษัท

ก่อนเปิดขั้น 1

เมื่อสังเกตการณ์ครบ 14 วัน

ตรวจให้ครบ

- [ ] ครบ 14 วันแล้ว (ปุ่ม **เปิดขั้นถัดไป** จะกดได้เอง)
- [ ] เครื่องที่ "ป้องกันอยู่" ครอบคลุมพนักงานที่ใช้ AI อย่างน้อย 90% ดูการ์ด "เครื่องที่ไม่ได้รับการป้องกัน" ใน **ภาพรวม** และคอลัมน์ **เครื่อง** ในหน้าสมาชิก
- [ ] อ่าน "ผลสังเกตการณ์" ใน **นโยบาย**: จะบล็อก จะปิดบัง จะเตือนกี่ครั้ง กฎที่ทำงานบ่อยสุด และแผนกที่กระทบมากสุด
- [ ] สุ่มดูเหตุการณ์ในหน้า **ความเสี่ยง** 10–20 รายการว่าตรงกับข้อมูลเสี่ยงจริง ถ้าไม่ตรง แก้กฎก่อน
- [ ] ใช้ **ทดสอบข้อความ** กับทั้งข้อความที่ควรถูกจับ และข้อความงานปกติที่ไม่ควรถูกจับ
- [ ] จัดหมวดแอปใน **การใช้ AI** เป็นอนุญาต / เฝ้าระวัง / ห้ามใช้ เพราะแอปที่ห้ามจะเริ่มถูกบล็อกตั้งแต่ขั้นนี้

มาตรการกับพนักงาน

- แจ้งพนักงานล่วงหน้า 2–3 วันทำการว่าระบบจะเริ่มทำงาน แนบคู่มือพนักงานและลิงก์ promptrity.com/employees
- กำหนดคนรับเรื่องเมื่อระบบเตือนผิดหรือขวางงาน
- ถ้าผลสังเกตการณ์พบ API key ถูกส่งเข้า AI ให้ฝ่าย IT เปลี่ยนรหัสนั้น รหัสที่ส่งออกไปแล้วถือว่าหลุดแล้ว

ก่อนเปิดขั้น 2

อยู่ขั้น 1 อย่างน้อย 1 สัปดาห์

ตรวจให้ครบ

- [ ] ไม่มีเครื่อง "ขาดการติดต่อ" ค้าง และส่วนขยายเป็นเวอร์ชันล่าสุด (คอลัมน์ "เบราว์เซอร์ · เวอร์ชัน extension")
- [ ] การบล็อกรหัสลับไม่ไปโดนข้อความงานปกติ เช่น เลขอ้างอิงยาวๆ ที่หน้าตาคล้าย key
- [ ] ไม่มีเรื่องร้องเรียนจากพนักงานที่ยังไม่ได้ตอบ

มาตรการกับพนักงาน

- บอกพนักงานว่าจะเริ่มเห็นกล่องเตือน และแต่ละปุ่มหมายถึงอะไร (หน้า 2 ของคู่มือพนักงาน)
- ย้ำว่าการกด **ไม่ใช่ข้อมูลลับ ส่งได้เลย** เมื่อระบบเตือนผิด ช่วยให้ระบบดีขึ้น ไม่มีผลเสียกับพนักงาน

ก่อนเปิดขั้น 3

อยู่ขั้น 2 อย่างน้อย 2 สัปดาห์

ตรวจให้ครบ

- [ ] "อัตราการเตือนผิด" ในหน้า **ความเสี่ยง** ต่ำกว่า 10% ทุกกฎ (กฎที่เกินจะถูกไฮไลต์)
- [ ] กฎที่เกิน 10% แก้แล้ว: ปรับเงื่อนไข จำกัดแผนกหรือแอป หรือลดผลเป็นเตือน
- [ ] ใช้ **ทดสอบข้อความ** กับตัวอย่างงานจริงของแต่ละแผนก ดูว่าข้อความหลังปิดบังยังส่งให้ AI ทำงานต่อได้
- [ ] ถามหัวหน้าทีมที่ใช้ AI มากที่สุดว่ากฎข้อไหนขวางงาน

