รายละเอียดคุณลักษณะเฉพาะของพัสดุ
เพื่อจัดซื้อจัดหาระบบรักษาความปลอดภัยของระบบเครือข่าย กพท.

1. ความเป็นมา

ปัจจุบันระบบและซอฟต์แวร์บางส่วนที่ใช้งานในด้านการรักษาความปลอดภัยต่อโครงสร้างพื้นฐานระบบเครือข่ายของสำนักงานการบินพลเรือนแห่งประเทศไทย (กพท.) ได้เข้าสู่สถานะ End of Support (EOS) ซึ่งหมายถึงระบบและซอฟต์แวร์ได้ถูกใช้งานมาเป็นเวลานานจนถึงจุดที่ผู้ผลิตยกเลิกการให้การสนับสนุน ทั้งในด้านการอัปเดตความปลอดภัย (Security Patch) การแก้ไขปัญหาที่เกิดขึ้น (Bug Fixes) และการรับซ่อมบำรุงรักษา (Corrective and Preventive Maintenance) โครงการนี้จึงถูกจัดทำขึ้นเพื่อจัดซื้อระบบ อุปกรณ์และซอฟต์แวร์รุ่นใหม่ที่ทันสมัย ทดแทนระบบและซอฟต์แวร์ที่หมดอายุการใช้งานไปแล้ว อาทิ Next Generation Firewall, Switch, และ Central Log Management รวมถึงเพิ่มประสิทธิภาพในการป้องกันและตอบสนองภัยคุกคามบนระบบเครือข่ายที่ซับซ้อน อาทิ Network Detection and Response (NDR), Network Sensor, Network Monitoring Tool อีกทั้งยังจัดซื้อระบบเครื่องแม่ข่ายแบบ Hyper-Converged Infrastructure (HCI) เพื่อรองรับการใช้งาน NTP Server, NDR, Backup server และรองรับการขยายตัวของระบบงานต่างๆ ของ กพท. ที่จะเกิดขึ้นในอนาคตได้อย่างมีประสิทธิภาพ โดย HCI สามารถจัดสรรทรัพยากรภายในระบบแบบอัตโนมัติ เพื่อให้ภาพรวมของระบบทำงานได้อย่างเสถียรมากที่สุด

ทั้งนี้ การจัดซื้อระบบดังกล่าว ยังเป็นการปฏิบัติตามมาตรการขั้นต่ำในการป้องกัน มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ สอดคล้องตาม มาตรา 54 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 รวมถึง มาตรา 37 (1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 อีกทั้ง การเก็บและรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของระบบ Central Log ยังเป็นการปฏิบัติตาม มาตรา 26 วรรคสาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

2. วัตถุประสงค์

2.1 ทดแทนระบบที่ถูกใช้งานมาเป็นเวลานานจนถึงจุดที่ผู้ผลิตยกเลิกการให้การสนับสนุน (End of Support: EOS) ซึ่งเป็นการลดความเสี่ยงจากช่องโหว่ที่เกิดจากการใช้งานระบบที่ล้าสมัย

2.2 เพิ่มประสิทธิภาพด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบเครือข่ายของ กพท. โดยใช้ระบบที่ทันสมัยป้องกันและตอบสนองต่อภัยคุกคามที่ซับซ้อนในปัจจุบัน

2.3 รองรับการขยายตัวของระบบงานต่าง ๆ ของ กพท. ในอนาคต เพื่อให้ภาพรวมระบบงานของทั้ง กพท. สามารถทำงานได้อย่างมีเสถียรภาพ

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

2.4 เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และการรักษาความมั่นคงปลอดภัยไซเบอร์ ของ กพท. สอดคล้องและเป็นไปตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

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 มีคุณสมบัติหรือลักษณะต้องห้ามอื่นตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้าง 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

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในหนังสือเชิญชวน

3.10.3 การยื่นข้อเสนอของกิจการร่วมค้า

(1) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

(2) การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ 3.10.3 (1) ดำเนินการซื้อและดาวน์โหลดเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารจึงจะมีสิทธิในการเข้ายื่นข้อเสนอในนามกิจการร่วมค้าได้

3.11 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (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 ต้องมีทุนจดทะเบียนไม่ต่ำกว่า 3 ล้านบาท

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

3.12.4 กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการ หรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

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

(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 ไม่ใช้ข้อบังคับกับกรณีดังต่อไปนี้

3.13.1 กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

3.13.2 นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการ ตามพระราชบัญญัติล้มละลาย พ.ศ. 2483 และที่แก้ไขเพิ่มเติม

3.13.3 งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงาน ก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้าง ที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

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 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นเอกสารรับรองขณะเข้าเสนอราคา (ข้อ 4.1, 4.2, 4.5 และ 4.8)

4. รายละเอียดคุณลักษณะเฉพาะของพัสดุ

4.1 **อุปกรณ์รักษาความปลอดภัยระดับเครือข่าย (Next Generation Firewall) จำนวน 2 ชุด ติดตั้งในรูปแบบ Appliance มีคุณสมบัติอย่างน้อยดังนี้**

4.1.1 มี Firewall Throughput ไม่น้อยกว่า 70 Gbps และ Threat Protection Throughput ไม่น้อยกว่า 10 Gbps

4.1.2 รองรับการสร้าง session พร้อมกันสูงสุดไม่น้อยว่า 500,000 New session/second หรือ New Connection/second

4.1.3 รองรับการใช้งาน session พร้อมกันสูงสุดไม่น้อยกว่า 7,000,000 Concurrent sessions หรือ Concurrent connections

4.1.4 อุปกรณ์ต้องมี SSD สำหรับเก็บข้อมูลระบบไม่น้อยกว่า 480 GB

4.1.5 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 8 ช่อง

4.1.6 มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1 Gbps (SFP) หรือ 10 Gbps (SFP+) จำนวนไม่น้อยกว่า 8 ช่อง พร้อมเสนออุปกรณ์ Module สำหรับช่องเชื่อมต่อแบบ 10G SFP+ SR จำนวนไม่น้อยกว่า 4 Port

4.1.7 รองรับการทำ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้เป็นอย่างน้อย

4.1.8 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS และ SSH ได้เป็นอย่างน้อย

4.1.9 สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่าง ๆ อย่างน้อย ดังนี้ Syn Flood, UDP Flood, ICMP Flood, ARP Spoofing, Port Scan, DoS หรือ DDoS, Teardrop Attack, Land Attack, IP Fragment เป็นต้นได้เป็นอย่างน้อย

4.1.10สามารถป้องกันภัยคุกคามประเภท Virus, Vulnerability Protection, Spyware และมีระบบตรวจจับ Malware แบบ AI เพื่อใช้ ป้องกัน Malware ประเภทใหม่ (Zero-day Malware) เป็นอย่างน้อย

