ประกาศโรงพยาบาลปราสาท

เรื่อง นโยบายความมั่นคงปลอดภัยสำหรับผู้ให้บริการภายนอก (Vendor/Supplier Security Policy)

โรงพยาบาลปราสาท ในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ตระหนักถึงความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล ที่อาจเกิดขึ้นจากการใช้บริการของบุคคลหรือนิติบุคคลภายนอก ไม่ว่าจะเป็นผู้จัดจำหน่ายซอฟต์แวร์ ผู้ให้บริการระบบเครือข่าย ผู้ให้บริการคลาวด์ ผู้รับจ้างบำรุงรักษาอุปกรณ์ หรือผู้ให้บริการ Outsource อื่นใด ซึ่งการเชื่อมต่อหรือการเข้าถึงระบบสารสนเทศโดยบุคคลภายนอกถือเป็นจุดเสี่ยง (Attack Surface) ที่สำคัญที่สุดประการหนึ่งขององค์กร

ดังนั้น เพื่อให้การบริหารจัดการความเสี่ยงจากห่วงโซ่อุปทาน (Supply Chain Risk Management) เป็นไปอย่างเป็นระบบ สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) มาตรฐาน ISO/IEC ๒๗๐๐๑ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) จึงกำหนดนโยบายฉบับนี้ขึ้นเพื่อใช้เป็นแนวทางปฏิบัติของโรงพยาบาลปราสาท

๑. วัตถุประสงค์

๑.๑ เพื่อควบคุมและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดจากการจัดซื้อจัดจ้างการใช้บริการ และการเชื่อมต่อระบบสารสนเทศกับบุคคลหรือนิติบุคคลภายนอก (Vendors/Suppliers /Outsource)

๑.๒ เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลของผู้รับบริการ บุคลากร และผู้มีส่วนได้ส่วนเสียจะได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) ตลอดวงจรชีวิตของสัญญา

๑.๓ เพื่อกำหนดกรอบการประเมิน คัดเลือก กำกับดูแล และสิ้นสุดความสัมพันธ์กับผู้ให้บริการภายนอกอย่างเป็นระบบ สอดคล้องกับมาตรฐานสากล ISO/IEC ๒๗๐๐๑

๑.๔ เพื่อสร้างความต่อเนื่องในการให้บริการทางการแพทย์ โดยป้องกันมิให้เหตุละเมิดความปลอดภัยจากผู้ให้บริการภายนอกส่งผลกระทบต่อระบบสุขภาพของประชาชน

๑.๕ เพื่อปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) และมาตรฐาน HAIT Plus ด้านความมั่นคงปลอดภัยสารสนเทศ

๒. ขอบเขต

นโยบายฉบับนี้มีผลบังคับใช้กับบุคคลหรือนิติบุคคลภายนอกทุกรายที่มีความสัมพันธ์ทางสัญญาหรือข้อตกลงกับโรงพยาบาลปราสาท ในลักษณะใดลักษณะหนึ่ง ดังต่อไปนี้

๒.๑ ผู้จัดจำหน่ายและผู้ให้บริการด้านเทคโนโลยีสารสนเทศ ได้แก่ ผู้จำหน่ายซอฟต์แวร์ ฮาร์ดแวร์ ระบบเครือข่าย อุปกรณ์การแพทย์ที่เชื่อมต่อระบบสารสนเทศ และผู้ให้บริการคลาวด์ (Cloud Service Provider)

๒.๒ ผู้รับจ้างบำรุงรักษาและซ่อมแซม ได้แก่ ผู้รับจ้างดูแลระบบเซิร์ฟเวอร์ ระบบเครือข่าย ระบบไฟฟ้า ระบบปรับอากาศห้องเซิร์ฟเวอร์ อุปกรณ์ทางการแพทย์ และระบบ CCTV

๒.๓ ผู้ให้บริการ Outsource ได้แก่ บริษัทรับจ้างประมวลผลข้อมูล ผู้ให้บริการ Data Center

