รายละเอียดคุณลักษณะเฉพาะ
งานเช่าใช้ระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์
(Endpoint Protection)

1. ความเป็นมา

ตามที่ กพท. มีโครงการเช่าใช้ลิขสิทธิ์ซอฟต์แวร์ Antivirus และ Malware จำนวน 570 Licenses สิ้นสุดสัญญาวันที่ 31 ธันวาคม 2567 และโครงการเช่าใช้ลิขสิทธิ์ซอฟต์แวร์ Antivirus และ Malware จำนวน 130 Licenses สิ้นสุดสัญญาวันที่ 28 กุมภาพันธ์ 2568 นั้น จึงจำเป็นต้องเริ่มดำเนินการงานเช่าใช้ระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) เพื่อทดแทนซอฟต์แวร์ Antivirus และ Malware ที่จะหมดอายุและไม่สามารถใช้งานได้ในเดือนมกราคม และมีนาคม 2568 รวมถึงการปรับเพิ่มจำนวนลิขสิทธิ์ซอฟต์แวร์ เป็น 800 Licenses เพื่อรองรับจำนวนเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และพนักงานของ กพท. ที่เพิ่มมากขึ้น อีกทั้งยังเป็นการเพิ่มเติมเทคโนโลยีใหม่เพื่อให้การป้องกันและรักษาความปลอดภัยเครื่องคอมพิวเตอร์มีประสิทธิภาพมากยิ่งขึ้น

ระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) ที่เพิ่มเติมเทคโนโลยีใหม่เป็นระบบที่ช่วยป้องกันการโจมตีจากมัลแวร์ที่ไม่เคยพบเห็นมาก่อน โดยใช้ข้อมูลการวิเคราะห์อย่างละเอียดเปรียบเทียบกับพฤติกรรมของการโจมตีที่น่าสงสัย และจัดเก็บข้อมูลเป็นลำดับเหตุการณ์จากเริ่มต้นจนสิ้นสุดเพื่อช่วยในการสอบสวนในเหตุการณ์ที่น่าสงสัยและมองเห็นภาพรวมภัยคุกคามอย่างเต็มรูปแบบสามารถวิเคราะห์หาสาเหตุที่แท้จริงของการโจมตี และตอบสนองต่อภัยคุกคามที่มาจากเครื่องคอมพิวเตอร์ได้ทันที

ทั้งนี้การที่ กพท. จัดให้มีระบบดังกล่าว เป็นการใช้มาตรการป้องกัน มาตรการตรวจสอบและเฝ้าระวัง เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศของ กพท. สอดคล้องและเป็นไปตาม มาตรา 13 วรรคหนึ่ง (4) และมาตรา 45 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 รวมถึง มาตรา 37 (1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

ในการนี้ กพท. จึงมีความจำเป็นต้องเช่าใช้ระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) เพื่อให้ กพท. มีความปลอดภัยสูงสุดจากความเสี่ยงของภัยคุกคามทางไซเบอร์ที่มีแนวโน้มทวีความรุนแรงมากยิ่งขึ้น และเพื่อให้มีมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์สอดคล้องและเป็นไปตามกฎหมาย กฎระเบียบ และข้อบังคับที่เกี่ยวข้อง

2. วัตถุประสงค์

2.1. เพื่อจัดหาระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) ที่เพียงพอต่ออุปกรณ์คอมพิวเตอร์ และระบบคอมพิวเตอร์แม่ข่ายทั้งหมดของ กพท.

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ

2.2. เพื่อให้อุปกรณ์คอมพิวเตอร์ และระบบคอมพิวเตอร์แม่ข่ายทุกเครื่องของ กพท. มีความปลอดภัยจากภัยคุกคาม และโปรแกรมไม่พึงประสงค์

2.3. เพื่อดูแลบำรุงรักษาให้ระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) สามารถทำงานได้อย่างมีประสิทธิภาพและมีสภาพพร้อมใช้งานอยู่ตลอดเวลา

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1. มีความสามารถตามกฎหมาย

3.2. ไม่เป็นบุคคลล้มละลาย

3.3. ไม่อยู่ระหว่างเลิกกิจการ

3.4. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7. เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพให้เช่างานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10. ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง

3.11. ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริการพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) 0405.2/ว 124 ลงวันที่ 1 มีนาคม 2566 ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอ

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ

จะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ โดยต้องมีทุนจดทะเบียนไม่ต่ำกว่า 1,000,000 บาท

(3) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเกิน 500,000 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา ให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการ หรือรายการยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้าง หรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มูลค่าดังกล่าวอีกครั้งในวันลงนามในสัญญา

(4) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการ หรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการ หรือรายการที่ยื่นเสนอในแต่ละครั้ง (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตในประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นเสนอนับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน)

(5) กรณีตามข้อ (1) – (4) ยกเว้นสำหรับกรณีดังต่อไปนี้

(5.1) การจัดซื้อจัดจ้างครั้งหนึ่งไม่เกิน 500,000 บาท

(5.2) กรณีผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

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

(5.4) การซื้อและการเช่าอสังหาริมทรัพย์

3.12. ผู้ยื่นข้อเสนอที่เสนอราคาในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ

3.13. ผู้ยื่นข้อเสนอจะต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์หรือสาขาของเจ้าของผลิตภัณฑ์ ในกรณีผู้ยื่นข้อเสนอมิใช่ตัวแทนจำหน่ายตามข้อกำหนดข้างต้น ผู้ยื่นข้อเสนอจะต้องมีหนังสือยืนยันการแต่งตั้งให้เป็นตัวแทนจำหน่ายเฉพาะในการเสนอราคาครั้งนี้จากเจ้าของผลิตภัณฑ์ หรือตัวแทนจำหน่าย หรือสาขาของเจ้าของผลิตภัณฑ์ โดยผู้ยื่นข้อเสนอต้องนำส่งหนังสือยืนยันการเป็นตัวแทนจำหน่ายในวันยื่นข้อเสนอ

4. รายละเอียดคุณลักษณะเฉพาะของพัสดุ

4.1 ผู้ให้เช่าต้องจัดหาระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) อย่างน้อยเป็นแบบ Endpoint Detection and Response (EDR) โดยมีคุณสมบัติและคุณลักษณะเฉพาะอย่างน้อยดังนี้

4.1.1 จำนวนและระยะเวลาลิขสิทธิ์ซอฟต์แวร์สามารถใช้งานได้อย่างน้อยดังนี้

- 670 สิทธิ์ สำหรับใช้งานได้เป็นระยะเวลา 24 เดือน
- 130 สิทธิ์ สำหรับใช้งานได้เป็นระยะเวลา 22 เดือน

โดยมีวันสิ้นสุดของทั้ง 800 สิทธิ์ เป็นวันเดียวกัน

4.1.2 สามารถรองรับการใช้งานกับเครื่องคอมพิวเตอร์ที่มีระบบปฏิบัติการ อย่างน้อยดังนี้

- Windows 10
- Windows 11
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Linux

4.1.3 สามารถตรวจจับและตอบสนองภัยคุกคามที่เกิดขึ้นบนเครื่องคอมพิวเตอร์โดยมีความสามารถด้านการตรวจจับและตอบสนองภัยคุกคามอย่างน้อยดังนี้

(1) สามารถป้องกันมัลแวร์ (Malware Prevention) ทั้งแบบ Known และ Unknown malware

(2) ตรวจจับและตอบสนองภัยคุกคามที่ใช้เทคนิคการโจมตีแบบไม่ใช้ไฟล์ (Fileless Attacks)

(3) ป้องกันการโจมตีที่ช่องโหว่ของระบบ (Exploit Prevention)

(4) ตรวจจับและตอบสนองการโจมตีโดยใช้เทคนิค AI-based หรือ Machine Learning

(5) ตรวจจับและตอบสนองโดยใช้การวิเคราะห์พฤติกรรม (Behavior)

(6) สามารถตรวจจับและตอบสนองการโจมตีแบบ Zero-day

4.1.4 ซอฟต์แวร์ Agent ต้องสามารถป้องกัน Exploit และ Malware ในกรณีที่ไม่สามารถติดต่อกับระบบบริหารจัดการส่วนกลางได้ (Offline Agent)

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ

4.1.5 สามารถทำการปรับปรุง (Update) ข้อมูลภัยคุกคาม และซอฟต์แวร์ Version จาก Cloud ของผลิตภัณฑ์ได้โดยตรง ทั้งนี้ กรณีเป็นการปรับปรุง (Update) ในเครื่องคอมพิวเตอร์ที่ใช้เครือข่ายแบบปิด หากจำเป็นต้องมีอุปกรณ์ หรือ appliance สำหรับ distributor ผู้ให้เช่าต้องเป็นผู้จัดหาและบำรุงรักษาอุปกรณ์ หรือ appliance ดังกล่าวตลอดอายุสัญญา โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

4.1.6 สามารถทำการกู้คืน (Restore) ไฟล์ที่ถูกกักกัน (Quarantine) ได้

4.1.7 ซอฟต์แวร์ที่นำเสนอต้องผ่านการประเมินการทดสอบตามเกณฑ์ Leader ของรายงานการวิจัย Gartner Magic Quadrant for Endpoint Protection Platforms Report ฉบับปี 2024 หรือฉบับล่าสุด

4.2 มีระบบบริหารจัดการส่วนกลาง (Centralized Management หรือ Management Console) ที่ทำงานภายใต้สถาปัตยกรรมแบบ Cloud โดยมีคุณสมบัติอย่างน้อยดังนี้

4.2.1. ระบบมีการบริหารจัดการผ่านรูปแบบ Web Application (Web based Console)

4.2.2. มีเครื่องมือแสดงภาพรวมการตรวจจับและตอบสนองภัยคุกคาม เช่น Investigation หรือ Dashboard ที่สามารถปรับแต่งได้ (Customization)

4.2.3. สามารถแสดงภาพและข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ในรูปแบบ Story หรือ Chain หรือ Timeline หรือ Events Record ได้ โดยมีรายละเอียดอย่างน้อยดังนี้

(1) ระบุประเภทภัยคุกคาม

(2) วัน - เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

(3) ระบุต้นทาง (Source) และปลายทาง (Destination) หรือสามารถแสดงลำดับเหตุการณ์ที่เกิดขึ้นได้

(4) รายละเอียดเหตุการณ์และพฤติกรรม

(5) ค่าคะแนน (Scoring) ของภัยคุกคาม

(6) สามารถนำข้อมูลภัยคุกคามที่ตรวจพบมาแสดงให้อยู่ในรูปแบบ MITRE ATT&CK Framework ใน Stage ต่าง ๆ ได้

4.2.4. มีการ Authentication เข้าใช้งานระบบแบบ 2- Factor Authentication เป็นอย่างน้อย

4.2.5. สามารถกำหนดสิทธิผู้ดูแลระบบที่แตกต่างกันได้ (User Roles)