4.1.11 มีฟังก์ชันระบบป้องกันการบุกรุก (Intrusion Prevention System: IPS) ที่ทำงานโดยใช้ฐานข้อมูลลายเซ็น (Signatures Database) ร่วมกับการวิเคราะห์ข้อมูลบนคลาวด์ (Cloud-Based Analysis Engine) หรือ Cloud Sandbox และต้องสามารถอ้างอิงฐานข้อมูลช่องโหว่ (Common Vulnerabilities and Exposures: CVE) หรือมาตรฐานที่เทียบเท่าได้

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

4.1.12 สามารถทำ Web Application Firewall เพื่อตรวจสอบ และป้องกันการโจมตี Web Application Server เช่น SQL Injection ได้เป็นอย่างน้อย หรือเสนอระบบเพิ่มเติมได้

4.1.13 สามารถทำงานลักษณะ Transparent Mode เพื่อใช้งานกับเครือข่ายเดิมได้ โดยไม่มีผลกระทบกับระบบ Network เดิม

4.1.14 สามารถทำรายงานการถูกโจมตีได้ในรูปแบบ HTML หรือ PDF หรือ XLS ได้เป็นอย่างน้อย

4.1.15 สามารถส่งข้อมูลต่าง ๆ ไปเก็บยังอุปกรณ์เก็บบันทึก logs (Syslog Server) หรืออุปกรณ์อื่นเพื่อเป็นการเก็บสถิติ ตรวจสอบ หรือทำรายงาน log ได้เป็นอย่างน้อย

4.1.16 สามารถสร้าง Security Policy โดยใช้ URL ,IP Address ,Range IP Address และ MAC Address ได้เป็นอย่างน้อย

4.1.17 รองรับการทำงานแบบ High Availability ชนิด Active-Standby ได้เป็นอย่างน้อย

4.1.18 สามารถใช้งานตามมาตรฐาน IPv4 และ IPv6 ได้เป็นอย่างน้อย

4.1.19 สามารถทำ Routing แบบ Static, Dynamic Routing ได้เป็นอย่างน้อย

4.1.20 สามารถทำ SD-WAN (Software-Defined Wide Area Network) ได้

4.1.21 สามารถรองรับการเชื่อมต่อแบบ Remote Access VPN ผ่าน IPsec หรือ SSL-VPN พร้อมกันไม่น้อยกว่า 730 Concurrent Connections หรือ Concurrent sessions/User โดยไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม

4.1.22 มีแหล่งจ่ายไฟ (Power Supply) แบบ Redundant สามารถทำ Hot Swap หรือ Hot-Plug ได้ไม่น้อยกว่า จำนวน 2 หน่วย

4.1.23 บริษัทผู้นำเสนอจะต้องได้รับการแต่งตั้งอย่างเป็นทางการจากเจ้าของผลิตภัณฑ์

4.1.24 มีการรับประกันสินค้าจากเจ้าของผลิตภัณฑ์ทั้งในส่วนซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) รวมทั้งสิทธิ์ในการอัปเกรดระบบที่นำเสนอเป็นเวลาไม่น้อยกว่า 1 ปี

4.2 **เครื่องคอมพิวเตอร์แม่ข่ายสำหรับติดตั้งระบบ Hyper Converged Infrastructure จำนวน 2 ชุด โดยแต่ละชุดมีคุณสมบัติอย่างน้อยดังนี้**

4.2.1 เป็นเครื่องคอมพิวเตอร์แม่ข่ายที่มีสถาปัตยกรรมแบบ Hyper-Converged Infrastructure (HCI)

4.2.2 มีหน่วยประมวลผลกลาง (CPU) แบบ 16 แกนหลัก (16 core) หรือดีกว่า มีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2.4 GHz จำนวน 2 หน่วย

4.2.3 มีหน่วยความจำหลัก (Memory) ชนิด DDR4 หรือดีกว่า ขนาดไม่น้อยกว่า 768 GB

4.2.4 มีหน่วยจัดเก็บข้อมูล Solid State Drive ที่มีความจุ ไม่น้อยกว่า 480 GB สำหรับติดตั้งระบบปฏิบัติการ Hyper Converged Infrastructure โดยสามารถทำงานแบบ RAID 1 ได้เป็นอย่างน้อย จำนวน 2 หน่วย

4.2.5 มีหน่วยจัดเก็บข้อมูลแบบ Solid State Drive ที่มีความจุ ไม่น้อยกว่า 3.8 TB จำนวนไม่น้อยกว่า 4 หน่วย

4.2.6 มีหน่วยจัดเก็บข้อมูลแบบจานหมุนที่มีความจุ ไม่น้อยกว่า 12 TB มีความเร็วรอบไม่น้อยกว่า 7,200 รอบต่อนาที จำนวนไม่น้อยกว่า 8 หน่วย

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

4.2.7 มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10 Gbps (SFP+) หรือดีกว่า พร้อม Transceiver Module จำนวนไม่น้อยกว่า 4 ช่อง

4.2.8 มีแหล่งจ่ายไฟ (Power Supply) แบบ Redundant สามารถทำ Hot Swap หรือ Hot-Plug ได้ จำนวน 2 หน่วย

4.2.9 เครื่องคอมพิวเตอร์แม่ข่ายที่เสนอผ่านการรับรองมาตรฐาน เช่น FCC หรือ TUV หรือ CE เป็นอย่างน้อย

4.2.10 สามารถทำ VM HA (High Availability) เพื่อให้ VM ทำงานได้อย่างต่อเนื่องในกรณีที่มี Node Down

4.2.11 สามารถย้าย VM ไปยัง Node อื่นได้ตามความเหมาะสมเพื่อรักษาประสิทธิภาพการทำงานของระบบได้โดยอัตโนมัติ เมื่อ Node ถูกใช้ CPU หรือ Memory มากเกินกว่าสัดส่วนที่กำหนดไว้

4.2.12 สามารถเพิ่ม Resource ในส่วนของ CPU และ Memory ไปยัง VM แบบอัตโนมัติ เมื่อ VM ถูกใช้ CPU หรือ Memory มากเกินกว่าที่กำหนดไว้

4.2.13 สามารถทำสำเนาข้อมูลแบบ 2 ชุดให้กับแต่ละ VM เพื่อลดความเสี่ยงไม่ให้เกิดการสูญหายของข้อมูลในกรณี Hard Disk ชำรุด

4.2.14 ระบบที่เสนอมีความสามารถในการสำรองข้อมูลแบบ Scheduled Backup ได้แก่ Weekly, Daily โดยสามารถกำหนดระยะเวลาการเก็บรักษาข้อมูล (Retention Period) เป็นเวลาอย่างน้อย 1 ปี และสามารถเก็บข้อมูลไปยัง External Storage ผ่านโปรโตคอล iSCSI และ Fiber Channel (FC) ได้เป็นอย่างน้อย โดยไม่จำกัดจำนวน VM ที่ต้องการสำรองข้อมูล หรือเสนอซอฟต์แวร์ที่มีความสามารถเทียบเท่า

4.2.15 มีความสามารถหรือมีซอฟต์แวร์บริหารจัดการระบบเครือข่ายเสมือน (Virtual Network) เช่น Virtual Switch, Distributed Firewall ได้เป็นอย่างน้อย

