DIP DATA SERVICE
DOCUMENTATION PORTAL

คู่มือผู้ดูแลระบบ
ระบบบริการข้อมูล (DIP Data Service)

แนวทางการตั้งค่า บริหารจัดการ และดูแลระบบ
เพื่อให้บริการอย่างมั่นคง ปลอดภัย และมีประสิทธิภาพ



กรมควบคุมโรค
Department of Disease Control

สารบัญ

1 วัตถุประสงค์และขอบเขต

2 ภาพรวมระบบและบทบาทผู้ใช้งาน

3 ข้อมูลจำเพาะของระบบ

4 การเข้าถึงและความปลอดภัย

5 การจัดการคำขอข้อมูล

6 การพิจารณาคำขอโดย DPO

7 การจัดการผู้ใช้งานและ API Token

8 การจัดการข้อมูลและเอกสาร

9 การส่งออกข้อมูลและรายงาน

10 Database Design และ Data Dictionary

11 การดูแลรักษาและแก้ไขปัญหา

1 วัตถุประสงค์และขอบเขต

เอกสารนี้อธิบายวิธีปฏิบัติงานของเจ้าหน้าที่ผู้ดูแลระบบ DIP Data Service สำหรับบริหารคำขอข้อมูล ผู้ใช้บริการ สิทธิ์การเข้าถึงข้อมูล เอกสารสาธารณะ และข้อมูลเปิด ให้สอดคล้องกับ TOR และการทำงานของระบบปัจจุบัน

2 ภาพรวมระบบและบทบาทผู้ใช้งาน

บทบาท	สิทธิ์หลัก
ผู้ใช้บริการ	ยื่น ติดตาม และตอบกลับคำขอข้อมูลของตนเอง ดาวน์โหลดผลลัพธ์ และประเมินความพึงพอใจ
เจ้าหน้าที่ผู้ดูแลระบบ	บริหารคำขอ ผู้ใช้บริการ เจ้าหน้าที่ ข้อมูล และเอกสาร
DPO	พิจารณาคำขอที่ส่งเข้ากระบวนการคุ้มครองข้อมูลส่วนบุคคล พร้อมบันทึกการตัดสินใจและความเห็น

สถานะคำขอที่แสดงในเมนูผู้ดูแลคือ งานใหม่ กำลังดำเนินการ ปิดงาน และยกเลิก โดยใช้สถานะระบบ 1, 2, 3 และ 0 ตามลำดับ

3 ข้อมูลจำเพาะของระบบ

รายการ	รายละเอียด
รูปแบบระบบ	เว็บแอปพลิเคชัน DIP Data Service
เทคโนโลยีหลัก	PHP 8.0 ขึ้นไป, Laravel 9, Laravel Sanctum สำหรับ API Token
ฐานข้อมูลระบบ	ฐานข้อมูลเชิงสัมพันธ์ กำหนดการเชื่อมต่อจากค่าคอนฟิกสภาพแวดล้อมของหน่วยงาน
การยืนยันตัวตน	บัญชีผู้ใช้ รหัสผ่าน การเข้าสู่ระบบผ่าน ThaiID และอีเมลตามการตั้งค่าระบบ
การควบคุมสิทธิ์	แยกผู้ใช้บริการ เจ้าหน้าที่ และ DPO; API กำหนดสิทธิ์ระดับ

	ฐานข้อมูลและฟิลด์
ไฟล์แนบ	คำขอ เอกสารประกอบ ไฟล์ตอบกลับ และไฟล์ปิดงาน

ผู้ดูแลต้องเก็บค่าเชื่อมต่อฐานข้อมูล รหัสลับ และ Token ไว้ในพื้นที่ที่จำกัดสิทธิ์ และไม่บันทึกค่าเหล่านี้ในคู่มือหรือช่องทางสาธารณะ

