คู่มือ PDPA สำหรับ Biz-Flow

เอกสารนี้อธิบายเฉพาะฟีเจอร์คุ้มครองข้อมูลส่วนบุคคล (PDPA) ในระบบ Biz-Flow / บัญชีการจัดการ (MAS 3) — สำหรับผู้ดูแลระบบ Tenant, DPO/IR และ Superuser ของแพลตฟอร์ม
· เวอร์ชันเอกสาร 1.0 · อัปเดต 22 สิงหาคม 2569

1. บทนำ

Biz-Flow เป็นซอฟต์แวร์บัญชี SaaS ที่เก็บข้อมูลส่วนบุคคลหลายประเภท เช่น ผู้ใช้งาน ลูกค้า ผู้ขาย พนักงาน คำสั่งซื้อออนไลน์ และข้อความติดต่อ ระบบมีเครื่องมือ PDPA ดังนี้:

- ประกาศความเป็นส่วนตัว / เงื่อนไข / DPA บนเว็บ + ดาวน์โหลด PDF
- บันทึกความยินยอม (ConsentRecord) พร้อม IP, User-Agent, เวอร์ชันเอกสาร
- เครื่องมือ DSAR สำหรับ Tenant Admin — ค้นหา / ส่งออก JSON / ลบหรือปกปิด PII
- ระบบแจ้งเตือนความผิดปกติ + นาฬิกา 72 ชม. + escalation ก่อนครบกำหนด

คู่มือนี้เป็นเอกสารปฏิบัติการระบบ ไม่ใช่คำปรึกษากฎหมาย
องค์กรควรตรวจสอบนโยบายภายในและ DPA กับผู้ประมวลผลภายนอกให้ครบถ้วน

2. บทบาทและขอบเขตความรับผิด

บทบาทใครหน้าที่ PDPA

ผู้ควบคุมข้อมูล (Platform)
ผู้ให้บริการ Biz-Flow
ข้อมูลสมัครใช้งาน ผู้ใช้แพลตฟอร์ม การชำระแพ็กเกจ ข้อความติดต่อ

ผู้ควบคุมข้อมูล (Tenant)
ลูกค้าองค์กรที่ใช้ระบบ
ลูกค้า/ผู้ขาย/พนักงาน/ผู้ซื้อที่นำเข้าใน Tenant ของตน

ผู้ประมวลผล
Biz-Flow ต่อ Tenant
ประมวลผลข้อมูลใน Tenant ตามคำสั่งของลูกค้าองค์กร

DPO / IR
ทีมที่ตั้งใน App Setting
รับแจ้งเตือนเหตุการณ์ ตอบคำขอใช้สิทธิ ประสานแจ้งเหตุละเมิด 72 ชม.

3. เอกสารกฎหมายบนเว็บ

หน้าสาธารณะ (ไม่ต้อง login):

หน้าURLเนื้อหา

ประกาศความเป็นส่วนตัว
/privacy/
นโยบาย PDPA เวอร์ชัน 1.1 · ดาวน์โหลด PDF ที่ /privacy/download/

เงื่อนไขการใช้บริการ
/terms/
ข้อตกลงการใช้ SaaS · PDF ที่ /terms/download/

DPA / ผู้ประมวลผล
/dpa/
รายการ sub-processors (Hosting, SMTP, Google, n8n OCR, CDN)

ติดต่อ / คำขอ PDPA
/contact/
แบบฟอร์ม + อีเมล/โทร/LINE จาก App Setting

Superuser — อัปโหลดไฟล์กฎหมาย

Superuser
ไปที่ ตั้งค่าระบบ (Company Settings) → ส่วน เอกสารกฎหมาย (PDPA / เงื่อนไข)

- อัปโหลด PDF/Word ประกาศความเป็นส่วนตัว และเงื่อนไข (ถ้ามีไฟล์จากทนาย)
- ตั้งเวอร์ชันเอกสาร — ใช้ใน consent audit
- ถ้าไม่ได้อัปโหลด ระบบสร้าง PDF อัตโนมัติจากเนื้อหาหน้าเว็บ

4. ความยินยอม (Consent)

ทุกครั้งที่มีการยินยอม ระบบบันทึกลง ConsentRecord พร้อม:

- วัตถุประสงค์ (purpose) · granted/denied · เวอร์ชัน privacy/terms
- IP · User-Agent · ผู้ใช้ · Tenant (ถ้ามี) · หลักฐาน (evidence)

จุดที่บังคับขอความยินยอม

จุดPurposeหมายเหตุ

สมัครใช้งาน (Signup)
signup
Modal 2 ขั้น: อ่าน Privacy → Terms ต้อง scroll ถึงท้ายก่อนกดยอมรับ