4.2.16 บริษัทผู้นำเสนอจะต้องได้รับการแต่งตั้งอย่างเป็นทางการจากเจ้าของผลิตภัณฑ์

4.2.17 มีการรับประกันสินค้าจากเจ้าของผลิตภัณฑ์ทั้งในส่วนซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) รวมทั้งสิทธิ์ในการอัปเกรดระบบที่นำเสนอเป็นเวลาไม่น้อยกว่า 1 ปี

4.3 **อุปกรณ์กระจายสัญญาณ (L3 Switch) ขนาด 48 ช่อง จำนวน 2 ชุด มีคุณสมบัติอย่างน้อยดังนี้**

4.3.1 มีลักษณะการทำงานไม่น้อยกว่า Layer 3 ของ OSI Model

4.3.2 สามารถค้นหาเส้นทางเครือข่ายโดยใช้โปรโตคอล (Routing Protocol) RIPv2, OSPF ได้เป็นอย่างน้อย

4.3.3 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 RJ45 หรือดีกว่า จำนวนไม่น้อยกว่า 48 ช่อง

4.3.4 มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1/10 Gbps (SFP/SFP+) พร้อม Transceiver Module จำนวนไม่น้อยกว่า 4 ช่อง หรือดีกว่า

4.3.5 มี Switch Capacity ไม่น้อยกว่า 200Gbps

4.3.6 มีสัญญาณไฟแสดงสถานะของการทำงานช่องเชื่อมต่อระบบเครือข่ายทุกช่อง

4.3.7 รองรับ Mac Address ได้ไม่น้อยกว่า 32,000 Mac Address

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

4.3.8 สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser ได้เป็นอย่างน้อย

4.3.9 สามารถส่งข้อมูล Log File ในรูปแบบ Syslog ได้เป็นอย่างน้อย

4.3.10 สามารถใช้งานตามมาตรฐาน IPv6 ได้

4.3.11 มีการรับประกันสินค้าจากเจ้าของผลิตภัณฑ์ทั้งในส่วนซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) รวมทั้งสิทธิ์ในการอัปเกรดระบบที่นำเสนอเป็นเวลาไม่น้อยกว่า 1 ปี

4.4 **อุปกรณ์สำหรับจัดเก็บข้อมูลแบบภายนอก (External Storage) จำนวน 1 ชุด มีคุณสมบัติอย่างน้อยดังนี้**

4.4.1 เป็นอุปกรณ์ที่ทำหน้าที่จัดเก็บข้อมูลและบริหารการทำงานจากส่วนกลาง (Central Management System) สามารถติดตั้งบนตู้ Rack ขนาด 19 นิ้วได้เป็นอย่างน้อย

4.4.2 มีหน่วยประมวลผลกลางไม่น้อยกว่า 8 แกนหลัก ประมวลผลแบบ 64 บิต ความถี่ของสัญญาณนาฬิกาไม่น้อยกว่า 2.1 GHz หรือดีกว่า

4.4.3 มีหน่วยจัดเก็บข้อมูล ชนิด SATA หรือ SAS หรือดีกว่า ขนาดความจุไม่น้อยกว่า 12 TB จำนวนไม่น้อยกว่า 6 หน่วย

4.4.4 มีหน่วยความจำหลัก (RAM) ขนาดไม่น้อยกว่า 16 GB ประเภท DDR4 ECC หรือดีกว่า มีช่องใส่หน่วยความจำหลัก ไม่น้อยกว่า 4 หน่วย สามารถขยายความจุที่ 128 GB หรือมากกว่า

4.4.5 สามารถติดตั้ง Hard Disk ได้สูงสุด 12 หน่วย

4.4.6 สามารถทำงาน แบบ Raid ไม่น้อยกว่า Raid 0, 1, 5

4.4.7 มีพอร์ตเชื่อมต่อแบบ 1G จำนวนไม่น้อยกว่า 4 พอร์ต

4.4.8 มีพอร์ตเชื่อมต่อแบบ 10G จำนวนไม่น้อยกว่า 2 พอร์ต

4.4.9 รองรับการทำงานผ่านโพรโตคอล อย่างน้อยดังนี้ SMB , FTP , SNMP เป็นต้น

4.4.10 รองรับการใช้งานผ่านระบบเครือข่าย IPv4 ได้เป็นอย่างน้อย

4.4.11 มีการรับประกันสินค้าจากเจ้าของผลิตภัณฑ์ทั้งในส่วนซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) รวมทั้งสิทธิ์ในการอัปเกรดระบบที่นำเสนอเป็นเวลาไม่น้อยกว่า 1 ปี

4.5 **อุปกรณ์ระบบบริหารจัดเก็บข้อมูล Log (Central Log Management) จำนวน 1 ชุด มีคุณสมบัติอย่างน้อยดังนี้**

4.5.1 เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (Logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices, ระบบปฏิบัติการ (OS), Web Server ได้เป็นอย่างน้อย

4.5.2 รองรับระบบ Appliances, ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น ได้ไม่จำกัดจำนวนอุปกรณ์ต่อระบบ โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้เป็นอย่างน้อย

4.5.3 มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน MD5 หรือ SHA-1 หรือดีกว่า

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

4.5.4 สามารถเก็บ Log File ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall, VPN, Server เป็นต้น ได้เป็นอย่างน้อย

4.5.5 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้เป็นอย่างน้อย

4.5.6 สามารถจัดเก็บ log file ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ฉบับที่มีผลบังคับใช้ โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ที่ได้มาตรฐาน เช่น มาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ. 4003.1-2560) เป็นต้น

4.5.7 สามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น External Storage ได้เป็นอย่างน้อย

4.5.8 สามารถจัดเก็บข้อมูลเหตุการณ์ต่อวินาที (Events per Seconds) ได้ไม่น้อยกว่า 30,000 eps

4.5.9 Dashboard มีการแสดงผลเป็นแบบเรียลไทม์ และสามารถทราบสถานการณ์ปัจจุบัน ค่าจำนวน Log แต่ละ Source ภาพรวมการใช้งาน ค่า EPS ที่มีการรับและส่งข้อมูล ปริมาณค่าการใช้งานแรมและซีพียู เป็นต้น

4.5.10 สามารถทำการจัดการสิทธิ์การเข้าใช้งานระบบ Role-Based Access Control (RBAC) Device Setting, User Setting, Log Inspection และ Device Statistics เป็นอย่างน้อย

4.5.11 กำหนดการทำ Log Archive ด้วย สามารถจัดเก็บข้อมูลไฟล์ Log ขนาดใหญ่โดยมีเทคโนโลยีในการบีบอัดไฟล์กว่า 10 เท่า ใช้การ Compressed Files เพื่อลดขนาดไฟล์ดังเดิมได้ ลดพื้นที่การจัดเก็บพื้นที่ฮาร์ดดิสก์ เป็นอย่างน้อย

