รายละเอียดขอบเขตการจ้างงาน (Terms of Reference: TOR)
โครงการจ้างบริการระบบ Cloud Service

๑. หลักการและเหตุผล

ตามที่กระทรวงสาธารณสุข ได้กำหนดนโยบายและยุทธศาสตร์การพัฒนาระบบสาธารณสุขของประเทศ โดยมุ่งเน้นการยกระดับคุณภาพชีวิตของประชาชนผ่านการพัฒนาระบบสาธารณสุขที่มีประสิทธิภาพ สอดคล้องกับยุทธศาสตร์ชาติ ๒๐ ปี ด้านสาธารณสุข (พ.ศ. ๒๕๖๑-๒๕๘๐) ซึ่งมุ่งเน้นการสร้างเสริมความเป็นเลิศด้านบริการสุขภาพ (Service Excellence) (กระทรวงสาธารณสุข, ๒๕๖๐) ในปีงบประมาณ พ.ศ. ๒๕๖๙ กระทรวงสาธารณสุขได้พัฒนาการดำเนินงานของแพลตฟอร์มระบบสุขภาพดิจิทัลบน Digital Health Platform ของกระทรวงสาธารณสุข ตามภารกิจหลักของกระทรวงสาธารณสุขอย่างต่อเนื่อง ในการยกระดับระบบบริการสาธารณสุข พัฒนาคุณภาพชีวิตประชาชน สร้างความมั่นคงทางสุขภาพของคนไทยทุกมิติ ครอบคลุมทั้งการส่งเสริม ควบคุมป้องกันโรค รักษา และฟื้นฟูสุขภาพ สำหรับประชาชนทุกกลุ่ม เพื่อลดความเหลื่อมล้ำและเพิ่มการเข้าถึงบริการที่มีคุณภาพได้มาตรฐาน โดยการพัฒนาดังกล่าวจำเป็นต้องอาศัยนวัตกรรมและเทคโนโลยีที่ทันสมัย เพื่อยกระดับคุณภาพบริการสุขภาพของประชาชนด้วยการพัฒนาระบบบริการสุขภาพดิจิทัลด้วยการประยุกต์ใช้เทคโนโลยีที่ทันสมัยเพื่อสนับสนุนการบริการสุขภาพ การเชื่อมโยงข้อมูลและบูรณาการข้อมูลระหว่างหน่วยบริการสุขภาพเพื่อให้ประชาชนสามารถเข้ารับการรักษาพยาบาลได้ทุกหน่วยบริการและสามารถเข้าถึงข้อมูลสุขภาพของตนเองได้อย่างถูกต้อง มีความปลอดภัย สะดวกและรวดเร็ว โดยการบูรณาการข้อมูลที่ไร้รอยต่อในการเชื่อมโยงระบบข้อมูลของโรงพยาบาล คลินิก ร้านยา และสถานพยาบาลอื่น ๆ ที่เกี่ยวข้อง เพื่อให้สามารถเชื่อมโยงและแลกเปลี่ยนข้อมูลผ่านแพลตฟอร์มระบบสุขภาพดิจิทัล บน Digital Health Platform ของกระทรวงสาธารณสุขระหว่างกันได้อย่างมีประสิทธิภาพ สามารถเข้าถึงข้อมูลและบริการทางการแพทย์ได้อย่างสะดวก รวดเร็ว ทุกที่ ทุกเวลา ภายใต้มาตรฐานความปลอดภัยระดับสากล การพัฒนาระบบบริการสุขภาพดิจิทัลประกอบไปด้วย ระบบบริการสุขภาพและแพลตฟอร์มระบบสุขภาพดิจิทัล อาทิเช่น ระบบประวัติสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล (Personal Health Record: PHR) ระบบดิจิทัลไอดีของบุคลากรทางการแพทย์และผู้ให้บริการสาธารณสุข (Provider ID) ระบบดิจิทัลไอดีของประชาชนผู้รับบริการสาธารณสุข (Health ID) ระบบใบรับรองแพทย์ดิจิทัล (Digital Signature) ระบบใบสั่งยาออนไลน์ ระบบสั่งแล็บออนไลน์ (MOPH LAB) ระบบส่งต่อผู้ป่วย (MOPH Refer) ระบบบริการการแพทย์ทางไกลและเภสัชกรรมทางไกล และการปรึกษาแพทย์ผู้เชี่ยวชาญ (Telemedicine & Telepharmacy) ระบบการนัดหมายออนไลน์ (MOPH Appointment) ระบบการส่งยาและเวชภัณฑ์ที่บ้าน (Health Rider) ระบบเชื่อมโยงข้อมูลภาพเอกซเรย์ของประชาชน (Imaging Hub) ระบบ Health Wallet เป็นต้น โดยเป็นการพัฒนาแพลตฟอร์มระบบสุขภาพดิจิทัลบน Digital Health Platform ของกระทรวงสาธารณสุข ซึ่งต้องให้บริการอย่างต่อเนื่องตลอด ๒๔ ชั่วโมง เพื่อรองรับการให้บริการสุขภาพแก่ประชาชนทั่วประเทศ ตามแผนงานการจัดซื้อจัดจ้างของสำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข

ด้วยเหตุผลดังกล่าว สำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข จึงจัดทำโครงการจ้างบริการระบบ Cloud Service รองรับการให้บริการสุขภาพดิจิทัล ตามแผนแม่บทการพัฒนาระบบสุขภาพดิจิทัลแห่งชาติ (พ.ศ. ๒๕๖๖ - ๒๕๗๐) โดยคำนึงถึงมาตรฐานความปลอดภัยระดับสากล อาทิ ISO/IEC 27001, ISO/IEC 27017 และ ISO/IEC 27018 สำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในบริการคลาวด์ (กระทรวงสาธารณสุข, ๒๕๖๖) ทั้งนี้ การดำเนินการดังกล่าวจะสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และธรรมาภิบาลข้อมูลภาครัฐตามที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) กำหนด เพื่อให้บริการสุขภาพประชาชนได้อย่างมีประสิทธิภาพ ลดความซ้ำซ้อนในการรักษา เพิ่มประสิทธิภาพในการป้องกันโรค และบริหารจัดการทรัพยากรสาธารณสุขได้อย่างเหมาะสม ซึ่งจะสะท้อนให้เห็นถึงความคุ้มค่าในการลงทุนพัฒนาระบบดังกล่าว เพื่อยกระดับคุณภาพชีวิตของประชาชนไทยอย่างยั่งยืน

๒. วัตถุประสงค์...

๒. วัตถุประสงค์

๒.๑ เพื่อจ้างบริการระบบ Cloud Service แบบ Infrastructure as a Service (IaaS) ในลักษณะทรัพยากรรวม (Resource Pool) ที่มีประสิทธิภาพสูง มีความเสถียร และมั่นคงปลอดภัย เพื่อเป็นโครงสร้างพื้นฐานกลางรองรับการทำงานของ Digital Health Platform และระบบข้อมูลสุขภาพของกระทรวงสาธารณสุข ให้สามารถให้บริการแก่ประชาชนและหน่วยงานสาธารณสุขทั่วประเทศได้อย่างรวดเร็ว ต่อเนื่อง และมีมาตรฐานระดับสากล

๒.๒ เพื่อให้เกิดการบูรณาการและแลกเปลี่ยนข้อมูล โดยทำหน้าที่เป็นแหล่งข้อมูลอ้างอิง (Data Provider) ให้แก่ระบบงานอื่นและระบบวิเคราะห์ปัญญาประดิษฐ์ภายนอก ผ่านโครงสร้างพื้นฐานคลาวด์ (IaaS) ที่มีความพร้อมและทรัพยากรที่เพียงพอ (Readiness) สำหรับการติดตั้งซอฟต์แวร์ตามมาตรฐานสากล อาทิ HL7 FHIR R4, SNOMED CT, LOINC และ DICOM ตามแผนแม่บทการพัฒนาสุขภาพดิจิทัลแห่งชาติ ตลอดจนรองรับการเชื่อมต่อกับโครงข่ายและระบบแลกเปลี่ยนข้อมูลภาครัฐ และมีมาตรฐานความปลอดภัยในการรับส่งข้อมูลสุขภาพที่สอดคล้องกับมาตรฐานระดับสากล

๒.๓ เพื่อเพิ่มประสิทธิภาพและความยืดหยุ่นของระบบฐานข้อมูลกลางให้สามารถรองรับปริมาณข้อมูลและธุรกรรมที่ขยายตัวในอนาคตได้ทันที และ รองรับการบริหารจัดการระบบ (Managed Services) ซึ่งเปิดกว้างให้สามารถดำเนินการได้ทั้งโดยผู้ให้บริการระบบคลาวด์เอง หรือโดยผู้เชี่ยวชาญจากภายนอก (Third-Party Managed Service Provider) เพื่อลดภาระการดูแลรักษาของผู้ว่าจ้าง

๒.๔ เพื่อให้การดำเนินงานเป็นไปตามกฎหมายและมาตรฐานความปลอดภัย ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒, และมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศด้านสุขภาพ (Health Informatics) โดยคำนึงถึงความเป็นเจ้าของข้อมูล (Data Ownership) และถิ่นที่อยู่ของข้อมูล (Data Residency) ภายในราชอาณาจักรไทยเป็นสำคัญ

๓. คุณสมบัติของผู้เสนอราคา

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ เป็นนิติบุคคลผู้มีอาชีพรับจ้างที่ประกวดราคาอิเล็กทรอนิกส์

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานปลัดกระทรวงสาธารณสุข ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือวันที่หน่วยงานของรัฐมีหนังสือเชิญชวน และไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๓.๑๐ ผู้ยื่นข้อเสนอ...

๓.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

๓.๑๐.๑ การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

๓.๑๐.๒ กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลักผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

๓.๑๐.๓ การยื่นข้อเสนอของกิจการร่วมค้า

๓.๑๐.๓.๑ กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

๓.๑๐.๓.๒ การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e – bidding) ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ ๓.๑๐ ดำเนินการซื้อและดาวน์โหลดเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารจ้างทำของจึงจะมีสิทธิในการเข้ายื่นข้อเสนอในนามกิจการร่วมค้าได้

๓.๑๑ ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

๓.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

๓.๑๒.๑ กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ ๑ ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนอนั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก ๑ ปี ได้

๓.๑๒.๒ กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียนโดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๒๐ ล้านบาท

๓.๑๒.๓ สำหรับ...

๓.๑๒.๓ สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอโดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

๓.๑๒.๔ กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศหรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน)

๓.๑๒.๕ กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศหรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทยตามข้อ ๓.๑๒.๒ ข้อ ๓.๑๒.๓ และข้อ ๓.๑๒.๔ (๒) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e-GP) จนถึงวันเสนอราคา

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศว่าด้วยการรับรองเอกสาร พ.ศ. ๒๕๓๙ และที่แก้ไขเพิ่มเติมกำหนด โดยจะต้องยื่นเอกสารดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอมิได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่าผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

๓.๑๒.๖ กรณีตามข้อ ๓.๑๒.๑ - ข้อ ๓.๑๒.๕ ไม่ใช้บังคับกรณีดังต่อไปนี้

๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย พ.ศ. ๒๔๘๓ และที่แก้ไขเพิ่มเติม

๓) งานจ้างก่อสร้าง...

๓) งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

๔) การจัดซื้อจัดจ้างตามมาตรา ๕๖ วรรคหนึ่ง (๒) (ข) และ (ค) แห่งพระราชบัญญัติการจัดซื้อจัดจ้างฯ

๕) การซื้ออสังหาริมทรัพย์และการเช่าอสังหาริมทรัพย์

๖) กรณีงานจ้างบริการหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงานขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

๓.๑๓ ผู้ยื่นข้อเสนอต้องมีผลงานในการให้บริการระบบ (Cloud Service) ด้านการแพทย์และสุขภาพ ให้กับหน่วยงานภาครัฐ หรือรัฐวิสาหกิจหรือเอกชน หรือผลงานด้านการให้บริการโครงสร้างพื้นฐาน จำนวนไม่น้อยกว่า ๑ ผลงาน โดยมีวงเงินของสัญญาไม่น้อยกว่า ๕,๐๐๐,๐๐๐ บาท (ห้าล้านบาทถ้วน) ต่อสัญญา ทั้งนี้ พร้อมยื่นหลักฐานเป็นสำเนาหนังสือรับรองผลงานที่ออกโดยผู้ว่าจ้างหรือสำเนาสัญญา

๓.๑๔ ผู้ยื่นข้อเสนอต้องปฏิบัติตามมติคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เรื่องแนวทางการดำเนินการตามมติคณะรัฐมนตรีเกี่ยวกับการจัดซื้อจัดจ้างหรือเช่าใช้บริการระบบคลาวด์ ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ การกำหนดแนวทางการดำเนินการตามมติคณะรัฐมนตรีเกี่ยวกับการจัดซื้อจัดจ้างหรือเช่าใช้บริการ ระบบคลาวด์ของหน่วยงานภาครัฐ

๓.๑๕ ผู้ยื่นข้อเสนอต้องยื่นแผนการบริหารจัดการความเสี่ยงห่วงโซ่อุปทาน (Supply Chain Risk Management Plan) และแผนการเปลี่ยนผ่านระบบเบื้องต้น (Preliminary Transition Plan) มาพร้อมกับการยื่นข้อเสนอทางเทคนิค เพื่อแสดงความพร้อมในการบริหารจัดการความเสี่ยงจากบุคคลภายนอกและการโอนย้ายข้อมูล

๔. รายละเอียดขอบเขตของงาน

<u>หมวดโครงสร้างพื้นฐาน</u>

๔.๑ มาตรฐานและการรับรอง

ผู้ให้บริการระบบ Cloud Service ต้องได้รับการรับรองมาตรฐานสากลที่ยังมีผลบังคับใช้ดังต่อไปนี้ พร้อมยื่นหลักฐานประกอบ

๔.๑.๑ มาตรฐานบังคับพื้นฐาน

๔.๑.๑.๑ ISO/IEC 27001 (Information Security Management) การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๔.๑.๑.๒ ISO/IEC 27017 (Cloud Security) หรือ CSA-STAR Level 1 ขึ้นไป การรักษาความปลอดภัยสำหรับบริการคลาวด์

๔.๑.๑.๓ ISO/IEC 20000-1 (IT Service Management) หรือยื่นเอกสารคู่มือกระบวนการปฏิบัติงาน (SOP) ที่สอดคล้องกับกรอบการทำงาน ITIL เพื่อเทียบเคียง

๔.๑.๑.๔ มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

๔.๑.๒ มาตรฐานเฉพาะทางสำหรับมาตรฐานดังต่อไปนี้

๔.๑.๒.๑ ISO/IEC 27018 (Cloud Privacy Protection) การคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์สาธารณะ

๔.๑.๒.๒ ISO/IEC 27799 (Health Informatics Information Security)

๔.๑.๒.๓ ISO 22301 (Business Continuity Management) การบริหารความต่อเนื่องทางธุรกิจ

๔.๒ ทรัพยากร...