มาตรการกับพนักงาน

- แจ้งพนักงานว่าระบบจะเริ่มปิดบังข้อมูลเสี่ยงให้ก่อนส่ง งานยังเดินต่อได้ แต่ควรอ่านข้อความหลังปิดบังก่อนกดส่ง

ก่อนเปิดขั้น 4 อยู่ขั้น 3 อย่างน้อย 2 สัปดาห์

ตรวจให้ครบ

- [ ] อัตราการเตือนผิดยังต่ำกว่า 10% ทุกกฎ
- [ ] ทบทวนกฎที่ตั้งเป็น "บล็อก" ทีละข้อ ว่าต้องบล็อกจริงหรือปิดบังก็พอ เพราะการปิดบังให้งานเดินต่อได้
- [ ] ตัดสินใจว่ากฎไหนเปิดให้ส่งต่อพร้อมเหตุผล เหมาะกับงานที่บางตำแหน่งต้องใช้ข้อมูลนั้นจริง (กฎเรื่อง API key เปิดไม่ได้)
- [ ] ผู้บริหารรับทราบว่าจะมีข้อความถูกบล็อกประมาณเท่าไหร่ จากผลสังเกตการณ์และหน้าความเสี่ยง
- [ ] เลือกสิ่งที่ทำเมื่อระบบตอบไม่ทันใน **ตั้งค่า** : ปล่อยผ่าน (ค่าเริ่มต้น) / ใช้เฉพาะการตรวจในเครื่อง / บล็อกทุกข้อความจนกว่าระบบจะกลับมา

มาตรการกับพนักงาน

- ผู้บริหารแจ้งพนักงานเป็นทางการว่าข้อมูลประเภทใดส่งเข้า AI ไม่ได้ และถ้างานติดต้องทำอย่างไร
- เปิดช่องทางขอข้อยกเว้นที่ตอบได้ภายใน 1 วันทำการ เพื่อไม่ให้พนักงานหันไปใช้มือถือส่วนตัว

หลังขั้น 4: ดูแลต่อเนื่อง

- ทำงานประจำสัปดาห์ตามหัวข้อถัดไป และทบทวนกฎทั้งหมดทุกไตรมาส หรือเมื่อทีมเริ่มใช้แอป AI ใหม่
- กฎใหม่ใช้หลักเดียวกันกับการเปิดใช้ทีละขั้น: เริ่มที่ "เตือน" 1–2 สัปดาห์ ดูอัตราการเตือนผิด แล้วจึงเปลี่ยนเป็นปิดบังหรือบล็อก (กฎเฉพาะบริษัทที่สร้างใหม่เริ่มต้นเป็นเตือนอยู่แล้ว)
- เมื่อระบบนิ่งแล้ว พิจารณาเปลี่ยนสิ่งที่ทำเมื่อระบบตอบไม่ทันเป็น "ใช้เฉพาะการตรวจในเครื่อง" ซึ่งยังจับเลขบัตร เบอร์โทร และ API key ได้ระหว่างที่ระบบกลางติดต่อไม่ได้

งานประจำสัปดาห์ (ประมาณ 10 นาที)

- [ ] **สมาชิกและอุปกรณ์** : มีใคร "ยังไม่ติดตั้ง" หรือเครื่องไหน "ขาดการติดต่อ" ไหม
- [ ] **ความเสี่ยง** : ข้อมูลประเภทไหนเพิ่มขึ้น แผนกไหนควรได้คำแนะนำเพิ่ม (ดูระดับกลุ่ม ไม่ใช่จับผิดรายคน)
- [ ] **ความเสี่ยง** : กฎไหนมีอัตราการเตือนผิดเกิน 10% ให้ปรับกฎหรือข้อยกเว้นใน **นโยบาย**
- [ ] อ่านอีเมลสรุปประจำสัปดาห์ ส่งถึงเจ้าของและผู้ดูแลทุกวันจันทร์ 08:00