4.5.12 รองรับการส่งข้อมูลและรับข้อมูลผ่าน Network Protocol UDP และ TCP และสามารถใช้ TLS/SSL Certificate ที่สื่อสารกับอุปกรณ์ต้นทางแบบ Secure Protocol ได้เป็นอย่างน้อย

4.5.13 มีกลไกในการป้องกันการลบ / แก้ไขข้อมูลโดยมิชอบ และ Log Rotate ที่สามารถสำเนาข้อมูล และลบข้อมูลเก่าทิ้ง เพื่อนำเนื้อที่มาจัดเก็บข้อมูลใหม่แบบอัตโนมัติได้เป็นอย่างน้อย

4.5.14 มีความสามารถในการคัดกรอง ข้อความ เนื้อหา ฟิลด์ ของไฟล์ Log เพื่อทำการส่งต่อให้กับ SIEM หรือระบบในทำ AI เพื่อวิเคราะห์ผลต่อไปได้เป็นอย่างน้อย

4.5.15 สามารถค้นหาแบบ Full-Text Search และเป็น Expression Language ได้ โดยสามารถเลือกรูปแบบการค้นหาได้เป็นอย่างน้อย

4.5.16 เมื่อมีปริมาณข้อมูลจำนวนมากมาพร้อมกันอย่างต่อเนื่อง ระบบสามารถแจ้งเตือนให้แก่ผู้ดูแลระบบได้ผ่าน Email หรือ MS-Team ได้เป็นอย่างน้อย

4.5.17 มีหน่วยจัดเก็บข้อมูลที่มีความจุก่อน Format ไม่น้อยกว่า 2 TB จำนวน 3 หน่วย โดยสามารถติดตั้งใช้งาน RAID5 ได้เป็นอย่างน้อย

4.5.18 ต้องสามารถรับปริมาณ Log ได้โดยมีลิขสิทธิ์การใช้งานไม่น้อยกว่า 4 TB โดยไม่จำกัดจำนวน Devices

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

4.5.19 ระบบมีส่วนของการรายงานผลกราฟและตารางข้อมูล โดยมีข้อมูลดังต่อไปนี้เป็นอย่างน้อย Total Log Usage, Top 10 Total Event และผลลัพธ์ที่ได้จากการค้นหา สามารถส่งออก (Export) เป็นไฟล์รูปแบบ CSV ได้เป็นอย่างน้อย

4.5.20 ระบบต้องมีความสามารถแจ้งเตือนผู้ดูแลระบบ หากพบว่าไม่มี Log จากระบบต้นทางส่งมานานเกินเวลาที่กำหนด เป็นอย่างน้อย

4.5.21 ระบบต้องมีความสามารถการทำ Data Retention โดยสามารถปรับแต่งระยะเวลาที่จะจัดเก็บข้อมูลได้

4.5.22 ระบบต้องสามารถส่งต่อ Log ไปยัง Syslog Server อื่นหรืออุปกรณ์ประเภท SIEM ผ่าน Syslog Protocol ได้โดยที่ไม่เปลี่ยนแปลงข้อมูลต้นทาง

4.5.23 บริษัทผู้นำเสนอจะต้องได้รับการแต่งตั้งอย่างเป็นทางการจากเจ้าของผลิตภัณฑ์

4.5.24 มีการรับประกันสินค้าจากเจ้าของผลิตภัณฑ์ทั้งในส่วนซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) รวมทั้งสิทธิ์ในการอัปเกรดระบบที่นำเสนอเป็นเวลาไม่น้อยกว่า 1 ปี

4.6 **ระบบปฏิบัติการ Microsoft Windows Server 2025 (16 Core) จำนวน 4 ลิขสิทธิ์ พร้อมลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย และลิขสิทธิ์ Windows Server User Cal จำนวน 5 ลิขสิทธิ์**

4.7 **ซอฟต์แวร์ระบบตรวจสอบสถานะและเฝ้าระวัง (System Monitoring) จำนวน 1 ชุด มีคุณสมบัติอย่างน้อยดังนี้**

4.7.1 เป็นระบบที่ใช้สำหรับตรวจสอบสถานะการทำงานของ เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายได้ โดยสามารถแสดงสถานะในรูปแบบ Network Diagram และระบบต้องมี Mobile Application ที่รองรับการทำงานบน iOS และ Android เพื่อเข้ามาดูสถานะของอุปกรณ์ที่ทำการติดตามได้เป็นอย่างน้อย

4.7.2 สามารถตรวจสอบสถานภาพและประสิทธิภาพอุปกรณ์ โดยใช้โพรโตคอลมาตรฐาน เช่น SNMPV1, 2c และ 3, ICMP, Telnet, SSH, WMI เป็นต้น

4.7.3 สามารถตรวจสอบสถานภาพ ของอุปกรณ์ เช่น Router, Switch, Firewall, Server, OS Windows Server หรือ OS Linux เป็นต้น

4.7.4 สามารถทำงานได้ทั้งแบบ Agent less หรือ Agent Base

4.7.5 สามารถติดตั้งบนระบบปฏิบัติการ Windows หรือ Linux ได้เป็นอย่างน้อย

4.7.6 สามารถเข้าบริหารจัดการผ่าน Web-Browser และ Application GUI ได้เป็นอย่างน้อย

4.7.7 สามารถแจ้งเตือน (Notification) ไปยังผู้ดูแลระบบผ่าน Email, Syslog Message ได้เป็นอย่างน้อย

4.7.8 สามารถทำการตรวจสอบสถานะของการทำงานของ Virtual Machine ได้ เช่น VMware, Microsoft Hyper-V ได้เป็นอย่างน้อย

4.7.9 สามารถทำการตรวจสอบสถานะของการทำงานของ Mail Server ได้ เช่น การส่ง Mail ไปกลับได้ (Round Trip Email) ได้เป็นอย่างน้อย

4.7.10 สามารถรับและตรวจสอบสถานะข้อมูลโดย Packet Sniffing, SNMP, WMI, HTTP, NetFlow, sFlow, JFlow และ ข้อมูล Syslog ได้เป็นอย่างน้อย

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

4.7.11 มีสิทธิในการใช้งานได้ไม่น้อยกว่า 500 Sensors ระยะเวลาไม่น้อยกว่า 1 ปี

4.8 **ระบบตรวจจับและตอบสนองภัยคุกคามในระบบเครือข่าย (Network Detection and Response: NDR) ที่รองรับได้ทั้งแบบ Appliance (มี Sensor ในตัว) หรือแบบ Distributed (แยก Sensor/Collector และระบบประมวลผล) จำนวน 1 ชุด โดยมีคุณสมบัติต่อชุดดังนี้**

4.8.1 เป็นระบบที่ทำหน้าที่ตรวจจับและตอบสนองภัยคุกคามในระบบเครือข่าย (Network Detection and Response :NDR) โดยเฉพาะและไม่ได้เป็น Next-generation Firewall สามารถบริหารจัดการด้วยการ Monitor, ตั้งค่าและสามารถเป็น Network Sensor รับข้อมูลจากเครือข่ายด้วยวิธี Mirror หรือ SPAN เพื่อนำข้อมูลจากเครือข่ายมาวิเคราะห์ภัยคุกคามหรือนำเสนออุปกรณ์เพิ่มเติมในกรณีที่ระบบบริหารจัดการและ Network Sensor แยกออกจากกัน