๔.๒ ทรัพยากรระบบประมวลผล

ระบบ Cloud Service ต้องมีสถาปัตยกรรมแบบ Software Defined Infrastructure (SDI) หรือเทียบเท่า ที่ช่วยให้ผู้ดูแลระบบสามารถบริหารจัดการทรัพยากร (Compute, Network, Storage) ได้อย่างยืดหยุ่นผ่านซอฟต์แวร์ หรือ API โดยจัดเตรียมทรัพยากรในรูปแบบ Virtual Private Cloud (VPC) หรือ Dedicated Resource Pool ที่มีความมั่นคงปลอดภัยและมีประสิทธิภาพสูง โดยต้องมีการรับประกันการจัดสรรทรัพยากร ดังนี้

๔.๒.๑ Virtual Machine (VM) Capacity ระบบต้องรองรับการสร้างเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (VM) ได้รวมไม่น้อยกว่า 672 VMs ภายใต้ทรัพยากรรวมที่กำหนด

๔.๒.๒ หน่วยประมวลผลกลางเสมือน (vCPU Pool) จัดสรรรวมไม่น้อยกว่า 5,376 vCores โดยต้องไม่มีการแชร์ทรัพยากรกับผู้ใช้บริการรายอื่นจนส่งผลกระทบต่อประสิทธิภาพ

๔.๒.๓ หน่วยความจำหลักเสมือน (vRAM Pool) จัดสรรรวมไม่น้อยกว่า 10,752 GB

๔.๒.๔ ทรัพยากรจัดเก็บข้อมูลเสมือน (vDisk/Block Storage) ผู้ให้บริการต้องจัดสรรพื้นที่จัดเก็บข้อมูลรวมไม่น้อยกว่า 672 TB ทั้งนี้ ผู้ให้บริการต้องจัดทำรายงานประสิทธิภาพ (Performance Report)
เพื่อแสดงการใช้พื้นที่จัดเก็บข้อมูลต่อหน่วยพื้นที่

๔.๒.๕ ระบบปฏิบัติการและลิขสิทธิ์ รองรับการติดตั้งระบบปฏิบัติการพร้อม License ที่ถูกต้องตามกฎหมาย ครอบคลุมทั้ง Microsoft Windows Server (รุ่น Standard หรือ Datacenter) และ Linux Enterprise (เช่น Red Hat, SUSE, Ubuntu) โดยผู้ให้บริการต้องรับผิดชอบค่าใช้จ่ายในการบริหารจัดการลิขสิทธิ์และการอัปเดตแพตช์ (Patch Management) ตลอดอายุสัญญา

๔.๒.๖ ระบบป้องกันเครื่องแม่ข่าย ติดตั้งระบบป้องกัน มัลแวร์ และภัยคุกคาม (Anti-malware/EDR) บนเครื่อง VM ทุกเครื่อง โดยบริหารจัดการแบบศูนย์กลาง (Centralized Management) และใช้โปรแกรมแบบ Lightweight Agent ที่ไม่กระทบต่อประสิทธิภาพแอปพลิเคชัน พร้อมทั้งต้องแสดงหลักฐานเอกสารสิทธิ์ (License Agreement) ที่ถูกต้องตามกฎหมายของการให้บริการซอฟต์แวร์ดังกล่าว

๔.๒.๗ ระบบบริหารจัดการเครือข่าย API (API Management Readiness) เพื่อรองรับการเป็นศูนย์กลางเชื่อมโยงข้อมูลสุขภาพระดับประเทศ โครงสร้างพื้นฐานเครือข่ายและระบบกระจายภาระงาน (Load Balancer) ต้องมีคุณสมบัติในการบริหารจัดการปริมาณการจราจรข้อมูล ดังนี้

๔.๒.๗.๑ การรักษาเสถียรภาพและความต่อเนื่อง ระบบต้องสามารถกำหนดค่าจำกัดอัตราการเรียกใช้งาน (Rate Limiting) และการหน่วงสัญญาณคำขอ (Throttling) ได้ทั้งในระดับ IP Address และระดับ Service Endpoint เพื่อป้องกันสภาวะระบบขัดข้องอันเนื่องมาจากการส่งข้อมูลพร้อมกันปริมาณมหาศาลจากหน่วยงานบริการสุขภาพทั่วประเทศ

๔.๒.๗.๒ การบริหารจัดการโควตารายโครงการ (Project-based Quota Management) ระบบต้องสามารถจำกัดปริมาณการรับส่งข้อมูลแยกตามรายโครงการของผู้พัฒนาแต่ละราย หรือรายผู้ใช้งานภายนอก เพื่อป้องกันการแย่งทรัพยากรโครงข่าย (Network Congestion) และการันตีประสิทธิภาพสูงสุดให้แก่ระบบงานหลัก

๔.๒.๗.๓ ระบบเฝ้าระวังและแจ้งเตือนเหตุผิดปกติ ผู้ให้บริการต้องจัดเตรียมเครื่องมือในการติดตามปริมาณการใช้งาน API แบบ Real-time โดยต้องมีระบบแจ้งเตือนไปยังผู้ว่าจ้างเมื่อพบพฤติกรรมการเรียกใช้ข้อมูลที่ผิดปกติ หรือมีการใช้งานทรัพยากรใกล้ถึงขีดจำกัดที่กำหนดไว้

๔.๒.๗.๔ การรองรับมาตรฐานความปลอดภัย ระบบ Load Balancer หรือ API Gateway ต้องรองรับการเชื่อมต่อผ่านมาตรฐานความปลอดภัยระดับสากล อาทิ mTLS (mutual TLS) หรือ OAuth 2.0 เพื่อรองรับการพิสูจน์ตัวตนจากระบบภายนอกก่อนอนุญาตให้ดึงข้อมูลสุขภาพ

๔.๒.๘ การขยายตัว...

๔.๒.๘ การขยายตัวกรณีฉุกเฉิน (Burst Capability) ในกรณีระบบมีปริมาณการใช้งานเพิ่มขึ้นชั่วคราว ผู้ให้บริการต้องสามารถเพิ่มทรัพยากร vCPU และ vRAM ให้ระบบใช้งานได้อย่างต่อเนื่องไม่น้อยกว่าร้อยละ ๓๐ ของทรัพยากรที่กำหนดในสัญญา โดยต้องพร้อมใช้งานภายใน ๔ ชั่วโมงหลังได้รับแจ้ง และไม่มีค่าใช้จ่ายเพิ่มเติมจากราคาที่เสนอ โดยผู้ให้บริการต้องจัดทำกระบวนการการบริหารจัดการคำร้องขอบริการ (Service Request Management) เพื่อบันทึกขั้นตอนการขออนุมัติและระยะเวลาในการปรับขยายทรัพยากรฉุกเฉินให้ผู้ว่าจ้างทราบ

๔.๓ ศูนย์ข้อมูลและระบบเครือข่าย

๔.๓.๑ Data Center ตั้งอยู่ในประเทศไทย ไม่น้อยกว่า ๒ แห่ง (Site หลัก และ Site สำรอง) ห่างกันอย่างน้อย ๓๐ กิโลเมตร ได้รับมาตรฐาน Tier III หรือเทียบเท่า และมีการเชื่อมต่อวงจรสื่อสารความเร็วสูงระหว่างศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรองที่มีความซ้ำซ้อน (Redundancy) เพื่อรองรับการสำรองและกู้คืนข้อมูลได้อย่างมีประสิทธิภาพ โดยผู้ให้บริการต้องแสดงหลักฐานที่ตั้งของ Data Center ที่ใช้งานจริงทั้ง ๒ แห่ง ให้ผู้ว่าจ้างทราบ

๔.๓.๒ Connectivity

๔.๓.๒.๑ Bandwidth ภายในประเทศ (Domestic) รวมไม่น้อยกว่า 40 Gbps

๔.๓.๒.๒ Bandwidth ต่างประเทศ (International) รวมไม่น้อยกว่า 1 Gbps และสามารถรองรับการขยายตัวชั่วคราว (Burstable) ได้เมื่อมีการ Update Security Patch หรือการเชื่อมต่อ API ขนาดใหญ่

๔.๓.๒.๓ ผู้ให้บริการต้องจัดทำรายงานการใช้งาน Bandwidth ประจำเดือน

โดยผู้ให้บริการต้องจัดทำรายงานการใช้งานแบนด์วิดท์ (Bandwidth Report) ส่งมอบเป็นประจำทุกเดือน

๔.๓.๓ Fair Usage Policy (FUP)

๔.๓.๓.๑ Inbound ไม่จำกัดปริมาณข้อมูลขาเข้า

๔.๓.๓.๒ Outbound รองรับปริมาณข้อมูลขาออกไม่น้อยกว่า ๑๐๐ เทราไบต์ (TB) ต่อเดือน โดยไม่มีค่าใช้จ่ายเพิ่มเติม หรือเป็นแบบไม่จำกัดภายใต้เงื่อนไขการใช้งานที่เป็นธรรม

๔.๓.๓.๓ การป้องกันค่าใช้จ่ายแอบแฝง ผู้ให้บริการขอรับรองว่า ราคาที่เสนอเป็นราคาสุทธิ (Fixed Price) หากในระหว่างการให้บริการจริง มีปริมาณการดึงข้อมูลขาออก (Data Egress), ปริมาณการเรียกใช้ API (API Requests), การถ่ายโอนข้อมูลข้ามโซน (Cross-zone transfer) หรือค่าใช้จ่ายแฝงอื่นใดที่เกินกว่าแพ็กเกจที่ผู้ให้บริการกำหนด ผู้ให้บริการจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายส่วนเกินนั้นเองทั้งสิ้น โดยไม่สามารถนำมาเรียกเก็บเพิ่มจากผู้ว่าจ้างได้ในทุกกรณีตลอดอายุสัญญา

๔.๓.๓.๔ ต้องมีวงจรเชื่อมโยงกับศูนย์แลกเปลี่ยนข้อมูลอินเทอร์เน็ตภายในประเทศ (NIX) และต่างประเทศ (IIG) ไม่น้อยกว่า ๒ เส้นทาง จากผู้ให้บริการวงจรที่แตกต่างกัน และมีการออกแบบระบบสำรองที่มั่นใจได้ว่าหาก Gateway หรือโครงข่ายของผู้ให้บริการรายใดรายหนึ่งขัดข้อง ระบบยังสามารถสลับการทำงานไปยังโครงข่ายสำรองได้โดยอัตโนมัติ (Automated Failover) โดยไม่ทำให้ระบบหยุดชะงัก

๔.๓.๔ Latency ภายในประเทศไม่เกิน 30 ms และต่างประเทศไม่เกิน 150 ms

๔.๓.๕ Internal Throughput โครงข่ายภายในต้องรองรับการรับส่งข้อมูลระหว่าง VM และ Storage ด้วยความเร็วไม่น้อยกว่า 10 Gbps

๔.๓.๖ Public IP จัดเตรียม Public IP Address จำนวนเพียงพอต่อการใช้งาน (ไม่น้อยกว่า 64 IPs หรือตามตกลง)

๔.๓.๗ การแบ่งแยก...

๔.๓.๗ การแบ่งแยกสภาพแวดล้อมเครือข่าย (Network Segmentation) ผู้ให้บริการต้องออกแบบและกำหนดค่าระบบเครือข่ายให้มีการแบ่งแยกสภาพแวดล้อมอย่างชัดเจน (Logical or Physical Separation) ระหว่างสภาพแวดล้อมสำหรับการพัฒนา (Development), การทดสอบ (UAT/Staging) และระบบใช้งานจริง (Production) เพื่อป้องกันผลกระทบข้ามระบบและรักษาความมั่นคงปลอดภัยของข้อมูลในระบบใช้งานจริง ทั้งนี้ ผู้ให้บริการต้องจัดทำแผนผังเครือข่าย (Network Diagram) ที่แสดงรายละเอียดของการแบ่งโซน (Zone/Segmentation) และการบริหารจัดการหมายเลขไอพี (IP Management) อย่างชัดเจน

๔.๓.๘ สิทธิในการเข้าตรวจสอบ ผู้ว่าจ้างและคณะกรรมการตรวจรับพัสดุสงวนสิทธิ์ในการขอเข้าเยี่ยมชมและตรวจสอบ (Audit) ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) และศูนย์ปฏิบัติการเฝ้าระวัง (SOC) ของผู้ให้บริการ ได้ตลอดระยะเวลาสัญญา โดยจะแจ้งให้ทราบล่วงหน้าตามสมควร เพื่อตรวจสอบความมีอยู่จริงและประสิทธิภาพของมาตรการรักษาความมั่นคงปลอดภัยทางกายภาพ โดยผู้ให้บริการต้องให้ความร่วมมือและอำนวยความสะดวกในการตรวจสอบดังกล่าว

<u>หมวดความปลอดภัย</u>

๔.๔ ความมั่นคงปลอดภัยและการกู้คืนระบบ

๔.๔.๑ ระบบความปลอดภัยเครือข่าย

ต้องมีระบบป้องกันและตรวจสอบสิทธิ์การเข้าถึงข้อมูลตามมาตรฐาน Secure Access Service Edge (SASE) หรือ Virtual Firewall ที่มีคุณสมบัติ ดังนี้

๔.๔.๑.๑ สามารถรองรับ Traffic แบบ North-South และ East-West

๔.๔.๑.๒ สามารถรองรับ Throughput ไม่น้อยกว่า 10 Gbps หรือเพียงพอต่อการใช้งานจริงโดยไม่เกิดคอขวด

๔.๔.๑.๓ สามารถบริหารจัดการนโยบาย (Policy) ได้จากศูนย์กลาง

๔.๔.๑.๔ ระบบการเข้าถึงระยะไกล (เช่น SSL-VPN) ต้องมีมาตรการป้องกันการเคลื่อนที่แนวราบ (Lateral Movement) โดยสิทธิผู้ใช้งานระดับดูแลระบบ (Admin) หรือ Power Users จะต้องถูกจำกัดสิทธิและตรวจสอบได้ผ่านระบบศูนย์กลาง ไม่อนุญาตให้เข้าถึงระบบอื่น ๆ ในเครือข่ายเดียวกัน (เช่น ผ่าน SSH) โดยปราศจากการควบคุมและบันทึกหลักฐาน

๔.๔.๑.๕ ผู้ให้บริการต้องจัดทำเอกสารตารางสิทธิผู้ใช้งาน (User Right Matrix) และรายงานสถานะการเข้าถึงระบบ

๔.๔.๒ ระบบกระจายภาระงาน (Load Balancer)

๔.๔.๒.๑ มีความสามารถในการช่วยกระจายโหลดงาน (Load Balance) โดยรองรับ Throughput สูงสุดไม่น้อยกว่า 5 Gbps

๔.๔.๒.๒ รองรับการเชื่อมต่อ (Concurrent Connections) ไม่น้อยกว่า ๑๐๐,๐๐๐ การเชื่อมต่อ

๔.๔.๒.๓ รองรับ Algorithm การกระจายงานได้หลากหลาย เช่น Round Robin, Least Connection, IP-Hash, HTTP Headers, URI, URL หรือเทียบเท่า

๔.๔.๒.๔ สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTP, HTTPS ได้

๔.๔.๓ ระบบป้องกันเว็บแอปพลิเคชัน (Web Application Firewall: WAF)

ต้องมีระบบป้องกันการโจมตี Web Server จากผู้ไม่ประสงค์ดี ด้วยอุปกรณ์ป้องกันเสมือน จำนวน 1 domain แบบ wild-card (หรือตามจำนวนใช้งานจริง) โดยมีคุณสมบัติ ดังนี้

๔.๔.๓.๑ สามารถ...

๔.๔.๓.๑ สามารถป้องกันการโจมตีผ่านทาง Website ตามมาตรฐาน OWASP Top 10 (เช่น SQL injection, XSS) ได้อย่างมีประสิทธิภาพ

๔.๔.๓.๒ มี Security Dashboard แสดงผลแบบ Real-time ระบุแหล่ง ที่มาการโจมตี (IP, Country) ได้

๔.๔.๓.๓ สามารถตั้งค่ากฎ (Custom WAF rules) ได้ไม่จำกัดจำนวน และการตั้งค่าต้องมีผลบังคับใช้ (Effective) ภายในเวลาไม่เกิน ๕ นาที

๔.๔.๓.๔ รองรับ SSL Offloading

๔.๔.๔ ระบบการบริหารจัดการตัวตนและสิทธิการเข้าถึง (Identity and Access Management: IAM & PAM)

ผู้ให้บริการต้องจัดเตรียมระบบควบคุมการเข้าถึงระบบคลาวด์และเครื่องแม่ข่ายที่มีความมั่นคงปลอดภัยและบริหารจัดการแบบรวมศูนย์ โดยมีคุณสมบัติและขอบเขตการทำงาน ดังนี้

๔.๔.๔.๑ การเข้าถึงจากภายนอก (Remote Access) รองรับการทำ VPN (Site-to-Site และ Client-to-Site) และ User VPN (Admin VPN) สำหรับผู้ดูแลระบบไม่น้อยกว่า 50 Users ทั้งนี้ระบบการเข้าถึงระยะไกล (เช่น SSL-VPN) ต้องมีมาตรการป้องกันการเคลื่อนที่แนวราบ (Lateral Movement) โดยสิทธิผู้ใช้งานระดับผู้ดูแลระบบ (Admin) หรือ Power Users จะต้องถูกจำกัดสิทธิและตรวจสอบได้ผ่านระบบศูนย์กลาง ไม่อนุญาตให้ผู้ใช้งานเข้าถึงระบบอื่น ๆ ในเครือข่ายเดียวกัน (เช่น ผ่าน SSH) โดยปราศจากการควบคุมและบันทึกหลักฐาน

๔.๔.๔.๒ การยืนยันตัวตนและการกำหนดสิทธิ ต้องรองรับการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) ก่อนอนุญาตให้เข้าถึงระบบ และรองรับการกำหนดสิทธิการใช้งานตามบทบาทอย่างละเอียด (Granular Role-Based Access Control: RBAC) เพื่อให้ผู้ว่าจ้างสามารถมอบสิทธิระดับ Admin ให้แก่บุคคลที่สาม (Third-party) เฉพาะส่วนงานที่รับผิดชอบได้ โดยไม่จำเป็นต้องใช้หรือเปิดเผยบัญชีหลัก (Root Account) ของผู้ให้บริการคลาวด์ นอกจากนี้ต้องรองรับการจัดการสิทธิการเข้าถึงผ่านระบบ API Key Management หรือ OAuth 2.0 สำหรับควบคุมระบบภายนอก

๔.๔.๔.๓ ระบบบริหารจัดการสิทธิขั้นสูง (Privileged Access Management: PAM): ต้องมีระบบศูนย์กลาง สำหรับให้ผู้ดูแลระบบ (System Admin) และนักพัฒนา (Developer) ทั้งของหน่วยงานและบุคคลภายนอกเข้าใช้งาน โดยมีคุณสมบัติดังนี้

(๑) การเข้าถึงแบบศูนย์กลาง (Centralized Access) ทำหน้าที่เป็นประตูทางเดียว (Gateway) ในการเข้าถึงเครื่องแม่ข่ายเสมือนผ่านโปรโตคอล SSH และ RDP โดยไม่ต้องเปิดพอร์ตเหล่านี้สู่สาธารณะโดยตรง

(๒) การบันทึกและตรวจสอบ (Session Recording & Audit) สามารถบันทึกการใช้งานในรูปแบบวิดีโอ หรือบันทึกชุดคำสั่ง (Command Log) ที่ผู้ใช้งานพิมพ์ลงไปได้ เพื่อใช้เป็นหลักฐานในการตรวจสอบทางนิติวิทยาศาสตร์คอมพิวเตอร์ (Digital Forensics)

(๓) การจัดการรหัสผ่าน (Credential Vault) มีระบบจัดเก็บและหมุนเวียนรหัสผ่านอัตโนมัติ (Password Rotation) เพื่อลดความเสี่ยงจากการใช้รหัสผ่านซ้ำหรือรหัสผ่านหลุดรอด

๔.๔.๔.๔ เอกสารส่งมอบและการตรวจสอบ ผู้ให้บริการต้องจัดทำและส่งมอบตารางสิทธิผู้ใช้งาน (User Right Matrix) ที่ครอบคลุมทุกระบบ พร้อมทั้งนำส่งรายงานแสดงสถานการณ์เข้าถึงเครื่องแม่ข่าย (PAM Access Report) ตามรอบการส่งมอบงานที่กำหนดไว้ในข้อ ๖.๒

๔.๔.๕ การสำรอง...