4.2.6. สามารถดู Log สำหรับตรวจสอบการกระทำของผู้ดูแลระบบได้

4.2.7. สามารถส่งข้อมูล Log หรือ Alert ของภัยคุกคามไปยังระบบจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ของสำนักงาน ผ่านทาง API/JSON หรือ Syslog หรือ การติดตั้ง Agent ได้

4.2.8. สามารถควบคุมและบริหารจัดการ Agent ในแต่ละเครื่องคอมพิวเตอร์ได้

4.2.9. สามารถดูรายการ (Host Inventory) และรายละเอียดเครื่องคอมพิวเตอร์ (Detail) ที่ติดตั้งซอฟต์แวร์ได้ เช่น User, Application, Services, Driver, Autorun เป็นต้น

4.2.10. สามารถแสดงสถานะเครื่องคอมพิวเตอร์ที่ติดตั้งซอฟต์แวร์ได้

4.2.11. สามารถตั้งค่า (Policy) และจัดกลุ่มการตั้งค่า (Group Policy) ให้แต่ละเครื่องคอมพิวเตอร์ที่ติดตั้งซอฟต์แวร์ได้

4.2.12. สามารถสั่งสแกนตามช่วงเวลาที่กำหนดได้ (on-demand scan หรือ schedule scan)

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ

4.2.13. สามารถสั่งตอบสนองต่อภัยคุกคาม (Response) โดยการสั่งกักกันหรือแยกเครื่องคอมพิวเตอร์ที่มีความเสี่ยงออกจากระบบเครือข่าย (Quarantine หรือ Isolate หรือ Containment) ได้เป็นอย่างน้อย

4.2.14. สามารถเพิ่ม หรือแก้ไข Behavior Indicators of Compromise (BIOC) หรือ Indicator of Attack (IOA) เพื่อสร้าง Alert ในการตรวจจับพฤติกรรมที่ผิดปกติ (Malicious Behaviors) หรือเหตุการณ์ภัยคุกคามที่เคยเกิดขึ้นในอดีตได้ หรือนำเสนอระบบอื่นๆ เพิ่มเติมให้สามารถทำได้ตามความต้องการดังกล่าว

4.2.15. สามารถควบคุมเครื่องคอมพิวเตอร์ลูกข่าย (Client) ด้วยระบบบริหารจัดการส่วนกลางผ่าน Terminal หรือ Connect to Host ได้

4.2.16. สามารถทำ Automatic Workflow หรือ Automatic Rule ในการรับมือภัยคุกคามได้เป็นอย่างน้อย

4.2.17. สามารถกำหนดรหัสผ่าน หรือ Token เพื่อป้องกันการถอนซอฟต์แวร์ (Uninstall) และป้องกันการแก้ไขการตั้งค่า (Policy) ของซอฟต์แวร์บนเครื่องคอมพิวเตอร์ได้

4.2.18. สามารถทำการยกเว้นการตรวจสอบสแกนไวรัส (Whitelist หรือ allow list) โดยกำหนดรูปแบบ File, Folder และ Process ได้เป็นอย่างน้อย

4.2.19. สามารถควบคุมและกำหนดสิทธิการใช้งานอุปกรณ์ต่อพ่วงได้ (Device Control) เช่น Removable drive และ USB Drives เป็นต้น

4.2.20. สามารถสร้างรายงานในรูปแบบไฟล์ csv, pdf หรือ html ได้เป็นอย่างน้อย

4.2.21. สามารถตั้งค่าการแจ้งเตือนของระบบ ไปยัง E-Mail ที่สำนักงานกำหนดได้

4.2.22. สามารถตรวจสอบข้อมูลการใช้งานลิขสิทธิ์ได้ (License Information)

4.2.23. สามารถกำหนดการ upgrade Agent ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ลูกข่ายและแม่ข่ายได้แบบอัตโนมัติ โดยที่จะต้องระบุได้ว่า version ที่ต่ำกว่า version ที่ออกใหม่ล่าสุด 1 version (n-1) และสามารถเลือกการหน่วงเวลา (Delay) ในการ update content / signature version เพื่อป้องกันผลกระทบที่เกิดขึ้นจาก Content / signature version ที่มีปัญหาได้

4.2.24. สามารถวิเคราะห์ตรวจจับภัยคุกคามบนระบบเครือข่ายเพื่อให้เห็นภัยคุกคามเป็นภาพรวมเดียวกันได้ โดยต้องสามารถทำงานร่วมกับอุปกรณ์เครือข่ายของ กพท. และต้องสามารถรับข้อมูลเครือข่ายได้ไม่น้อยกว่า 10 GB ต่อวัน

ทั้งนี้ หากระบบดังกล่าวไม่สามารถรับข้อมูลเครือข่ายจากอุปกรณ์เครือข่ายของ กพท. ผู้ให้เช่าต้องเสนออุปกรณ์หรือระบบอื่นใด โดยไม่คิดค่าใช้จ่ายเพิ่มเติม และดำเนินการสนับสนุนเพื่อให้ระบบบริหารจัดการส่วนกลางสามารถรับข้อมูลเครือข่ายของ กพท. และแสดงผลการวิเคราะห์ตรวจจับภัยคุกคามเป็นภาพรวมเดียวกันได้

4.3 ผู้ให้เช่าต้องดำเนินการติดตั้ง ดูแล บำรุงรักษา แก้ไขระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) และให้บริการต่าง ๆ รายละเอียดอย่างน้อยดังต่อไปนี้

