แบบฟอร์มประเมินคู่สัญญา (Vendor Due Diligence Checklist)

ชื่อเอกสาร: แบบประเมินมาตรฐานความปลอดภัยและการคุ้มครองข้อมูลของผู้ให้บริการภายนอก

หน่วยงานที่ถูกประเมิน (Vendor): .....

ระบบงานที่รับผิดชอบ: .....

ลำดับ	รายการตรวจสอบมาตรฐานความปลอดภัย	มี (Yes)	ไม่มี (No)	หมายเหตุ เอกสารแนบ
1.	ด้านนโยบายและมาตรฐาน (Policies & Standards)			
1.1	มี Privacy Policy สอดคล้อง PDPA			
1.2	ได้รับรองมาตรฐาน ISO/IEC 27001 หรือเทียบเท่า			
2.	ด้านการคุ้มครองข้อมูลและการเข้าถึง			
2.1	มีการเข้ารหัสข้อมูล			
2.2	มี Access Control และ Log File			
2.3	มี NDA สำหรับพนักงาน			
3.	ด้าน Incident Response			
3.1	มี IT DRP และ Backup			
3.2	แจ้งเหตุภายใน 24 ชม.			
4.	ด้านการสิ้นสุดสัญญา			
4.1	ส่งมอบข้อมูลครบถ้วน			
4.2	ทำลายข้อมูลถาวร			

สรุปผลการประเมิน:

[ ] ผ่านเกณฑ์ (สามารถดำเนินการจัดซื้อจัดจ้างได้)

[ ] ไม่ผ่านเกณฑ์ (ต้องปรับปรุงมาตรการก่อนทำสัญญา)

ผู้ประเมิน: ..... (เจ้าหน้ากลุ่มงานเทคโนโลยีสารสนเทศ)

เอกสารแนบท้ายสัญญาจ้าง

เรื่อง ข้อกำหนดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความลับ

(Data Protection and Confidentiality Clause)

แนบท้ายสัญญาจ้างเลขที่ .....

เอกสารแนบท้ายสัญญาฉบับนี้ เป็นส่วนหนึ่งของสัญญาจ้างระหว่าง โรงพยาบาลปากช่องนานา (ในฐานะ "ผู้ว่าจ้าง" หรือ "ผู้ควบคุมข้อมูลส่วนบุคคล") กับ ..... (ในฐานะ "ผู้รับจ้าง" หรือ "ผู้ประมวลผลข้อมูลส่วนบุคคล") โดยคู่สัญญาทั้งสองฝ่ายตกลงให้มีข้อกำหนดเพิ่มเติม ดังต่อไปนี้:

ข้อ 1. สถานะและหน้าที่ของผู้รับจ้าง

ผู้รับจ้างตกลงปฏิบัติหน้าที่ในฐานะ "ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)" ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยจะประมวลผล จัดเก็บ หรือเข้าถึงข้อมูลผู้ป่วยและข้อมูลทางราชการของโรงพยาบาลปากช่องนานา ตามคำสั่งที่เป็นลายลักษณ์อักษรของโรงพยาบาลเท่านั้น ห้ามมิให้นำข้อมูลไปใช้เพื่อวัตถุประสงค์อื่นโดยเด็ดขาด

ข้อ 2. มาตรการรักษาความมั่นคงปลอดภัย

ผู้รับจ้างต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสมตามมาตรฐานสากล เพื่อป้องกันการสูญหาย เข้าถึง ใช้ ดัดแปลง แก้ไข หรือเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ

ข้อ 3. การแจ้งเหตุละเมิดข้อมูล (Data Breach Notification)

ในกรณีที่ผู้รับจ้างทราบหรือมีเหตุอันควรสงสัยว่ามีการละเมิด ปลอมแปลง หรือข้อมูลรั่วไหล ผู้รับจ้างต้องแจ้งให้โรงพยาบาลทราบเป็นลายลักษณ์อักษร ภายใน 24 ชั่วโมง นับแต่ทราบเหตุ พร้อมทั้งดำเนินการแก้ไขเพื่อระงับความเสียหายทันที โดยผู้รับจ้างจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการละเมิดข้อมูลดังกล่าวทุกประการ

ข้อ 4. การจัดการข้อมูลเมื่อสิ้นสุดสัญญา

เมื่อสิ้นสุดสัญญาจ้าง ผู้รับจ้างต้องดำเนินการส่งมอบข้อมูลทั้งหมดคืนแก่โรงพยาบาลในรูปแบบที่สามารถนำไปใช้งานต่อได้ และต้องทำการทำลายหรือลบข้อมูล (Data Wipe) ออกจากอุปกรณ์ เครือข่าย หรือระบบคลาวด์ของผู้รับจ้างอย่างถาวร ภายใน 15 วัน พร้อมจัดทำหนังสือรับรองการทำลายข้อมูลส่งมอบให้แก่โรงพยาบาล

(ลงชื่อ)..... ผู้ว่าจ้าง (ผู้ควบคุมข้อมูลส่วนบุคคล)

(.....)

ตำแหน่ง ผู้อำนวยการโรงพยาบาลปากช่องนานา

วันที่: ...../...../.....

(ลงชื่อ)..... ผู้รับจ้าง (ผู้ประมวลผลข้อมูลส่วนบุคคล)

(.....)

ตำแหน่ง .....