ประกาศจังหวัดเชียงใหม่

เรื่อง ประกวดราคาเช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์ของโรงพยาบาลนครพิงค์ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข จำนวน ๑ ระบบ ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

จังหวัดเชียงใหม่ มีความประสงค์จะประกวดราคาเช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์ของโรงพยาบาลนครพิงค์ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข จำนวน ๑ ระบบ ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ราคากลางของงานเช่า ในการประกวดราคาครั้งนี้ เป็นเงินทั้งสิ้น ๑,๙๗๓,๖๘๐.๐๐ บาท (หนึ่งล้านเก้าแสนเจ็ดหมื่นสามพันหกร้อยแปดสิบบาทถ้วน) จำนวน ๑ รายการ

ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอโดยแสดงหลักฐานถึงขีดความสามารถและความพร้อมที่มีอยู่ในวันยื่นข้อเสนอ โดยมีรายละเอียดดังนี้

๑. ผู้ยื่นข้อเสนอจะต้องมีคุณสมบัติให้เป็นไปตามเอกสารประกวดราคาอิเล็กทรอนิกส์กำหนด

๒. ผู้ยื่นข้อเสนอต้องเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ในวันที่ ๑๕ ก.ค. ๒๕๖๘ ระหว่างเวลา ๑๓.๐๐ น. ถึง ๑๖.๐๐ น. ซึ่งสามารถจัดเตรียมเอกสารข้อเสนอได้ตั้งแต่วันที่ประกาศจนถึงวันเสนอราคา

๓. ผู้สนใจสามารถดูรายละเอียดและดาวน์โหลดเอกสารประกวดราคาอิเล็กทรอนิกส์เลขที่ ๑๔๐/๒๕๖๘ ลงวันที่ ๔ กรกฎาคม พ.ศ. ๒๕๖๘ ผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ ได้ตั้งแต่วันที่ประกาศจนถึงวันเสนอราคา ได้ที่เว็บไซต์ http://www.nkp-hospital.go.th/th/nkpNews1.php หรือ www.gprocurement.go.th ทั้งนี้ หากต้องการทราบรายละเอียดเพิ่มเติมเกี่ยวกับรายละเอียดคุณลักษณะเฉพาะ โปรดสอบถามมายัง จังหวัดเชียงใหม่ ผ่านทางไปรษณีย์อิเล็กทรอนิกส์ หรือช่องทางตามที่กรมบัญชีกลางกำหนด ภายในวันที่ ในเวลาราชการ โดยจังหวัดเชียงใหม่ จะชี้แจงรายละเอียดดังกล่าวผ่านทางเว็บไซต์ http://www.nkp-hospital.go.th/th/nkpNews1.php และ www.gprocurement.go.th ในวันที่

ประกาศ ณ วันที่ ๔ กรกฎาคม พ.ศ. ๒๕๖๘

(นายพงษ์ศักดิ์ โสภณ)

ผู้อำนวยการโรงพยาบาลนครพิงค์

ปฏิบัติราชการแทนผู้ว่าราชการจังหวัดเชียงใหม่

เอกสารประกวดราคาเช่าด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

เลขที่ ๑๔๐/๒๕๖๘

การเช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์ของโรงพยาบาลนครพิงค์ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข จำนวน ๑ ระบบ

ตามประกาศ จังหวัดเชียงใหม่

ลงวันที่ ๕ กรกฎาคม ๒๕๖๘

จังหวัดเชียงใหม่ ซึ่งต่อไปนี้เรียกว่า "จังหวัด" มีความประสงค์จะประกวดราคาเช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์ของโรงพยาบาลนครพิงค์ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข จำนวน ๑ ระบบ ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ตามรายการ ดังนี้

เช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์ของโรงพยาบาลนครพิงค์ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข	จำนวน	๑	ระบบ

พัสดุที่จะเช่านี้ต้องเป็นของแท้ ไม่เป็นของเก่าเก็บ อยู่ในสภาพที่จะใช้งานได้ทันที และมีคุณลักษณะเฉพาะตรงตามที่กำหนดไว้ในเอกสารประกวดราคาเช่าด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ฉบับนี้ โดยมีข้อแนะนำและข้อกำหนด ดังต่อไปนี้

๑. **เอกสารแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์**

๑.๑ รายละเอียดคุณลักษณะเฉพาะ

๑.๒ แบบใบเสนอราคาที่กำหนดไว้ในระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๑.๓ แบบสัญญาเช่าคอมพิวเตอร์

๑.๔ แบบหนังสือค้ำประกัน

(๑) หลักประกันสัญญา

๑.๕ บทนิยาม

(๑) ผู้มีผลประโยชน์ร่วมกัน

(๒) การขัดขวางการแข่งขันอย่างเป็นธรรม

๑.๖ แบบบัญชีเอกสารที่กำหนดไว้ในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

(๑) บัญชีเอกสารส่วนที่ ๑

(๒) บัญชีเอกสารส่วนที่ ๒

๒. คุณสมบัติของผู้ยื่นข้อเสนอ

๒.๑ มีความสามารถตามกฎหมาย

๒.๒ ไม่เป็นบุคคลล้มละลาย

๒.๓ ไม่อยู่ระหว่างเลิกกิจการ

๒.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบ ที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๒.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๒.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๒.๗ เป็นนิติบุคคลผู้มีอาชีพให้เช่าพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๒.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ จังหวัด ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวาง การแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๒.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๒.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

(๑) การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

(๒) กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

(๓) การยื่นข้อเสนอของกิจการร่วมค้า

(๓.๑) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

(๓.๒) การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e - bidding) ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ (๓.๑) ดำเนินการซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารซื้อหรือจ้าง

ซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ เพื่อประกอบการพิจารณา หลักฐานดังกล่าวนี้ จังหวัดจะยึดไว้เป็นเอกสารของทางราชการ

สำหรับแค็ตตาล็อกที่แนบให้พิจารณา หากเป็นสำเนา และคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ มีความประสงค์จะขอดูต้นฉบับแคตตาล็อก ผู้ยื่นข้อเสนอจะต้องนำต้นฉบับมาให้คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ตรวจสอบภายใน ๕ วัน นับถัดจากวันเสนอราคา

๔.๕ ก่อนเสนอราคา ผู้ยื่นข้อเสนอควรตรวจดูร่างสัญญา รายละเอียดคุณลักษณะเฉพาะ ของพัสดุให้ถี่ถ้วนและเข้าใจเอกสารประกวดราคาอิเล็กทรอนิกส์ทั้งหมดเสียก่อนที่จะตกลงยื่นข้อเสนอตามเงื่อนไข ในเอกสารประกวดราคาอิเล็กทรอนิกส์

๔.๖ ผู้ยื่นข้อเสนอจะต้องยื่นข้อเสนอและเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐ ด้วยอิเล็กทรอนิกส์ในวันที่ ๑๕ ก.ค. ๒๕๖๘ ระหว่างเวลา ๑๓.๐๐ น. ถึง ๑๖.๐๐ น. และเวลาในการเสนอราคาให้ถือตามเวลาของระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์เป็นเกณฑ์

เมื่อพ้นกำหนดเวลายื่นข้อเสนอและเสนอราคาแล้ว จะไม่รับเอกสารการยื่นข้อเสนอและการเสนอราคาใดๆ โดยเด็ดขาด

๔.๗ ผู้ยื่นข้อเสนอต้องจัดทำเอกสารสำหรับใช้ในการเสนอราคาในรูปแบบไฟล์เอกสารประเภท PDF File (Portable Document Format) โดยผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบตรวจสอบความครบถ้วนถูกต้อง และชัดเจนของเอกสาร PDF File ก่อนที่จะยืนยันการเสนอราคา แล้วจึงส่งข้อมูล (Upload) เพื่อเป็นการเสนอราคาให้แก่ จังหวัด ผ่านทางระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์

๔.๘ คณะกรรมการพิจารณาผลฯ จะดำเนินการตรวจสอบคุณสมบัติของผู้ยื่นข้อเสนอแต่ละรายว่า เป็นผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่น ตามข้อ ๑.๕ (๑) หรือไม่ หากปรากฏว่าผู้ยื่นข้อเสนอรายใดเป็นผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่น คณะกรรมการพิจารณาผลฯ จะตัดรายชื่อผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันนั้นออกจากการเป็นผู้ยื่นข้อเสนอ

หากปรากฏต่อคณะกรรมการพิจารณาผลฯ ว่า ก่อนหรือ ในขณะที่มีการพิจารณาข้อเสนอ มีผู้ยื่นข้อเสนอรายใดกระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมตามข้อ ๑.๕ (๒) และคณะกรรมการพิจารณาผลฯ เชื่อว่ามีการกระทำอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม คณะกรรมการพิจารณาผลฯ จะตัดรายชื่อผู้ยื่นข้อเสนอรายนั้นออกจากการเป็นผู้ยื่นข้อเสนอ และ จังหวัด จะพิจารณาลงโทษผู้ยื่นข้อเสนอดังกล่าวเป็นผู้ทิ้งงาน เว้นแต่ จังหวัด จะพิจารณาเห็นว่า ผู้ยื่นข้อเสนอรายนั้นมิใช่เป็นผู้ริเริ่มให้มีการกระทำดังกล่าวและได้ให้ความร่วมมือเป็นประโยชน์ ต่อการพิจารณาของ จังหวัด

๔.๙ ผู้ยื่นข้อเสนอจะต้องปฏิบัติ ดังนี้

(๑) ปฏิบัติตามเงื่อนไขที่ระบุไว้ในเอกสารประกวดราคาอิเล็กทรอนิกส์

(๒) ราคาที่เสนอจะต้องเป็นราคาที่รวมภาษีมูลค่าเพิ่ม และภาษีอื่นๆ (ถ้ามี) รวมค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว

(๓) ผู้ยื่นข้อเสนอจะต้องลงทะเบียนเพื่อเข้าสู่กระบวนการเสนอราคา ตามวัน เวลา ที่กำหนด

(๔) ผู้ยื่นข้อเสนอจะถอนการเสนอราคาที่เสนอแล้วไม่ได้

(๕) ผู้ยื่นข้อเสนอต้องศึกษาและทำความเข้าใจในระบบและวิธีการเสนอราคา ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ ของกรมบัญชีกลางที่แสดงไว้ในเว็บไซต์ www.gprocurement.go.th

๕. หลักเกณฑ์และสิทธิ์ในการพิจารณา

๕.๑ ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ จังหวัดจะพิจารณาตัดสินโดยใช้ หลักเกณฑ์ราคา

๕.๒ การพิจารณาผู้ชนะการยื่นข้อเสนอ

กรณีใช้หลักเกณฑ์ราคาในการพิจารณาผู้ชนะการยื่นข้อเสนอ จังหวัด จะพิจารณาจากราคารวม

๕.๓ หากผู้ยื่นข้อเสนอรายใดมีคุณสมบัติไม่ถูกต้องตามข้อ ๒ หรือยื่นหลักฐานการยื่นข้อเสนอไม่ถูกต้อง หรือไม่ครบถ้วนตามข้อ ๓ หรือยื่นข้อเสนอไม่ถูกต้องตามข้อ ๔ คณะกรรมการพิจารณาผลฯ จะไม่รับพิจารณาข้อเสนอของผู้ยื่นข้อเสนอรายนั้น เว้นแต่ ผู้ยื่นข้อเสนอรายใด เสนอเอกสารทางเทคนิคหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะให้เช่าไม่ครบถ้วน หรือเสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่จังหวัดกำหนดไว้ในประกาศและเอกสารประกวดราคาอิเล็กทรอนิกส์ ในส่วนที่มิใช่สาระสำคัญและความแตกต่างนั้นไม่มีผลทำให้เกิดการได้เปรียบเสียเปรียบ ต่อผู้ยื่นข้อเสนอรายอื่น หรือเป็นการผิดพลาดเล็กน้อย คณะกรรมการพิจารณาผลฯ อาจพิจารณาผ่อนปรนการตัดสิทธิ ผู้ยื่นข้อเสนอรายนั้น

๕.๔ จังหวัดสงวนสิทธิ์ไม่พิจารณาข้อเสนอของผู้ยื่นข้อเสนอโดยไม่มีการผ่อนผัน ในกรณีดังต่อไปนี้

(๑) ไม่กรอกชื่อผู้ยื่นข้อเสนอในการเสนอราคาทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์

(๒) เสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่กำหนดในเอกสารประกวดราคาอิเล็กทรอนิกส์ที่เป็นสาระสำคัญ หรือมีผลทำให้เกิดความได้เปรียบเสียเปรียบแก่ผู้ยื่นข้อเสนอรายอื่น

๕.๕ ในการตัดสินการประกวดราคาอิเล็กทรอนิกส์หรือในการทำสัญญา คณะกรรมการพิจารณาผลฯ หรือจังหวัดมีสิทธิให้ผู้ยื่นข้อเสนอชี้แจงข้อเท็จจริงเพิ่มเติมได้ จังหวัด มีสิทธิที่จะไม่รับข้อเสนอ ไม่รับราคา หรือไม่ทำสัญญา หากข้อเท็จจริงดังกล่าว ไม่เหมาะสมหรือไม่ถูกต้อง