4.3.1. ดำเนินการติดตั้งซอฟต์แวร์ให้กับเครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์แม่ข่ายของ กพท. โดยในระหว่างการดำเนินการติดตั้ง ต้องมีเจ้าหน้าที่ช่วยให้คำปรึกษา แก้ไขปัญหาหรือผลกระทบที่อาจเกิดขึ้น

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ

4.3.2. ผู้ให้เช่าต้องมีผู้เชี่ยวชาญในผลิตภัณฑ์ที่ให้เช่า เพื่อดำเนินการให้บริการและปรับปรุงความเหมาะสมของซอฟต์แวร์ที่ติดตั้ง (Tuning) ให้มีประสิทธิภาพและเหมาะสมกับสภาพแวดล้อมของสำนักงาน ตลอดระยะเวลาสัญญา

4.3.3. สำนักงาน สามารถขอรับคำปรึกษาด้านเทคนิคผ่านทาง E-Mail หรือ Group Chat หรือโทรศัพท์ได้โดยไม่จำกัดจำนวนครั้งตลอด 24 x 7 ตลอดระยะเวลาสัญญา

4.3.4. ผู้ให้เช่าต้องตรวจสอบ และปรับปรุง Version ของซอฟต์แวร์อย่างน้อยเดือนละ 1 ครั้ง (ถ้ามี) โดยผู้เช่าต้องสามารถใช้ระบบได้เป็นปกติ

4.3.5. ผู้ให้เช่าต้องจัดทำรายงานประจำเดือน (Monthly Report) เป็นไฟล์ข้อมูลอิเล็กทรอนิกส์และจัดส่งรายงานให้แก่ กพท. ผ่านช่องทาง Email หรือ Shared File หรือช่องทางอื่นใดที่ กพท. กำหนด โดยจัดส่งให้แก่ กพท. ภายในวันที่ 10 ของเดือนถัดไป มีรายละเอียดของรายงานอย่างน้อยดังนี้

(1) สถานะของเครื่องคอมพิวเตอร์ปลายทาง (Endpoint Security Posture)
- จำนวนเครื่องคอมพิวเตอร์ที่ใช้งาน Agent (Active Agent) เปรียบเทียบกับเดือนก่อนหน้า (ถ้ามี)
- จำนวนและรายการเครื่องคอมพิวเตอร์ที่ไม่ได้ใช้งานหรือไม่ได้ติดตั้ง Agent (Inactive Agent) เปรียบเทียบกับเดือนก่อนหน้า (ถ้ามี)
- จำนวนและรายการเครื่องคอมพิวเตอร์ที่ขาดการติดต่อกับระบบ Management Console มากกว่า 7 วัน (Last Communication > 7 Days)
- จำนวนและรายการสถานะ Agent Version ปัจจุบันที่ติดตั้งบนเครื่องคอมพิวเตอร์และ Agent Version ล่าสุดที่เจ้าของผลิตภัณฑ์ปล่อยให้ Update ได้

(2) สถานะการ Tuning ระบบ
- จำนวนและรายการภัยคุกคามที่ตรวจสอบแล้วว่าเป็นการแจ้งเตือนผิดพลาด (False Positive) รวมถึงจำนวนและรายการภัยคุกคามที่ยังไม่ยืนยันว่าเป็นการแจ้งเตือนผิดพลาด (False Positive)

(3) สถิติภัยคุกคาม (Threat Statistic)
- จำนวนและรายการเหตุการณ์ผิดปกติ หรือภัยคุกคามที่ตรวจพบแบ่งตามประเภทหรือชนิดของภัยคุกคามในเดือนปัจจุบัน เปรียบเทียบกับเดือนก่อนหน้า (ถ้ามี)
- จำนวนและรายการเครื่องคอมพิวเตอร์ลูกข่าย (Client) พร้อมแสดงชื่อ Client User ที่ตรวจพบภัยคุกคามในเดือนปัจจุบัน เปรียบเทียบกับเดือนก่อนหน้า (ถ้ามี)
- จำนวนและรายการเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ตรวจพบภัยคุกคามในเดือนปัจจุบัน เปรียบเทียบกับเดือนก่อนหน้า (ถ้ามี)

(4) การตรวจสอบและกำหนดค่ากลุ่มนโยบาย (Group Policy and Configuration Monitoring)
- รายการกลุ่มนโยบาย และรายละเอียดการกำหนดค่าแต่ละกลุ่มนโยบาย

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ

- จำนวนและรายการเครื่องคอมพิวเตอร์ที่อยู่ในแต่ละกลุ่มนโยบาย

(5) รายงานการวิเคราะห์และตรวจสอบไฟล์ที่ต้องสงสัย (ถ้ามี)

(6) รายงานการแจ้งเตือนภัยคุกคามเชิงรุก (Threat Hunting Service)

- รวบรวมและระบุรายการการแจ้งเตือนจากบริการภัยคุกคามเชิงรุกของเดือนปัจจุบัน
- รวบรวมและระบุรายการการแจ้งเตือนจากบริการภัยคุกคามเชิงรุกของทุกเดือนที่ยังปิดเคสไม่สำเร็จ

(7) รายงานการให้คำปรึกษา แนะนำ ชี้แจง รับแจ้งปัญหา และแก้ไขปัญหา (ถ้ามี) โดยให้รวบรวมและระบุหัวข้อ รายละเอียด และสถานะของทุกคำถาม-คำตอบจากรายงานทุกเดือน ตลอดระยะเวลาสัญญา

