รายละเอียดขอบเขตการจ้างงาน (Terms of Reference: TOR)
โครงการจ้างบริการระบบ Cloud Service

๑. หลักการและเหตุผล

ตามที่กระทรวงสาธารณสุขได้กำหนดนโยบายและยุทธศาสตร์การพัฒนาระบบสาธารณสุขของประเทศ มุ่งเน้นการยกระดับคุณภาพชีวิตของประชาชนผ่านการพัฒนาระบบสาธารณสุขที่มีประสิทธิภาพ สอดคล้องกับยุทธศาสตร์ชาติ ๒๐ ปี ด้านสาธารณสุข (พ.ศ. ๒๕๖๐-๒๕๗๙) ที่มุ่งเน้นการสร้างเสริมความเป็นเลิศด้านบริการสุขภาพ (Service Excellence) (กระทรวงสาธารณสุข, ๒๕๖๐) สืบเนื่องจากนโยบายสาธารณสุข ปีงบประมาณ พ.ศ. ๒๕๖๘ ได้กำหนดภารกิจหลักของกระทรวงสาธารณสุข ในการยกระดับระบบบริการสาธารณสุข พัฒนาคุณภาพชีวิตประชาชน สร้างความมั่นคงทางสุขภาพคนไทยทุกมิติ

จากแผนการขับเคลื่อนนโยบายกระทรวงสาธารณสุข พ.ศ. ๒๕๖๘ ระบุว่า การพัฒนาระบบสาธารณสุขต้องครอบคลุมทั้งการส่งเสริม ควบคุมป้องกันโรค รักษา และฟื้นฟูสุขภาพ สำหรับประชาชนทุกกลุ่ม เพื่อลดความเหลื่อมล้ำและเพิ่มการเข้าถึงบริการที่มีคุณภาพได้มาตรฐาน (กระทรวงสาธารณสุข, ๒๕๖๗) โดยการพัฒนาดังกล่าวจำเป็นต้องอาศัยนวัตกรรมและเทคโนโลยีที่ทันสมัย ซึ่งสอดคล้องกับแนวทางขององค์การอนามัยโลกที่สนับสนุนให้ประเทศสมาชิกพัฒนาระบบสุขภาพดิจิทัลเพื่อเพิ่มประสิทธิภาพการให้บริการสุขภาพแก่ประชาชน (WHO, ๒๐๒๑)

แผนการขับเคลื่อนนโยบายกระทรวงสาธารณสุข พ.ศ. ๒๕๖๘ ได้กำหนดเป้าหมายการขับเคลื่อน ๗ นโยบายสำคัญ โดยนโยบายสำคัญประเด็นที่ ๑ คือ ยกระดับ “๓๐ บาท รักษาทุกที่” เพื่อเพิ่มการเข้าถึงบริการสุขภาพ (กระทรวงสาธารณสุข, ๒๕๖๗) ซึ่งสอดคล้องกับผลการศึกษาของสำนักงานพัฒนานโยบายสุขภาพระหว่างประเทศ (๒๕๖๗) ที่พบว่าการเชื่อมโยงระบบข้อมูลสุขภาพในระบบบริการทุกระดับช่วยเพิ่มประสิทธิภาพการให้บริการและลดความซ้ำซ้อนในการรักษาได้ถึงร้อยละ ๓๕

จากรายงานการศึกษาของสถาบันวิจัยระบบสาธารณสุข (๒๕๖๗) พบว่า การบูรณาการข้อมูลสุขภาพบนแพลตฟอร์มดิจิทัลช่วยลดความซ้ำซ้อนในการให้บริการได้ถึงร้อยละ ๔๐ และเพิ่มความพึงพอใจของผู้รับบริการร้อยละ ๖๕ เมื่อเทียบกับระบบแบบเดิม และจากรายงานวิจัยของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ร่วมกับคณะแพทยศาสตร์จุฬาลงกรณ์มหาวิทยาลัย (๒๕๖๖) เรื่อง “ผลกระทบของการลงทุนด้านเทคโนโลยีสารสนเทศต่อประสิทธิภาพการให้บริการของสถานพยาบาลในประเทศไทย” ยังพบว่าโรงพยาบาลที่มีการลงทุนในระบบสารสนเทศอย่างเพียงพอสามารถเพิ่มประสิทธิภาพการทำงานของบุคลากรทางการแพทย์ได้ร้อยละ ๒๕-๒๘ และลดต้นทุนการดำเนินงานลงได้ร้อยละ ๑๒-๑๘

การปรับระบบจากการให้บริการรูปแบบเดิม สู่ระบบการให้บริการแบบดิจิทัล สอดคล้องกับนโยบาย Digital Transformation ของประเทศไทยที่ส่งเสริมการพัฒนาบริการภาครัฐสู่รูปแบบดิจิทัลเพื่อยกระดับคุณภาพชีวิตของประชาชน (สำนักงานพัฒนารัฐบาลดิจิทัล, ๒๕๖๖) สำนักงานส่งเสริมเศรษฐกิจดิจิทัล (DEPA) (๒๕๖๗) ได้เผยแพร่รายงาน “แนวโน้มการพัฒนาเศรษฐกิจดิจิทัลของประเทศไทย” ซึ่งคาดการณ์ว่าอุตสาหกรรมสุขภาพดิจิทัลในประเทศไทยจะเติบโตที่อัตราเฉลี่ยร้อยละ ๒๒.๔ ต่อปี และในระหว่างปี พ.ศ.๒๕๖๗-๒๕๗๐ มีมูลค่าตลาดคาดการณ์สูงถึง ๕.๘ หมื่นล้านบาท ในปี พ.ศ. ๒๕๗๐

การใช้บริการ Cloud Service สำหรับระบบสุขภาพดิจิทัลเป็นแนวปฏิบัติที่ได้รับการยอมรับในระดับสากล โดย Gartner (๒๐๒๓) รายงานว่าองค์กรด้านสาธารณสุขทั่วโลกกว่าร้อยละ ๗๕ ใช้บริการ Cloud Service เพื่อเพิ่มความยืดหยุ่น ประสิทธิภาพ และความปลอดภัยของระบบข้อมูลสุขภาพ ซึ่งสอดคล้องกับข้อเสนอแนะขององค์การอนามัยโลก (WHO, ๒๐๒๒) ที่สนับสนุนให้ประเทศสมาชิกพัฒนาโครงสร้างพื้นฐานด้านดิจิทัลที่มีความปลอดภัยและมีประสิทธิภาพสูง

เพื่อให้ระบบ...

เพื่อให้ระบบการดำเนินงานนโยบายสำคัญประเด็นที่ ๑ คือ ยกระดับ “๓๐ บาท รักษาทุกที่” สามารถใช้งานได้อย่างต่อเนื่องและมีประสิทธิภาพ เพิ่มศักยภาพการให้บริการสุขภาพประชาชนด้วยการเชื่อมโยงระบบข้อมูลสุขภาพในระบบบริการทุกระดับ และพัฒนาและสนับสนุนการขับเคลื่อนการดำเนินงานด้านดิจิทัลสุขภาพตามนโยบายของกระทรวงสาธารณสุขในการยกระดับคุณภาพบริการสุขภาพของประชาชนด้วยการพัฒนาระบบบริการสุขภาพด้วยดิจิทัล การประยุกต์ใช้เทคโนโลยีที่ทันสมัยเพื่อสนับสนุนการบริการสุขภาพ การเชื่อมโยงข้อมูลและบูรณาการข้อมูลระหว่างหน่วยบริการสุขภาพเพื่อให้ประชาชนสามารถเข้ารับการรักษาพยาบาลได้ทุกหน่วยบริการและสามารถเข้าถึงข้อมูลสุขภาพของตนเองได้อย่างถูกต้อง มีความปลอดภัย สะดวกและรวดเร็ว โดยการบูรณาการข้อมูลที่ไร้รอยต่อในการเชื่อมโยงระบบข้อมูลของโรงพยาบาล คลินิก ร้านยา และสถานพยาบาลอื่น ๆ ที่เกี่ยวข้อง เพื่อให้สามารถเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกันได้อย่างมีประสิทธิภาพ สามารถเข้าถึงข้อมูลและบริการทางการแพทย์ได้ทุกที่

สำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข ซึ่งมีหน้าที่พัฒนาแพลตฟอร์มสุขภาพดิจิทัล ได้พัฒนาระบบและปรับปรุงการเข้าถึงระบบบริการทางการแพทย์และยกระดับการให้บริการสุขภาพประชาชน ปรับระบบจากการให้บริการรูปแบบเดิมสู่ระบบการให้บริการแบบดิจิทัล เพื่อให้ประชาชนได้รับการบริการที่สะดวกยิ่งขึ้น ด้วยการเชื่อมโยงข้อมูลสุขภาพให้เป็นระบบเดียว บน Digital Health Platform ของกระทรวงสาธารณสุขและแพลตฟอร์มหมอพร้อม สอดคล้องตามภารกิจการดำเนินงานตามนโยบาย “๓๐ บาท รักษาทุกที่” ให้สามารถให้บริการสุขภาพในรูปแบบดิจิทัลตามแนวทางปฏิบัติและกรอบการดำเนินงานที่ถูกต้องตามหลักธรรมาภิบาล มาตรฐานสากล และกฎหมายที่เกี่ยวข้องกับการดำเนินงานของกระทรวงสาธารณสุข พร้อมทั้งส่งเสริม สนับสนุน การพัฒนาและประยุกต์ใช้แพลตฟอร์มสุขภาพดิจิทัล ในการเพิ่มประสิทธิภาพการเข้าถึงระบบบริการทางการแพทย์ สนับสนุนให้หน่วยบริการใช้ประโยชน์จากการเก็บรวบรวม ประมวลผลข้อมูลการให้บริการ วิเคราะห์ การให้บริการและการประเมินเพื่อพัฒนาระบบการให้บริการสุขภาพได้ และมีระบบฐานข้อมูลกลางของกระทรวงสาธารณสุข สำหรับจัดเก็บข้อมูลที่เกี่ยวข้องกับการให้บริการ จากหน่วยบริการทั่วประเทศทั้งภาครัฐและเอกชน ที่มีประสิทธิภาพมีความมั่นคงปลอดภัย บน Digital Health Platform ของกระทรวงสาธารณสุข

การพัฒนาประกอบไปด้วยระบบบริการสุขภาพและแพลตฟอร์มสุขภาพดิจิทัล อาทิเช่น ระบบประวัติสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล (Personal Health Record: PHR) ระบบดิจิทัลไอดีของบุคลากรทางการแพทย์และผู้ให้บริการสาธารณสุข (Provider ID) ระบบดิจิทัลไอดีของประชาชนผู้รับบริการสาธารณสุข (Health ID) ระบบใบรับรองแพทย์ดิจิทัล (Digital Signature) ระบบใบสั่งยาออนไลน์ ระบบสั่งแล็บออนไลน์ (MOPH LAB) ระบบส่งต่อผู้ป่วย (MOPH Refer) ระบบบริการการแพทย์ทางไกลและเภสัชกรรมทางไกลและการปรึกษาแพทย์ผู้เชี่ยวชาญ (Telemedicine & Tele pharmacy) ระบบการนัดหมายออนไลน์ (MOPH Appointment) ระบบการส่งยาและเวชภัณฑ์ที่บ้าน (Health Rider) ระบบเชื่อมโยงข้อมูลภาพเอกซเรย์ของประชาชน (Imaging Hub) ระบบ Health Wallet ระบบ MOPH Station เป็นต้น ซึ่งระบบได้ดำเนินการตามแนวทางปฏิบัติและกรอบการดำเนินงานที่ถูกต้องตามหลักธรรมาภิบาล มาตรฐาน และกฎหมายที่เกี่ยวข้องกับการดำเนินงานของกระทรวงสาธารณสุข

ทั้งนี้ การพัฒนาระบบจะใช้แนวคิด Patient-Centric Healthcare ที่มุ่งเน้นผู้ป่วยเป็นศูนย์กลาง โดยให้ความสำคัญกับการเข้าถึงข้อมูลสุขภาพของตนเองอย่างปลอดภัยผ่านระบบประวัติสุขภาพอิเล็กทรอนิกส์ส่วนบุคคล (Personal Health Record: PHR) และผ่านแพลตฟอร์มระบบสุขภาพดิจิทัลที่กระทรวงสาธารณสุข (แพลตฟอร์มหมอพร้อม) ได้จัดทำขึ้น เพื่อให้ประชาชนซึ่งเป็นเจ้าของข้อมูลสามารถดูประวัติสุขภาพของตนเองผ่าน Mobile Application หมอพร้อมหรือไลน์หมอพร้อม และบุคลากรทางการแพทย์สามารถเข้าถึงข้อมูลสุขภาพประชาชนที่จำเป็น เพื่อการวินิจฉัยและการตรวจรักษา

ด้วยเหตุผล...

(นายทรงยศ ชญานินปรเมศ)	(นายสุรพงศ์ แสนโภชน์)	(นายศุภณัฐ ถวิลลาภ)	(นายนิรทร ศรีสุโข)	(นายจารุพล ตวงศิริทรัพย์)	(นายภาณุพงศ์ ตันติรัตน์)	(นายราชี ปาลือซา)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

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 และธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) ตามที่สำนักงานพัฒนารัฐบาลดิจิทัลกำหนด เพื่อให้บริการสุขภาพประชาชนได้อย่างมีประสิทธิภาพ ลดความซ้ำซ้อนในการรักษา เพิ่มประสิทธิภาพในการป้องกันโรค และบริหารจัดการทรัพยากรสาธารณสุขได้อย่างเหมาะสม ซึ่งจะสะท้อนให้เห็นถึงความคุ้มค่าในการลงทุนพัฒนาระบบดังกล่าวเพื่อยกระดับคุณภาพชีวิตของประชาชนไทยอย่างยั่งยืน

๒. วัตถุประสงค์

๑. เพื่อจ้างบริการระบบ Cloud Service รองรับการทำงานของระบบข้อมูลและเป็นฐานข้อมูลกลางโดยกระทรวงสาธารณสุข รองรับการให้บริการสุขภาพดิจิทัลของกระทรวงสาธารณสุขที่มีมาตรฐานและสามารถให้บริการได้อย่างมีประสิทธิภาพ รวดเร็ว ต่อเนื่อง โดยคำนึงถึงความปลอดภัยของข้อมูลเป็นสำคัญ

๒. เพื่อให้เกิดการบูรณาการข้อมูลและแลกเปลี่ยนข้อมูล โดยการเชื่อมโยงระบบข้อมูลของโรงพยาบาล คลินิก ร้านยา และสถานพยาบาลอื่น ๆ เป็นไปอย่างมีมาตรฐานในระดับสากล มีความมั่นคงปลอดภัยและมีประสิทธิภาพ

๓. เพื่อเพิ่มประสิทธิภาพของระบบฐานข้อมูลกลางกระทรวงสาธารณสุข สำหรับจัดเก็บข้อมูลการให้บริการจากหน่วยบริการ ให้มีคุณสมบัติการทำงานรองรับภารกิจ ที่มีการขยายตัวและปรับเปลี่ยนไปได้อย่างถูกต้อง เหมาะสม และทันสมัย

๔. เพื่อให้การดำเนินงานเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายอื่นที่เกี่ยวข้อง

๓. คุณสมบัติของผู้เสนอราคา

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ เป็นนิติบุคคลผู้มีอาชีพรับจ้างที่ประกวดราคาอิเล็กทรอนิกส์

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานปลัดกระทรวงสาธารณสุข ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๓.๑๐ ผู้ยื่นข้อเสนอ...