๔.๔.๕ การสำรองข้อมูลและการกู้คืน

๔.๔.๕.๑ Backup Strategy & Retention: มีระบบสำรองข้อมูล (Backup) และ Snapshot ทั้ง Site หลักและ Site สำรอง โดยเก็บข้อมูลย้อนหลังไม่น้อยกว่า ๓๐ วัน

๔.๔.๕.๒ RPO/ RTO: ระบบต้องสามารถสำรองและกู้คืนข้อมูลได้ตามระยะเวลาเป้าหมาย (Recovery Point Objective: RPO) และระยะเวลาการกู้คืนระบบ (Recovery Time Objective: RTO) ตามเกณฑ์ที่กำหนดไว้ในตารางระดับการให้บริการ (SLA) ข้อ ๔.๑๑ โดยผู้ให้บริการต้องสนับสนุนทรัพยากรในการดึงข้อมูลกลับมาให้เป็นปัจจุบันโดยเร็วที่สุด

โดยผู้ให้บริการต้องจัดทำรายงานสถานการณ์สำรองข้อมูลเพื่อประเมินความสอดคล้องตามเกณฑ์ RTO, RPO และ Retention Period ประจำเดือน

๔.๔.๖ การซ้อมแผน (DR Drill)

๔.๔.๖.๑ ผู้ให้บริการต้องดำเนินการซ้อมแผนกู้คืนระบบสารสนเทศ (DR Drill) ร่วมกับคณะทำงานของผู้ว่าจ้าง อย่างน้อยปีละ ๑ ครั้ง

๔.๔.๖.๒ ต้องจำลองสถานการณ์เสมือนจริงทั้งกรณีระบบล่มบางส่วนและล่มทั้งหมด

๔.๔.๖.๓ ต้องส่งรายงานผลการซ้อม (Drill Report) ที่ระบุเวลาที่ใช้จริง (Actual RTO) ปัญหาที่พบ และแนวทางปรับปรุง เพื่อประกอบการตรวจรับงาน

๔.๔.๗ ระบบบริหารจัดการสิทธิ์และการเข้าถึงเครื่องแม่ข่าย (Privileged Access Management: PAM) ผู้ให้บริการต้องจัดเตรียมระบบบริหารจัดการการเข้าถึงเครื่องแม่ข่ายเสมือน มีความมั่นคงปลอดภัยสูงสำหรับให้ผู้ดูแลระบบ (System Admin) และนักพัฒนา (Developer) ทั้งของหน่วยงานและบุคคลภายนอกเข้าใช้งาน โดยมีคุณสมบัติดังนี้

๔.๔.๗.๑ การเข้าถึงแบบศูนย์กลาง (Centralized Access) ทำหน้าที่เป็นประตูทางเดียว (Gateway) ในการเข้าถึงเครื่องแม่ข่ายเสมือนผ่านโปรโตคอล SSH และ RDP โดยไม่ต้องเปิดพอร์ตเหล่านี้สู่สาธารณะโดยตรง

๔.๔.๗.๒ การยืนยันตัวตน (Authentication) รองรับการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) ก่อนอนุญาตให้เข้าถึงระบบ

๔.๔.๗.๓ การบันทึกและตรวจสอบ (Session Recording & Audit) สามารถบันทึกการใช้งาน (Session Recording) ในรูปแบบวิดีโอ หรือบันทึกชุดคำสั่ง (Command Log) ที่ผู้ใช้งานพิมพ์ลงไปได้ เพื่อใช้เป็นหลักฐาน ในการตรวจสอบทางนิติวิทยาศาสตร์ (Digital Forensics)

๔.๔.๗.๕ การจัดการรหัสผ่าน (Credential Vault) มีระบบจัดเก็บและหมุนเวียนรหัสผ่านอัตโนมัติ (Password Rotation) เพื่อลดความเสี่ยงจากการใช้รหัสผ่านซ้ำหรือรหัสผ่านหลุดรอด

๔.๔.๘ ระบบบริหารจัดการการเข้ารหัสข้อมูลระดับโครงสร้างพื้นฐาน (Infrastructure Key Management) ระบบ Cloud Computing ต้องมีความสามารถในการเข้ารหัสข้อมูลในระดับพื้นที่จัดเก็บข้อมูล (Storage/Volume Encryption) เพื่อป้องกันการเข้าถึงข้อมูลระดับฮาร์ดแวร์โดยไม่ได้รับอนุญาต โดยมีคุณสมบัติ ดังนี้

๔.๔.๘.๑ มีระบบบริหารจัดการกุญแจเข้ารหัส (Key Management Service: KMS) ที่รองรับการเข้ารหัสฮาร์ดดิสก์เสมือน (vDisk) และพื้นที่จัดเก็บข้อมูลแบบวัตถุ (Object Storage)

๔.๔.๘.๒ รองรับมาตรฐานการเข้ารหัสขั้นต่ำ AES-256 หรือเทียบเท่า

๔.๔.๘.๓ อนุญาตให้ผู้ว่าจ้างสามารถบริหารจัดการวงจรชีวิตของกุญแจ (Key Lifecycle) หรือเป็นผู้ถือกุญแจเข้ารหัส (Customer-Managed Keys) ได้เอง เพื่อให้มั่นใจว่าผู้ให้บริการจะไม่สามารถเข้าถึงข้อมูลของผู้ว่าจ้างได้

๔.๕ ระบบบริหาร...

๔.๕ ระบบบริหารจัดการฐานข้อมูล

ผู้ให้บริการต้องจัดเตรียมบริการฐานข้อมูลแบบบริหารจัดการ เพื่อลดภาระการดูแลรักษาและโอนความเสี่ยงด้านการบริหารจัดการระบบให้แก่ผู้ให้บริการ โดยมีคุณสมบัติและขอบเขตความรับผิดชอบ ดังนี้

๔.๕.๑ ขอบเขตหน้าที่และจุดตัดความรับผิดชอบ

๔.๕.๑.๑ หน้าที่ของผู้ให้บริการ รับผิดชอบการบริหารจัดการในระดับ Database Engine และ Instance ซึ่งครอบคลุมถึงการติดตั้งซอฟต์แวร์ฐานข้อมูล, การปรับแต่งคุณสมบัติ (Configuration), การทำ Patch Management ทั้งในระดับระบบปฏิบัติการและซอฟต์แวร์ฐานข้อมูล การสำรองข้อมูลตามรอบเวลา และการจัดทำระบบความพร้อมใช้งานสูง (High Availability)

๔.๕.๑.๒ หน้าที่ของผู้พัฒนา ผู้ให้บริการไม่ต้องรับผิดชอบในส่วนของการออกแบบโครงสร้างตารางข้อมูล (Schema Design), การบริหารจัดการเนื้อหาข้อมูล (Data Content), การเขียนหรือแก้ไขชุดคำสั่ง SQL และการปรับแต่งประสิทธิภาพของคำสั่ง SQL (Query Optimization) ซึ่งถือเป็นความรับผิดชอบโดยตรงของผู้พัฒนาแต่ละราย

๔.๕.๒ ความเข้ากันได้ของซอฟต์แวร์ รองรับฐานข้อมูลมาตรฐานระดับองค์กร (Enterprise Grade) ที่เป็นที่นิยม อาทิ PostgreSQL, MySQL, SQL Server หรือ NoSQL ตามความเหมาะสมและความต้องการของแต่ละระบบงาน

๔.๕.๓ การบริหารจัดการและการบำรุงรักษา ผู้ให้บริการต้องดำเนินการดูแลรักษาระบบฐานข้อมูลอย่างครบวงจร ประกอบด้วยการปรับแต่งความปลอดภัย (OS & DB Hardening) ตามมาตรฐานสากล และการตั้งค่าการสำรองข้อมูลอัตโนมัติ (Automated Backup) ที่สามารถกู้คืนข้อมูลได้อย่างถูกต้องแม่นยำ

๔.๕.๔ ความมั่นคงปลอดภัยและความต่อเนื่อง ระบบต้องรองรับการทำงานแบบความพร้อมใช้งานสูง (High Availability: HA) เพื่อให้ธุรกิจดำเนินไปได้อย่างต่อเนื่อง และต้องเปิดใช้งานการเข้ารหัสข้อมูลทั้งในขณะจัดเก็บ (Encryption at Rest) และขณะรับส่งข้อมูล (Encryption in Transit) ตามมาตรฐานความปลอดภัยสารสนเทศ

๔.๕.๕ ข้อกำหนดพิเศษสำหรับธุรกรรมสำคัญ สำหรับฐานข้อมูลที่รองรับระบบงานที่มีความสำคัญสูง (เช่น ระบบใบส่งตัวอิเล็กทรอนิกส์, Health ID) ผู้ให้บริการต้องกำหนดค่าให้มีการทำสำเนาข้อมูลแบบทันที (Synchronous/Near-Real-time Replication) เพื่อให้มั่นใจว่าข้อมูลธุรกรรมล่าสุดจะสูญหายไม่เกินระยะเวลา (RPO) ที่กำหนดไว้ในตารางระดับการให้บริการ (SLA) ข้อ ๔.๑๑

๔.๕.๖ การป้องกันการผูกขาดทางเทคโนโลยี ซอฟต์แวร์ ระบบบริหารจัดการฐานข้อมูลหรือบริการ Platform as a Service (PaaS) ที่ผู้ให้บริการนำมาใช้เพื่อรองรับโครงการนี้ จะต้องอ้างอิงมาตรฐานเปิด (Open Standards) หรือเป็นซอฟต์แวร์ Open Source ที่เป็นที่นิยมและได้รับการยอมรับระดับสากล ห้ามมิให้ผู้ให้บริการบังคับใช้เทคโนโลยีที่มีลิขสิทธิ์ผูกขาดเฉพาะ (Proprietary Services) ซึ่งจะส่งผลให้ผู้ว่าจ้างไม่สามารถย้ายข้อมูลหรือระบบงาน (Migration) ไปยังผู้ให้บริการคลาวด์รายอื่นได้ในอนาคต เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้ว่าจ้าง

ทั้งนี้ ผู้ให้บริการต้องจัดทำรายงานการจัดการสินทรัพย์ (Asset Management Report) ที่ระบุรายละเอียดของ Database Version, OS Version, และ Configuration Version ให้เป็นปัจจุบันเสมอ

๔.๖ ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัย (SOC 24/7)

ผู้ยื่นข้อเสนอต้องจัดให้มีบริการเฝ้าระวังความปลอดภัยและตรวจจับภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดดังนี้

๔.๖.๑ เวลาทำการ ผู้ให้บริการให้บริการเฝ้าระวังภัยคุกคามตลอด ๒๔ ชั่วโมง

๔.๖.๒ บุคลากร

๔.๖.๒.๑ Tier 1...

๔.๖.๒.๑ Tier 1 (Security Monitor) เจ้าหน้าที่เฝ้าระวังประจำการตลอด ๒๔ ชั่วโมง

๔.๖.๒.๒ Tier 2/3 (Lead Analyst) หัวหน้าทีมวิเคราะห์ภัยคุกคามอย่างน้อย ๑ คน ต้องมีใบรับรองความเชี่ยวชาญระดับสากลที่ยังไม่หมดอายุ เช่น CompTIA CySA+, CISSP, GIAC (GCIH/GCIA) หรือเทียบเท่า

๔.๖.๒.๓ เจ้าหน้าที่ Tier 1, 2 และ 3 ต้องมีความสามารถในการสื่อสารและรายงานเหตุการณ์เป็นภาษาไทยได้อย่างคล่องแคล่วเพื่อประสานงานกับเจ้าหน้าที่เทคนิคของผู้ว่าจ้างได้ทันทีตลอด ๒๔ ชั่วโมง

๔.๖.๓ Threat Intelligence ผู้ให้บริการต้องใช้ฐานข้อมูลภัยคุกคามไม่ต่ำกว่า ๕ แหล่ง โดยต้องมีแหล่งข้อมูลเชิงพาณิชย์ (Commercial Feed) อย่างน้อย ๑ แหล่ง เพื่อความแม่นยำสูงสุด

๔.๖.๔ ระบบบริหารจัดการข้อมูลความมั่นคงปลอดภัย (SIEM Specification)

๔.๖.๔.๑ ต้องใช้ผลิตภัณฑ์ SIEM ที่ได้รับการจัดอันดับอยู่ในกลุ่ม Leader หรือ Challenger ในรายงาน Gartner Magic Quadrant for SIEM ฉบับปี ค.ศ. ๒๐๒๔ หรือปีล่าสุด

๔.๖.๔.๒ ระบบ SIEM ต้องมีความพร้อมใช้งาน (Availability) ไม่ต่ำกว่า ๙๙.๙๕% ต่อเดือน

๔.๖.๔.๓ สามารถเขียนเงื่อนไข (Rules) หรือกรณีการใช้งาน (Use Cases) เพิ่มเติมได้

๔.๖.๔.๔ สามารถวิเคราะห์แบบรวมศูนย์ (Correlation) เพื่อเชื่อมโยงเหตุการณ์ต่าง ๆ ได้

๔.๖.๕ การบริหารจัดการ Log และรายงาน

๔.๖.๕.๑ การค้นหาข้อมูล สามารถค้นหาข้อมูลดิบ (Raw Data) ย้อนหลังแบบ Online ได้อย่างน้อย ๓๐ วัน

๔.๖.๕.๒ การจัดเก็บตามกฎหมาย ผู้ให้บริการจัดเก็บ Log ไว้อย่างน้อย ๙๐ วัน ตาม พ.ร.บ. คอมพิวเตอร์ฯ และต้องป้องกันการแก้ไข (Tamper Proof)

๔.๖.๕.๓ การส่งข้อมูลจราจรคอมพิวเตอร์ไปยังระบบกลาง (Log Shipping / Forwarding) ระบบต้องรองรับการส่งข้อมูลจราจรคอมพิวเตอร์ (Log Forwarding) จากเครื่องแม่ข่ายเสมือนและอุปกรณ์ความปลอดภัย ไปยังระบบบริหารจัดการข้อมูลความมั่นคงปลอดภัยกลาง (Centralized SIEM/Log Server) ของกระทรวงสาธารณสุข หรือหน่วยงานภายนอกได้โดยอัตโนมัติ เพื่อป้องกันการแก้ไขหรือลบทำลายหลักฐาน

๔.๖.๕.๔ รายงานมาตรฐาน ผู้ให้บริการต้องสามารถจัดทำรายงานสอดคล้องกับมาตรฐาน ISO/IEC 27001, ISO/IEC 27799, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้

๔.๖.๖ SLA การตอบสนอง ผู้ให้บริการแจ้งเตือนเหตุการณ์ระดับ Critical ภายใน ๓๐ นาที และระดับ High ภายใน ๑ ชั่วโมง

๔.๖.๗ การทดสอบเจาะระบบ (Penetration Testing) ผู้ให้บริการต้องจัดให้มีการทดสอบเจาะระบบโดยผู้เชี่ยวชาญจากภายนอกอย่างน้อยปีละ ๑ ครั้ง ครอบคลุมระบบจัดการคลาวด์และ API Endpoints พร้อมส่งรายงานสรุปผลและแนวทางการแก้ไขให้ผู้ว่าจ้าง

โดยผู้ให้บริการต้องจัดทำรายงานผลการประเมินช่องโหว่ (Vulnerability Assessment Report) รายงานการเฝ้าระวัง (Monitoring Report) สำหรับการโจมตีทางไซเบอร์ และต้องจัดทำแผนผังขั้นตอนการยกระดับการแจ้งเตือนและการรับมือเหตุการณ์ (Incident Escalation Flow) อย่างเป็นลายลักษณ์อักษร

หมวดการบริหาร...

