Rubric ตรวจให้คะแนน A5 — Backend / Frontend / DevOps

สำหรับใช้ตรวจงานตามเอกสาร A5\_อลงกรณ์ส่ง.docx (ระดับง่าย→ปานกลาง)

|  |  |  |  |
| --- | --- | --- | --- |
| ผู้ถูกประเมิน | ............................. | ผู้ประเมิน | ............................. |
| หน่วยงาน/แผนก | ............................. | รอบประเมิน / วันที่ | ............................. |

# ส่วนที่ 1: Backend (API) — 20 คะแนน

หมายเหตุ: คงเกณฑ์เดิม โดยแตก B1–B2 เป็นเช็กลิสต์ย่อย เงื่อนไขละ 1 คะแนน

## B1) ความครบถ้วนของโมดูล API (CRUD) + List Query — 5 คะแนน

ทรัพยากรที่เกี่ยวข้อง: 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

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–B6 (คงเกณฑ์เดิม) — รวม 11 คะแนน

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| รหัส | หัวข้อ | วิธีตรวจ (สรุป) | หลักฐาน | คะแนนเต็ม | ให้คะแนน |
| B3 | Validation & Evidence Rule | ส่งค่า score ในช่วง; yes\_no=1 ต้องมีไฟล์ใน attachments ก่อน submit; ตรวจ 413/415 | ชุด TC: score range, submit without evidence, upload>10MB, type not allowed | 4 |  |
| B4 | Unique Assignment (409) | POST /assignments ซ้ำชุดเดิม → 409 DUPLICATE\_ASSIGNMENT | Request+Response ซ้ำชุดเดิม | 2 |  |
| B5 | Reports API (Normalized /60, Progress) | เรียก /reports/normalized และ /reports/progress → สูตร/ผลลัพธ์ถูกต้อง | ตัวอย่าง JSON + วิธีคำนวณประกอบ | 3 |  |
| B6 | การทดสอบแบบบูรณาการ (API) | Functional/Security/Non-functional อย่างน้อย 1 ชุดต่อหมวด พร้อมสรุปผล | ตาราง TC → ผลรันจริง (ผ่าน/ตก) | 2 |  |

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

# ส่วนที่ 2: Frontend (ผู้ใช้/ผู้ประเมิน/ผู้ดูแล) — 15 คะแนน

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| รหัส | หัวข้อ | วิธีตรวจ (สรุป) | หลักฐาน | คะแนนเต็ม | ให้คะแนน |
| F1 | Role-based Navigation | เข้าสู่ระบบ 3 บทบาท → เมนู/เส้นทางแตกต่างตามสิทธิ์ | วิดีโอ/สกรีนช็อต 3 บทบาท | 3 |  |
| F2 | Form + Validation ครบ | กรอกผิด→แจ้งเตือน/บล็อก, กรอกถูก→บันทึกได้ (อย่างน้อย Users/Topics/Indicators/Assignments/Results/Evidence) | เดโมฟอร์ม 2–3 โมดูล | 4 |  |
| F3 | List/Filter/Sort/Pagination | ตารางแสดงผล ค้นหา/เรียง/แบ่งหน้าได้จริง | สกรีนช็อตก่อน–หลัง + พารามิเตอร์ | 2 |  |
| F4 | Evidence Upload UI | จำกัดขนาด/ชนิดไฟล์ แสดง error ที่เข้าใจง่าย | เดโมอัปโหลดไฟล์ใหญ่/นามสกุลต้องห้าม | 2 |  |
| F5 | Status/Badges/Filter | แสดง draft/submitted/locked + filter ตามสถานะ | สกรีนช็อต list + filter | 2 |  |
| F6 | E2E เบื้องต้น | Login→ทำงานหลัก→เห็นผลตรงสิทธิ์ (3 เส้นทาง) | ตาราง TC + วิดีโอสั้น | 2 |  |

รวมคะแนนส่วน Frontend: 15 / 15 ลงชื่อผู้ประเมิน: \_\_\_\_\_\_\_\_\_\_\_\_\_ วันที่: \_\_\_\_\_\_\_\_\_\_\_\_\_

# ส่วนที่ 3: เครื่องมือโครงสร้างพื้นฐานและปฏิบัติการ (DevOps) — 5 คะแนน

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| รหัส | หัวข้อ | วิธีตรวจ (สรุป) | หลักฐาน | คะแนนเต็ม | ให้คะแนน |
| D1 | Dockerized Stack (Compose + .env) | docker compose up -d รันผ่าน (API+DB(+phpMyAdmin)) | docker-compose.yml + .env.example + ภาพ docker ps | 2 |  |
| D2 | Health/Logs/Restart | ตรวจ /health; ตรวจ docker logs; ระบุ restart policy | curl ผลลัพธ์ + ตัวอย่างคำสั่ง/ผล logs | 1 |  |
| D3 | Reverse Proxy/Scale + mini-load test | ตั้งค่า Nginx หรือ scale API=2 + ยิงโหลดสั้น ๆ และสรุปผล | config + สรุปผลทดสอบ | 1 |  |
| D4 | Runbook & Backup | README วิธีรัน/ทดสอบ + สคริปต์ dump/restore DB | README.md + mysqldump ตัวอย่าง | 1 |  |

รวมคะแนนส่วน DevOps: 5 / 5 ลงชื่อผู้ประเมิน: \_\_\_\_\_\_\_\_\_\_\_\_\_ วันที่: \_\_\_\_\_\_\_\_\_\_\_\_\_

# สรุปคะแนนรวม (40 คะแนน)

Backend (API): \_\_\_\_ / 20  
Frontend: \_\_\_\_ / 15  
DevOps: \_\_\_\_ / 5  
  
รวม: \_\_\_\_ / 40