4.8.2 สามารถตรวจสอบด้วยข้อมูลด้านพฤติกรรม User and Entity Behavior Analytics (UEBA) หรือ Machine Learning Detection เพื่อเพิ่มความแม่นยำในการตรวจสอบการโจมตีแบบเป็นการโจมตีแบบใหม่ๆ

4.8.3 มีระบบวิเคราะห์จาก Traffic ที่ได้จากเครือข่ายได้ และ มีSoftware ในการตรวจสอบ (Security Engines) เพื่อเพิ่มประสิทธิภาพในการตรวจจับ อย่างน้อยดังนี้

4.8.3.1 สามารถตรวจสอบด้วย Artificial intelligence (AI) เพื่อเพิ่มประสิทธิภาพในการตรวจจับ

4.8.3.2 สามารถตรวจสอบด้วยข้อมูลที่ได้รับ Threat Intelligence ที่เป็นศูนย์กลางรวบรวมข้อมูลภัยคุกคามรูปแบบใหม่ๆ

4.8.3.3 สามารถตรวจสอบด้วยข้อมูลด้านพฤติกรรม User and Entity Behavior Analytics (UEBA) หรือ Machine Learning Detection เพื่อเพิ่มความแม่นยำในการตรวจสอบการโจมตีแบบเป็นการโจมตีแบบใหม่ๆ

4.8.4 มีความสามารถในการตรวจสอบไฟล์ที่ไม่ปลอดภัย ได้แก่ File Threat Detection หรือ Malicious Files หรือ File-based Attack ที่อยู่ภายใน Network ภายในองค์กร

4.8.5 มีความสามารถในการวิเคราะห์ และสร้างความสัมพันธ์การโจมตีภาพด้านไซเบอร์มาตรฐาน Cyber Kill Chain หรือ MITE ATT&CK หรือเทียบเท่า เพื่อใช้เป็นข้อมูลในการตัดสินใจสร้างแนวทางหรือวิธีการในการตอบสนอง (Response) หรือบรรเทาเหตุการณ์การโจมตีที่เกิดขึ้น (Mitigation) ได้เป็นอย่างน้อย

4.8.5.1 สามารถวิเคราะห์และตรวจจับแหล่งที่มาของภัยคุกคาม (patient zero หรือ Entry Point) ได้เป็นอย่างน้อย

4.8.5.2 สามารถเชื่อมโยงการแพร่กระจายหรือการโจมตีของภัยคุกคามที่เกิดขึ้นภายในระบบเครือข่ายได้ในแบบรูปแบบ Diagram Topology หรือ Attack Timeline ได้เป็นอย่างน้อย

4.8.6 สามารถระบุหรือชี้ให้เห็นจุดเสี่ยงของระบบ (Weakness) เช่น Vulnerabilities, Weak Password, Web Traffic หากไม่สามารถรองรับคุณสมบัติดังกล่าวได้ สามารถเสนอระบบ/โมดูลเสริมเพิ่มเติมที่มีความสามารถเทียบเท่า

4.8.7 สามารถกำหนดกระบวนการตอบสนองภัยคุกคามตามเงื่อนไขหรือเหตุการณ์ที่กำหนดและสั่งการไปยังอุปกรณ์รักษาความปลอดภัยระดับเครือข่าย (Next Generation Firewall) ที่นำเสนอในโครงการนี้

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

4.8.8 สามารถออกรายงาน (Security Risk Reports) และแจ้งเตือน (Security Alarms) ผ่าน Email ได้เป็นอย่างน้อย

4.8.9 ต้องรองรับการทำงานร่วมกับระบบรักษาความปลอดภัย อย่างน้อยหนึ่ง ในรายการต่อไปนี้ Firewall หรือ Endpoint Detection and Response (EDR) หรือ Endpoint Protection Platform (EPP) (หรือระบบที่มีคุณสมบัติเทียบเท่า) หากไม่สามารถรองรับคุณสมบัติดังกล่าวได้ครบตามที่กำหนด สามารถเสนอระบบ/โมดูลเสริมเพิ่มเติมที่มีความสามารถเทียบเท่า

4.8.10 สามารถทำการแชร์ข้อมูลทางด้านไซเบอร์ (Data sharing) ผ่านช่องทาง Syslog ได้เป็นอย่างน้อย

4.8.11 NDR ต้องมีความสามารถในการวิเคราะห์ภัยคุกคามทางเครือข่าย Throughput ไม่น้อยกว่า 5 Gbps

4.8.12 มีข้อกำหนดของพอร์ตเชื่อมต่อระบบเครือข่าย (Network Interface) อย่างน้อยดังต่อไปนี้

1) แบบ Appliance (มี Sensor ในตัว) ต้องมีพอร์ต แบบ 10/100/1000 หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง และพอร์ต แบบ 10G SFP+หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง

2) แบบ Distributed: ส่วน Sensor/Collector ต้องมีพอร์ต แบบ 10G SFP+ หรือดีกว่า ไม่น้อยกว่า 2 ช่อง และส่วนระบบประมวลผล NDR มีพอร์ต แบบ 10/100/1000 หรือดีกว่า ไม่น้อยกว่า 2 ช่อง

4.8.13 บริษัทผู้นำเสนอจะต้องได้รับการแต่งตั้งอย่างเป็นทางการจากเจ้าของผลิตภัณฑ์

4.8.14 มีการรับประกันสินค้าจากเจ้าของผลิตภัณฑ์รวมทั้งสิทธิ์ในการอัปเกรดระบบที่นำเสนอเป็นเวลาไม่น้อยกว่า 1 ปี

4.9 **การติดตั้งและตั้งค่าอุปกรณ์**

4.9.1 ผู้ขายต้องดำเนินการออกแบบ จัดหา ติดตั้ง เชื่อมต่อและตั้งค่าระบบและอุปกรณ์ที่เสนอให้สามารถใช้งานได้ถูกต้อง ครบถ้วน และต้องดำเนินการให้เป็นไปตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 ที่เกี่ยวข้อง เป็นอย่างน้อย หากจำเป็นต้องใช้อุปกรณ์เพิ่มเติมเพื่อให้ระบบทำงานได้อย่างสมบูรณ์ ผู้ขายต้องจัดหาโดยไม่คิดค่าใช้จ่ายเพิ่มเติม รวมถึงดำเนินการอื่น ๆ ที่เกี่ยวข้อง เพื่อให้อุปกรณ์และระบบทั้งหมดสามารถใช้งานได้ต่อเนื่องและมีเสถียรภาพ โดยต้องจัดประชุมชี้แจงแผนการดำเนินงานล่วงหน้าเพื่อให้ กพท. พิจารณาเห็นชอบก่อนเริ่มการติดตั้ง