ผู้ให้บริการเชื่อมต่อระบบ (System Integrator) ผู้ให้บริการ Managed Security Service Provider (MSSP) และผู้ให้บริการ SaaS/PaaS/IaaS

๒.๔ ที่ปรึกษาและผู้เชี่ยวชาญภายนอก ได้แก่ ที่ปรึกษาด้าน IT ผู้ตรวจประเมิน (Auditor) นักวิจัย และบุคลากรชั่วคราวที่จำเป็นต้องเข้าถึงระบบสารสนเทศ

๒.๕ คู่สัญญาอื่นที่เกี่ยวข้อง ได้แก่ หน่วยงานภาครัฐหรือเอกชนที่มีการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์กับโรงพยาบาล เช่น สำนักงานหลักประกันสุขภาพแห่งชาติ (สปสช.) สำนักงานประกันสังคม บริษัทประกันภัย

๓. นิยามศัพท์

"ผู้ให้บริการภายนอก (Vendor/Supplier)" หมายถึง บุคคลหรือนิติบุคคลภายนอกที่ทำสัญญาหรือข้อตกลงให้บริการแก่โรงพยาบาล ไม่ว่าจะเป็นการจัดหาสินค้า ซอฟต์แวร์ หรือบริการ

"ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)" หมายถึง ผู้ให้บริการภายนอกที่ดำเนินการประมวลผลข้อมูลส่วนบุคคลในนามของโรงพยาบาล (ผู้ควบคุมข้อมูลส่วนบุคคล)

"ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data)" หมายถึง ข้อมูลสุขภาพ ข้อมูลชีวมิติ ข้อมูลเชื้อชาติ ข้อมูลความพิการ และข้อมูลอื่นตามมาตรา ๒๖ แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

"ระดับความเสี่ยงของผู้ให้บริการ (Vendor Risk Tier)" หมายถึง การจัดระดับความเสี่ยงของผู้ให้บริการภายนอกตามระดับการเข้าถึงข้อมูลและระบบของโรงพยาบาล แบ่งเป็นระดับสูง กลาง และต่ำ

"การเข้าถึงระยะไกล (Remote Access)" หมายถึง การเชื่อมต่อเข้าสู่ระบบสารสนเทศของโรงพยาบาลจากภายนอกเครือข่ายผ่านช่องทางอิเล็กทรอนิกส์

"IoMT (Internet of Medical Things)" หมายถึง อุปกรณ์ทางการแพทย์ที่เชื่อมต่อกับระบบเครือข่ายและสามารถส่งหรือรับข้อมูลได้

๔. การจัดระดับความเสี่ยงของผู้ให้บริการภายนอก (Vendor Risk Tiering)

เพื่อให้การกำกับดูแลเป็นไปตามหลัก Risk-Based Approach โรงพยาบาลจัดระดับความเสี่ยงของผู้ให้บริการภายนอกออกเป็น ๓ ระดับ ดังนี้

ระดับความเสี่ยง	ลักษณะการเข้าถึง	ตัวอย่าง	มาตรการกำกับดูแล
สูง (Critical)	เข้าถึงข้อมูลส่วนบุคคลอ่อนไหว หรือเชื่อมต่อระบบ Core System โดยตรง	ผู้ให้บริการ HIS/EMR, Cloud Provider, MSSP, ผู้ให้บริการ Lab Online	ประเมินก่อนสัญญา + DPA + NDA + ตรวจสอบรายปี + Right to Audit
กลาง (Significant)	เข้าถึงระบบ IT แต่ไม่สัมผัสข้อมูลส่วนบุคคลอ่อนไหวโดยตรง หรือเข้าถึงจำกัด	ผู้ดูแล Network, ผู้บำรุงรักษาเครื่อง IT, ผู้ให้บริการอินเทอร์เน็ต	ประเมินก่อนสัญญา + NDA + ตรวจสอบตามวงรอบ
ต่ำ (Low)	ไม่เข้าถึงระบบ IT หรือข้อมูลส่วนบุคคล ปฏิบัติงานทั่วไปในพื้นที่	ผู้รับจ้างทำความสะอาด ผู้รับจ้างก่อสร้าง ผู้จำหน่ายเครื่องเขียน	NDA (ตามความเหมาะสม) + ข้อกำหนดพื้นฐาน