๕.๖ จังหวัดทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดก็ได้ และอาจพิจารณาเลือกเช่าในจำนวน หรือขนาด หรือเฉพาะรายการหนึ่งรายการใด หรืออาจจะยกเลิกการประกวดราคาอิเล็กทรอนิกส์โดยไม่พิจารณาเช่าเลยก็ได้ สุดแต่จะพิจารณา ทั้งนี้ เพื่อประโยชน์ของทางราชการเป็นสำคัญ และให้ถือว่าการตัดสินของ จังหวัดเป็นเด็ดขาด ผู้ยื่นข้อเสนอจะเรียกร้องค่าใช้จ่าย หรือค่าเสียหายใดๆ มิได้ รวมทั้งจังหวัด จะพิจารณายกเลิกการประกวดราคาอิเล็กทรอนิกส์และลงโทษผู้ยื่นข้อเสนอเป็นผู้ทิ้งงาน ไม่ว่าจะเป็นผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่เชื่อถือได้ว่าการยื่นข้อเสนอกระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ชื่อบุคคลธรรมดา หรือนิติบุคคลอื่นมาเสนอราคาแทน เป็นต้น

ในกรณีที่ผู้ยื่นข้อเสนอรายที่เสนอราคาต่ำสุด เสนอราคาต่ำจนคาดหมายได้ว่าไม่อาจดำเนินงานตามเอกสารประกวดราคาอิเล็กทรอนิกส์ได้ คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์หรือจังหวัด จะให้ผู้ยื่นข้อเสนอนั้นชี้แจงและแสดงหลักฐานที่ทำให้เชื่อได้ว่า ผู้ยื่นข้อเสนอสามารถดำเนินการตามเอกสารประกวดราคาอิเล็กทรอนิกส์ให้เสร็จสมบูรณ์ หากคำชี้แจงไม่เป็นที่รับฟังได้ จังหวัด มีสิทธิที่จะไม่รับข้อเสนอหรือไม่รับราคาของผู้ยื่นข้อเสนอรายนั้น ทั้งนี้ ผู้ยื่นข้อเสนอดังกล่าวไม่มีสิทธิเรียกร้องค่าใช้จ่ายหรือค่าเสียหายใดๆ จากจังหวัด

๕.๗ ก่อนลงนามในสัญญาจังหวัดอาจประกาศยกเลิกการประกวดราคาอิเล็กทรอนิกส์ หากปรากฏว่ามีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการประกวดราคาหรือที่ได้รับการคัดเลือกมีผลประโยชน์ร่วม

กัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือส่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา

๕.๘ หากผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs เสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นที่ไม่เกินร้อยละ ๑๐ ให้จัดซื้อจัดจ้างกับผู้ประกอบการ SMEs ดังกล่าว โดยจัดเรียงลำดับผู้ยื่นข้อเสนอซึ่งเป็นผู้ประกอบการ SMEs ซึ่งเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ ๑๐ ที่จะเรียกมาทำสัญญาไม่เกิน ๓ ราย

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกรายจะต้องเป็นผู้ประกอบการ SMEs

ทั้งนี้ ผู้ประกอบการ SMEs ที่จะได้แต้มต่อด้านราคาตามวรรคหนึ่ง จะต้องมีวงเงินสัญญาสะสมตามปีปฏิทินรวมกับราคาที่เสนอในครั้งนี้แล้ว มีมูลค่ารวมกันไม่เกินมูลค่าของรายได้ตามขนาดที่ขึ้นทะเบียนไว้กับ สสว.

๕.๙ หากผู้ยื่นข้อเสนอได้เสนอพัสดุที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทย (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย เสนอราคาสูงกว่าราคาต่ำสุดของผู้เสนอราคารายอื่น ไม่เกินร้อยละ ๕ ให้จัดซื้อจัดจ้างจากผู้ยื่นข้อเสนอที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิต ภายในประเทศไทย (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย

กรณีที่มีการเสนอราคาหลายรายการและกำหนดเงื่อนไขการพิจารณาราคารวม หากผู้ยื่นข้อเสนอได้เสนอพัสดุที่เป็นพัสดุที่ผลิตภายในประเทศ ที่ได้รับการรับรองและออกเครื่องหมายสินค้าที่ผลิตภายในประเทศไทย (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย มีสัดส่วนมูลค่าตั้งแต่ร้อยละ ๖๐ ขึ้นไป ให้ได้แต้มต่อในการเสนอราคาตามวรรคหนึ่ง

อนึ่ง หากในการเสนอราคาครั้งนั้น ผู้ยื่นข้อเสนอรายใดมีคุณสมบัติทั้งข้อ ๕.๘ และข้อ ๕.๙ ให้ผู้ยื่นข้อเสนอรายนั้นได้แต้มต่อในการเสนอราคาสูงกว่าผู้ยื่นข้อเสนอรายอื่นไม่เกินร้อยละ ๑๕

๕.๑๐ หากผู้ยื่นข้อเสนอซึ่งมิใช่ผู้ประกอบการ SMEs แต่เป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยเสนอราคาสูงกว่าราคาต่ำสุดของผู้ยื่นข้อเสนอซึ่งเป็นบุคคลธรรมดาที่มิได้ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายของต่างประเทศไม่เกินร้อยละ ๓ ให้จัดซื้อจัดจ้างกับบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยดังกล่าว

ผู้ยื่นข้อเสนอที่เป็นกิจการร่วมค้าที่จะได้สิทธิตามวรรคหนึ่ง ผู้เข้าร่วมค้าทุกรายจะต้องเป็นบุคคลธรรมดาที่ถือสัญชาติไทยหรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย

๖. การทำสัญญาเช่า

๖.๑ ในกรณีที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ สามารถส่งมอบพัสดุที่ให้เช่าได้ครบถ้วนภายใน ๕ วันทำการ นับแต่วันที่ทำข้อตกลงเช่า จังหวัดจะพิจารณาจัดทำข้อตกลงเป็นหนังสือแทน การทำสัญญาตามแบบสัญญาดังระบุ ในข้อ ๑.๓ ก็ได้

๖.๒ ในกรณีที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ไม่สามารถส่งมอบสิ่งของได้ครบถ้วนภายใน ๕ วันทำการ หรือ จังหวัดเห็นว่าไม่สมควรจัดทำข้อตกลงเป็นหนังสือ ตามข้อ ๖.๑ ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์จะต้องทำสัญญาเช่าตามแบบสัญญาดังระบุในข้อ ๑.๓ หรือทำข้อตกลงเป็นหนังสือ กับจังหวัดภายใน ๗ วัน นับถัดจากวันที่ได้รับแจ้ง และจะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละ ๕ ของราคาค่าพัสดุที่ให้เช่าที่ประกวดราคาอิเล็กทรอนิกส์ให้จังหวัดยึดถือไว้ในขณะทำสัญญา โดยใช้หลักประกันอย่างหนึ่งอย่างใดดังต่อไปนี้

(๑) เงินสด

(๒) เช็คหรือดราฟท์ที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือดราฟท์ลงวันที่ที่ใช้เช็ค หรือดราฟท์นั้นชำระต่อเจ้าหน้าที่ในวันทำสัญญา หรือก่อนวันนั้นไม่เกิน ๓ วันทำการ

(๓) หนังสือค้ำประกันของธนาคารภายในประเทศ ตามตัวอย่างที่คณะกรรมการนโยบายกำหนด ดังระบุในข้อ ๑.๔ (๒) หรือจะเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนด

(๔) หนังสือค้ำประกันของบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือ ค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด ดังระบุในข้อ ๑.๔ (๒)

(๕) พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้ โดยไม่มีดอกเบี้ยภายใน ๑๕ วัน นับถัดจากวันที่ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ (ผู้ให้เช่า) พ้นจากข้อผูกพันตามสัญญาเช่าแล้ว

หลักประกันนี้จะคืนให้ โดยไม่มีดอกเบี้ย ตามอัตราส่วนของพัสดุที่ให้เช่าซึ่งจังหวัด ได้รับมอบไว้แล้ว

๗. ค่าจ้างและการจ่ายเงิน

จังหวัด จะจ่ายค่าเช่าซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงด้วยแล้วให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ให้เช่า เมื่อผู้ให้เช่าได้ส่งมอบพัสดุที่ให้เช่าครบถ้วนตามสัญญาเช่าหรือข้อตกลงเป็นหนังสือ และจังหวัดได้ตรวจรับมอบพัสดุที่ให้เช่าไว้เรียบร้อยแล้ว โดยแบ่งออกเป็น ๑๒ งวดดังนี้

งวดที่ ๑ เป็นจำนวนเงินในอัตราร้อยละ ๘.๓๗ ของค่าเช่า เมื่อผู้ให้เช่าได้ให้เช่าเช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์ของโรงพยาบาลนครพิงค์ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข จำนวน ๑ ระบบ งวดที่ ๑ ให้แล้วเสร็จภายใน ๓๑ วัน

งวดที่ ๒ เป็นจำนวนเงินในอัตราร้อยละ ๘.๓๓ ของค่าเช่า เมื่อผู้ให้เช่าได้ให้เช่าเช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์ของโรงพยาบาลนครพิงค์ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข จำนวน ๑ ระบบ งวดที่ ๒ ให้แล้วเสร็จภายใน ๖๒ วัน

งวดที่ ๓ เป็นจำนวนเงินในอัตราร้อยละ ๘.๓๓ ของค่าเช่า เมื่อผู้ให้เช่าได้ให้เช่าเช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์ของโรงพยาบาลนครพิงค์ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข จำนวน ๑ ระบบ งวดที่ ๓ ให้แล้วเสร็จภายใน ๙๒ วัน

งวดที่ ๔ เป็นจำนวนเงินในอัตราร้อยละ ๘.๓๓ ของค่าเช่า เมื่อผู้ให้เช่าได้ให้เช่าเช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์ของโรงพยาบาลนครพิงค์ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข จำนวน ๑ ระบบ งวดที่ ๔ ให้แล้วเสร็จภายใน ๑๒๓ วัน

งวดที่ ๕ เป็นจำนวนเงินในอัตราร้อยละ ๘.๓๓ ของค่าเช่า เมื่อผู้ให้เช่าได้ให้เช่าเช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์ของโรงพยาบาลนครพิงค์ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข จำนวน ๑ ระบบ งวดที่ ๕ ให้แล้วเสร็จภายใน ๑๕๓ วัน

งวดที่ ๖ เป็นจำนวนเงินในอัตราร้อยละ ๘.๓๓ ของค่าเช่า เมื่อผู้ให้เช่าได้ให้เช่าเช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์ของโรงพยาบาลนครพิงค์ภายใต้โครงการ

(๑) แจ้งการสั่งหรือนำพัสดุที่ให้เช่าที่เช่าดังกล่าวเข้ามาจากต่างประเทศต่อกรมเจ้าท่าภายใน ๗ วัน นับตั้งแต่วันที่ผู้ให้เช่าสั่ง หรือเช่าของจากต่างประเทศ เว้นแต่เป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่นได้

(๒) จัดการให้สิ่งของที่เช่าดังกล่าวบรรทุกโดยเรือไทย หรือเรือที่มีสิทธิเช่นเดียวกับเรือไทย จากต่างประเทศมายังประเทศไทย เว้นแต่จะได้รับอนุญาตจากกรมเจ้าท่า ให้บรรทุกสิ่งของนั้นโดยเรืออื่นที่มิใช่เรือไทย ซึ่งจะต้องได้รับอนุญาตเช่นนั้นก่อนบรรทุกของลงเรืออื่น หรือเป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่น

(๓) ในกรณีที่ไม่ปฏิบัติตาม (๑) หรือ (๒) ผู้ให้เช่าจะต้องรับผิดตามกฎหมายว่าด้วยการส่งเสริมการพาณิชยนาวี

๑๐.๓ ผู้ยื่นข้อเสนอซึ่งจังหวัดได้คัดเลือกแล้ว ไม่ไปทำสัญญาหรือข้อตกลงเช่า เป็นหนังสือภายในเวลาที่กำหนด ดังระบุไว้ในข้อ ๖ จังหวัดจะริบหลักประกันการยื่นข้อเสนอ หรือเรียกร้องจากผู้ออกหนังสือค้ำประกันการยื่นข้อเสนอทันที และอาจพิจารณาเรียกร้องให้ชดใช้ความเสียหายอื่น (ถ้ามี) รวมทั้งจะพิจารณาให้เป็นผู้ทิ้งงาน ตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและ การบริหารพัสดุภาครัฐ

๑๐.๔ จังหวัดสงวนสิทธิ์ที่จะแก้ไขเพิ่มเติมเงื่อนไข หรือข้อกำหนดในแบบสัญญาหรือข้อตกลงเช่าเป็นหนังสือ ให้เป็นไปตามความเห็นของสำนักงานอัยการสูงสุด (ถ้ามี)

๑๐.๕ ในกรณีที่เอกสารแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ มีความขัดหรือแย้งกัน ผู้ยื่นข้อเสนอจะต้องปฏิบัติตามคำวินิจฉัยของจังหวัด คำวินิจฉัยดังกล่าวให้ถือเป็นที่สุด และผู้ยื่นข้อเสนอไม่มีสิทธิเรียกร้องค่าใช้จ่ายใดๆ เพิ่มเติม