<u>หมวดการบริหารจัดการ</u>

๔.๗ การบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third-Party Risk Management)

ผู้ให้บริการต้องมีมาตรการบริหารจัดการความเสี่ยงที่เกิดจากผู้รับจ้างภายนอกหรือผู้รับจ้างช่วง ดังนี้

๔.๗.๑ การแจ้งและขออนุมัติการใช้ผู้รับจ้างช่วง

ห้ามมิให้ผู้ให้บริการว่าจ้างช่วงงานที่เกี่ยวข้องกับการเข้าถึงข้อมูลความลับ หรือข้อมูลส่วนบุคคลของผู้ว่าจ้างให้แก่บุคคลภายนอก โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ว่าจ้าง ในกรณีที่มีการเปลี่ยนแปลง หรือเพิ่มรายชื่อผู้รับจ้างช่วง ผู้ให้บริการต้องแจ้งให้ผู้ว่าจ้างทราบล่วงหน้าไม่น้อยกว่า ๓๐ วัน เพื่อให้ผู้ว่าจ้างมีสิทธิคัดค้านหากเห็นว่าผู้รับจ้างช่วงรายใหม่มีความเสี่ยงสูง

หากมีการเปลี่ยนแปลงทีมงานหรือผู้รับจ้างช่วง (Change Management) ผู้ให้บริการต้องรายงานและขออนุมัติต่อผู้ว่าจ้างก่อนดำเนินการ ทั้งนี้ ผู้ให้บริการต้องจัดทำข้อตกลงการรักษาความลับ (NDA) ในระดับองค์กร (Corporate NDA) กับผู้รับจ้างช่วง โดยผู้รับจ้างช่วงจะต้องมีมาตรการควบคุมและผูกพันพนักงานของตน (Employee Confidentiality Agreement) ไม่ให้เปิดเผยข้อมูลของผู้ว่าจ้าง และจำกัดสิทธิการเข้าถึงข้อมูลเฉพาะผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้น (Need-to-know basis)

๔.๗.๒ การส่งผ่านข้อกำหนดความมั่นคงปลอดภัย

ผู้ให้บริการต้องรับรองว่า สัญญาที่ทำกับผู้รับจ้างช่วงหรือผู้รับจ้างภายนอก จะต้องมีข้อกำหนดด้านความมั่นคงปลอดภัยข้อมูล และการคุ้มครองข้อมูลส่วนบุคคลไม่ต่ำกว่ามาตรฐานที่ระบุไว้ในสัญญาฉบับนี้ (เช่น ต้องทำ NDA, ต้องมีมาตรฐาน ISO, ต้องแจ้งเหตุละเมิดภายในเวลาที่กำหนด)

๔.๗.๓ สิทธิในการตรวจสอบ (Right to Audit)

ผู้ว่าจ้างสงวนสิทธิในการขอตรวจสอบ หรือขอเรียกดูรายงานผลการตรวจสอบอิสระ (เช่น SOC 2 Type II Report หรือ ISO 27001 Audit Report) ของผู้รับจ้างช่วง (Sub-contractors) ที่มีความสำคัญต่อระบบ (Critical Vendor) เพื่อประเมินความเสี่ยง

๔.๗.๔ การการกำหนดตารางความรับผิดชอบ

ผู้ให้บริการต้องจัดทำตารางความรับผิดชอบและอำนาจการตัดสินใจ (RACI Matrix) ระหว่างผู้ให้บริการ ผู้ว่าจ้าง และบุคคลภายนอก ทั้งนี้ ตาราง RACI ดังกล่าวจะต้องสอดคล้องและไม่ขัดแย้งกับเอกสารแนบท้ายตารางเมทริกซ์ความรับผิดชอบ (Shared Responsibility Matrix) ในข้อ ๑๔. ของเอกสารฉบับนี้ โดยเด็ดขาด โดยผู้ให้บริการหลักยังคงต้องมีภาระรับผิดชอบต่อระบบโดยรวม

๔.๗.๕ การจัดการช่องโหว่ของซอฟต์แวร์ภายนอก (Third-Party Vulnerability Management)

ผู้ให้บริการต้องมีกระบวนการติดตามและบริหารจัดการช่องโหว่ (Vulnerability Patching) ของซอฟต์แวร์ หรือไลบรารี (Libraries) ที่จัดหามาจากบุคคลภายนอก (รวมถึง Open Source Software) โดยต้องดำเนินการแก้ไขภายในระยะเวลาที่กำหนดใน SLA ทันทีที่ผู้ผลิตซอฟต์แวร์ต้นทางประกาศแพตช์

๔.๘ การบริหารจัดการการเปลี่ยนผ่าน

๔.๘.๑ การย้ายเข้าระบบใหม่

ผู้ชนะการเสนอราคา (รายใหม่) ต้องดำเนินการโอนย้ายข้อมูลจากผู้ให้บริการรายเดิมให้แล้วเสร็จภายใน ๖๐ วันนับถัดจากวันที่ได้รับหนังสือแจ้งให้เริ่มทำงาน โดยผู้ชนะการเสนอราคาต้องเป็นผู้รับผิดชอบค่าใช้จ่ายในการดำเนินการทั้งปวงซึ่งรวมถึง

๔.๘.๑.๑ ค่าบุคลากรและเครื่องมือในการนำเข้าข้อมูล (Data Ingestion)

๔.๘.๑.๒ ค่าเช่าใช้บริการระบบของผู้ให้บริการรายเดิม ในช่วงเวลาที่ต้องเปิดระบบขนานกัน (Parallel Run) เพื่อการทดสอบ หรือกรณีที่การโอนย้ายล่าช้ากว่ากำหนดสัญญาเดิม ผู้ให้บริการต้องจัดให้มีเจ้าหน้าที่เทคนิคสนับสนุนการเริ่มต้นใช้งาน (Onboarding Support) ให้แก่ผู้พัฒนาทุกราย รวมถึงการสนับสนุนการสร้าง VM Template มาตรฐานตามที่กระทรวงฯ กำหนด และการให้คำปรึกษาในการจัดตั้ง

VPC Isolation...

VPC Isolation เพื่อให้ผู้พัฒนาสามารถเริ่มดำเนินงานได้ทันทีหลังจากวันที่ได้รับหนังสือแจ้งให้เริ่มทำงาน

ทั้งนี้ กรณีมีการเปลี่ยนผ่าน ผู้ให้บริการต้องสนับสนุนการดำเนินการดังนี้

(๑) จัดทำแผนดำเนินการย้ายระบบ และแผนสำรอง (Rollback Plan) กรณีดำเนินการไม่แล้วเสร็จ โดยต้องได้รับอนุมัติจากคณะทำงานของผู้ว่าจ้างก่อนดำเนินการทุกครั้ง

(๒) แต่งตั้งผู้ประสานงานหลัก (Single Point of Contact) เพื่อให้ความช่วยเหลือ ติดตั้ง และแก้ไขปัญหา

(๓) ผู้ให้บริการต้องมีเครื่องมือหรือผู้เชี่ยวชาญในการจัดการ Image ข้อมูล และรองรับการแปลงรูปแบบ (Convert Image) ให้อยู่ในรูปแบบที่สามารถใช้งานได้ ในกรณีที่เทคโนโลยีระบบเดิมและระบบใหม่มีความไม่เข้ากัน

(๔) ในกรณีที่มีการส่งออกข้อมูล ผู้ให้บริการต้องจัดเตรียมพื้นที่บนคลาวด์หรืออุปกรณ์ทางกายภาพ (Physical Media/Storage) ถ่ายโอนข้อมูลเพื่อรองรับการส่งออกข้อมูล (Export) ในกรณีที่ผู้ว่าจ้างประสงค์จะย้ายหรือดำเนินการส่งออกข้อมูลไปยังผู้ให้บริการรายใหม่

๔.๘.๒ การย้ายออกเมื่อสิ้นสุดสัญญา

เมื่อสัญญาฉบับนี้สิ้นสุดลง หรือถูกบอกเลิกสัญญาไม่ว่าด้วยเหตุใด ๆ ผู้ให้บริการตกลงที่จะรับผิดชอบดำเนินการส่งคืนข้อมูลและสนับสนุนกระบวนการย้ายออกตามเงื่อนไขดังนี้

๔.๘.๒.๑ ความสามารถในการโอนย้ายข้อมูลและเครื่องแม่ข่ายเสมือน

(๑) ผู้ให้บริการต้องดำเนินการส่งออกข้อมูลทั้งหมด (Full Data Export) ในรูปแบบมาตรฐานสากลที่เป็นกลาง (Open Standard Format) อาทิ JSON, FHIR, DICOM หรือ SQL Dump ตามที่ผู้ว่าจ้างกำหนด

(๒) ผู้ให้บริการต้องสนับสนุนการส่งออกภาพลักษณ์ของเครื่องแม่ข่ายเสมือนทั้งหมด (VM Image Export) ในรูปแบบมาตรฐานที่ไม่ติดสิทธิ์การใช้งานเฉพาะ (Standard Virtual Appliance) อาทิ OVA (Open Virtual Appliance) หรือ OVF (Open Virtualization Format) เพื่อให้ผู้ว่าจ้างสามารถนำไปติดตั้งใช้งานต่อบนระบบคลาวด์อื่นหรือศูนย์ข้อมูลภายใน (On-premise) ได้ทันที

๔.๘.๒.๒ การงดเว้นค่าธรรมเนียมการนำข้อมูลออก

(๑) ผู้ให้บริการตกลงงดเว้นการเรียกเก็บค่าธรรมเนียมการนำข้อมูลออก (Data Egress Charges) ทั้งหมด โดยไม่มีเงื่อนไขด้านปริมาณข้อมูล รวมถึงไม่มีค่าธรรมเนียมการใช้ช่องสัญญาณ (Bandwidth Costs) หรือค่าบริการทางเทคนิคใด ๆ ที่เกี่ยวข้องกับการนำข้อมูลออกในช่วงเปลี่ยนผ่าน

(๒) ในกรณีที่ข้อมูลมีขนาดใหญ่เกินกว่าจะส่งผ่านระบบโครงข่ายได้ภายในระยะเวลาที่กำหนด ผู้ให้บริการต้องสนับสนุนการโอนย้ายข้อมูลผ่านสื่อบันทึกข้อมูลทางกายภาพ (Physical Data Transfer) ตามมาตรฐานความปลอดภัยที่ผู้ว่าจ้างยอมรับ

(๓) ผู้ให้บริการตกลงงดเว้นการเรียกเก็บค่าธรรมเนียมการรับส่งข้อมูลออก (Data Egress Charges) ทั้งหมดสำหรับการเชื่อมต่อภายในประเทศ เพื่อสนับสนุนการนำข้อมูลสุขภาพไปวิเคราะห์ต่อยอดด้วยระบบ AI ของหน่วยงานภายนอก โดยไม่มีข้อจำกัดด้านปริมาณข้อมูล

๔.๘.๒.๓ การสนับสนุนในช่วงเปลี่ยนผ่าน

(๑) ผู้ให้บริการตกลงให้การสนับสนุนทางเทคนิคแก่ผู้ว่าจ้างหรือผู้ให้บริการรายใหม่อย่างเต็มความสามารถ เพื่อให้การเชื่อมต่อและโอนย้ายระบบเป็นไปอย่างราบรื่น เป็นระยะเวลาไม่น้อยกว่า ๓๐ วัน นับจากวันที่สิ้นสุดสัญญา

(๒) ผู้ให้บริการตกลงไม่คิดค่าบริการด้านแรงงาน สำหรับการสนับสนุนในช่วงเปลี่ยนผ่านและการโอนย้ายข้อมูล

๔.๘.๓ การขยาย...

๔.๘.๓ การขยายระยะเวลาให้บริการกรณีพิเศษ

เมื่อครบกำหนดระยะเวลาสัญญา หรือช่วงเวลาสนับสนุนตามข้อ (๒) แล้ว หากผู้ว่าจ้างยังมีความจำเป็นต้องใช้งานระบบต่อไป ระหว่างรอการจัดหาผู้ให้บริการรายใหม่หรือรอการย้ายระบบ

๔.๘.๓.๑ ผู้ให้บริการต้องยินยอมให้บริการระบบ Cloud Computing ต่อไปภายใต้เงื่อนไขและมาตรฐานการให้บริการ (SLA) เดิม เป็นระยะเวลาไม่เกิน ๑๘๐ วัน นับจากวันสิ้นสุดสัญญา

๔.๘.๓.๒ การคิดค่าใช้จ่ายให้คำนวณตามอัตราค่าบริการเดิมในสัญญา (Pro-rate) เป็นรายวันหรือรายเดือนตามการใช้งานจริง

๔.๘.๔ ความรับผิดกรณีความล่าช้าในการย้ายออก

หากการโอนย้ายข้อมูลล่าช้าเนื่องจากความบกพร่องของผู้ให้บริการ (เช่น ส่งออกข้อมูลไม่สมบูรณ์, รูปแบบข้อมูลผิดพลาด หรือเจ้าหน้าที่ไม่เพียงพอ)

๔.๘.๔.๑ ผู้ให้บริการต้องรับผิดชอบค่าปรับและค่าเสียหายที่เกิดขึ้น รวมถึงรับผิดชอบค่าใช้จ่ายในการขยายเวลาการเช่าระบบของผู้ให้บริการรายใหม่ (ถ้ามี)

๔.๘.๔.๒ ผู้ให้บริการต้องให้บริการต่อไปจนกว่าการโอนย้ายจะแล้วเสร็จ โดยไม่มีสิทธิเรียกร้องค่าบริการเพิ่มเกินกว่าราคาตลาดหรือราคาตามสัญญาเดิม

๔.๘.๕ การทำลายข้อมูล

ภายหลังจากเสร็จสิ้นภารกิจการโอนย้ายข้อมูล หรือหลังจากสิ้นสุดระยะเวลาตามข้อ (๒) และ (๓) แล้ว

๔.๘.๕.๑ ระยะเวลา ผู้ให้บริการต้องดำเนินการลบ หรือทำลายข้อมูลทั้งหมดของผู้ว่าจ้างที่จัดเก็บบนระบบ Cloud Service โดยสมบูรณ์ ภายใน ๓๐ วัน

๔.๘.๕.๒ มาตรฐาน การทำลายข้อมูลต้องเป็นไปตามมาตรฐานสากล เช่น NIST SP 800-88 (Guidelines for Media Sanitization) หรือมาตรฐานอื่นที่เทียบเท่า เพื่อให้มั่นใจว่าข้อมูลไม่สามารถกู้คืนกลับมาได้

๔.๘.๕.๓ การทำลายกุญแจเข้ารหัส (Crypto-shredding) ในกรณีที่มีการใช้ระบบบริหารจัดการกุญแจเข้ารหัส (KMS) หรือการเข้ารหัสพื้นที่จัดเก็บข้อมูล ผู้ให้บริการต้องดำเนินการทำลายกุญแจเข้ารหัส (Cryptographic Keys) ที่ใช้สำหรับข้อมูลของผู้ว่าจ้างอย่างถาวร เพื่อให้มั่นใจว่าข้อมูลที่อาจตกค้างอยู่ในสื่อบันทึกข้อมูลทางกายภาพจะไม่สามารถถูกถอดรหัสหรือนำกลับมาใช้ใหม่ได้อีก ทั้งนี้การดำเนินการต้องไม่กระทบกับระบบการทำงานอื่น ๆ หรือข้อมูลอื่นของผู้ว่าจ้างที่ไม่ได้ประสงค์จะทำลาย

๔.๘.๕.๔ การรับรอง ผู้ให้บริการต้องจัดทำหนังสือรับรองการทำลายข้อมูล (Certificate of Data Destruction) พร้อมแนบรายงานบันทึกการทำลายกุญแจ (Key Destruction Audit Log) ส่งมอบให้ผู้ว่าจ้างภายใน ๑๐ วัน หลังจากดำเนินการแล้วเสร็จ

๔.๙ การบริการและสนับสนุนการบริหารจัดการระบบ

ผู้ให้บริการต้องจัดให้มีบริการบริหารจัดการระบบ และต้องเตรียมความพร้อมของระบบให้รองรับการบริหารจัดการโดยผู้ให้บริการเอง หรือโดยบุคคลที่สามตามความประสงค์ของผู้ว่าจ้าง โดยมีข้อกำหนดและขอบเขตการดำเนินงานดังนี้

๔.๙.๑ ขอบเขตหน้าที่ในการบริหารจัดการระบบ (Managed Services Roles) ในกรณีที่ผู้ว่าจ้างมอบหมายให้ผู้ให้บริการเป็นผู้ดูแลระบบ หรือในส่วนที่ต้องปฏิบัติงานร่วมกับบุคคลที่สาม ผู้ให้บริการต้องปฏิบัติหน้าที่ดังนี้