4.3.6. ผู้ให้เช่าต้องมีผู้เชี่ยวชาญในผลิตภัณฑ์ที่ให้เช่า เพื่อสนับสนุนการวิเคราะห์และตรวจสอบไฟล์ที่ต้องสงสัย ตามที่ กพท. ร้องขอ โดยให้สรุปผลการวิเคราะห์และตรวจสอบไฟล์ลงในรายงานตามหัวข้อ 4.3.5. ข้อ (5) (ถ้ามี)

4.3.7. ผู้ให้เช่าต้องมีบริการในการค้นหาภัยคุกคามเชิงรุก (Threat Hunting Service) โดยต้องมีขอบเขตการให้บริการอย่างน้อยดังนี้

(1) มีการค้นหาและแจ้งเตือนภัยคุกคามเชิงรุกโดยผู้เชี่ยวชาญในการทำ Threat Hunting แบบ 24 x 7

(2) การค้นหาภัยคุกคามเชิงรุกต้องครอบคลุมทุกเครื่องคอมพิวเตอร์ที่ติดตั้งซอฟต์แวร์ Agent ที่ผู้ให้เช่าเสนอ

(3) มีการแจ้งเตือนภัยคุกคามผ่าน Email Notification และต้องสามารถติดต่อกลับผู้เชี่ยวชาญผ่านการ Reply Email ได้

(4) การค้นหาภัยคุกคามเชิงรุก ต้องทำจากข้อมูลการใช้งาน (Telemetry) ที่เก็บมาจาก Agent ต่าง ๆ และต้องทำการตรวจสอบสิ่งผิดปกติจากการใช้งานของ User, Process และ Workstation Activity เป็นอย่างน้อย

4.3.8. ผู้ให้เช่ามีหน้าที่สนับสนุน และดำเนินการปิดหรือลดช่องโหว่ ตามที่ กพท. แจ้ง (ถ้ามี) โดย กพท. จะใช้เครื่องมือของ กพท. ในการตรวจสอบช่องโหว่ของระบบของผู้ให้เช่า และจะแจ้งให้ทราบเป็นลายลักษณ์อักษร เพื่อให้ผู้ให้เช่าดำเนินการปิดหรือลดช่องโหว่ ต่อไป

4.3.9. หากซอฟต์แวร์หรือระบบที่เกี่ยวข้องทั้งหมดหรือบางส่วนของโครงการมีปัญหา ผู้ให้เช่าจะต้องแก้ไขให้แล้วเสร็จภายใน 6 ชั่วโมง นับจากที่ได้รับแจ้งจาก กพท.

4.4 ผู้ให้เช่าต้องจัดฝึกอบรมการบริหารจัดการและการใช้งานระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) ให้แก่สำนักงาน รายละเอียดอย่างน้อย ดังนี้

4.4.1. ก่อนการฝึกอบรม ผู้ให้เช่าต้องจัดทำคู่มือการบริหารจัดการและการใช้งานซอฟต์แวร์และระบบที่เกี่ยวข้องทั้งหมด ในรูปแบบรูปเล่มและ Soft file เพื่อให้ผู้ดูแลระบบใช้ประกอบการฝึกอบรม โดยต้องมีหัวข้อและรายละเอียดในคู่มือตามหัวข้อการฝึกอบรมเป็นอย่างน้อย

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ

4.4.2. ผู้ให้เช่าต้องจัดฝึกอบรมเชิงปฏิบัติการ การบริหารจัดการระบบ Endpoint Protection (Endpoint Detection and Response หรือ EDR) ให้แก่ผู้ดูแลระบบของ กพท. อย่างน้อย 5 วัน และมีผู้เข้าอบรมจำนวนไม่น้อยกว่า 4 คน ทั้งนี้สามารถอบรมในรูปแบบ online หรือ onsite ขึ้นอยู่กับสถานการณ์ที่เหมาะสมและเป็นไปตามที่ กพท. กำหนด

4.4.3. หัวข้อการฝึกอบรมต้องมีอย่างน้อยดังนี้

(1) แนะนำระบบ EDR (Introduction to EDR)
- ภาพรวมและการทำงานของระบบ EDR

(2) สถาปัตยกรรมและการติดตั้ง EDR (EDR Architecture and Deployment)
- องค์ประกอบของระบบ EDR
- การติดตั้งในสภาพแวดล้อม และระบบปฏิบัติการต่าง ๆ
- การวางแผนติดตั้ง: ข้อกำหนดเครือข่ายและความเข้ากันได้
- การถอนการติดตั้ง
- Lab/Workshop: ติดตั้ง agents บนอุปกรณ์ทดสอบ
- Lab/Workshop: การถอนการติดตั้ง agents บนอุปกรณ์ทดสอบ

(3) การจัดการสิทธิ์และการเข้าถึง (Access and Permissions Management)
- การกำหนดบทบาทและสิทธิ์สำหรับผู้ใช้และผู้ดูแลระบบ
- Lab/Workshop: ตั้งค่าบทบาทและสิทธิ์ในระบบ EDR

(4) การกำหนดค่าและบริหารจัดการนโยบาย (Policy Configuration and Management)
- การสร้างและปรับแต่งนโยบายการตรวจจับ
- การตั้งค่าการตอบสนอง เช่น การกักกันหรือการแยกตัว
- การปรับแต่งนโยบายเพื่อลด False Positives
- Lab/Workshop: ตั้งค่านโยบายการตรวจจับและตอบสนอง

