ขอบเขตของงาน

จ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์

(Cyber Security Managed Services)

1. ความเป็นมา

ปัจจุบันภัยคุกคามทางไซเบอร์มีรูปแบบที่ซับซ้อน เปลี่ยนแปลงรวดเร็ว และสามารถส่งผลกระทบอย่างมีนัยสำคัญต่อระบบเทคโนโลยีสารสนเทศ ข้อมูลที่สำคัญต่อภารกิจของกพท. รวมถึงกระบวนการดำเนินงานของกพท. โดยรวม ความเสียหายที่เกิดขึ้นอาจนำไปสู่การหยุดชะงักของระบบที่สำคัญ การสูญหายหรือรั่วไหลของข้อมูล การถูกทำลายชื่อเสียง และความเสียหายในมูลค่าทางเศรษฐกิจที่สูง โดยเฉพาะในสภาพแวดล้อมเทคโนโลยีดิจิทัลในปัจจุบันที่มีการเชื่อมต่อและพึ่งพาระบบสารสนเทศอย่างต่อเนื่องตลอดเวลา การมีมาตรการเฝ้าระวังและป้องกันภัยคุกคามอย่างเป็นระบบจึงเป็นสิ่งจำเป็น

ดังนั้น กพท. จำเป็นต้องมีระบบและบริการเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามหรือเหตุการณ์ผิดปกติที่อาจเกิดขึ้นในระบบเทคโนโลยีสารสนเทศและข้อมูล ได้อย่างต่อเนื่องตลอด 24 ชั่วโมง 7 วัน โดยต้องมีผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศคอยตรวจสอบ ติดตาม วิเคราะห์เหตุการณ์ และให้คำแนะนำ รวมถึงตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างทันท่วงทีและเป็นไปตามมาตรฐาน ซึ่งจะช่วยลดความเสี่ยง เพิ่มประสิทธิภาพการตรวจจับ รับมือ และป้องกันไม่ให้เกิดความเสียหายร้ายแรงก่อนขยายวงกว้าง

นอกจากนี้ การยกระดับความตระหนักรู้ของบุคลากรเป็นสิ่งจำเป็นอย่างยิ่ง เนื่องจากภัยคุกคามจำนวนมากในปัจจุบันเกิดจากการกระทำของบุคลากรเอง เช่น อีเมลฟิชชิ่ง หน่วยงานจึงต้องมีการทดสอบจำลองภัยคุกคาม เช่น Email Phishing และ USB Drop Test ควบคู่กับการฝึกอบรมด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ เพื่อให้บุคลากรสามารถรับรู้สัญญาณความเสี่ยง ป้องกัน และรายงานเหตุการณ์ต้องสงสัยได้อย่างถูกต้อง

ในการนี้ กพท. จึงมีความจำเป็นในการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) เพื่อให้มีการเฝ้าระวัง แจ้งเตือนเหตุการณ์ภัยคุกคามทางไซเบอร์ ทำให้ กพท. สามารถดำเนินงานด้านเทคโนโลยีสารสนเทศได้อย่างปลอดภัย มั่นใจและมีประสิทธิภาพ พร้อมทั้งสามารถปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้องได้อย่างครบถ้วน นอกจากนี้ยังมีการอบรมบุคลากรของ กพท. เพื่อเพิ่มศักยภาพและความรู้ความสามารถในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์อีกด้วย

2. วัตถุประสงค์

2.1 เพื่อให้ กพท. มีระบบสำหรับเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามหรือเหตุการณ์ผิดปกติอันอาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและข้อมูล ตลอด 24 ชั่วโมง

2.2 เพื่อยกระดับมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐานสากล ซึ่งสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.3 เพื่อสร้างความตระหนักให้เจ้าหน้าที่ที่เกี่ยวข้องของ กพท. มีความพร้อมในการรับมือต่อเหตุภัยคุกคามทางไซเบอร์

2.4 เพื่อเสริมความเชื่อมั่นต่อระบบเทคโนโลยีสารสนเทศขององค์กร และรักษาความมั่นคงของข้อมูลที่เกี่ยวข้องกับภารกิจด้านการบินพลเรือนของประเทศ

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ชาชุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐ ตามมาตรา 106 วรรคสาม (หมายถึง ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญา กับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง)

3.5 ไม่เป็นบุคคลซึ่งถูกแจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐตามมาตรา 109 (หมายถึง ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร หรือผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย)

3.6 คุณสมบัติหรือลักษณะต้องห้ามอื่นตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐประกาศกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

3.10.1 การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

3.10.2 งานซื้อหรือจ้าง และงานก่อสร้าง

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

3.10.3 การยื่นข้อเสนอของกิจการร่วมค้า

(1) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ซาซุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

(2) การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ 3.10.3 ดำเนินการซื้อและดาวน์โหลดเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารจ้างจึงจะมีสิทธิในการเข้ายื่นข้อเสนอในนามกิจการร่วมค้าได้

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

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

3.12.1 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือ ต่างประเทศซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหัก ด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ 1 ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนอนั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก 1 ปี ได้

3.12.2 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า 1 ล้านบาท

3.12.3 สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้าง หรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

3.12.4 กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการ หรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือ ที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอ ไม่เกิน 90 วัน

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ชาชุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุน เพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศ หรือบริษัทเงินทุนหลักทรัพย์ ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับ มอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน)

3.12.5 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทยตามข้อ 3.12.2, 3.12.3 และ 3.12.4 (2) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) จนถึงวันเสนอราคา

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศว่าด้วยการรับรองเอกสาร พ.ศ. 2539 และที่แก้ไขเพิ่มเติมกำหนด โดยจะต้องยื่นเอกสารดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอมิได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่าผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

3.13 กรณีตามข้อ 3.12.1 – 3.12.5 ไม่ใช้บังคับกับกรณีดังต่อไปนี้

3.13.1 กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

3.13.2 นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการ ตามพระราชบัญญัติล้มละลาย พ.ศ. 2483 และที่แก้ไขเพิ่มเติม

3.13.3 งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงาน ก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้าง ที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

3.13.4 การจัดซื้อจัดจ้างตามมาตรา 56 วรรคหนึ่ง (2) (ข) และ (ค) แห่งพระราชบัญญัติการจัดซื้อจัดจ้างฯ

3.13.5 การซื้ออสังหาริมทรัพย์และการเช่าอสังหาริมทรัพย์

3.13.6 กรณีงานจ้างบริการหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงานขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

3.14 ผู้ยื่นข้อเสนอต้องมีผลงานด้านการให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (Security Operation Center) หรือผลงานที่มีลักษณะเกี่ยวข้องทางด้านความมั่นคงปลอดภัยทางเครือข่าย (Network Security) หรือความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) หรือประเภทเดียวกันกับงานที่จ้างในวงเงินไม่น้อยกว่า 2,000,000 บาท (สองล้านบาทถ้วน) และเป็นผลงานที่แล้วเสร็จไม่เกินกว่า 5 ปี

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ชาชุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

นับถึงวันที่ยื่นเสนอราคา โดยสัญญาต้องมีอายุสัญญาไม่น้อยกว่า 1 ปี และเป็นผลงานที่เป็นสัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงานเอกชนที่ กพท. เชื่อถือ

3.14.1 หากเป็นผลงานกับหน่วยงานของรัฐ จะต้องแนบหนังสือรับรองผลงาน และสำเนาสัญญาจ้าง พร้อมรับรองสำเนาถูกต้องมาพร้อมกันในวันยื่นข้อเสนอ

3.14.2 หากเป็นผลงานกับหน่วยงานของเอกชน จะต้องแนบหนังสือรับรองผลงาน และสำเนาสัญญาจ้าง และใบกำกับภาษี พร้อมรับรองสำเนาถูกต้องมาพร้อมกันในวันยื่นข้อเสนอ

3.15 ผู้รับจ้างต้องยื่นเอกสารประวัติ คุณวุฒิ ประสบการณ์ทำงาน และสำเนาใบประกาศนียบัตรสากลของบุคลากรในโครงการซึ่งได้รับมอบหมายให้ปฏิบัติงานภายใต้สัญญาจ้างนี้ โดยเอกสารดังกล่าวจะต้องยื่นมาพร้อมกับประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

4. ขอบเขตของงาน

4.1 ผู้รับจ้างต้องมีบริการศูนย์เฝ้าระวังเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security/ Security Operation Center: CSOC หรือ SOC) ที่มีขอบเขตการดำเนินงานและคุณลักษณะอย่างน้อยดังนี้