Checkout ออนไลน์
checkout
Checkbox ก่อนส่งคำสั่งซื้อ

AI-OCR อ่านใบเสร็จ
ocr
ก่อนส่งเอกสารไป n8n workflow

ชำระค่าแพ็กเกจ
package_payment
ก่อนยืนยันการโอน/ชำระ

DSAR export / erase
dsar_export / dsar_erase
บันทึกเมื่อ Admin ดำเนินการให้เจ้าของข้อมูล

ดู consent ใน Django Admin → บันทึกความยินยอม (PDPA)
หรือ export จากฐานข้อมูลตาราง accounting_consentrecord

5. สิทธิเจ้าของข้อมูล (DSAR)

Tenant Admin
เมนู: ตั้งค่าบริษัท → สิทธิเจ้าของข้อมูล (PDPA)
หรือ URL /{tenant}/company-settings/privacy-rights/

ขั้นตอนการใช้งาน

• ค้นหา — ใส่ชื่อ อีเมล เบอร์ เลขผู้เสียภาษี (อย่างน้อย 2 ตัวอักษร)

• ส่งออก JSON — ดาวน์โหลดชุดข้อมูลส่วนบุคคล (customer / supplier / employee / online_order / contact)

• ลบ/ปกปิด — ต้องติกยืนยัน · ระบบ anonymize ฟิลด์ติดต่อ · ตั้ง pdpa_erased_at

ข้อจำกัดสำคัญ

• ถ้ามีเอกสารภาษี/บัญชีอ้างอิง (ใบกำกับ ใบเสร็จ ซื้อ เงินเดือน) — ไม่ลบ master ทิ้ง แต่ล้างข้อมูลติดต่อ/ธนาคาร

• ระบบแสดงจำนวนเอกสารที่ยังผูกอยู่ (tax_links) ก่อน erase

• การ export จำนวนมากอาจ trigger Security Incident (bulk PII export)

คำขอจากบุคคลภายนอก (ไม่ใช่ Admin)

ให้เจ้าของข้อมูลติดต่อผ่าน /contact/ หรืออีเมล DPO
แล้ว Admin ดำเนินการผ่านเครื่องมือ DSAR ข้างต้น

6. การเก็บรักษาและเอกสารภาษี

ประเภทข้อมูลแนวปฏิบัติในระบบ

เอกสาร VAT / บัญชี / WHT / Payroll
เก็บตาม Tax Audit Trail — ไม่ลบเมือ DSAR erase master ทีมีเอกสารอ้างอิง

ข้อมูลติดต่อลูกค้า/ผู้ขาย/พนักงาน
ลบ/ปกปิดได้เมือไม่มีข้อจำกัดภาษี · ตั้ง pdpa_erased_at

บันทึกความยินยอม / Activity log
เก็บเพือ audit — ไม่ลบอัตโนมัติ

Security Incident timeline
เก็บเพือหลักฐาน IR · สถานะ Pending Review / รับทราบ / ปิดแล้ว

7. มาตรการความปลอดภัย

• HTTPS บน production (Cloudflare + HSTS)

• Session idle timeout — 15 นาที (ค่าเริมต้น)

• 2FA (TOTP) — Superuser / staff สิทธิสูง · /security/2fa/

• เข้ารหัสความลับ — SMTP App Password, Telegram token (Fernet)

• แยก Tenant — ข้อมูลธุรกิจแยกตามองค์กร

• Activity log — login/logout, DSAR, เอกสารสำคัญ

การตรวจ IP แปลกปลอม

ระบบเทียบ IPv6 แบบ prefix /64 (ลด false positive จากมือถือ)
และใช้ baseline login ทัง user ก่อนแจ้งเตือน
ปิดได้ที Company Settings → แจ้ง login จาก IP ใหม่

8. เหตุการณ์ความปลอดภัย / นาฬิกา 72 ชม.