เมื่อพนักงานเข้า–ออก

กรณี	ทำอย่างไร
พนักงานใหม่	**เชิญพนักงาน** แล้วส่งคู่มือพนักงานฉบับย่อให้
ลาพักยาว	**จัดการ** → **ระงับชั่วคราว** ไม่นับ seat และส่วนขยายจะหยุดตรวจ
ลาออก	**จัดการ** → นำออกจากองค์กร ประวัติเดิมถูกแทนด้วยนามแฝง และเครื่องถูกเพิกถอน
ขอลบข้อมูลตาม PDPA	**จัดการ** → ลบข้อมูล ระบบลบเหตุการณ์ทั้งหมดของคนนั้น ตรวจตัวตนผู้ขอก่อนทุกครั้ง

ค่าบริการ (เจ้าของเท่านั้น)

- ช่วงทดลอง 14 วันไม่มีค่าใช้จ่าย
- นับ seat จากคนที่สถานะ "ใช้งานอยู่" คนที่ระงับหรือยังไม่ตอบรับไม่นับ ถ้าเกิน seat ที่จ่าย ระบบยังป้องกันทุกคนต่อ
- เมนู **การเรียกเก็บเงิน** : เลือกแพ็กเกจและรอบบิล → กรอกข้อมูลภาษี (ชื่อนิติบุคคล เลขผู้เสียภาษี 13 หลัก ที่อยู่) → สร้างใบแจ้งหนี้แล้วโอนเงิน → ทีมงานยืนยันเมื่อได้รับเงิน
- ถ้าค้างชำระ: 14 วันแรกยังป้องกันเต็มที่ → จากนั้นหน้าจัดการเป็นแบบอ่านอย่างเดียว → ครบ 30 วันพักการตรวจ

สิ่งที่ควรบอกพนักงาน

- ระบบไม่เก็บข้อความเต็มโดยค่าเริ่มต้น ถ้าจำเป็นต้องเปิด ต้องให้เจ้าของเริ่มคำขอใน **ตั้งค่า** และผู้ดูแลอีกคนอนุมัติ แล้วพนักงานทุกคนจะเห็นแถบแจ้ง
- ไม่มีการจัดอันดับรายคน และพนักงานดู "ประวัติของฉัน" ได้เสมอ
- ส่งลิงก์ promptrity.com/employees ให้อ่านว่าระบบเห็นและเก็บอะไร

> เวลาสื่อสารกับพนักงาน ใช้คำว่า "ช่วยให้ไม่พลาด" หลีกเลี่ยงคำว่า "ละเมิด" "บันทึกแล้ว" หรือ "รายงานหัวหน้า" เพื่อให้ทีมไม่รู้สึกว่าถูกจับผิด

ข้อจำกัดที่ควรรู้

- ตรวจเฉพาะ Google Chrome และ Microsoft Edge ที่ติดตั้งส่วนขยาย มือถือและแอปบนเครื่องไม่ครอบคลุม
- รูปภาพและไฟล์สแกนยังตรวจไม่ได้
- ระบบอาจเตือนผิดหรือตรวจไม่พบได้ ควรใช้ร่วมกับนโยบายและการอบรมของบริษัท

แก้ปัญหาเบื้องต้น

อาการ	ตรวจอะไร
ยังไม่เห็นการบล็อก	ยังอยู่ในช่วงสังเกตการณ์ 14 วัน หรืออยู่ในขั้นที่ยังไม่บล็อก ดูแถบด้านบนของหน้าภาพรวม
พนักงานไม่ได้รับอีเมลเชิญ	ให้ดูในกล่องจดหมายขยะ หรือใช้ **สร้างลิงก์เชิญ** แล้วส่งเอง
เครื่องขาดการติดต่อ	ให้พนักงานเปิด Chrome หรือ Edge แล้วคลิกไอคอน promptrity ดูว่ายังเข้าสู่ระบบอยู่
แก้กฎแล้วเครื่องยังไม่ตาม	เครื่องรับนโยบายใหม่เองภายในประมาณ 5 นาที หรือทันทีเมื่อพนักงานกด "ตรวจสอบตอนนี้" ในส่วนขยาย
เมนูแก้ไขถูกปิด	ตรวจบทบาทของบัญชี และแถบสถานะการชำระเงินด้านบน

ติดต่อทีมงาน: official@promptrity.com · คู่มือฉบับเต็มอยู่ในลิงก์ "เอกสารคู่มือ" ท้ายเว็บไซต์ promptrity.com