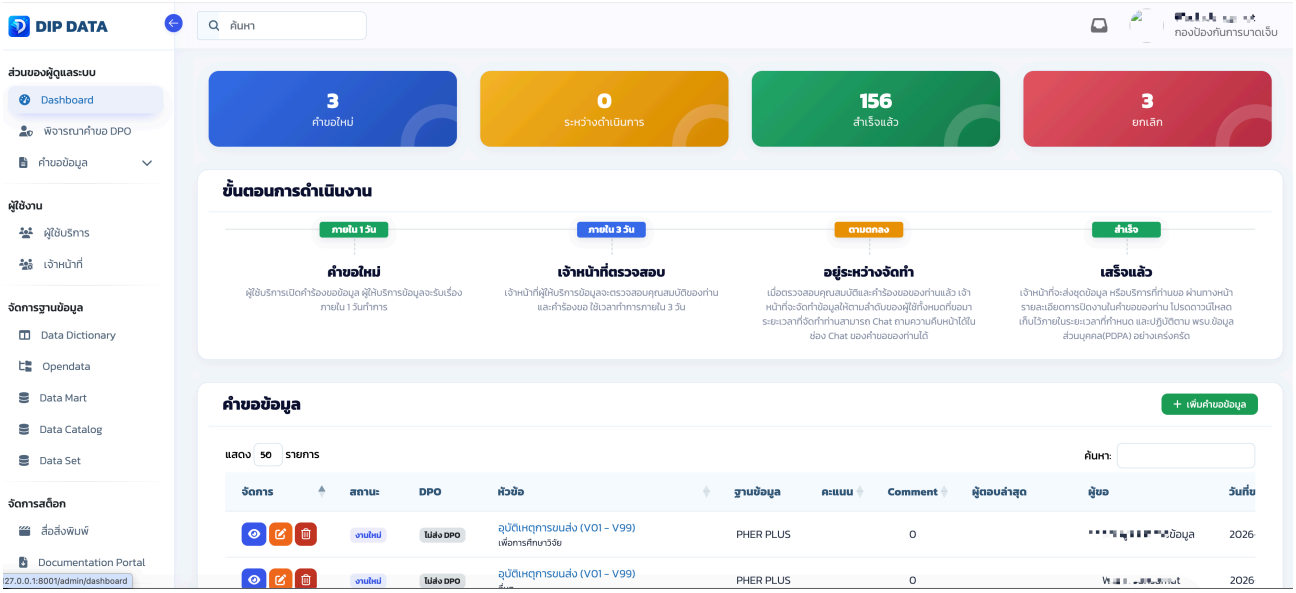
4 การเข้าถึงและความปลอดภัย

4.1 การเข้าสู่ระบบและเมนูผู้ดูแล

1. เข้าสู่ระบบด้วยบัญชีเจ้าหน้าที่ที่มีสถานะใช้งาน

2. ระบบนำไปยัง Dashboard สำหรับบัญชีที่กำหนดเป็นผู้ดูแล

3. ตรวจสอบเมนูด้านซ้าย ได้แก่ Dashboard คำขอข้อมูล ผู้ใช้งาน จัดการฐานข้อมูล Documentation Portal Open Data รายงาน และคู่มือ API



ภาพประกอบ: หน้าจอ Dashboard ของผู้ดูแลระบบ

4.2 หลักปฏิบัติด้านความปลอดภัย

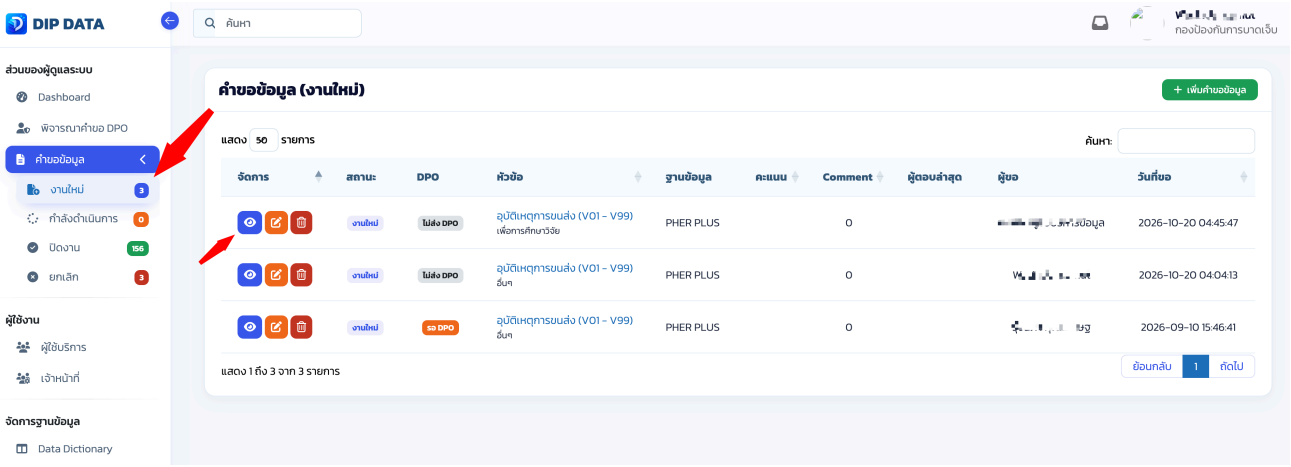
- ให้สิทธิ์เจ้าหน้าที่เท่าที่จำเป็นต่อหน้าที่ และทบทวนบัญชีผู้ใช้งานเป็นระยะ
- ห้ามส่ง API Token หรือไฟล์ข้อมูลออนไหวผ่านช่องทางที่ไม่ปลอดภัย
- กำหนดวันหมดอายุ ช่วงเวลาที่ใช้งาน และ IP ที่อนุญาตสำหรับ Token เมื่อมีความจำเป็น

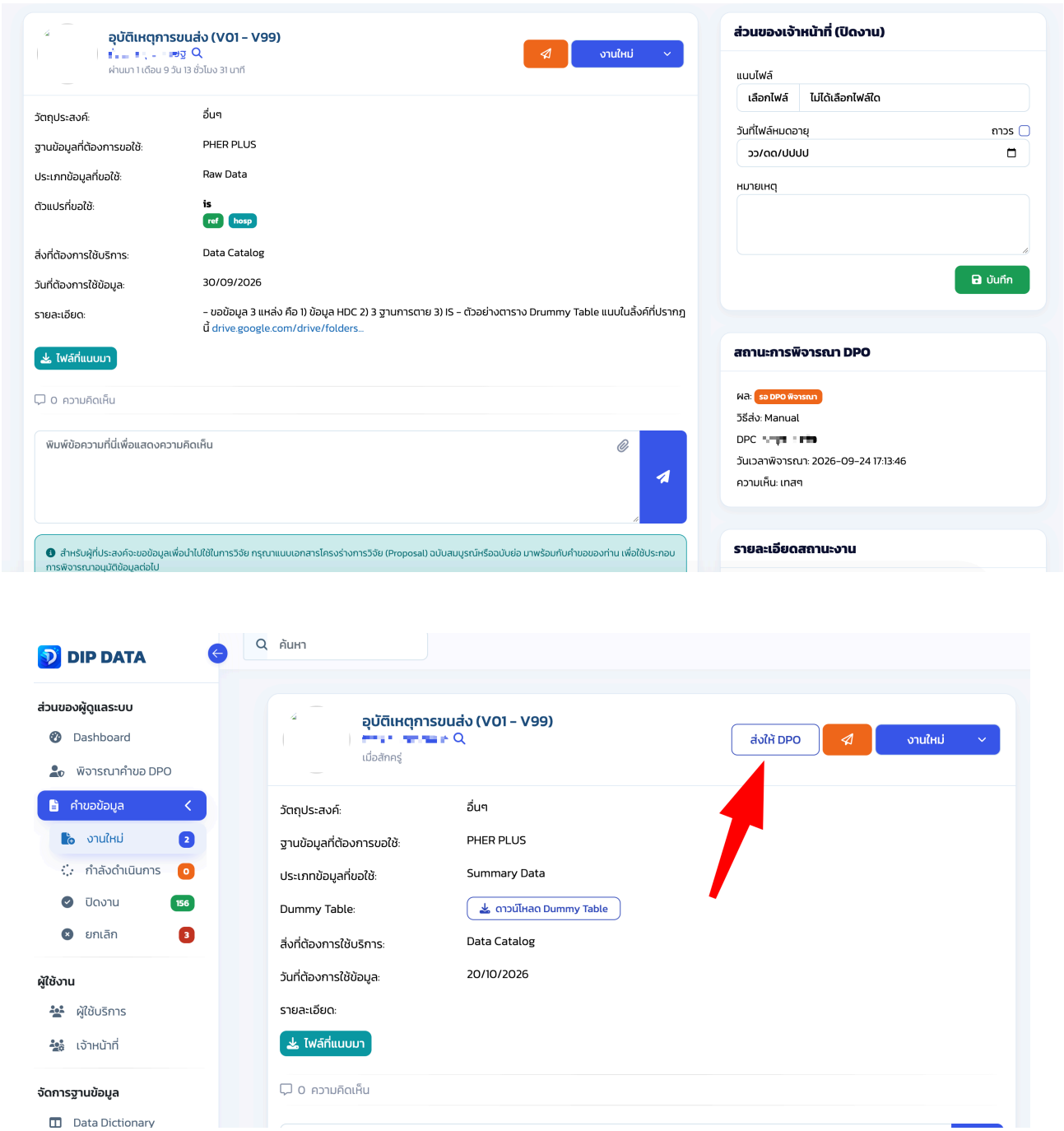
- ยกเลิกหรือหมุนเวียน Token ทันทีเมื่อสงสัยว่ารั่วไหล
- ตรวจสอบไฟล์แนบและการเข้าถึงข้อมูลก่อนปิดงาน

