แบบประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

Data Protection Impact Assessment (DPIA)

ศูนย์ส่งเสริมการคุ้มครองข้อมูลส่วนบุคคล และการธรรมาภิบาลข้อมูล (PDPG) มหาวิทยาลัยเชียงใหม่

เลขที่ DPIA: ..... คำขอ API เลขที่: ..... วันที่ประเมิน: ...../...../..... ทบทวนครั้งถัดไป: ...../...../.....

ส่วน A — การคัดกรองความจำเป็นต้องทำ DPIA (Screening)

ทำเครื่องหมาย x เพื่อเลือกลักษณะของ ข้อมูล/วิธีการ ที่ใช้ประมวลผล (หากเลือกตั้งแต่ 1 ข้อ ต้องจัดทำ DPIA)

☐ ประมวลผลข้อมูลอ่อนไหว (มาตรา 26) เช่น ข้อมูลสุขภาพ ศาสนา เชื้อชาติ ประวัติอาชญากรรม ข้อมูลชีวภาพ	☐ ประมวลผลข้อมูลขนาดใหญ่ (large scale)
☐ การเฝ้าติดตามพฤติกรรมหรือทำโปรไฟล์อย่างเป็นระบบ	☐ ใช้เทคโนโลยีใหม่หรือ AI ในการประมวลผล
☐ เชื่อมโยง/ผสานชุดข้อมูลจากหลายแหล่ง (data matching)	☐ มีการโอนข้อมูลไปต่างประเทศ (มาตรา 28)
☐ ประมวลผลข้อมูลของกลุ่มเปราะบาง (เช่น ผู้เยาว์ ผู้ป่วย)	☐ เปิดเผยข้อมูลแก่บุคคลภายนอกมหาวิทยาลัยผ่าน API

นิยาม “ขนาดใหญ่” (large scale) ในบริบทมหาวิทยาลัยเชียงใหม่:

- จำนวนเจ้าของข้อมูล < 1,000 ราย และไม่ใช่ข้อมูลอ่อนไหว ไม่ต้องทำ DPIA
- จำนวนเจ้าของข้อมูล ระหว่าง 1,000–4,999 ราย หากมีปัจจัยเสี่ยงอื่นร่วม (ข้อมูลอ่อนไหว การทำโปรไฟล์ ผู้รับภายนอก การเชื่อมต่อแบบถาวร) ต้องทำ DPIA
- จำนวนเจ้าของข้อมูล ≥ 5,000 ราย ต้องทำ DPIA

ผลการคัดกรอง ☐ ต้องทำ DPIA

☐ ไม่ต้องทำ DPIA (บันทึกเหตุผล) .....

.....

.....

ขั้นตอนถัดไป

➥ หาก “ต้องทำ DPIA” ให้กรอกข้อมูลต่อส่วน B–H และส่งแบบฟอร์มเพื่อพิจารณา

➥ หาก “ไม่ต้องทำ DPIA” ให้ส่งแบบฟอร์มเพื่อพิจารณา

วันที่ทบทวนการคัดกรองครั้งถัดไป: ..... (กรอกโดยผู้ควบคุมข้อมูล หรือผู้ได้รับมอบหมาย)

ส่วน B — คำอธิบายกิจกรรมการประมวลผล

ชื่อโครงการ / ระบบ / บริการ API	
ผู้ควบคุมข้อมูล / ผู้ประมวลผล (ระบุบทบาท)	
วัตถุประสงค์ของการประมวลผล (เฉพาะเจาะจง)	

ประเภทข้อมูลส่วนบุคคล / scope ที่เข้าถึง	
มีข้อมูลอ่อนไหว (ม.26) หรือไม่ — หากมี ให้ระบุประเภทข้อมูลให้ครบ	☐ ไม่มี ☐ มี: (โปรดระบุรายละเอียดเพิ่มเติม)
กลุ่มเจ้าของข้อมูล และจำนวนโดยประมาณ	
แหล่งที่มาของข้อมูล / ระบบต้นทาง	
ผู้รับข้อมูล / ปลายทาง (recipients)	
การไหลของข้อมูล (data flow) และการจัดเก็บ	
ระยะเวลาเก็บรักษา และการลบ/ทำลาย	
โอนต่างประเทศ (ม.28) — ประเทศ/คลาวด์ (ระบุประเทศที่รับโอน)	☐ ไม่มี ☐ มี: (ระบุประเทศที่รับโอน)