ทั้งนี้ กลุ่มภารกิจสุขภาพดิจิทัลร่วมกับกลุ่มงานพัสดุและจัดซื้อ เป็นผู้ประเมินและจัดระดับความเสี่ยงของผู้ให้บริการภายนอกทุกรายก่อนเริ่มกระบวนการจัดซื้อจัดจ้าง

๕. มาตรการก่อนการทำสัญญา (Pre-contract Due Diligence)

๕.๑ การประเมินความพร้อมด้านความมั่นคงปลอดภัย (Security Assessment)

(ก) ผู้ให้บริการภายนอกระดับความเสี่ยงสูงและกลาง ต้องผ่านการประเมินความพร้อมด้านความมั่นคงปลอดภัยก่อนเริ่มทำสัญญา โดยใช้แบบประเมิน Vendor Security Assessment Questionnaire ของโรงพยาบาล

(ข) ตรวจสอบใบรับรองมาตรฐานความปลอดภัย (ถ้ามี) เช่น ISO/IEC ๒๗๐๐๑ หรือใบรับรองอื่นที่เกี่ยวข้อง

(ค) ประเมินความสามารถในการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเฉพาะกรณีที่ผู้ให้บริการทำหน้าที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

(ง) ตรวจสอบประวัติการเกิดเหตุละเมิดข้อมูลหรือเหตุการณ์ด้านความปลอดภัย (Security Incident History) ของผู้ให้บริการ (เท่าที่สามารถตรวจสอบได้)

(จ) กรณีผู้ให้บริการ Cloud ต้องตรวจสอบสถานที่ตั้งของ Data Center ว่าตั้งอยู่ในประเทศไทยหรือประเทศที่มีมาตรฐานการคุ้มครองข้อมูลเพียงพอ

๕.๒ หลักสิทธิ์ขั้นต่ำ (Principle of Least Privilege)

(ก) กำหนดขอบเขตการเข้าถึงข้อมูลและระบบให้เฉพาะเจาะจงเท่าที่จำเป็นตามภารกิจที่ได้รับมอบหมายเท่านั้น (Need-to-Know / Need-to-Access)

(ข) จัดทำรายการระบบและข้อมูลที่ผู้ให้บริการจะเข้าถึง (Access Scope Matrix) ไว้เป็นส่วนหนึ่งของเอกสารประกอบสัญญา

(ค) ห้ามให้สิทธิ์ระดับ Administrator หรือ Root Access แก่ผู้ให้บริการ เว้นแต่มีความจำเป็นอย่างยิ่งและได้รับอนุมัติจากหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษร

๕.๓ การตรวจสอบบุคลากรของผู้ให้บริการ (Personnel Screening)

(ก) ผู้ให้บริการต้องแจ้งรายชื่อบุคลากรที่จะเข้าปฏิบัติงานหรือเข้าถึงระบบสารสนเทศของโรงพยาบาลล่วงหน้า

(ข) บุคลากรของผู้ให้บริการที่จะเข้าถึงข้อมูลส่วนบุคคลอ่อนไหว ต้องผ่านการตรวจสอบประวัติเบื้องต้นตามที่โรงพยาบาลกำหนด

(ค) กรณีมีการเปลี่ยนแปลงบุคลากร ผู้ให้บริการต้องแจ้งโรงพยาบาลล่วงหน้าอย่างน้อย ๓ วันทำการ

๖. ข้อกำหนดในสัญญาและข้อตกลง (Contractual Requirements)