5 การจัดการคำขอข้อมูล

5.1 ตรวจสอบคำขอใหม่

1. เลือก คำขอข้อมูล > งานใหม่
2. ค้นหาหรือเปิดรายละเอียดคำขอที่ต้องการ
3. ตรวจสอบผู้ขอ หัวข้อ วัตถุประสงค์ ฐานข้อมูล ตัวแปรที่ร้องขอ และเอกสารประกอบ
4. พิจารณาว่าเป็นข้อมูลเปิดหรือข้อมูลนอกขอบเขต Open Data; หากเข้าเงื่อนไขให้ส่งต่อ DPO
5. สื่อสารกับผู้ขอผ่านการตอบกลับในคำขอ และปรับสถานะตามขั้นตอนงาน





ภาพประกอบ: รายการงานใหม่และปุ่มเปิดรายละเอียดคำขอ

5.2 ดำเนินการ ตอบกลับ และปิดงาน

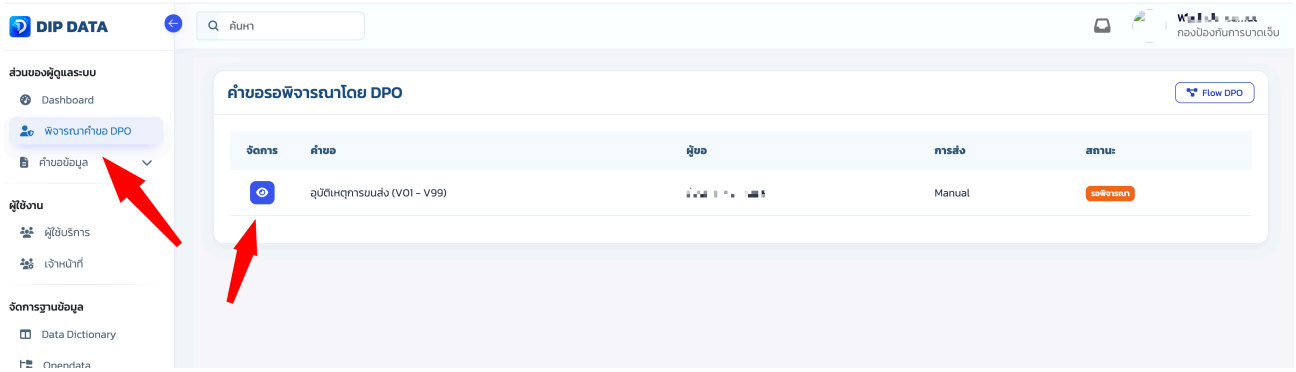
งาน	วิธีดำเนินการ
เปลี่ยนสถานะ	เปิดคำขอและเลือกการดำเนินการให้สอดคล้องกับผลพิจารณา
ตอบกลับ	พิมพ์ข้อความและแนบไฟล์ที่อนุญาต ระบบเก็บประวัติการสื่อสารไว้กับคำขอ

ส่งอีเมล	ใช้คำสั่งส่งอีเมลในหน้าคำขอเมื่อจำเป็นต้องแจ้งผู้ขอ
ปิดงาน	แนบไฟล์ผลลัพธ์ ระบุวันหมดอายุของไฟล์ (ถ้ามี) บันทึกหมายเหตุ และยืนยันปิดงาน
ยกเลิก	ใช้เมื่อคำขอไม่สามารถดำเนินการได้ โดยบันทึกเหตุผลที่ตรวจสอบได้