(5) การบูรณาการ Threat Intelligence (Threat Intelligence Integration) (ถ้ามี)
- การใช้ข้อมูล Threat Intelligence ที่มีอยู่ในระบบ
- การเพิ่ม Threat Feeds ภายนอกเข้าสู่ระบบ EDR
- Lab/Workshop: บูรณาการ Threat Feeds และวิเคราะห์ผล

(6) การตรวจสอบแบบเรียลไทม์ (Real-Time Monitoring)
- การทำงานของ Dashboard และการจัดการการแจ้งเตือน
- การจัดลำดับความสำคัญและการวิเคราะห์การแจ้งเตือน

(7) การตรวจจับและการวิเคราะห์ (Detection and Analysis)
- การตรวจสอบการแจ้งเตือนและวิเคราะห์เหตุการณ์
- การใช้ Behavioral Analytics ในการตรวจจับภัยขั้นสูง
- เทคนิคการวิเคราะห์ต้นเหตุและการตรวจสอบเชิงนิติวิทยาศาสตร์

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ

(8) แนวทางปฏิบัติในการตอบสนองเหตุการณ์ (Incident Response Best Practices)
- ขั้นตอนการควบคุม กำจัด และกู้คืนระบบ
- การใช้ระบบอัตโนมัติเพื่อการตอบสนองที่รวดเร็ว
- Lab/Workshop: ตรวจสอบและตอบสนองต่อเหตุการณ์จำลอง

(9) การค้นหาภัยคุกคามเชิงรุก (Proactive Threat Hunting)
- การใช้เครื่องมือ EDR ในการค้นหาภัยคุกคาม
- การสร้าง Query ขั้นสูงเพื่อตรวจจับภัยที่ซ่อนอยู่
- Lab/Workshop: ค้นหาภัยคุกคามในระบบโดยใช้เครื่องมือ EDR

(10) การบูรณาการ EDR กับเครื่องมือความปลอดภัยอื่น ๆ (EDR Integration with Other Security Tools)
- การบูรณาการ EDR กับ SIEM, SOAR, และ ITSM
- การตั้งค่า API สำหรับงานอัตโนมัติและการปรับแต่ง

(11) ความสามารถขั้นสูงของฟีเจอร์อื่น ๆ (Additional Advanced Capabilities)
- การเปิดใช้งานและการทำงานของฟีเจอร์ขั้นสูงอื่น ๆ เช่น Extended Detection and Response หรือ XDR (Cross-layer Detection และ Advanced Analytics)

(12) การทำงานอัตโนมัติขั้นสูงและ Playbooks (Advanced Automation and Playbooks) หรือ Automation Rule
- การตั้งค่า Workflow หรือ Automation Rule อัตโนมัติสำหรับการจัดการเหตุการณ์
- การสร้าง Playbook หรือ Automation Rule เพื่อลดงานที่ซ้ำซ้อน
- Lab/Workshop: ตั้งค่า Workflow อัตโนมัติ และสร้าง Playbook หรือการตั้งค่า Automation Rule

(13) การรายงาน (Reporting)
- การสร้างและปรับแต่งรายงาน
- Lab/Workshop: สร้างและปรับแต่งรายงาน

5. กำหนดเวลาส่งมอบพัสดุ

5.1. ผู้ให้เช่าต้องส่งมอบลิขสิทธิ์ซอฟต์แวร์ ฯ จำนวน 670 Licenses ระยะเวลาเช่า 24 เดือน เริ่มตั้งแต่วันที่ 1 มกราคม 2568 ถึงวันที่ 31 ธันวาคม 2569

5.2. ผู้ให้เช่าต้องส่งมอบลิขสิทธิ์ซอฟต์แวร์ ฯ จำนวน 130 Licenses ระยะเวลาเช่า 22 เดือน เริ่มตั้งแต่วันที่ 1 มีนาคม 2568 ถึงวันที่ 31 ธันวาคม 2569

6. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

เกณฑ์ราคา

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ

7. วงเงินงบประมาณ

งบประมาณทั้งสิ้นจำนวน 4,386,000,00 บาท (สี่ล้านสามแสนแปดหมื่นหกพันบาทถ้วน) ผูกพันงบประมาณประจำปี 2568 จำนวน 2,193,000.00 บาท (สองล้านหนึ่งแสนเก้าหมื่นสามพันบาทถ้วน) และผูกพันงบประมาณประจำปี 2569 จำนวนเงิน 2,193,000.00 บาท (สองล้านหนึ่งแสนเก้าหมื่นสามพันบาทถ้วน) ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายอื่นทั้งปวงไว้ด้วยแล้ว

8. งวดงานและการจ่ายเงิน

สำนักงานการบินพลเรือนแห่งประเทศไทย จะแบ่งจ่ายเงินค่าเช่าเป็นจำนวน 8 งวด โดยจะชำระเงินเมื่อมีการส่งมอบงานเอกสารหลักฐานต่าง ๆ และคณะกรรมการตรวจรับฯ ได้ดำเนินการตรวจรับ และเห็นว่าถูกต้องครบถ้วนตามรายละเอียดในสัญญาเช่าทุกประการ รายละเอียดดังนี้