๑๐.๖ จังหวัดอาจประกาศยกเลิกการเช่าในกรณีต่อไปนี้ได้ โดยที่ผู้ยื่นข้อเสนอ จะเรียกร้องค่าเสียหายใดๆ จากจังหวัดไม่ได้

(๑) จังหวัดไม่ได้รับการจัดสรรเงินที่จะใช้ในการเช่าหรือที่ได้รับจัดสรรแต่ไม่เพียงพอที่จะทำการเช่าครั้งนี้ต่อไป

(๒) มีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการเช่าหรือที่ได้รับการคัดเลือก มีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่น หรือเจ้าหน้าที่ในการเสนอราคา หรือส่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา

(๓) การทำการเช่าครั้งนี้ต่อไปอาจก่อให้เกิดความเสียหายแก่จังหวัด หรือกระทบต่อประโยชน์สาธารณะ

(๔) กรณีอื่นในทำนองเดียวกับ (๑) (๒) หรือ (๓) ตามที่กำหนดในกฎกระทรวง ซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

๑๐.๗ ผู้ยื่นข้อเสนอจะต้องเลือกช่องทางการอุทธรณ์และช่องทางการรับหนังสือแจ้งตอบผลการพิจารณาอุทธรณ์ไว้ตั้งแต่ขั้นตอนการยื่นข้อเสนอ และหากผู้ยื่นข้อเสนอมีความประสงค์ที่จะอุทธรณ์ผลการประกาศผู้ชนะการจัดซื้อจัดจ้าง จะต้องยื่นอุทธรณ์และรับหนังสือแจ้งตอบการพิจารณาอุทธรณ์ผ่านช่องทางที่ได้เลือกไว้เท่านั้น

๑๑. การปฏิบัติตามกฎหมายและระเบียบ

ในระหว่างระยะเวลาการเช่า ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ให้เช่าต้องปฏิบัติ ตามหลักเกณฑ์ที่กฎหมายและระเบียบได้กำหนดไว้โดยเคร่งครัด

๑๒. การประเมินผลการปฏิบัติงานของผู้ประกอบการ

จังหวัด สามารถนำผลการปฏิบัติงานแล้วเสร็จตามสัญญาของผู้ยื่นข้อเสนอที่ได้รับ การคัดเลือกให้เป็นผู้ให้เช่าเพื่อนำมาประเมินผลการปฏิบัติงานของผู้ประกอบการ

ทั้งนี้ หากผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกไม่ผ่านเกณฑ์ที่กำหนดจะถูกระงับการยื่นข้อเสนอหรือทำสัญญากับจังหวัด ไว้ชั่วคราว

จังหวัดเชียงใหม่

๔ กรกฎาคม ๒๕๖๘

ขอบเขตของงาน (Terms of Reference: TOR)
โครงการเช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์และโต้ตอบต่อภัยคุกคามไซเบอร์
ของ โรงพยาบาลนครพิงค์
ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข

1. หลักการและเหตุผล

โรงพยาบาลเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องลักษณะหน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564 จึงมีความจำเป็นอย่างยิ่งที่จะต้องดำเนินการให้ระบบบริการและระบบงานดิจิทัลมีความมั่นคงปลอดภัยทางไซเบอร์

ในปีงบประมาณ พ.ศ. 2568 โรงพยาบาลนครพิงค์ ได้รับคัดเลือกให้เข้าร่วมโครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข ภายใต้แผนงานบูรณาการรัฐบาลดิจิทัลจึงเป็นโอกาสที่จะพัฒนาให้โรงพยาบาลมีศักยภาพเพียงพอที่จะรับมือเหตุฉุกเฉินทางคอมพิวเตอร์ สามารถป้องกันตรวจจับวิเคราะห์และโต้ตอบต่อภัยคุกคามทางไซเบอร์ได้ โดยข้อมูลจะเชื่อมไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT) ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข จังหวัดนนทบุรี

2. วัตถุประสงค์

2.1 เพื่อให้โรงพยาบาลได้รับการติดตั้งระบบตรวจจับและวิเคราะห์ภัยคุกคามขั้นสูงในระดับเครือข่ายคอมพิวเตอร์และเทคโนโลยีสารสนเทศ

2.2 เพื่อให้โรงพยาบาลได้รับบริการเฝ้าระวัง รับมือ ตรวจจับภัยคุกคามเชิงรุกและโต้ตอบเหตุภัยคุกคามจากผู้เชี่ยวชาญ และเชื่อมโยงข้อมูลไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT) ได้

2.3 เพื่อให้โรงพยาบาลได้รับการอบรมพัฒนาบุคลากรให้มีความพร้อมในการรับมือเหตุฉุกเฉินที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพให้บริการ ประเภทเดียวกันกับงานที่ประกวดราคาอิเล็กทรอนิกส์นี้

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สำนักงานปลัดกระทรวงสาธารณสุข ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงานสิ่งของหรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อ

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

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า 1 ล้านบาท

(3) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณที่ยื่นข้อเสนอในครั้งนั้น (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน)

(4) กรณีตาม (1) - (3) ยกเว้นสำหรับกรณีดังต่อไปนี้

(4.1) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(4.2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ 10) พ.ศ. 2561

3.13 ผู้ยื่นข้อเสนอต้องมีผลงานประเภทเดียวกันกับงานที่ประกวดราคา และเป็นผลงานที่มีวงเงินไม่น้อยกว่า 500,000 บาท (ห้าแสนบาทถ้วน) โดยแนบเอกสารผลงานหรือสำเนาสัญญาจ้างมาพร้อมการยื่นเอกสารเสนอราคา

4. คุณลักษณะเฉพาะทางเทคนิคและสิ่งส่งมอบ

ผู้ยื่นข้อเสนอต้องให้บริการในการป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ รวมถึงปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงาน ภายใต้การดูแลเพื่อเฝ้าระวังติดตามและเตรียมความพร้อมในการรับมือ เมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งในประเทศและต่างประเทศ ประสานงานกับหน่วยงานภายใต้การดูแล เพื่อตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์อย่างเหมาะสมและทันท่วงที ตลอดจนให้การช่วยเหลือแนะนำและสนับสนุน ในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยประสานงานร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานนั้น ๆ โดยสามารถรายงานลำดับความสำคัญของสิ่งผิดปกติที่เกิดขึ้นในระบบด้วยอุปกรณ์ป้องกันตรวจจับ วิเคราะห์ภัยคุกคามขั้นสูง พร้อมทั้งดำเนินการพัฒนาบุคลากร ให้มีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ และให้บริการเฝ้าระวังรับมือตรวจจับภัยคุกคามเชิงรุก โต้ตอบเหตุการณ์ฉุกเฉินที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์

ในการพัฒนาระบบงานดังกล่าวข้างต้นผู้ยื่นข้อเสนอจะต้องดำเนินการภายใต้ขอบเขตของงาน โดยมีรายละเอียดสิ่งส่งมอบและคุณลักษณะเฉพาะทางเทคนิค ดังนี้

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.1 จัดหาให้มีระบบการจัดเก็บข้อมูลสำรอง (Backup) ในส่วนของข้อมูลศูนย์ข้อมูลคอมพิวเตอร์ (Data Center และบริการระบบคลาวด์ (Cloud Computing) ได้รับการรับรองมาตรฐานอย่างน้อยดังต่อไปนี้

1. มีมาตรฐานการบริหารการรักษาความความปลอดภัย ISO/IEC 27001
2. มีมาตรฐานความปลอดภัยสำหรับระบบคลาวด์ CSA-STAR Cloud Security (CSA STAR)
3. มีมาตรฐานความปลอดภัยข้อมูลส่วนบุคคล ISO/IEC 27701 หรือ ข้อมูลด้านสุขภาพโดยเฉพาะ ISO27799
4. มีมาตรฐานการให้บริการด้านเทคโนโลยีสารสนเทศระบบคลาวด์ (IT Services Management) ISO/IEC 20000-1 เป็นอย่างน้อย
5. มาตรฐานการจัดการความมั่นคงปลอดภัยด้านสารสนเทศในระบบคลาวด์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ISO/IEC 27017 หรือ CSA STAR และ ISO/IEC 27018 หรือ CSA STAR เป็นอย่างน้อย
6. ต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
7. ต้องดำเนินการลบ หรือทำลายข้อมูลโดยสมบูรณ์ ภายใน 30วัน หลังจากวันที่สิ้นสุดสัญญา หรือวันที่บอกเลิกสัญญา
8. ในส่วนของศูนย์บริการระบบคลาวด์ต้องมีคุณลักษณะอย่างน้อยดังนี้
   - ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ตั้งอยู่ในประเทศไทย อย่างน้อย 2 ศูนย์ข้อมูล มีระยะทางห่างกันไม่น้อยกว่า 30 กิโลเมตร และศูนย์คอมพิวเตอร์ (Data Center) ทุกแห่งต้องมีระบบเครือข่ายสื่อสารหลัก ที่เชื่อมเป็นเครือข่ายเดียวกันด้วยเทคโนโลยีบริหารจัดการระบบเครือข่าย (Software Define Infrastructure: SDI) เพื่อรองรับแผนการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning: BCP)
   - มีระบบสำรองไฟฟ้าฉุกเฉินในกรณีที่เกิดเหตุฉุกเฉินกับแหล่งจ่ายไฟฟ้าหลัก และต้องสามารถทำงานได้อย่างต่อเนื่องตลอดเวลา
   - ผู้ยื่นข้อเสนอต้องจัดให้มีการสำรองข้อมูล (Backup) เพื่อทำการบันทึกข้อมูลของระบบทั้งหมดเก็บไว้ภายในศูนย์ ข้อมูลคอมพิวเตอร์หลัก (DC Site) และศูนย์ข้อมูลคอมพิวเตอร์สำรอง (Backup Site) พร้อมกัน

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

- ผู้ยื่นข้อเสนอต้องจัดหาระบบสำรองข้อมูลบนระบบเสมือน โดยมีการจัดเตรียม Software Backup ที่มีการรองรับการส่งข้อมูลความปลอดภัย TLS 1.2 ขึ้นไปและรองรับการเข้ารหัส SHA 256 หรือดีกว่า พร้อมทั้งมีระบบป้องกันไม่ให้ไฟล์ข้อมูลสำรองถูกลบหรือแก้ไขได้ (Immutable หรือ Immutability หรือ WORM)
- Software Backup ต้องรองรับการสำรองข้อมูล (Backup) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ระบบปฏิบัติการ Microsoft Windows Server 2008 R2 SP12 ขึ้นไปถึงปัจจุบันหรือระบบปฏิบัติการ Linux Distro ที่ออกตั้งแต่ปี 2014 ที่ยังมีการสนับสนุนอยู่
- จัดเตรียมพื้นที่เก็บข้อมูล (Disk) สำหรับสำรองข้อมูลที่มีพื้นที่ไม่น้อยกว่า 1,000 กิกะไบต์ (GB)
- มีการสำรองข้อมูลที่ศูนย์ข้อมูลคอมพิวเตอร์หลัก (DC Site) และ ศูนย์ข้อมูลคอมพิวเตอร์สำรอง (DR Site) โดยทำการเก็บสำรองข้อมูลไว้เป็นรายวัน จำนวน 7 สำเนา เป็นรายสัปดาห์ จำนวน 1 สำเนา และเป็นรายเดือน จำนวน 1 สำเนา
- กรณีที่ผู้ใช้บริการ ต้องการกู้ข้อมูลสามารถแจ้งดำเนินการผ่านช่องทางการ support ตลอดเวลา โดยจะทำการ export ข้อมูลในระดับ file ส่งผ่าน ftp ที่มีการเข้ารหัส และจัดส่งให้กับผู้ใช้บริการ นำไปใช้งานในลำถัดไปโดยไม่รวม service ภายในเครื่อง

4.2 จัดหาให้มีระบบป้องกันตรวจจับและโต้ตอบภัยคุกคาม Endpoint Detection & Response (EDR) จำนวน 1 ระบบ โดยแต่ละระบบมีคุณลักษณะอย่างน้อยดังต่อไปนี้

4.2.1. สามารถควบคุมและบริหารจัดการระบบ Endpoint Detection & Response (EDR) ผ่าน web-basedmanagement console เพื่อการกำหนดนโยบายด้านความปลอดภัยและบังคับใช้การป้องกันไปยังเครื่องแม่ข่าย (agent) ผ่านทางทีม Security Operation

4.2.2. มีสิทธิ์การใช้งาน EDR ที่ถูกต้องตามกฎหมายได้อย่างน้อย 60 Licenses สำหรับ Server

4.2.2.1. เป็น Platform ที่สามารถวิเคราะห์ตรวจจับภัยคุกคามโดยใช้เทคโนโลยี AI/ML ในการวิเคราะห์ พฤติกรรมที่เกิดขึ้นโดยการหาความสัมพันธ์ของข้อมูลที่ได้มาจากเครื่อง Endpoint, Network, Cloud และ ข้อมูลระบุตัวตนของผู้ใช้งาน (Identity) เป็นอย่างน้อย