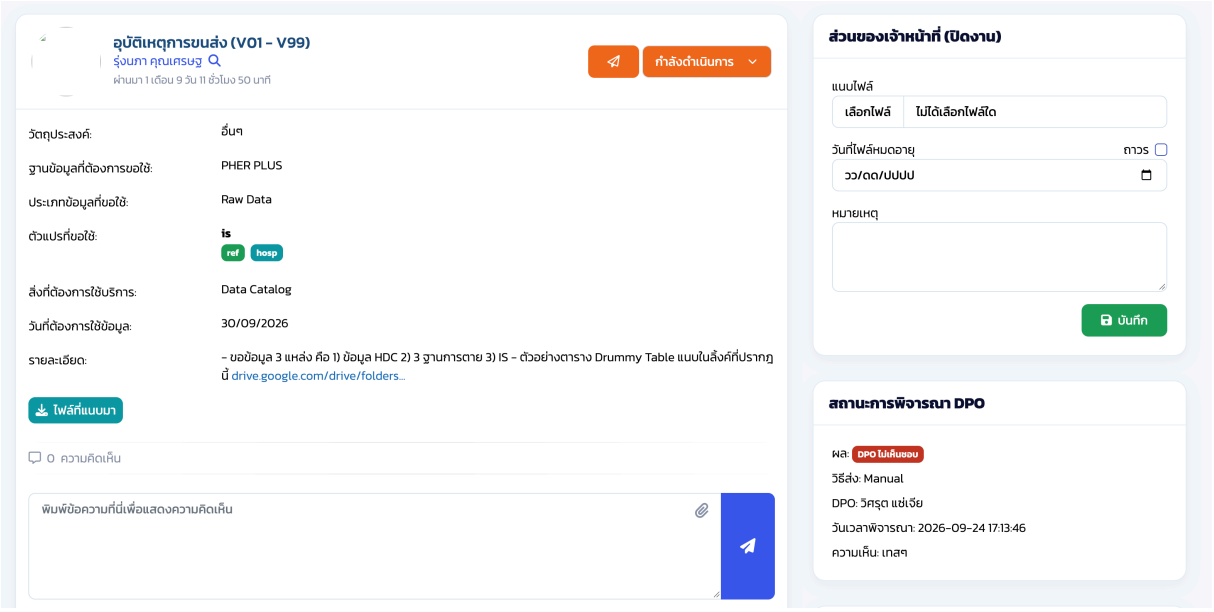
6 การพิจารณาคำขอโดย DPO

เมนู พิจารณาคำขอ DPO จะแสดงเฉพาะบัญชีเจ้าหน้าที่ที่ได้รับกำหนดบทบาท DPO เท่านั้น ใช้สำหรับตรวจสอบคำขอที่ต้องพิจารณาด้านข้อมูลส่วนบุคคลและบันทึกผลการตัดสินใจ

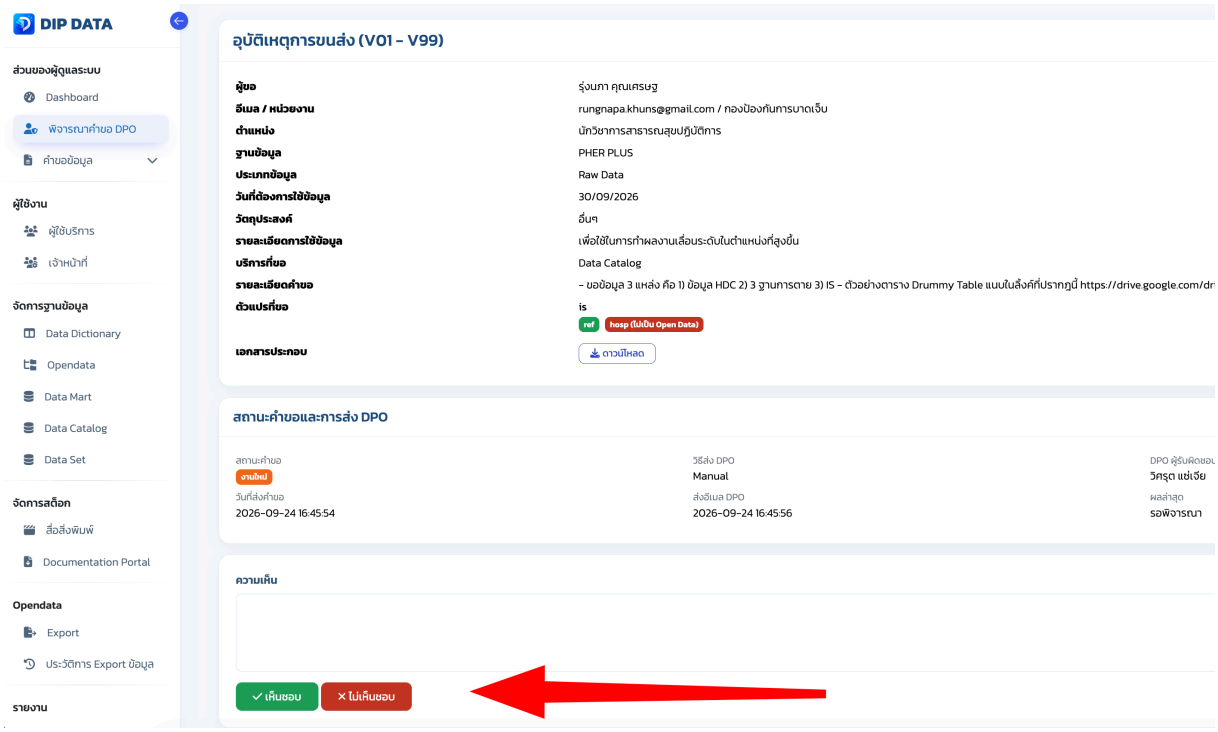
1. เปิดเมนู พิจารณาคำขอ DPO



2. เลือกคำขอและทบทวนวัตถุประสงค์ ตัวแปรที่ร้องขอ และเอกสารแนบ



3. ระบุผลพิจารณาและความเห็นตามกระบวนการของหน่วยงาน



4. ตรวจสอบประวัติการพิจารณา ก่อนส่งผลกลับสู่การดำเนินงานของเจ้าหน้าที่

7 การจัดการผู้ใช้งานและ API Token

7.1 ผู้ใช้บริการและเจ้าหน้าที่

เมนู	การใช้งาน
ผู้ใช้บริการ	เพิ่ม แก้ไข ระงับ หรือลบข้อมูลผู้ขอรับบริการ รวมถึงเข้าหน้าจัดการ API Token
เจ้าหน้าที่	เพิ่ม แก้ไข หรือลบบัญชีเจ้าหน้าที่ และกำหนดบทบาท DPO ให้เจ้าหน้าที่ที่เหมาะสม
โปรไฟล์	ผู้ใช้แต่ละรายปรับปรุงข้อมูลส่วนบุคคลของตนได้ตามสิทธิ์