สัญญาจ้างหรือข้อตกลงการใช้บริการกับผู้ให้บริการภายนอกทุกราย (ระดับความเสี่ยงสูงและกลาง) ต้องมีข้อกำหนดอย่างน้อยดังต่อไปนี้

๖.๑ ข้อตกลงรักษาความลับ (Non-Disclosure Agreement: NDA)

(ก) ผู้ให้บริการและบุคลากรของผู้ให้บริการทุกคนที่เข้าถึงข้อมูลของโรงพยาบาล ต้องลงนามในข้อตกลงรักษาความลับก่อนเริ่มปฏิบัติงาน

(ข) NDA ต้องครอบคลุมข้อมูลทุกประเภทที่ผู้ให้บริการอาจเข้าถึง รวมถึงข้อมูลสุขภาพผู้ป่วย ข้อมูลระบบ รหัสผ่าน โครงสร้างเครือข่าย และข้อมูลทางธุรกิจ

(ค) ข้อตกลงรักษาความลับต้องมีผลบังคับใช้ต่อไปอย่างน้อย ๕ ปี หลังสิ้นสุดสัญญา

๖.๒ ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA)

(ก) กรณีผู้ให้บริการมีการเข้าถึงหรือประมวลผลข้อมูลส่วนบุคคลของผู้ป่วย บุคลากรหรือผู้มี

ส่วนได้ส่วนเสีย ต้องจัดทำ DPA แนบท้ายสัญญา ซึ่งระบุรายละเอียดอย่างน้อยดังนี้

(๑) วัตถุประสงค์และขอบเขตของการประมวลผลข้อมูล

(๒) ประเภทของข้อมูลส่วนบุคคลที่ประมวลผล

(๓) ระยะเวลาในการประมวลผล

(๔) หน้าที่และความรับผิดชอบของผู้ประมวลผลข้อมูลตามมาตรา ๔๐ แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

(๕) มาตรการรักษาความมั่นคงปลอดภัยที่ผู้ประมวลผลต้องจัดให้มี

(๖) เงื่อนไขการใช้ผู้ประมวลผลช่วง (Sub-processor) ต้องได้รับอนุมัติจากโรงพยาบาลเป็นลายลักษณ์อักษร

(๗) ข้อกำหนดเรื่องการลบหรือส่งคืนข้อมูลเมื่อสิ้นสุดสัญญา

(ข) ห้ามผู้ให้บริการนำข้อมูลส่วนบุคคลไปใช้นอกเหนือจากวัตถุประสงค์ที่กำหนดไว้ใน DPA โดยเด็ดขาด

๖.๓ สิทธิในการตรวจสอบ (Right to Audit)

(ก) โรงพยาบาลสงวนสิทธิ์ในการตรวจสอบมาตรการความมั่นคงปลอดภัยของผู้ให้บริการทั้งในรูปแบบการตรวจสอบ ณ สถานที่ (On-site Audit) และการตรวจสอบระยะไกล (Remote Audit)

(ข) ผู้ให้บริการต้องให้ความร่วมมือในการตรวจสอบอย่างเต็มที่ และจัดเตรียมหลักฐานประกอบตามที่ร้องขอ

(ค) โรงพยาบาลอาจมอบหมายให้บุคคลที่สามที่เป็นอิสระ (Independent Third Party) ดำเนินการตรวจสอบแทนได้

๖.๔ การแจ้งเหตุละเมิดความปลอดภัย (Security Incident Notification)

(ก) ผู้ให้บริการต้องแจ้งโรงพยาบาลโดยทันที และไม่เกิน ๒๔ ชั่วโมง นับจากทราบหรือมีเหตุอันควรสงสัยว่าเกิดเหตุละเมิดความปลอดภัยหรือข้อมูลรั่วไหลที่เกี่ยวข้องกับข้อมูลของโรงพยาบาล

(ข) การแจ้งต้องระบุรายละเอียดอย่างน้อยดังนี้ ลักษณะของเหตุการณ์ ประเภทและจำนวนข้อมูลที่ได้รับผลกระทบ มาตรการเยียวยาเบื้องต้น และแผนการแก้ไข