4.9.2 ผู้ขายต้องประชุมร่วมกับเจ้าหน้าที่ผู้ดูแลระบบของ กพท. เพื่อสำรวจพื้นที่จริงและรวบรวมข้อมูลเพิ่มเติม เช่น สภาพห้อง Data Center, การจัดวางอุปกรณ์ในตู้ Rack, ระบบไฟฟ้าและปรับอากาศ รวมถึงข้อกำหนดเชิงเทคนิคอื่น ๆ จากนั้นต้องออกแบบระบบให้สอดคล้องกับพื้นที่และเงื่อนไขการใช้งาน จากนั้นจัดทำเอกสารดังต่อไปนี้เพื่อเสนอต่อ กพท. พิจารณาเห็นชอบก่อนเริ่มการติดตั้ง

4.9.2.1 เอกสารออกแบบรายละเอียดระบบ (System Detail Design Document) ต้องประกอบด้วยอย่างน้อยดังนี้ Logical Architecture, Physical Architecture, การเชื่อมต่อกับระบบเดิม (Integration Flow) และข้อกำหนดเชิงเทคนิคที่เกี่ยวข้อง

4.9.2.2 ผังโครงสร้างพื้นฐานและการตั้งค่าระบบเครือข่าย (Infrastructure Diagram & Network Configuration) ต้องแสดงโครงสร้างเครือข่าย (Topology), แผนการจัดสรร IP/VLAN, เส้นทางการเชื่อมต่อ (Routing/Link), หลักการกำหนดนโยบายความปลอดภัยเบื้องต้น (Security Policy)

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

4.9.2.3 แบบการติดตั้งเบื้องต้น (Installation Drawing) ต้องระบุอย่างน้อยดังนี้ ผังการจัดวางอุปกรณ์ในตู้ Rack, แผนการเดินสาย และจุดเชื่อมต่อกับระบบเดิมตามพื้นที่จริง

4.9.3 ผู้ขายต้องจัดทำแผนการดำเนินงานและกำหนดการติดตั้งเพื่อเสนอ กพท. พิจารณาเห็นชอบก่อนเริ่มดำเนินการ โดยให้จัดทำในรูปแบบ เอกสารแผนการติดตั้งและดำเนินงาน (Implementation Plan & Installation Schedule) ซึ่งต้องแสดงอย่างน้อยดังนี้ ลำดับกิจกรรม วิธีการดำเนินงาน ระยะเวลา ผู้รับผิดชอบ และเหตุการณ์สำคัญของงาน (Milestone) ของแต่ละขั้นตอน

4.9.4 ผู้ขายต้องดำเนินการติดตั้งอุปกรณ์ทั้งหมดตามแบบที่ได้รับอนุมัติ โดยต้องดำเนินการติดตั้งเดินสาย เก็บสายให้เรียบร้อยหลังการติดตั้ง และต้องติดป้ายกำกับ (Label) ทั้งต้นทาง-ปลายทาง ของสายสัญญาณแต่ละเส้น ป้ายกำกับจะต้องมีความแข็งแรงทนทานและใช้งานได้ในระยะยาว และจัดทำเอกสารแบบการติดตั้งจริง (Installation As-built Drawing) ซึ่งต้องประกอบด้วยอย่างน้อย ผังการจัดวางอุปกรณ์ในตู้ Rack ผังการเดินสาย

4.9.5 ผู้ขายต้องปฏิบัติงานด้วยความเรียบร้อย สะอาด และปลอดภัย รวมทั้งต้องป้องกันมิให้เกิดความเสียหายต่อทรัพย์สินของ กพท. หรือบุคคลที่สาม และหากเกิดความเสียหายอันเนื่องมาจากการปฏิบัติงานของผู้ขาย ผู้ขายต้องรับผิดชอบในความเสียหายที่เกิดขึ้นทั้งหมดโดยไม่มีเงื่อนไข

4.9.6 ผู้ขายต้องติดตั้งและกำหนดค่าการทำงาน (Configuration) ของระบบและอุปกรณ์ต่าง ๆ ตามมาตรฐานที่กำหนด และตามข้อกำหนดที่เจ้าหน้าที่ผู้ดูแลระบบแจ้ง เพื่อให้ระบบสามารถทำงานได้ถูกต้องและปลอดภัย และจัดทำเอกสารค่าการตั้งค่าที่ใช้งานจริง (Running Configuration / Parameter Summary)

4.9.7 หากจำเป็นต้องรื้อถอนอุปกรณ์เดิม ผู้ขายต้องดำเนินการโดยไม่ก่อให้เกิดผลกระทบต่อความต่อเนื่องของบริการ และภายหลังการรื้อถอนต้องจัดเก็บอุปกรณ์ดังกล่าวอย่างเหมาะสม เพื่อป้องกันความเสียหายระหว่างการเคลื่อนย้ายและการเก็บรักษา (ตามที่ กพท. แจ้ง) และต้องจัดทำเอกสารทะเบียนอุปกรณ์เดิมที่รื้อถอนส่งให้ กพท. (ถ้ามี)

4.9.8 ผู้ขายต้องจัดทำเอกสารรายงานการติดตั้งและเชื่อมต่อระบบ (System Integration & Installation Report) หลังการติดตั้งแล้วเสร็จ ซึ่งอย่างน้อยต้องประกอบด้วย ผังการเชื่อมต่อจริงของ Physical Diagram และ Logical Diagram รายการอุปกรณ์ที่ติดตั้งจริง และรายละเอียดเชิงเทคนิคที่เกี่ยวข้องทั้งหมด

4.9.9 ผู้ขายต้องกำหนดค่าด้านความมั่นคงปลอดภัยขั้นต่ำ (Security Baseline) ให้กับระบบและอุปกรณ์เครือข่ายที่ติดตั้ง โดยต้องสอดคล้องกับมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศและนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy) ของ กพท. และจัดทำเอกสารสรุปการตั้งค่าความมั่นคงปลอดภัย (Security Baseline Summary) ของระบบและอุปกรณ์ทั้งหมดที่เกี่ยวข้องในโครงการ

4.9.10 ผู้ขายต้องทดสอบการทำงานของระบบทั้งในส่วนการใช้งานปกติ การทำงานร่วมกับระบบเดิม และการสำรอง/กู้คืน (ถ้ามี) โดยต้องจัดทำเอกสารแผนและผลการทดสอบ (Test Plan & Test Report) ซึ่งต้องมีอย่างน้อย ขอบเขตการทดสอบ วิธีดำเนินการ และหลักฐานผลการทดสอบ

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

4.10 **การฝึกอบรม**

4.10.1 ผู้ขายต้องจัดอบรมให้กับเจ้าหน้าที่ของ กพท. ในหัวข้อที่เกี่ยวกับการใช้งาน การบริหารจัดการและการดูแลรักษาอุปกรณ์ และการบริการจัดการระบบพร้อมอุปกรณ์ที่ทำงานร่วมกันทั้งหมด โดยนำเสนอแผนการฝึกอบรมในรายละเอียด เช่น หัวข้อการฝึกอบรม ระยะเวลา วิทยากร ทั้งนี้ผู้ขายเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งสิ้น โดยให้มีอย่างน้อย 5 หลักสูตร ดังนี้