7.2 การจัดการ API Token

1. เปิด ผู้ใช้บริการ และเลือก จัดการ API Token ของผู้ใช้ที่ได้รับอนุมัติ

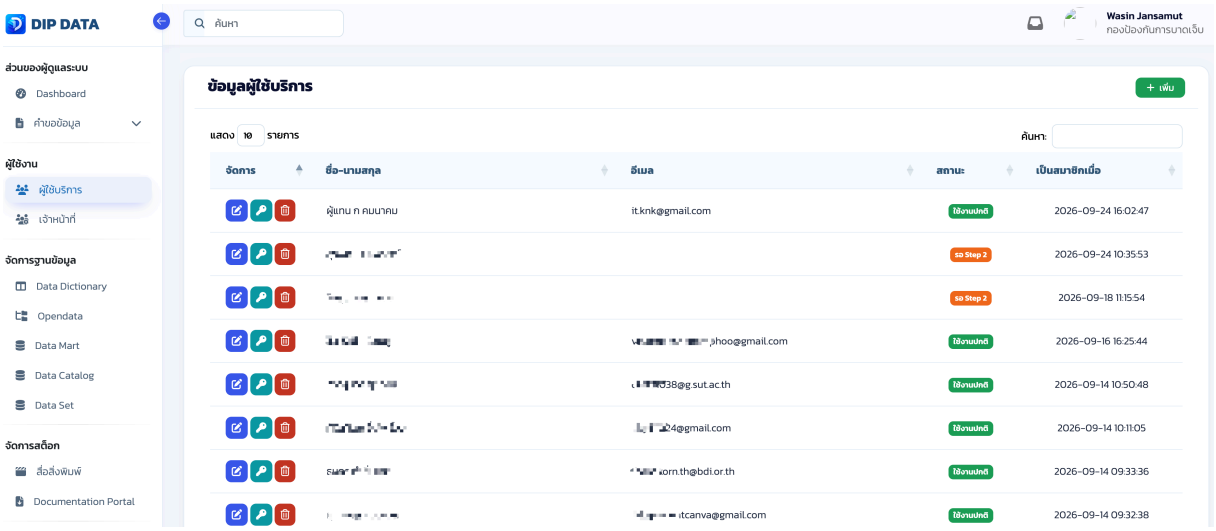
2. สร้าง Token โดยกำหนดชื่อ วันเริ่มใช้ วันหมดอายุ อัตราจำกัดการเรียก และ IP ที่อนุญาตตามนโยบาย

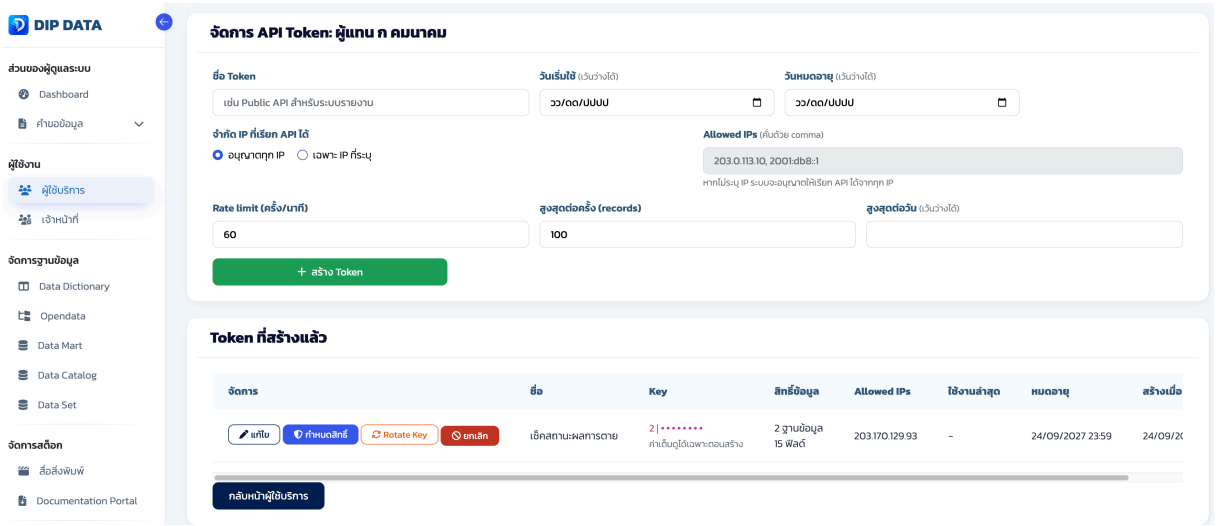
3. คัดลอก Token ในครั้งที่ระบบแสดงค่าเต็ม แล้วส่งให้ผู้รับบริการผ่านช่องทางปลอดภัย