๔.๙.๑.๑ System Administration ดูแลรักษา ปรับแต่ง และอัปเดตระบบปฏิบัติการ (OS Patching) และซอฟต์แวร์พื้นฐานให้ทันสมัยและมั่นคงปลอดภัยอยู่เสมอ

๔.๙.๑.๒ Database ...

๔.๙.๑.๒ Database Administration ดูแลประสิทธิภาพ เสถียรภาพ และการสำรองข้อมูลของระบบฐานข้อมูลในระดับ Engine และ Instance (แต่ไม่รวมถึงการแก้ไขโครงสร้างข้อมูลภายในที่เกี่ยวข้องกับตรรกะของแอปพลิเคชัน)

๔.๙.๑.๓ Security Operation บริหารจัดการกฎและนโยบายความปลอดภัย (Rules/Policies) ของระบบป้องกันเครือข่าย อาทิ Firewall, WAF และการบริหารจัดการสิทธิ์ผู้ใช้งาน (User Management) ตามคำขอของผู้ว่าจ้าง

๔.๙.๑.๔ Monitoring & Incident Response เฝ้าระวัง แจ้งเตือน และแก้ไขปัญหาทางเทคนิคตลอด ๒๔ ชั่วโมง เพื่อให้ระบบมีความพร้อมใช้งานตามเกณฑ์ SLA ที่กำหนด

๔.๙.๑.๕ Resource Scaling ดำเนินการปรับเพิ่มหรือลดทรัพยากร (vCPU/RAM/Disk) ระหว่างรายเครื่องภายใต้กลุ่มทรัพยากรรวม (Resource Pool) ตามการใช้งานจริง และคำสั่งของผู้ว่าจ้าง

๔.๙.๒ กระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management) เพื่อลดความเสี่ยงจากการปฏิบัติงาน ผู้ให้บริการต้องดำเนินการภายใต้มาตรฐานดังนี้

๔.๙.๒.๑ ต้องจัดให้มีกระบวนการ Change Management ระดับ Normal, Standard, Emergency ที่เป็นลายลักษณ์อักษร โดยต้องแจ้งแผนการติดตั้ง Patch หรือการปรับเปลี่ยนค่าคุณสมบัติระบบให้ผู้ว่าจ้างและผู้พัฒนาซอฟต์แวร์ทราบล่วงหน้าอย่างน้อย ๗ วันทำการ

๔.๙.๒.๒ ต้องมีการแยกสภาพแวดล้อม (Environment Isolation) สำหรับการพัฒนา (Development), การทดสอบ (Testing), และการปฏิบัติงานจริง (Production) ออกจากกันอย่างเด็ดขาด และต้องทดสอบระบบให้เรียบร้อยก่อนนำมาปรับใช้บนสภาพแวดล้อมจริง

๔.๙.๓ การรองรับการบริหารจัดการโดยบุคคลที่สามและการบริหารจัดการผู้พัฒนาหลายราย

ผู้ว่าจ้างสงวนสิทธิ์ในการจ้างหรือแต่งตั้งบริษัทภายนอก เพื่อทำหน้าที่บริหารจัดการระบบแทนหรือร่วมกับผู้ให้บริการ โดยระบบคลาวด์ที่เสนอต้องรองรับการทำงานร่วมกันดังนี้

๔.๙.๓.๑ Granular IAM & Access Control รองรับการกำหนดสิทธิ์ตามบทบาท (RBAC) อย่างละเอียด เพื่อให้ผู้ว่าจ้างมอบสิทธิ์ระดับ Admin ให้แก่บุคคลที่สามได้โดยไม่ต้องใช้ Root Account ของผู้ให้บริการ และต้องรองรับการจัดการสิทธิ์ผ่านระบบ API Key Management หรือ OAuth 2.0 เพื่อควบคุมและบันทึกหลักฐานการเข้าถึงข้อมูลของระบบภายนอกได้อย่างแม่นยำ

๔.๙.๓.๒ Environment Isolation ต้องจัดสรรทรัพยากรและเครือข่ายเสมือนแยกส่วนออกจากกันอย่างชัดเจน (Isolate Virtual Network: VPC/VLAN) ตามรายโครงการหรือกลุ่มผู้พัฒนา เพื่อป้องกันการเข้าถึงข้อมูลข้ามโครงการและจำกัดขอบเขตความเสียหาย (Blast Radius)

๔.๙.๓.๓ Audit & Compliance ต้องจัดเก็บบันทึกกิจกรรม (Audit Logs) ของผู้ใช้งานทุกคนอย่างละเอียด ระบุตัวตน วันเวลา และกิจกรรมที่ดำเนินการได้ครบถ้วน เพื่อใช้เป็นหลักฐานตามมาตรฐานนิติวิทยาศาสตร์คอมพิวเตอร์

๔.๙.๓.๔ Delegated Support ต้องจัดให้มีช่องทางประสานงานเทคนิคหรือระบบเปิดใบงานแจ้งซ่อม (Ticketing System) ให้แก่บุคคลที่สามที่ได้รับมอบอำนาจ เพื่อให้สามารถประสานงานกับเจ้าหน้าที่ของผู้ให้บริการได้โดยตรงตลอด ๒๔ ชั่วโมง

๔.๙.๓.๕ Management APIs ต้องเปิดให้มีการเชื่อมต่อผ่าน API มาตรฐาน เพื่อให้เครื่องมือบริหารจัดการจากภายนอกสามารถดึงข้อมูลสถานะ ตรวจสอบประสิทธิภาพ หรือสั่งการระบบอัตโนมัติได้

๔.๙.๓.๖ Technical Account Manager (TAM) ผู้ให้บริการต้องจัดให้มีวิศวกรประสานงานโครงการ เพื่อเป็นตัวกลางในการประชุมร่วมระหว่างผู้ว่าจ้าง ผู้พัฒนา และบริษัทบุคคลที่สาม อย่างน้อยเดือนละ ๑ ครั้ง หรือตามเหตุการณ์สำคัญ เพื่อความบูรณาการในการแก้ไขปัญหา

หมวดการวัดผล...

<u>หมวดการวัดผล</u>

๔.๑๐ การทดสอบและการเฝ้าระวังระบบ

๔.๑๐.๑ Load Testing ต้องทำการทดสอบประสิทธิภาพระบบภายใต้ภาระงานสูง (Load Testing) ก่อนการส่งมอบงานงวดที่ ๑ หรือหลังการโอนย้ายข้อมูลเสร็จสิ้น ตามสถานการณ์จำลองที่ผู้ว่าจ้างกำหนด (เช่น รองรับ Concurrent Users ๑๐,๐๐๐ คน) ผลการทดสอบต้องแสดงให้เห็นว่าระบบยังสามารถตอบสนองได้ (Response Time) ภายในเกณฑ์ หากไม่ผ่านต้องปรับจูน (Tuning) หรือเพิ่มทรัพยากรโดยไม่มีค่าใช้จ่ายเพิ่มเติม

๔.๑๐.๒ ระบบติดตามสถานะและบริหารจัดการออนไลน์ (Centralized Monitoring & Dashboard) ผู้ให้บริการต้องจัดเตรียมเครื่องมือในการติดตามสถานะ (Monitoring Tools) ที่มีขีดความสามารถในการจัดเก็บข้อมูลประสิทธิภาพ (Performance & Resource Utilization), ความมั่นคงปลอดภัย (Security & Log), สถานะการสำรองข้อมูล (Backup/DR), และปริมาณการใช้งานเครือข่าย (Bandwidth) ได้อย่างครบถ้วน ทั้งนี้ ข้อมูลที่ได้จากระบบเฝ้าระวังทั้งหมด ผู้ให้บริการจะต้องนำมาจัดทำเป็นรายงานผลการดำเนินงาน และส่งมอบให้แก่ผู้ว่าจ้างตามรายละเอียดและหัวข้อที่กำหนดบังคับไว้ใน ข้อ ๖.๒ (รายละเอียดงานที่ส่งมอบในแต่ละงวด) อย่างเคร่งครัด

๔.๑๐.๓ ระบบติดตามและแจ้งเตือนสถานะโครงสร้างพื้นฐาน

ผู้ให้บริการต้องจัดเตรียมเครื่องมือสำหรับติดตามสถานะการทำงานของทรัพยากรระบบ (Infrastructure Monitoring) ให้แก่ผู้ว่าจ้าง โดยมีคุณสมบัติดังนี้

๔.๑๐.๓.๑ สามารถตรวจสอบสถานะการทำงานของ CPU, Memory, Disk Usage, Network Traffic (In/Out) และ Disk I/O ของเครื่องแม่ข่ายเสมือน (VM) แต่ละเครื่องได้อย่างละเอียด

๔.๑๐.๓.๒ สามารถตั้งค่าการแจ้งเตือน (Threshold Alerting) เมื่อมีการใช้งานทรัพยากรเกินกำหนด (เช่น CPU สูงเกิน ๙๐%) ผ่านทาง Email, SMS หรือ LINE Notify ได้

๔.๑๐.๓.๓ มีระบบเก็บข้อมูลประวัติการใช้งานทรัพยากรย้อนหลังไม่น้อยกว่า ๑ ปี เพื่อใช้ในการวิเคราะห์แนวโน้มและวางแผนขยายระบบ

๔.๑๐.๔ Incident Reporting เมื่อเกิดภัยคุกคาม ต้องจัดทำรายงานประกอบด้วย

๔.๑๐.๔.๑ ประเภทภัยคุกคาม, วัน - เวลาที่พบ

๔.๑๐.๔.๒ Source/Destination IP, อุปกรณ์ที่ได้รับผลกระทบ, ระดับความรุนแรง

๔.๑๐.๔.๓ รายละเอียดเหตุการณ์ และคำแนะนำ/ขั้นตอนการแก้ไข

๔.๑๐.๕ Monthly Meeting ส่งรายงานสรุปผลรายเดือน (รายงาน SLA, รายงานความปลอดภัย, และรายงานการใช้ทรัพยากร) และเข้าร่วมประชุมเพื่อชี้แจงความก้าวหน้า

๔.๑๐.๖ Service Support

๔.๑๐.๖.๑ ระบุช่องทางติดต่อสำหรับแจ้งปัญหา ๒๔ ชั่วโมง

๔.๑๐.๖.๒ การแก้ไขปัญหาและตอบสนอง ให้เป็นไปตามตาราง SLA ที่กำหนด (ในข้อ ๔.๑๑)

๔.๑๑ ข้อกำหนด...

๔.๑๑ ข้อกำหนดระดับการให้บริการ (Service Level Agreement: SLA)

ผู้ให้บริการต้องให้บริการโดยยึดถือเกณฑ์มาตรฐานและกรอบเวลาตามตารางดังนี้

ระดับความรุนแรง	คำอธิบาย	เวลาตอบสนอง (Response Time)	เวลาแก้ไขแล้วเสร็จ (Resolution Time / RTO)
Critical	**ระบบหยุดทำงานโดยสิ้นเชิง (System Down)** - ผู้ใช้งานทั้งหมดไม่สามารถเข้าถึงระบบ Digital Health Platform ได้ - บริการหลักหยุดชะงัก (เช่น ไม่สามารถดึงข้อมูลข้ามโรงพยาบาลได้เลย) - กรณีเกิดภัยพิบัติที่ต้องกู้คืนระบบ (Disaster Recovery)	๓๐ นาที	- System Down (Non-Disaster) แก้ไขภายใน ๖ ชั่วโมง (เช่น Server Hang, Service Stop) - Disaster Recovery (Site Failover) กู้คืนภายใน ๑๒ ชั่วโมง (เช่น ไฟไหม้, น้ำท่วม DC หลัก)
High	**ประสิทธิภาพลดลงอย่างรุนแรง/ฟังก์ชันหลักใช้งานไม่ได้** - ผู้ใช้งานสามารถเข้าระบบได้ แต่ฟังก์ชันสำคัญไม่ทำงาน (เช่น หน้า Dashboard ไม่แสดงผล, ระบบ Refer ส่งข้อมูลไม่ได้) - การซิงค์ข้อมูลล้มเหลวเป็นวงกว้าง (กระทบหน่วยบริการ > ๒๐%) - ระบบตอบสนองช้ามากจนเป็นอุปสรรคต่อการใช้งาน	๑ ชั่วโมง	๑๒ ชั่วโมง
Medium	**ข้อบกพร่องบางส่วน/กระทบวงจำกัด** - ฟังก์ชันรองใช้งานไม่ได้หรือทำงานผิดพลาด - ปัญหาเกิดขึ้นเฉพาะกับหน่วยบริการบางแห่งหรือผู้ใช้บางกลุ่ม - ระบบยังสามารถทำงานต่อได้โดยใช้วิธีอื่น (Workaround Available)	๒ ชั่วโมง	๒๔ ชั่วโมง

ระดับ...

ระดับความรุนแรง	คำอธิบาย	เวลาตอบสนอง (Response Time)	เวลาแก้ไขแล้วเสร็จ (Resolution Time / RTO)
Low	**ข้อบกพร่องเล็กน้อย/การสอบถามข้อมูล** - ปัญหาความสวยงาม, การแสดงผลหน้าจอผิดเพี้ยนเล็กน้อย - การสอบถามวิธีการใช้งาน (General Inquiry) - การขอข้อมูล Log หรือรายงานทั่วไป	๔ ชั่วโมง	๕ วันทำการ

เงื่อนไขเพิ่มเติมในการคำนวณ SLA

(๑) การเริ่มนับเวลาหยุดชะงัก (Downtime) ให้เริ่มนับตั้งแต่ระบบเฝ้าระวัง (Monitoring) ของผู้ให้บริการหรือของผู้ว่าจ้างตรวจพบความผิดปกติ หรือระบบไม่สามารถให้บริการได้ตามปกติ ไม่ให้นับจากเวลาที่ผู้ว่าจ้างเปิดใบงานแจ้งซ่อม (Open Ticket)

(๒) การหยุดระบบเพื่อบำรุงรักษาตามวาระ (Planned Maintenance) จะต้องแจ้งผู้ว่าจ้างเป็นลายลักษณ์อักษรล่วงหน้าไม่น้อยกว่า ๗ วัน และอนุญาตให้ดำเนินการได้ไม่เกิน ๔ ชั่วโมงต่อเดือน ในช่วงเวลาที่มีการใช้งานต่ำสุด (Off-peak) หากใช้เวลาเกินกว่าที่กำหนด หรือดำเนินการโดยไม่ได้รับอนุมัติล่วงหน้า ให้นำเวลาที่เกินดังกล่าวมาคำนวณรวมเป็นเวลาหยุดชะงัก (Downtime) ทันที

หมายเหตุ

(๑) การนับเวลาแก้ไข เริ่มนับตั้งแต่เวลาที่ผู้ให้บริการได้รับแจ้งเหตุ หรือเวลาที่ระบบตรวจพบความผิดปกติ จนถึงเวลาที่ระบบกลับมาให้บริการได้ตามปกติ หรือมีวิธีการแก้ไขชั่วคราวที่ผู้ว่าจ้างยอมรับได้

(๒) ข้อยกเว้น ระยะเวลาในการแก้ไขปัญหานี้ ไม่รวมถึงความล่าช้าที่เกิดจากปัจจัยภายนอกที่อยู่นอกเหนือการควบคุมของผู้ให้บริการ เช่น ระบบอินเทอร์เน็ตของโรงพยาบาลปลายทางล่ม, ระบบ HIS ของโรงพยาบาลต้นทางขัดข้อง หรือเหตุสุดวิสัยอื่น ๆ

(๓) เกณฑ์การกู้คืนระบบกรณีภัยพิบัติ ในกรณีที่เกิดเหตุขัดข้องรุนแรงจนต้องมีการประกาศใช้แผนกู้คืนระบบ (Disaster Recovery Plan) ให้ยึดถือเกณฑ์มาตรฐาน ดังนี้

- RPO (Recovery Point Objective) ข้อมูลสูญหายได้ไม่เกิน ๒๔ ชั่วโมง (ยึดตามรอบการสำรองข้อมูลรายวัน)
- RTO (Recovery Time Objective) ระบบต้องกลับมาพร้อมใช้งานภายใน ๑๒ ชั่วโมง

(๔) ผู้ให้บริการต้องรักษาระดับค่าเฉลี่ยเวลาในการแก้ไขปัญหา (Mean Time To Recovery: MTTR) สำหรับเหตุการณ์ความรุนแรงระดับสูง (High Severity) ให้ไม่เกิน ๖ ชั่วโมงต่อเดือน

๔.๑๒ การเชื่อมโยงกับระบบบริหารจัดการคลาวด์กลาง

ผู้ให้บริการรองรับการเชื่อมโยงระบบคลาวด์กับระบบบริหารจัดการคลาวด์กลาง (Cloud Management Platforms) ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) ผ่านช่องทาง API เพื่อเชื่อมโยงข้อมูลได้ ดังนี้

๔.๑๒.๑ ข้อมูลการบริหารจัดการทรัพยากรคลาวด์

๔.๑๒.๒ ข้อมูลการคำนวณค่าใช้จ่ายตามการใช้งานจริง (Pay per use)

๔.๑๒.๓ ข้อมูลการใช้งานทรัพยากรระบบคลาวด์

๔.๑๒.๔ การปฏิบัติตามมาตรฐานและโปรโตคอลที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) กำหนด

๔.๑๓ นโยบาย...