งวดที่ 1 เดือนที่ 1-3 เบิกจ่ายร้อยละ 9 โดยผู้ให้เช่าต้องดำเนินการดังนี้

- ผู้ให้เช่าส่งมอบลิขสิทธิ์ซอฟต์แวร์ Endpoint protection พร้อมเอกสารรายละเอียดใบอนุญาตลิขสิทธิ์ซอฟต์แวร์ ตามข้อ 4.1.1 (ระยะเวลาใช้งาน 24 เดือน)
- ผู้ให้เช่าส่งมอบลิขสิทธิ์ซอฟต์แวร์ Endpoint protection พร้อมเอกสารรายละเอียดใบอนุญาตลิขสิทธิ์ซอฟต์แวร์ ตามข้อ 4.1.2 (ระยะเวลาใช้งาน 22 เดือน)
- ผู้ให้เช่าดำเนินการติดตั้ง ดูแล บำรุงรักษา แก้ไขระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) และให้บริการต่าง ๆ ตามข้อ 4.3
- ผู้ให้เช่าต้องรวบรวมและส่งมอบรายงานประจำเดือน (Monthly Report) ตลอดทั้งงวดงาน ตามข้อ 4.3.5
- ผู้ให้เช่าดำเนินการจัดฝึกอบรมและส่งมอบหลักฐานการฝึกอบรม ตามข้อ 4.4
- ผู้ให้เช่าส่งมอบคู่มือการบริหารจัดการและการใช้งานซอฟต์แวร์ ตามข้อ 4.4.1
- ผู้ให้เช่าส่งมอบรายงานผลการสนับสนุน และดำเนินการปิดหรือลดช่องโหว่ ตามที่ กพท. แจ้ง ตามข้อ 4.3.8 (ถ้ามี)

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ตรวจรับงานเรียบร้อยแล้ว

งวดที่ 2 เดือนที่ 4-6 เบิกจ่ายร้อยละ 13 โดยผู้ให้เช่าต้องดำเนินการดังนี้

- ผู้ให้เช่าดำเนินการติดตั้ง ดูแล บำรุงรักษา แก้ไขระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) และให้บริการต่าง ๆ ตามข้อ 4.3
- ผู้ให้เช่าต้องรวบรวมและส่งมอบรายงานประจำเดือน (Monthly Report) ตลอดทั้งงวดงาน ตามข้อ 4.3.5
- ผู้ให้เช่าส่งมอบรายงานผลการสนับสนุน และดำเนินการปิดหรือลดช่องโหว่ ตามที่ กพท. แจ้ง ตามข้อ 4.3.8 (ถ้ามี)

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ตรวจรับงานเรียบร้อยแล้ว

งวดที่ 3 เดือนที่ 7-9 เบิกจ่ายร้อยละ 13 โดยผู้ให้เช่าต้องดำเนินการดังนี้

- ผู้ให้เช่าดำเนินการติดตั้ง ดูแล บำรุงรักษา แก้ไขระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) และให้บริการต่าง ๆ ตามข้อ 4.3
- ผู้ให้เช่าต้องรวบรวมและส่งมอบรายงานประจำเดือน (Monthly Report) ตลอดทั้งงวดงาน ตามข้อ 4.3.5
- ผู้ให้เช่าส่งมอบรายงานผลการสนับสนุน และดำเนินการปิดหรือลดช่องโหว่ ตามที่ กพท. แจ้ง ตามข้อ 4.3.8 (ถ้ามี)

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ตรวจรับงานเรียบร้อยแล้ว

งวดที่ 4 เดือนที่ 10-12 เบิกจ่ายร้อยละ 13 โดยผู้ให้เช่าต้องดำเนินการดังนี้

- ผู้ให้เช่าดำเนินการติดตั้ง ดูแล บำรุงรักษา แก้ไขระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) และให้บริการต่าง ๆ ตามข้อ 4.3
- ผู้ให้เช่าต้องรวบรวมและส่งมอบรายงานประจำเดือน (Monthly Report) ตลอดทั้งงวดงาน ตามข้อ 4.3.5
- ผู้ให้เช่าส่งมอบรายงานผลการสนับสนุน และดำเนินการปิดหรือลดช่องโหว่ ตามที่ กพท. แจ้ง ตามข้อ 4.3.8 (ถ้ามี)

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ตรวจรับงานเรียบร้อยแล้ว

งวดที่ 5 เดือนที่ 13-15 เบิกจ่ายร้อยละ 13 โดยผู้ให้เช่าต้องดำเนินการดังนี้

- ผู้ให้เช่าดำเนินการติดตั้ง ดูแล บำรุงรักษา แก้ไขระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) และให้บริการต่าง ๆ ตามข้อ 4.3
- ผู้ให้เช่าต้องรวบรวมและส่งมอบรายงานประจำเดือน (Monthly Report) ตลอดทั้งงวดงาน ตามข้อ 4.3.5
- ผู้ให้เช่าส่งมอบรายงานผลการสนับสนุน และดำเนินการปิดหรือลดช่องโหว่ ตามที่ กพท. แจ้ง ตามข้อ 4.3.8 (ถ้ามี)

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ตรวจรับงานเรียบร้อยแล้ว

งวดที่ 6 เดือนที่ 16-18 เบิกจ่ายร้อยละ 13 โดยผู้ให้เช่าต้องดำเนินการดังนี้

- ผู้ให้เช่าดำเนินการติดตั้ง ดูแล บำรุงรักษา แก้ไขระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) และให้บริการต่าง ๆ ตามข้อ 4.3

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ

- ผู้ให้เช่าต้องรวบรวมและส่งมอบรายงานประจำเดือน (Monthly Report) ตลอดทั้งงวดงาน ตามข้อ 4.3.5

- ผู้ให้เช่าส่งมอบรายงานผลการสนับสนุน และดำเนินการปิดหรือลดช่องโหว่ ตามที่ กพท. แจ้ง ตามข้อ 4.3.8 (ถ้ามี)

