

**ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)
ในการเข้าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์และโต้ตอบต่อภัยคุกคามไซเบอร์
ของโรงพยาบาลกระบี่**

๑. ชื่อโครงการ.เข้าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามไซเบอร์
ของโรงพยาบาลกระบี่ จำนวน ๑ รายการ ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)
หน่วยงานเจ้าของโครงการ.....โรงพยาบาลกระบี่
๒. วงเงินงบประมาณที่ได้รับจัดสรร ๒,๕๐๐,๐๐๐.-บาท (สองล้านห้าแสนบาทถ้วน)
๓. วันที่กำหนดราคากลาง (ราคาอ้างอิง) วันที่ ๑ เมษายน ๒๕๖๘
เข้าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์และโต้ตอบต่อภัยคุกคามไซเบอร์ฯ จำนวน ๑ รายการ
๒,๕๐๐,๐๐๐.- บาท (สองล้านห้าแสนบาทถ้วน)
๔. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
สำนักงานปลัดกระทรวงสาธารณสุข โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.)
๕. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง)

๕.๑ นายศิริวิทย์ อัสวีวัฒน์	เภสัชกรชำนาญการพิเศษ	ประธานกรรมการ
๕.๒ นายทรงพล ถึงพร้อม	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ
๕.๓ นายกฤษฎา แท้มทอง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการ

ขอบเขตของงาน (Terms of Reference: TOR)
โครงการเข้าใช้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์และโต้ตอบภัยคุกคาม
ไซเบอร์ ของโรงพยาบาลกระบี่
ภายใต้โครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข

๑. หลักการและเหตุผล

โรงพยาบาลเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องลักษณะหน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ.๒๕๖๔ จึงมีความจำเป็นอย่างยิ่งที่จะต้องดำเนินการให้ระบบบริการและระบบงานดิจิทัลมีความมั่นคงปลอดภัยทางไซเบอร์

ในปีงบประมาณ พ.ศ. ๒๕๖๘ โรงพยาบาลกระบี่ได้รับคัดเลือกให้เข้าร่วมโครงการสนับสนุนการจัดตั้ง Sectoral CERT ด้านสาธารณสุข ภายใต้แผนงานบูรณาการรัฐบาลดิจิทัลจึงเป็นโอกาสที่จะพัฒนาให้โรงพยาบาลมีศักยภาพเพียงพอที่จะรับมือเหตุฉุกเฉินทางคอมพิวเตอร์ สามารถป้องกันตรวจจับวิเคราะห์และโต้ตอบภัยคุกคามทางไซเบอร์ได้ โดยข้อมูลจะเชื่อมโยงไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (HealthCERT) ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข จังหวัดนนทบุรี

๒. วัตถุประสงค์

๒.๑ เพื่อให้โรงพยาบาลได้รับการติดตั้งระบบตรวจจับและวิเคราะห์ภัยคุกคามขั้นสูงในระดับเครือข่ายคอมพิวเตอร์และเทคโนโลยีสารสนเทศ

๒.๒ เพื่อให้โรงพยาบาลได้รับบริการเฝ้าระวัง รับมือ ตรวจจับภัยคุกคามเชิงรุกและโต้ตอบเหตุภัยคุกคามจากผู้เชี่ยวชาญ และเชื่อมโยงข้อมูลไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (HealthCERT) ได้

๒.๓ เพื่อให้โรงพยาบาลได้รับการอบรมพัฒนาบุคลากรให้มีความพร้อมในการรับมือเหตุฉุกเฉินที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์

๓. คุณสมบัติของผู้ยื่นข้อเสนอ

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

.....นายศิริวิทย์ อัสวีวัฒน์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายภุชญา แต้มทอง กรรมการ

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ เป็นนิติบุคคลผู้มีอาชีพให้บริการ ประเภทเดียวกันกับงานที่ประกวดราคาอิเล็กทรอนิกส์นี้

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สำนักงาน ปลัดกระทรวงสาธารณสุข ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการ อันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่น ข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

๓.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงานสิ่งของหรือ มูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค่านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็น ผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อ

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

๓.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะ การเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีงบการเงินงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่น ข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๑ ล้านบาท

(๓) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอ เป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมี เงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่น ข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือ รับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

.....นายศิริวิทย์ อัสวฒิมวงศ์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายภุชญา แท้มทอง กรรมการ

(๔) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณที่ยื่นข้อเสนอในครั้งนั้น (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน)

(๕) กรณีตาม (๑) - (๔) ยกเว้นสำหรับกรณีดังต่อไปนี้

(๕.๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(๕.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑

๓.๑๓ ผู้ยื่นข้อเสนอต้องมีผลงานประเภทเดียวกันกับงานที่ประกวดราคา และเป็นผลงานที่มีวงเงินไม่น้อยกว่า ๕๐๐,๐๐๐.-บาท (ห้าแสนบาทถ้วน) โดยแนบเอกสารผลงานหรือสำเนาสัญญาจ้างมาพร้อมการยื่นเอกสารเสนอราคา

๔. คุณสมบัติเฉพาะทางเทคนิคและสิ่งส่งมอบ

ผู้ยื่นข้อเสนอต้องให้บริการในการป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ รวมถึงปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงาน ภายใต้การดูแลเพื่อเฝ้าระวังติดตามและเตรียมความพร้อมในการรับมือ เมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งในประเทศและต่างประเทศ ประสานงานกับหน่วยงานภายใต้การดูแล เพื่อตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์อย่างเหมาะสมและทันทั่วทั้งที่ ตลอดจนให้การช่วยเหลือแนะนำ จัดอบรมการใช้งานเครื่องมือทั้งหมด ณ สถานที่ทำการของหน่วยงาน และสนับสนุนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยประสานงานร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานนั้น ๆ โดยสามารถรายงานลำดับความสำคัญของสิ่งผิดปกติที่เกิดขึ้นในระบบด้วยอุปกรณ์ป้องกันตรวจจับ วิเคราะห์ภัยคุกคามขั้นสูง พร้อมทั้งดำเนินการพัฒนาบุคลากร ให้มีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ และให้บริการเฝ้าระวังรับมือตรวจจับภัยคุกคามเชิงรุก ได้ตอบเหตุการณ์ฉุกเฉินที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์

ในการพัฒนาระบบงานดังกล่าวข้างต้นผู้ยื่นข้อเสนอจะต้องดำเนินการภายใต้ขอบเขตของงาน โดยมีรายละเอียดสิ่งส่งมอบและคุณสมบัติเฉพาะทางเทคนิค ดังนี้

๔.๑ จัดให้มีระบบการจัดเก็บข้อมูลสำรอง (Backup) ในส่วนของข้อมูลศูนย์ข้อมูลคอมพิวเตอร์ (Data Center และบริการระบบคลาวด์ (Cloud Computing) ได้รับการรับรองมาตรฐานอย่างน้อยดังต่อไปนี้

(๑) มาตรฐานการบริหารการรักษาความปลอดภัย ISO/IEC ๒๗๐๐๑

(๒) มาตรฐานความปลอดภัยสำหรับระบบคลาวด์ CSA-STAR Cloud Security (CSA STAR)

(๓) มาตรฐานความปลอดภัยบนมาตรฐาน Healthcare ISO ๒๗๗๙๙ หรือแสดงให้เห็นได้ว่า มีกระบวนการในการปกป้องข้อมูลสุขภาพได้ตามแนวทาง ISO ๒๗๗๙๙

(๔) มาตรฐานสากลสำหรับการปกป้องข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ ISO/IEC ๒๗๐๑๘

.....นายศิริวิทย์ อัสวีฌิงค์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายกฤษฎา แต้มทอง กรรมการ