4.1.1 ต้องให้บริการเฝ้าระวังและวิเคราะห์ความเชื่อมโยงของเหตุการณ์ภัยคุกคามทางไซเบอร์จากข้อมูล Log ของ Log Source ต่างๆ ของ กพท. ตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ (24 x 7)

4.1.2 รองรับการวิเคราะห์ข้อมูล Log ได้อย่างน้อย 2,000 Event Per Second (EPS) หรือ 100 GB/Day และรองรับการเพิ่มขยายในอนาคต

4.1.3 ระบบจัดเก็บรวบรวมและวิเคราะห์ข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ (Security Information and Event Management: SIEM) ต้องเป็นผลิตภัณฑ์หรือบริการที่ได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของรายงานการวิจัย Gartner Magic Quadrant for Security Information and Event Management (SIEM) Report ฉบับปี 2024 หรือฉบับล่าสุด หรือ Gartner Peer Insight

4.1.4 ระบบจัดเก็บรวบรวมและวิเคราะห์ข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ ต้องสามารถ Export ข้อมูล Log ในรูปแบบ XML หรือ CSV ได้เป็นอย่างน้อยและสามารถ Export รายงานในรูปแบบ PDF และ CSV ได้เป็นอย่างน้อย

4.1.5 ผู้รับจ้างต้องดำเนินการและให้การสนับสนุนในการติดตั้งระบบ อุปกรณ์ Hardware Appliance และ Software ทั้งหมดที่เกี่ยวข้องกับการส่งข้อมูล Log และการให้บริการเฝ้าระวังเหตุการณ์ภัยคุกคามทางไซเบอร์ เพื่อให้ Log Source สามารถส่งข้อมูล Log ไปยังระบบของศูนย์ SOC ได้ ทั้งนี้ ผู้รับจ้างต้องดำเนินการและให้การสนับสนุนในการติดตั้งเพื่อส่งข้อมูล Log จาก Log Source ของ กพท. อย่างน้อย 1 Log Source ตามข้อ 4.1.7 ให้สามารถแสดงผลที่ศูนย์ SOC ของผู้รับจ้างได้ ภายใน 1 วัน นับถัดจากวันลงนามในสัญญา

4.1.6 กรณีตรวจพบ Log Source ของ กพท. ไม่ส่งข้อมูล Log ไปยังศูนย์ SOC ผู้รับจ้างต้องแจ้งเตือน กพท. ตามที่ SLA กำหนด และต้องดำเนินการประสานงานร่วมกับเจ้าหน้าที่ของ กพท. เพื่อดำเนินการนำเข้าข้อมูล Log ของ Log Source ดังกล่าว ไปยังศูนย์ SOC ให้ครบถ้วน

4.1.7 รองรับการส่งข้อมูล Log จากระบบเครือข่ายคอมพิวเตอร์ต้นทางของ กพท. (Log Source) ไปที่ศูนย์ SOC ของผู้รับจ้าง ด้วยช่องทางที่ปลอดภัยผ่านอุปกรณ์ Hardware Appliance, Software หรือเครื่องมือที่ผู้รับจ้างจัดเตรียม ครอบคลุมรายการอุปกรณ์ Log Source อย่างน้อยดังนี้

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ชาชุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

(1) ระบบศูนย์กลาง Antivirus หรือ Endpoint Detection and Response (Management Console)

(2) อุปกรณ์เครือข่าย (Network Devices) เช่น Core Switch, Load Balancer, Wireless Controller หรือ Privileged Account Management เป็นต้น

(3) อุปกรณ์ป้องกันทางเครือข่าย (Network Security Devices) เช่น Firewall, Web Application Firewall (WAF) หรือ Network Detection and Response เป็นต้น

(4) อุปกรณ์และเครื่องคอมพิวเตอร์แม่ข่ายทางด้านระบบไอทีพื้นฐาน เช่น DNS Server, DHCP Server หรือ Active Directory Server เป็นต้น

(5) เครื่องคอมพิวเตอร์แม่ข่ายเว็บไซต์ และฐานข้อมูล เช่น IIS, Apache, NGINX, Tomcat, JBoss, Microsoft SQL Server หรือ Oracle เป็นต้น

(6) ระบบปฏิบัติการ (Operating System) เช่น Microsoft Windows, Unix หรือ Linux เป็นต้น

(7) ระบบ Cloud Services เช่น Microsoft 365, Amazon Web Services (AWS), Microsoft Azure Cloud, Google Cloud Platform (GCP), Cloudflare, Cloud WAF และ บริการอื่นๆที่อยู่บน Cloud เป็นต้น

หากไม่สามารถจัดเก็บข้อมูล Log จาก Log Source ข้างต้นได้ ผู้รับจ้างต้องสามารถปรับแต่ง (Customize Parsing) เพิ่มเติมให้สามารถจัดเก็บข้อมูล Log ได้ ทั้งนี้ ระหว่างสัญญา กพท. ขอสงวนสิทธิ์ในการปรับเปลี่ยน เพิ่ม/ลด Log Source ได้ตามความต้องการ

4.1.8 สามารถตั้งค่ารูปแบบการเฝ้าระวังตรวจจับเหตุการณ์ภัยคุกคาม ครอบคลุมในเรื่องอย่างน้อยดังนี้

(1) Unauthorized Access

(2) Create/Delete/Transfer Account

(3) Privilege Escalation

(4) Denial-of-Service (DoS) Attack

(5) Distributed Denial-of-Service (DDoS) Attack

(6) Brute Force Attacks

(7) Password Spraying

(8) Suspicious Traffic

(9) Lateral Movement

โดยการกำหนดเงื่อนไข Use Case ต้องมีการตกลงเห็นชอบร่วมกับ กพท. ทั้งนี้ ระหว่างสัญญา กพท. ขอสงวนสิทธิ์ในการปรับเปลี่ยน เพิ่ม/ลด Use Case ได้ตามความต้องการ

4.1.9 มีระบบ อุปกรณ์ Software หรือเครื่องมือ ที่สามารถแสดงผลและปรับแต่งรูปแบบการแสดงผล Dashboard ให้สอดคล้องกับ Use Case ที่กำหนด โดย กพท. สามารถค้นหา และ Query ข้อมูล Log ที่ต้องการตรวจสอบเพิ่มเติมได้แบบ Real Time ตลอดจนย้อนหลัง 90 วัน ซึ่ง กพท. สามารถเข้าใช้งานได้ไม่น้อยกว่า 5 ผู้ใช้งาน

4.1.10 ผู้รับจ้างต้องมีการใช้งานระบบข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์จากระบบ Threat Intelligence อย่างน้อย 2 แหล่งขึ้นไปในการให้บริการ กพท.

4.1.11 ต้องตกลงวิธีการแจ้งเตือนเหตุการณ์ภัยคุกคามทางไซเบอร์ร่วมกับ กพท. โดยต้องสามารถแจ้งเตือนผ่านช่องทาง Email และ โทรศัพท์ ได้เป็นอย่างน้อย

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ซาซุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

4.1.12 ดำเนินการแจ้งเตือนเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ ตาม Service Level Agreement (SLA) ที่ กพท. กำหนด รวมทั้งให้คำแนะนำทางเทคนิคในการรับมือตอบสนองเหตุการณ์ภัยคุกคามดังกล่าวแก่ กพท. ตลอดระยะเวลาสัญญา ตามเงื่อนไข SLA ดังนี้