ส่วน C — การทดสอบความจำเป็นและความได้สัดส่วน

ฐานทางกฎหมาย (ม.24) และฐานเฉพาะสำหรับข้อมูลอ่อนไหว (ม.26)	
การประมวลผล “จำเป็น” ต่อวัตถุประสงค์หรือไม่ มีทางเลือกที่กระทบน้อยกว่าหรือไม่	
การลดปริมาณข้อมูล (ม.22) — เข้าถึงเฉพาะเท่าที่จำเป็น	☐ ใช่ ☐ ต้องปรับ: .....
ความถูกต้องและการปรับให้เป็นปัจจุบันของข้อมูล	
ความโปร่งใส / การแจ้งเจ้าของข้อมูล (ม.23)	
กลไกรองรับสิทธิเจ้าของข้อมูล (ม.30–36)	สามารถใช้สิทธิได้ : แจ้งไว้ก่อนจะขอรับบริการ → ผู้ใช้บริการสามารถลบประวัติการสนทนาได้ด้วยตนเอง

ส่วน D — การประเมินระดับผลกระทบ (Impact Assessment)

ประเมินผลกระทบต่อเจ้าของข้อมูลในแต่ละมิติ แล้วเลือกระดับสูงสุดเป็น “ระดับผลกระทบรวม” (1 ต่ำ / 2 กลาง / 3 สูง / 4 สูงมาก)

มิติผลกระทบ	1 ต่ำ	2 กลาง	3 สูง	4 สูงมาก
การเข้าถึง/เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (Confidentiality) *(โปรดระบุ)*.....				
การเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต (Integrity) *(โปรดระบุ)*.....				
การสูญหาย/ไม่สามารถเข้าถึงข้อมูล (Availability) *(โปรดระบุ)*.....				
ผลต่อสิทธิ เสรีภาพ ชื่อเสียง การเลือกปฏิบัติ ความเสียหายต่อชีวิต และทรัพย์สิน *(โปรดระบุ)*.....				

นิยามระดับผลกระทบ: ต่ำ = ความไม่สะดวกเล็กน้อยที่แก้ไขได้ง่าย · กลาง = ความไม่สะดวกที่มีนัยสำคัญแต่ยังแก้ไขได้ · สูง = ผลกระทบรุนแรงที่แก้ไขได้ด้วยความยากลำบาก · สูงมาก = ผลกระทบรุนแรงหรือไม่อาจแก้ไขกลับคืนได้

➥ **ระดับผลกระทบ (Impact) ใช้ระดับที่สูงที่สุดจาก 4 มิติ:** ☐ ต่ำ ☐ กลาง ☐ สูง ☐ สูงมาก

ส่วน E — การประเมินโอกาสเกิดจากภัยคุกคาม (Likelihood Assessment)

ให้คะแนนปัจจัยเสี่ยง (0 = ไม่ใช่/ควบคุมดีมาก, 1 = บางส่วน, 2 = ใช่/ควบคุมอ่อน) แล้วรวมคะแนนเพื่อกำหนดระดับโอกาสเกิด

ปัจจัยภัยคุกคาม	0	1	2
1. เครือข่ายและทรัพยากรทางเทคนิค — ระบบเชื่อมต่ออินเทอร์เน็ตสาธารณะ ไม่มีการเข้ารหัส/แบ่งแยกเครือข่าย *(โปรดระบุ)*.....			
2. กระบวนการและขั้นตอน — ไม่มีการจำกัดสิทธิ ไม่มี log ไม่มีนโยบายรักษาความปลอดภัยที่ชัดเจน *(โปรดระบุ)*.....			
3. บุคคลและคู่สัญญาที่เกี่ยวข้อง — ผู้พัฒนา/บุคคลภายนอกจำนวนมาก ขาดการอบรม ไม่มี DPA			

ปัจจัยภัยคุกคาม	0	1	2
(โปรดระบุ).....			
4. ขนาดการประมวลผล และขอบเขตข้อมูล — ปริมาณข้อมูลสูง ครอบคลุมข้อมูลหลายส่วนงาน *(โปรดระบุ)*.....			

