

## เอกสารแนบท้าย ๒

## แบบฟอร์มเปิดเผยข้อมูลผู้ให้บริการคลาวด์ (Cloud Service Provider Disclosure Form)

## สำหรับโครงการจ้างบริการระบบ Cloud Service สำนักสุขภาพดิจิทัล

(ผู้ยื่นข้อเสนอต้องกรอกข้อมูลให้ครบถ้วนตามความเป็นจริง พร้อมแนบหลักฐานประกอบ)

## ส่วนที่ ๑ ข้อมูลผู้ให้บริการ (Provider Information)

หัวข้อ	รายละเอียด
ชื่อบริษัท	.....
ที่อยู่สำนักงานใหญ่	.....
เว็บไซต์	.....
ชื่อผู้ติดต่อ	.....
อีเมล/เบอร์โทรศัพท์	.....
ประเภทผู้ให้บริการ	<input type="checkbox"/> ผู้ให้บริการเจ้าของระบบ (Cloud Service Provider) <input type="checkbox"/> ผู้แทนจำหน่าย (Reseller/Broker)

## ส่วนที่ ๒ รายละเอียดบริการคลาวด์ (Cloud Service Background)

หัวข้อ	รายละเอียด (โปรดเลือกและระบุข้อมูล)
รูปแบบบริการ	<input type="checkbox"/> IaaS (Infrastructure as a Service) <input type="checkbox"/> PaaS (Platform as a Service) <input type="checkbox"/> SaaS (Software as a Service)
รูปแบบการใช้งาน	<input type="checkbox"/> Private Cloud (ส่วนตัว) <input type="checkbox"/> Public Cloud (สาธารณะ) <input type="checkbox"/> Hybrid Cloud (ผสม) <input type="checkbox"/> Community Cloud (กลุ่มองค์กรภาครัฐ)
ที่ตั้งศูนย์ข้อมูล	Site หลัก: จังหวัด..... ประเทศ..... Site สำรอง (DR): จังหวัด..... ประเทศ..... (หมายเหตุ: TOR กำหนดให้ต้องตั้งอยู่ในประเทศไทย)

## ส่วนที่ ๓ การปฏิบัติตามกฎหมายและมาตรฐาน (Legal &amp; Compliance)

มาตรฐาน/ กฎหมาย	สถานะการรับรอง (แนบใบรับรอง)	หมายเลขใบรับรอง /วันหมดอายุ
ISO/IEC 27001 (ISMS)	<input type="checkbox"/> มี <input type="checkbox"/> ไม่มี	.....
ISO/IEC 27017 (Cloud Security)	<input type="checkbox"/> มี <input type="checkbox"/> ไม่มี	.....
ISO/IEC 27018 (Cloud Privacy)	<input type="checkbox"/> มี <input type="checkbox"/> ไม่มี	.....
ISO/IEC 27799 (Health Info)	<input type="checkbox"/> มี <input type="checkbox"/> ไม่มี	.....
CSA STAR	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2	.....
PDPA Compliance	<input type="checkbox"/> มีนโยบายรองรับ PDPA ครบถ้วน <input type="checkbox"/> มี DPO (Data Protection Officer)	(แนบนโยบายความเป็นส่วนตัว)

#### ส่วนที่ ๔ การควบคุมข้อมูล (Data Control)

หัวข้อ	รายละเอียดการเปิดเผยข้อมูล
ความเป็นเจ้าของข้อมูล (Data Ownership)	ผู้ให้บริการยืนยันว่าข้อมูลทั้งหมดเป็นกรรมสิทธิ์ของ [ ] ลูกค้า (กระทรวงสาธารณสุข) แต่เพียงผู้เดียว [ ] อื่น ๆ (โปรดระบุ).....
อำนาจอธิปไตยของข้อมูล (Data Sovereignty)	ข้อมูลจะถูกจัดเก็บและประมวลผลภายในราชอาณาจักรไทยเท่านั้นหรือไม่ ? [ ] ใช่ (Local Only) [ ] ไม่ใช่ (มีการส่งออกไปต่างประเทศ โปรดระบุประเทศปลายทาง).....
การเข้าถึงข้อมูลโดยบุคคลที่ ๓	มีผู้รับจ้างช่วง (Sub-processors) ที่สามารถเข้าถึงข้อมูลได้หรือไม่ ? [ ] ไม่มี [ ] มี (โปรดระบุรายชื่อและขอบเขตงาน) .....
การลบ/ทำลายข้อมูล (Data Deletion)	วิธีการทำลายข้อมูลเมื่อเลิกสัญญา [ ] Crypto-shredding (ลบกุญแจเข้ารหัส) [ ] Overwriting (เขียนทับตามมาตรฐาน NIST 800-88) [ ] Physical Destruction (ทำลายสื่อบันทึก)

#### ส่วนที่ ๕ ประสิทธิภาพและความต่อเนื่อง (Performance & Resiliency)

หัวข้อ	รายละเอียด
SLA (Service Level Agreement)	การันตี Uptime ที่ระดับ: .....% (เช่น ๙๙.๙๕%) บทลงโทษหากผิด SLA: .....
ความยืดหยุ่น (Elasticity)	รองรับการขยายทรัพยากร (Auto-scaling) ได้สูงสุดกี่เท่าของปกติ: .....
แผนกู้คืนระบบ (DR Plan)	ระยะเวลา RPO (ข้อมูลหายได้สูงสุด): ..... (TOR: ≤ ๒๔ ชม.) ระยะเวลา RTO (กู้คืนเสร็จ): ..... (TOR: ≤ ๑๒ ชม.)
การทดสอบ DR	มีการซ้อมแผนกู้คืนระบบอย่างน้อยปีละ: ..... ครั้ง

#### ส่วนที่ ๖ การสนับสนุนและบริหารจัดการ (Service Support)

หัวข้อ	รายละเอียด
ช่องทางการแจ้งเหตุ (Incident Reporting)	[ ] โทรศัพท์ [ ] Email [ ] Web Portal [ ] Chatbot
ระยะเวลาตอบสนอง (Response Time)	กรณีวิกฤต (Critical Impact): ภายใน ..... นาที (TOR: 15 นาที)
การแจ้งเตือนบำรุงรักษา (Maintenance)	แจ้งล่วงหน้าอย่างน้อย: ..... วัน
การจัดการการเปลี่ยนแปลง (Change Management)	มีกระบวนการแจ้งเตือนเมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานหรือไม่? [ ] มี [ ] ไม่มี

ส่วนที่ ๗ การกำหนดค่าความปลอดภัย (Security Configuration)

หัวข้อ	มาตรการที่ให้บริการ (โปรดติ๊กเลือก)
Network Security	<input type="checkbox"/> DDoS Protection (ระบุขนาด Gbps: .....) <input type="checkbox"/> Firewall / WAF <input type="checkbox"/> Private Link / VPN
Identity & Access	<input type="checkbox"/> MFA (Multi-Factor Authentication) <input type="checkbox"/> Role-based Access Control (RBAC) <input type="checkbox"/> SSO Integration
Encryption	<input type="checkbox"/> Encryption at Rest (AES-256) <input type="checkbox"/> Encryption in Transit (TLS 1.2+) <input type="checkbox"/> Key Management Service (BYOK Support)
Log & Monitoring	<input type="checkbox"/> เก็บบันทึก Log อย่างน้อย ๙๐ วัน <input type="checkbox"/> ส่งออก Log ไปยัง SIEM ภายนอกได้ <input type="checkbox"/> Real-time Alerting

ส่วนที่ ๘ สิทธิในการตรวจสอบ (Right to Audit)

หัวข้อ	รายละเอียด
สิทธิของลูกค้า	ยินยอมให้กระทรวงสาธารณสุขหรือตัวแทนเข้าตรวจสอบ (Audit) ศูนย์ข้อมูลหรือไม่ ? <input type="checkbox"/> ยินยอม <input type="checkbox"/> ไม่ยินยอม (ให้ดูรายงาน SOC 2 แทน)
สิทธิของ หน่วยงานกำกับ	ยินยอมให้ สกมช. หรือ สคส. เข้าตรวจสอบตามกฎหมายหรือไม่ ? <input type="checkbox"/> ยินยอม <input type="checkbox"/> ไม่ยินยอม

(ลงชื่อ).....

(ผู้มีอำนาจลงนามของบริษัทผู้ยื่นข้อเสนอ)

ประทับตราบริษัท (ถ้ามี)

วันที่ .....