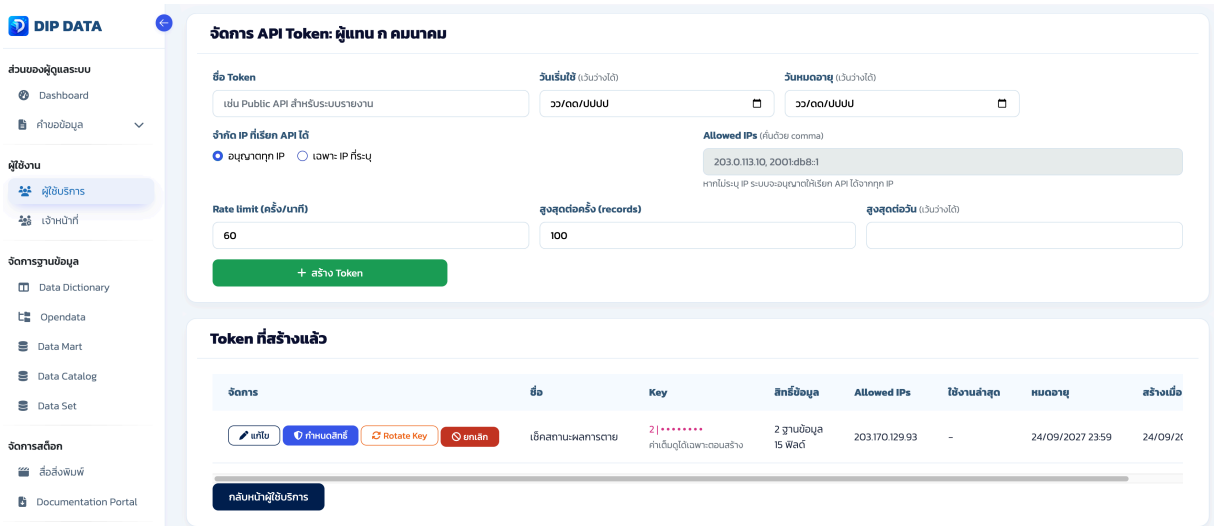
4. เลือก กำหนดสิทธิ์ เพื่อเลือกฐานข้อมูลที่ Token เข้าถึงได้

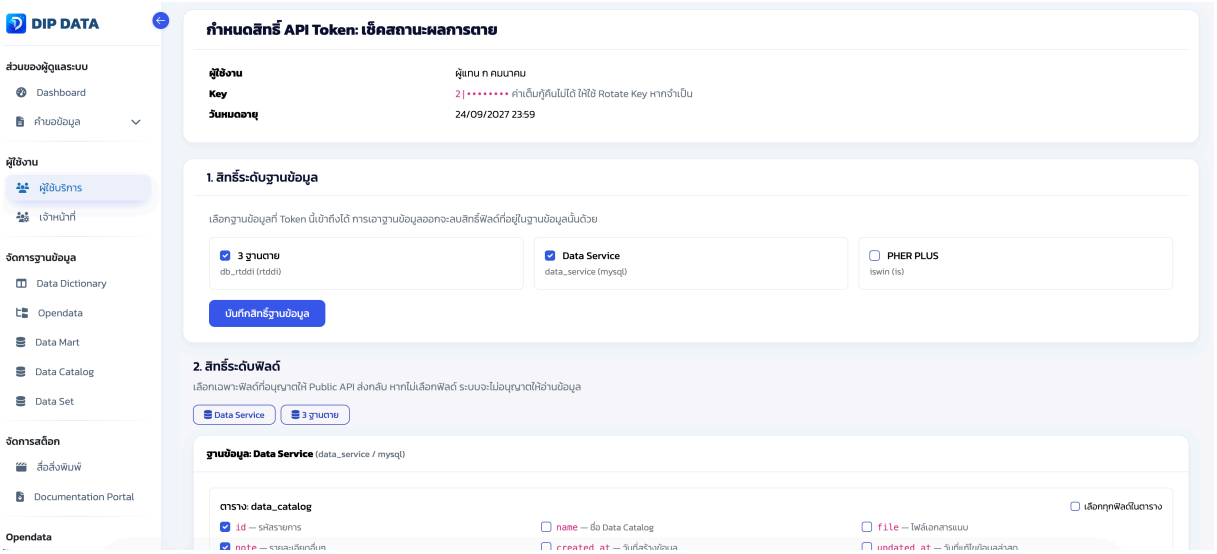
5. เลือกฟิลด์ที่อนุญาตเฉพาะภายใต้ฐานข้อมูลที่เลือก บันทึกการตั้งค่า และทดสอบตามคู่มือ API

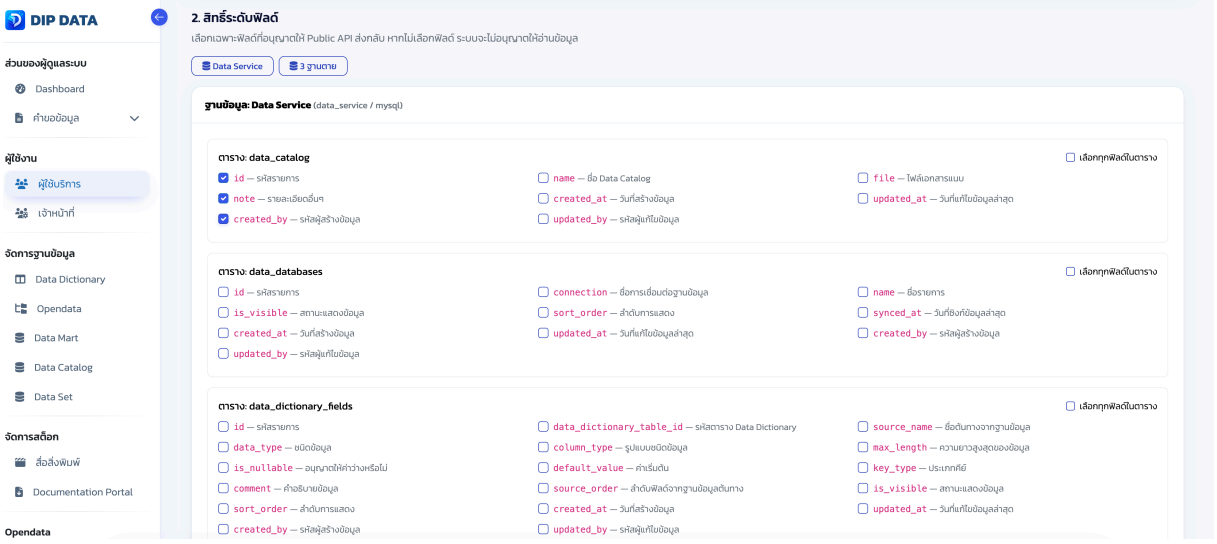
6. แก้ไข หมุนเวียน หรือยกเลิก Token เมื่อต้องเปลี่ยนสิทธิ์หรือยุติการใช้งาน







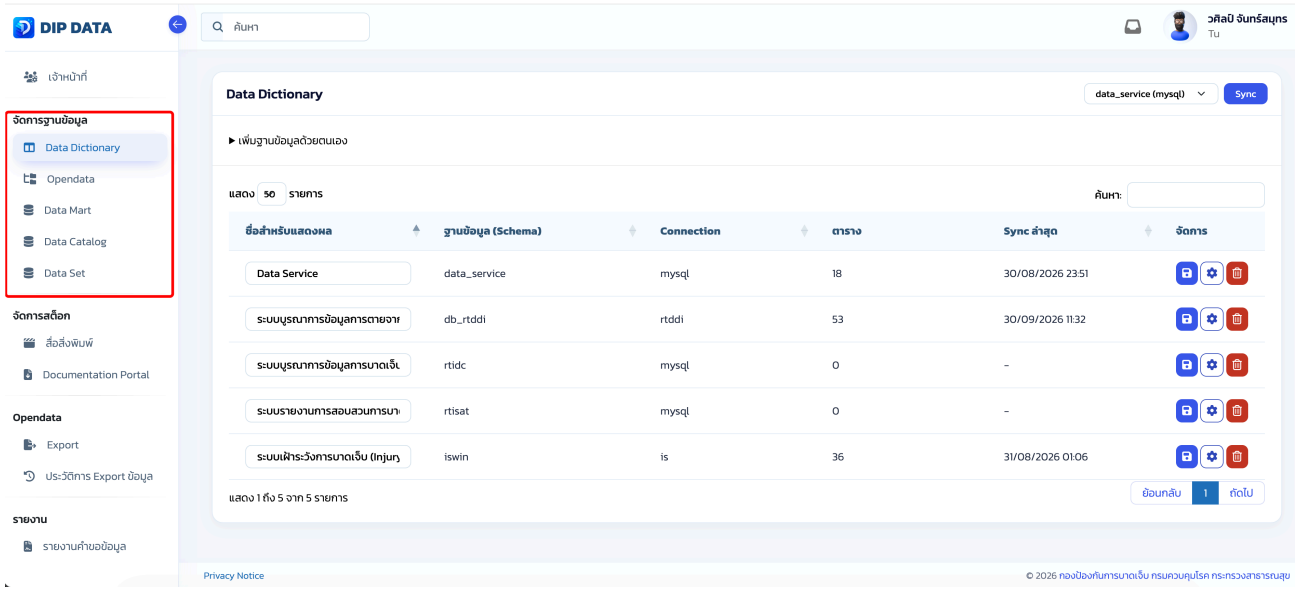




ภาพประกอบ: หน้าจอจัดการ API Token และการกำหนดสิทธิ์

8 การจัดการข้อมูลและเอกสาร

เมนู	การปฏิบัติงาน
Data Dictionary	ลงทะเบียนฐานข้อมูล ตาราง และฟิลด์; ระบุการแสดงผล Open Data การกรอง และการเรียงลำดับตามที่ระบบรองรับ
Opendata	เพิ่ม แก้ไข หรือลบชุดข้อมูลเปิด พร้อมไฟล์และ Data Dictionary ที่เกี่ยวข้อง
Data Catalog / Data Set	จัดการรายการข้อมูลและไฟล์แนบที่เผยแพร่ในระบบ
Documentation Portal	อัปโหลดเอกสาร แหล่งต้นฉบับ และภาพหน้าปก; เลือกหมวด คู่มือการใช้งาน, Data Dictionary หรือ ตัวอย่างไฟล์ข้อมูล
สื่อสิ่งพิมพ์	จัดการรายการสื่อและประวัติการปรับสต็อก



ก่อนเผยแพร่เอกสารหรือชุดข้อมูล ให้ตรวจสอบความถูกต้องของชื่อ หมวดหมู่ สิทธิ์ในการเผยแพร่ ไฟล์แนบ และความไม่มีข้อมูลส่วนบุคคลเกินความจำเป็น

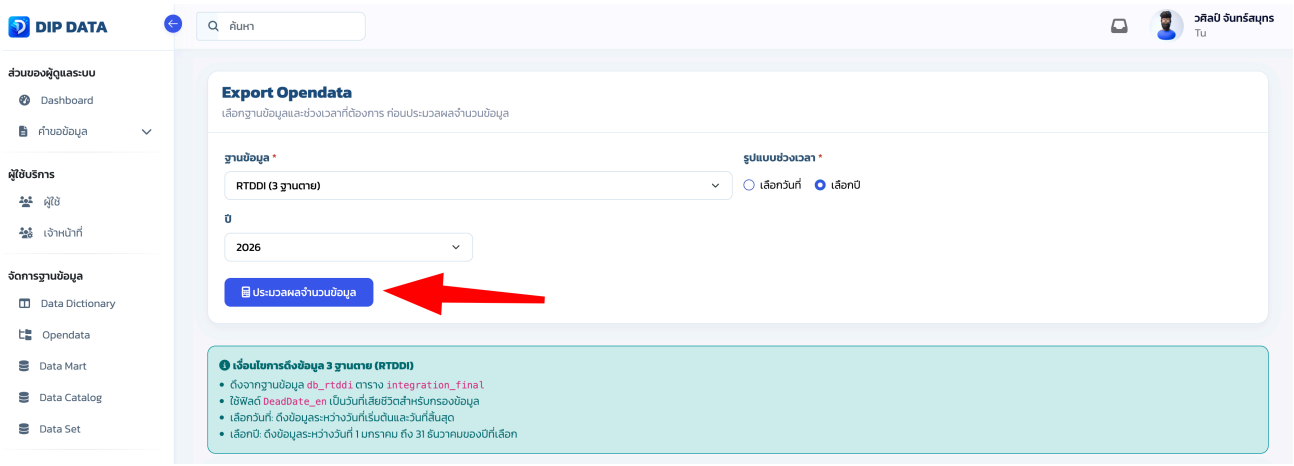
9 การส่งออกข้อมูลและรายงาน สำหรับอัพโหลดไปที่ Opendata DDC และ สพร. Data.go.th

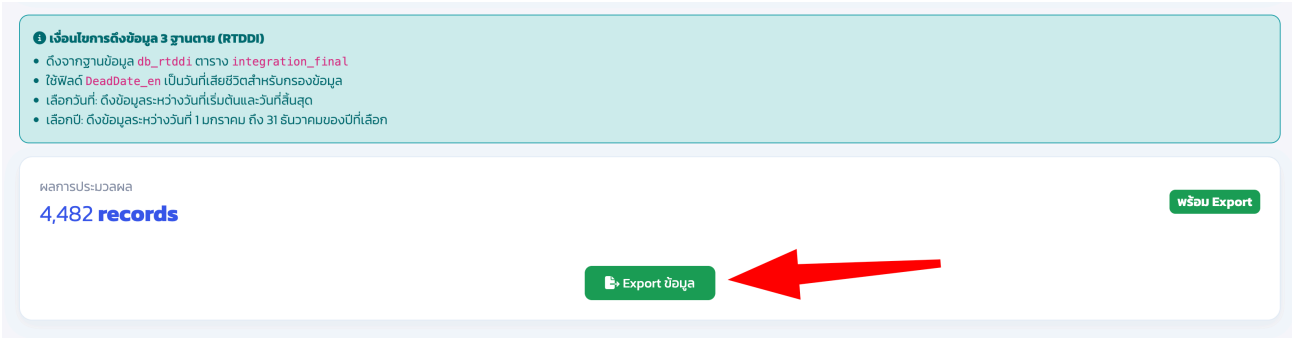
1. เลือก Opendata > Export
2. กำหนดเงื่อนไขการส่งออกตามหน้าจอ และเริ่มประมวลผล

3. ดาวน์โหลดไฟล์จากผลลัพธ์เมื่อระบบประมวลผลแล้วเสร็จ

4. ตรวจสอบเมนู ประวัติการ Export ข้อมูล เพื่อทวนสอบรายการส่งออก

5. เลือก รายงาน > รายงานคำขอข้อมูล เพื่อกรองและส่งออกรายงานตามปีงบประมาณ





ภาพประกอบ: หน้าจอส่งออกข้อมูลและประวัติการ Export

10 Database Design และ Data Dictionary

แผนผังเชิงตรรกะต่อไปนี้สรุปความสัมพันธ์ที่ตรวจจากโมเดลของระบบ ใช้เพื่อการดูแลระบบและอ้างอิงการกำหนดสิทธิ์ ไม่ใช้แทนเอกสารโครงสร้างฐานข้อมูลจริงของสภาพแวดล้อมผลิต

กลุ่มข้อมูล	ตารางหลัก	ความสัมพันธ์สำคัญ
บัญชีและสิทธิ์	users, personal_access_tokens, token_database_scopes, token_field_permissions	ผู้ใช้ 1 คนมีหลาย Token; Token กำหนดขอบเขตฐานข้อมูลและฟิลด์
พจนานุกรมข้อมูล	data_databases, data_dictionary_tables,	ฐานข้อมูล 1 รายการมีหลายตาราง; ตาราง 1 รายการมีหลายฟิลด์

	data_dictionary_fields	
คำขอข้อมูล	jobs, job_data_request_fields, jobs_reply, jobs_status	คำขอเลือกหลายฟิลด์ มีประวัติการตอบกลับ และอ้างอิงสถานะ
การพิจารณา DPO	job_dpo_reviews, job_dpo_review_logs	คำขอหนึ่งรายการมีประวัติการพิจารณาและบันทึกกิจกรรม
ข้อมูลเผยแพร่	open_data, data_catalog, data_set, documentation_files, opendata_export_logs	จัดเก็บชุดข้อมูล เอกสาร และประวัติการส่งออก

10.1 Data Dictionary ระดับระบบ

ตาราง	วัตถุประสงค์	ฟิลด์อ้างอิง
users	บัญชีผู้ใช้และบทบาท	is_admin, is_dpo, status, department
jobs	รายการคำขอข้อมูล	created_by, status, data_database_id, subject, closejob_file
data_databases	รายการฐานข้อมูลสำหรับบริการ	name, display_name, is_visible
data_dictionary_tables	ตารางข้อมูลภายในฐานข้อมูล	data_database_id, source_name, is_visible
data_dictionary_fields	ตัวแปร/ฟิลด์ข้อมูล	data_dictionary_table_id, source_name, is_open_data, is_visible
personal_access_tokens	Token สำหรับ API	expires_at, allowed_ips, active_from, rate_limit_per_minute

11 การดูแลรักษาและแก้ไขปัญหา

อาการ	แนวทางตรวจสอบเบื้องต้น
ผู้ใช้เข้าเมนูผู้ดูแลไม่ได้	ตรวจสอบสถานะบัญชีและค่า is_admin; ให้ผู้ใช้ลงชื่อเข้าใช้อีกครั้ง
DPO ไม่เห็นเมนูพิจารณา	ตรวจสอบว่าบัญชีเป็นเจ้าหน้าที่และถูกกำหนด is_dpo
API เรียกใช้ไม่ได้	ตรวจสอบ Token, ช่วงเวลาที่ใช้งาน, วันหมดอายุ, IP ที่อนุญาต, Rate Limit และสิทธิ์ฐานข้อมูล/ฟิลด์
ผู้ใช้ดาวน์โหลดไฟล์ไม่ได้	ตรวจสอบสิทธิ์เจ้าของคำขอ สถานะไฟล์ และวันหมดอายุของไฟล์ปิดงาน
ข้อมูลไม่ปรากฏในคำขอ	ตรวจสอบ is_visible ของฐานข้อมูล ตาราง และฟิลด์ใน Data Dictionary

หากพบเหตุการณ์ด้านความมั่นคงปลอดภัย ให้ระงับ Token หรือบัญชีที่เกี่ยวข้อง บันทึกรายละเอียดเหตุการณ์ และแจ้งผู้รับผิดชอบตามกระบวนการของหน่วยงานทันที