เมือระบบตรวจพบความผิดปกติ จะสร้าง SecurityIncident โดย:

• detected_at = จุดเริมนับ 72 ชม. ตามแนวปฏิบัติแจ้งเหตุ PDPA

• สถานะเริมต้น Pending Review

• แจ้งทันที: Email DPO/IR · Telegram · Slack · Webhook (ตามทีตังค่า)

ประเภทที่ตรวจจับ

ประเภทเงื่อนไข

Export PII จำนวนมาก≥ 1,000 รายการ / 5 นาที (ปรับได้) — DSAR, Excel contacts, SQL dump
Login IP ใหม่IP fingerprint ไม่อยู่ใน baseline 90 วัน
ยกระดับสิทธิ์เปลี่ยน role เป็น tenant_admin

หน้าจัดการเหตุการณ์

• Platform /security/incidents/ (Superuser)

• Tenant /{tenant}/security/incidents/

• กด รับทราบ → หยุด escalation · กด ปิดแล้ว เมื่อดำเนินการครบ

Alert มีลิงก์ สคส. — https://www.pdpc.or.th/ และ https://complaint.pdpc.or.th/

9. Escalation ก่อนครบ 72 ชม. (<12 ชม.)

กันเคสตกหล่น — ถ้ายัง Pending Review และเหลือ ≤ 12 ชม. ก่อน deadline:

• Cron บนเซิร์ฟเวอร์: manage.py poll_security_escalations ทุก 15 นาที

• หรือ n8n workflow: docs/n8n_pdpa_escalation_poll.json

• ไม่ escalate ซ้ำภายใน 6 ชม. (dedup)

API สำหรับ n8n: GET /security/incidents/poll.json
· POST /security/incidents/escalate-poll/
(ต้องมี header X-Security-Poll-Token)

10. การตั้งค่า (สรุป)

Superuser Company Settings

• อีเมล IR / DPO · Telegram Bot + Chat ID · Slack / Webhook

• เกณฑ์ export PII · เปิด/ปิด unusual login · privilege alert

• ปุ่ม ทดสอบ Telegram

• อัปโหลดเอกสาร Privacy / Terms + เวอร์ชัน

• ข้อมูลติดต่อ (แสดงบนหน้า /privacy/ และ /contact/)

Tenant Admin

• DSAR tool — privacy-rights

• Security incidents (เฉพาะ Tenant)

• Activity log — ตรวจ login / DSAR

11. ผู้ประมวลผลภายนอก (Sub-processors)

รายละเอียดเต็มอยู่ที่ /dpa/ สรุป:

• Hosting / Cloud server

• SMTP (อีเมล)

• Google OAuth (เมื่อเปิดใช้)

• n8n AI-OCR (เมื่อเปิดใช้ — ต้องมี consent + DPA)

• CDN / Google Fonts

ก่อนเปิด OCR หรือ Google login ใน production ควรมี DPA กับผู้ให้บริการและอัปเดตหน้า DPA

12. ช่องทาง สคส. (PDPC)

• เว็บไซต์: https://www.pdpc.or.th/

• ยื่นเรื่องร้องเรียนออนไลน์: https://complaint.pdpc.or.th/

ใช้เมื่อเจ้าของข้อมูลต้องการร้องเรียนต่อหน่วยงาน — ระบุในประกาศความเป็นส่วนตัวข้อ 7

13. Checklist สำหรับ DPO / IR

• ตั้งอีเมล DPO และทดสอบ Telegram ใน Company Settings

• ตรวจประกาศ /privacy/ และ /terms/ ให้ตรงกับองค์กร (ชื่อ ที่อยู่ เลขผู้เสียภาษี)

• อัปโหลด PDF จากทนาย (ถ้ามี) หรือใช้ PDF อัตโนมัติจากระบบ

• ตรวจ DPA /dpa/ ครบ sub-processors ที่เปิดใช้จริง

• กำหนดผู้รับผิดชอบ DSAR ในแต่ละ Tenant

• ฝึกใช้เครื่องมือ privacy-rights (export + erase ทดลอง)

• ตรวจ /security/incidents/ เป็นประจำ · รับทราบภายใน 72 ชม.

• ยืนยัน cron poll_security_escalations ทำงาน (log ที่เซิร์ฟเวอร์)

• เปิด 2FA สำหรับ Superuser ทุกคน

• จัดทำแผนแจ้งเหตุละเมิดภายนอก (ลูกค้า / สคส.) แยกจากระบบ

14. ลิงก์อ้างอิงด่วน

รายการPath

คู่มือ PDPA (เอกสารนี)/manual-pdpa/
ดาวน์โหลดคู่มือ PDF/manual-pdpa/download/
ดาวน์โหลดคู่มือ HTML/manual-pdpa/download.html
ประกาศความเป็นส่วนตัว/privacy/
ดาวน์โหลด Privacy PDF/privacy/download/
เงื่อนไขการใช้บริการ/terms/
ดาวน์โหลด Terms PDF/terms/download/
DPA/dpa/
ติดต่อ / คำขอ PDPA/contact/
DSAR (Tenant)/{tenant}/company-settings/privacy-rights/
Security Incidents (Platform)/security/incidents/
Security Incidents (Tenant)/{tenant}/security/incidents/
2FA Setup/security/2fa/