รวมคะแนน: ..... เกณฑ์: 0–2 = ต่ำ · 3–4 = กลาง · 5–6 = สูง · 7–8 = สูงมาก

➥ **ระดับโอกาสเกิด (Likelihood):** ☐ ต่ำ ☐ กลาง ☐ สูง ☐ สูงมาก

ส่วน E — การประเมินระดับความเสี่ยง (Risk Level)

คะแนนความเสี่ยง = ระดับผลกระทบ (1–4) × ระดับโอกาสเกิด (1–4) = ช่วง 1–16 เกณฑ์ระดับ: 1–2 ต่ำ · 3–4 กลาง · 6–9 สูง · 12–16 สูงมาก

โอกาสเกิด ↓ / ผลกระทบ ⟶	ต่ำ (1)	กลาง (2)	สูง (3)	สูงมาก (4)
สูงมาก (4)	กลาง 4	สูง 8	สูงมาก 12	สูงมาก 16
สูง (3)	กลาง 3	สูง 6	สูง 9	สูงมาก 12
กลาง (2)	ต่ำ 2	กลาง 4	สูง 6	สูง 8
ต่ำ (1)	ต่ำ 1	ต่ำ 2	กลาง 3	กลาง 4

➥ **คะแนนความเสี่ยงเริ่มต้น (Inherent risk score):** ..... / 16

➥ **ระดับความเสี่ยงเริ่มต้น:** ☐ ต่ำ ☐ กลาง ☐ สูง ☐ สูงมาก

ส่วน G — มาตรการลดความเสี่ยง (Risk Treatment)

ความเสี่ยงที่ระบุ	มาตรการทางเทคนิค / องค์กร	ผู้รับผิดชอบ	ความเสี่ยงคงเหลือ

ตัวอย่างมาตรการ: เข้ารหัส TLS/at-rest · จำกัด scope ตามหลัก least-privilege · หมุนเวียน Security Keys · บันทึกและตรวจสอบ log · จัดทำ DPA กับผู้รับข้อมูล · กำหนดเพดานปริมาณ request · ลบข้อมูลตามกำหนด · ปกปิด/นิรนาม (masking/pseudonymisation)

ส่วน H — ความเสี่ยงคงเหลือและการรับรอง (Residual Risk & Sign-off)

วิธีคำนวณความเสี่ยงคงเหลือ: ประเมินระดับโอกาสเกิด (Likelihood) ใหม่หลังใช้มาตรการในส่วน G แล้วคูณกับระดับผลกระทบเดิม — เว้นแต่มาตรการลดความรุนแรงของผลกระทบได้โดยตรง จึงปรับระดับผลกระทบด้วย

คะแนนความเสี่ยงคงเหลือหลังมาตรการ: ..... / 16 ☐ ต่ำ ☐ กลาง ☐ สูง ☐ สูงมาก

หมายเหตุสำคัญ: หากความเสี่ยงคงเหลืออยู่ในระดับสูง/สูงมาก และไม่อาจลดลงได้ ผู้ควบคุมข้อมูลควรทบทวนการดำเนินกิจกรรมและพิจารณาหารือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส./PDPC) ก่อนเริ่มประมวลผล

จัดทำโดย (เจ้าของกิจกรรม)	**ความเห็นเจ้าหน้าที่คุ้มครองข้อมูล (DPO)**
ลงชื่อ ..... (.....) ตำแหน่ง ..... วันที่	☐ รับทราบผลคัดกรอง: ไม่ต้องทำ DPIA (กรณีหยุดที่ส่วน A) ☐ เห็นชอบ ☐ เห็นชอบโดยมีเงื่อนไข ☐ ไม่เห็นชอบ ☐ ต้องหารือ สคส. ลงชื่อ ..... วันที่ ..... ทบทวนถัดไป .....