4.2.2.2. เป็น Platform ที่สามารถรับ Security Events จากอุปกรณ์อื่น ๆ เพื่อนำมาวิเคราะห์ร่วมกับ Endpoint Agent ได้ โดยผ่านช่องทาง Syslog, Kafka, DB, CSV file, FTP, NetFlow และ Windows events ได้เป็นอย่างน้อย

ลงชื่อ.....	นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....	นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....	นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....	นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....	นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.2.2.3. ระบบที่เสนอต้องมีเทคโนโลยี AI/ML การการให้ scoring ของแต่ละ Incident โดยอัตโนมัติ เพื่อจัดลำดับความเร่งด่วนในการจัดการกับ Incident

4.2.2.4. Agent Software ที่นำเสนอต้องมีคุณลักษณะความสามารถดังนี้

- สามารถป้องกันการโจมตีที่ช่องโหว่ของระบบ (Exploit Prevention) ซึ่งรองรับ Platform Windows, Linux และ MacOS
- สามารถป้องกันมัลแวร์ หรือไวรัส (Malware Prevention หรือ Antivirus)
- สามารถป้องกันการโจมตีของมัลแวร์ระดับสูงที่ใช้เทคนิคโจมตีแบบไม่ใช้ไฟล์ (Fileless Attacks)
- สามารถป้องกันการโจมตีโดยใช้การวิเคราะห์พฤติกรรม (Behavior Threat Prevention)
- สามารถป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware Protection)
- สามารถป้องกัน Exploit และ Malware ในกรณีที่ไม่สามารถติดต่อกับ Management Console ได้ (Offline)

4.2.2.5. เป็น Platform ที่มีความสามารถในการค้นหาและระบุภัยคุกคามที่เกิดขึ้น (Threat Hunting) โดยวิเคราะห์จากพฤติกรรมการใช้งานที่ผิดปกติ (Behavior Threat) และสามารถแสดงรายละเอียดของเครื่องปลายทาง เช่น Application, System Information เป็นต้น

4.2.2.6. สามารถทำงานร่วมกับ Cloud Sandbox หรือ On-Premise Sandbox เพื่อวิเคราะห์ภัยคุกคาม และนำผลลัพธ์มาใช้ในการป้องกันได้ กรณีที่ต้องทำงานร่วมกับ On-Premise Sandbox ให้เสนอ On-Premise Sandbox เพิ่มเติมให้ครอบคลุม และเพียงพอต่อการทำงาน

4.2.2.7. สามารถเพิ่มและแก้ไข Behavior indicators of compromise (BIOC) เพื่อให้สามารถสร้าง Alert จากเหตุการณ์ที่เคยเกิดขึ้นในอดีตย้อนหลังได้

4.2.2.8. สามารถแชร์ IP และ Domain list เพื่อให้อุปกรณ์ Firewall ที่ใช้งานอยู่เพื่อนำไปสร้าง Policy เพื่อ Block ได้

4.2.2.9. สามารถเก็บ Ingested Data หรือ Raw Data ได้ไม่น้อยกว่า 30 วัน และเก็บ Incident Data ได้ไม่น้อยกว่า 180 วัน

4.2.2.10. สามารถกำหนด Password สำหรับถอดการติดตั้ง Agent จาก Management Console เพื่อป้องกันไม่ให้ User ถอนการติดตั้ง Agent software ได้

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.2.2.11. สามารถตรวจสอบช่องโหว่ของระบบปฏิบัติการ (Vulnerability Assessment) บนระบบปฏิบัติการ Windows และ Linux โดยอ้างอิงช่องโหว่ตาม Common Vulnerabilities and Exposures (CVE) โดยไม่ต้องติดตั้ง Agent เพิ่มเติม หรือนำเสนอระบบอื่นๆเพิ่มเติม เพื่อสามารถทำได้ตามความต้องการดังกล่าว

4.2.2.12. สามารถแสดง Host Inventory เช่น User, Application, Services, Driver, Autorun, Share ของเครื่องคอมพิวเตอร์ได้ เพื่อสามารถตรวจสอบข้อมูลได้อย่างรวดเร็ว หรือนำเสนอระบบอื่น ๆเพิ่มเติม เพื่อทำได้ตามความต้องการดังกล่าว

4.2.2.13. ระบบที่นำเสนอต้องผ่านการประเมินทดสอบของ The Forrester New Wave™: Extended Detection And Response (XDR) Providers, Q4 2021 โดยถูกจัดให้อยู่ใน Leaders หรือ Strong Performers ได้เป็นอย่างน้อย

4.2.2.14. สามารถสร้างแดชบอร์ด หรือ Report โดยใช้การ custom query มาเป็นเงื่อนไขในการแสดงข้อมูล

4.2.2.15. มีความสามารถในการแจ้งเตือน (Alert) ผ่าน Email, Slack หรือ SYSLOG โดยสามารถเลือกจาก Severity Level ได้เป็นอย่างน้อย

4.2.3. <u>มีสิทธิ์การใช้งาน Next-generation Antivirus ที่ถูกต้องตามกฎหมาย ได้อย่างน้อย 50Licenses สำหรับ Client</u>

4.2.3.1 เป็น Platform ที่สามารถวิเคราะห์ตรวจจับภัยคุกคามโดยใช้เทคโนโลยี AI/ML ในการวิเคราะห์พฤติกรรมที่เกิดขึ้นโดยการหาความสัมพันธ์ของข้อมูลที่ได้มาจากเครื่อง Endpoint, Network, Cloud และ ข้อมูลระบุตัวตนของผู้ใช้งาน (Identity) เป็นอย่างน้อย

4.2.3.2 เป็น Platform ที่สามารถรับ Security Events จากอุปกรณ์อื่น ๆ เพื่อนำมาวิเคราะห์ร่วมกับ Endpoint Agent ได้ โดยผ่านช่องทาง Syslog, Kafka, DB, CSV file, FTP, NetFlow และ Windows events ได้เป็นอย่างน้อย

4.2.3.3 ระบบที่เสนอต้องมีเทคโนโลยี AI/ML การการให้ scoring ของแต่ละ Incident โดยอัตโนมัติ เพื่อจัดลำดับความเร่งด่วนในการจัดการกับ Incident

4.2.3.4 Agent Software ที่นำเสนอต้องสามารถป้องกันการโจมตีที่ช่องโหว่ของระบบ (Exploit Prevention) ซึ่งรองรับ Platform Windows, Linux และ MacOS

4.2.3.5 Agent Software ที่นำเสนอต้องสามารถป้องกันมัลแวร์ หรือไวรัส (Malware Prevention หรือ Antivirus)

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.2.3.6 Agent Software ที่นำเสนอต้องสามารถป้องกันการโจมตีของมัลแวร์ระดับสูงที่ใช้เทคนิคโจมตีแบบไม่ใช้ไฟล์ (Fileless Attacks)

4.2.3.7 Agent Software ที่นำเสนอต้องสามารถป้องกันการโจมตีโดยใช้การวิเคราะห์พฤติกรรม (Behavior Threat Prevention)

4.2.3.8 Agent Software ที่นำเสนอต้องสามารถป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware Protection)

4.2.3.9 Agent Software ที่นำเสนอต้องสามารถป้องกัน Exploit และ Malware ในกรณีที่ไม่สามารถ ติดต่อกับ Management Console ได้ (Offline)

4.2.3.10 เป็น Platform ที่มีความสามารถในการค้นหาและระบุภัยคุกคามที่เกิดขึ้น (Threat Hunting) โดยวิเคราะห์จากพฤติกรรมการใช้งานที่ผิดปกติ (Behavior Threat) และสามารถแสดงรายละเอียดของเครื่องปลายทาง เช่น Application, System Information เป็นต้น

4.2.3.11 สามารถทำงานร่วมกับ Cloud Sandbox หรือ On-Premise Sandbox เพื่อวิเคราะห์ภัยคุกคาม และนำผลลัพธ์มาใช้ในการป้องกันได้ กรณีที่ต้องทำงานร่วมกับ On-Premise Sandbox ให้เสนอ On-Premise Sandbox เพิ่มเติมให้ครอบคลุม และเพียงพอต่อการทำงาน

4.2.3.12 สามารถเพิ่มและแก้ไข Behavior indicators of compromise (BIOC) เพื่อให้สามารถสร้าง Alert จากเหตุการณ์ที่เคยเกิดขึ้นในอดีตย้อนหลังได้

4.2.3.13 สามารถแชร์ IP และ Domain list เพื่อให้อุปกรณ์ Firewall ที่ใช้งานอยู่เพื่อนำไปสร้าง Policy เพื่อ Block ได้

4.2.3.14 สามารถเก็บ Ingested Data หรือ Raw Data ได้ไม่น้อยกว่า 30 วัน และเก็บ Incident Data ได้ไม่น้อยกว่า 180 วัน

4.2.3.15 สามารถกำหนด Password สำหรับถอดการติดตั้ง Agent จาก ManagementConsole เพื่อป้องกันไม่ให้ User ถอนการติดตั้ง Agent software ได้

4.2.3.16 สามารถตรวจสอบช่องโหว่ของระบบปฏิบัติการ (Vulnerability Assessment) บนระบบปฏิบัติการ Windows และ Linux โดยอ้างอิงช่องโหว่ตาม Common Vulnerabilities and Exposures (CVE) โดยไม่ต้องติดตั้ง Agent เพิ่มเติม หรือนำเสนอระบบอื่นๆเพิ่มเติม เพื่อสามารถทำได้ตามความต้องการดังกล่าว

4.2.3.17 สามารถแสดง Host Inventory เช่น User, Application, Services, Driver, Autorun, Share ของเครื่องคอมพิวเตอร์ได้ เพื่อสามารถตรวจสอบข้อมูลได้อย่างรวดเร็ว หรือนำเสนอระบบอื่น ๆเพิ่มเติม เพื่อทำได้ตามความต้องการดังกล่าว

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.2.3.18 ระบบที่นำเสนอต้องผ่านการประเมินทดสอบของ The Forrester New Wave™: Extended Detection and Response (XDR) Providers, Q4 2021 โดยถูกจัดให้อยู่ใน Leaders หรือ Strong Performers ได้เป็นอย่างน้อย

4.2.3.19 สามารถสร้างแดชบอร์ด หรือ Report โดยใช้การ custom query มาเป็นเงื่อนไขในการแสดงข้อมูล

4.2.3.20 มีความสามารถในการแจ้งเตือน (Alert) ผ่าน Email, Slack หรือ SYSLOG โดยสามารถเลือกจาก Severity Level ได้เป็นอย่างน้อย

4.2.4 ระบบที่ให้บริการต้องมีหน่วยงาน ศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ (Cyber Security Operation Center: CSOC) เพื่อทำการเฝ้าระวังตลอด 24ชั่วโมง รวมถึงแจ้งเตือนตาม Escalation Flow ที่กำหนดร่วมกัน

4.3 จัดหาให้มีระบบตรวจสอบการเข้าถึงอย่างปลอดภัยและการยืนยันตัวตน 2ชั้น (Multi-factor Authentication) จำนวนไม่น้อยกว่า20 ผู้ใช้งาน (user) โดยมีคุณลักษณะอย่างน้อยดังต่อไปนี้

4.3.1 สามารถทำหน้าที่ควบคุมความปลอดภัยในการใช้งานบัญชีรายชื่อที่มีสิทธิ์ (Privileged Account) โดยสามารถบริหารจัดการรหัสผ่าน และควบคุมเฝ้าระวังการใช้งาน Privileged Account (Privileged Session) ได้

4.3.2 สามารถทำงานได้โดยไม่ต้องติดตั้ง Software บนอุปกรณ์ปลายทางที่ต้องการเก็บบันทึกกิจกรรมการทำงาน (Agentless)

4.3.3 รองรับทำงานลักษณะ High Availability แบบ Active / Passive ในกรณีอุปกรณ์ที่ Active เสียหาย อุปกรณ์ Passive ต้องขึ้นมาทำหน้าที่แทนโดย ไม่ส่งผลกระทบต่อการ ใช้งานระบบ (Automatic) หรือต้องทำงานลักษณะ High Availability แบบ Active/Active

4.3.4 ต้องสามารถควบคุมความปลอดภัยในการใช้งานได้ไม่จำกัดอุปกรณ์ (Device) โดยต้องสามารถโยกย้ายอุปกรณ์ได้โดยไม่จำกัดจำนวนครั้ง

4.3.5 ผู้ดูแลสามารถกำหนดสิทธิ์ควบคุมผู้ใช้งาน (Role-based access control) ได้อย่างน้อย ดังนี้

4.3.5.1 Clipboard control

4.3.5.2 Upload / download control

4.3.5.3 Drive / Device redirection

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.3.6 ต้องสามารถบันทึกการใช้งาน (Session Recording) การใช้งาน Remote Privileged Session ที่ใช้งานพร้อมกันไม่จำกัด Sessions ในรูปแบบของ Video Recordings, Keystrokes, และ Commands โดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