โดยมีคุณลักษณะอย่างน้อยดังต่อไปนี้

- ๔.๑.๑ ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ตั้งอยู่ในประเทศไทย อย่างน้อย ๒ ศูนย์ข้อมูล มีระยะทางห่างกันอย่างน้อย ๕๐ กิโลเมตร และศูนย์คอมพิวเตอร์ (Data Center) ทุกแห่ง ต้องมีระบบเครือข่ายสื่อสารหลัก ที่เชื่อมเป็นเครือข่ายเดียวกันด้วยเทคโนโลยีบริหารจัดการระบบเครือข่าย (Software Define Infrastructure: SDI) เพื่อรองรับแผนการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning: BCP)
- ๔.๑.๒ มีระบบสำรองไฟฟ้าฉุกเฉินในกรณีที่เกิดเหตุฉุกเฉินกับแหล่งจ่ายไฟฟ้าหลัก และต้องสามารถทำงานได้อย่างต่อเนื่องตลอดเวลา
- ๔.๑.๓ ผู้ยื่นข้อเสนอต้องจัดให้มีการสำรองข้อมูล (Backup) เพื่อทำการบันทึกข้อมูลของระบบทั้งหมด เก็บไว้ในศูนย์ ข้อมูลคอมพิวเตอร์หลัก (DC Site) และศูนย์ข้อมูลคอมพิวเตอร์สำรอง (Backup Site) พร้อมกัน
- ๔.๑.๔ ผู้ยื่นข้อเสนอต้องจัดหาระบบสำรองข้อมูลบนระบบเสมือน โดยมีการจัดเตรียม Software Backup ที่มีการรองรับการส่งข้อมูลความปลอดภัย TLS ๑.๒ ขึ้นไปและรองรับการเข้ารหัส SHA ๒๕๖ หรือดีกว่า พร้อมทั้งมีระบบป้องกันไม่ให้ไฟล์ข้อมูลสำรองถูกลบหรือแก้ไขได้ (Immutable หรือ Immutability หรือ WORM)
- ๔.๑.๕ Software Backup ต้องรองรับการสำรองข้อมูล (Backup) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ระบบปฏิบัติการ Microsoft Windows Server ๒๐๐๘ R๒ SP๑๒ ขึ้นไปถึงปัจจุบันหรือระบบปฏิบัติการ Linux Distro ที่ออกตั้งแต่ปี ๒๐๑๔ ที่ยังมีการสนับสนุนอยู่
- ๔.๑.๖ จัดเตรียมพื้นที่เก็บข้อมูล (Disk) สำหรับสำรองข้อมูลที่มีพื้นที่สูงสุด ๒,๐๐๐ กิกะไบต์ (GB)
- ๔.๑.๗ มีการสำรองข้อมูลที่ศูนย์ข้อมูลคอมพิวเตอร์หลัก (DC Site) และศูนย์ข้อมูลคอมพิวเตอร์สำรอง (DR Site) โดยทำการเก็บสำรองข้อมูลไว้เป็นรายวัน จำนวน ๗ สำเนา เป็นรายสัปดาห์ จำนวน ๑ สำเนา และเป็นรายเดือน จำนวน ๑ สำเนา
- ๔.๑.๘ กรณีที่ผู้ใช้บริการต้องการกู้ข้อมูลสามารถแจ้งดำเนินการผ่านช่องทางการ support ตลอดเวลา โดยจะทำการ export ข้อมูลในระดับ file ส่งผ่าน ftp ที่มีการเข้ารหัส และจัดส่งให้กับผู้ใช้บริการ นำไปใช้งานในลำดับต่อไปโดยไม่รวม service ภายในเครื่อง

๔.๒ จัดหาให้มีระบบป้องกันตรวจจับและได้ตอบภัยคุกคาม Endpoint Detection & Response (EDR) จำนวน ๑ ระบบ โดยแต่ละระบบมีคุณลักษณะอย่างน้อยดังต่อไปนี้

- ๔.๒.๑ สามารถควบคุมและบริหารจัดการระบบ Endpoint Detection & Response (EDR) ผ่าน Cloud-based management console เพื่อกำหนดนโยบายด้านความปลอดภัยและบังคับใช้การป้องกันไปยังเครื่องแม่ข่าย (agent) ผ่านทาง Web Browser
- ๔.๒.๒ มีสิทธิ์การใช้งาน EDR ที่ถูกต้องตามกฎหมาย ได้อย่างน้อย ๖๐ Licenses สำหรับ Server
 - ๔.๒.๒.๑ สามารถติดตั้ง EDR agent เพื่อทำการป้องกันเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ระบบปฏิบัติการ Microsoft Windows Server ๒๐๑๖ ขึ้นไปถึงปัจจุบัน หรือระบบปฏิบัติการ Linux Distro ที่ยังมีการสนับสนุนอยู่

.....นายศิริวิทย์ อัสวฒินวงศ์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายภุชญา แท้มทอง กรรมการ

- ๔.๒.๒.๒ ระบบบริหารจัดการต้องรองรับการบริหารจัดการแบบแยกส่วนได้ในอนาคต (Sub-estate) สำหรับบริหารจัดการแบบหลายสาขา โดยมี Admin Console แยกสำหรับผู้ดูแลระบบ (Admin) ของแต่ละสาขา และมี Enterprise Console สำหรับผู้ดูแลระบบจากส่วนกลาง (Enterprise Admin)
- ๔.๒.๒.๓ ระบบจะต้องมีความสามารถในการตรวจจับภัยคุกคามดังต่อไปนี้ได้ virus, trojans, backdoors, worms, rootkits, packer, ransomware, cryptocurrency mining และ spyware
- ๔.๒.๒.๔ สามารถทำการตรวจสอบกระบวนการที่ถูกบุกรุก (compromised) และทำการยุติกระบวนการ (terminate) เพื่อป้องกันการติดไวรัส (infection) เพิ่มเติมได้
- ๔.๒.๒.๕ สามารถทำ Machine learning เพื่อการวิเคราะห์ unknown files และ zero – day threats ได้
- ๔.๒.๒.๖ มีเทคโนโลยีป้องกัน Malware ที่เครื่องแม่ข่ายในรูปแบบ Real-time cloud database online หรือ Live Protection ได้
- ๔.๒.๒.๗ มี Root Cause Analysis หรือ Threat Graph Analysis เพื่อแสดงให้เห็นเส้นทางและการทำงานของภัยคุกคามหรือโปรแกรมที่ต้องสงสัย สำหรับใช้ในการวิเคราะห์เพื่อหาต้นตอสาเหตุ โดยจะแสดงให้เห็นรายละเอียดต่างๆ เช่น จุดกำเนิด (Root Cause), Process, IP Address, URL, Domain, Application ที่เกี่ยวข้อง, File ที่เกี่ยวข้อง และอื่นๆ
- ๔.๒.๒.๘ สามารถทำ Real - time scans เพื่อตรวจสอบการเปลี่ยนแปลงที่เกิดขึ้นได้
- ๔.๒.๒.๙ สร้างนโยบายเพื่อควบคุมการเข้าถึงเว็บไซต์ เช่น Block/Allow/Warning โดยอ้างอิงจาก Category หรือ URL หรือ Web domain ได้
- ๔.๒.๓ มีสิทธิการใช้งาน Next-generation Antivirus ที่ถูกต้องตามกฎหมาย ได้อย่างน้อย ๑๐๐ Licenses สำหรับ Client
- ๔.๒.๓.๑ สามารถติดตั้ง Next-generation Antivirus agent เพื่อทำการป้องกันเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ระบบปฏิบัติการ Microsoft Windows หรือระบบปฏิบัติการ Linux client ที่ยังมีการสนับสนุนอยู่
- ๔.๒.๓.๒ ระบบบริหารจัดการสามารถรองรับการบริหารจัดการผลิตภัณฑ์อื่นๆ นอกเหนือจากโปรแกรมป้องกันไวรัสได้ในอนาคต ภายใต้ brand เดียวกัน ประกอบไปด้วย Mobile Device Management (MDM), Disk Encryption, Next-Generation Firewall, Email Gateway และ Zero Trust Network Access (ZTNA) ได้เป็นอย่างน้อย
- ๔.๒.๓.๓ มีเทคโนโลยีในการป้องกันเทคนิคการโจมตีผ่านช่องโหว่ระบบ (Exploit Prevention) โดยป้องกันจาก Process Hollowing attacks, DLLs loading, Credential Theft, Code cave, APC violation และ Privilege escalation ได้เป็นอย่างน้อย
- ๔.๒.๓.๔ สามารถป้องกันโค้ดที่เป็นอันตราย (ตัวอย่างเช่น PowerShell script) โดยใช้ Microsoft Antimalware Scan Interface (AMSI) ได้

.....นายศิริวิทย์ อัสวฒิมวงศ์ ประธานกรรมการ
..........นายทรงพล ถึงพร้อม กรรมการ
..........นายกฤษฎา แต้มทอง กรรมการ

- ๔.๒.๓.๕ สามารถตรวจจับและกักกันแบบ Real-time
- ๔.๒.๓.๖ สามารถแสดงให้เห็นรายละเอียดของ Command line ที่ถูกสร้างขึ้นจากภัยคุกคามที่เกิดจากการใช้งาน PowerShell หรือ Windows Command Process (CMD) ได้
- ๔.๒.๓.๗ มี Live Protection สำหรับตรวจสอบไฟล์ที่น่าสงสัยโดยเทียบกับฐานข้อมูลของเจ้าของผลิตภัณฑ์ แบบ Real time เพื่อตรวจจับอันตรายล่าสุดและป้องกัน False positives ได้
- ๔.๒.๓.๘ แสดงผลของภัยคุกคามที่เกิดขึ้นออกมาเป็นรูปภาพ Process Tree, Process Table และ Process Activity ได้
- ๔.๒.๓.๙ สามารถทำ Automatic exclusion บนเครื่องคอมพิวเตอร์แม่ข่ายเพื่อยกเว้นการสแกนการทำงานของซอฟต์แวร์โดยอัตโนมัติ เช่น Microsoft Exchange และ Microsoft SQL ได้เป็นอย่างดี
- ๔.๒.๓.๑๐ สามารถบริหารจัดการโปรแกรมป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ที่ไม่สามารถใช้งานอินเทอร์เน็ตได้โดยผ่าน Relays Server หรือ Proxy Server
- ๔.๒.๓.๑๑ สามารถตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ลูกข่ายที่มีสถานะไม่ปลอดภัยออกจากเครือข่ายได้โดยอัตโนมัติ (Auto-Isolation) โดยอนุญาตให้เชื่อมต่อได้เพียงระบบบริหารจัดการของผู้ให้บริการเท่านั้น
- ๔.๒.๓ สามารถสร้างรายงานในรูปแบบของ PDF หรือ CSV ได้
- ๔.๒.๔ ระบบที่ให้บริการต้องมีหน่วยงาน ศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ (Security Operation Center : SOC) เพื่อทำการเฝ้าระวังตลอด ๒๔ ชั่วโมง รวมถึงแจ้งเตือนตาม Escalation Flow ที่กำหนดร่วมกัน
- ๔.๓ จัดหาให้มีระบบตรวจสอบการเข้าถึงอย่างปลอดภัยและการยืนยันตัวตน ๒ ชั้น (Multi-factor Authentication) จำนวนไม่น้อยกว่า ๒๐ ผู้ใช้งาน (user) โดยมีคุณลักษณะอย่างน้อยดังต่อไปนี้**
- ๔.๓.๑ เป็นระบบตรวจสอบการเข้าถึงอย่างปลอดภัยที่ทำงานอยู่บน Cloud สำหรับตรวจสอบและยืนยันตัวตนหลายขั้นตอนการพิสูจน์ ตัวจริงด้วยปัจจัยหลายอย่าง (Multi-Factor Authentication: MFA) สำหรับเครื่องแม่ข่าย (Server) ได้ไม่น้อยกว่า ๒๐ ผู้ใช้งาน (user)
- ๔.๓.๒ ระบบบริหารจัดการข้อมูล Log File แบบศูนย์กลาง (centralized management) ของระบบการพิสูจน์ตัวจริงด้วยปัจจัยหลายอย่าง (Multi-factor) ต้องอยู่บน Cloud base ทั้งภายในประเทศหรือภายนอกประเทศ
- ๔.๓.๓ ระบบบริหารจัดการข้อมูล Log File แบบศูนย์กลาง (centralized management) จะรองรับการเข้าถึงแบบเข้ารหัส HTTPS เท่านั้น
- ๔.๓.๔ ระบบสามารถส่งข้อความแจ้งเตือนและขอการยืนยัน Push notification บนอุปกรณ์ที่ใช้ระบบปฏิบัติการ iOS และ Android ได้เป็นอย่างดี
- ๔.๓.๕ ระบบสามารถส่งข้อความแจ้งเตือน และขอการยืนยัน Push Message พร้อมตัวเลขเพื่อให้ผู้ใช้งานทำการยืนยันการแจ้งเตือน (Verified Push) ได้เป็นอย่างดี
- ๔.๓.๖ ระบบสามารถส่งรหัสยืนยัน (Security keys หรือ OTP) ผ่านไปทาง Mobile Application

.....นายศิริวิทย์ อัสวดีวงศ์ ประธานกรรมการ

.....นายทรงพล ถึงพร้อม กรรมการ

.....นายกฤษฎา แต้มทอง กรรมการ

- ๔.๓.๗ ระบบสามารถตรวจสอบอุปกรณ์ที่ใช้ในการเข้าถึงว่าเป็นอุปกรณ์ที่องค์กรสามารถบริหารจัดการได้ (Trusted Endpoints)
- ๔.๓.๘ ระบบสามารถให้ผู้ใช้งานทำการลงทะเบียนอุปกรณ์เพื่อเข้าใช้งานได้ด้วยตัวเอง (Self-enrollment) และบริหารจัดการตัวเอง (Self-management) ได้เป็นอย่างดี
- ๔.๓.๙ ระบบสามารถตรวจสอบ และระบุความเสี่ยงของอุปกรณ์ (Risk-Based Authentication) ที่ใช้ในการเข้าถึงได้
- ๔.๓.๑๐ ระบบสามารถตรวจสอบการโจมตีตามรูปแบบการใช้งานของผู้ใช้ (machine learning-based) เพื่อวิเคราะห์ (Threat Detection/Trust Monitor) การเข้าถึงที่ผิดปกติ
- ๔.๓.๑๑ ระบบสามารถกำหนดนโยบายการเข้าถึงตาม Location หรือระบบเครือข่ายได้
- ๔.๓.๑๒ ระบบสามารถป้องกันเครื่องที่มาจากเครือข่าย Tor และ Anonymous ได้
- ๔.๓.๑๓ ระบบสามารถควบคุมการเข้าถึงแอปพลิเคชันตาม Device health และ Security Posture ได้
- ๔.๓.๑๔ ระบบสามารถแจ้งเตือนผู้ใช้งานให้อัพเดทอุปกรณ์ของตนเองแบบอัตโนมัติได้
- ๔.๓.๑๕ ระบบสามารถยืนยันตัวตนแบบ Single Sign-On (SSO) สำหรับ On-premise Application, Native Cloud Application, Federated Cloud Application ผ่าน SAML ๒.๐ ได้
- ๔.๓.๑๖ ระบบสามารถจัดทำ Authentication Policy ตาม Application รวมถึงสามารถจัดทำ Authentication Policy ตาม User Group ได้เป็นอย่างดี
- ๔.๓.๑๗ ระบบสามารถตรวจสอบ Device Health ระดับ Operating system (OS) ที่ทำการ Authentication ได้
- ๔.๓.๑๘ ระบบสามารถติดตั้ง agent เพื่อทำการป้องกันเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ระบบปฏิบัติการดังต่อไปนี้
- ๔.๓.๑๘.๑ Windows ๑๐, ๑๑
 - ๔.๓.๑๘.๒ Windows Server ๒๐๑๖ (as of v๒.๑.๐)
 - ๔.๓.๑๘.๓ Windows Server ๒๐๑๙ (as of v๔.๐.๐)
 - ๔.๓.๑๘.๔ Windows Server ๒๐๒๒ (as of v๔.๒.๐)
- ๔.๓.๑๙ ระบบสามารถใช้งานร่วมกับผลิตภัณฑ์ด้านระบบเครือข่ายหรือด้านระบบ (System) ดังนี้
- ๔.๓.๑๙.๑ LDAP, RADIUS, Windows Remote Desktop
 - ๔.๓.๑๙.๒ Sophos Firewall
 - ๔.๓.๑๙.๓ Cisco
 - ๔.๓.๑๙.๔ Akamai
 - ๔.๓.๑๙.๕ Juniper
 - ๔.๓.๑๙.๖ F๕
 - ๔.๓.๑๙.๗ NetScaler
 - ๔.๓.๑๙.๘ VMware, Nutanix, Microsoft, Oracle
- ๔.๓.๒๐ ระบบสามารถแสดงผลรายชื่อที่มีการลงชื่อเข้าใช้(Login) ผ่านระบบแผงควบคุม (Dashboard) ได้

.....นายศิริวิทย์ อัสวดีวงศ์ ประธานกรรมการ

.....นายทรงพล ถึงพร้อม กรรมการ

.....นายกฤษฎา แต้มทอง กรรมการ

- ๔.๓.๒๑ ระบบสามารถแสดงผลจำนวนการ ยืนยันตัวตนทางอิเล็กทรอนิกส์ (Authentication) แบบการพิสูจน์ตัวตนจริงด้วยปัจจัยหลายอย่าง (multi-factor) ผ่านแผงควบคุม (Dashboard) ได้
- ๔.๓.๒๒ ระบบสามารถแสดงผลจำนวนรายชื่อที่มีการ Bypass การใช้งานแบบการพิสูจน์ตัวตนจริงด้วยปัจจัยหลายอย่าง (multi-factor) ได้
- ๔.๓.๒๓ ระบบสามารถแสดงผลเหตุการณ์ (Event) การลงชื่อเข้าใช้ (Login) ที่ผิดปกติได้

๔.๔. จัดหาให้มีและตั้งค่าระบบป้องกันการโจมตีเว็บไซต์และแอปพลิเคชัน (Web Application Firewall: WAF) จากการโจมตีในระดับเครือข่าย จำนวน ๑ โดเมน โดยครอบคลุมระบบสารสนเทศที่ให้บริการในรูปแบบเว็บไซต์ให้สามารถใช้งานได้โดยระบบต้องมีคุณลักษณะอย่างน้อยดังต่อไปนี้

- ๔.๔.๑ ความสามารถในการป้องกันการโจมตีประเภท DDoS (DDoS Protections)
- ๔.๔.๑.๑ สามารถป้องกันการโจมตีจากในระดับเครือข่าย (DDoS attack) ที่ระดับ Network Layer ๓ Layer ๔ และ Layer ๗
- ๔.๔.๑.๒ ผู้ให้เช่าหรือผู้ยื่นข้อเสนอต้องให้บริการป้องกันการโจมตีในระดับเครือข่าย (DDoS attack) แบบไม่จำกัดจำนวนครั้ง และขนาดของการโจมตี โดยไม่มีค่าใช้จ่ายเพิ่มเติม (Unlimited DDOS protection)
- ๔.๔.๑.๓ ผู้ให้เช่าหรือผู้ยื่นข้อเสนอต้องมีเครือข่ายที่มีความสามารถในการป้องกันการโจมตีจากในระดับเครือข่าย (DDoS) ขนาด ๓๔๘ Tbps. เป็นอย่างน้อย
- ๔.๔.๑.๔ ผู้ให้เช่าหรือผู้ยื่นข้อเสนอต้องมี Point of Presence (PoP) อย่างน้อย ๓๓๕ จุดทั่วโลก และ POP อย่างน้อย ๙ จุดในไทยที่มีการเชื่อมต่อกับโครงข่ายอินเทอร์เน็ตระหว่างประเทศ (International Internet Gateway: IIG) ในประเทศไทย ซึ่งแต่ละ POP ต้องมีความสามารถ DDoS mitigation, WAF และ CDN ได้
- ๔.๔.๑.๕ เป็นผลิตภัณฑ์ที่ถูกจัดอยู่ในกลุ่ม Leader ของ The Forester Wave ในหัวข้อของ DDoS Mitigation Solution ปี ๒๐๒๑ หรือ ปีล่าสุด
- ๔.๔.๒ ความสามารถในการป้องกันเว็บแอปพลิเคชัน (Web Security Functions)
- ๔.๔.๒.๑ สามารถแสดงรายงานบน Security Dashboard แบบ Real-time หรือ Near Real-time โดยสามารถแสดงถึงข้อมูลแหล่งที่มาของการโจมตี เช่น IP Addresses, User Agents, Countries และ ASNs ได้ไม่น้อยกว่า ๓๐ วัน
- ๔.๔.๒.๒ สามารถป้องกันการโจมตีผ่านทาง Website ตาม OWASP TOP ๑๐ เช่น SQL injection, Broken Authentication, Cross-site Scripting ได้
- ๔.๔.๒.๓ สามารถตั้งค่า IP Firewall โดยสามารถกำหนดเงื่อนไขด้วย IP address, IP address range, Autonomous System Number (ASN) or country ได้
- ๔.๔.๒.๔ สามารถตั้งค่า Rate Limit Rules ซึ่งสามารถกำหนดการป้องกันการเข้าถึง Website ได้ไม่น้อยกว่า ๑๐๐ Rules
- ๔.๔.๒.๕ สามารถทำการตรวจสอบการออกใบรับรอง(Certificate transparency monitoring) SSL โดยสามารถแจ้งเตือนเมื่อมีผู้ทำการออกใบรับรองภายใต้ชื่อโดเมนเดียวกัน

.....นายศิริวิทย์ อัสวดีวงศ์ ประธานกรรมการ

.....นายทรงพล ถึงพร้อม กรรมการ

.....นายฤทธิญา แท้มทอง กรรมการ

๔.๔.๓ ความสามารถในการเพิ่มประสิทธิภาพเว็บแอปพลิเคชัน (CDN & Optimization function)

๔.๔.๓.๑ ผู้ให้เช่าหรือผู้ยื่นข้อเสนอต้องให้บริการ authoritative DNS services สำหรับโดเมนสาธารณะ และผู้ยื่นข้อเสนอต้องมี Host Domains ทุกภูมิภาคทั่วโลก โดยต้องมี Node หลายจุดในแต่ละพื้นที่โดยเฉพาะในประเทศไทย ไม่น้อยกว่า ๙ จุด

๔.๔.๓.๒ มีระบบ Content Caching โดยสามารถทำ Static Content Caching และสามารถกำหนด Cache ในระดับ File Type ได้

๔.๔.๓.๓ สามารถทำการ Purge Cache ทั้งหมดได้ในทันที หรือทำการ Custom Purge เฉพาะ URL, Host name และ Tag ได้ โดยต้องสามารถใช้ API ในการอัปเดต Cache เมื่อมีการอัปเดต Content ได้

๔.๔.๓.๔ บริการต้องสามารถรองรับการใช้ Bandwidth Consumption ได้ไม่น้อยกว่า ๑ TB ต่อเดือน

๔.๔.๓.๕ สามารถลดขนาด บีบอัด และทำการลบ Metadata ของไฟล์ โดยสามารถเลือกได้ทั้งแบบ Lossless และ Lossy รวมถึงรองรับ WebP

๔.๔.๓.๖ สามารถทำการลบตัวอักษรที่ไม่จำเป็นใน Source code เช่น Whitespace และ Comments เพื่อช่วยเพิ่มประสิทธิภาพให้กับ Page load time

๔.๔.๓.๗ มีระบบที่ช่วยเพิ่มประสิทธิภาพและลด Latency ให้กับ Dynamic Content โดยสามารถดูเปอร์เซ็นต์ประสิทธิภาพที่เพิ่มขึ้น และ Response time ได้ผ่านทางแผงควบคุม (Dashboard)

๔.๔.๔ ความสามารถในการเพิ่มเสถียรภาพ (Web Reliability)

๔.๔.๔.๑ สามารถแสดงการแจ้งเตือนไปยัง Email ที่ระบุไว้ได้ ในกรณีที่เว็บไซต์ไม่สามารถใช้งานได้ โดยสามารถรองรับการตั้งค่าในการ Monitor ได้ในระดับ Type, Method, Port และ Path รวมถึงสามารถระบุ Expected codes ที่ต้องการได้

๔.๔.๕ ความสามารถในการแสดงรายงาน (Dashboard Functions)

๔.๔.๕.๑ สามารถแสดงรายงาน (Analytic) บน Dashboard แบบ Real-time หรือ Near Real-time โดย Dashboard ที่แสดงต้องประกอบด้วยข้อมูล Total Requests, Cached Request, Bandwidth Saved, Threat Sources, Top Threat Origin และ Top Traffic Origin ได้อย่างน้อย ๓๐ วัน

๔.๔.๕.๒ บริการที่เสนอรองรับการส่ง Raw Log ผ่านทาง Log pull REST API และสามารถเรียกดู Firewall Event Log และ Audit Log ได้ผ่านทาง Portal ที่ใช้งาน

๔.๕ จัดหาให้มีระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log management) คุณลักษณะอย่างน้อยดังต่อไปนี้

๔.๕.๑ สามารถจัดเก็บรวบรวมข้อมูล (Data Collection) แบบไม่จำกัดจำนวนอุปกรณ์ จากแหล่งต่างๆ เช่น ข้อมูล Log Server, Windows, Linux, Proxy Server, Active Directory Server, File Server, Mail Server, Web Service, Firewall, Router เพื่อทำการบันทึกข้อมูล และนำไปวิเคราะห์หาจุดอ่อนภายใน ได้ไม่น้อยกว่า ๙๐ วัน

.....นายศิริวิทย์ อัสวฒินวงศ์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายกฤษฎา แต้มทอง กรรมการ

- ๔.๕.๒ มีระบบ File Integrity ด้วย Algorithm แบบ SHA-๒๕๖ เป็นอย่างน้อย เพื่อยืนยันว่าข้อมูลที่ได้ถูกเก็บบันทึกไม่มีการถูกแก้ไขหรือเปลี่ยนแปลงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์
- ๔.๕.๓ สามารถเชื่อมโยงเหตุการณ์ (Correlation) และจัดจำรูปแบบเหตุการณ์ (Pattern recognition) หรือเทคโนโลยีเทียบเท่าจาก Log Source ต่าง ๆ เข้าด้วยกัน โดยมี Predefined rules มาพร้อมกับระบบ และสามารถ Customize เพิ่มเติมได้
- ๔.๕.๔ สามารถแสดงค่าเฉลี่ยของการรับ Log (Average EPS) และแสดงจำนวน Log ที่รับสูงสุด (Peak EPS) ในแบบรายวัน รายสัปดาห์ และรายเดือนได้
- ๔.๕.๕ จัดเตรียมและพัฒนาระบบ Dashboard เพื่อใช้สำหรับวิเคราะห์ Log แบบ Real-time ในรูปแบบของแผนภูมิ (Chart) และ สามารถ Customize เพิ่มเติมได้โดยแสดงข้อมูลย้อนหลังอย่างน้อย ๓๐ วัน และสามารถปรับเปลี่ยนมุมมองการแสดงผลได้โดยไม่ต้องจำกัดจำนวนครั้งและไม่มีค่าใช้จ่ายเพิ่ม
- ๔.๕.๖ สามารถร้องขอให้ผู้ให้บริการค้นหาหรือนำข้อมูลจราจรทางคอมพิวเตอร์มาใช้เป็นพยานหลักฐานในการดำเนินคดีกับผู้กระทำความผิด ตามที่ “พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐” ได้ตามคำร้องขอของผู้ใช้บริการ
- ๔.๕.๗ รองรับการทํางานแบบ HTTPS ที่มีความปลอดภัย
- ๔.๕.๘ ได้ผ่านการตรวจตามมาตรฐาน มคอ. ๔๐๐๓๑-๒๕๖๐ มาตรฐานศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เล่ม ๑ หรือได้ผ่านการรับรองมาตรฐาน FIPS ๑๔๐-๒ เป็นอย่างน้อย
- ๔.๕.๙ สนับสนุนการให้บริการแบบตลอด ๒๔ ชั่วโมง กรณีผู้ให้บริการไม่ได้รับข้อมูลจราจรจะทำการแจ้งเตือนไปยังผู้ดูแลระบบจัดเก็บ Log ผ่านทางอีเมล หรือทางโทรศัพท์
- ๔.๖ จัดหาให้มีระบบบริหารเหตุการณ์และข้อมูลการรักษาความมั่นคงปลอดภัย (Security Information and Event Management: SIEM) คุณลักษณะอย่างน้อยดังต่อไปนี้**
- ๔.๖.๑ ผู้ยื่นข้อเสนอจะต้องรองรับและวิเคราะห์ข้อมูลได้ไม่น้อยกว่า ๑๕,๐๐๐ เหตุการณ์ต่อวินาที (Events per Second) และรองรับการเพิ่มขยายได้ในอนาคต
- ๔.๖.๒ ผู้ยื่นข้อเสนอจะต้องสามารถให้บริการได้อย่างต่อเนื่อง โดยโครงสร้างระบบที่ให้บริการนั้นจะต้องถูกติดตั้งในรูปแบบ High Availability หรือดีกว่า
- ๔.๖.๓ ผู้ยื่นข้อเสนอต้องสามารถรับ Log จาก Log source ได้ในรูปแบบ SysLog (TCP, UDP), SNMP, JDBC, WMI และ NetFlow ได้เป็นอย่างน้อย
- ๔.๖.๔ ผู้ยื่นข้อเสนอต้องสามารถรับเหตุการณ์จากอุปกรณ์เครือข่ายได้ไม่น้อยกว่า ๑๐๐ อุปกรณ์ ได้เป็นอย่างน้อย
- ๔.๖.๕ ระบบที่เสนอต้องมีพีเจียร์หรือฟังก์ชัน Threat Intelligence ภายใต้เครื่องหมายการค้าเดียวกันกับระบบ SIEM
- ๔.๖.๖ ระบบฐานข้อมูลเกี่ยวกับภัยคุกคาม (Threat Intelligence) ที่มาพร้อมระบบ SIEM ต้องสามารถตรวจสอบความเสี่ยงจาก IP, file, Application และ MD๕ ได้เป็นอย่างน้อย

.....นายศิริวิทย์ อัสวพัฒน์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายภุชญา แต้มทอง กรรมการ

๔.๖.๗ สามารถวิเคราะห์พฤติกรรมผู้ใช้ User behavior analytics (UBA) ได้ไม่น้อยกว่า ๔๐,๐๐๐ ผู้ใช้ และสามารถเพิ่มหน่วยความจำหรือหน่วยประมวลผลหรืออุปกรณ์อื่น ๆ เพื่อให้รองรับผู้ใช้งานได้สูงสุด ๒๒๐,๐๐๐ ผู้ใช้งาน

๔.๖.๘ ผู้ยื่นข้อเสนอต้องสามารถรับข้อมูลผ่าน Logs, Performance metrics, SNMP Traps, Security Alerts และ Configuration Change ได้ เพื่อสามารถวิเคราะห์ข้อมูลได้ทั้งในรูปแบบ NOC (Network Operation Center) และ SOC (Security Operation Center) ได้

๔.๖.๙ ต้องสามารถส่งข้อมูลเป็น IOC (Indicator of Compromise) มายังส่วนกลางได้

๔.๖.๑๐ ผู้ยื่นข้อเสนอต้องสามารถแจ้งเตือนเมื่อมีเหตุการณ์ตรงตามเงื่อนไข (Correlation Rules) ที่สร้างไว้ และเหตุการณ์ผิดปกติของตัวอุปกรณ์ผ่าน Email ได้เป็นอย่างน้อย

๔.๖.๑๑ ผู้ยื่นข้อเสนอต้องจัดเก็บ on-line log file เป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน และทำการจัดเก็บ off-line log เป็นระยะเวลา ๑ ปี รวมทั้งรองรับการนำ off-line log ไม่น้อยกว่า ๑ ปี มาค้นหาข้อมูลย้อนหลัง

๔.๗ จัดหาให้มีการตรวจสอบช่องโหว่ในระดับระบบปฏิบัติการ (Vulnerability Assessment) จำนวนอย่างน้อย ๑๕ IP Address คุณลักษณะอย่างน้อยดังต่อไปนี้

๔.๗.๑ ผู้ยื่นข้อเสนอจะต้องเข้าดำเนินการตรวจสอบเพื่อหาจุดที่เป็นช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์ และสารสนเทศ เพื่อจะได้หาแนวทางในการป้องกันก่อนที่จะเกิดเหตุ จำนวน ๑ รอบ โดยการดำเนินการ ๑ รอบนั้น จะดำเนินการตรวจสอบหาช่องโหว่ ๑ ครั้ง เพื่อตรวจสอบหาช่องโหว่ที่เกิดขึ้นกับระบบ และอีก ๑ ครั้ง หลังจากดำเนินการแก้ไขช่องโหว่ที่เกิดขึ้นเรียบร้อยแล้ว

๔.๗.๑.๑ บริการที่นำเสนอต้องใช้งานโปรแกรมที่มีลิขสิทธิ์ถูกกฎหมาย และอยู่ใน The ForesterWave

๔.๗.๑.๒ สามารถตรวจสอบช่องโหว่ของอุปกรณ์บนระบบเครือข่ายได้ทั้งเครือข่ายสาธารณะ (Public) และเครือข่ายภายใน (Private)

๔.๗.๑.๓ สามารถรองรับการตรวจสอบช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่ายที่มีระบบปฏิบัติการอย่างน้อยต่อไปนี้

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

๔.๗.๑.๔ รองรับการ scan ทั้งแบบ Non Credential Scan และ Credential Scan ได้

๔.๗.๑.๕ สามารถสร้างรายงานได้หลายรูปแบบ เช่น Executive Summary หรือแบบแยกตาม Host หรือ Plugin

๔.๗.๑.๖ รายงานจะต้องมีการอ้างอิงกับ CVSS และ CVE และมีการระบุ Severity ของช่องโหว่ที่พบในการตรวจสอบ

.....นายศิริวิทย์ อัสวีตวิวงศ์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายกฤษฎา แต้มทอง กรรมการ

๔.๗.๒ บุคคลหรือกลุ่มบุคคลผู้เข้าดำเนินการตรวจสอบช่องโหว่จะต้องมีความรู้ความสามารถ ในด้านการวิเคราะห์ ตรวจสอบหาจุดที่เป็นช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์ และสารสนเทศ ที่จะเป็นภัยคุกคามต่อหน่วยงาน รวมถึงให้คำแนะนำในการตรวจสอบแก้ไขปัญหาที่พบ โดยบุคคลหรือกลุ่มบุคคลผู้เข้าดำเนินการจะต้องได้รับใบรับรองความรู้ความสามารถ อย่างใดอย่างหนึ่งเป็นอย่างน้อย ดังนี้

๔.๗.๒.๑ CEH (Certified Ethical Hacker)

๔.๗.๒.๒ ISACA Certified Information Security Manager (CISM)

๔.๗.๒.๓ SACA Certified Information Systems Auditor (CISA)

๔.๗.๒.๔ (ISC)๒ CC – Certified in Cybersecurity

๔.๗.๒.๕ CompTIA CySA+

๔.๗.๒.๖ CompTIA Pentest+

๔.๗.๓ ผู้ยื่นข้อเสนอจะต้องจัดทำรายงานผลการวิเคราะห์ และตรวจสอบช่องโหว่ โดยต้องระบุรายละเอียดช่องโหว่ที่ตรวจสอบพบบนอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ และสารสนเทศ ที่จะเป็นภัยคุกคามต่อหน่วยงาน รวมถึงระบุแนวทางการแก้ไขช่องโหว่ที่ตรวจสอบพบ ซึ่งจะต้องประกอบด้วย

๔.๗.๓.๑ รายงานสรุปภาพรวมของการตรวจสอบ

๔.๗.๓.๒ ระบุการจัดระดับความรุนแรง (Severity) หรือผลกระทบที่อาจจะเกิดจากช่องโหว่ที่พบ

๔.๗.๓.๓ รายละเอียดช่องโหว่ที่ตรวจสอบพบของแต่ละอุปกรณ์ โดยจัดเรียงตามระดับความรุนแรงหรือผลกระทบที่อาจจะเกิดจากช่องโหว่ดังกล่าว

๔.๗.๓.๔ คำแนะนำและขั้นตอนในการแก้ไข (Action & Recommendation)

๔.๘ จัดหาให้มีการดำเนินการทดสอบเจาะระบบ (Penetration Testing) จำนวนอย่างน้อย ๑ ระบบ จำนวน ๑ ครั้ง มีคุณลักษณะดังต่อไปนี้

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

๔.๘.๒ ดำเนินการทดสอบบุกรุกระบบสารสนเทศ (เว็บไซต์, แอปพลิเคชัน) ของโรงพยาบาล

๔.๘.๓ วิเคราะห์และรายงานผลการทดสอบพร้อมคำแนะนำในการปรับปรุงและระบบความปลอดภัยคอมพิวเตอร์

๔.๘.๔ ดำเนินการค้นหาช่องโหว่ประเมินหาจุดอ่อนประเมินความเสี่ยงและผลกระทบพร้อมข้อเสนอแนะแนวทางแก้ไขระบบสารสนเทศและระบบที่เกี่ยวข้องโดยครอบคลุมรายละเอียดดังนี้

๔.๘.๔.๑ การดำเนินการจะต้องครอบคลุมในระดับ

- แอปพลิเคชัน (Application) และ ซอฟต์แวร์ (Software) ได้แก่
 - เว็บแอปพลิเคชัน (Web Application)
 - โมบายแอปพลิเคชัน (Mobile Application)

.....	นายศิริวิทย์ อัสวีวัฒน์	ประธานกรรมการ
.....	นายทรงพล ถึงพร้อม	กรรมการ
.....	นายภานุญา แต่มทอง	กรรมการ

- โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT Infrastructure) และ อุปกรณ์เครือข่าย (Network Device) ได้แก่
 - ระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย (Server Operating Systems)
 - อุปกรณ์ในระบบเครือข่าย(Network Equipment)
 - อุปกรณ์ระบบรักษาความปลอดภัย (Security Equipment)

๔.๘.๔.๒ สำหรับ เว็บแอปพลิเคชัน(Web Application) จะใช้มาตรฐาน Open Web Application Security Testing Guide version ๔.๒ 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

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

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

๔.๘.๔.๔ สำหรับโมบายแอปพลิเคชัน จะใช้มาตรฐาน OWASP Mobile Application Security Testing Guide (MASTG) version ๑.๕ ประกอบด้วยหัวข้อดังนี้

- Platform Overview
- Basic Security Testing
- Tampering and Reverse Engineering
- Data Storage
- Cryptographic APIs
- Local Authentication

	นายศิริวิทย์ อัสวพัฒน์	ประธานกรรมการ
	นายทรงพล ถึงพร้อม	กรรมการ
	นายกฤษฎา แต้มทอง	กรรมการ

- Network Communication
- Platform APIs
- Code Quality and Build Settings
- Anti-Reversing Defenses
- User Privacy Protection

๔.๘.๔.๕ ดำเนินการโดยใช้โปรแกรมหรือซอฟต์แวร์ที่มีความน่าเชื่อถือไม่น้อยกว่า ๒ โปรแกรม ยกตัวอย่างเช่น

- Commercial เช่น Nessus Professional, Burp Suite Professional เป็นต้น
- Non-commercial เช่น Metasploit, Burp Suite Community Edition, Nmap, SQLMap, FFUF, Manual Script, Exploit-DB, SecLists, PayloadAllTheThings, CVE Details เป็นต้น

๔.๙ จัดหาให้มีการดำเนินการวิเคราะห์และให้คำแนะนำในการปรับปรุงเพื่อให้ระบบมีความปลอดภัย

๔.๙.๑ วิเคราะห์และให้คำแนะนำในกรณีที่ระบบเครือข่ายสื่อสารมีความจำเป็นต้องได้รับการติดตั้งระบบหรืออุปกรณ์เพิ่มเติมเพื่อเป็นการเพิ่มระดับการรักษาความปลอดภัยของระบบเครือข่ายและระบบความปลอดภัยคอมพิวเตอร์

๔.๙.๒ จัดทำรายงานผลการวิเคราะห์และให้คำแนะนำในการปรับปรุงความปลอดภัยของระบบเครือข่ายและ ความปลอดภัยคอมพิวเตอร์

๔.๙.๓ รายงานผลการปรับปรุงระบบเครือข่ายและผลการดำเนินการปิดช่องโหว่(Hardening)

๔.๙.๓.๑ ในการทดสอบเจาะระบบจะต้องมีการดำเนินการทั้งหมดไม่น้อยกว่า ๑๐ วัน บุคคลหรือกลุ่มบุคคลผู้เข้าดำเนินการทดสอบเจาะระบบจะต้องมีความรู้ความสามารถ ในด้านการวิเคราะห์ ตรวจสอบหาจุดที่เป็นช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์ และสารสนเทศ ที่จะเป็นภัยคุกคามต่อหน่วยงาน รวมถึงให้คำแนะนำในการตรวจสอบแก้ไขปัญหาที่พบ โดยบุคคลหรือกลุ่มบุคคลผู้เข้าดำเนินการจะต้องได้รับใบรับรองความรู้ความสามารถ อย่างใดอย่างหนึ่งเป็นอย่างน้อยดังนี้

- ๔.๙.๓.๑.๑.๑ CEH (Certified Ethical Hacker)
- ๔.๙.๓.๑.๑.๒ ISACA Certified Information Security Manager (CISM)
- ๔.๙.๓.๑.๑.๓ ISACA Certified Information Systems Auditor (CISA)
- ๔.๙.๓.๑.๑.๔ (ISC)๒ CC – Certified in Cybersecurity
- ๔.๙.๓.๑.๑.๕ CompTIA CySA+
- ๔.๙.๓.๑.๑.๖ CompTIA Pentest+

๔.๑๐ ดำเนินการจัดให้มีการจัดเตรียมทรัพยากรบนระบบเสมือนเพื่อทดสอบการอัปเดตระบบปฏิบัติการ (Operating System Patching) คุณลักษณะอย่างน้อยดังต่อไปนี้

๔.๑๐.๑ จัดเตรียมเครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน (Virtual Server) รวมถึงระบบปฏิบัติการ (OS) สำหรับทดสอบการอัปเดต Patching ใหม่ ๆ จำนวน ๑ เครื่อง โดยมีคุณสมบัติขั้นต่ำดังนี้

.....นายศิริวิทย์ อัสวณิงค์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายกฤษฎา แต้มทอง กรรมการ

- หน่วยประมวลผลกลาง (vCPU) ๒ Cores
 - หน่วยความจำ (Memory) ๔ GB
 - หน่วยบันทึก (Disk) แบบ SATA ขนาดไม่น้อยกว่า ๓๐๐GB และ แบบ SSD ไม่น้อยกว่า ๔ GB
- ๔.๑๐.๒ ต้องจัดเตรียม Bandwidth Internet สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (server) รวมถึงระบบปฏิบัติการ (OS) ในการทดสอบ ๑ Gbps เป็นอย่างน้อย
- ๔.๑๐.๓ ระบบที่ใช้ในการทดสอบจะต้องรองรับการเข้าถึงผ่านทาง Virtual Private Network (VPN) และมีการเข้ารหัสแบบ ๒ ขั้นตอน (Multi-factor Authentication)
- ๔.๑๐.๔ ระบบที่ใช้ในการทดสอบจะต้องรองรับการเข้าถึงแบบ Console ผ่านทางระบบ Web Application
- ๔.๑๐.๕ ระบบที่ใช้ในการทดสอบจะต้องมีระยะเวลาให้ทดสอบไม่น้อยกว่า ๓ เดือน

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

๔.๑๑.๑ ดำเนินด้านเฝ้าระวัง ตรวจสอบการคุกคามทางไซเบอร์

- ๔.๑๑.๑.๑ ต้องมีการวิเคราะห์แบบรวมศูนย์ (Correlation) และสามารถสร้างเงื่อนไขการโจมตี (Rule or Use case) เพื่อช่วยในการเฝ้าระวังและ แจ้งเตือนภัยคุกคามทางไซเบอร์
- ๔.๑๑.๑.๒ ต้องมีระบบการจัดเก็บ Ticket management หากพบเหตุการณ์ความผิดปกติ ด้าน Cyber security

๔.๑๑.๑.๓ ต้องมี Rules ที่ใช้ในการเฝ้าระวัง และสามารถตรวจจับภัยคุกคาม รูปแบบต่าง ๆ

๔.๑๑.๑.๔ ต้องจัดให้มีทีมงานที่มีความรู้ความสามารถในด้านการวิเคราะห์ เฝ้าระวัง และแจ้งเตือนภัยคุกคามด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้คำปรึกษาด้านเทคนิค ตลอดระยะเวลาอายุสัญญา

๔.๑๑.๑.๕ แจ้งเตือนเมื่อตรวจพบภัยคุกคามหรือการบุกรุกระบบเทคโนโลยีสารสนเทศที่มีระดับความรุนแรงสำคัญ (Critical) หรือระดับความรุนแรงสูง (High) ผ่านทางอีเมล หรือโทรศัพท์ ตลอด ๒๔ ชั่วโมง

๔.๑๑.๑.๖ ต้องสามารถจัดทำรายงานตามความต้องการของมาตรฐานความปลอดภัยต่าง ๆ ดังนี้ PCI, SOX, ISO/IEC ๒๗๐๐๑ หรือ ISO/IEC ๒๗๐๐๒, FISMA, HIPAA ได้ เป็นอย่างน้อย

๔.๑๑.๑.๗ ต้องสามารถเลือกช่วงเวลาของข้อมูลดิบ (Raw Data) ที่จะค้นหาได้ ทั้งของช่วงเวลาปัจจุบันและของช่วงเวลาย้อนหลัง โดยระบุช่วงเวลาเริ่มต้นและสิ้นสุด

๔.๑๑.๑.๘ ต้องสามารถทำการจัดเก็บข้อมูลในลักษณะแบบ Online และ Offline(Raw Log) ได้

๔.๑๑.๑.๙ ต้องสามารถให้บริการได้อย่างต่อเนื่อง โดยมีระดับของการให้บริการ (Service Level Agreement) ไม่ต่ำกว่า ๙๙.๙๐% ต่อเดือน

๔.๑๑.๑.๑๐ ผู้ยื่นข้อเสนอต้องปฏิบัติตามเงื่อนไขระดับของบริการ Service Level Agreement (SLA) ดังนี้

.....นายศิริวิทย์ อัสวัฒนวงศ์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายกฤษฎา แต้มทอง กรรมการ

ระดับความรุนแรง	คำอธิบาย	เวลาในการตอบสนอง (Response time)
Critical	ผลกระทบกับระบบสารสนเทศหลักทำให้การดำเนินธุรกิจหยุดชะงักและจะต้องแก้ไขอย่างเร่งด่วนที่สุด	ภายใน ๑๕ นาที
High	ผลกระทบกับระบบสารสนเทศที่ทำให้ธุรกิจไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพ และจำเป็นต้องแก้ไขอย่างเร่งด่วน	ภายใน ๓ ชั่วโมง
Medium	ผลกระทบกับระบบสารสนเทศที่มีผลต่อการดำเนินธุรกิจ และจำเป็นต้องแก้ไขอย่างทันท่วงที	ภายใน ๖ ชั่วโมง
Low	ผลกระทบกับระบบสารสนเทศที่มีผลต่อประสิทธิภาพการทำงานทั่วไป แต่ไม่มีผลกระทบต่อการทำงานโดยรวม	ภายใน ๒๔ ชั่วโมง

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

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

๔.๑๑.๑.๑๒ รายงานสรุปผลการดำเนินงานแบบรายเดือนประกอบด้วย การวิเคราะห์เฝ้าระวังเหตุการณ์ทั้งหมดที่เกิดขึ้น เหตุที่น่าสนใจ และเข้าร่วมประชุมเพื่ออธิบายสรุปผลการดำเนินงาน

๔.๑๑.๒ ต้องมีศูนย์ปฏิบัติการเฝ้าระวังเหตุการณ์ที่เป็นภัยคุกคามระบบเทคโนโลยีสารสนเทศ (SOC) ตั้งอยู่ในประเทศไทย โดยมีเจ้าหน้าที่ประจำปฏิบัติงานในศูนย์ตลอด ๒๔ ชั่วโมง และต้องได้รับการรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ หรือใหม่กว่า เป็นอย่างน้อย

.....นายศิริวิทย์ อัสวดีวงศ์ ประธานกรรมการ
นายทรงพล ถึงพร้อม กรรมการ
นายกฤษฎา แด้มทอง กรรมการ

๕. ระยะเวลาการดำเนินการ

ระยะเวลาของสัญญานับถัดจากวันลงนามในสัญญา และสิ้นสุดสัญญาวันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๘ ดังนี้

๕.๑ ผู้ยื่นข้อเสนอจะต้องส่งมอบระบบและสิทธิ์การใช้งานซอฟต์แวร์ภายใน ๖๐ วัน นับถัดจากวันลงนามในสัญญา

๕.๒ ระยะเวลาการดำเนินของระบบ (Hardware และ Software) ในโครงการจะต้องใช้งานได้อย่างน้อย ๓๖๕ วันนับถัดจากวันที่ส่งมอบระบบ

๕.๓ ระยะเวลาบริการศูนย์เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ (Security Operation Center:SOC) ทั้งสิ้น ๑ ปี นับถัดจากวันที่ส่งมอบ

๖. การส่งมอบงานและการชำระเงิน

ผู้ยื่นข้อเสนอจะต้องปฏิบัติงานและรายงานผลการให้บริการตามสัญญาพร้อมส่งมอบงานในแต่ละงวดเป็นเอกสาร จำนวน ๒ ชุด พร้อมไฟล์อิเล็กทรอนิกส์ในรูปแบบที่ปรับแก้ไขได้ (MSOffice) และปรับแก้ไขไม่ได้ (PDF) พร้อมบันทึกลงใน USB flash drive หรือสื่อแบบถอดได้อื่น ๆ (Removable) หรือแผ่นซีดี (CD) จำนวน ๒ ชุด รวมถึงเอกสารหลักฐานต่างๆ ที่เกี่ยวข้องครบถ้วน และผ่านการตรวจรับงานจ้างจากคณะกรรมการตรวจรับงานจ้างเรียบร้อยแล้ว ผู้เช่าตกลงชำระค่าจ้างดำเนินการโครงการให้แก่ผู้ยื่นข้อเสนอเป็นเช็คขีดคร่อมหรือการโอนเงินทางอิเล็กทรอนิกส์ โดย ผู้เช่าจะหักภาษีค่าธรรมเนียมนานาการและค่าธรรมเนียมอื่นๆ ที่เกี่ยวข้องจากมูลค่าของค่าจ้างซึ่งผู้ยื่นข้อเสนอ จะต้องชำระไว้ตามกฎหมายด้วยแบ่งเป็นงวดการส่งมอบงานและงวดการจ่ายเงินดังนี้

๖.๑ ส่งมอบภายใน ๑๕ วันนับถัดจากวันลงนามในสัญญา ประกอบด้วย

๖.๑.๑ ตัวอย่างรายงานการปฏิบัติการให้บริการระบบในการป้องกัน ตรวจจับ วิเคราะห์และโต้ตอบภัยคุกคามไซเบอร์

๖.๑.๒ ตารางแผนกิจกรรมการดำเนินงานและการเข้าปฏิบัติงานในโรงพยาบาลตลอดระยะเวลาสัญญา

๖.๑.๓ รายชื่อเจ้าหน้าที่ของผู้ยื่นข้อเสนอ พร้อมข้อมูลสำหรับการติดต่อประสานงาน และการเข้าพื้นที่โรงพยาบาลเพื่อติดตั้งระบบ และให้บริการระบบต่างๆ

๖.๒ ติดตั้งอุปกรณ์ ซอฟต์แวร์ และดำเนินการให้ครบตามที่กำหนดไว้ในข้อ ๔ คุณลักษณะเฉพาะทางเทคนิคและสิ่งส่งมอบ ให้แล้วเสร็จภายใน ๖๐ วันนับถัดจากวันลงนามในสัญญา

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

๖.๒.๒ ระบบป้องกันตรวจจับและโต้ตอบภัยคุกคาม Endpoint Detection & Response (EDR) จำนวน ๑ ระบบ พร้อมคู่มือการใช้งานระบบ

๖.๒.๓ ระบบตรวจสอบการเข้าถึงอย่างปลอดภัยและการยืนยันตัวตน ๒ ชั้น (Multi-factor Authentication) จำนวนไม่น้อยกว่า ๒๐ ผู้ใช้งาน (user) พร้อมคู่มือการใช้งานระบบ

๖.๒.๔ ระบบป้องกันการโจมตีเว็บไซต์และแอปพลิเคชัน (Web Application Firewall: WAF) จากการโจมตีในระดับเครือข่าย จำนวน ๑ โดเมน โดยครอบคลุมระบบสารสนเทศที่ให้บริการในรูปแบบเว็บไซต์ให้สามารถใช้งานได้ พร้อมคู่มือการใช้งานระบบ

๖.๒.๕ ระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log management) พร้อมคู่มือการใช้งานระบบ (ถ้ามี)

.....นายศิริวิทย์ อัสวัฒน์วงศ์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายภฤชญา แด้มทอง กรรมการ

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

๖.๒.๗ ผลการตรวจสอบช่องโหว่ในระดับระบบปฏิบัติการ (Vulnerability Assessment)

๖.๒.๘ ผลดำเนินการทดสอบเจาะระบบ (Penetration Testing)

๖.๒.๙ ผลการวิเคราะห์และให้คำแนะนำในการปรับปรุงเพื่อให้ระบบมีความปลอดภัย

๖.๒.๑๐ ผลดำเนินการจัดให้มีการจัดเตรียมทรัพยากรบนระบบเสมือนเพื่อทดสอบการอัปเดตระบบปฏิบัติการ (Operating System Patching)

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

๖.๒.๑๒ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๖.๒.๑๓ คู่มือการตอบรับเหตุการณ์ (Incident Response Playbook) ตามประเภทของภัยคุกคามเพื่อใช้อ้างอิงในการปฏิบัติการในการจัดการหรือตอบรับภัยคุกคามต่าง ๆ ได้อย่างถูกต้องให้กับโรงพยาบาล

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

๖.๒.๑๕ รายงานผลการฝึกอบรมการใช้งานระบบต่างๆ ให้แก่เจ้าหน้าที่โรงพยาบาล

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

๖.๒.๑๗ รายงานผลการให้บริการระบบในการป้องกัน ตรวจสอบ วิเคราะห์และโต้ตอบต่อภัยคุกคามไซเบอร์ของเดือน และข้อมูลสะสมภาพรวม ทุกสิ้นเดือน

๖.๒.๑๘ รายงานสรุปเหตุภัยคุกคามทางไซเบอร์ และการแก้ไขปัญหาที่เกิดขึ้น ของเดือน และข้อมูลสะสมภาพรวม ทุกสิ้นเดือน

๖.๒.๑๙ รายงานการตรวจสอบและติดตามผลการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ ของเดือน และข้อมูลสะสมภาพรวม ทุกสิ้นเดือน

๖.๒.๒๐ รายงานผลการได้สิทธิ์ใช้งาน Next-generation Antivirus ที่ถูกต้องตามกฎหมาย ได้อย่างน้อย ๑๐๐ Licenses สำหรับ Client

๖.๓ ชำระเงินเป็นรายงวดจำนวน ๑ งวด นับถัดจากวันที่ส่งมอบงานตามข้อ ๖.๒ และให้บริการระบบในการป้องกัน ตรวจสอบ วิเคราะห์และโต้ตอบต่อภัยคุกคามไซเบอร์เป็นระยะเวลาครบ ๑ เดือน

๗. หลักเกณฑ์การพิจารณาข้อเสนอ

๗.๑ การพิจารณาผลการยื่นข้อเสนอการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ โรงพยาบาลจะพิจารณาตัดสินโดยใช้เกณฑ์ราคา

.....นายศิริวิทย์ อัสวดีวงศ์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายกฤษฎา แต้มทอง กรรมการ

๗.๒ ผู้ยื่นข้อเสนอจะต้องเสนอแผนการดำเนินงานของกิจกรรมฯ ตามขอบเขตของงานข้อ ๔ และจัดทำเอกสารเปรียบเทียบระหว่างข้อกำหนดรายละเอียดคุณลักษณะเฉพาะกับแนวทางหรือแผนการดำเนินงาน กิจกรรมของผู้ยื่นข้อเสนอมาเพื่อประกอบการพิจารณา โดยต้องระบุเลขหน้า เลขข้อ กำกับให้ชัดเจน สะดวกในการเทียบเคียง มิฉะนั้นจะไม่ได้รับการพิจารณา

๗.๓ ในการตัดสินใจการประกวดราคาอิเล็กทรอนิกส์หรือในการทำสัญญา คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์มีสิทธิให้ผู้ยื่นข้อเสนอชี้แจงข้อเท็จจริง สภาพฐานะ หรือข้อเท็จจริงอื่นใดที่เกี่ยวข้องกับผู้ยื่นข้อเสนอได้ โดยผู้เข้ามีสิทธิที่จะไม่รับข้อเสนอ ไม่รับราคาหรือไม่ทำสัญญา หากหลักฐานดังกล่าวไม่มีความเหมาะสมหรือไม่ถูกต้อง

๗.๔ ในกรณีที่ปรากฏข้อเท็จจริงภายหลังจากการพิจารณาข้อเสนอว่า ผู้ยื่นข้อเสนอที่มีสิทธิได้รับการคัดเลือกเป็นผู้ยื่นข้อเสนอที่มีผลประโยชน์ร่วมกันกับผู้ยื่นเสนอรายอื่น ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือเป็นผู้ยื่นข้อเสนอที่กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ผู้เข้ามีอำนาจที่จะตัดรายชื่อผู้ยื่นข้อเสนอที่ได้รับคัดเลือกรายดังกล่าวออกและยกเลิกผลการพิจารณาและแจ้งกรมบัญชีกลางดำเนินการต่อไป

๗.๕ ผลการพิจารณาให้ถือการตัดสินใจของคณะกรรมการเป็นสำคัญผู้ใดจะนำไปเป็นเหตุกล่าวอ้างเพื่อเรียกร้องค่าเสียหายต่อโรงพยาบาลภายหลังไม่ได้

๘. ค่าปรับ

๘.๑ ค่าปรับการส่งมอบงานล่าช้า

หากผู้ยื่นข้อเสนอไม่สามารถส่งมอบงานได้ตามเวลาที่ กำหนดไว้ในสัญญาและผู้ว่าจ้างยังมิได้บอกเลิกสัญญา ผู้ยื่นข้อเสนอจะต้องชำระค่าปรับให้แก่โรงพยาบาล เป็นรายวันในอัตราร้อยละ ๐.๒๐ (ศูนย์จุดสองศูนย์) ของราคาค่าเช่าตามสัญญา กรณีมีการเปลี่ยนแปลงใดๆ ให้อยู่ในดุลยพินิจของโรงพยาบาล เว้นแต่เหตุสุดวิสัยรวมถึงสถานการณ์เหตุการณ์ความไม่สงบในประเทศ ทั้งนี้ต้องได้รับความเห็นชอบจากโรงพยาบาลก่อน

๘.๒ ค่าปรับในระยะเวลารับประกัน

หากผู้ยื่นข้อเสนอไม่เข้ามาแก้ไขให้แล้วเสร็จตามการรับประกันความชำรุดบกพร่อง ภายใน ๗ วันทำการ นับจากวันที่ได้รับแจ้งจากโรงพยาบาล ผู้ยื่นข้อเสนอจะต้องชำระค่าปรับให้ผู้ว่าจ้างเป็นรายวันในอัตราร้อยละ ๐.๒๐ (ศูนย์จุดสองศูนย์) ของวงเงินตามสัญญาจนกว่าจะแก้ไขปัญหาแล้วเสร็จ

๙. ข้อสงวนสิทธิ์

๙.๑ โรงพยาบาลสงวนสิทธิ์ในการตัดสินใจชี้ขาดปัญหาที่เกิดขึ้นทุกกรณี และให้ถือว่าคำวินิจฉัยของโรงพยาบาลเป็นที่สิ้นสุด ผู้ยื่นข้อเสนอตลอดจนผู้ยื่นข้อเสนอต้องยอมรับคำวินิจฉัยดังกล่าว โดยไม่มีข้อโต้แย้งหรือ ข้อแม้ใดทั้งสิ้น

๙.๒ การดำเนินงาน ผู้ยื่นข้อเสนอจะต้องไม่ละเมิดลิขสิทธิ์ผลงานของผู้อื่นโดยไม่ได้รับอนุญาต ข้อมูลอันเกิดจากการจัดจ้าง ตลอดจนรายงานสรุปที่จัดทำขึ้น เป็นกรรมสิทธิ์ของโรงพยาบาล ซึ่งผู้ยื่นข้อเสนอจะต้องไม่มอบข้อมูลในการดำเนินงานให้แก่ผู้ใด รวมทั้งไม่เผยแพร่ข้อมูลรายงานสรุป โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากโรงพยาบาล

.....นายศิริวิทย์ อัสวดีวงศ์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายกฤษฎา แต้มทอง กรรมการ

๙.๓ ในกรณีที่ผู้ว่าจ้างมีความจำเป็นไม่อาจทำสัญญาได้หรือมีเหตุจำเป็นด้านอื่นๆที่เป็นอุปสรรคผู้ว่าจ้าง ขอสงวนสิทธิ์ที่จะยกเลิกการว่าจ้างครั้งนี้ได้ทุกขั้นตอนโดยไม่จำเป็นต้องแจ้งเหตุผลใดๆ ให้ผู้ยื่นข้อเสนอทราบ และผู้ยื่นข้อเสนอไม่มีสิทธิ์โต้แย้งและเรียกร้องค่าใช้จ่ายหรือค่าเสียหายใดๆ ทั้งสิ้น

๙.๔ ผู้ว่าจ้างมีสิทธิ์ที่จะเปลี่ยนแปลงแก้ไขเพิ่มเติมหรือลดเนื้องานตามรายละเอียดในสัญญาได้การเพิ่มหรือลดเนื้องานคู่ สัญญาทั้งสองฝ่ายจะได้ตกลงเรื่องราคาราคาใหม่โดยถือราคาระบุไว้ในสัญญาเป็นฐานถ้าการเพิ่มหรือลดงานจำเป็นต้องการขยายหรือลดเวลาให้ตกลงไปในคราวเดียวกัน

๙.๕ การจัดซื้อจัดจ้างจะสามารถดำเนินการได้ก็ต่อเมื่อโครงการได้รับการจัดสรรงบประมาณแล้วเท่านั้น

๙.๖ ข้อมูล เอกสาร หรือสัญญาที่เกี่ยวข้องกับโครงการทั้งหมดที่ผู้ยื่นข้อเสนอดำเนินการและจัดทำมาให้ ตามสัญญาถือเป็นความลับและเป็นสมบัติของผู้ว่าจ้างผู้ยื่นข้อเสนอจะไม่เปิดเผยข้อมูลและผลการดำเนินการให้แก่ผู้ใด ยกเว้นแต่จะได้รับอนุญาตจากผู้ว่าจ้างเป็นลายลักษณ์อักษร หากที่ผู้ยื่นข้อเสนอละเมิดโดยการนำไปเผยแพร่และเปิดเผย โดยไม่ได้รับอนุญาตจากผู้ว่าจ้างมีสิทธิ์ฟ้องเรียกค่าเสียหายและดำเนินการตามกฎหมายตามแต่กรณี ทั้งนี้บุคลากรของผู้ยื่นข้อเสนอที่มาปฏิบัติงานในโครงการทุกคนจะต้องลงลายมือชื่อรับทราบข้อตกลง ห้ามเปิดเผยข้อมูลด้วยตนเอง

๙.๗ ผู้ว่าจ้างมีสิทธิ์ร้องขอให้ผู้ยื่นข้อเสนอสนับสนุนการบรรยาย/ให้ข้อมูลผลการปฏิบัติตามโครงการฯ ตามที่ โรงพยาบาลขอ

๑๐. การรับประกันความชำรุดบกพร่องของพัสดุที่ส่งมอบ

๑๐.๑ ผู้ยื่นข้อเสนอต้องรับประกันความชำรุดบกพร่องหรือข้อขัดข้องของระบบสัญญานี้เป็นตามระยะเวลา รับประกันนับแต่วันที่ผู้ว่าจ้างได้รับมอบถ้าภายในระยะเวลาดังกล่าวหากชำรุดบกพร่องหรือใช้งานไม่ได้ทั้งหมด หรือ แต่บางส่วนและความชำรุดบกพร่อง มิใช่ความผิดของผู้ว่าจ้าง กรณีข้อชำรุดบกพร่อง อันเกิดจากการประกอบ ติดตั้งที่ไม่ได้มาตรฐานต้องทำการแก้ไขทันที ผู้ยื่นข้อเสนอจะต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้งานได้ดังเดิม ภายใน ๗ วัน ทำการนับแต่วันเวลาที่ได้รับแจ้งจากผู้ว่าจ้าง และรับผิดชอบค่าใช้จ่ายทั้งหมด การรับประกันการชำรุด บกพร่องเป็นการขยายความซึ่งไม่ใช่การชำรุดโดยการใช้งานโดยไม่คิดค่าใช้จ่ายใดๆ จากผู้ว่าจ้างทั้งสิ้น

๑๐.๒ ผู้ยื่นข้อเสนอต้องรับประกันความชำรุดบกพร่องของงานตลอดอายุสัญญาการให้บริการ

๑๑. งบประมาณ

วงเงินงบประมาณในการจัดหา จำนวน ๒,๕๐๐,๐๐๐ บาท (สองล้านห้าแสนบาทถ้วน)

.....นายศิริวิทย์ อัสวดีวงศ์ ประธานกรรมการ
.....นายทรงพล ถึงพร้อม กรรมการ
.....นายกฤษฎา แท้มทอง กรรมการ