ความรุนแรง (Severity)	ผลกระทบและการดำเนินการ	เวลาในการแจ้งเตือนแก่ กพท.	ให้คำแนะนำในการตอบสนอง
สูงมาก (Very High)	**ผลกระทบ:** - การโจมตีทางไซเบอร์ที่ส่งผลกระทบให้ระบบไม่สามารถใช้งานได้มากกว่า 1 ระบบ - ได้รับผลกระทบทั้งสำนักงาน - ระบบเครือข่ายไม่สามารถใช้งานได้ทั้งหมด **การดำเนินการ:** - แจ้งเตือนและให้คำแนะนำในการตอบสนองผ่านทางโทรศัพท์ - หลังจากนั้นส่งรายละเอียดการแจ้งเตือนและคำแนะนำในการตอบสนองผ่านช่องทางปกติที่ตกลงร่วมกับ กพท. อีกครั้ง	ภายใน 30 นาที	ภายใน 1 ชั่วโมง
สูง (High)	**ผลกระทบ:** - การโจมตีทางไซเบอร์ที่ส่งผลกระทบให้ระบบไม่สามารถใช้งานได้ - ได้รับผลกระทบมา กกว่า 1 สำนัก/ฝ่าย/ศูนย์ - ระบบเครือข่ายล้มเหลวบางส่วน และมีแนวโน้มว่าจะส่งผลกระทบต่อผู้ใช้งานทั้งหมด - เกิดผลกระทบต่อผู้บริหารระดับผู้จัดการเป็นต้นไป **การดำเนินการ:** - แจ้งเตือนผ่านช่องทางโทรศัพท์ - หลังจากนั้นส่งรายละเอียดการแจ้งเตือนและคำแนะนำในการตอบสนองผ่านช่องทางปกติที่ตกลงร่วมกับ กพท.	ภายใน 30 นาที	ภายใน 2 ชั่วโมง
ปานกลาง (Medium)	**ผลกระทบ:** - พบการโจมตีที่ส่งผลกระทบต่อการทำงานของระบบ - ได้รับผลกระทบในระดับสำนัก/ฝ่าย/ศูนย์ - ผู้ใช้ระบบยังสามารถใช้งานระบบได้แต่ประสิทธิภาพการทำงานของระบบลดลง - กรณีพบ Log Source ไม่ส่งข้อมูล Log ไปยังระบบ SIEM หรือ ศูนย์ SOC **การดำเนินการ:** แจ้งเตือนและให้คำแนะนำในการตอบสนองผ่านช่องทางปกติที่ตกลงร่วมกับ กพท.	ภายใน 3 ชั่วโมง	ภายใน 12 ชั่วโมง
ต่ำ (Low)	**ผลกระทบ:** เกิดเหตุการณ์ที่ส่งผลกระทบเฉพาะส่วน และไม่กระทบต่อการให้บริการ **การดำเนินการ:** แจ้งเตือนและให้คำแนะนำในการตอบสนองผ่านช่องทางปกติที่ตกลงร่วมกับ กพท.	ภายใน 12 ชั่วโมง	ภายใน 24 ชั่วโมง

นางสาวอรวรรณ ใจเอื้อ
ประธานกรรมการ

นายสราวุฒิ ล่วงเขตต์
กรรมการ

นางสาวณัฐชา ซาซุม
กรรมการ

นายธามรัฐ กุญชร ณ อยุธยา
กรรมการ

4.1.13 การแจ้งเตือนเหตุการณ์ภัยคุกคามทางไซเบอร์ตาม SLA ต้องครอบคลุมเนื้อหาอย่างน้อยดังต่อไปนี้

(1) กำหนดหมายเลขเหตุการณ์ภัยคุกคาม (Incident Number)

(2) ระบุประเภทของภัยคุกคาม

(3) วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

(4) ระบุต้นทาง (Source หรือ Attacker) และปลายทาง (Destination หรือ Target)

(5) ระดับความรุนแรงตาม SLA (Severity)

(6) รายละเอียดเหตุการณ์ และพฤติกรรม

(7) ระบุตัวบ่งชี้การโจมตี (Indicator of Attack: IOA) หรือ ตัวบ่งชี้การถูกโจมตี (Indicator of Compromise: IOC) (ถ้ามี) โดยต้องมีแหล่งอ้างอิงเพื่อยืนยันความถูกต้องจาก Threat Intelligence ตั้งแต่ 2 แหล่งขึ้นไป

(8) สิ่งที่ควรดำเนินการเป็นลำดับแรก (First Action)

4.1.14 การให้คำแนะนำการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ตาม SLA ต้องครอบคลุมเนื้อหาอย่างน้อยดังต่อไปนี้

(1) ระบุหมายเลขเหตุการณ์ภัยคุกคาม (Incident Number)

(2) ทวนซ้ำตามรายละเอียดการแจ้งเตือนเหตุการณ์ภัยคุกคาม

(3) อธิบายภาพการเชื่อมโยงเหตุการณ์ภัยคุกคามที่เกิดขึ้น (ถ้ามี)

(4) คำแนะนำและขั้นตอนการดำเนินการแก้ไขเชิงเทคนิค

4.1.15 ผู้รับจ้างต้องให้บริการค้นหาภัยคุกคามเชิงรุก (Threat Hunting) หรือดำเนินการค้นหารูปแบบการโจมตีจาก Threat Intelligence โดยใช้เครื่องมือของผู้รับจ้าง และแจ้งเตือนให้ทราบถึงภัยคุกคามที่จะเกิดขึ้นกับ กพท.

4.1.16 เมื่อพบเหตุการณ์ต้องสงสัยว่ามีระดับความรุนแรงสูงมาก (Very High) ผู้รับจ้างต้องจัดให้มีทีมงานผู้เชี่ยวชาญเพื่อดำเนินการเข้าตอบสนองรับมือ สืบสวน วิเคราะห์หาสาเหตุ และพิสูจน์หลักฐาน (Forensic) ภัยคุกคามที่เกิดขึ้นตามที่ กพท. ร้องขอ จำนวนไม่เกิน 3 เคสต่อสัญญา (ถ้ามี) พร้อมนำส่งรายงานการวิเคราะห์และพิสูจน์หลักฐานภัยคุกคามทางไซเบอร์ (Cyber Threat Analysis and Forensic Investigation Report) ภายใน 15 วันนับถัดจากวันที่ตรวจพบภัยคุกคามดังกล่าว

รายงานการวิเคราะห์และพิสูจน์หลักฐานภัยคุกคามทางไซเบอร์ (Cyber Threat Analysis and Forensic Investigation Report) ต้องมีหัวข้ออย่างน้อยดังนี้

(1) แผนภูมิรูปภาพสรุปเหตุการณ์

(2) องค์ประกอบที่เกี่ยวข้องกับภัยคุกคาม (Components Involved in the Threat)

(3) ตัวบ่งชี้การโจมตี (Indicator of Attack: IOA) และ ตัวบ่งชี้การถูกโจมตี (Indicator of Compromise: IOC) ที่เกี่ยวข้องทั้งหมด

(4) การรับมือตอบสนองที่ กพท. และผู้รับจ้างดำเนินการ

(5) การวิเคราะห์เพื่อระบุช่องทางที่เข้ามาโจมตี

(6) การบันทึกและถอดบทเรียน (Lessons Learned)

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ชาชุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

ก. การรับมือตอบสนองที่ทำได้ดี และที่ควรปรับปรุง

ข. การประเมินผลกระทบที่เกิดขึ้น หรืออาจเกิดขึ้น

ค. การวิเคราะห์ต้นเหตุ (Root Cause Analysis)

ง. การปรับปรุงแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan: CIRP) ของ กพท.

จ. คำแนะนำในการปรับปรุงเทคโนโลยี กระบวนการขั้นตอนปฏิบัติ และการพัฒนาบุคลากร เพื่อลดความเสี่ยงจากเหตุการณ์ภัยคุกคามในอนาคต

(7) ข้อกำหนดในการแบ่งปันข้อมูล (Information Sharing Requirements) โดยเป็นการกำหนดผู้ที่สามารถรับข้อมูลรายงาน และเนื้อหาส่วนใดบ้างของรายงานที่สามารถแบ่งปันได้

4.1.17 ต้องดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่มีความถูกต้อง ครบถ้วน และสมบูรณ์ เป็นไปตามที่กำหนดไว้ในกฎหมายที่เกี่ยวข้องทั้งหมด เป็นระยะเวลาไม่น้อยกว่า 90 วัน สามารถส่งให้ กพท. ได้ตามที่ร้องขอ

4.1.18 ต้องตกลงวิธีการแจ้งเตือนเหตุการณ์ภัยคุกคามทางไซเบอร์ร่วมกับ กพท. โดยต้องสามารถแจ้งเตือนผ่านช่องทาง Email และ โทรศัพท์ ได้เป็นอย่างน้อย

4.1.19 ศูนย์ SOC ต้องตั้งอยู่ในประเทศไทย และได้รับการรับรองมาตรฐาน ISO27001 เป็นอย่างน้อย

4.2 ผู้รับจ้างต้องมีบุคลากรผู้เชี่ยวชาญและเจ้าหน้าที่ประจำศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ ที่มีหน้าที่และคุณสมบัติอย่างน้อย ดังนี้

4.2.1 ผู้เชี่ยวชาญด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จำนวนอย่างน้อย 1 คน มีหน้าที่ให้คำแนะนำเรื่องการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และให้คำปรึกษาในการป้องกันรับมือตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ของ กพท. โดยต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้

(1) มีประสบการณ์การทำงานด้านการรับมือตอบสนองเหตุการณ์ภัยคุกคามทางไซเบอร์ หรือบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ หรือไซเบอร์ อย่างน้อย 10 ปี

(2) ได้รับใบประกาศนียบัตรที่ถูกยอมรับในระดับสากล เทียบเท่าหรือมากกว่า อย่างน้อย 1 ใบ ดังนี้ ISC2: Certified Information Systems Security Professional (CISSP), CompTIA: CompTIA SecurityX, GIAC: Certified Incident Handler (GCIH), Offensive Security: Offensive Security Certified Expert 3 (OSCE3) โดยใบประกาศนียบัตรต้องยังไม่หมดอายุ ณ วันที่ยื่นเสนอราคา

(3) ต้องเป็นพนักงานประจำของบริษัท โดยจะต้องแนบสำเนาบัตรประชาชน ประวัติการทำงาน และสำเนาใบประกาศนียบัตรสากล ในวันที่ยื่นเสนอราคา

4.2.2 ผู้เชี่ยวชาญด้านการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ หรือด้านการวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ อย่างน้อย 1 คน เพื่อเข้าปฏิบัติงานที่ กพท. อย่างน้อย 1 วัน/สัปดาห์ ในวันเวลาทำการของ กพท. โดยมีหน้าที่ในการประสานงานจัดการเหตุภัยคุกคามไซเบอร์ และสนับสนุน กพท. ด้านการวิเคราะห์ ให้ความรู้ และแนะนำกรอบการปฏิบัติที่เป็นมาตรฐาน (Best Practice) รวมถึงเทคนิคการจัดการภัยคุกคามประเภทต่างๆ และต้องส่งบันทึกลงเวลาพร้อมรายงานการปฏิบัติงาน (Service Report) เพื่อรวมในรายงานประจำเดือน (Monthly Report) แก่ กพท. โดยต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้

(1) มีประสบการณ์การทำงานด้านการรับมือตอบสนองเหตุการณ์ภัยคุกคามทางไซเบอร์ อย่างน้อย 3 ปี

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ชาชุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

(2) ได้รับใบประกาศนียบัตรที่ถูกยอมรับในระดับสากล เทียบเท่าหรือมากกว่า อย่างน้อย 1 ใบ ดังนี้ CompTIA: Cybersecurity Analyst (CySA+), CompTIA: Penetration Testing+ (PenTest+), Offensive Security: Offensive Security Certified Professional (OSCP), Cisco: Cisco Certified Network Professional (CCNP), EC Council: Computer Hacking Forensic Investigator (CHFI), GIAC: Penetration Tester (GPEN), GIAC: Security Leadership (GSLC) หรือ GIAC: Certified Enterprise Defender (GCED) โดยใบประกาศนียบัตรต้องยังไม่หมดอายุ ณ วันที่ยื่นเสนอราคา

(3) ต้องเป็นพนักงานประจำของบริษัท โดยจะต้องแนบสำเนาบัตรประชาชน ประวัติการทำงาน และสำเนาใบประกาศนียบัตรสากล ในวันที่ยื่นเสนอราคา

4.2.3 เจ้าหน้าที่ประจำศูนย์ SOC ระดับ 1 จำนวนอย่างน้อย 4 คน ปฏิบัติหน้าที่วิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ระดับ 1 ประจำศูนย์ SOC ของผู้รับจ้าง โดยต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้

(1) ได้รับใบประกาศนียบัตรที่ถูกยอมรับในระดับสากล เทียบเท่าหรือมากกว่า อย่างน้อย 1 ใบ ดังนี้ CompTIA: Security+, ISC2: Certified in Cybersecurity Certification (CC), Cisco: Cisco Certified Network Associate (CCNA) หรือ GIAC: GIAC Security Essentials (GSEC) โดยใบประกาศนียบัตรต้องยังไม่หมดอายุ ณ วันที่ยื่นเสนอราคา

(2) ต้องเป็นพนักงานประจำของบริษัท โดยจะต้องแนบสำเนาบัตรประชาชน ประวัติการทำงาน และสำเนาใบประกาศนียบัตรสากล ในวันที่ยื่นเสนอราคา

4.2.4 เจ้าหน้าที่ประจำศูนย์ SOC ระดับ 2 จำนวนอย่างน้อย 2 คน ปฏิบัติหน้าที่วิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ระดับ 2 ประจำศูนย์ SOC ของผู้รับจ้าง โดยต้องมีคุณสมบัติอย่างน้อยดังต่อไปนี้

(1) มีประสบการณ์การทำงานด้านการรับมือตอบสนองเหตุการณ์ภัยคุกคามทางไซเบอร์ อย่างน้อย 3 ปี

(2) ได้รับใบประกาศนียบัตรที่ถูกยอมรับในระดับสากล เทียบเท่าหรือมากกว่า อย่างน้อย 1 ใบ ดังนี้ CompTIA: Cybersecurity Analyst (CySA+), CompTIA: Penetration Testing+ (PenTest+), Offensive Security: Offensive Security Certified Professional (OSCP), Cisco: Cisco Certified Network Professional (CCNP), EC Council: Computer Hacking Forensic Investigator (CHFI), GIAC: Penetration Tester (GPEN), GIAC: Security Leadership (GSLC) หรือ GIAC: Certified Enterprise Defender (GCED) โดยใบประกาศนียบัตรต้องยังไม่หมดอายุ ณ วันที่ยื่นเสนอราคา

(3) ต้องเป็นพนักงานประจำของบริษัท โดยจะต้องแนบสำเนาบัตรประชาชน ประวัติการทำงาน และสำเนาใบประกาศนียบัตรสากล ในวันที่ยื่นเสนอราคา

4.3 การทดสอบและเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (User Awareness Exercise & Training) ประกอบด้วยอย่างน้อยดังนี้

4.3.1 ทำการทดสอบ Email Phishing Simulation เพื่อประเมินพฤติกรรมการตอบสนองของผู้ใช้งานต่ออีเมลที่มีความเสี่ยงหรือมีลักษณะเป็นการหลอกลวง โดยจัดทำเนื้อหาอีเมลและรูปแบบสถานการณ์ตามบริบทของ กพท. จำนวน 2 รอบ โดยมีรายละเอียดการดำเนินการ ดังนี้

(1) จัดทำแผนการทดสอบ Phishing Email จำนวน 2 รอบ โดยที่รอบที่ 1 จัดขึ้นก่อนทำการฝึกอบรม (User Awareness Training) และรอบที่ 2 จัดขึ้นหลังจากฝึกอบรม (User Awareness Training) โดยกำหนดกลุ่มเป้าหมาย จำนวนไม่น้อยกว่า 550 คนต่อรอบ หรือจำนวนตามที่ กพท. กำหนด

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ชาชุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

(2) ช่วงเวลาในการทดสอบ Phishing Email ในแต่ละรอบให้เป็นไปตามที่ กพท. กำหนด

(3) การทดสอบ Phishing Email แต่ละรอบ ต้องมีรูปแบบเหตุการณ์ (Campaign) ที่แตกต่างกันอย่างน้อย 4 Campaign และทุก Campaign ต้องได้รับการเห็นชอบจาก กพท.

(4) จัดทำรายงานผลการทดสอบ Phishing Email รอบที่ 1 และรายงานผลการทดสอบ Phishing Email รอบที่ 2 พร้อมเปรียบเทียบผลการทดสอบ และสรุปผลรายงานภาพรวม

(5) การทำการทดสอบ Phishing Email จะต้องไม่มีผลกระทบต่อบุคคลหรือหน่วยงานภายนอก และต้องไม่ส่งผลกระทบให้ กพท. เสียหาย

4.3.2 ทำการทดสอบ USB Drop Test เพื่อประเมินพฤติกรรมผู้ใช้งานเมื่อพบอุปกรณ์จัดเก็บข้อมูลภายนอกที่ไม่ทราบแหล่งที่มา และทดสอบความตระหนักด้านความเสี่ยงจากสื่อบันทึกข้อมูลภายนอก จำนวน 2 รอบ รอบละไม่เกิน 40 อัน โดยมีรายละเอียดการดำเนินการ ดังนี้

(1) จัดทำแผนการทดสอบ USB Drop Test จำนวน 2 รอบ โดยรอบที่ 1 จัดขึ้นก่อนทำการฝึกอบรม (User Awareness Training) และรอบที่ 2 จัดขึ้นหลังจากฝึกอบรม (User Awareness Training) โดยกำหนดกลุ่มเป้าหมายที่เป็นพนักงานของ กพท. โดยแผนการทดสอบต้องได้รับความเห็นชอบจาก กพท. ก่อน

(2) ช่วงเวลาในการทดสอบ USB Drop Test ในแต่ละรอบให้เป็นไปตามที่ กพท. กำหนด

(3) ในการทดสอบ USB Drop Test จะต้องควบคุมไม่ให้เกิดผลกระทบต่อบุคคลหรือองค์กรภายนอก และต้องกำหนดเทคนิคหรือวิธีการที่ทำให้กลุ่มเป้าหมายรู้ตัวล่วงหน้าน้อยที่สุดเพื่อให้ได้ประสิทธิภาพสูงสุด

(4) จัดทำรายงานผลการทดสอบ USB Drop Test รอบที่ 1 และรายงานผลการทดสอบ USB Drop Test รอบที่ 2 พร้อมเปรียบเทียบผลการทดสอบ และสรุปผลรายงานภาพรวม

(5) การทำการทดสอบ USB Drop Test จะต้องไม่มีผลกระทบต่อบุคคลหรือหน่วยงานภายนอก และต้องไม่ส่งผลกระทบให้ กพท. เสียหาย

4.3.3 User Awareness Training ดำเนินการฝึกอบรม/ให้ความรู้แก่ผู้ใช้งานในประเด็นการรู้เท่าทันภัยคุกคามไซเบอร์ และต้องจัดทำเอกสารประกอบ เนื้อหาแบบเข้าใจง่าย พร้อมสรุปเนื้อหาและตัวอย่างเหตุการณ์ที่ทันสมัย โดยมุ่งเน้นปรับพฤติกรรม ลดความเสี่ยง และยกระดับความตระหนักรู้ของผู้ใช้งาน

4.4 ผู้รับจ้างต้องให้บริการด้านข้อมูลด้านการป้องกันความเสี่ยงทางดิจิทัล (Digital Risk Protection) การเฝ้าระวังพื้นที่เสี่ยงจากการโจมตีภายนอก (Attack Surface Monitoring) และข่าวกรองด้านสื่อสังคม (Social Media Intelligence) โดยต้องสามารถรองรับการติดตามอย่างน้อย 10 คำสำคัญ (Keywords) ทั้งนี้ต้องดำเนินการตรวจสอบและอัปเดตข้อมูลอย่างน้อยวันละ 2 ครั้ง โดยผู้รับจ้างต้องดำเนินการตามรายละเอียดดังต่อไปนี้

4.4.1 ผู้รับจ้างต้องทำการเฝ้าระวังการรั่วไหลของข้อมูลประจำตัว (Credential Leak Monitoring) โดยผู้รับจ้างต้องรายงานข้อมูลบัญชีรั่วไหลให้แก่ กพท.

4.4.2 ผู้รับจ้างต้องสามารถทำการตรวจจับเว็บไซต์ฟิชชิ่ง (Domain Impersonation) และต้องรายงานข้อมูลเว็บไซต์ที่ตรวจพบให้แก่ กพท. เพื่อทำการยืนยันว่าอยู่ภายใต้การดูแลของ กพท. หรือไม่

4.4.3 ผู้รับจ้างต้องทำการเฝ้าระวังข้อมูลบนเว็บไซต์ปกติ รวมถึงเว็บไซต์ผิดกฎหมาย (Dark Web) และต้องดำเนินการเฝ้าระวังอย่างต่อเนื่องตลอดระยะเวลาโครงการ

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ซาซุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

4.4.4 ผู้รับจ้างต้องมีผู้เชี่ยวชาญด้านการให้คำแนะนำและการสนับสนุนทางเทคนิค ตลอดระยะเวลาการให้บริการ เพื่อให้สามารถให้การสนับสนุนในกรณีการเลียนแบบแบรนด์ (Brand Impersonation) หรือการรั่วไหลของข้อมูลประจำตัว (Credential Leaks) ได้อย่างเหมาะสม

4.5 ผู้รับจ้างต้องแจ้งเตือนข่าวช่องโหว่หรือความเสี่ยง ที่เกี่ยวกับ กพท. หรือภาคอุตสาหกรรมการบิน รวมถึงแจ้งเตือนข่าวกรองทางไซเบอร์ (Cyber Threat Intelligence) เมื่อพบข้อมูลส่วนบุคคล ข้อมูลสำคัญ หรือข้อมูลความลับของ กพท. รั่วไหลในเว็บไซต์ที่ผิดกฎหมาย เว็บไซต์ใต้ดิน แอปพลิเคชั่น หรือกลุ่ม Threat Actor ต่าง ๆ ทั้งนี้ เอกสารแจ้งเตือนข่าวช่องโหว่หรือความเสี่ยงดังกล่าวต้องอยู่ในรูปแบบที่ กพท. สามารถแก้ไขได้ และสามารถนำไปเผยแพร่ต่อในนาม กพท. ได้

4.6 ผู้รับจ้างต้องติดตามข้อมูลข่าวสารที่เกี่ยวกับความปลอดภัยเทคโนโลยีสารสนเทศและไซเบอร์ หรือ กพท. หรือภาคอุตสาหกรรมการบิน เพื่ออัพเดทข้อมูลข่าวสาร หรือข่าวสารที่ทันสมัย และ/หรือภัยคุกคามร้ายแรงที่มีความเสี่ยงให้แก่ กพท. อย่างสม่ำเสมอ ไม่น้อยกว่าเดือนละ 1 ครั้ง ในรูปแบบไฟล์ข้อมูลอิเล็กทรอนิกส์ โดยจัดส่งให้ กพท. ผ่านช่องทาง Email หรือ Shared File หรือช่องทางอื่นใดที่ กพท. กำหนด ซึ่งข้อมูลข่าวสารดังกล่าวประกอบด้วยเนื้อหาที่สำคัญอย่างน้อยดังนี้

(1) คำอธิบายทั่วไป (Overview)

(2) คำอธิบายอย่างละเอียด (Description)

(3) ผลกระทบ (Impact)

(4) ระบบที่ได้รับผลกระทบ (System Affected)

(5) ทางแก้ไข (Solution) (ถ้ามี) และ

(6) อ้างอิง (Reference)

ทั้งนี้ เอกสารแจ้งเตือนข่าวช่องโหว่หรือความเสี่ยงดังกล่าวต้องอยู่ในรูปแบบที่ กพท. สามารถแก้ไขได้และสามารถนำไปเผยแพร่ต่อในนาม กพท. ได้

4.7 ผู้รับจ้างต้องดำเนินการศึกษาและปรับปรุงแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan: CIRP) ของ กพท. และดำเนินการจัดทำคู่มือการตอบรับเหตุการณ์ทางไซเบอร์ (Cyber Incident Response Playbook) จำนวนอย่างน้อย 4 รูปแบบ นำส่งตามงวดงานอย่างน้อยงวดงานละ 1 รูปแบบ โดยต้องมีหัวข้อและเนื้อหาสอดคล้องตามแผน CIRP ของ กพท. หรือเป็นไปตามที่ กพท. กำหนด

4.8 ผู้รับจ้างต้องดำเนินการซ้อมแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) อย่างน้อย 1 ครั้ง พร้อมจัดทำรายงานสรุปผลในรูปแบบที่ กพท.กำหนด

4.9 ผู้รับจ้างต้องเข้าร่วมการทดสอบแผนสร้างความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) หรือแผนการกู้คืนระบบในสถานการณ์ฉุกเฉิน (Disaster Recovery Plan: DRP) อย่างน้อยปีละ 1 ครั้ง (ถ้ามี)

4.10 การจัดทำรายงานผลการดำเนินงาน

4.10.1 รายงานประจำวัน (Daily Report)

ผู้รับจ้างต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ กพท. ผ่านช่องทาง Email หรือ Shared File หรือช่องทางอื่นใดที่ กพท. กำหนด โดยจัดส่งให้แก่ กพท. ภายในเวลา 08.30 น. ของทุกวัน มีรายละเอียดของรายงานอย่างน้อยดังนี้

(1) รายงานสถานะอุปกรณ์ Log Source ประกอบด้วย

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ซาซุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

- ชื่อระบบงาน (System Name ที่นิยามโดย กพท.)
- ชื่อเครื่อง/อุปกรณ์ (Hostname)
- IP Address
- ปริมาณการส่งข้อมูล Log ของแต่ละ Log Source ไปที่ศูนย์ SOC (Daily Log Usage (GB/Day)
- ปริมาณการส่งข้อมูล Log ทั้งหมดของ กพท. ไปที่ศูนย์ SOC (Total Daily Log Usage (GB)
- สถานะ (Log Source Status)

(2) สรุปเหตุการณ์ผิดปกติ หรือเหตุการณ์ภัยคุกคามที่เกิดขึ้น (ถ้ามี)

- รายละเอียดครอบคลุมตามการแจ้งเตือนในข้อ 4.1.13 และ การให้คำแนะนำในข้อ 4.1.14 (ถ้ามี)
- สถานะเหตุการณ์ภัยคุกคามประจำวัน (Daily Incident Status)

(3) สรุปเหตุการณ์ผิดปกติ หรือเหตุการณ์ภัยคุกคามทั้งหมดที่ยังไม่ได้ปิด (All Pending Status Incident) (ถ้ามี)

4.10.2 รายงานประจำเดือน (Monthly Report)

ผู้รับจ้างต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ กพท. ผ่านช่องทาง Email หรือ Shared File หรือช่องทางอื่นใดที่ กพท. กำหนด โดยจัดส่งให้แก่ กพท. ภายในวันที่ 10 ของเดือนถัดไป มีรายละเอียดของรายงานอย่างน้อยดังนี้

(1) บทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังเหตุการณ์ภัยคุกคามในแต่ละเดือน

(2) สรุปปริมาณการส่งข้อมูล Log ในแต่ละวัน ตลอดทั้งเดือน (Monthly Log Usage Summary) และเปรียบเทียบปริมาณการส่งข้อมูล Log ในแต่ละวัน ของเดือนที่แล้ว (ถ้ามี)

(3) จัดอันดับ Log Source ทั้งหมดตามปริมาณการส่งข้อมูล Log ตลอดทั้งเดือน (Top 10 Log Source – Total Log Usage)

(4) สรุปรายการรูปแบบการเฝ้าระวัง (Use Case) ตามข้อ 4.1.8 ที่ กพท. ใช้อยู่ในแต่ละเดือน และสรุปเหตุการณ์ที่มีการแจ้งเตือนตาม Use Case ดังกล่าว

(5) สรุปเหตุการณ์ผิดปกติและเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในแต่ละเดือน โดยมีการจัดระดับความรุนแรง และวิเคราะห์ผลกระทบต่อการดำเนินธุรกิจของ กพท.

(6) สรุปการแจ้งเตือนเหตุการณ์ภัยคุกคามทางไซเบอร์ตาม Service Level Agreement (SLA) และสรุปสถานะการดำเนินการบริหารจัดการภัยคุกคามที่เกิดขึ้นในแต่ละเดือน

(7) รวบรวมข้อมูลข่าวสารเกี่ยวกับความปลอดภัยเทคโนโลยีสารสนเทศและไซเบอร์ตามข้อ 4.6 ตลอดทั้งเดือน

(8) ผู้รับจ้างต้องจัดประชุมประจำเดือน (Monthly Meeting) กับ กพท. ภายในวันที่ 15 ของเดือนถัดไป เพื่อรายงานและสรุปภาพรวมของรายงานประจำเดือน (Monthly Meeting)

(9) ผู้รับจ้างต้องส่งรายงานการปฏิบัติงาน (Service Report) ของผู้เชี่ยวชาญด้านการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ หรือด้านการวิเคราะห์ข้อมูลภัยคุกคามทางไซเบอร์ ตามข้อ 4.2.2

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ซาซุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

4.10.3 รายงานสรุปรายไตรมาส หรือรายงวดงาน (Quarterly Report)

ผู้รับจ้างต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ กพท. ผ่านช่องทาง Email หรือ Shared File หรือช่องทางอื่นใดที่ กพท. กำหนด โดยจัดส่งให้แก่ กพท. ภายใน 15 วัน นับถัดจากวันสุดท้ายของไตรมาส มีรายละเอียดของรายงานอย่างน้อยดังนี้

(1) บทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังเหตุการณ์ภัยคุกคามในแต่ละไตรมาส หรือรายงวดงาน

(2) สรุปรายการรูปแบบการเฝ้าระวัง (Use Case) ตามข้อ 4.1.8 ที่ กพท. ใช้อยู่ในแต่ละไตรมาส และสรุปเหตุการณ์ที่มีการแจ้งเตือนตาม Use Case ดังกล่าว

(3) สรุปเหตุการณ์ผิดปกติและเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในแต่ละไตรมาส หรือรายงวดงาน โดยมีการจัดระดับความรุนแรง และวิเคราะห์ผลกระทบต่อการดำเนินธุรกิจของ กพท.

(4) สรุปสถิติประเภทภัยคุกคามด้านความปลอดภัยเทคโนโลยีสารสนเทศหรือไซเบอร์ที่ กพท. เผชิญตลอดทั้งไตรมาส และวิเคราะห์สาเหตุหรือความเป็นไปได้

(5) สรุปการแจ้งเตือนเหตุการณ์ภัยคุกคามทางไซเบอร์ตาม Service Level Agreement (SLA) และสรุปสถานการณ์ดำเนินการบริหารจัดการภัยคุกคามที่เกิดขึ้นในแต่ละไตรมาส

(6) สรุปรายการสถานะการส่งรายงานประจำวัน (Daily Report) ตลอดทั้งไตรมาส รวมถึงระบุเวลาและวันที่ในการรายงานซึ่งต้องเป็นไปตามข้อ 4.10.1 (1)

(7) รวบรวมข้อมูลข่าวสารเกี่ยวกับความปลอดภัยเทคโนโลยีสารสนเทศและไซเบอร์ตามข้อ 4.6 ตลอดทั้งไตรมาส

4.10.4 รายงานประจำปี (Yearly Report)

ผู้รับจ้างต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ กพท. ผ่านช่องทาง Email หรือ Shared File หรือช่องทางอื่นใดที่ กพท. กำหนด โดยจัดส่งให้แก่ กพท. ภายใน 15 วัน นับถัดจากวันสุดท้ายของปี มีรายละเอียดของรายงานอย่างน้อยดังนี้

(1) บทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังเหตุการณ์ภัยคุกคามโดยสรุปเป็นภาพรวมตลอดทั้งปี

(2) สรุปเหตุการณ์ผิดปกติและเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งหมดตลอดทั้งปี โดยมีการจัดระดับความรุนแรง และวิเคราะห์ผลกระทบต่อการดำเนินธุรกิจของ กพท.

(3) สรุปสถิติประเภทภัยคุกคามด้านความปลอดภัยเทคโนโลยีสารสนเทศหรือไซเบอร์ที่ กพท. เผชิญตลอดทั้งปี และวิเคราะห์สาเหตุหรือความเป็นไปได้

(4) สรุปการแจ้งเตือนเหตุการณ์ภัยคุกคามทางไซเบอร์ตาม Service Level Agreement (SLA) และสรุปสถานการณ์ดำเนินการบริหารจัดการภัยคุกคามที่เกิดขึ้นเป็นภาพรวมตลอดทั้งปี

(5) รวบรวมข้อมูลข่าวสารเกี่ยวกับความปลอดภัยเทคโนโลยีสารสนเทศและไซเบอร์ตามข้อ 4.6 ตลอดทั้งปี

(6) สรุปแนวโน้ม หรือ Trend ของเหตุการณ์ภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นใน 3 ปีข้างหน้า และให้ข้อแนะนำที่ กพท. ควรดำเนินการเตรียมพร้อมเพื่อรับมือกับภัยคุกคามเหล่านั้น และเพื่อพิจารณาการปรับปรุงเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Technology Roadmap) ในระยะ 3 ปี

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ซาซุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

4.10.5 ผู้รับจ้างต้องจัดประชุมประจำเดือน (Monthly Meeting) กับ กพท. ภายในวันที่ 15 ของเดือนถัดไป เพื่อรายงานและสรุปภาพรวม รายงานประจำเดือน (Monthly Report) ตามข้อ 4.10.2

4.11 ผู้รับจ้างต้องดำเนินการจัดทำคู่มือการใช้งานระบบ อุปกรณ์ Software หรือเครื่องมือที่เกี่ยวข้อง และจัดฝึกอบรมการใช้งานฯ และวิธีการติดตั้งซอฟต์แวร์สำหรับส่ง Log ไปยังศูนย์ SOC ให้แก่เจ้าหน้าที่ผู้ดูแลระบบของ กพท.

4.12 ผู้รับจ้างต้องให้คำปรึกษาด้านเทคนิคแก่ กพท. ผ่านทาง Email โทรศัพท์ หรือช่องทางที่ กพท. กำหนด ได้ทุกวัน ตลอด 24 ชั่วโมง ตลอดระยะเวลาที่กำหนด

4.13 ผู้รับจ้างมีหน้าที่สนับสนุน และดำเนินการปิดหรือลดช่องโหว่ของอุปกรณ์และระบบของผู้รับจ้าง (ถ้ามี) โดยรายงานผลตามรูปแบบที่ กพท. กำหนด

4.14 ในกรณีที่ กพท. มีการย้ายสถานที่ทำการในช่วงระหว่างระยะเวลาของสัญญา ผู้รับจ้างต้องดำเนินการให้ระบบสามารถใช้งานได้ตามปกติ และสนับสนุนการแก้ไขปัญหาการใช้งานเป็นระยะเวลาอย่างน้อย 1 เดือน หลังจากทำการย้ายสถานที่ติดตั้ง โดยไม่มีค่าใช้จ่ายเพิ่มเติม

5. กำหนดเวลาส่งมอบพัสดุ

ระยะเวลา 12 เดือน (1 มกราคม 2569 – 31 ธันวาคม 2569)

6. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

เกณฑ์ราคา

7. วงเงินงบประมาณ

งบประมาณ จำนวน 4,130,000.00 บาท (สี่ล้านหนึ่งแสนสามหมื่นบาทถ้วน) ซึ่งได้รวมภาษีมูลค่าเพิ่มและค่าใช้จ่ายอื่นทั้งปวงไว้ด้วยแล้ว

8. งวดงานและการจ่ายเงิน

สำนักงานการบินพลเรือนแห่งประเทศไทยจะจ่ายเงินค่าจ้างให้แก่ผู้รับจ้าง โดยกำหนดการจ่ายเงินเป็นงวด ๆ ดังนี้

งวดที่ 1 เป็นจำนวนเงินในอัตราร้อยละ 25 เมื่อผู้รับจ้างได้ปฏิบัติงานโครงการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) เดือนที่ 1-3 ดังนี้

- ส่งมอบรายงานการดำเนินการ และให้การสนับสนุนในการติดตั้งระบบ อุปกรณ์ Hardware Appliance และ Software ทั้งหมดที่เกี่ยวข้องกับการส่งข้อมูล Log เพื่อให้ Log Source สามารถส่งข้อมูล Log ไปยังระบบของศูนย์ SOC ตามข้อ 4.1.5
- ส่งมอบคู่มือการใช้งานระบบ อุปกรณ์ Software หรือเครื่องมือ ตามข้อ 4.1.5
- ส่งมอบรายงานการทดสอบและเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ตามข้อ 4.3 (ถ้ามี)
- จัดฝึกอบรมการใช้งานตามคู่มือที่จัดทำให้แก่ผู้เข้าอบรมอย่างน้อย 3 คน และส่งมอบรายงานการจัดฝึกอบรม ตามข้อ 4.11
- ส่งมอบคู่มือการตอบรับเหตุการณ์ทางไซเบอร์ (Cyber Incident Response Playbook) จำนวนอย่างน้อย 1 รูปแบบ ตามข้อ 4.7

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ซาซุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

- ดำเนินการซ้อมแผนรับมือเหตุภัยคุกคามทางไซเบอร์ พร้อมจัดทำรายงานสรุปผล ตามข้อ 4.8 (ถ้ามี)
- เข้าร่วมการทดสอบแผนสร้างความต่อเนื่องทางธุรกิจ หรือแผนการกู้คืนระบบในสถานการณ์ฉุกเฉิน ตามข้อ 4.9 (ถ้ามี)
- จัดประชุมประจำเดือน (Monthly Meeting) ตามข้อ 4.10.2 (8)
- ส่งมอบรายงานประจำเดือน (Monthly Report) ตามข้อ 4.10.2
- ส่งมอบรายงานสรุปรายไตรมาส (Quarterly Report) ตามข้อ 4.10.3
- ส่งมอบรายงานการวิเคราะห์และพิสูจน์หลักฐานภัยคุกคามทางไซเบอร์ (Cyber Threat Analysis and Forensic Investigation Report) ตามข้อ 4.1.15 (ถ้ามี)
- ส่งมอบรายงานการดำเนินการ และให้การสนับสนุนในการติดตั้ง ปรับเปลี่ยน เพิ่ม/ลด ระบบ อุปกรณ์ Hardware Appliance และ Software ทั้งหมดที่เกี่ยวข้องกับการส่งข้อมูล Log เพื่อให้ Log Source สามารถส่งข้อมูล Log ไปยังระบบของศูนย์ SOC ตามข้อ 4.1.5 และ 4.1.7 (ถ้ามี)

ทั้งนี้ ส่งมอบในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 2 เป็นจำนวนเงินในอัตราร้อยละ 25 เมื่อผู้รับจ้างได้ปฏิบัติงานโครงการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) เดือนที่ 4-6 ดังนี้

- ส่งมอบรายงานการทดสอบและเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ตามข้อ 4.3 (ถ้ามี)
- ส่งมอบคู่มือการตอบรับเหตุการณ์ทางไซเบอร์ (Cyber Incident Response Playbook) จำนวนอย่างน้อย 1 รูปแบบ ตามข้อ 4.7
- ดำเนินการซ้อมแผนรับมือเหตุภัยคุกคามทางไซเบอร์ พร้อมจัดทำรายงานสรุปผล ตามข้อ 4.8 (ถ้ามี)
- เข้าร่วมการทดสอบแผนสร้างความต่อเนื่องทางธุรกิจ หรือแผนการกู้คืนระบบในสถานการณ์ฉุกเฉิน ตามข้อ 4.9 (ถ้ามี)
- จัดประชุมประจำเดือน (Monthly Meeting) ตามข้อ 4.10.2 (8)
- ส่งมอบรายงานประจำเดือน (Monthly Report) ตามข้อ 4.10.2
- ส่งมอบรายงานสรุปรายไตรมาส (Quarterly Report) ตามข้อ 4.10.3
- ส่งมอบรายงานการวิเคราะห์และพิสูจน์หลักฐานภัยคุกคามทางไซเบอร์ (Cyber Threat Analysis and Forensic Investigation Report) ตามข้อ 4.1.15 (ถ้ามี)
- ส่งมอบรายงานการดำเนินการ และให้การสนับสนุนในการติดตั้ง ปรับเปลี่ยน เพิ่ม/ลด ระบบ อุปกรณ์ Hardware Appliance และ Software ทั้งหมดที่เกี่ยวข้องกับการส่งข้อมูล Log เพื่อให้ Log Source สามารถส่งข้อมูล Log ไปยังระบบของศูนย์ SOC ตามข้อ 4.1.5 และ 4.1.7 (ถ้ามี)

ทั้งนี้ ส่งมอบในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ชาชุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

งวดที่ 3 เป็นจำนวนเงินในอัตราร้อยละ 25 เมื่อผู้รับจ้างได้ปฏิบัติงานโครงการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) เดือนที่ 7-9 ดังนี้

- ส่งมอบรายงานการทดสอบและเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ตามข้อ 4.3 (ถ้ามี)
- ส่งมอบคู่มือการตอบรับเหตุการณ์ทางไซเบอร์ (Cyber Incident Response Playbook) จำนวนอย่างน้อย 1 รูปแบบ ตามข้อ 4.7
- ดำเนินการซ้อมแผนรับมือเหตุภัยคุกคามทางไซเบอร์ พร้อมจัดทำรายงานสรุปผล ตามข้อ 4.8 (ถ้ามี)
- เข้าร่วมการทดสอบแผนสร้างความต่อเนื่องทางธุรกิจ หรือแผนการกู้คืนระบบในสถานการณ์ฉุกเฉิน ตามข้อ 4.9 (ถ้ามี)
- จัดประชุมประจำเดือน (Monthly Meeting) ตามข้อ 4.10.2 (8)
- ส่งมอบรายงานประจำเดือน (Monthly Report) ตามข้อ 4.10.2
- ส่งมอบรายงานสรุปรายไตรมาส (Quarterly Report) ตามข้อ 4.10.3
- ส่งมอบรายงานการวิเคราะห์และพิสูจน์หลักฐานภัยคุกคามทางไซเบอร์ (Cyber Threat Analysis and Forensic Investigation Report) ตามข้อ 4.1.15 (ถ้ามี)
- ส่งมอบรายงานการดำเนินการ และให้การสนับสนุนในการติดตั้ง ปรับเปลี่ยน เพิ่ม/ลด ระบบ อุปกรณ์ Hardware Appliance และ Software ทั้งหมดที่เกี่ยวข้องกับการส่งข้อมูล Log เพื่อให้ Log Source สามารถส่งข้อมูล Log ไปยังระบบของศูนย์ SOC ตามข้อ 4.1.5 และ 4.1.7 (ถ้ามี)

ทั้งนี้ ส่งมอบในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

งวดที่ 4 (งวดสุดท้าย) เป็นจำนวนเงินในอัตราร้อยละ 25 เมื่อผู้รับจ้างได้ปฏิบัติงานโครงการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) เดือนที่ 10-12 ดังนี้

- ส่งมอบรายงานการทดสอบและเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ตามข้อ 4.3 (ถ้ามี)
- ส่งมอบคู่มือการตอบรับเหตุการณ์ทางไซเบอร์ (Cyber Incident Response Playbook) จำนวนอย่างน้อย 1 รูปแบบ ตามข้อ 4.7
- ดำเนินการซ้อมแผนรับมือเหตุภัยคุกคามทางไซเบอร์ พร้อมจัดทำรายงานสรุปผล ตามข้อ 4.8 (ถ้ามี)
- เข้าร่วมการทดสอบแผนสร้างความต่อเนื่องทางธุรกิจ หรือแผนการกู้คืนระบบในสถานการณ์ฉุกเฉิน ตามข้อ 4.9 (ถ้ามี)
- จัดประชุมประจำเดือน (Monthly Meeting) ตามข้อ 4.10.2 (8)
- ส่งมอบรายงานประจำเดือน (Monthly Report) ตามข้อ 4.10.2
- ส่งมอบรายงานสรุปรายไตรมาส (Quarterly Report) ตามข้อ 4.10.3
- ส่งมอบรายงานสรุปประจำปี (Yearly Report) ตามข้อ 4.10.4

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ซาซุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

- ส่งมอบรายงานการวิเคราะห์และพิสูจน์หลักฐานภัยคุกคามทางไซเบอร์ (Cyber Threat Analysis and Forensic Investigation Report) ตามข้อ 4.1.15 (ถ้ามี)

- ส่งมอบรายงานการดำเนินการ และให้การสนับสนุนในการติดตั้ง ปรับเปลี่ยน เพิ่ม/ลด ระบบ อุปกรณ์ Hardware Appliance และ Software ทั้งหมดที่เกี่ยวข้องกับการส่งข้อมูล Log เพื่อให้ Log Source สามารถส่งข้อมูล Log ไปยังระบบของศูนย์ SOC ตามข้อ 4.1.5 และ 4.1.7 (ถ้ามี)

ทั้งนี้ ส่งมอบในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ทำการตรวจรับงานจ้างเรียบร้อยแล้ว

9. การรับประกันความชำรุดบกพร่อง

ผู้รับจ้างซึ่งได้ทำสัญญาจ้าง หรือข้อตกลงเป็นหนังสือ จะต้องรับประกันความชำรุดบกพร่องของงานที่เกิดขึ้นภายในระยะเวลาไม่น้อยกว่า..-..เดือน นับถัดจากวันที่สำนักงาน ได้รับมอบงาน โดยต้องรีบจัดการซ่อมแซมแก้ไขให้ใช้การได้ดีดังเดิมภายใน..-..วัน นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง

10. อัตราค่าปรับ

ค่าปรับตามสัญญาจ้างหรือข้อตกลงจ้างเป็นหนังสือจะกำหนด ดังนี้

10.1 กรณีที่ผู้รับจ้างนำงานที่รับจ้างไปจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจากสำนักงาน จะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนร้อยละ 10 ของวงเงินของงานจ้างช่วงนั้น

10.2 กรณีผู้รับจ้างปฏิบัติผิดสัญญาจ้าง นอกเหนือจากข้อ 10.1. จะกำหนดค่าปรับเป็นรายวันเป็นจำนวนเงินตายตัวในอัตราร้อยละ 0.10 ของราคางานจ้าง

10.3 หากอุปกรณ์/ระบบ ในโครงการชำรุด บกพร่อง หรือใช้งานไม่ได้ทั้งหมดหรือเพียงบางส่วน ผู้รับจ้างต้องจัดการซ่อมแก้ไขให้แล้วเสร็จภายใน 6 ชั่วโมง นับจากได้รับแจ้งจาก กพท. หากไม่สามารถดำเนินการได้ตามเวลาดังกล่าว ผู้รับจ้างจะต้องจ่ายค่าปรับให้แก่ กพท. เป็นรายวันในอัตราร้อยละ 0.10 ของราคางานจ้าง

11. ข้อตกลงห้ามเปิดเผยข้อมูล

ข้อมูล เอกสาร หรือสัญญาที่เกี่ยวข้องกับโครงการนี้ทั้งหมดที่ กพท. จัดหาให้ หรือผู้รับจ้างดำเนินการและจัดหาให้ กพท. ถือเป็นความลับ และเป็นสมบัติของ กพท. โดยผู้รับจ้างต้องไม่เปิดเผยข้อมูลและผลการดำเนินการให้แก่ผู้ใด ยกเว้นแต่จะได้รับอนุญาตจาก กพท. เป็นลายลักษณ์อักษร หากผู้รับจ้างละเมิดโดยมีการนำไปเผยแพร่ และเปิดเผยโดยไม่ได้รับอนุญาต กพท. มีสิทธิ์ฟ้องร้องเรียกค่าเสียหายและดำเนินการตามกฎหมายได้

12. ความคุ้มครองเกี่ยวกับลิขสิทธิ์

ข้อมูลรายงาน เอกสาร ผลการวิเคราะห์และศึกษาทั้งหมดที่ใช้ในการจัดทำโครงการนี้ ซึ่งผู้รับจ้างเป็นผู้ดำเนินการและจัดหามาตามสัญญานี้ จะตกเป็นกรรมสิทธิ์ของ กพท. ทันทีที่ส่งมอบ และ กพท. ขอสงวนสิทธิ์ในผลงานทุกอย่าง ผู้รับจ้างจะนำไปใช้หรือเผยแพร่ หรืออนุญาตให้ผู้ใดใช้ทั้งหมดหรือบางส่วนไม่ได้ เว้นแต่ได้รับความยินยอมเป็นลายลักษณ์อักษรจาก กพท.

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องใด ๆ ว่ามีการละเมิดลิขสิทธิ์เกี่ยวกับงานจ้างตามสัญญานี้ โดย กพท. มิได้แก้ไขดัดแปลงไปจากเดิม ผู้รับจ้างจะต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว เพื่อให้ กพท. สามารถใช้งานจ้างนั้นต่อไปได้ หากผู้รับจ้างมิอาจกระทำได้และ กพท. ต้องรับผิดชอบชดใช้ค่าเสียหายต่อบุคคลภายนอก เนื่องจากผลแห่งการละเมิดลิขสิทธิ์ดังกล่าว ผู้รับจ้างต้องเป็นผู้ชำระค่าเสียหาย ค่าปรับและค่าใช้จ่ายอื่น ๆ รวมทั้งค่าธรรมเนียม และค่า

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ชาชุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

ทนายความ ทั้งนี้ กพท. จะแจ้งผู้รับจ้างทราบเป็นลายลักษณ์อักษรในเมื่อได้มีการกล่าวอ้างหรือใช้สิทธิเรียกร้องดังกล่าว โดยไม่ชักช้า

13. เงื่อนไขอื่น ๆ

13.1 ผู้รับจ้างต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายคุ้มครองข้อมูลส่วนบุคคล และประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กพท. รวมถึงกฎหมาย นโยบาย คำสั่งและขั้นตอนปฏิบัติอื่น ๆ ที่เกี่ยวข้อง

13.2 ผู้รับจ้างต้องใช้พัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างทั้งหมดตามสัญญา

13.3 ผู้รับจ้างต้องจัดทำแผนการใช้พัสดุที่ผลิตภายในประเทศ โดยยื่นให้แก่ผู้ว่าจ้างภายใน 60 วัน นับถัดจากวันลงนามในสัญญา

13.4 ผู้รับจ้างจะต้องจัดทำและนำเสนอ แผนการดำเนินงานโครงการทั้งหมด โดยมีรายละเอียดครบถ้วน เพื่อให้ กพท. พิจารณาและให้ความเห็นชอบ ภายใน 15 วันนับถัดจากวันลงนามในสัญญา

14. หน่วยงานผู้รับผิดชอบโครงการ

ฝ่ายบริหารเทคโนโลยีดิจิทัล กองพัฒนามาตรฐานการจัดการและความปลอดภัยไซเบอร์ สำนักงานการบินพลเรือนแห่งประเทศไทย เลขที่ 222 ซอยวิภาวดีรังสิต 28 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900 โทรศัพท์ 02 568 8809 อีเมล์ itd_is@caat.or.th

นางสาวอรวรรณ ใจเอื้อ	นายสราวุฒิ ล่วงเขตต์	นางสาวณัฐชา ซาซุม	นายธามรัฐ กุญชร ณ อยุธยา
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