4.3.6.1 RDP Sessions ในรูปแบบของ Video Recordings Remote desktop

4.3.6.2 SSH Sessions ในรูปแบบของ Video Recordings และ Commands List

4.3.6.3 สามารถค้นหาบันทึกการใช้งานจาก Commands จาก SSH ได้แบบ Free Text Search

4.3.7 ต้องสามารถเฝ้าระวัง (Monitor) การใช้งาน Remote Privileged Session ได้แบบ Real-Time และ Terminate Session ได้ทันทีเมื่อพบพฤติกรรมที่ผิดปกติ

4.3.8 ต้องมีการเข้ารหัสข้อมูลของ Privileged Account ที่จัดเก็บไว้ ด้วย Algorithm แบบ AES-256 หรือ RSA-2048 หรือดีกว่า

4.3.9 ต้องสามารถทำ Multi-Factor Authentication เมื่อมีการเข้าใช้งานด้วยเทคนิค/วิธีการ Username/Password (Local Database) และ LDAP ได้เป็นอย่างน้อย และต้องรองรับรูปแบบ 3rd party, SMS และ Email ได้เป็นอย่างน้อย

4.3.10 ต้องสามารถบริหารจัดการบัญชีผู้ใช้งานและรหัสผ่านของระบบงานต่อไปนี้ได้เป็นอย่างน้อย หากไม่รองรับสามารถเสนออุปกรณ์หรือ Customize เพิ่มเติมเพื่อให้สามารถทำงานได้โดยประสิทธิภาพของระบบไม่ลดลง

4.3.10.1 Operating Systems: Microsoft Windows Server, VMWare ESX / ESXi

4.3.10.2 Databases: Oracle, Microsoft SQL, MySQL

4.3.10.3 Network /Security Appliances Cisco, Fortinet, Palo Alto

4.3.11 ต้องสามารถเปลี่ยนรหัสผ่านของ Privileged Account ได้โดยกำหนดนโยบายของรหัสผ่าน (Password Policy) ได้อย่างน้อย ดังนี้

4.3.11.1 เปลี่ยนรหัสผ่านของ Privileged Account ตามช่วงเวลาที่กำหนด เช่น ดำเนินการทุก 30 วัน

4.3.11.2 กำหนดความยาว และองค์ประกอบของรหัสผ่าน เช่น ตัวอักษรตัวใหญ่ (Upper Case), ตัวอักษรตัวเล็ก (Lower Case), ตัวเลข (Digit) และอักขระพิเศษ(Special Character) ได้

4.3.12 ต้องสามารถบริหารจัดการรหัสผ่านของเครื่องแม่ข่ายปลายทางได้โดยไม่จำเป็นต้องมีการติดตั้ง Software Agent ที่อุปกรณ์ปลายทาง

4.3.13 ต้องสามารถกำหนด Workflow การเข้าใช้งาน Privileged Account ที่ถูกควบคุมได้อย่างน้อย โดยกำหนดให้มี Workflow ลักษณะ Request - Approver แต่ละ Device ที่อยู่ในการควบคุมได้

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.3.14 ต้องสามารถเชื่อมต่อไปยังระบบปลายทาง (Transparent Connection) โดยเข้าสู่ระบบงานปลายทางที่ไม่ต้องแสดงรหัสผ่านให้ผู้ใช้ทราบ

4.3.15 ต้องสามารถสร้างรายงาน (Create/Generate Report) กรองข้อมูลของรายงาน (Filters Report) และส่งออกรายงาน (Export/Download Report) ในรูปแบบของ JSON และ CSV ได้ โดยรายงานต้องมีข้อมูลอย่างน้อย ดังต่อไปนี้

4.3.15.1 แสดงข้อมูลหรือรายงาน Privileged User Activity ต้องมีข้อมูลการใช้งานของ Privileged Account ที่ถูกเรียกใช้งาน, วัน-เวลาที่ถูกใช้งาน, Device IP ที่เข้าใช้งาน, ผู้อนุมัติการใช้งาน

4.3.15.2 แสดงข้อมูลหรือรายงาน Audit Log ต้องมีข้อมูลการใช้งานของ System Log (Admin Account) ที่เข้าใช้งาน, วัน-เวลาที่เข้าใช้งาน, Configuration ที่เกิดขึ้น

4.3.16 ต้องสามารถกำหนดระดับสิทธิ์ของผู้ใช้งาน (User Roles) ในการเข้าใช้งานระบบได้อย่างน้อย ดังนี้

4.3.16.1 ผู้ร้องขอ Privileged Session (Requestor)

4.3.16.2 ผู้อนุมัติการใช้งาน Privileged Session (Approver)

4.3.16.3 ผู้ดูแลระบบ (System Administrator)

4.3.17 ต้องจัดเก็บข้อมูลประวัติกิจกรรม (Log/Event) โดยมีคุณสมบัติอย่างน้อยดังนี้

4.3.17.1 ข้อมูลการบันทึกการใช้งาน (Session Recording) อยู่ภายในองค์กร และไม่มีฐานข้อมูลอยู่ภายนอกองค์กร

4.3.17.2 ระบบสามารถแสดงผลเหตุการณ์ (Event) การลงชื่อเข้าใช้ (Login) ที่ผิดปกติได้

4.3.17.3 ระบบรองรับการเก็บข้อมูล (Logging) และ ทำรายงาน (Report) อย่างน้อย 90 วัน

4.3.18 การติดตั้ง Application Gateway ได้โดยไม่จำเป็นต้องใช้วิธีการผ่าน Jump Server และไม่ส่งผลกระทบหรือเปลี่ยนแปลงทรัพยากรที่มีอยู่เดิมขององค์กร

4.3.19 สามารถกำหนด Device Posture Policy ให้กับอุปกรณ์ที่ต้องการเข้าถึง ระบบภายในองค์กรได้ เช่น ระบบปฏิบัติการ (OS Version) เป็นต้น

4.3.20 ระบบที่นำเสนอต้องสามารถใช้งานผ่านเว็บเบราว์เซอร์ และรองรับเว็บเบราว์เซอร์ ดังต่อไปนี้ Firefox, Chrome, Opera, Safari, and Edge. เป็นต้น

4.3.21 ต้องมี Connection Locations เพื่อรองรับการเชื่อมต่อของ Remote Users ในพื้นที่ทั่วโลก และต้องมี Connection Location อยู่ที่ประเทศไทยด้วย

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.4. จัดหาอุปกรณ์ระบบป้องกันการโจมตีเว็บไซต์และแอปพลิเคชัน (Web Application Firewall: WAF) จากการโจมตีในระดับเครือข่าย โดยอุปกรณ์ต้องมีคุณลักษณะดังต่อไปนี้

4.4.1.มี Web Application Protection Throughput (64K HTTP) ไม่น้อยกว่า 3.2Gbps

4.4.2.มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) ชนิด 10/100/1000 Base-T หรือดีกว่า จำนวนรวมไม่น้อยกว่า 16 ช่อง

4.4.3.มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) ชนิด 10G SFP+ หรือดีกว่า จำนวนรวมไม่น้อยกว่า 6 ช่อง

4.4.4.มี Interface ที่สามารถรองรับการทำ Hardware Bypass จำนวน 2 คู่ เป็นอย่างน้อย ในกรณีฮาร์ดแวร์ขัดข้อง หรือเสนอ อุปกรณ์ต่อพ่วงที่สามารถทำงานได้ในลักษณะเดียวกัน

4.4.5.มีช่องสำหรับเพิ่ม Network Interface ไม่น้อยกว่า 2 ช่อง สำหรับเชื่อมต่อระบบเครือข่ายในอนาคต

4.4.6.มีความสามารถหรือมีเครื่องมือเสริมในการป้องกันการบุกรุกโจมตีเว็บไซต์เพื่อให้มีประสิทธิภาพในการป้องกันการโจมตี Cross-site Scripting (XSS), Cookie Poisoning (Cookie-Base Attack), Buffer Overflow , SQL injection , XML Parser หรือ XML Data Protection หรือ XXE เป็นอย่างน้อย

4.4.7.มีความสามารถในการป้องกัน Vulnerability Protection, Content Security, Botnet Detection และ Brute-Force Attacks เพื่อป้องกันการโจมตีจาก Ransomware Attack

4.4.8.มีความสามารถตรวจสอบการเปิดพอร์ต, ช่องโหว่ และการสแกนรหัสผ่านที่ไม่รัดกุมในการป้องกันแรนซัมแวร์ ช่วยให้ผู้ดูแลระบบสร้างนโยบายการป้องกันแรนซัมแวร์ได้

4.4.9.สามารถตรวจสอบ Malware บน protocol เช่น HTTP, HTTPS, FTP, SMB, SMTP, POP3 และ IMAP

4.4.10. มีฟังก์ชั่น SOC Lite เพื่อตรวจสอบและแสดงภัยคุกคามต่อระบบงาน (Business System) และเครื่องผู้ใช้งาน (Client) รวมถึงระดับความรุนแรง (Severity), ประเภทภัยคุกคาม (Threats Type), และ Top Security Event เป็นต้น

4.4.11. รองรับการทำ SSL Decryption บน TLS 1.3 ได้

4.4.12. สามารทำงานลักษณะ Transparent Mode ได้

4.4.13. สามารถ Routing แบบ Static, Dynamic Routing ได้

4.4.14. สามารถร่วมทำงานร่วมกับระบบพิสูจน์ตัวตน แบบ SSO เช่น Active Directory และ RADIUS ได้

4.4.15. สามารถทำ HA แบบ Active-Active หรือ Active-Standby ได้

4.4.16. สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.4.17. สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้

4.4.18. สามารถใช้งานตามมาตรฐาน IPv6 ได้

4.4.19. ผลิตภัณฑ์ได้รับมาตรฐานความปลอดภัย เช่น UL หรือ CE หรือ FCC เป็นอย่างน้อย

4.5 จัดหาระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log management) โดยต้องมีคุณลักษณะดังต่อไปนี้

4.5.1 ระบบต้องสามารถจัดเก็บ Log File บน Cloud ได้

4.5.2 มีหน่วยประมวลผลกลาง (CPU) จำนวนไม่น้อยกว่า 4 แกนหลัก (Core)

4.5.3 มีหน่วยความจำหลัก (RAM) ขนาดไม่น้อยกว่า 4 GB

4.5.4 มีหน่วยจัดเก็บข้อมูล (Storage) เพื่อเก็บ Log file ขนาดความจุไม่น้อยกว่า 1 TB

4.5.5 สามารถเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ตได้

4.5.6 มีระบบป้องกันการบุกรุกเครือข่าย (Firewall) พร้อมใช้งาน

4.5.7 มีการดำเนินการสำรองเครื่องคอมพิวเตอร์แม่ข่ายเสมือนที่ให้บริการเช่า

4.5.8 สามารถจัดเก็บ Log File ได้ไม่น้อยกว่า 90 วัน

4.6 จัดหาให้มีระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (Security Information and Event Management: SIEM) คุณลักษณะอย่างน้อยดังต่อไปนี้

4.6.1. ให้บริการทั้งระดับ Infrastructure และ Operating system โดยผู้เสนอ ต้องจัดเตรียมที่สำหรับจัดเก็บข้อมูลที่ใช้ในการจัดการกับ Log และ Event ต่าง ๆ ไว้ จำนวนไม่น้อยกว่า 100Devices

4.6.2. ตรวจจับและแจ้งเตือนการบุกรุกที่เข้าถึงระบบเครือข่าย การพยายาม Brute force Login เข้าระบบ และการ Scan port (port scaning)

4.6.3. Malware-Virus Detection ตรวจจับและแจ้งเตือน Malware หรือ Virus จากพฤติกรรมต่างที่เกิดขึ้นหรือจาก signature

4.6.4. Blackist IP การตรวจจับและแจ้งเตือนการเข้าถึง IP Address ที่เป็น Blackist และระบุการเปิด connection ได้

4.6.5. Unauthorized Access การตรวจจับการเข้าถึงข้อมูลหรือระบบที่ไม่ได้รับอนุญาต หรือไม่มีสิทธิเข้าถึงระบบ

4.6.6. DDoS Attack การตรวจจับพฤติกรรมการโจมตีในรูปแบบของ DDoS ได้ทั้งภายนอกและภายในสามารถแจ้งเตือนผ่าน IOC ไปยังหน่วยงานอื่นๆ ได้

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.6.7. มี Dashboard เพื่อควบคุมและตรวจสอบพฤติกรรมผิดปกติที่เกิดขึ้นกับระบบโดยสามารถแบ่งตาม Severity ได้ชัดเจนรวมถึงมี Timestamp

4.6.8. มีการสรุป Report ประจำเดือนเพื่อรายงานเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในระบบ

4.7 จัดหาให้มีการตรวจสอบช่องโหว่ในระดับระบบปฏิบัติการ (Vulnerability Assessment) คุณลักษณะอย่างน้อยดังต่อไปนี้

4.7.1 ผู้ยื่นข้อเสนอจะต้องเข้าดำเนินการตรวจสอบเพื่อหาจุดที่เป็นช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์และสารสนเทศ เพื่อจะได้หาแนวทางในการป้องกันก่อนที่เหตุจะเกิดจำนวน 1 รอบ โดยการดำเนินการ 1 รอบนั้น จะดำเนินการตรวจสอบหาช่องโหว่ 1 ครั้ง เพื่อตรวจสอบหาช่องโหว่ที่เกิดขึ้นกับระบบ และอีก 1 ครั้ง หลังจากดำเนินการแก้ไขช่องโหว่ที่เกิดขึ้นเรียบร้อยแล้ว

4.7.1.1 บริการที่นำเสนอต้องใช้งานโปรแกรมที่มีลิขสิทธิ์ถูกกฎหมายและอยู่ใน

4.7.1.2 สามารถตรวจสอบช่องโหว่ของอุปกรณ์บนระบบเครือข่ายได้ทั้งเครือข่ายสาธารณะ(Public) และเครือข่ายภายใน (Private) และมุมมองบุคคลภายนอก outsider's perspective พร้อมทั้งตั้งเวลาการ Scan ได้

4.7.1.3 สามารถรองรับการตรวจสอบช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่ายที่มีระบบปฏิบัติการอย่างน้อยต่อไปนี้

- ระบบปฏิบัติการด้านคอมพิวเตอร์ (Operating System) เช่น Windows OS หรือ Linux OS
- ระบบปฏิบัติการด้านเครือข่าย (Network) เช่น Firewall
- ระบบปฏิบัติการด้าน Service Application ภายใต้บริการ Port ที่มีการเปิดใช้งาน

4.7.1.4 รองรับการ scan ทั้งแบบ Non Credential Scan และ Credential Scan ได้

4.7.1.5 สามารถสร้างรายงานได้หลายรูปแบบ เช่น Executive Summary หรือแบบแยกตาม Host หรือ Plugin

4.7.1.6 สามารถตั้งเวลาในการตรวจสอบ (Schedule Scan) และเชื่อมต่อตารางการแสกนที่ตั้งค่าไว้ไปยัง Microsoft Outlook แบบอัตโนมัติเมื่อมีการสร้างและแก้ไข (Subscribe Calendar)

4.7.1.7 รายงานจะต้องมีการอ้างอิงกับ CVSS และ CVE และมีการระบุ Severity ของช่องโหว่ที่พบในการตรวจสอบ

4.7.2 บุคคลหรือกลุ่มบุคคลผู้เข้าดำเนินการตรวจสอบช่องโหว่จะต้องมีความรู้ความสามารถ ในด้านการวิเคราะห์ ตรวจสอบหาจุดที่เป็นช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์ และสารสนเทศที่จะเป็นภัยคุกคามต่อหน่วยงาน รวมถึงให้คำแนะนำในการตรวจสอบแก้ไขปัญหาที่พบ โดยบุคคลหรือกลุ่มบุคคลผู้เข้าดำเนินการจะต้องได้รับใบรับรองความรู้ความสามารถ อย่างน้อยดังนี้

ลงชื่อ.....	นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....	นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....	นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....	นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....	นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.7.2.1 CEH (Certified Ethical Hacker)

4.7.2.2 ISACA Certified Information Security Manager (CISM)

4.7.2.3 SACA Certified Information Systems Auditor (CISA)

4.7.2.4 (ISC)2 CC – Certified in Cybersecurity

4.7.2.5 CompTIA CySA+

4.7.2.6 CompTIA Pentest+

4.7.3 ผู้ยื่นข้อเสนอจะต้องจัดทำรายงานผลการวิเคราะห์ และตรวจสอบช่องโหว่ โดยต้องระบุรายละเอียดช่องโหว่ที่ตรวจสอบพบบนอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ และสารสนเทศ ที่จะเป็นภัยคุกคามต่อหน่วยงาน รวมถึงระบุแนวทางการแก้ไขช่องโหว่ที่ตรวจสอบพบ ซึ่งจะต้องประกอบด้วย

4.7.3.1.1 รายงานสรุปภาพรวมของการตรวจสอบ

4.7.3.1.2 ระบุการจัดระดับความรุนแรง (Severity)หรือผลกระทบที่อาจจะเกิดจากช่องโหว่ที่พบ

4.7.3.1.3 รายละเอียดช่องโหว่ที่ตรวจสอบพบของแต่ละอุปกรณ์ โดยจัดเรียงตามระดับความรุนแรงหรือผลกระทบที่อาจจะเกิดจากช่องโหว่ดังกล่าว

4.7.3.1.4 คำแนะนำและขั้นตอนในการแก้ไข (Action & Recommendation)

4.8 จัดหาให้มีการดำเนินการทดสอบเจาะระบบ(Penetration Testing) อย่างน้อย 1ครั้ง มีคุณลักษณะดังต่อไปนี้

4.8.1 ทดสอบการบุกรุกระบบสารสนเทศโดยใช้รูปแบบการทดสอบการบุกรุกแบบ (ไม่ทราบข้อมูล, ทราบข้อมูลบางส่วน) (Black-Box, Gray-Box) โดยดำเนินการจากอินเทอร์เน็ต

4.8.2 ดำเนินการทดสอบบุกรุกระบบสารสนเทศ (เว็บไซต์, แอปพลิเคชัน) ของโรงพยาบาล

4.8.3 วิเคราะห์และรายงานผลการทดสอบพร้อมคำแนะนำในการปรับปรุงและระบบความปลอดภัยคอมพิวเตอร์

4.8.4 สามารถสร้าง payload (Payload Generator) และสามารถเลือก payload ที่จะใช้โจมตีเครื่องปลายทางได้

4.8.5 รองรับการจำลองการโจมตีในรูปแบบของอีเมล template ได้และสามารถปรับแต่ง landing page ได้

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.8.6 ดำเนินการค้นหาช่องโหว่ประเมินหาจุดอ่อนประเมินความเสี่ยงและผลกระทบพร้อมข้อเสนอแนะแนวทางแก้ไขระบบสารสนเทศและระบบที่เกี่ยวข้องโดยครอบคลุมรายละเอียดดังนี้

4.8.6.1 การดำเนินการจะต้องครอบคลุมในระดับ

- แอปพลิเคชัน (Application) และ ซอฟต์แวร์ (Software) ได้แก่
  - เว็บแอปพลิเคชัน(Web Application)
  - โมบายแอปพลิเคชัน (Mobile Application)
- โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT Infrastructure) และ อุปกรณ์เครือข่าย (Network Device) ได้แก่
  - ระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย (Server Operating Systems)
  - อุปกรณ์ในระบบเครือข่าย(Network Equipment)
  - อุปกรณ์ระบบรักษาความปลอดภัย (Security Equipment)

4.8.6.2 สำหรับ เว็บแอปพลิเคชัน(Web Application) จะใช้มาตรฐาน Open Web Application Security Testing Guide version 4.2 ประกอบด้วยหัวข้อดังนี้

- Introduction and Objectives
- Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Testing for Weak Cryptography
- Business Logic Testing
- Client-side Testing

4.8.6.3 สำหรับ IT Infrastructure and Network Device จะใช้มาตรฐาน The Penetration Testing Execution Standard (PTES) ประกอบด้วยหัวข้อดังนี้

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

- Exploitation
- Post Exploitation
- Reporting

4.8.6.4 สำหรับโมบายแอปพลิเคชัน จะใช้มาตรฐาน OWASP Mobile Application Security Testing Guide (MASTG) version 1.5 ประกอบด้วยหัวข้อดังนี้

- Platform Overview
- Basic Security Testing
- Tampering and Reverse Engineering
- Data Storage
- Cryptographic APIs
- Local Authentication
- Network Communication
- Platform APIs
- Code Quality and Build Settings
- Anti-Reversing Defenses
- User Privacy Protection

4.8.6.5 ดำเนินการโดยใช้โปรแกรมหรือซอฟท์แวร์ที่มีความน่าเชื่อถือเช่น Nessus Professional หรือ Burp Suite Professional หรือ Metasploit professional เป็นต้น

4.9 จัดหาให้มีการดำเนินการวิเคราะห์และให้คำแนะนำในการปรับปรุงเพื่อให้ระบบมีความปลอดภัย

4.9.1 วิเคราะห์และ ให้คำแนะนำในกรณีที่ระบบเครือข่ายสื่อสารมีความจำเป็นต้องได้รับการติดตั้งระบบหรืออุปกรณ์เพิ่มเติมเพื่อเป็นการเพิ่มระดับการรักษาความปลอดภัยของระบบเครือข่ายและระบบความปลอดภัยคอมพิวเตอร์

4.9.2 จัดทำรายงานผลการวิเคราะห์และให้คำแนะนำในการปรับปรุงความปลอดภัยของระบบเครือข่ายและความปลอดภัยคอมพิวเตอร์

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.9.3 รายงานผลการปรับปรุงระบบเครือข่ายและผลการดำเนินการปิดช่องโหว่(Hardening)

4.9.4 ในการทดสอบเจาะระบบจะต้องมีการดำเนินการทั้งหมดไม่น้อยกว่า10 วัน บุคคลหรือกลุ่มบุคคลผู้เข้าดำเนินการทดสอบเจาะระบบจะต้องมีความรู้ความสามารถ ในด้านการวิเคราะห์ตรวจสอบหาจุดที่เป็นช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์ และสารสนเทศ ที่จะเป็นภัยคุกคามต่อหน่วยงาน รวมถึงให้คำแนะนำในการตรวจสอบแก้ไขปัญหาที่พบ โดยบุคคลหรือกลุ่มบุคคลผู้เข้าดำเนินการจะต้องได้รับใบรับรองความรู้ความสามารถ อย่างน้อยดังนี้

4.9.4.1 CEH (Certified Ethical Hacker)

4.9.4.2 ISACA Certified Information Security Manager (CISM)

4.9.4.3 ISACA Certified Information Systems Auditor (CISA)

4.9.4.4 (ISC)2 CC – Certified in Cybersecurity

4.9.4.5 CompTIA CySA+

4.9.4.6 CompTIA Pentest+

4.10 ดำเนินการจัดให้มีการจัดเตรียมทรัพยากรบนระบบเสมือนเพื่อทดสอบการอัปเกรดระบบปฏิบัติการ (Operating System Patching) คุณลักษณะอย่างน้อยดังต่อไปนี้

4.10.1 จัดเตรียมเครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน (Virtual Server) รวมถึงระบบปฏิบัติการ (OS) สำหรับทดสอบการอัพเดท Patching ใหม่ ๆ จำนวน 1 เครื่อง โดยมีคุณสมบัติขั้นต่ำดังนี้

- หน่วยประมวลผลกลาง (vCPU) 2 Cores
- หน่วยความจำ (Memory) 4 GB
- หน่วยบันทึก (Disk) แบบ SATA ขนาดไม่น้อยกว่า 300GB และ แบบ SSD ไม่น้อยกว่า 4 GB

4.10.2 ต้องจัดเตรียม Bandwidth Internet สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (server) รวมถึงระบบปฏิบัติการ (OS) ในการทดสอบ 1 Gbps เป็นอย่างน้อย

4.10.3 ระบบที่ใช้ในการทดสอบจะต้องรองรับการเข้าถึงผ่านทาง Virtual Private Network (VPN) และมีการเข้ารหัสแบบ 2 ขั้นตอน (Multi-factor Authentication)

4.10.4 ระบบที่ใช้ในการทดสอบจะต้องรองรับการเข้าถึงแบบ Console ผ่านทางระบบ Web Application

4.10.5 ระบบที่ใช้ในการทดสอบจะต้องมีระยะเวลาให้ทดสอบไม่น้อยกว่า 3 เดือน

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.11 จัดให้มีบริการศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ (Security Operation Center: SOC) โดยมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ เพื่อทำการวิเคราะห์และแจ้งเตือนภัยคุกคามฯ ให้กับโรงพยาบาล โดยมีขอบเขตดังต่อไปนี้

4.11.1 มีบริการเฝ้าระวังและตอบสนองต่อเหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคามทางไซเบอร์ (Threat Alert notification)

4.11.2 ต้องจัดให้มีทีมเฝ้าระวังและติดตามเหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคามทางไซเบอร์ โดยปฏิบัติงานที่ศูนย์ปฏิบัติการของผู้ให้บริการ โดยจะต้องครอบคลุมตลอด 24 ชั่วโมง (24x7)

4.11.3 ต้องจัดให้มีทีมดำเนินการตรวจสอบและวิเคราะห์เหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคามทางไซเบอร์ เช่น ระบุผลลัพธ์การวิเคราะห์ (Analyst Verdict) กำหนดสถานะของเหตุการณ์ (Incident Status) ระบุรายละเอียดเพิ่มเติม (Incident Note)

4.11.4 ต้องมีเจ้าหน้าที่วิเคราะห์ความปลอดภัย (Security Analyst) เพื่อให้บริการเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและคอยให้ข้อมูลภัยคุกคามเพื่อสนับสนุนการทำงานของเจ้าหน้าที่ เมื่อเกิดเหตุต้องสงสัย เหตุฉุกเฉิน หรือเหตุความผิดปรกติ

4.11.5 ต้องจัดให้มีทีมแจ้งเตือนและประสานงานไปยังเจ้าหน้าที่หรือหน่วยงานที่รับผิดชอบ (Triage & Event Prioritization)

4.11.6 ต้องจัดให้มีทีมสนับสนุนและตอบสนองต่อเหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคาม ระงับ ยับยั้ง หรือยุติกระบวนการที่เป็นอันตรายต่อระบบ โดยต้องดำเนินการอย่างน้อยดังนี้

- ทำความเข้าใจเกี่ยวกับขอบเขตของผลกระทบที่อาจจะเกิดจากภัยคุกคามดังกล่าว
- ทำการระงับ ยับยั้ง หรือ ยุติกระบวนการที่เป็นอันตรายต่อระบบโดยผ่านเทคโนโลยีที่ให้บริการ
- สรุปเหตุการณ์ภัยคุกคาม (Threat Response Summary)

4.11.7 ต้องจัดให้มีทีมคอยทำการปรับจูนเคสต่าง ๆ ในระบบ ทั้งในกรณีที่เป็นเคส False Positive, False Negative รวมถึงการกำหนด Blacklist หรือ Whitelist Asset ต่าง ๆ

4.11.8 ต้องมีผู้เชี่ยวชาญระบบ (Security Specialist) เมื่อเกิดเหตุต้องสงสัย หรือเหตุความผิดปกติ ผู้เชี่ยวชาญระบบ (Security Specialist) ต้องให้ความช่วยเหลือ ให้คำปรึกษารวมถึงแนะแนวทางการแก้ไขปัญหา ในกรณีที่ผู้เชี่ยวชาญระบบ (Security Analyst) ไม่สามารถให้คำปรึกษารวมถึงแนะแนวทางการแก้ไขปัญหาให้แก่เจ้าหน้าที่ ผ่านช่องทาง Email

ลงชื่อ.....	นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....	นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....	นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....	นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....	นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

4.11.9 ต้องจัดให้มีทีมผู้เชี่ยวชาญคอยทำการค้นหาข้อมูล เชื่อมโยงพฤติกรรม หรือข้อมูลบ่งชี้สัญญาณภัยคุกคามไซเบอร์ต่าง ๆ ในกรณีที่มีเหตุการณ์ ข่าวสาร หรือลักษณะพฤติกรรมที่อยู่ในข่ายน่าสงสัย

4.11.10 ต้องจัดให้มีการแจ้งเตือน พร้อมให้คำแนะนำและข้อมูลที่จำเป็นแก่ทีมงาน หรือเจ้าหน้าที่ที่เกี่ยวข้อง หากตรวจพบลักษณะพฤติกรรมที่อยู่ในข่ายน่าสงสัย

4.11.11 บริการจัดทำรายงานผลการดำเนินการ และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคามเหตุการณ์ผิดปกติที่เป็นภัยคุกคามเป็นรายเดือน (Monthly report)

4.11.12 ระยะเวลาบริการศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ (Cyber Security Operations Center : CSOC) ทั้งสิ้น 12 เดือน นับถัดจากวันที่ส่งมอบ

4.11.13 ต้องทำการเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ผ่านทาง E-mail ตาม Service Level Agreement ที่กำหนดดังต่อไปนี้

ระดับความรุนแรง	ผลกระทบ	เวลาในการแจ้งเตือนนับจากเกิดเหตุ	เวลาในการให้คำแนะนำแก้ไขปัญหานับจากเกิดเหตุ
วิกฤต (Critical)	การให้บริการทุกระบบงานหยุดชะงักและจำเป็นต้องแก้ไขอย่างเร่งด่วนที่สุด	ภายใน 15 นาที	ภายใน 30 นาที
สูง (High)	การให้บริการบางระบบงานหยุดชะงักและจำเป็นต้องแก้ไขอย่างเร่งด่วน	ภายใน 30 นาที	ภายใน 60 นาที
ปานกลาง (Medium)	ผลกระทบต่อบางระบบงานภายในหยุดชะงักและมีความจำเป็นต้องแก้ไขทันที	ภายใน 60 นาที	ภายใน 4 ชั่วโมง
ต่ำ (Low)	ผลกระทบต่อประสิทธิภาพการทำงานทั่วไปและมีผลกระทบต่อระบบงานโดยภาพรวมเล็กน้อย	ภายใน 24ชั่วโมง	ภายใน 48 ชั่วโมง

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์ นายแพทย์ชำนาญการพิเศษ ประธานกรรมการ

ลงชื่อ.....นายพิริยะ พิริยะกฤต นายแพทย์ชำนาญการ กรรมการ

ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล พยาบาลวิชาชีพชำนาญการพิเศษ กรรมการ

ลงชื่อ.....นายณรงค์ รวมสุข นักวิชาการคอมพิวเตอร์ปฏิบัติการ กรรมการ

ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต เจ้าพนักงานสถิติ กรรมการ

5.ระยะเวลาการดำเนินการ

ระยะเวลาของสัญญาครอบคลุม 12 เดือน นับตั้งแต่เดือนที่ลงนามในสัญญา ดังนี้

5.1 ผู้ยื่นข้อเสนอจะต้องส่งมอบระบบและสิทธิ์การใช้งานซอฟต์แวร์ภายใน 60 วัน นับถัดจากวันลงนามในสัญญา

5.2 ระยะเวลาการดำเนินของระบบในโครงการจะต้องใช้งานได้อย่างน้อย 365 วัน (Hardware และ Software) นับถัดจากวันที่ส่งมอบระบบ

5.3 ระยะเวลาบริการศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ (Security Operation Center: SOC) ทั้งสิ้น 1 ปี นับถัดจากวันที่ส่งมอบ

6. การส่งมอบงานและการชำระเงิน

ผู้ยื่นข้อเสนอจะต้องปฏิบัติงาน และรายงานผลการให้บริการตามสัญญาพร้อมส่งมอบงานในแต่ละงวด เป็นเอกสาร จำนวน 2 ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบที่ปรับแก้ไขได้ (MSOffice) และปรับแก้ไขไม่ได้ (PDF) พร้อมบันทึกลงใน USBflash drive หรือสื่อแบบถอดได้อื่น ๆ (Removable) หรือแผ่นซีดี (CD) จำนวน 2 ชุด รวมถึงเอกสารหลักฐานต่างๆ ที่เกี่ยวข้องครบถ้วน และผ่านการตรวจรับงานจ้างจากคณะกรรมการตรวจรับงานจ้างเรียบร้อยแล้ว ผู้เช่าตกลงชำระค่าจ้างดำเนินการโครงการให้แก่ผู้ยื่นข้อเสนอเป็นเช็คขีดคร่อมหรือการโอนเงินทางอิเล็กทรอนิกส์ โดยผู้เช่าจะหักภาษีค่าธรรมเนียมธนาคารและค่าธรรมเนียมอื่นๆ ที่เกี่ยวข้องจากมูลค่าของค่าจ้างซึ่งผู้ยื่นข้อเสนอจะต้องชำระไว้ตามกฎหมายด้วยแบ่งเป็นงวดการส่งมอบงานและงวดการจ่ายเงินดังนี้

6.1 ส่งมอบภายใน 15 วันนับถัดจากวันลงนามในสัญญา ประกอบด้วย

6.1.1 ตัวอย่างรายงานการปฏิบัติการให้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์และโต้ตอบต่อภัยคุกคามไซเบอร์

6.1.2 ตารางแผนกิจกรรมการดำเนินงานและการเข้าปฏิบัติงานในโรงพยาบาลตลอดระยะเวลาสัญญา

6.1.3 รายชื่อเจ้าหน้าที่ของผู้ยื่นข้อเสนอ พร้อมข้อมูลสำหรับการติดต่อประสานงาน และการเข้าพื้นที่โรงพยาบาลเพื่อติดตั้งระบบ และให้บริการระบบต่างๆ

6.2 ติดตั้งอุปกรณ์ ซอฟต์แวร์ และดำเนินการให้ครบตามที่กำหนดไว้ในข้อ 4 คุณลักษณะเฉพาะทางเทคนิคและสิ่งส่งมอบให้แล้วเสร็จภายใน 60 วันนับถัดจากวันลงนามในสัญญา

6.2.1 ระบบการจัดเก็บข้อมูลสำรอง (Backup) ในส่วนของข้อมูลศูนย์ข้อมูลคอมพิวเตอร์ (Data Center และบริการระบบคลาวด์ (Cloud Computing) พร้อมคู่มือการใช้งานระบบ

6.2.2 ระบบป้องกันตรวจจับและโต้ตอบภัยคุกคาม Endpoint Detection & Response (EDR) จำนวน 1 ระบบ พร้อมคู่มือการใช้งานระบบ

6.2.3 ระบบตรวจสอบการเข้าถึงอย่างปลอดภัยและการยืนยันตัวตน 2 ชั้น (Multi-factor Authentication) จำนวนไม่น้อยกว่า 20 ผู้ใช้งาน (user) พร้อมคู่มือการใช้งานระบบ

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

6.2.4 ติดตั้งอุปกรณ์ระบบป้องกันการโจมตีเว็บไซต์และแอปพลิเคชัน (Web Application Firewall: WAF) จากการโจมตีในระดับเครือข่ายโดยครอบคลุมระบบสารสนเทศที่ให้บริการ ให้สามารถใช้งานได้ พร้อมคู่มือการใช้งาน

6.2.5 ติดตั้งระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log management) พร้อมคู่มือการใช้งาน

6.2.6 ระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (Security Information and Event Management: SIEM) พร้อมคู่มือการใช้งานระบบ (ถ้ามี)

6.2.7 ผลการตรวจสอบช่องโหว่ในระดับระบบปฏิบัติการ (Vulnerability Assessment)

6.2.8 ผลดำเนินการทดสอบเจาะระบบ (Penetration Testing)

6.2.9 ผลการวิเคราะห์และให้คำแนะนำในการปรับปรุงเพื่อให้ระบบมีความปลอดภัย

6.2.10 ผลดำเนินการจัดให้มีการจัดเตรียมทรัพยากรบนระบบเสมือนเพื่อทดสอบการอัปเกรดระบบปฏิบัติการ (Operating System Patching)

6.2.11รายงานการวิเคราะห์สถานการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Gap Analysis) เพื่อค้นหา As Is และ To Be

6.2.12 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

6.2.13 คู่มือการตอบรับเหตุการณ์ (Incident Response Playbook) ตามประเภทของภัยคุกคามเพื่อใช้อ้างอิงในการปฏิบัติการในการจัดการหรือตอบรับภัยคุกคามต่าง ๆ ได้อย่างถูกต้องให้กับโรงพยาบาล

6.2.14 แผนภูมิรูปภาพสรุปเหตุการณ์ ที่แสดงถึงการวิเคราะห์แบบ Dynamic และแบบ Static ในรายงานสรุปผลวิเคราะห์เฝ้าระวังและแนวทางการป้องกันภัยคุกคาม รวมถึงรายงานภัยคุกคามต่าง ๆ กรณีที่พบเหตุการณ์ต้องสงสัยให้ดำเนินการพิสูจน์หลักฐาน (Forensic) วิเคราะห์ภัยคุกคาม เช่น Malware,Ransomware พร้อมนำเสนอ

6.2.15 รายงานผลการฝึกอบรมการใช้งานระบบต่างๆ ให้แก่เจ้าหน้าที่โรงพยาบาล

6.2.16 รายงานการปฏิบัติงานของศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ (Security Operation Center :SOC) โดยมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ เพื่อทำการวิเคราะห์และแจ้งเตือนภัยคุกคามฯ ให้กับโรงพยาบาล ทุกสิ้นเดือน

6.2.17 รายงานผลการให้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์และโต้ตอบต่อภัยคุกคามไซเบอร์ของเดือน และข้อมูลสะสมภาพรวม ทุกสิ้นเดือน

6.2.18 รายงานสรุปเหตุภัยคุกคามทางไซเบอร์ และการแก้ไขปัญหาที่เกิดขึ้น ของเดือน และข้อมูลสะสมภาพรวม ทุกสิ้นเดือน

6.2.19 รายงานการตรวจสอบและติดตามผลการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ ของเดือน และข้อมูลสะสมภาพรวม ทุกสิ้นเดือน

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

6.2.20 รายงานผลการได้สิทธิ์ใช้งาน Next-generation Antivirus ที่ถูกต้องตามกฎหมาย ได้อย่างน้อย 50 Licenses สำหรับ Client

6.3 ชำระเงินเป็นรายงวดจำนวน 12 งวด โดยเริ่มนับงวดที่ 1 เมื่อส่งมอบงานตามข้อ 6.2 แล้วและให้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์และโต้ตอบต่อภัยคุกคามไซเบอร์เป็นระยะเวลาครบ 1 เดือน