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ตรวจรับงานเรียบร้อยแล้ว

งวดที่ 7 เดือนที่ 19-21 เบิกจ่ายร้อยละ 13 โดยผู้ให้เช่าต้องดำเนินการดังนี้

- ผู้ให้เช่าดำเนินการติดตั้ง ดูแล บำรุงรักษา แก้ไขระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) และให้บริการต่าง ๆ ตามข้อ 4.3

- ผู้ให้เช่าต้องรวบรวมและส่งมอบรายงานประจำเดือน (Monthly Report) ตลอดทั้งงวดงาน ตามข้อ 4.3.5

- ผู้ให้เช่าส่งมอบรายงานผลการสนับสนุน และดำเนินการปิดหรือลดช่องโหว่ ตามที่ กพท. แจ้ง ตามข้อ 4.3.8 (ถ้ามี)

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ตรวจรับงานเรียบร้อยแล้ว

งวดที่ 8 (งวดสุดท้าย) เดือนที่ 22-24 เบิกจ่ายร้อยละ 13 โดยผู้ให้เช่าต้องดำเนินการดังนี้

- ผู้ให้เช่าดำเนินการติดตั้ง ดูแล บำรุงรักษา แก้ไขระบบป้องกันความปลอดภัยเครื่องคอมพิวเตอร์ (Endpoint Protection) และให้บริการต่าง ๆ ตามข้อ 4.3

- ผู้ให้เช่าต้องรวบรวมและส่งมอบรายงานประจำเดือน (Monthly Report) ตลอดทั้งงวดงาน ตามข้อ 4.3.5

- ผู้ให้เช่าส่งมอบรายงานผลการสนับสนุน และดำเนินการปิดหรือลดช่องโหว่ ตามที่ กพท. แจ้ง ตามข้อ 4.3.8 (ถ้ามี)

ในรูปแบบเอกสารและไฟล์เอกสาร (USB Drive) จำนวน 1 ชุด และคณะกรรมการตรวจรับได้ตรวจรับงานเรียบร้อยแล้ว

9. อัตราค่าปรับ

ค่าปรับตามแบบสัญญาเช่าหรือข้อตกลงเป็นหนังสือ ให้คิดในอัตราร้อยละ 0.10 ของราคาค่าเช่าของที่ยังไม่ได้รับมอบต่อวัน

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ

11. ข้อตกลงห้ามเปิดเผยข้อมูล

ข้อมูล เอกสาร หรือสัญญาที่เกี่ยวข้องกับโครงการนี้ทั้งหมดที่ กพท. จัดหาให้ หรือผู้ให้เช่าดำเนินการและจัดหาให้ กพท. ถือเป็นความลับ และเป็นสมบัติของ กพท. โดยผู้ให้เช่าต้องไม่เปิดเผยข้อมูลและผลการดำเนินการให้แก่ผู้ใด ยกเว้นแต่จะได้รับอนุญาตจาก กพท. เป็นลายลักษณ์อักษร หากผู้ให้เช่าละเมิดโดยมีการนำไปเผยแพร่ และเปิดเผยโดยไม่ได้รับอนุญาต กพท. มีสิทธิ์ฟ้องร้องเรียกค่าเสียหายและดำเนินการตามกฎหมายได้

12. ความคุ้มครองเกี่ยวกับลิขสิทธิ์

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องใด ๆ ว่ามีการละเมิดลิขสิทธิ์เกี่ยวกับงานเช่าตามสัญญานี้ โดย กพท. มิได้แก้ไขดัดแปลงไปจากเดิม ผู้ให้เช่าจะต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว เพื่อให้ กพท. สามารถใช้งานเช่านั้นต่อไปได้ หากผู้ให้เช่ามิอาจกระทำได้และ กพท. ต้องรับผิดชอบชดใช้ค่าเสียหายต่อบุคคลภายนอก เนื่องจากผลแห่งการละเมิดลิขสิทธิ์ดังกล่าว ผู้ให้เช่าต้องเป็นผู้ชำระค่าเสียหาย ค่าปรับและค่าใช้จ่ายอื่น ๆ รวมทั้งค่าธรรมเนียม และค่าทนายความ ทั้งนี้ กพท. จะแจ้งผู้ให้เช่าทราบเป็นลายลักษณ์อักษรในเมื่อได้มีการกล่าวอ้างหรือใช้สิทธิเรียกร้องดังกล่าว โดยไม่ชักช้า

13. เงื่อนไขอื่น ๆ

ผู้ให้เช่าต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายคุ้มครองข้อมูลส่วนบุคคล และประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กพท. รวมถึงกฎหมาย นโยบาย คำสั่งและขั้นตอนปฏิบัติอื่น ๆ ที่เกี่ยวข้อง

14. หน่วยงานผู้รับผิดชอบโครงการ

ฝ่ายบริหารเทคโนโลยีดิจิทัล กองพัฒนามาตรฐานการจัดการและความปลอดภัยไซเบอร์ สำนักงานการบินพลเรือนแห่งประเทศไทย 222 ซอยวิภาวดีรังสิต 28 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพมหานคร 10900 โทร. 0 2568 8808 อีเมล์ itd_is@caat.or.th

(นางสาวอรวรรณ ใจเอื้อ)	(นายศราวุธ กิติศรีวรพันธุ์)	(นายมนต์ชัย เชาวะปรีชากุล)	(นายคณิตสรณ์ พินทุสรศรี)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรรมการ