Rubric ตรวจให้คะแนน — ส่วน Backend (API) B1–B6 แบบเช็กลิสต์ย่อย

คงเนื้อหาเดิม และขยายหัวข้อ B3–B6 ให้ทดสอบแบบ “เงื่อนไขละ 1 คะแนน” เหมือน B1–B2

# ส่วนที่ 1: Backend (API) — 20 คะแนน (สรุปคะแนนเดิม)

B1=5, B2=4, B3=4, B4=2, B5=3, B6=2 (รวม 20 คะแนน)

## B1) CRUD + List Query — 5 คะแนน (5 เงื่อนไข × 1)

ทรัพยากร: Users, Topics, Indicators, Periods, Assignments, Results, Evidence

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | เงื่อนไข (1 คะแนน/ข้อ) | วิธีทดสอบ (ต้องทำจริง) | หลักฐานที่ส่ง | ผล (ผ่าน/ตก) | ให้คะแนน |
| B1-1 | สเปกพร้อมใช้งาน (ทุกหมวดมี endpoint) | เปิด Swagger UI หรือ Import Postman แล้วเรียกได้ทุกหมวดอย่างน้อย 1 endpoint/หมวด | openapi.yaml/json หรือ Postman\_Collection.json + สกรีนช็อตการเรียกสำเร็จ | □ | 0 / 1 |
| B1-2 | Search (`?q=`) ทำงานถูกต้อง | GET /api/<resource>?q=keyword บนอย่างน้อย 2 หมวด → เคสพบ/ไม่พบต้องสอดคล้อง | Request + Response 2 กรณี (พบ/ไม่พบ) | □ | 0 / 1 |
| B1-3 | Sort (`sort=field:asc/desc`) ถูกต้อง | เรียก asc และ desc บนฟิลด์เดียวกัน → ลำดับกลับด้านจริง (ตรวจ 3–5 แถวแรก) | สกรีนช็อต/Log ก่อน–หลัง พร้อมไฮไลต์ความต่าง | □ | 0 / 1 |
| B1-4 | Pagination ถูกต้อง | GET ด้วย page/pageSize (หน้าแรก/ท้าย) → จำนวนแถว + meta.total/page/pageSize ถูกต้อง | Request+Response อย่างน้อย 2–3 ชุด (หน้าแรก/กลาง/ท้าย) | □ | 0 / 1 |
| B1-5 | คิวรีรวม (q+sort+page) เสถียร (idempotent) | เรียกซ้ำด้วยพารามิเตอร์เดิม 2 รอบ → ผลต้องเหมือนกัน 100% | ผลลัพธ์ 2 รอบ (หรือ Postman Tests ที่ assert เท่ากัน) | □ | 0 / 1 |

## B2) Auth + Role + IDOR Guard — 4 คะแนน (4 เงื่อนไข × 1)

บทบาท: admin / evaluator / evaluatee (เตรียม token แยกบทบาทใน Postman Environment)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | เงื่อนไข (1 คะแนน/ข้อ) | วิธีทดสอบ (ต้องทำจริง) | หลักฐานที่ส่ง | ผล (ผ่าน/ตก) | ให้คะแนน |
| B2-1 | Authentication & 401 | POST /api/auth/login ได้ token; เรียก /api/results โดยไม่ใส่ token → 401 | Request+Response ทั้งสองกรณี (มี/ไม่มี token) | □ | 0 / 1 |
| B2-2 | Admin มองเห็นทั้งหมด (สิทธิ์ถูกต้อง) | ใช้ token admin เรียก /api/results?period\_id=… → มีหลาย evaluatee\_id | Response ตัวอย่าง แสดงหลาย evaluatee\_id | □ | 0 / 1 |
| B2-3 | Evaluator จำกัดตาม assignments (403 เมื่อเกินสิทธิ์) | เรียกผลที่อยู่ใน assignments ของตน → 200; ข้ามสิทธิ์ → 403 | 2 กรณี allowed(200)/forbidden(403) + อ้างอิง assignments | □ | 0 / 1 |
| B2-4 | Evaluatee เห็นเฉพาะของตน (403 เมื่อเกินสิทธิ์) | เรียกผลของตนเอง → 200; เข้าถึงของคนอื่น → 403 | 2 กรณี self(200)/others(403) | □ | 0 / 1 |

## B3) Validation & Evidence Rule — 4 คะแนน (4 เงื่อนไข × 1)

ตรวจทั้งฝั่งข้อมูลและกติกาไฟล์/สถานะ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | เงื่อนไข (1 คะแนน/ข้อ) | วิธีทดสอบ (ต้องทำจริง) | หลักฐานที่ส่ง | ผล (ผ่าน/ตก) | ให้คะแนน |
| B3-1 | Score Range Validation (score\_1\_4) | POST/PUT ผลด้วย score=0 หรือ 5 → ต้อง 400 พร้อมข้อความชัดเจน; score 1–4 → 200/201 | Request+Response 2 เคส (นอกช่วง=400, ในช่วง=ผ่าน) | □ | 0 / 1 |
| B3-2 | Evidence Submit Rule (yes\_no=1 → ต้องมีไฟล์ก่อน submit) | PATCH /results/:id status=submitted โดย value\_yes\_no=1 แต่ไม่มีไฟล์ใน attachments → 400 EVIDENCE\_REQUIRED; กรณีมีไฟล์ → ผ่าน | สองกรณี Before/After แนบไฟล์ + Response code | □ | 0 / 1 |
| B3-3 | 413 Payload Too Large (จำกัดขนาดไฟล์) | อัปโหลดไฟล์ > ขนาดกำหนด (เช่น >10MB) → 413 | ตัวอย่างไฟล์/สคริปต์อัปโหลด + Response 413 | □ | 0 / 1 |
| B3-4 | 415 Unsupported Media Type (ชนิดไฟล์ต้องห้าม) | อัปโหลดไฟล์ชนิดต้องห้าม (เช่น .exe) → 415 พร้อมข้อความอธิบาย | Request+Response 415 + รายการ MIME ที่ยอมรับ/ไม่ยอมรับ | □ | 0 / 1 |

## B4) Unique Assignment — 2 คะแนน (2 เงื่อนไข × 1)

ตรวจ UNIQUE(period\_id, evaluator\_id, evaluatee\_id) และจัดการข้อผิดพลาด

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | เงื่อนไข (1 คะแนน/ข้อ) | วิธีทดสอบ (ต้องทำจริง) | หลักฐานที่ส่ง | ผล (ผ่าน/ตก) | ให้คะแนน |
| B4-1 | Create Assignment สำเร็จ (กรณีไม่ซ้ำ) | POST /assignments ด้วยชุดข้อมูลใหม่ → 201 และ GET ยืนยันว่ามี 1 ระเบียน | Request+Response 201 + GET แสดงระเบียนที่สร้าง | □ | 0 / 1 |
| B4-2 | Duplicate Assignment → 409 | POST /assignments ซ้ำชุดเดิม (period\_id,evaluator\_id,evaluatee\_id) → 409 DUPLICATE\_ASSIGNMENT | Request+Response 409 พร้อม error code | □ | 0 / 1 |

## B5) Reports API (Normalized /60, Progress) — 3 คะแนน (3 เงื่อนไข × 1)

ตรวจสูตร คะแนนรวม /60 และตัวกรอง/ความเสถียร

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | เงื่อนไข (1 คะแนน/ข้อ) | วิธีทดสอบ (ต้องทำจริง) | หลักฐานที่ส่ง | ผล (ผ่าน/ตก) | ให้คะแนน |
| B5-1 | Reports: Normalized /60 ถูกสูตร | GET /reports/normalized?period\_id=…&evaluatee\_id=… → ได้ฟิลด์ A5-1..A5-4 + total และค่าตรงกับการคำนวณมือ (r=(score-1)/3, yes\_no=0/1, ชั่งน้ำหนัก indicators & topics) | Response JSON + ตารางคำนวณมือ (แนบไฟล์หรือภาพ) | □ | 0 / 1 |
| B5-2 | Reports: Progress per Department ถูกต้อง | GET /reports/progress?period\_id=… → ตรวจ submitted/total/percent ต่อแผนก ตรงกับการนับจากฐานข้อมูลจริง | Response JSON + สคริปต์/คิวรีที่นับเทียบ | □ | 0 / 1 |
| B5-3 | Filters/Idempotency เสถียร | ลองเปลี่ยนพารามิเตอร์ filter (period\_id/department\_id/evaluatee\_id) แล้วผลลดลง/ตรงเงื่อนไข; เรียกซ้ำพารามิเตอร์เดิม 2 รอบ → ผลเท่ากัน | Request+Response หลายชุด + ผลซ้ำเท่ากัน | □ | 0 / 1 |

## B6) การทดสอบแบบบูรณาการ (API) — 2 คะแนน (2 เงื่อนไข × 1)

รวม Functional + Security/Non‑functional ในการรันเดียว

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | เงื่อนไข (1 คะแนน/ข้อ) | วิธีทดสอบ (ต้องทำจริง) | หลักฐานที่ส่ง | ผล (ผ่าน/ตก) | ให้คะแนน |
| B6-1 | Functional E2E (อย่างน้อย 1 เส้นทางครบ) | Login → ดู assignments → อัปโหลด evidence → กรอกผล → submit → ตรวจผลใน reports | สรุปผลรันจาก Postman/Newman (หรือวิดีโอสั้น) แสดงทุกขั้นตอนผ่าน | □ | 0 / 1 |
| B6-2 | Security/Non‑functional ในชุด E2E | แทรก TC IDOR (403) + อัปโหลดไฟล์เกินกำหนด (413) หรือชนิดต้องห้าม (415) ในชุดเดียวกัน แล้วสรุปผลผ่าน | รายงานรวม (HTML/JSON) จาก Newman/k6/JMeter ระบุ TC ดังกล่าวผ่าน | □ | 0 / 1 |

รวมคะแนนส่วน Backend (API): 20 / 20 ลงชื่อผู้ประเมิน: \_\_\_\_\_\_\_\_\_\_\_\_\_ วันที่: \_\_\_\_\_\_\_\_\_\_\_\_\_