๔.๑๓ นโยบายและแนวปฏิบัติเพิ่มเติมตามมาตรฐานคลาวด์

ผู้ให้บริการต้องดำเนินการและส่งมอบเอกสารนโยบายดังต่อไปนี้ให้แก่ผู้ว่าจ้าง

๔.๑๓.๑ การซิงโครไนซ์นาฬิกา (Clock Synchronization) ระบบทั้งหมดภายใต้การให้บริการต้องมีการตั้งค่าและซิงโครไนซ์เวลามาตรฐาน (NTP) ให้ตรงกัน เพื่อความถูกต้องในการตรวจสอบเหตุการณ์ทางไซเบอร์

๔.๑๓.๒ นโยบายและขั้นตอนปฏิบัติในการถ่ายโอนข้อมูล (Information Transfer Policies and Procedures)

๔.๑๓.๓ นโยบายการพัฒนาที่ปลอดภัย (Secure Development Policy)

๔.๑๓.๔ นโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)

๕. ระยะเวลาการดำเนินการ

ระยะเวลา ๑๒ เดือน นับถัดจากวันที่ได้รับหนังสือแจ้งให้เริ่มทำงาน

๖. การส่งมอบงานและการจ่ายเงิน

ผู้ให้บริการจะได้รับค่าจ้างแบ่งเป็น ๑๒ งวด (รายเดือน) งวดละเท่า ๆ กัน โดยจะชำระเมื่อผู้ให้บริการได้ส่งมอบงานและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุเรียบร้อยแล้ว ตามรายละเอียดดังนี้

๖.๑ กำหนดการส่งมอบงาน

ผู้ให้บริการต้องส่งมอบงานภายในวันที่ ๑๕ ของเดือนถัดไป (หรือภายใน ๓๐ วันนับถัดจากวันที่ได้รับหนังสือแจ้งให้เริ่มทำงาน สำหรับงวดที่ ๑) หากตรงกับวันหยุดราชการให้เลื่อนเป็นวันทำการถัดไป

๖.๒ รายละเอียดงานที่ส่งมอบในแต่ละงวด

ผู้ให้บริการต้องจัดทำและส่งมอบรายงานผลการดำเนินงานประจำเดือน โดยต้องมีเนื้อหาครอบคลุมหัวข้อดังต่อไปนี้เป็นอย่างน้อย

๖.๒.๑ เอกสารที่ต้องส่งมอบทุกงวดเดือน

(๑) รายงานระดับการให้บริการ (SLA) และประสิทธิภาพ (Performance & Resource Utilization Report)

- แสดงค่าความพร้อมใช้งาน (Availability/Uptime) และสรุปยอดค่าปรับ (ถ้ามี)
- แสดงปริมาณการใช้งานทรัพยากร (vCPU, RAM, Storage) และระยะเวลาการตอบสนอง (Response Time)
- แสดงปริมาณการใช้งานเครือข่ายและแบนด์วิดท์ (Bandwidth & Quota Management)

(๒) รายงานความมั่นคงปลอดภัย (Monthly Security & SOC Report)

- สรุปสถิติภัยคุกคามที่ตรวจพบและการบล็อกการโจมตี (Threat Summary)
- รายงานเหตุการณ์ผิดปกติและการยกระดับการแจ้งเตือน (Incident Escalation Report)
- ผลการสแกนช่องโหว่ (Vulnerability Scan Result) และสถานะการติดตั้ง Patch

(๓) รายงานการสำรองข้อมูลและการกู้คืน (Backup & DR Report)

- สถานะความสำเร็จ/ล้มเหลว ของการสำรองข้อมูลรายวัน
- รายงานการประเมินความสอดคล้องของระยะเวลา RTO, RPO และ Retention Period ตามเกณฑ์ที่กำหนด

(๔) รายงานการจัดการสิทธิการเข้าถึงและสินทรัพย์ (IAM & Asset Management Report)

- ตารางสิทธิผู้ใช้งาน...

- ตารางสิทธิผู้ใช้งาน (User Right Matrix) ปัจจุบัน
- รายงานสถานะการเข้าถึงเครื่องแม่ข่ายของผู้ดูแลระบบ (PAM Access Log)
- รายงานการจัดการสินทรัพย์ (Asset Management) ระบุ Database Version, OS Version, และ Configuration Version

(๕) รายงานอุบัติการณ์และการแจ้งปัญหา ให้จัดส่งเฉพาะกรณีที่มีเหตุการณ์ผิดปกติเกิดขึ้นในเดือนนั้น โดยต้องระบุรายละเอียดเชิงลึก (Root Cause Analysis), Timeline การแก้ไข, และแนวทางป้องกันการเกิดซ้ำ

๖.๒.๒ เอกสารที่ส่งมอบเฉพาะงวด

- งวดที่ ๑

(๑) แผนผังสถาปัตยกรรมระบบ (Architecture Diagram) และ Network & Logical Diagram (แสดง Zone/Segmentation)

(๒) เอกสารคู่มือการใช้งาน Cloud Portal

(๓) แผนการเปลี่ยนผ่านระบบ (Transition Plan)

(๔) แผนบริหารความเสี่ยงห่วงโซ่อุปทาน (Supply Chain Risk Management Plan)

(๕) ข้อตกลงการรักษาความลับ (NDA) ของผู้ให้บริการและผู้รับจ้างช่วง (ระดับองค์กร)

(๖) แผนผังขั้นตอนการยกระดับการแจ้งเตือน (Incident Escalation Flow)

(๗) ตารางกำหนดความรับผิดชอบ (RACI Matrix)

(๘) เอกสารนโยบายความปลอดภัยตามข้อ ๔.๑๓

- งวดที่ ๖ และ ๑๒ (หรือตามตกลง)

(๑) รายงานผลการซ้อมแผนกู้คืนระบบ (DR Drill Report) ต้องประกอบด้วยหลักฐานเชิงประจักษ์ ได้แก่

- บันทึกเหตุการณ์ (Log Files) ที่แสดงช่วงเวลาการสลับระบบ (Failover) และการกู้คืน (Failback) ภาพถ่ายหน้าจอ (Screenshots) ขณะระบบสำรองทำงาน
- ผลการทดสอบการใช้งานข้อมูลบนระบบสำรอง (Data Integrity Check)
- สรุปเวลาที่ใช้จริง (Actual RTO/RPO) เปรียบเทียบกับค่าเป้าหมาย

๖.๓ รูปแบบการส่งมอบเอกสาร

ผู้ให้บริการต้องส่งมอบเอกสารในรูปแบบเอกสารและไฟล์อิเล็กทรอนิกส์ (PDF และ Editable File เช่น .docx/.xlsx) ผ่านช่องทางที่ผู้ว่าจ้างกำหนด หรือบันทึกลงสื่อบันทึกข้อมูล จำนวน ๒ ชุด

๖.๔ การส่งมอบสิทธิ์เข้าถึงระบบติดตามสถานะ

นอกเหนือจากการส่งมอบงานรายเดือน ผู้ให้บริการต้องเปิดสิทธิ์ให้ผู้ว่าจ้างสามารถเข้าถึงระบบติดตามสถานะและบริหารจัดการออนไลน์ ตามคุณลักษณะที่กำหนดไว้ในข้อ ๔.๑๐ (๒) ได้ตลอด ๒๔ (ยี่สิบสี่) ชั่วโมง ตลอดอายุสัญญา

๖.๕ เงื่อนไขการจ่ายเงิน การจ่ายเงินแต่ละงวดจะเกิดขึ้นเมื่อ

๖.๕.๑ ผู้ให้บริการได้ส่งมอบเอกสารและรายงานผลการดำเนินงานครบถ้วน ถูกต้องตามรายการที่ระบุในข้อ ๖.๒

๖.๕.๒ คณะกรรมการตรวจรับพัสดุได้ทำการตรวจรับงานเรียบร้อยแล้ว และเห็นว่าการดำเนินงานเป็นไปตามขอบเขตของงานและเงื่อนไขในสัญญา

๖.๕.๓ การพิจารณา...

๖.๕.๓ การพิจารณาผลระดับการให้บริการ (SLA)

๖.๕.๓.๑ ในกรณีที่ผู้ให้บริการปฏิบัติตาม SLA ด้านความพร้อมใช้งาน (Availability) ได้ไม่ต่ำกว่าร้อยละ ๙๙.๙๕ ในเดือนนั้น ผู้ว่าจ้างจะจ่ายเงินค่าจ้างเต็มจำนวน

๖.๕.๓.๒ ในกรณีที่ SLA ด้านความพร้อมใช้งาน (Availability) ต่ำกว่าร้อยละ ๙๙.๙๕ หรือมีการปฏิบัติผิดเงื่อนไข SLA อื่น ๆ ผู้ว่าจ้างจะดำเนินการหักค่าปรับตามหลักเกณฑ์และอัตราที่ระบุไว้ในข้อ ๘.๒ ออกจากค่าจ้างในงวดนั้น

๖.๕.๔ หากยอดค่าปรับมีจำนวนสูงกว่าค่าจ้างในงวดนั้น ให้ผู้ว่าจ้างมีสิทธินำยอดส่วนที่เหลือไปหักออกจากค่าจ้างในงวดถัดไป หรือหากเป็นงวดสุดท้าย ให้ผู้ให้บริการนำเงินมาชำระคืนให้แก่ผู้ว่าจ้างจนครบถ้วนภายในระยะเวลาที่กำหนด

๗. หลักเกณฑ์การพิจารณาข้อเสนอ

พิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ โดยใช้เกณฑ์ราคา (Price) ภายใต้เงื่อนไขผู้ยื่นข้อเสนอต้องผ่านการพิจารณาคุณสมบัติและข้อเสนอด้านเทคนิคครบถ้วน

๘. อัตราค่าปรับ

๘.๑ ค่าปรับกรณีส่งมอบงานล่าช้า

ในกรณีที่ผู้ให้บริการไม่สามารถส่งมอบงาน (เอกสารรายงานต่าง ๆ) ได้ภายในกำหนดเวลาตามข้อ ๖.๑ ผู้ให้บริการยินยอมให้ปรับเป็นรายวัน ในอัตราร้อยละ ๐.๑๐ (ศูนย์จุดหนึ่งศูนย์) ของมูลค่าสัญญา นับถัดจากวันครบกำหนดจนถึงวันที่ส่งมอบงานครบถ้วน

๘.๒ ค่าปรับกรณีไม่ปฏิบัติตาม SLA

ในกรณีที่ผู้ให้บริการไม่สามารถให้บริการได้ตามเกณฑ์มาตรฐาน (SLA) ที่กำหนดไว้ในข้อ ๔.๑๑ ผู้ให้บริการยินยอมให้หักเงินค่าจ้างในงวดนั้น ๆ โดยปรับในอัตราร้อยละ ๐.๑๐ ต่อวันของมูลค่าสัญญา (หรือเทียบเท่ามูลค่าความเสียหายที่คำนวณได้จริง) จนกว่าระบบจะกลับมาใช้งานได้ปกติ ทั้งนี้ ยอดรวมค่าปรับต้องไม่เกินวงเงินค่างวดประจำเดือนนั้น

๘.๓ เงื่อนไขการงดหรือลดค่าปรับ

ผู้ให้บริการจะไม่ถูกปรับในกรณีที่เหตุล่าช้าหรือความเสียหายเกิดจาก

๘.๓.๑ เหตุสุดวิสัย (Force Majeure) เช่น ภัยธรรมชาติ สงคราม จลาจล โรคระบาดร้ายแรง

๘.๓.๒ ความผิดของผู้ว่าจ้างเอง (เช่น เจ้าหน้าที่ผู้ว่าจ้างตั้งค่าผิด)

๘.๓.๓ เหตุปัจจัยภายนอกที่ไม่อาจควบคุมได้และไม่ใช่ความผิดของผู้ให้บริการ (เช่น ระบบอินเทอร์เน็ตของผู้ว่าจ้างล่มเอง)

๘.๔ สิทธิในการบอกเลิกสัญญา

นอกเหนือจากสิทธิในการบอกเลิกสัญญาตามกฎหมายทั่วไปแล้ว ผู้ว่าจ้างทรงไว้ซึ่งสิทธิที่จะบอกเลิกสัญญาฉบับนี้ได้ทันที โดยมิต้องแจ้งล่วงหน้า และมีสิทธิริบหลักประกันสัญญา รวมถึงเรียกร้องค่าเสียหายจากผู้ให้บริการ หากเกิดกรณีใดกรณีหนึ่ง ดังต่อไปนี้

๘.๔.๑ ความล้มเหลวในการให้บริการอย่างร้ายแรง

๘.๔.๑.๑ ผู้ให้บริการมีระดับความพร้อมใช้งาน (Availability) ต่ำกว่าร้อยละ ๙๙.๐๐ (๙๙.๐๐%) เป็นเวลา ๒ เดือนติดต่อกัน หรือ

๘.๔.๑.๒ ผู้ให้บริการมีระดับความพร้อมใช้งาน (Availability) ต่ำกว่าร้อยละ ๙๙.๐๐ (๙๙.๐๐%) รวมกันเกิน ๓ ครั้ง ภายในระยะเวลา ๑ ปีของสัญญา

๘.๔.๒ การละเมิด...

๘.๔.๒ การละเมิดความมั่นคงปลอดภัยอย่างร้ายแรง

๘.๔.๒.๑ เกิดเหตุข้อมูลรั่วไหลหรือข้อมูลสูญหายที่ส่งผลกระทบต่อข้อมูลส่วนบุคคลหรือข้อมูลความลับของผู้ว่าจ้าง โดยมีสาเหตุจากความประมาทเลินเล่ออย่างร้ายแรง หรือความบกพร่องในมาตรการรักษาความมั่นคงปลอดภัยของผู้ให้บริการ

๘.๔.๒.๒ ผู้ให้บริการปกปิดข้อมูล หรือรายงานข้อมูลเท็จเกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

๘.๔.๓ การไม่ปฏิบัติตามข้อกำหนดทางกฎหมาย

๘.๔.๓.๑ ผู้ให้บริการนำข้อมูลของผู้ว่าจ้างไปแสวงหาผลประโยชน์ ไปขาย หรือนำไปประมวลผลนอกเหนือจากวัตถุประสงค์แห่งสัญญานี้

๘.๔.๓.๒ ผู้ให้บริการฝ่าฝืนข้อกำหนดเรื่องสถานที่จัดเก็บข้อมูล (Data Residency) โดยลักลอบส่งข้อมูลออกนอกราชอาณาจักรไทยโดยไม่ได้รับอนุญาต

๘.๔.๔ การโอนสิทธิหรือช่วงงานโดยมิชอบ

๘.๔.๔.๑ ผู้ให้บริการนำงานทั้งหมดหรือส่วนสำคัญแห่งสัญญาไปจ้างช่วง (Sub-contract) ให้ผู้อื่นทำแทน หรือโอนสิทธิเรียกร้องตามสัญญานี้ให้แก่บุคคลภายนอก โดยไม่ได้รับความยินยอมเป็นหนังสือจากผู้ว่าจ้าง

๘.๔.๕ ปัญหาด้านสถานะของกิจการ

๘.๔.๕ ผู้ให้บริการตกเป็นบุคคลล้มละลาย หรือถูกพิทักษ์ทรัพย์ หรือประสบปัญหาทางการเงินจนทำให้เชื่อได้ว่าไม่สามารถให้บริการต่อไปได้ตามสัญญา

๙. งบประมาณ

งบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๙ งบดำเนินงาน แผนงานบูรณาการรัฐบาลดิจิทัลจำนวนเงิน ๘๔,๐๐๐,๐๐๐ บาท (แปดสิบสี่ล้านบาทถ้วน)

๑๐. การรับประกันความชำรุดบกพร่องของงานจ้าง

๑๐.๑ ผู้ให้บริการต้องรับประกันการให้บริการตามรายละเอียดขอบเขตของงานภายในกำหนดระยะเวลา ๑ ปี นับถัดจากวันที่ได้รับมอบงานดังกล่าว รวมถึงการย้ายระบบต่าง ๆ ที่อยู่บน Cloud Computing ของผู้ว่าจ้างรายเดิม

๑๐.๒ ระยะเวลาการรับประกันเริ่มต้นเมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานเรียบร้อยครบถ้วน

๑๐.๓ หากมีเหตุชำรุดบกพร่องหรือเสียหายเกิดขึ้นแก่ระบบ ซึ่งความชำรุดบกพร่องหรือเสียหายนั้นเกิดจากความบกพร่องของผู้ให้บริการ ผู้ให้บริการต้องรีบทำการแก้ไขให้ระบบใช้งานได้ตามปกติภายใน SLA ที่ระบุไว้ นับถัดจากเวลาที่ได้รับแจ้งเหตุ โดยผู้ให้บริการไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

ในกรณีเร่งด่วนจำเป็นต้องรีบแก้ไขเหตุชำรุดบกพร่องหรือเสียหายโดยเร็ว และไม่อาจรอให้ผู้ให้บริการแก้ไขในระยะเวลาที่กำหนดไว้ได้ ผู้ว่าจ้างมีสิทธิเข้าจัดการแก้ไขเหตุชำรุดบกพร่องหรือเสียหายนั้นเอง หรือจ้างผู้อื่นให้ซ่อมแซมความชำรุดบกพร่องหรือเสียหาย โดยผู้ให้บริการต้องรับผิดชอบชำระค่าใช้จ่ายทั้งหมดแก่ผู้ว่าจ้าง ที่ผู้ว่าจ้างได้ชำระไปก่อนหน้าทั้งสิ้น

๑๑. ทรัพย์สินทางปัญญา

๑๑.๑. สิทธิในทรัพย์สินทางปัญญาที่มีอยู่เดิม

ทรัพย์สินทางปัญญา ความลับทางการค้า เทคโนโลยี องค์ความรู้และข้อมูลที่คู่สัญญาฝ่ายใดฝ่ายหนึ่งเป็นเจ้าของอยู่ก่อนการดำเนินงานโครงการนี้ ให้ยังคงเป็นกรรมสิทธิ์ของฝ่ายนั้น แม้จะนำมาใช้ในการดำเนินงานโครงการนี้ก็ตาม การดำเนินงานตามโครงการนี้ไม่ถือเป็นการอนุญาตให้คู่สัญญาฝ่ายหนึ่งฝ่ายใดมีสิทธิใช้ประโยชน์จากทรัพย์สินทางปัญญาของอีกฝ่ายนอกเหนือไปจากขอบเขตที่ระบุไว้ในสัญญาเว้นแต่จะได้ตกลงกันเป็นลายลักษณ์อักษร

๑๑.๒. สิทธิในทรัพย์สิน...