งวดที่ 1 จ่ายค่าเช่าใช้บริการ จำนวนร้อยละ 8.37 ของวงเงินในสัญญา
งวดที่ 2 จ่ายค่าเช่าใช้บริการ จำนวนร้อยละ 8.33 ของวงเงินในสัญญา
งวดที่ 3 จ่ายค่าเช่าใช้บริการ จำนวนร้อยละ 8.33 ของวงเงินในสัญญา
งวดที่ 4 จ่ายค่าเช่าใช้บริการ จำนวนร้อยละ 8.33 ของวงเงินในสัญญา
งวดที่ 5 จ่ายค่าเช่าใช้บริการ จำนวนร้อยละ 8.33 ของวงเงินในสัญญา
งวดที่ 6 จ่ายค่าเช่าใช้บริการ จำนวนร้อยละ 8.33 ของวงเงินในสัญญา
งวดที่ 7 จ่ายค่าเช่าใช้บริการ จำนวนร้อยละ 8.33 ของวงเงินในสัญญา
งวดที่ 8 จ่ายค่าเช่าใช้บริการ จำนวนร้อยละ 8.33 ของวงเงินในสัญญา
งวดที่ 9 จ่ายค่าเช่าใช้บริการ จำนวนร้อยละ 8.33 ของวงเงินในสัญญา
งวดที่ 10 จ่ายค่าเช่าใช้บริการ จำนวนร้อยละ 8.33 ของวงเงินในสัญญา
งวดที่ 11 จ่ายค่าเช่าใช้บริการ จำนวนร้อยละ 8.33 ของวงเงินในสัญญา
งวดที่ 12 จ่ายค่าเช่าใช้บริการ จำนวนร้อยละ 8.33 ของวงเงินในสัญญา

7. หลักเกณฑ์การพิจารณาข้อเสนอ

7.1. การพิจารณาผลการยื่นข้อเสนอการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ โรงพยาบาลจะพิจารณาตัดสินโดยใช้เกณฑ์ราคา

7.2. ผู้ยื่นข้อเสนอจะต้องเสนอแผนการดำเนินงานของกิจกรรมฯ ตามขอบเขตของงานข้อ 4 และจัดทำเอกสารเปรียบเทียบระหว่างข้อกำหนดรายละเอียดคุณลักษณะเฉพาะกับแนวทางหรือแผนการดำเนินงาน กิจกรรมของผู้ยื่นข้อเสนอมาเพื่อประกอบการพิจารณา โดยต้องระบุเลขหน้า เลขข้อ กำกับให้ชัดเจน สะดวกในการเทียบเคียง มิฉะนั้นจะไม่ได้รับการพิจารณา

7.3. ในการตัดสินการประกวดราคาอิเล็กทรอนิกส์หรือในการทำสัญญา คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์มีสิทธิให้ผู้ยื่นข้อเสนอชี้แจงข้อเท็จจริง สภาพฐานะ หรือข้อเท็จจริงอื่นใดที่เกี่ยวข้องกับผู้ยื่นข้อเสนอได้ โดยผู้เช่ามีสิทธิที่จะไม่รับข้อเสนอ ไม่รับราคาหรือไม่ทำสัญญา หากหลักฐานดังกล่าวไม่มีความเหมาะสมหรือไม่ถูกต้อง

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

7.4. ในกรณีที่ปรากฏข้อเท็จจริงภายหลังจากการพิจารณาข้อเสนอว่า ผู้ยื่นข้อเสนอที่มีสิทธิได้รับการคัดเลือกเป็นผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่น ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือเป็นผู้ยื่นข้อเสนอที่กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ผู้เช่ามีอำนาจที่จะตัดรายชื่อผู้ยื่นข้อเสนอที่ได้รับคัดเลือกรายดังกล่าวออกและยกเลิกผลการพิจารณาและแจ้งกรมบัญชีกลางดำเนินการต่อไป

7.5. ผลการพิจารณาให้ถือการตัดสินของคณะกรรมการเป็นสำคัญผู้ใดจะนำไปเป็นเหตุกล่าวอ้างเพื่อเรียกร้องค่าเสียหายต่อโรงพยาบาลภายหลังไม่ได้

8. ค่าปรับ

8.1 ค่าปรับการส่งมอบงานล่าช้า

หากผู้ยื่นข้อเสนอไม่สามารถส่งมอบงานได้ตามเวลาที่ กำหนดไว้ในสัญญาและผู้ว่าจ้างยังมิได้บอกเลิกสัญญา ผู้ยื่นข้อเสนอจะต้องชำระค่าปรับให้แก่โรงพยาบาล เป็นรายวันในอัตราร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ของราคาค่าจ้าง ตามสัญญา แต่ต้องไม่ต่ำกว่าวันละ 100 บาท (หนึ่งร้อยบาท) กรณีมีการเปลี่ยนแปลงใดๆ ให้อยู่ในดุลยพินิจของโรงพยาบาล เว้นแต่เหตุสุดวิสัย รวมถึงสถานการณ์เหตุการณ์ความไม่สงบในประเทศ ทั้งนี้ต้องได้รับความเห็นชอบจากโรงพยาบาลก่อน

8.2 ค่าปรับในระยะเวลารับประกัน

หากผู้ยื่นข้อเสนอไม่เข้ามาแก้ไขให้แล้วเสร็จตามการรับประกันความชำรุดบกพร่อง ภายใน 7 วันทำการนับจากวันที่ได้รับแจ้งจากโรงพยาบาล ผู้ยื่นข้อเสนอจะต้องชำระค่าปรับให้ผู้ว่าจ้างเป็นรายวันในอัตราร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ของวงเงินตามสัญญาจนกว่าจะแก้ไขปัญหาแล้วเสร็จ

9. ข้อสงวนสิทธิ์

9.1 โรงพยาบาลสงวนสิทธิ์ในการตัดสินวินิจฉัย ชี้ขาดปัญหาที่เกิดขึ้นทุกกรณี และให้ถือว่าคำวินิจฉัยของโรงพยาบาลเป็นที่สิ้นสุด ผู้ยื่นข้อเสนอตลอดจนผู้ยื่นข้อเสนอต้องยอมรับคำวินิจฉัยดังกล่าว โดยไม่มีข้อโต้แย้งหรือข้อแม้ใดทั้งสิ้น

9.2 การดำเนินงาน ผู้ยื่นข้อเสนอจะต้องไม่ละเมิดลิขสิทธิ์ผลงานของผู้อื่นโดยไม่ได้รับอนุญาต ข้อมูลอันเกิดจากการจัดจ้าง ตลอดจนรายงานสรุปที่จัดทำขึ้น เป็นกรรมสิทธิ์ของโรงพยาบาล ซึ่งผู้ยื่นข้อเสนอจะต้องไม่มอบข้อมูลในการดำเนินงานให้แก่ผู้ใด รวมทั้งไม่เผยแพร่ข้อมูลรายงานสรุป โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากโรงพยาบาล

9.3 ในกรณีที่ผู้ว่าจ้างมีความจำเป็นไม่อาจทำสัญญาได้หรือมีเหตุจำเป็นด้านอื่นๆที่เป็นอุปสรรคผู้ว่าจ้าง ขอสงวนสิทธิ์ที่จะยกเลิกการว่าจ้างครั้งนี้ได้ทุกขั้นตอนโดยไม่จำเป็นต้องแจ้งเหตุผลใดๆ ให้ผู้ยื่นข้อเสนอทราบ และผู้ยื่นข้อเสนอไม่มีสิทธิ์โต้แย้งและเรียกร้องค่าใช้จ่ายหรือค่าเสียหายใดๆ ทั้งสิ้น

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

9.4 ผู้ว่าจ้างมีสิทธิ์ที่จะเปลี่ยนแปลงแก้ไขเพิ่มเติมหรือลดเนื้องานตามรายละเอียดในสัญญาได้การเพิ่ม หรือลดเนื้องานคู่ สัญญาทั้งสองฝ่ายจะได้ตกลงเรื่องราคาใหม่โดยถือราคาที่ระบุไว้ในสัญญาเป็นฐานถ้าการเพิ่ม หรือลดงานจำเป็นต้องมีการขยายหรือลดเวลาให้ตกลงไปในคราวเดียวกัน

9.5 การจัดซื้อจัดจ้างจะสามารถดำเนินการได้ก็ต่อเมื่อโครงการได้รับการจัดสรรงบประมาณแล้วเท่านั้น

9.6 ข้อมูล เอกสาร หรือสัญญาที่เกี่ยวข้องกับโครงการทั้งหมดที่ผู้ยื่นข้อเสนอดำเนินการและจัดหามาให้ตามสัญญาถือเป็นความลับและเป็นสมบัติของผู้ว่าจ้างผู้ยื่นข้อเสนอจะไม่เปิดเผยข้อมูลและผลการดำเนินการให้แก่ผู้ใดยกเว้นแต่จะได้รับอนุญาตจากผู้ว่าจ้างเป็นลายลักษณ์อักษร หากที่ผู้ยื่นข้อเสนอละเมิดโดยการนำไปเผยแพร่และเปิดเผย โดยไม่ได้รับอนุญาตผู้ว่าจ้างมีสิทธิ์ฟ้องเรียกค่าเสียหายและดำเนินการตามกฎหมายตามแต่กรณี ทั้งนี้บุคลากรของผู้ยื่นข้อเสนอที่มาปฏิบัติงานในโครงการทุกคนจะต้องลงลายมือชื่อรับทราบข้อตกลง ห้ามเปิดเผยข้อมูลด้วยตนเอง

9.7 ผู้ว่าจ้างมีสิทธิ์ร้องขอให้ผู้ยื่นข้อเสนอสนับสนุนการบรรยาย/ให้ข้อมูลผลการปฏิบัติตามโครงการฯ ตามที่โรงพยาบาลขอ

10. การรับประกันความชำรุดบกพร่องของพัสดุที่ส่งมอบ

10.1 ผู้ยื่นข้อเสนอต้องรับประกันความชำรุดบกพร่องหรือขัดข้องของระบบสัญญานี้เป็นตามระยะเวลารับประกันนับแต่วันที่ผู้ว่าจ้างได้รับมอบถ้าภายในระยะเวลาดังกล่าวหากชำรุดบกพร่องหรือใช้งานไม่ได้ทั้งหมด หรือแต่บางส่วนและความชำรุดบกพร่อง มิใช่ความผิดของผู้ว่าจ้าง กรณีข้อชำรุดบกพร่อง อันเกิดจากการประกอบ ติดตั้งที่ไม่ได้มาตรฐานต้องทำการแก้ไขทันที ผู้ยื่นข้อเสนอจะต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้การได้ดีดังเดิม ภายใน 7 วัน ทำการนับแต่วันเวลาที่ได้รับแจ้งจากผู้ว่าจ้าง และรับผิดชอบค่าใช้จ่ายทั้งหมด การรับประกันการชำรุด บกพร่องเป็นการขยายความซึ่งไม่ใช่การชำรุดโดยการใช้งานโดยไม่คิดค่าใช้จ่ายใดๆ จากผู้ว่าจ้างทั้งสิ้น

10.2 ผู้ยื่นข้อเสนอต้องรับประกันความชำรุดบกพร่องของงานตลอดอายุสัญญาการให้บริการ

11. งบประมาณ

วงเงินงบประมาณในการจัดหา จำนวน 2,000,000 บาท (สองล้านบาทถ้วน)

ลงชื่อ.....นายฉันทวัฒน์ สุทธิพงษ์	นายแพทย์ชำนาญการพิเศษ	ประธานกรรมการ
ลงชื่อ.....นายพิริยะ พิริยะกฤต	นายแพทย์ชำนาญการ	กรรมการ
ลงชื่อ.....นางสาวเกษณี ศรีพัฒนตระกูล	พยาบาลวิชาชีพชำนาญการพิเศษ	กรรมการ
ลงชื่อ.....นายณรงค์ รวมสุข	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
ลงชื่อ.....นายภาณุพงศ์ เชื่อมชิต	เจ้าพนักงานสถิติ	กรรมการ

<u>ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)</u>
<u>ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง</u>

๑. ชื่อโครงการ เช่าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์ของโรงพยาบาลนครพิงค์ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข จำนวน ๑ ระบบ

๒. หน่วยงานเจ้าของโครงการ โรงพยาบาลนครพิงค์ จังหวัดเชียงใหม่

๓. วงเงินงบประมาณที่ได้รับจัดสรร ๒,๐๐๐,๐๐๐.๐๐ บาท (สองล้านบาทถ้วน)

๔. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ๑๕ พ.ค. ๒๕๖๘

เป็นเงิน ๑,๙๗๓,๖๘๐.๐๐ บาท (หนึ่งล้านเก้าแสนเจ็ดหมื่นสามพันหกร้อยแปดสิบบาทถ้วน)

๕. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

ใช้ราคากลางตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ มาตรา ๔ (๔) ราคาที่สืบจากท้องตลาด ตามใบเสนอราคาของบริษัท ดังนี้

๕.๑. บริษัท วีเอสที อีซีเอส (ประเทศไทย) จำกัด

๕.๒. ห้างหุ้นส่วนจำกัด พาวเวอร์ โซลูชั่น โพรไวเดอร์

๕.๓. บริษัท ชิชาง คอมพิวเตอร์ (ประเทศไทย) จำกัด

๖. รายชื่อผู้รับผิดชอบกำหนดราคากลาง

๖.๑ นายฉันทวัฒน์ สุทธิพงษ์ นายแพทย์ชำนาญการพิเศษ.....

๖.๒ นายพิริยะ พิริยะกฤต นายแพทย์ชำนาญการ.....

๖.๓ นางสาวเกษณี ศรีพัฒนตระกูล พยาบาลวิชาชีพชำนาญการพิเศษ.....

๖.๔ นายณรงค์ รวมสุข นักวิชาการคอมพิวเตอร์ปฏิบัติการ.....

๖.๕ นายภาณุพงศ์ เชื่อมชิต เจ้าพนักงานสถิติ.....