(ค) ผู้ให้บริการต้องให้ความร่วมมืออย่างเต็มที่ในการสืบสวนสอบสวนและแก้ไขเหตุละเมิด

๖.๕ ข้อกำหนดด้านประกันภัยและการชดเชยความเสียหาย (Liability and Indemnification)

(ก) ผู้ให้บริการระดับความเสี่ยงสูง ควรมีการทำประกันภัยความรับผิดทางไซเบอร์ (Cyber Liability Insurance) ตามความเหมาะสม

(ข) สัญญาต้องระบุข้อกำหนดเรื่องการรับผิดชดใช้ค่าเสียหาย กรณีเหตุละเมิดเกิดจากความบกพร่องของผู้ให้บริการ

๖.๖ สิทธิในการยกเลิกสัญญา (Termination Rights)

(ก) โรงพยาบาลสงวนสิทธิ์ในการยกเลิกสัญญาทันที กรณีผู้ให้บริการฝ่าฝืนข้อกำหนดด้านความมั่นคงปลอดภัยอย่างร้ายแรง หรือปฏิเสธการให้ความร่วมมือในการตรวจสอบ

(ข) สัญญาต้องระบุขั้นตอนการถ่ายโอนข้อมูลและระบบ (Transition Plan) กรณีเปลี่ยนผู้ให้บริการ

๗. มาตรการระหว่างการดำเนินงาน (Operational Security Controls)

๗.๑ การควบคุมการเข้าถึงระยะไกล (Remote Access Control)

(ก) ผู้ให้บริการที่ต้องเชื่อมต่อระบบสารสนเทศของโรงพยาบาลจากระยะไกล ต้องขออนุญาต

เป็นลายลักษณ์อักษรจากกลุ่มงานเทคโนโลยีสารสนเทศทุกครั้ง โดยระบุวัน เวลา ระบบที่ต้องเข้าถึง และวัตถุประสงค์

(ข) ต้องเชื่อมต่อผ่าน VPN (Virtual Private Network) ที่โรงพยาบาลกำหนดเท่านั้น และใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA)

(ค) ห้ามเปิดการเชื่อมต่อค้างไว้แบบถาวร (Persistent/Stale Connection) เมื่อเสร็จสิ้นภารกิจต้องยุติการเชื่อมต่อทันที

(ง) กลุ่มงานเทคโนโลยีสารสนเทศ ต้องบันทึก Log การเชื่อมต่อระยะไกลทุกครั้ง และเก็บรักษาไม่น้อยกว่า ๙๐ วัน

(จ) กรณีการเข้าถึงระบบที่มีข้อมูลส่วนบุคคลอ่อนไหว ต้องได้รับอนุมัติจากหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ และผู้อำนวยการโรงพยาบาลหรือผู้ที่ได้รับมอบหมาย

๗.๒ การจัดการบัญชีผู้ใช้งาน (Account Management)

(ก) บัญชีผู้ใช้งานสำหรับผู้ให้บริการภายนอกต้องเป็นบัญชีเฉพาะบุคคล (Named Account) ห้ามใช้บัญชีร่วม (Shared Account)

(ข) บัญชีทุกบัญชีต้องมีวันหมดอายุชัดเจน (Expiration Date) ไม่เกินระยะเวลาตามสัญญา โดยต้องมีการทบทวนทุก ๙๐ วัน

(ค) รหัสผ่านต้องเป็นไปตามนโยบายรหัสผ่านของโรงพยาบาล ความยาวไม่น้อยกว่า ๘ ตัวอักษร ประกอบด้วยตัวอักษรใหญ่ เล็ก ตัวเลข และอักขระพิเศษ

(ง) เมื่อเสร็จสิ้นภารกิจในแต่ละครั้ง หรือเมื่อบุคลากรของผู้ให้บริการสิ้นสุดการปฏิบัติงาน ต้องระงับบัญชีทันที (Disable Account)