4.10.1.1 หลักสูตรการบริหารจัดการอุปกรณ์รักษาความปลอดภัยระดับเครือข่าย (Next Generation Firewall) ระยะเวลาไม่น้อยกว่า 2 วัน จำนวนไม่น้อยกว่า 5 คน

4.10.1.2 หลักสูตรการบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายสำหรับติดตั้งระบบ Hyper Converged Infrastructure ระยะเวลาไม่น้อยกว่า 1 วัน จำนวนไม่น้อยกว่า 5 คน

4.10.1.3 หลักสูตรการบริหารจัดการระบบบริหารจัดเก็บข้อมูล Log (Central Log Management) ระยะเวลาไม่น้อยกว่า 0.5 วัน จำนวนไม่น้อยกว่า 5 คน

4.10.1.4 หลักสูตรการบริหารจัดการระบบตรวจสอบสถานะและเฝ้าระวัง (System Monitoring) ระยะเวลาไม่น้อยกว่า 0.5 วัน จำนวนไม่น้อยกว่า 5 คน

4.10.1.5 หลักสูตรการบริหารจัดการระบบตรวจจับและตอบสนองภัยคุกคามในระบบเครือข่าย (Network Detection and Response: NDR) ระยะเวลาไม่น้อยกว่า 2 วัน จำนวนไม่น้อยกว่า 5 คน

4.10.2 ผู้ขายต้องจัดการอบรมเชิงปฏิบัติการ (Workshop) เพื่อจำลองการรับมือภัยคุกคามทางไซเบอร์โดยใช้อุปกรณ์ด้านความมั่นคงปลอดภัยที่อยู่ในโครงการนี้ เป็นระยะเวลาไม่น้อยกว่า 1 วัน และต้องให้ความร่วมมือกับ กพท. ในการซักซ้อมและฝึกปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ตามที่ร้องขอ

4.10.3 ผู้ขายต้องเสนอแผนและรายละเอียดหลักสูตรการอบรมทั้งหมดให้สำนักงานการบินพลเรือนแห่งประเทศไทย พิจารณาก่อนจัดการฝึกอบรม

5. กำหนดเวลาส่งมอบพัสดุ

ผู้ขายต้องส่งมอบพัสดุทั้งหมดพร้อมติดตั้งและฝึกอบรม ภายใน 120 วัน นับถัดจากวันลงนามสัญญา

6. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

เกณฑ์ราคา

7. วงเงินงบประมาณ

งบประมาณ 13,000,000.00 บาท (สิบสามล้านบาทถ้วน) ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายอื่นทั้งปวงไว้ด้วยแล้ว

8. งวดงานและการจ่ายเงิน

สำนักงานการบินพลเรือนแห่งประเทศไทยจะจ่ายเงินค่าระบบรักษาความปลอดภัยของระบบเครือข่าย กพท. ซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงแล้ว เมื่อผู้ขายได้ส่งมอบพัสดุครบถ้วนตามสัญญาซื้อขาย ภายใน 120 วันนับถัดจากวันที่ลงนามในสัญญา และคณะกรรมการตรวจรับได้ทำการตรวจรับมอบงานไว้เรียบร้อยแล้วนั้น

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

- ส่งมอบอุปกรณ์ทั้งหมดตามข้อ 4.1 – 4.8 ณ กพท. หรือสถานที่ที่ กพท. กำหนด พร้อมติดตั้งอุปกรณ์และระบบแล้วเสร็จพร้อมใช้งานร่วมกับระบบเดิมได้อย่างดีตามข้อ 4.9
- จัดทำ Configuration ของระบบใหม่ให้ทำงานร่วมกับระบบเดิมได้ตามวัตถุประสงค์ตามข้อ 4.9.6
- ทดสอบคุณสมบัติของอุปกรณ์ ตามข้อ 4.9.10
- จัดอบรมการใช้งานอุปกรณ์ตามข้อ 4.10
- ส่งมอบรายละเอียดเอกสารอย่างน้อย ดังนี้
  - เอกสารออกแบบรายละเอียดระบบ (System Detail Design Document) ตามข้อ 4.9.2.1
  - ผังโครงสร้างพื้นฐานและการตั้งค่าระบบเครือข่าย (Infrastructure Diagram & Network Configuration) ตามข้อ 4.9.2.2
  - เอกสารแบบการติดตั้งอย่างละเอียดก่อนการติดตั้ง (Installation Drawing) ตามข้อ 4.9.2.3
  - เอกสารแผนการดำเนินงานและการติดตั้ง (Implementation Plan & Installation Schedule) ตามข้อ 4.9.3
  - เอกสารแบบการติดตั้งจริง (Installation As-built Drawing) ตามข้อ 4.9.4
  - เอกสารค่าการตั้งค่าที่ใช้งานจริง (Running Configuration / Parameter Summary) ตามข้อ 4.9.6
  - เอกสารทะเบียนอุปกรณ์เดิมที่รื้อถอน (ถ้ามี) ตามข้อ 4.9.7
  - เอกสารรายงานการติดตั้งและเชื่อมต่อระบบ (System Integration & Installation Report) ตามข้อ 4.9.8
  - เอกสารรายการอุปกรณ์ทั้งหมด ตามข้อ 4.1 – 4.8
  - เอกสารสรุปการตั้งค่าความมั่นคงปลอดภัย (Security Baseline Summary) ตามข้อ 4.9.9
  - เอกสารแผนและผลการทดสอบ (Test Plan & Test Report) ตามข้อ 4.9.10
  - เอกสารประกอบการอบรม และหลักฐานการฝึกอบรม ตามข้อ 4.10
  - รายงานสรุปผลโครงการ (Final Report)
  - เอกสารรายการสิทธิ์การเข้าถึงและรหัสผ่าน (Handover Document)
  - เอกสารคู่มือการบริหารจัดการและการปฏิบัติงาน (System Administration & Operation Manual) ตามข้อ 4.1, 4.2, 4.3, 4.4, 4.5, 4.7 และ 4.8

9. การรับประกันความชำรุดบกพร่อง

9.1 ผู้ขายต้องรับประกันความชำรุดบกพร่องหรือขัดข้องของพัสดุทุกรายการตามสัญญานี้ เป็นเวลา 1 ปี แบบรวมอะไหล่และค่าใช้จ่ายอื่น ๆ ทั้งปวง รวมไปถึงการปรับปรุงเวอร์ชั่นซอฟต์แวร์ นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุได้ตรวจรับงานเรียบร้อยแล้ว ถ้าภายในระยะเวลาดังกล่าว พัสดุชำรุดบกพร่องใช้งานไม่ได้ทั้งหมดหรือแค่บางส่วน ผู้ขายจะต้องจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพใช้การได้ดีดังเดิม

9.2 ผู้ขายมีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไขแบบ Corrective Maintenance (CM) รายการพัสดุตามสัญญา ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอ ตลอดระยะเวลาที่รับประกันด้วยค่าใช้จ่ายของผู้ขาย โดยต้องเริ่มจัดการซ่อมแซมแก้ไขภายในระยะเวลาตามที่กำหนด ดังนี้

9.2.1 ปัญหาทางด้าน Hardware ต้องเข้ามาดำเนินการแก้ไขให้แล้วเสร็จ ภายใน 24 ชั่วโมง นับจากเวลาที่ได้รับแจ้งปัญหา

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

9.2.2 ปัญหาทางด้าน Software ต้องเข้าดำเนินการแก้ไขให้แล้วเสร็จ ภายใน 48 ชั่วโมง นับจากเวลาที่ได้รับแจ้งปัญหา

9.3 ผู้ขายมีหน้าที่บำรุงรักษาแบบ Preventive Maintenance (PM) และจัดรายงานการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance : PM) รายการพัสดุตามสัญญาโดยต้องดำเนินการเป็นประจำทุก 6 เดือน ในระยะเวลารับประกัน เริ่มนับจากวันที่คณะกรรมการตรวจรับพัสดุได้ตรวจรับงานเรียบร้อยแล้ว

9.4 ผู้ขายต้องจัดให้มีช่องทางสื่อสารเพื่อให้ กพท. แจ้งเหตุชำรุดบกพร่องหรือความขัดข้องของอุปกรณ์ได้ตลอด 24 ชั่วโมง ตั้งแต่วันจันทร์ – วันอาทิตย์ ผ่านทางอีเมลและโทรศัพท์เป็นอย่างน้อย

9.5 ผู้ขายต้องมีทีมงานให้คำปรึกษาและแก้ไขปัญหาหรือปรับแก้ Configuration ทางด้าน ระบบ และ Hardware, Software ที่เสนอ ได้ทั้ง 3 ช่องทาง คือ Telephone, Remote Support, Onsite Support เมื่อทาง กพท. ร้องขอโดยไม่มีค่าใช้จ่ายเป็นเวลา 1 ปี หลังจากติดตั้งและตรวจรับงานเรียบร้อยแล้ว

9.6 ผู้ขายมีหน้าที่ดำเนินการสนับสนุนการปิดหรือลดช่องโหว่ด้านความมั่นคงปลอดภัยของอุปกรณ์และระบบที่เกี่ยวข้องกับสัญญาตามข้อกำหนดของ กพท. ดังนี้

9.6.1 การแจ้งช่องโหว่ ผู้ขายต้องแจ้งช่องโหว่ที่ตรวจพบในอุปกรณ์หรือซอฟต์แวร์ที่ใช้ในระบบให้ กพท. ทราบทันทีที่พบ

9.6.2 การจัดหาแพตช์ (Patch) ผู้ขายต้องจัดหาแพตช์หรือการแก้ไขช่องโหว่ให้แก่ กพท. อย่างรวดเร็วหลังจากที่มีการประกาศอย่างเป็นทางการ

9.6.3 การติดตั้งและทดสอบแพตช์ ผู้ขายต้องให้การสนับสนุนทางเทคนิคในการติดตั้งแพตช์และทดสอบระบบหลังการติดตั้ง เพื่อให้มั่นใจว่าระบบยังคงทำงานได้อย่างปกติ

9.6.4 การรายงาน: ผู้ขายต้องจัดทำรายงานการแก้ไขช่องโหว่ตามรูปแบบที่ กพท.กำหนด

9.7 ในกรณีที่ กพท. มีการย้ายสถานที่ทำการในช่วงระหว่างระยะเวลาของสัญญา ผู้ขายต้องดำเนินการให้ระบบสามารถใช้งานได้ตามปกติ และสนับสนุนการแก้ไขปัญหาการใช้งานเป็นระยะเวลาอย่างน้อย 1 เดือน หลังจากทำการย้ายสถานที่ติดตั้ง โดยไม่มีค่าใช้จ่ายเพิ่มเติม

10. ข้อตกลงห้ามเปิดเผยข้อมูล

ข้อมูล เอกสาร หรือสัญญาที่เกี่ยวข้องกับโครงการนี้ทั้งหมดที่ กพท.จัดหาให้ หรือผู้ขายดำเนินการและจัดหาให้ กพท. ถือเป็นความลับ และเป็นสมบัติของ กพท. ผู้ขายต้องไม่เปิดเผยข้อมูลและผลการดำเนินการให้แก่ผู้ใด ยกเว้นแต่จะได้รับอนุญาตจาก กพท. เป็นลายลักษณ์อักษร หากผู้ขายละเมิดโดยมีการนำไปเผยแพร่และเปิดเผยโดยไม่ได้รับอนุญาต กพท. มีสิทธิ์ฟ้องร้องเรียกค่าเสียหายและดำเนินการตามกฎหมายได้

11. ความคุ้มครองเกี่ยวกับลิขสิทธิ์

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิเรียกร้องใด ๆ ว่ามีการละเมิดลิขสิทธิ์เกี่ยวกับการซื้อขายตามสัญญานี้ โดย กพท. มิได้แก้ไขดัดแปลงไปจากเดิม ผู้ขายจะต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว เพื่อให้ กพท. สามารถใช้งานนั้นต่อไปได้ หากผู้ขายมิอาจกระทำได้และ กพท. ต้องรับผิดชอบชดใช้ค่าเสียหายต่อบุคคลภายนอก เนื่องจากผลแห่งการละเมิดลิขสิทธิ์ดังกล่าว

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ

ผู้ขายต้องเป็นผู้ชำระค่าเสียหาย ค่าปรับและค่าใช้จ่ายอื่น ๆ รวมทั้งค่าธรรมเนียม และค่าทนายความ ทั้งนี้ กพท. จะแจ้งผู้ขายทราบเป็นลายลักษณ์อักษรในเมื่อได้มีการกล่าวอ้างหรือใช้สิทธิเรียกร้องดังกล่าว โดยไม่ชักช้า

12. เงื่อนไขอื่น ๆ

ผู้ขายต้องปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายคุ้มครองข้อมูลส่วนบุคคล และประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กพท. รวมถึงกฎหมาย นโยบาย คำสั่งและขั้นตอนปฏิบัติอื่น ๆ ที่เกี่ยวข้อง

13. ผู้รับผิดชอบโครงการ

ฝ่ายบริหารเทคโนโลยีดิจิทัล กองพัฒนามาตรฐานการจัดการและความปลอดภัยไซเบอร์ สำนักงานการบินพลเรือนแห่งประเทศไทย 222 ซอยวิภาวดีรังสิต 28 ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร กรุงเทพฯ 10900 โทร. 0 2568 8808 Email: itd_team@caat.or.th

(นายวีระ ระบายศรี)	(นางสาวอรวรรณ ใจเอื้อ)	(นายณัฐธัญ เรวดีเรขา)	(นายทวีศักดิ์ จงราช)	(นายรักพิรุนห์ รุจิรวงษ์สกุล)
ประธานกรรมการ	กรรมการ	กรรมการ	กรรมการ	กรรมการ