(นายทรงยศ ชญานินปรเมศ)	(นายสุรพงศ์ แสนโภชน์)	(นายศุภฤกษ์ ถวิลลาภ)	(นายนิรทร ศรีสุโข)	(นายจารุพล ตวงศิริทรัพย์)	(นายภาณุพงศ์ ตันติรัตน์)	(นายราชี ปาลือซา)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

๓.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

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

๓.๑๒ ผู้ยื่นข้อเสนอต้องมีผลงานในการให้บริการระบบ (Cloud Service) ด้านการแพทย์และสุขภาพให้กับหน่วยงานภาครัฐ หรือรัฐวิสาหกิจหรือเอกชน หรือผลงานด้านการให้บริการโครงสร้างพื้นฐาน ไม่น้อยกว่า ๑ ผลงาน โดยมีวงเงินของสัญญาไม่น้อยกว่า ๕,๐๐๐,๐๐๐ บาท (ห้าล้านบาทถ้วน) พร้อมยื่นหลักฐานเป็นสำเนาหนังสือรับรองผลงานหรือสำเนาสัญญา

๔. รายละเอียดขอบเขตของงาน

ระบบประมวลผล Cloud Computing

สำหรับติดตั้งระบบงานดังกล่าว โดยมีคุณลักษณะเฉพาะที่เทียบเท่าหรือดีกว่า ดังนี้

๔.๑ ภาพรวมของระบบ (Computing Resource and Environment Specification) สามารถให้บริการได้อย่างต่อเนื่อง โดยมีระดับของการให้บริการ (Service Level Agreement) ไม่ต่ำกว่า ๙๙.๙๕ % ต่อเดือน หรือหยุดให้บริการได้ (Down Time) ไม่เกิน ๒๓ นาที ต่อเดือน

๔.๒ ผู้ให้บริการระบบคลาวด์ (Cloud Computing) ต้องได้รับการรับรองมาตรฐาน ดังต่อไปนี้ พร้อมยื่นหลักฐานเอกสารการรับรองมาตรฐาน

๑) มาตรฐานการให้บริการด้านเทคโนโลยีสารสนเทศระบบคลาวน์ (Service Management System: SMS) ISO/IEC 20000-1

๒) มาตรฐานการบริหารจัดการความปลอดภัยของข้อมูล (Information Security Management System: ISMS) ISO/IEC 27001

๓) มาตรฐานความปลอดภัยสำหรับระบบคลาวด์ CSA-STAR Cloud Security โดยต้องได้รับการรับรอง CSA-STAR Level 2/CCM

๔) มาตรฐานการจัดการความปลอดภัยด้านสารสนเทศ ในระบบคลาวน์ ISO/IEC 27017 สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII)

๕) มาตรฐานการบริหารความต่อเนื่องทางธุรกิจ Business Continuity Management :BCM ISO/IEC 22301

๖) มาตรฐานการดูแลข้อมูลสารสนเทศด้านสุขภาพ Information Security Management in Healthcare) ISO/IEC 27799

๔.๓ ศูนย์ข้อมูล...

๔.๓ ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ตั้งอยู่ในประเทศไทย ไม่ต่ำกว่า ๓ ศูนย์ข้อมูล และ Data Center ทุกแห่ง ต้องมีระบบเครือข่ายสื่อสารหลักที่เชื่อมเป็นเครือข่ายเดียวกันด้วยเทคโนโลยีบริหารจัดการระบบเครือข่าย (Software Define Infrastructure: SDI) เพื่อรองรับแผนการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning : BCP)

๔.๔ จัดเตรียมเครื่องคอมพิวเตอร์แม่ข่ายสำหรับรองรับการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายเสมือน โดยมีทรัพยากรรวม ดังนี้

๑) สามารถสร้างเครื่องคอมพิวเตอร์แม่ข่ายเสมือนไม่น้อยกว่า ๓๘๔ VM

๒) มีจำนวนหน่วยประมวลผลกลาง (vCPU) ไม่น้อยกว่า ๔,๘๐๐ vCore

๓) มีจำนวนหน่วยความจำหลัก (vRAM) ไม่น้อยกว่า ๑๓,๐๕๖ GB

๔) มีจำนวนพื้นที่เก็บข้อมูล (vDisk) ไม่น้อยกว่า ๓๓๖,๐๐๐ GB

๕) เครื่องคอมพิวเตอร์แม่ข่ายเสมือนต้องติดตั้งระบบปฏิบัติการลิขสิทธิ์ (Operating System) จำนวนตามการออกแบบ

๖) มีการติดตั้ง Anti-virus และ Anti-malware บนเครื่องคอมพิวเตอร์แม่ข่ายเสมือน จำนวนตามการออกแบบ

๔.๕ มีระบบ Snapshot ที่ฝั่งบริการหลัก (On Site) ทุกวัน วันละ ๑ ชุด โดยทำการเก็บข้อมูลไว้ระยะเวลา ๗ วัน

๔.๖ มีระบบ Snapshot ที่ฝั่งบริการสำรอง (Backup Site) ทุกวัน วันละ ๑ ชุด โดยทำการเก็บข้อมูลไว้ระยะเวลา ๗ วัน

๔.๗ คุณสมบัติด้านเครือข่าย (Network Specification)

๔.๗.๑ Unlimited Data Transfer ภายใน Public Cloud Environment

๔.๗.๒ จัดเตรียมชุด Public IP จำนวนตามการออกแบบของกระทรวงสาธารณสุขโดยไม่มีค่าใช้จ่ายเพิ่มเติม

๔.๗.๓ Shared Domestic Internet Bandwidth ของ Cloud Services รวมกันไม่น้อยกว่า ๔๐ Gbps.

๔.๗.๔ Shared International Internet Bandwidth ของ Cloud Services รวมกันไม่น้อยกว่า ๔๐๐ Mbps.

๔.๗.๕ มีระบบการเฝ้าระวังเครือข่าย (Network Monitoring) ที่สามารถตรวจจับปัญหา (Detection) และส่งการแจ้งเตือน (Notification) เมื่อเกิดปัญหาภายในระยะเวลาไม่เกิน ๑๕ นาที

๔.๗.๖ ต้องรับประกันความพร้อมใช้งานของเครือข่าย (Network Uptime SLA) ไม่น้อยกว่า ๙๙.๙% ต่อเดือน

๔.๗.๗ มีระบบป้องกันเครือข่าย (Network Security) ที่รวมถึง Firewall และระบบป้องกัน DDoS (DDoS Protection)

๔.๗.๘ มีบริการเชื่อมต่อแบบเครือข่ายส่วนตัว (Private Network) สำหรับการเชื่อมต่อกับระบบ On-premise หรือ Cloud อื่นๆ เช่น VPN หรือ Direct Connect

๔.๗.๙ รับประกัน Network Latency ภายในประเทศไม่เกิน ๓๐ ms และระหว่างประเทศไม่เกิน ๑๕๐ ms (วัดจากภายใน Cloud ไปยังจุดวัดมาตรฐาน)

๔.๘ ความปลอดภัยทางสารสนเทศ (IT Security Specification)

๔.๘.๑ มีระบบการป้องกันและตรวจสอบสิทธิ์การเข้าถึงข้อมูลตามมาตรฐาน Secure Assesses Service Edge (SASE) หรือ Virtual Firewall

๔.๘.๒ มีระบบ...

(นายทรงยศ ชญานินปรเมศ)	(นายสุรพงศ์ แสนโภชน์)	(นายศุภกฤษ์ ถวิลลาภ)	(นายนิรทร ศรีสุโข)	(นายจารุพล ตวงศิริทรัพย์)	(นายภาณุพงศ์ ตันติรัตน์)	(นายราชิ ปาลือซา)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

๔.๘.๒ มีระบบป้องกันเครื่องแม่ข่ายเสมือนจากภายใน โดยใช้งานระบบรักษาความปลอดภัยเสมือน (Virtual Firewall) โดยจัดให้มี Virtual Firewall ในปริมาณที่เหมาะสม ไม่เป็นอุปสรรคต่อการให้บริการ และต้องมีคุณสมบัติอย่างน้อยดังนี้

๑) สามารถรองรับ Traffic แบบ North-South และ East-West

๒) สามารถรองรับ Throughput ไม่น้อยกว่า ๓ Gbps

๓) รองรับ User VPN ไม่น้อยกว่า ๑๐ Users

๔) สามารถบริหารจัดการโดยกำหนดนโยบายการเข้าถึงหรือ Policy ได้

๕) มีความสามารถในการช่วยกระจายโหลดงาน (Load Balance) โดยรองรับ Throughput สูงสุดไม่น้อยกว่า ๓ Gbps รองรับการเชื่อมต่อได้ไม่น้อยกว่า ๒,๐๐๐ connection per second

๖) รองรับการทำงานได้อย่างน้อย ดังนี้ Round Robin, Least Connection, IP-Hash, HTTP Headers, URI, URL หรือเทียบเท่า

๗) สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTP, HTTPS ได้เป็นอย่างน้อย

๔.๙ ระบบป้องกันการโจมตีผ่านหน้าเว็บ (Web Application Firewall) (เฉพาะศูนย์ข้อมูลหลัก) สามารถป้องกันการโจมตี Web Server จากผู้ไม่ประสงค์ดี และภัยคุกคามทางอินเทอร์เน็ต ด้วยอุปกรณ์ป้องกันเสมือน จำนวน ๑ domain แบบ wild-card โดยต้องมีคุณสมบัติอย่างน้อยดังนี้

๔.๙.๑ มีระบบการป้องกันและตรวจสอบสิทธิ์การเข้าถึงข้อมูลตามมาตรฐาน Secure Access Service Edge (SASE) หรือ Virtual Firewall

๔.๙.๒ ระบบป้องกันเครื่องแม่ข่ายเสมือนจากภายใน โดยใช้งานระบบรักษาความปลอดภัยเสมือน (Virtual Firewall) โดยจัดให้มี Virtual Firewall ในปริมาณที่เหมาะสม ไม่เป็นอุปสรรคต่อการให้บริการ และต้องมีคุณสมบัติอย่างน้อยดังนี้

๑) สามารถรองรับ Traffic แบบ North-South และ East-West

๒) สามารถรองรับ Throughput ไม่น้อยกว่า ๓ Gbps

๓) รองรับ User VPN ไม่น้อยกว่า ๑๐ Users

๔) สามารถบริหารจัดการโดยกำหนดนโยบายการเข้าถึงหรือ Policy ได้

๔.๑๐ ความสามารถในการป้องกันเว็บแอพพลิเคชัน (Web Security Functions)

๑) สามารถแสดงรายงานบน Security Dashboard แบบ Real-time หรือ Near Real-time โดย สามารถแสดงถึงข้อมูลแหล่งที่มาของการโจมตี เช่น IP Addresses, User Agents, Countries และ ASNs ได้

๒) สามารถป้องกันการโจมตีผ่านทาง Website ตาม OWASP TOP ๑๐ เช่น SQL injection, Broken Authentication, Cross-site Scripting ได้

๓) สามารถตั้งค่า Web Application Firewall (WAF) ได้แบบไม่จำกัดจำนวน (Unlimited Custom WAF rules) และการตั้งค่าการเปิดปิด WAF Rule ต้องมีผลบังคับใช้ (Effective) ภายในเวลาไม่เกิน ๓๐ นาที

๔) สามารถตั้งค่า IP Firewall โดยสามารถกำหนดเงื่อนไขด้วย IP address, IP address range, Autonomous System Number (ASN) or country ได้

๕) สามารถตั้งค่า Rate Limit Rules ซึ่งสามารถกำหนดการป้องกันการเข้าถึง Website โดย Rule สามารถกำหนด ๑ Rule ต่อ ๑ Web Path

๔.๑๑ ให้บริการ...

(นายทรงยศ ชญานินปรเมศ)	(นายสุรพงศ์ แสนโภชน์)	(นายศุภกฤษ์ ถวิลลาภ)	(นายนิรทร ศรีสุโข)	(นายจารุพล ตวงศิริทรัพย์)	(นายภาณุพงศ์ ตันติรัตน์)	(นายราชี ปาลือซา)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

๔.๑๑ ให้บริการเฝ้าระวังความปลอดภัยและ ตรวจจับภัยคุกคามทางไซเบอร์ Security Operations Center (SOC)

ผู้ยื่นข้อเสนอต้องจัดให้มีบริการเฝ้าระวังความปลอดภัยและตรวจจับภัยคุกคามทางไซเบอร์สำหรับระบบ Cloud Computing ที่จัดหาในโครงการนี้ โดยไม่มีค่าใช้จ่ายเพิ่มเติม ซึ่งมีคุณสมบัติและรายละเอียดดังนี้

๔.๑๑.๑ คุณสมบัติทั่วไปของระบบเฝ้าระวังความปลอดภัยและตรวจจับภัยคุกคาม

๑) ดำเนินการเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ตลอด ๒๔ ชั่วโมง ๗ วันต่อสัปดาห์

๒) สามารถตรวจจับภัยคุกคามประเภทต่างๆ อย่างน้อยดังนี้

- การบุกรุกระบบเครือข่าย (Network Intrusion)
- มัลแวร์และแรนซัมแวร์ (Malware and Ransomware)
- การโจมตีเว็บแอปพลิเคชัน (Web Application Attack)
- การพยายามเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access)
- พฤติกรรมที่ผิดปกติ (Anomalous Behavior)

๓) ใช้เทคโนโลยีที่ทันสมัยในการตรวจจับและวิเคราะห์ภัยคุกคาม เช่น ระบบ SIEM, IDS/IPS, หรือเทคโนโลยีอื่นที่เทียบเท่า

๔) มีระบบแจ้งเตือนอัตโนมัติเมื่อตรวจพบภัยคุกคาม โดยส่งการแจ้งเตือนผ่านช่องทางที่ผู้ว่าจ้างกำหนด

๔.๑๑.๒ บริการศูนย์เฝ้าระวังความปลอดภัยทางด้านไซเบอร์ ตรวจสอบเหตุการณ์ผิดปกติที่จะเป็นภัยคุกคาม รวมถึงให้คำแนะนำในการตรวจสอบแก้ไขปัญหา ในระบบ Cloud Computing ที่ผู้ยื่นข้อเสนอจัดหาในโครงการนี้ โดยไม่มีค่าใช้จ่ายเพิ่มเติม และมีรายละเอียดดังนี้

- SOC (Security Operations Center)
  - a) ศูนย์ปฏิบัติการเฝ้าระวังเหตุการณ์ที่เป็นภัยคุกคาม ระบบเทคโนโลยีสารสนเทศ (SOC)
  - b) ตรวจสอบเหตุการณ์ผิดปกติที่อาจเป็นภัยคุกคามต่อระบบ Digital Health Platform กระทรวงสาธารณสุข
  - c) วิเคราะห์ Log ที่ส่งมาจากอุปกรณ์ของระบบ Digital Health Platform กระทรวงสาธารณสุข
  - d) แจ้งเตือนเมื่อพบเหตุการณ์ที่น่าสงสัย
  - e) ให้คำแนะนำในการตรวจสอบแก้ไขปัญหา
  - f) ดำเนินการ Remote เพื่อตรวจสอบแก้ไขปัญหา (กรณีพบภัยคุกคาม)
- IR (Incident Response)
  - a) รับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์
  - b) จำกัดขอบเขตของความเสียหาย
  - c) ฟื้นฟูระบบให้กลับมาใช้งานได้ปกติ
  - d) วิเคราะห์สาเหตุของเหตุการณ์
  - e) เสนอแนะแนวทางป้องกันเพื่อไม่ให้เกิดเหตุการณ์ซ้ำ
- Log Monitoring
  - a) รวบรวม Log จากอุปกรณ์ของระบบ Digital Health Platform กระทรวงสาธารณสุข

b) วิเคราะห์...

(นายทรงยศ ชญานินปรเมศ) ประธานกรรมการ | (นายสุรพงศ์ แสนโภชน์) กรรมการ | (นายศุภฤกษ์ ถวิลลาภ) กรรมการ | (นายนิรทร ศรีสุโข) กรรมการ | (นายจาตุพล ตวงศิริทรัพย์) กรรมการ | (นายภาณุพงศ์ ตันติรัตน์) กรรมการ | (นายรวิช ปาลือชา) กรรมการ

b) วิเคราะห์ Log เพื่อหาความผิดปกติ

c) เก็บ Log ไว้สำหรับการตรวจสอบย้อนหลัง เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน โดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

d) มีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึก เหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๔.๑๑.๓ ต้องมีการวิเคราะห์แบบรวมศูนย์ (Correlation) และสามารถสร้างเงื่อนไขการโจมตี (Rule or Use case) เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคามทางไซเบอร์

๔.๑๑.๔ ต้องมี Rules ที่ใช้ในการเฝ้าระวัง และสามารถตรวจจับภัยคุกคามซึ่งครอบคลุมหัวข้อต่าง ๆ อย่างน้อยดังนี้

- Denial of Service (DOS)
- Unauthorized Access
- Inappropriate Usage
- Network Attack Techniques

๔.๑๑.๕ ต้องจัดให้มีทีมงานที่มีความรู้ความสามารถในด้านการวิเคราะห์ เฝ้าระวัง และแจ้งเตือนภัยคุกคามด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้คำปรึกษาด้านเทคนิคตลอดระยะเวลาอายุสัญญา

๔.๑๑.๖ แจ้งเตือนเมื่อตรวจพบภัยคุกคามหรือการบุกรุกระบบเทคโนโลยีสารสนเทศที่มีระดับความรุนแรงสำคัญ (Critical) หรือระดับความรุนแรงสูง (High) ผ่านทางอีเมล์ หรือโทรศัพท์ ตลอด ๒๔ ชั่วโมง

๔.๑๑.๗ ต้องมีการตรวจสอบสถานะของการส่งข้อมูล Log ระหว่างหน่วยงานและผู้รับจ้าง ในกรณีที่ตรวจสอบพบว่าอุปกรณ์หยุดส่ง Log ไปเกินกว่า ๖ ชั่วโมง ให้แจ้งเตือนไปยังเจ้าหน้าที่ของหน่วยงาน ผ่านทางอีเมล์ หรือโทรศัพท์

๔.๑๑.๘ ต้องมีการอัพเดทข้อมูลข่าวสารเกี่ยวกับความปลอดภัยเทคโนโลยีสารสนเทศ หรือภัยคุกคามใหม่ ให้แก่หน่วยงานอย่างสม่ำเสมอ อย่างน้อยเดือนละ ๑ ครั้ง

๔.๑๑.๙ ต้องมีใช้ข้อมูลภัยคุกคามที่ทันสมัย (Threat Intelligence) เพื่อวิเคราะห์ข้อมูล และสามารถเพิ่มเติมได้ ไม่ต่ำกว่า ๕ แหล่งข้อมูล

๔.๑๑.๑๐ ต้องสามารถเขียน Rules หรือ Use Cases เพิ่มเติมได้

๔.๑๑.๑๑ ต้องสามารถจัดทำรายงานตามความต้องการของมาตรฐานความปลอดภัยต่าง ๆ ดังนี้ PCI, SOX, ISO/IEC 27001 หรือ ISO/IEC 27002, FISMA, HIPAA ได้เป็นอย่างน้อย

๔.๑๑.๑๒ ต้องสามารถเลือกช่วงเวลาของข้อมูลดิบ (Raw Data) ที่จะค้นหาได้ ทั้งของช่วงเวลาปัจจุบันและของช่วงเวลาย้อนหลังได้อย่างน้อย ๓๐ วัน

๔.๑๑.๑๓ ต้องสามารถทำการจัดเก็บข้อมูลในลักษณะแบบ Online ได้ และ Offline (raw log) ได้

๔.๑๑.๑๔ ต้องสามารถให้บริการได้อย่างต่อเนื่อง โดยมีระดับของการให้บริการ (Service Level Agreement) ไม่ต่ำกว่า 99.95 % ต่อเดือน

๔.๑๑.๑๕ ระบบ SIEM ที่นำมาให้บริการภายในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC) จะต้องอยู่ในกลุ่ม Challenger หรือสูงกว่าของ Gartner Magic Quadrant for Security Information and Event Management for the seventh time ปี ค.ศ. ๒๐๒๔ หรือปีล่าสุด

๔.๑๑.๑๖ ผู้ให้บริการ...

(นายทรงยศ ชญานินปรเมศ)	(นายสุรพงศ์ แสนโภชน์)	(นายศุภฤกษ์ ถวิลลาภ)	(นายนิรทร ศรีสุโข)	(นายจาฤพล ตวงศิริทรัพย์)	(นายภาณุพงศ์ ตันติรัตน์)	(นายราชี ปาลือชา)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

๔.๑๑.๑๖ ผู้ให้บริการจะต้องปฏิบัติตามเงื่อนไขระดับของบริการ Service Level Agreement (SLA) ดังนี้

ระดับความรุนแรง	คำอธิบาย	เวลาในการตอบสนอง (Response time)
Critical	ผลกระทบกับระบบสารสนเทศหลักทำให้ระบบหยุดชะงักและจะต้องแก้ไขอย่างเร่งด่วนที่สุด	ภายใน ๓๐ นาที
High	ผลกระทบกับระบบสารสนเทศที่ทำให้ระบบไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพและจำเป็นต้องแก้ไขอย่างเร่งด่วน	ภายใน ๓ ชั่วโมง
Medium	ผลกระทบกับระบบสารสนเทศทีมีผลต่อการดำเนินระบบและจำเป็นต้องแก้ไขอย่างทันท่วงที	ภายใน ๖ ชั่วโมง
Low	ผลกระทบกับระบบสารสนเทศที่มีผลต่อประสิทธิภาพการทำงานทั่วไป แต่ไม่มีผลกระทบต่อการดำเนินระบบโดยรวม	ภายใน ๒๔ ชั่วโมง

๔.๑๑.๑๗ ดำเนินงานบริการรับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident Response) รายงานวิเคราะห์ปัญหาที่เกิดจากภัยคุกคาม (Incident Report) ซึ่งจะต้องประกอบด้วย

- ระบุประเภทของภัยคุกคาม
- วัน - เวลาที่ตรวจสอบพบ
- ต้นทาง (Source IP Address) และ ปลางทาง (Destination IP Address)
- อุปกรณ์ที่ได้รับผลกระทบ และระดับความรุนแรง (Severity)
- รายละเอียดของเหตุการณ์ที่เกิดขึ้น
- คำแนะนำ และขั้นตอนในการแก้ไข (Action & Recommendation)

๔.๑๑.๑๘ รายงานสรุปผลการดำเนินงานแบบรายเดือนประกอบด้วย การวิเคราะห์ เฝ้าระวังเหตุการณ์ทั้งหมดที่เกิดขึ้น เหตุที่น่าสนใจ และเข้าร่วมประชุมเพื่ออธิบายสรุปผลการดำเนินงาน

๔.๑๑.๑๙ ผู้ให้บริการจะต้องมีใบรับรองความรู้ความสามารถด้าน cyber security เช่น Comptia Cysa + หรือเทียบเท่าอย่างน้อย ๑ คน

๔.๑๒ คุณสมบัติอื่นๆ

๔.๑๒.๑ สามารถควบคุมการทำงานของ Public Cloud โดยผ่านช่องทาง Self Service Portal หรือ Secure Shell หรือ Remote Desktop Protocol

๔.๑๒.๒ ผู้ให้บริการจะต้องให้บริการ Data Center และ Cloud Services

๔.๑๒.๓ Data Center ที่ติดตั้งอุปกรณ์ Cloud Service จะต้องได้รับมาตรฐาน ISO/IEC 27001 ด้าน Internet Data Center Service

๔.๑๒.๔ รองรับการให้บริการ Public Cloud มากกว่า ๑ Site เพื่อรองรับ Business Continuity Planning (BCP)

๔.๑๒.๕ มีวงจรเชื่อมโยงกับศูนย์แลกเปลี่ยนข้อมูลอินเทอร์เน็ตภายในประเทศ (National Internet Exchange: NIX) ไม่น้อยกว่าน้อย ๓ แห่ง และวงจรเชื่อมโยงกับศูนย์แลกเปลี่ยนข้อมูลอินเทอร์เน็ตเพื่อออกต่างประเทศ (International Internet Gateway: IIG) ไม่น้อยกว่าน้อย ๓ แห่ง ในกรณีที่ Gateway ใด Gateway หนึ่งขัดข้องก็สามารถใช้งานอีก Gateway ได้โดยอัตโนมัติ

๔.๑๒.๖ ผู้ให้บริการจะต้องระบุ Contact Point สำหรับแจ้งปัญหาหลังติดตั้ง

๔.๑๒.๗ กรณีเกิดเหตุที่มีผลต่อประสิทธิภาพการทำงานทั่วไป แต่ไม่มีผลกระทบต่อการดำเนินระบบโดยรวม...

(นายทรงยศ ชญานินปรเมศ)	(นายสุรพงศ์ แสนโภชน์)	(นายศุภฤกษ์ ถวิลลาภ)	(นายนิรทร ศรีสุโข)	(นายจารุพล ตวงศิริทรัพย์)	(นายภาณุพงศ์ ตันติรัตน์)	(นายราชิ ปาลือชา)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

ระบบโดยรวม ผู้ให้บริการต้องให้บริการสนับสนุน ให้คำปรึกษา และตอบสนองตลอด ๒๔ (ยี่สิบสี่) ชั่วโมง ตลอดอายุการรับประกัน

๔.๑๒.๘ กรณีที่เกิดเหตุอันส่งผลกระทบต่อระบบ ผู้ให้บริการต้องแก้ไขและซ่อมแซมปัญหาหรือข้อขัดข้องในการให้บริการให้ระบบสามารถกลับมาใช้งานได้ภายใน ๔ ชั่วโมง นับถัดจากเวลาที่ได้รับแจ้งเหตุ

๔.๑๒.๙ จัดเตรียมและพัฒนาแผงควบคุมด้านความปลอดภัย Cyber (Cyber Security Dashboard) โดยสามารถแสดงผลและตรวจสอบสถานการณ์ทำงาน SOC, SIEM รวมถึงการสำรองข้อมูลบนระบบเสมือน และตรวจสอบการโจมตีแบบการสุ่มเดารหัสการเข้าถึงระบบ (Brute force) และตรวจสอบการแจ้งเตือน Malware รวมถึง Access Control ผ่านช่องทางเครือข่ายสาธารณะ (Public) โดยการเข้าใช้ Dashboard จะต้องลงชื่อเข้าใช้งานผ่านระบบการยืนยันตัวตน ของกระทรวงสาธารณสุข พร้อมยื่นหลักฐานเอกสารประกอบ

๔.๑๓ กรณีระบบมีปริมาณการใช้งานเพิ่มขึ้นชั่วคราวไม่เกิน ๗ วันติดต่อกัน ผู้รับจ้างต้องดำเนินการเพิ่มทรัพยากร Cloud ให้ระบบใช้งานได้อย่างต่อเนื่อง ไม่เกินศักยภาพร้อยละ ๓๐ ของทรัพยากรที่กำหนดในสัญญา โดยไม่มีค่าใช้จ่ายเพิ่มเติม

๔.๑๔ ผู้ให้บริการบริการ Cloud Service ตามสัญญาฉบับนี้ ต้องทำการโอนย้ายข้อมูลและระบบต่าง ๆ จากระบบ Cloud เดิม มาที่ระบบ Cloud ของผู้ให้บริการโดยทันที โดยต้องไม่กระทบกับการใช้งานของระบบ รวมทั้งตรวจสอบความถูกต้องครบถ้วนและความสมบูรณ์ของข้อมูลหลังจากการโอนย้าย โดยผู้ชนะการประกวดราคาจะต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด รวมถึงค่าบริการของผู้ให้บริการรายเดิม กรณีโอนย้ายข้อมูลไม่ทันตามกำหนด

๔.๑๕ เมื่อครบกำหนดระยะเวลาการเช่า หากสำนักงานฯ มีความประสงค์ที่จะเช่าระบบ Cloud Computing ต่อไป ในระหว่างช่วงเวลาที่สำนักงานฯ ดำเนินการจัดหาผู้ให้บริการรายใหม่ หรือในระหว่างช่วงเวลาที่ผู้ให้บริการรายใหม่ดำเนินการย้ายระบบต่าง ๆ ที่อยู่บน Cloud Computing ของผู้ให้บริการรายเดิม ผู้ให้บริการจะยินยอมให้สำนักงานฯ ใช้บริการระบบ Cloud Computing ต่อไป ภายใต้เงื่อนไขของสัญญาฉบับนี้ เป็นระยะเวลาไม่เกิน ๙๐ วัน นับจากวันสิ้นสุดสัญญา

๔.๑๖ ผู้ให้บริการต้องดำเนินการลบ หรือทำลายข้อมูลทั้งหมดของสำนักงานฯ ที่จัดเก็บบนระบบ Cloud Service โดยสมบูรณ์ ภายใน ๓๐ วัน หลังจากวันที่สิ้นสุดสัญญา หรือวันที่บอกเลิกสัญญา โดยการทำลายข้อมูลต้องเป็นไปตามมาตรฐาน ISO/IEC 27001 หรือมาตรฐานการลบข้อมูลที่เทียบเท่า ทั้งนี้การดำเนินงานดังกล่าวต้องไม่กระทบกับระบบการทำงานอื่น ๆ ของสำนักงานฯ ที่ไม่เกี่ยวข้องกับข้อมูลที่จะทำลาย โดยผู้ให้บริการต้องจัดทำหนังสือรับรองการทำลายข้อมูล (Certificate of Data Destruction) ส่งมอบให้สำนักงานฯ ภายใน ๑๐ วันหลังจากดำเนินการแล้วเสร็จ

๕. ระยะเวลาการดำเนินการ

ระยะเวลา ๑๒ เดือน นับถัดจากวันที่ลงนามในสัญญา

๖. การส่งมอบงานและการจ่ายเงิน

สำนักงานฯ จะแบ่งชำระค่าบริการให้แก่ผู้ให้บริการเป็นรายเดือน รวมทั้งสิ้นจำนวน ๑๒ เดือน และผู้ให้บริการต้องส่งมอบงานในแต่ละงวด ดังนี้

งวด ๑ ...

(นายทรงยศ ชญานินปรเมศ)	(นายสุรพงศ์ แสนโภชน์)	(นายศุภฤกษ์ ถวิลลาภ)	(นายนิรทร ศรีสุโข)	(นายจารุพล ตวงศิริทรัพย์)	(นายภาณุพงศ์ ตันติรัตน์)	(นายราชี ปาลือชา)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

งวด	ระยะเวลาการดำเนินงาน	งานที่ส่งมอบ	การชำระเงิน
๑	๑ เดือน นับถัดจากวันที่ลงนามในสัญญา	จัดส่งเอกสารรายการ (๑) – (๙)*	ภายใน ๓๐ วันหลังจากส่งมอบงานเรียบร้อย
๒	๒ เดือน นับถัดจากวันที่ลงนามในสัญญา	จัดส่งเอกสารรายการ (๑) – (๙)*	ภายใน ๓๐ วันหลังจากส่งมอบงานเรียบร้อย
๓	๓ เดือน นับถัดจากวันที่ลงนามในสัญญา	จัดส่งเอกสารรายการ (๑) – (๙)*	ภายใน ๓๐ วันหลังจากส่งมอบงานเรียบร้อย
๔	๔ เดือน นับถัดจากวันที่ลงนามในสัญญา	จัดส่งเอกสารรายการ (๑) – (๙)*	ภายใน ๓๐ วันหลังจากส่งมอบงานเรียบร้อย
๕	๕ เดือน นับถัดจากวันที่ลงนามในสัญญา	จัดส่งเอกสารรายการ (๑) – (๙)*	ภายใน ๓๐ วันหลังจากส่งมอบงานเรียบร้อย
๖	๖ เดือน นับถัดจากวันที่ลงนามในสัญญา	จัดส่งเอกสารรายการ (๑) – (๙)*	ภายใน ๓๐ วันหลังจากส่งมอบงานเรียบร้อย
๗	๗ เดือน นับถัดจากวันที่ลงนามในสัญญา	จัดส่งเอกสารรายการ (๑) – (๙)*	ภายใน ๓๐ วันหลังจากส่งมอบงานเรียบร้อย
๘	๘ เดือน นับถัดจากวันที่ลงนามในสัญญา	จัดส่งเอกสารรายการ (๑) – (๙)*	ภายใน ๓๐ วันหลังจากส่งมอบงานเรียบร้อย
๙	๙ เดือน นับถัดจากวันที่ลงนามในสัญญา	จัดส่งเอกสารรายการ (๑) – (๙)*	ภายใน ๓๐ วันหลังจากส่งมอบงานเรียบร้อย
๑๐	๑๐ เดือน นับถัดจากวันที่ลงนามในสัญญา	จัดส่งเอกสารรายการ (๑) – (๙)*	ภายใน ๓๐ วันหลังจากส่งมอบงานเรียบร้อย
๑๑	๑๑ เดือน นับถัดจากวันที่ลงนามในสัญญา	จัดส่งเอกสารรายการ (๑) – (๙)*	ภายใน ๓๐ วันหลังจากส่งมอบงานเรียบร้อย
๑๒	๑๒ เดือน นับถัดจากวันที่ลงนามในสัญญา	จัดส่งเอกสารรายการ (๑) – (๙)*	ภายใน ๓๐ วันหลังจากส่งมอบงานเรียบร้อย

* หมายเหตุ ต้องมีการส่งมอบรายงานอุบัติการณ์ (Incident Report) และรายงานการแจ้งปัญหาการใช้งาน (Problem Report) ที่เกิดขึ้นในงวดนั้น (หากมี)

สำนักงานฯ จะชำระค่าเช่าให้ผู้ให้บริการแบ่งเป็น ๑๒ งวด งวดละเท่าๆ กัน โดยจะชำระเมื่อผู้ให้บริการส่งมอบงานและได้รับการตรวจรับจากคณะกรรมการตรวจรับเรียบร้อยแล้ว สำหรับงวดที่ ๑ ผู้ให้บริการต้องส่งมอบงานภายใน ๓๐ วัน นับจากวันลงนามในสัญญา และสำหรับงวดที่ ๒-๑๒ ผู้ให้บริการต้องส่งมอบงานภายในวันที่ ๕ ของเดือนถัดไป โดยในแต่ละงวดผู้ให้บริการต้องส่งมอบงาน ดังนี้

๑. รายงานผลการใช้งานระบบประจำงวด ประกอบด้วย รายงานประสิทธิภาพ (Performance Report) ของระบบคลาวด์ (Cloud Computing) ซึ่งระบุรายละเอียดปริมาณการใช้งานของ CPU, RAM และ Disk ในแต่ละ VM ทั้งค่าเฉลี่ยและค่าสูงสุดประจำ

๒. แผนผังสถาปัตยกรรมระบบทั้งหมด (Architecture Diagram) และเอกสารแผนผังเชิงตรรกะ (Logical Diagram) สำหรับระบบคลาวด์ (Cloud Services) ที่ให้บริการ โดยแสดงโครงสร้างและความสัมพันธ์ระหว่างองค์ประกอบต่างๆ, รายละเอียดของแต่ละเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (VM) ที่ใช้งาน, หมายเลข IP Address ทั้งภายในและภายนอกทั้งหมด, และการกำหนดค่าเครือข่ายและความปลอดภัย

๓. เอกสารแสดงรายละเอียดสถานที่ติดตั้งศูนย์คอมพิวเตอร์ Data Center พร้อมหมายเลขโทรศัพท์ติดต่อ Call Center และอีเมล

๔. เอกสารคู่มือการใช้งาน Cloud Portal

๕. รายการใช้งานระบบ (System Utilization) ของเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (VM) ทั้งหมด

๖. ข้อมูลการสำรองข้อมูล (Backup) ของเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (VM) ทั้งหมด

๗. ข้อมูลระดับของการให้บริการ (Service Level Agreement) ซึ่งระบุรายละเอียดเป้าหมาย

การให้บริการ...

(นายทรงยศ ชญานินปรเมศ)	(นายสุรพงศ์ แสนโภชน์)	(นายศุภฤกษ์ ถวิลสาภ)	(นายนิรทร ศรีสุโข)	(นายจารุพล ตวงศิริทรัพย์)	(นายภาณุพงศ์ ตันติรัตน์)	(นายราชิ ปาลือซา)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

การให้บริการด้านความพร้อมใช้งานของระบบ (System Availability), ประสิทธิภาพการทำงาน (Performance), ระยะเวลาตอบสนองต่อเหตุการณ์ (Response Time), ระยะเวลาในการแก้ไขปัญหา (Resolution Time), รวมถึงเงื่อนไขและบทปรับกรณีไม่เป็นไปตามข้อตกลง

๘. ข้อมูลจัดเก็บขอมูลจราจรคอมพิวเตอร์ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๙. ข้อมูลรายงานอุบัติการณ์ (Incident Report) และรายงานการแจ้งปัญหาการใช้ (Problem Report)

๑๐. รายงานอุบัติการณ์ (Incident Report) และรายงานการแจ้งปัญหาการใช้งาน (Problem Report) ที่เกิดขึ้นในงวดนั้น (หากมี)

โดยส่งมอบในรูปแบบเอกสาร จำนวน ๒ ชุด และในรูปแบบไฟล์อิเล็กทรอนิกส์นามสกุล .docx และ .pdf ใน CD หรือ Flash Drive จำนวน ๒ ชุด

๗. หลักเกณฑ์การพิจารณาข้อเสนอ

พิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ พิจารณาตัดสินโดยใช้เกณฑ์ราคา

๘. อัตราค่าปรับ

๘.๑ ในกรณีผู้ให้บริการไม่สามารถให้บริการได้ตามที่กำหนดไว้ในสัญญา ผู้ให้บริการจะต้องชำระค่าปรับให้แก่สำนักงานฯ เป็นรายวันในอัตราร้อยละ ๐.๒๐ ของราคาค่าเช่า จนกว่าผู้ให้บริการจะสามารถให้บริการแก่สำนักงานฯ ได้ ในระหว่างการเช่า

๘.๒ ในกรณีผู้ให้บริการไม่สามารถปฏิบัติงานแก้ไขปัญหาตามข้อกำหนดใน Service Level Agreement (SLA) หรือผู้ให้บริการไม่ได้ดำเนินการแก้ไขหรือไม่สามารถแก้ไขให้แล้วเสร็จสามารถใช้งานตามปกติได้ ภายในระยะเวลาที่กำหนดตาม SLA รวมไปถึงผู้ให้บริการกระทำหรืองดเว้นการกระทำใด ๆ อันทำให้ เกิดผลกระทบกับระบบฯ เป็นเหตุให้สำนักงานฯ ได้รับความเสียหายจากการกระทำนั้น ผู้ให้บริการต้องยินยอมให้สำนักงานฯ ทำการเรียกค่าปรับ โดยมูลค่าของค่าปรับจะถูกคำนวณจากเวลาที่เกินจากเวลา SLA โดยจะคำนวณคิดค่าปรับเป็นรายชั่วโมง ในส่วนที่เกินนับถัดจากเวลาที่ครบกำหนดถึงเวลาที่ผู้รับจ้างดำเนินการแก้ไขเหตุขัดข้องเสร็จ ถ้าเศษของเวลาที่เกินกำหนดไม่ถึงชั่วโมง ให้คิดเป็น ๑ ชั่วโมง

๘.๓ ผู้ให้บริการจะต้องส่งมอบบงานตามที่ระบุในข้อ ๖ ตามระยะเวลาการส่งมอบ หากไม่สามารถดำเนินงานได้เสร็จสิ้นตามระยะเวลาที่กำหนดในแต่ละงวดงาน สำนักงานฯ จะปรับเป็นรายวันในอัตราร้อยละ ๐.๑๐ ต่อวัน โดยเศษของวันนับเป็น ๑ วัน จนกว่าผู้ให้บริการจะส่งมอบงานตามขอบเขตที่ระบุไว้อย่างครบถ้วนและสมบูรณ์

๘.๔ เว้นแต่กรณีดังต่อไปนี้

๘.๔.๑ เกิดจากความผิดพลาดหรือความบกพร่องของบุคลากร หรืออุปกรณ์ ซึ่งมีส่วนสัมพันธ์และส่งผลกระทบโดยตรง ทำให้ผู้ให้บริการไม่สามารถให้บริการตามเงื่อนไขของข้อกำหนดคุณสมบัติขั้นต่ำได้

๘.๔.๒ เมื่อเกิดเหตุสุดวิสัย (Force Majeure) หมายถึง เหตุใดๆ อันจะเกิดขึ้นก็ดี จะให้ผลพิบัติก็ดี เป็นเหตุที่ไม่อาจป้องกันได้แม้ทั้งบุคคลผู้ต้องประสบหรือใกล้จะต้องประสบเหตุนั้น จะได้จัดการระมัดระวังตามสมควรอันพึงคาดหมายได้จากบุคคลในฐานนะและภาวะเช่นนั้น และมีผลกระทบต่อการให้บริการ ซึ่งหมายถึงไม่สามารถให้บริการระบบคลาวด์ได้อย่างต่อเนื่อง เช่น ภัยที่เกิดจากธรรมชาติ โรคระบาดการกระทำทางรัฐบาล การปฏิวัติรัฐประหาร การเกิดสงครามกลางเมือง การก่อกบฏ การก่อวินาศกรรม การก่อการร้าย การชุมนุม การจลาจล สารเคมีรั่วไหล เป็นต้น

๘.๕ ในกรณีที่ผู้ให้บริการไม่รักษาความลับของข้อมูลหรือทำการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตจากสำนักงานฯ ตามข้อ ๑๒ ผู้ให้บริการจะต้องชำระค่าปรับให้แก่สำนักงานฯ ในอัตราร้อยละ ๐.๒ ของมูลค่าสัญญาทั้งหมดต่อครั้งที่มีการกระทำผิด และในกรณีที่การละเมิดดังกล่าวก่อให้เกิดความเสียหายต่อสำนักงานฯ หรือบุคคลที่สาม ผู้ให้บริการจะต้องรับผิดชอบชดใช้ค่าเสียหายที่เกิดขึ้นทั้งหมดนอกเหนือจากค่าปรับดังกล่าว ทั้งนี้สำนักงานฯ มีสิทธิ์ในการยกเลิกสัญญาได้ทันทีโดยไม่ต้องบอกกล่าวล่วงหน้า

๙. งบประมาณ...

(นายทรงยศ ชญานินปรเมศ)	(นายสุรพงศ์ แสนโภชน์)	(นายศุภฤกษ์ ถวิลลาภ)	(นายนิรทร ศรีสุโข)	(นายจรุพล ตวงศิริทรัพย์)	(นายภาณุพงศ์ ตันติรัตน์)	(นายรวี ปาลือชา)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

๙. งบประมาณ

งบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๘ งบดำเนินงาน สำนักงานปลัดกระทรวงสาธารณสุข จำนวน ๕๙,๕๓๒,๓๐๐ บาท (ห้าสิบเก้าล้านห้าแสนสามหมื่นสองพันสามร้อยบาทถ้วน)

๑๐. การรับประกันความชำรุดบกพร่องของงานจ้าง

๑๐.๑ ผู้ให้บริการต้องรับประกันการให้บริการตามรายละเอียดขอบเขตของงานภายในกำหนดระยะเวลา ๑ ปี นับถัดจากวันที่ได้รับมอบงานดังกล่าว รวมถึงการย้ายระบบต่างๆ ที่อยู่บน Cloud Computing ของสำนักงานฯ รายเดิม

๑๐.๒ ระยะเวลาการรับประกันเริ่มต้นเมื่อคณะกรรมการตรวจรับพัสดุได้ตรวจรับงานเรียบร้อยครบถ้วน

๑๐.๓ หากมีเหตุชำรุดบกพร่องหรือเสียหายเกิดขึ้นแก่ระบบ ซึ่งความชำรุดบกพร่องหรือเสียหายนั้นเกิดจากความบกพร่องของผู้ให้บริการ ผู้ให้บริการต้องรีบทำการแก้ไขให้ระบบใช้งานได้ตามปกติ ภายใน SLA ที่ระบุไว้ นับถัดจากเวลาที่ได้รับแจ้งเหตุ โดยผู้ให้บริการไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

ในกรณีเร่งด่วนจำเป็นต้องรีบแก้ไขเหตุชำรุดบกพร่องหรือเสียหายโดยเร็ว และไม่อาจรอให้ผู้ให้บริการแก้ไขในระยะเวลาที่กำหนดไว้ได้ สำนักงานฯ มีสิทธิเข้าจัดการแก้ไขเหตุชำรุดบกพร่องหรือเสียหายนั้นเอง หรือจ้างผู้อื่นให้ซ่อมแซมความชำรุดบกพร่องหรือเสียหาย โดยผู้ให้บริการต้องรับผิดชอบชำระค่าใช้จ่ายทั้งหมดแก่สำนักงานฯ ที่ สำนักงานฯ ได้ชำระไปก่อนหน้าทั้งสิ้น

๑๑. ทรัพย์สินทางปัญญา

๑. สิทธิในทรัพย์สินทางปัญญาที่มีอยู่เดิม (Pre-existing Intellectual Property)

ทรัพย์สินทางปัญญา ความลับทางการค้า เทคโนโลยี องค์ความรู้และข้อมูลที่คู่สัญญาฝ่ายใดฝ่ายหนึ่งเป็นเจ้าของอยู่ก่อนการดำเนินงานโครงการนี้ ให้ยังคงเป็นกรรมสิทธิ์ของฝ่ายนั้น แม้จะนำมาใช้ในการดำเนินงานโครงการนี้ก็ตาม การดำเนินงานตามโครงการนี้ไม่ถือเป็นการอนุญาตให้คู่สัญญาฝ่ายหนึ่งฝ่ายใดมีสิทธิใช้ประโยชน์จากทรัพย์สินทางปัญญาของอีกฝ่ายนอกเหนือไปจากขอบเขตที่ระบุไว้ในสัญญา เว้นแต่จะได้ตกลงกันเป็นลายลักษณ์อักษร

๒. สิทธิในทรัพย์สินทางปัญญาที่พัฒนาร่วมกัน (Joint Intellectual Property)

ทรัพย์สินทางปัญญาหรือลิขสิทธิ์ใดๆ ที่เกิดขึ้นจากการร่วมกันพัฒนาของทั้งสองฝ่ายในระหว่างการดำเนินงานโครงการนี้ ให้ถือเป็นกรรมสิทธิ์ร่วมของทั้งสองฝ่าย โดยแต่ละฝ่ายมีสิทธินำไปพัฒนาต่อยอดได้ แต่ต้องไม่กระทบต่อสิทธิของอีกฝ่ายที่มีอยู่หรือจะเกิดขึ้นในอนาคต ทั้งนี้ ฝ่ายที่ประสงค์จะพัฒนาต่อยอดจะต้องแจ้งให้อีกฝ่ายทราบเป็นลายลักษณ์อักษรล่วงหน้า และอีกฝ่ายจะปฏิเสธได้เฉพาะในกรณีที่มีเหตุผลอันสมควรเท่านั้น สิทธิในทรัพย์สินทางปัญญาที่เกิดจากการพัฒนาต่อยอดนั้นให้เป็นของฝ่ายที่ดำเนินการพัฒนาต่อยอด

๓. ข้อจำกัดการใช้ทรัพย์สินทางปัญญา

ทั้งสองฝ่ายตกลงจะไม่นำทรัพย์สินทางปัญญา ความลับทางการค้า เทคโนโลยี องค์ความรู้และข้อมูลที่เกิดขึ้นจากการดำเนินงานตามโครงการนี้ไปให้บริการหรือเปิดเผยแก่บุคคลภายนอก เว้นแต่จะได้รับความยินยอมเป็นลายลักษณ์อักษรจากอีกฝ่ายหนึ่ง

๑๒. การรักษาความลับของข้อมูล

ผู้ให้บริการต้องลงนามใน “สัญญาการเก็บรักษาข้อมูลที่เป็นความลับและข้อตกลงการประมวลผลข้อมูลส่วนบุคคล Non-Disclosure Agreement (NDA) and Data Processing Agreement (DPA)” พร้อมกับสัญญาฉบับนี้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลจากการดำเนินงานตามสัญญานี้เป็นความลับ และจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม ผู้ให้บริการจะไม่ดำเนินการใด ๆ กับข้อมูลบน Cloud ของสำนักงานฯ โดยเด็ดขาด

เว้นแต่...

(นายทรงยศ ชญานินปรเมศ)	(นายสุรพงศ์ แสนโภชน์)	(นายศุภฤกษ์ ถวิลลาภ)	(นายนิรทร ศรีสุโข)	(นายจารุพล ตวงศิริทรัพย์)	(นายภาณุพงศ์ ตันติรัตน์)	(นายราชี ปาลือซา)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

เว้นแต่จะได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจตามสัญญาเท่านั้น และจะไม่ปฏิบัติตามคำสั่งจากบุคลากรของสำนักงานฯ ที่ไม่มีอำนาจโดยตรง แม้จะอ้างว่าได้รับมอบหมายจากผู้บริหารก็ตาม กรณีฉุกเฉินต้องแจ้งและได้รับอนุมัติก่อนดำเนินการ หากละเมิดข้อกำหนดนี้ถือเป็นการผิดสัญญาร้ายแรง

ในกรณีที่ผู้ให้บริการไม่รักษาความลับของข้อมูลหรือทำการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตจากสำนักงานฯ ผู้ให้บริการจะต้องชำระค่าปรับ ตามข้อ ๘.๕

๑๓. หน่วยงานผู้รับผิดชอบ

สำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข

๑๔. เงื่อนไขการยื่นข้อเสนอและเอกสารแนบท้าย

๑๔.๑ เงื่อนไขการยื่นข้อเสนอ

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

๑๔.๒ เอกสารแนบท้าย

เอกสารแนบท้ายต่อไปนี้ให้ถือเป็นส่วนหนึ่งของข้อกำหนดและขอบเขตของงาน (Terms of Reference) ฉบับนี้

- เอกสารแนบท้าย ๑ แบบสัญญาการเก็บรักษาข้อมูลที่เป็นความลับและข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (NDA และ DPA)
- เอกสารแนบท้าย ๒ ข้อกำหนดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยไซเบอร์

(ลงชื่อ) ..... ประธานกรรมการ
(นายทรงยศ ชญานินปรเมศ)
ตำแหน่ง นายแพทย์เชี่ยวชาญ

(ลงชื่อ) ..... กรรมการ
(นายสุรพงศ์ แสนโภชน์)
ตำแหน่ง นายแพทย์ชำนาญการพิเศษ

(ลงชื่อ) ..... กรรมการ
(นายศุภฤกษ์ ถวิลลาภ)
ตำแหน่ง นายแพทย์ชำนาญการพิเศษ

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

(ลงชื่อ) ..... กรรมการ
(นายภาณุพงศ์ ตันติรัตน์)
ตำแหน่ง นายแพทย์ชำนาญการพิเศษ

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

(ลงชื่อ) ..... กรรมการ
(นายราชิ ปาลือชา)
ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