๗.๓ การควบคุมการเข้าถึงทางกายภาพ (Physical Access Control)

(ก) บุคลากรของผู้ให้บริการที่เข้าปฏิบัติงานในพื้นที่โรงพยาบาล ต้องลงทะเบียนที่จุดรับ-ส่ง และสวมบัตรแสดงตนตลอดเวลาที่อยู่ในพื้นที่

(ข) การเข้าพื้นที่อ่อนไหว ได้แก่ ห้องเซิร์ฟเวอร์ ห้องเก็บข้อมูล ห้อง Data Center ต้องมีเจ้าหน้าที่ของโรงพยาบาลกำกับดูแลตลอดเวลา (Escorted Access)

(ค) ต้องบันทึกเวลาเข้า – ออก พื้นที่อ่อนไหวในทะเบียนบันทึกการเข้าถึง (Access Log)

(ง) ห้ามนำอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล เช่น USB Drive, External Hard Disk เข้ามาในพื้นที่อ่อนไหว เว้นแต่ได้รับอนุญาตเป็นลายลักษณ์อักษร

๗.๔ การรักษาความปลอดภัยของข้อมูลระหว่างดำเนินงาน (Data Security During Operations)

(ก) ข้อมูลส่วนบุคคลที่ส่งผ่านระหว่างโรงพยาบาลกับผู้ให้บริการ ต้องเข้ารหัส (Encryption) ทั้งขณะส่ง (In Transit) โดยใช้ TLS ๑.๒ ขึ้นไป และขณะจัดเก็บ (At Rest) โดยใช้ AES-๒๕๖ หรือเทียบเท่า

(ข) ห้ามผู้ให้บริการคัดลอก ถ่ายโอน หรือจัดเก็บข้อมูลของโรงพยาบาลในอุปกรณ์ส่วนตัวหรือระบบที่ไม่ได้รับอนุญาต

(ค) กรณีจำเป็นต้องใช้ข้อมูลจริงในการทดสอบระบบ ต้องดำเนินการ Data Masking หรือ Anonymization ก่อน เว้นแต่ได้รับอนุมัติเป็นกรณีพิเศษ

(ง) ผู้ให้บริการต้องแยกข้อมูลของโรงพยาบาลออกจากข้อมูลของลูกค้ารายอื่น (Data Segregation) โดยเฉพาะกรณีใช้บริการ Cloud แบบ Multi-tenant

๗.๕ การบริหารจัดการช่องโหว่และการอัปเดต (Patch and Vulnerability Management)

(ก) ผู้ให้บริการที่ดูแลระบบสารสนเทศต้องดำเนินการอัปเดต Security Patch ภายในกรอบเวลาที่กำหนด โดยช่องโหว่ระดับวิกฤต (Critical) ต้องแก้ไขภายใน ๗๒ ชั่วโมง

(ข) การอัปเดตหรือเปลี่ยนแปลงระบบต้องผ่านกระบวนการ Change Management ของโรงพยาบาลก่อนดำเนินการ

๘. การติดตามผลและการประเมินผู้ให้บริการ (Vendor Performance Monitoring)

๘.๑ คณะกรรมการตรวจรับงานหรือผู้ดูแลโครงการ ต้องประเมินผลการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยของผู้ให้บริการอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการต่อสัญญา

๘.๒ การประเมินประจำปีต้องครอบคลุมรายการอย่างน้อยดังนี้

(ก) การปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยในสัญญา

(ข) การรายงานเหตุการณ์ด้านความปลอดภัยและการตอบสนอง

(ค) การปฏิบัติตาม DPA และ NDA

(ง) ความเพียงพอของมาตรการรักษาความมั่นคงปลอดภัยทางเทคนิค

(จ) การจัดการบุคลากรและการควบคุมการเข้าถึง

๘.๓ ผลการประเมินต้องจัดทำเป็นรายงานเสนอหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ และผู้อำนวยการโรงพยาบาลรับทราบ