๑๑.๒. สิทธิในทรัพย์สินทางปัญญาที่พัฒนาร่วมกัน

ทรัพย์สินทางปัญญาหรือลิขสิทธิ์ใด ๆ ที่เกิดขึ้นจากการร่วมกันพัฒนาของทั้งสองฝ่ายในระหว่างการดำเนินงานโครงการนี้ ให้ถือเป็นกรรมสิทธิ์ร่วมของทั้งสองฝ่าย โดยแต่ละฝ่ายมีสิทธินำไปพัฒนาต่อยอดได้ แต่ต้องไม่กระทบต่อสิทธิของอีกฝ่ายที่มีอยู่หรือจะเกิดขึ้นในอนาคต เว้นแต่ ในกรณีที่เป็นชุดคำสั่ง (Scripts), โค้ดสำหรับการตั้งค่าระบบ (Configuration Code), เครื่องมือ (Tools), หรือกระบวนการทางเทคนิค (Methodologies) ที่ผู้ให้บริการได้นำมาใช้เพื่อสนับสนุนการติดตั้ง หรือบริหารจัดการระบบภายใต้สัญญาฉบับนี้ ซึ่งถือเป็นทรัพย์สินทางปัญญาที่มีอยู่เดิมของผู้ให้บริการ หรือเป็นการปรับปรุงต่อยอดจากทรัพย์สินทางปัญญาที่มีอยู่เดิมของผู้ให้บริการ ให้ถือเป็นกรรมสิทธิ์ของผู้ให้บริการแต่เพียงผู้เดียว

ทั้งนี้ ผู้ให้บริการตกลงให้สิทธิ (License) แก่ผู้ว่าจ้างในการใช้งาน ทำซ้ำ หรือปรับปรุงแก้ไขผลลัพธ์ที่เกิดจากการใช้ชุดคำสั่งหรือเครื่องมือดังกล่าว เพื่อประโยชน์ในการดำเนินงานของระบบตามสัญญาฉบับนี้ได้โดยไม่มีค่าใช้จ่ายเพิ่มเติมและตลอดอายุการใช้งานของระบบ

๑๑.๓. ข้อจำกัดการใช้ทรัพย์สินทางปัญญา

ทั้งสองฝ่ายตกลงจะไม่นำทรัพย์สินทางปัญญา ความลับทางการค้า เทคโนโลยี องค์ความรู้และข้อมูลที่เกิดขึ้นจากการดำเนินงานตามโครงการนี้ไปให้บริการหรือเปิดเผยแก่บุคคลภายนอก เว้นแต่จะได้รับความยินยอมเป็นลายลักษณ์อักษรจากอีกฝ่ายหนึ่ง

๑๒. การรักษาความลับและการคุ้มครองข้อมูล

๑๒.๑ การปฏิบัติตามกฎหมาย

ผู้ให้บริการต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA), พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายอื่นที่เกี่ยวข้องอย่างเคร่งครัดตลอดระยะเวลาสัญญา

นอกเหนือจากกฎหมายที่ระบุข้างต้น ผู้รับจ้างต้องให้ความยินยอมและดำเนินการปรับปรุงการให้บริการให้สอดคล้องกับมาตรฐานการแลกเปลี่ยนข้อมูลสุขภาพดิจิทัล และแนวทางปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่กระทรวงสาธารณสุขประกาศกำหนดเพิ่มเติมในอนาคตตลอดระยะเวลาสัญญาโดยไม่มีเงื่อนไขในการเรียกเก็บค่าใช้จ่ายเพิ่มเติมจากราคาที่เสนอ

๑๒.๒ การลงนามในข้อตกลง

ผู้ให้บริการต้องลงนามในบันทึกข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) และ สัญญาการรักษาความลับ (Non-Disclosure Agreement: NDA) เพื่อให้ถือเป็นส่วนหนึ่งของสัญญาฉบับนี้

๑๒.๓ ความเป็นเจ้าของข้อมูลและถิ่นที่อยู่ของข้อมูล

๑๒.๓.๑ ข้อมูลและสารสนเทศทั้งหมดที่ถูกนำเข้า จัดเก็บ หรือประมวลผลในระบบภายใต้สัญญานี้ ถือเป็นกรรมสิทธิ์ของผู้ว่าจ้างแต่เพียงผู้เดียว

๑๒.๓.๒ ผู้ให้บริการต้องจัดเก็บและประมวลผลข้อมูลทั้งหมด (รวมถึงข้อมูลสำรอง) ภายในราชอาณาจักรไทยเท่านั้น ห้ามมิให้โอนย้ายหรือทำสำเนาข้อมูลออกนอกราชอาณาจักรไทย เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ว่าจ้าง

๑๒.๔ การเข้ารหัสและการบริหารจัดการกุญแจ

ในกรณีที่มีการเข้ารหัสข้อมูล ผู้ให้บริการตกลงว่ากุญแจเข้ารหัสที่ใช้ในการเข้าถึงข้อมูลของผู้ว่าจ้าง ถือเป็นทรัพย์สินและความลับของผู้ว่าจ้าง

๑๒.๔.๑ ผู้ให้บริการไม่มีสิทธิ และจะไม่พยายามกู้คืน ทำสำเนา หรือเข้าถึงกุญแจเข้ารหัสที่ผู้ว่าจ้างเป็นผู้บริหารจัดการเอง (Customer-Managed Keys / BYOK)

๑๒.๔.๒ การสูญหาย...

๑๒.๔.๒ การสูญหายหรือการเข้าถึงกุญแจเข้ารหัสโดยไม่ได้รับอนุญาต ให้ถือเป็นเหตุละเมิดข้อมูลส่วนบุคคล

๑๒.๕ การห้ามเปิดเผยและห้ามดำเนินการกับข้อมูล

ผู้ให้บริการจะไม่ดำเนินการใด ๆ (เช่น เข้าถึง, คัดลอก, แก้ไข, วิเคราะห์หาข้อมูลเชิงลึก) กับข้อมูลของผู้ว่าจ้างโดยเด็ดขาด เว้นแต่

๑๒.๕.๑ ได้รับคำสั่งที่เป็นลายลักษณ์อักษรจากผู้มีอำนาจของผู้ว่าจ้าง

๑๒.๕.๒ เป็นการดำเนินการตามคำสั่งศาล หรือเจ้าพนักงานตามกฎหมาย (โดยต้องแจ้งให้ผู้ว่าจ้างทราบก่อนดำเนินการ หากกฎหมายไม่ห้ามไว้)

๑๒.๕.๓ เป็นกรณีฉุกเฉินเร่งด่วนเพื่อป้องกันความเสียหายต่อระบบ ซึ่งต้องได้รับอนุมัติ (ทางวาจาหรืออิเล็กทรอนิกส์) จากผู้มีอำนาจก่อน และทำรายงานชี้แจงภายหลัง

๑๒.๕.๔ ห้ามผู้ให้บริการหรือผู้รับจ้างช่วง นำข้อมูล สารสนเทศ หรือข้อมูลจราจรคอมพิวเตอร์ (Log) ของผู้ว่าจ้าง ไปใช้ในการสร้างแบบจำลอง (Modeling), การฝึกอบรม (Training), การปรับแต่ง (Fine-tuning) ระบบปัญญาประดิษฐ์ (Artificial Intelligence), Machine Learning หรือ Large Language Models (LLMs) ของผู้ให้บริการหรือของบุคคลที่สามโดยเด็ดขาด

๑๒.๖ ความรับผิดกรณีเกิดเหตุละเมิดข้อมูล

ในกรณีที่เกิดเหตุละเมิดข้อมูลส่วนบุคคล หรือข้อมูลสูญหาย อันเนื่องมาจากความผิดของผู้ให้บริการ

(๑) ผู้ให้บริการตกลงที่จะรับผิดและชดใช้ค่าเสียหายทั้งปวงให้แก่ผู้ว่าจ้างอย่างเต็มจำนวน รวมถึงค่าใช้จ่ายในการกอบกู้ข้อมูล, ค่าปรับทางปกครองที่ผู้ว่าจ้างถูกสั่งปรับ, และค่าสินไหมทดแทนที่ต้องชดใช้แก่บุคคลภายนอก

(๒) ผู้ให้บริการต้องให้ความร่วมมือในการสืบสวนทางนิติวิทยาศาสตร์ (Digital Forensics) และส่งมอบข้อมูลจราจรคอมพิวเตอร์ (Log) หรือหลักฐานอื่นใดให้แก่ผู้ว่าจ้างทันทีที่ร้องขอ

(๓) ในกรณีที่เกิดเหตุละเมิดความมั่นคงปลอดภัย (Security Breach) ซึ่งมีสาเหตุมาจากความบกพร่องของผู้ให้บริการ ผู้ให้บริการจะต้องรับผิดชอบค่าใช้จ่ายทั้งหมด ในการจัดจ้างหน่วยงานหรือผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์คอมพิวเตอร์ (Third-Party Digital Forensics) ที่เป็นกลางและได้รับการยอมรับจากผู้ว่าจ้าง เพื่อเข้ามาสืบสวนหาสาเหตุและจัดทำรายงานความเสียหาย

๑๒.๗ ความรับผิดจากการกระทำของบุคคลภายนอก

หากเกิดความเสียหายจากการกระทำของผู้รับจ้างช่วง (Sub-contractors), ผู้ให้บริการภายนอก หรือคู่ค้าของผู้ให้บริการ ให้ถือเสมือนว่าเป็นการกระทำของผู้ให้บริการเอง ผู้ให้บริการต้องรับผิดชอบต่อผู้ว่าจ้างและบุคคลภายนอกอย่างเต็มจำนวน

๑๒.๘ การเข้าถึงข้อมูลโดยผู้บริหารจัดการระบบ

ในกรณีที่ผู้ว่าจ้างมอบหมายให้บุคคลที่สามเป็นผู้บริหารจัดการระบบ ผู้ให้บริการต้องให้ความร่วมมือในการกำหนดสิทธิ์การเข้าถึงข้อมูลให้แก่บุคคลดังกล่าวตามที่ได้รับแจ้งจากผู้ว่าจ้าง อย่างไรก็ตามผู้ให้บริการยังคงมีหน้าที่รักษาความมั่นคงปลอดภัยในระดับโครงสร้างพื้นฐานอย่างเคร่งครัด

๑๓. หน่วยงานผู้รับผิดชอบ

สำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข

๑๔. เงื่อนไข...

๑๔. เงื่อนไขการยื่นข้อเสนอและเอกสารแนบท้าย

๑๔.๑ เงื่อนไขการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอต้องกำหนดยืนราคาไม่น้อยกว่า ๑๘๐ วัน (หนึ่งร้อยแปดสิบวัน) นับตั้งแต่วันยื่นข้อเสนอ โดยภายในกำหนดยืนราคาดังกล่าว ผู้ยื่นข้อเสนอต้องรับผิดชอบราคาที่ตนได้เสนอไว้ และไม่สามารถถอนการเสนอราคาได้ ทั้งนี้ ผู้ยื่นข้อเสนอต้องรับรองว่าราคาที่เสนอครอบคลุมค่าใช้จ่ายทั้งหมดตามขอบเขตงานที่กำหนด

๑๔.๒ เอกสารแนบท้าย

เอกสารแนบท้ายต่อไปนี้ให้ถือเป็นส่วนหนึ่งของข้อกำหนดและขอบเขตของงาน (Terms of Reference) ฉบับนี้

๑๔.๒.๑ เอกสารแนบท้าย ๑ ตารางเมทริกซ์ความรับผิดชอบ (Shared Responsibility Matrix)

๑๔.๒.๒ เอกสารแนบท้าย ๒ แบบฟอร์มเปิดเผยข้อมูลการควบคุมความมั่นคงปลอดภัยของผู้ให้บริการคลาวด์ (Cloud Service Provider Disclosure Form)

ในกรณีที่มีข้อความขัดแย้งกันระหว่างเอกสารแนบท้ายกับข้อกำหนดหลักในเอกสารฉบับนี้ ให้ถือข้อความในข้อกำหนดหลักเป็นสำคัญ เว้นแต่จะระบุไว้เป็นอย่างอื่น

๑๔.๓ เอกสารประกอบการพิจารณาข้อเสนอด้านเทคนิค

ผู้ยื่นข้อเสนอต้องยื่นเอกสารดังต่อไปนี้ เพื่อประกอบการพิจารณาความเหมาะสมด้านเทคนิคและความมั่นคงปลอดภัย

๑๔.๓.๑ แบบฟอร์มเปิดเผยข้อมูลการควบคุมความมั่นคงปลอดภัย (Cloud Provider Disclosure Form) ผู้ยื่นข้อเสนอต้องจัดทำและยื่นเอกสารการเปิดเผยข้อมูลการควบคุมความมั่นคงปลอดภัยของผู้ให้บริการคลาวด์ (Cloud Service Provider Disclosure) ตามแบบฟอร์มที่กำหนดใน **เอกสารแนบท้าย หมายเลข ๒** โดยต้องระบุรายละเอียดให้ครบถ้วนตามความเป็นจริง พร้อมแนบหลักฐานอ้างอิง (ถ้ามี) ครอบคลุมหัวข้อดังนี้

(๑) ข้อมูลผู้ให้บริการและรูปแบบบริการ ระบุประเภทบริการ (IaaS/PaaS/SaaS) และโมเดลการใช้งาน (Public/Private/Hybrid)

(๒) การปฏิบัติตามกฎหมายและมาตรฐาน แสดงสถานะการรับรองมาตรฐาน ISO/IEC 27001, 27017, 27018, 27799, CSA STAR และความสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)

(๓) การควบคุมข้อมูล (Data Control) ระบุความเป็นเจ้าของข้อมูล (Data Ownership), สถานที่จัดเก็บข้อมูล (Data Residency) ซึ่งต้องอยู่ในประเทศไทย, และกระบวนการทำลายข้อมูลเมื่อสิ้นสุดสัญญา

(๔) ประสิทธิภาพและความต่อเนื่อง ระบุค่า SLA, ความยืดหยุ่นของระบบ (Elasticity) และค่าเป้าหมายการกู้คืนระบบ (RPO/RTO)

(๕) การบริหารจัดการความมั่นคงปลอดภัย ระบุมาตรการรักษาความปลอดภัยเครือข่าย, การเข้ารหัสข้อมูล, และการจัดการสิทธิ์การเข้าถึง

(๖) สิทธิในการตรวจสอบ (Right to Audit) การยินยอมให้ผู้ว่าจ้างหรือหน่วยงานกำกับดูแลเข้าตรวจสอบศูนย์ข้อมูล

หมายเหตุ หากผู้ยื่นข้อเสนอไม่ยื่นแบบฟอร์มดังกล่าว หรือกรอกข้อมูลไม่ครบถ้วน หรือตรวจสอบพบว่าเป็นเท็จ คณะกรรมการพิจารณาผลสงวนสิทธิ์ที่จะไม่พิจารณาข้อเสนอของรายนั้น

๑๕. การฝึกอบรม...

๑๕. การฝึกอบรมและการถ่ายทอดเทคโนโลยี

ผู้ให้บริการต้องจัดอบรมเชิงปฏิบัติการให้แก่เจ้าหน้าที่ของผู้ว่าจ้างและ/หรือ บุคลากรของผู้บริหารจัดการระบบที่ผู้ว่าจ้างมอบหมาย เพื่อให้มีความรู้ความเข้าใจในการบริหารจัดการ ควบคุม และตรวจสอบระบบได้อย่างมีประสิทธิภาพ โดยต้องจัดอบรมไม่น้อยกว่า ๔ หลักสูตร และมีรายละเอียดดังนี้

๑๕.๑ หลักสูตรการบริหารจัดการโครงสร้างพื้นฐานคลาวด์ (Cloud Infrastructure Administration)

๑๕.๑.๑ เนื้อหา การใช้งาน Self-Service Portal, การบริหารจัดการ VM (Create/Manage/Delete), การจัดการเครือข่าย (VPC/VPN), การใช้งานพื้นที่จัดเก็บข้อมูล (Block & Object Storage) และการบริหารจัดการป้ายกำกับทรัพยากร (Resource Tagging) เพื่อการตรวจสอบค่าใช้จ่าย

๑๕.๒ หลักสูตรการรักษาความมั่นคงปลอดภัยและการจัดการข้อมูล (Cloud Security & Data Protection)

๑๕.๒.๑ เนื้อหา การตั้งค่า Firewall และ WAF, การตรวจสอบ Log, และการตอบสนองต่อภัยคุกคาม, การบริหารจัดการกุญแจเข้ารหัส (Key Management Service: KMS) และกระบวนการ BYOK, การใช้งานระบบตรวจสอบกิจกรรมฐานข้อมูล (Database Activity Monitoring: DAM) เพื่อตรวจสอบการเข้าถึงข้อมูล และแนวปฏิบัติเพื่อความสอดคล้องกับ PDPA บนระบบคลาวด์

๑๕.๓ หลักสูตรการบริหารจัดการระบบสมัยใหม่และการติดตามผล (Modern Operations & Monitoring)

๑๕.๓.๑ เนื้อหา การใช้งานเครื่องมือติดตามสถานะ (Infrastructure Monitoring) การอ่านค่าประสิทธิภาพแอปพลิเคชัน (APM) เพื่อวิเคราะห์ปัญหาคอขวด และความรู้เบื้องต้นเกี่ยวกับ Infrastructure as Code (IaC) เพื่อความเข้าใจในกระบวนการกู้คืนระบบอัตโนมัติ (Disaster Recovery Automation)

๑๕.๔ หลักสูตรการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training) สำหรับเจ้าหน้าที่ผู้ปฏิบัติงานและผู้บริหาร เพื่อให้เข้าใจถึงความเสี่ยง การปฏิบัติตามกฎหมาย PDPA และการใช้งานระบบคลาวด์อย่างปลอดภัย

เงื่อนไขการฝึกอบรม

๑๕.๔.๑ ต้องจัดเตรียมเอกสารประกอบการอรมและคู่มือการปฏิบัติงานเป็นภาษาไทยหรือภาษาอังกฤษ ทั้งในรูปแบบเอกสารและไฟล์อิเล็กทรอนิกส์

๑๕.๔.๒ ต้องทำการบันทึกวิดีโอการฝึกอบรมและส่งมอบให้ผู้ว่าจ้างเพื่อใช้ทบทวนในภายหลัง

๑๕.๔.๓ จำนวนผู้เข้าอบรมหลักสูตรละไม่น้อยกว่า ๕ คน หรือตามที่ตกลงกัน

(ลงชื่อ).....ประธานกรรมการ
(นายศุภฤกษ์ ถวิลลาภ)
ตำแหน่ง นายแพทย์เชี่ยวชาญ

(ลงชื่อ)..... กรรมการ
(ผศ. (พิเศษ) นายวรเวทย์ โรจน์จรัสไพศาล)
ตำแหน่ง นายแพทย์เชี่ยวชาญ

(ลงชื่อ)..... กรรมการ
(นายจารุพล ตวงศิริทรัพย์)
ตำแหน่ง นายแพทย์ชำนาญการพิเศษ

(ลงชื่อ)..... กรรมการ
(นายนิรทร ศรีสุโข)
ตำแหน่ง นายแพทย์ชำนาญการพิเศษ

(ลงชื่อ)..... กรรมการ
(นายธนบูลย์ แตงจุด)
ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

เอกสารแนบท้าย ๑

ตารางเมทริกซ์ความรับผิดชอบ (Shared Responsibility Matrix)

คำนิยาม

- **P (Provider)** ผู้ให้บริการเป็นผู้รับผิดชอบหลักในการดำเนินการ จัดหา และดูแลรักษา
- **C (Customer)** ผู้ว่าจ้าง (กระทรวงสาธารณสุข) เป็นผู้รับผิดชอบหลักในการกำหนดนโยบาย ใช้งาน และบริหารจัดการข้อมูล
- **S (Shared)** ความรับผิดชอบร่วมกัน (เช่น ผู้ว่าจ้างกำหนดนโยบาย ผู้ให้บริการเป็นคนตั้งค่า)

๑. โครงสร้างพื้นฐานและกายภาพ (Infrastructure & Physical Security)

หัวข้อ (Domain)	รายละเอียดความรับผิดชอบ	ผู้รับผิดชอบ	คำอธิบายเพิ่มเติม
Physical Security	การรักษาความปลอดภัยทางกายภาพของ Data Center (กล้องวงจรปิด, ยาม, การเข้าถึงพื้นที่)	P	รวมไปถึง Site หลัก และ Site สำรอง
Environmental	ระบบไฟฟ้า, ระบบทำความเย็น, ระบบดับเพลิง และสิ่งอำนวยความสะดวก	P	ผู้ให้บริการต้องรับผิดชอบ ๑๐๐% หากไฟดับ หรือแอร์เสีย
Hardware	การบำรุงรักษาเครื่อง Server, Storage, Network Gear และอุปกรณ์ฮาร์ดแวร์ทั้งหมด	P	รวมถึงการเปลี่ยนอะไหล่เมื่อชำรุด
Virtualization	การบริหารจัดการ Hypervisor และ Cloud Management Platform	P	ดูแลให้ระบบ Virtualization พร้อมใช้งาน
Capacity Management	การจัดสรรทรัพยากร (vCPU, RAM, Storage) ให้เพียงพอตามสัญญา	P	รวมถึงการขยายทรัพยากร (Burst) เมื่อมีการร้องขอ

๒. ระบบเครือข่ายและความมั่นคงปลอดภัย (Network & Security)

หัวข้อ (Domain)	รายละเอียดความรับผิดชอบ	ผู้รับผิดชอบ	คำอธิบายเพิ่มเติม
Network Infrastructure	การเชื่อมต่อวงจรสื่อสาร (Link), Routing, Switching ระดับโครงสร้าง	P	รวมถึงการเชื่อมต่อ NIX/IIG
DDoS Protection	การป้องกันการโจมตีแบบ DDoS ที่ระดับ Network Layer	P	ผู้ให้บริการต้องบรรเทาการโจมตี (Mitigate) ให้ได้ตาม SLA
Firewall / WAF	การจัดหาและติดตั้งอุปกรณ์ Firewall และ WAF	P	ผู้ให้บริการเตรียมเครื่องมือและ Platform
Security Policy	การกำหนดกฎ (Rules/Policies) ของ Firewall และ WAF (เช่น เปิด Port ไหน, บล็อก IP ไหน)	S	C: กำหนดความต้องการ/นโยบาย P: ดำเนินการตั้งค่า (Config) ตามคำสั่ง

หัวข้อ (Domain)	รายละเอียดความรับผิดชอบ	ผู้รับผิดชอบ	คำอธิบายเพิ่มเติม
Vulnerability Management	การสแกนและอุดช่องโหว่ของระบบปฏิบัติการ (OS) และ Infrastructure	P	ตาม TOR ที่ระบุให้ดูแล OS License
App Vulnerability	การสแกนและอุดช่องโหว่ของ Application (Code ของ Digital Health Platform)	C	ผู้ว่าจ้าง/ผู้พัฒนาแอปฯ ต้องดูแล Code ตนเอง
Endpoint Protection	การติดตั้งและดูแลระบบ Anti-virus/ Anti-malware บน VM	P	TOR ระบุให้เป็น Centralized Management โดยผู้ให้บริการ

๓. ระบบปฏิบัติการและข้อมูล (OS, Data & Application)

หัวข้อ (Domain)	รายละเอียดความรับผิดชอบ	ผู้รับผิดชอบ	คำอธิบายเพิ่มเติม
OS License	การจัดหาลิขสิทธิ์ Windows/Linux ให้ถูกต้องตามกฎหมาย	P	ตามข้อกำหนดใน TOR
OS Patching	การอัปเดต Patch ความปลอดภัยของ OS	S	P: เตรียม Patch และแจ้งเตือน C: ทดสอบผลกระทบกับแอปฯ และอนุมัติให้ลง Patch
Application	การติดตั้ง, ตั้งค่า, และดูแลรักษา Application (Digital Health Platform)	C	ผู้ให้บริการดูแค่โครงสร้างพื้นฐาน ไม่แตะต้อง App Logic
Data Classification	การจำแนกชั้นความลับของข้อมูล (เช่น ข้อมูลทั่วไป vs ข้อมูลสุขภาพ)	C	ผู้ว่าจ้างต้องระบุเองว่าข้อมูลใดสำคัญ
Data Encryption	การเข้ารหัสข้อมูล (At Rest/ In Transit)	S	P: เตรียมฟีเจอร์เข้ารหัส (เช่น Storage Encryption) C: เลือกเปิดใช้งานและบริหารจัดการ Key
Access Control	การกำหนดสิทธิ์ผู้ใช้งาน (IAM) ว่าใครเข้าถึงข้อมูลใดได้บ้าง	C	ผู้ว่าจ้างเป็นผู้กำหนดสิทธิ์ User ของตนเอง

๔. การปฏิบัติการและการกู้คืน (Operations & DR)

หัวข้อ (Domain)	รายละเอียดความรับผิดชอบ	ผู้รับผิดชอบ	คำอธิบายเพิ่มเติม
Backup (Infra)	การทำ Snapshot และ Backup ระดับ VM (Daily)	P	ผู้ให้บริการต้องทำให้สำเร็จตามรอบที่กำหนด
Backup (Data)	การตรวจสอบความสมบูรณ์ของข้อมูลภายใน Database	C	ผู้ว่าจ้างต้องตรวจสอบว่า App เขียนข้อมูลลง DB ถูกต้องไหม

หัวข้อ (Domain)	รายละเอียดความรับผิดชอบ	ผู้รับผิดชอบ	คำอธิบายเพิ่มเติม
Monitoring (Infra)	เฝ้าระวัง CPU, RAM, Disk, Network Status (24/7)	P	แจ้งเตือนเมื่อทรัพยากรเต็มหรือระบบล่ม
Monitoring (App)	เฝ้าระวังว่า Application ทำงานผิดพลาดหรือไม่ (Error Logs)	C	ผู้ว่าจ้างดู Log ของแอปฯ เอง
Incident Response	การตอบสนองเมื่อเกิดภัยคุกคาม (SOC)	S	P: ตรวจจับ, แจ้งเตือน, บล็อกการโจมตีระดับ Infra C: ตัดสินใจในเชิงนโยบาย หรือแก้ไขที่ตัว App
Disaster Recovery	การกู้คืนระบบเมื่อเกิดภัยพิบัติ	P	ผู้ให้บริการต้องกู้ระบบให้ได้ตาม RTO/RPO ที่กำหนด

๕. ความรับผิดชอบตามกฎหมาย (PDPA & Liability)

หัวข้อ (Domain)	รายละเอียดความรับผิดชอบ	ผู้รับผิดชอบ	คำอธิบายเพิ่มเติม
Data Controller	บทบาท "ผู้ควบคุมข้อมูลส่วนบุคคล" (ตัดสินใจวัตถุประสงค์การใช้ข้อมูล)	C	กระทรวงสาธารณสุข
Data Processor	บทบาท "ผู้ประมวลผลข้อมูลส่วนบุคคล" (เก็บรักษาและประมวลผลตามคำสั่ง)	P	ผู้ให้บริการ Cloud
Data Breach Notification	การแจ้งเหตุละเมิดต่อ สคส. และเจ้าของข้อมูล	S	P: ต้องแจ้ง C ภายในเวลาที่กำหนด (เช่น 24 ชม.) C: แจ้ง สคส. และเจ้าของข้อมูลตามกฎหมาย
Third-Party Risk	ความเสี่ยงจากการกระทำของผู้ให้บริการช่วง (Sub-processors) ของผู้ให้บริการ	P	(Vicarious Liability) ผู้ให้บริการต้องรับผิดชอบเสมือนทำผิดเอง

ขอบเขตความรับผิดชอบแทน (Vicarious Liability Clause)

ในการตีความตารางเมทริกซ์นี้ หากเกิดความเสียหายใด ๆ ที่อยู่ในความรับผิดชอบของผู้ให้บริการ (P) ไม่ว่าการดำเนินการนั้นจะกระทำโดยพนักงานของผู้ให้บริการโดยตรง หรือโดยผู้รับจ้างช่วง (Sub-contractors), ผู้ให้บริการภายนอก (Third-party Vendors), หรือคู่ค้าทางธุรกิจของผู้ให้บริการ (เช่น เจ้าของ Data Center, ผู้ให้บริการวงจรสื่อสาร) ให้ถือว่าเป็นความรับผิดชอบของผู้ให้บริการแต่เพียงผู้เดียว ผู้ให้บริการไม่สามารถปฏิเสธความรับผิดโดยอ้างว่าเป็นความบกพร่องของบุคคลภายนอกได้

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	[ ] ผู้ให้บริการเจ้าของระบบ (Cloud Service Provider) [ ] ผู้แทนจำหน่าย (Reseller/Broker)

ส่วนที่ ๒ รายละเอียดบริการคลาวด์ (Cloud Service Background)

หัวข้อ	รายละเอียด (โปรดเลือกและระบุข้อมูล)
รูปแบบบริการ	[ ] IaaS (Infrastructure as a Service) [ ] PaaS (Platform as a Service) [ ] SaaS (Software as a Service)
รูปแบบการใช้งาน	[ ] Private Cloud (ส่วนตัว) [ ] Public Cloud (สาธารณะ) [ ] Hybrid Cloud (ผสม) [ ] Community Cloud (กลุ่มองค์กรภาครัฐ)
ที่ตั้งศูนย์ข้อมูล	**Site หลัก:** จังหวัด..... ประเทศ..... **Site สำรอง (DR):** จังหวัด..... ประเทศ..... *(หมายเหตุ: TOR กำหนดให้ต้องตั้งอยู่ในประเทศไทย)*

ส่วนที่ ๓ การปฏิบัติตามกฎหมายและมาตรฐาน (Legal & Compliance)

มาตรฐาน/ กฎหมาย	สถานะการรับรอง (แนบใบรับรอง)	หมายเลขใบรับรอง /วันหมดอายุ
ISO/IEC 27001 (ISMS)	[ ] มี [ ] ไม่มี	.....
ISO/IEC 27017 (Cloud Security)	[ ] มี [ ] ไม่มี	.....
ISO/IEC 27018 (Cloud Privacy)	[ ] มี [ ] ไม่มี	.....
ISO/IEC 27799 (Health Info)	[ ] มี [ ] ไม่มี	.....
CSA STAR	[ ] Level 1 [ ] Level 2	.....
PDPA Compliance	[ ] มีนโยบายรองรับ PDPA ครบถ้วน [ ] 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	[ ] DDoS Protection (ระบุขนาด Gbps: .....) [ ] Firewall / WAF [ ] Private Link / VPN
Identity & Access	[ ] MFA (Multi-Factor Authentication) [ ] Role-based Access Control (RBAC) [ ] SSO Integration
Encryption	[ ] Encryption at Rest (AES-256) [ ] Encryption in Transit (TLS 1.2+) [ ] Key Management Service (BYOK Support)
Log & Monitoring	[ ] เก็บบันทึก Log อย่างน้อย ๙๐ วัน [ ] ส่งออก Log ไปยัง SIEM ภายนอกได้ [ ] Real-time Alerting

ส่วนที่ ๘ สิทธิในการตรวจสอบ (Right to Audit)

หัวข้อ	รายละเอียด
สิทธิของลูกค้า	ยินยอมให้กระทรวงสาธารณสุขหรือตัวแทนเข้าตรวจสอบ (Audit) ศูนย์ข้อมูลหรือไม่ ? [ ] ยินยอม [ ] ไม่ยินยอม (ให้ดูรายงาน SOC 2 แทน)
สิทธิของหน่วยงานกำกับ	ยินยอมให้ สกมช. หรือ สคส. เข้าตรวจสอบตามกฎหมายหรือไม่ ? [ ] ยินยอม [ ] ไม่ยินยอม

(ลงชื่อ).....

(ผู้มีอำนาจลงนามของบริษัทผู้ยื่นข้อเสนอ)

ประทับตราบริษัท (ถ้ามี)

วันที่ .....