๘.๔ กรณีผู้ให้บริการไม่ผ่านเกณฑ์การประเมิน ต้องจัดทำแผนแก้ไข (Corrective Action Plan) และดำเนินการให้แล้วเสร็จภายในระยะเวลาที่กำหนด หากไม่ปรับปรุง ให้พิจารณาไม่ต่อสัญญาหรือยกเลิกสัญญาตามข้อกำหนด

๘.๕ กลุ่มงานเทคโนโลยีสารสนเทศต้องจัดทำและปรับปรุงทะเบียนผู้ให้บริการภายนอก (Vendor Register) ให้เป็นปัจจุบันอยู่เสมอ โดยระบุรายละเอียดอย่างน้อยดังนี้ ชื่อผู้ให้บริการ ระดับความเสี่ยง ขอบเขตการเข้าถึง วันเริ่มต้นและสิ้นสุดสัญญา และผลการประเมินล่าสุด

๙. การสิ้นสุดสัญญาและการเปลี่ยนผ่าน (Contract Termination and Transition)

เมื่อสัญญาสิ้นสุดลงหรือมีการยกเลิกสัญญาไม่ว่าด้วยเหตุใด ต้องดำเนินการดังต่อไปนี้ให้แล้วเสร็จภายใน ๕ วันทำการ นับจากวันสิ้นสุดสัญญา เว้นแต่จะมีข้อตกลงเป็นอย่างอื่น

๙.๑ การยกเลิกสิทธิ์การเข้าถึง (Access Revocation)

(ก) ยกเลิกบัญชีผู้ใช้งาน สิทธิ์การเข้าถึงระบบสารสนเทศ และสิทธิ์การเข้าถึงทางกายภาพทั้งหมดโดยทันที

(ข) เปลี่ยนรหัสผ่านของบัญชีระบบ (System Account) ที่ผู้ให้บริการเคยใช้งานหรือรับทราบ

(ค) ยกเลิกการเชื่อมต่อ VPN, API Key, SSH Key และช่องทางการเข้าถึงอื่นทั้งหมด

(ง) เก็บเครื่องมือ อุปกรณ์ บัตรผ่าน กุญแจ และทรัพย์สินของโรงพยาบาลคืนทั้งหมด

๙.๒ การจัดการข้อมูล (Data Handling)

(ก) ผู้ให้บริการต้องส่งคืนข้อมูลทั้งหมดของโรงพยาบาลในรูปแบบที่สามารถใช้งานได้ (Usable Format) ภายในระยะเวลาที่กำหนดในสัญญา

(ข) หลังส่งคืนข้อมูล ผู้ให้บริการต้องทำลายข้อมูลของโรงพยาบาลทั้งหมดที่อยู่ในครอบครองด้วยวิธีการที่ได้มาตรฐาน เช่น การลบข้อมูลแบบ Secure Erase, การทำลายสื่อบันทึกข้อมูลทางกายภาพ (Degaussing/Shredding)

(ค) ผู้ให้บริการต้องออกหนังสือรับรองการทำลายข้อมูล (Certificate of Data Destruction) โดยระบุวิธีการ วันที่ และรายการข้อมูลที่ทำลาย

(ง) กรณีข้อมูลจัดเก็บบน Cloud ผู้ให้บริการต้องยืนยันการลบข้อมูลจากทุก Data Center รวมถึง Backup ทั้งหมด

๙.๓ การถ่ายโอนงาน (Knowledge Transfer)

(ก) ผู้ให้บริการต้องให้ความร่วมมือในการถ่ายโอนความรู้ เอกสาร คู่มือ และข้อมูลทางเทคนิคที่จำเป็นต่อการดำเนินงานต่อเนื่อง

(ข) กรณีเปลี่ยนผู้ให้บริการ ต้องจัดทำแผนการเปลี่ยนผ่าน (Transition Plan) ที่ได้รับความเห็นชอบจากทั้งสองฝ่าย

๑๐. บทบาทและหน้าที่ความรับผิดชอบ

ผู้รับผิดชอบ	หน้าที่และความรับผิดชอบ
ผู้อำนวยการโรงพยาบาล	อนุมัตินโยบาย กำกับดูแลภาพรวม และลงนามในสัญญากับผู้ให้บริการระดับความเสี่ยงสูง
กลุ่มงานเทคโนโลยีสารสนเทศและกลุ่มงานสุขภาพสุขภาพดิจิทัล	ประเมินความเสี่ยง จัดระดับผู้ให้บริการ กำหนดมาตรการทางเทคนิค ควบคุมการเข้าถึง ติดตาม Log และจัดทำทะเบียนผู้ให้บริการ
กลุ่มงานพัสดุและจัดซื้อ	บรรจุข้อกำหนดด้านความมั่นคงปลอดภัยลงใน TOR/สัญญา ประสานงานจัดทำ NDA/DPA และดูแลกระบวนการจัดซื้อจัดจ้าง
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	ให้คำปรึกษาด้าน PDPA ตรวจสอบ DPA กำกับดูแลการประมวลผลข้อมูลส่วนบุคคลโดยผู้ให้บริการ
หัวหน้ากลุ่มงาน (เจ้าของโครงการ)	ดูแลให้ผู้ให้บริการปฏิบัติตามสัญญาและนโยบาย ประเมินผลงาน และรายงานปัญหาแก่ผู้บริหาร
คณะกรรมการบริหารความเสี่ยง/ไซเบอร์	กำกับดูแลเชิงนโยบาย ทบทวนผลการประเมินผู้ให้บริการ และพิจารณาแก้ไขปัญหาเชิงระบบ

๑๑.บทลงโทษและมาตรการบังคับใช้

๑๑.๑ ผู้ให้บริการที่ฝ่าฝืนนโยบายฉบับนี้ อาจถูกดำเนินการดังนี้

(ก) ตักเตือนเป็นลายลักษณ์อักษร

(ข) ระงับการเข้าถึงระบบชั่วคราวจนกว่าจะแก้ไขให้เป็นไปตามข้อกำหนด

(ค) ไม่พิจารณาต่อสัญญาหรือยกเลิกสัญญา

(ง) เรียกร้องค่าเสียหายตามสัญญาและกฎหมายที่เกี่ยวข้อง

(จ) แจ้งหน่วยงานกำกับดูแลที่เกี่ยวข้อง (กรณีมีการละเมิดกฎหมาย)

๑๑.๒ บุคลากรของโรงพยาบาลที่อนุญาตให้ผู้ให้บริการภายนอกเข้าถึงระบบ โดยไม่ปฏิบัติตามนโยบายฉบับนี้ อาจถูกพิจารณาทางวินัยตามระเบียบของทางราชการ

๑๒.กฎหมาย มาตรฐาน และเอกสารที่เกี่ยวข้อง

๑๒.๑ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑๒.๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑๒.๓ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑๒.๔ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยมาตรฐานความมั่นคงปลอดภัยไซเบอร์

๑๒.๕ มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศสำหรับโรงพยาบาล

๑๒.๖ นโยบายความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลปราสาท

๑๒.๗ นโยบายคุ้มครองข้อมูลส่วนบุคคลของโรงพยาบาลปราสาท

นโยบายฉบับนี้ มีผลบังคับใช้ตั้งแต่วันที่ผู้อำนวยการโรงพยาบาลลงนามประกาศ และให้ทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมาย มาตรฐาน หรือสภาพแวดล้อมด้านภัยคุกคามอย่างมีนัยสำคัญ

ประกาศ ณ วันที่ ๒๖ กุมภาพันธ์ ๒๕๖๙

(นางสาวชูหงส์ มหรรทัศนพงศ์)

ผู้อำนวยการโรงพยาบาลปราสาท