ร่าง คุณลักษณะเฉพาะ (Terms of Reference: TOR)
ระบบตรวจสอบและเฝ้าระวังการโจมตีทางไซเบอร์ (Cyber Security Awareness)

1. หลักการและเหตุผล

ด้วยสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มีศูนย์ข้อมูล (Data Center) จำนวน 2 แห่ง คือ ศูนย์ข้อมูล (Data Center) ราชดำเนินและเอกมัย โดยให้บริการระบบเครือข่ายและระบบเครื่องคอมพิวเตอร์แม่ข่าย เพื่อติดตั้งระบบงานต่าง ๆ ของหน่วยงานในสังกัดสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน และปัจจุบันการโจรกรรมข้อมูลหรือเหตุการณ์การละเมิดข้อมูลที่สำคัญมีอัตราการเกิดที่สูงขึ้น โดยผู้ไม่ประสงค์ดี (Threat Actor) จะมุ่งเป้าไปที่องค์กรขนาดใหญ่และหน่วยงานภาครัฐ ที่มีการเก็บและใช้ข้อมูลเป็นจำนวนมาก ผ่านกระบวนการเจาะระบบเพื่อโจมตีทางไซเบอร์ (Cyber Kill Chain) ดังนั้น สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ในฐานะหน่วยงานภาครัฐขนาดใหญ่ที่มีการจัดเก็บและใช้ การเชื่อมโยงแลกเปลี่ยนข้อมูลเป็นจำนวนมาก เช่น การให้บริการอินเทอร์เน็ตสำหรับหน่วยงาน สถานศึกษาในสังกัดทั้งส่วนกลางและส่วนภูมิภาค การให้บริการเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบสารสนเทศ ระบบบริหารจัดการด้านการศึกษา จำเป็นต้องมีการตรวจสอบ และตอบสนองต่อภัยคุกคามทางไซเบอร์ที่รวดเร็วและมีประสิทธิภาพ

สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน จึงจำเป็นต้องจัดหาระบบตรวจสอบ ตรวจจับ วิเคราะห์ และแจ้งเตือนพฤติกรรมผิดปกติหรือภัยคุกคามที่เกิดขึ้นในระบบเครือข่ายคอมพิวเตอร์เพื่อเฝ้าระวังการโจมตีทางไซเบอร์ (Cyber Security Awareness) และเครื่องมือสำคัญในการบริหารจัดการสิทธิ์การเข้าถึงระบบของผู้ใช้งานที่มีสิทธิ์พิเศษ (Privileged Users) เป็นสิ่งสำคัญในการปกป้องข้อมูลและระบบไอทีขององค์กรจากภัยคุกคามทางไซเบอร์ ซึ่งอาจเป็นการโจมตีจากแฮกเกอร์ มัลแวร์ หรือผู้ไม่ประสงค์ดี (Threat Actor) การเฝ้าระวังช่วยป้องกันการโจมตีทางไซเบอร์ทั้งจากภายนอกและภายในองค์กร โดยระบบจะตรวจสอบกิจกรรมที่น่าสงสัย และส่งการแจ้งเตือนเมื่อพบความผิดปกติ ซึ่งช่วยลดความเสียหายที่อาจเกิดขึ้นได้ การสร้างความตระหนักรู้ในด้านความปลอดภัยทางไซเบอร์เป็นการเสริมความรู้ให้กับพนักงานและบุคลากรในองค์กร เพื่อให้สามารถระมัดระวังและปฏิบัติตามแนวทางที่เหมาะสมเพื่อลดความเสี่ยง สามารถตอบสนองต่อเหตุการณ์โจมตีทางไซเบอร์ได้อย่างรวดเร็วและเพิ่มความน่าเชื่อถือให้กับองค์กร

2. วัตถุประสงค์

2.1 เพื่อเพิ่มสมรรถนะด้านความปลอดภัยทางไซเบอร์ ลดความเสี่ยงและผลกระทบจากภัยคุกคามทางด้านไซเบอร์

2.2 เพื่อเพิ่มสมรรถนะด้านความปลอดภัยทางไซเบอร์ ในการรับมือและตอบสนองภัยคุกคามทางด้านไซเบอร์ที่เกิดขึ้นได้อย่างรวดเร็ว

2.3 เพื่อตรวจสอบ ตรวจจับ วิเคราะห์ และแจ้งเตือนพฤติกรรมผิดปกติหรือภัยคุกคามที่เกิดขึ้นในระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของหน่วยงาน

2.4 เพื่อลดความเสี่ยงที่อาจเกิดจากการละเมิดความปลอดภัยทางข้อมูล การควบคุมและป้องกันการเข้าถึงระบบหรือข้อมูลที่สำคัญโดยบุคคลที่ไม่ได้รับอนุญาต

2.5 เพื่อเพิ่มความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ ให้ได้ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

2.6 เพื่อยกระดับมาตรฐานด้านความปลอดภัยทางไซเบอร์ของหน่วยงาน

3. คุณสมบัติผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

3.10.1 การกำหนดสัดส่วนการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

3.10.2 กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

3.10.3 การยื่นข้อเสนอของกิจการร่วมค้า

3.10.3.1 กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจสำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

3.10.3.2 การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e - bidding) ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ 3.10.3.1 ดำเนินการซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารซื้อหรือจ้าง

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

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

3.12.1 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งตามกฎหมายไทยหรือต่างประเทศซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันที่ยื่นข้อเสนอ งบแสดงฐานะการเงิน 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ 1 ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนอนั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนหลังไปอีก 1 ปี ได้

3.12.2 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่ต่ำกว่า 8 ล้านบาท

3.12.3 กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

3.12.3.1 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทย แจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

3.12.3.2 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุน หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศ หรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน

3.12.4 กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศที่มิได้ถือสัญชาติไทย ตามข้อ 3.12.2 และข้อ 3.12.3.2 มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารเชิญชวนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) หรือมีหนังสือเชิญชวน จนถึงวันเสนอราคา

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศว่าด้วยการรับรองเอกสาร พ.ศ. 2539 และที่แก้ไขเพิ่มเติม กำหนด โดยจะต้องยื่นเอกสารดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอมิได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่าผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

3.12.5 กรณีตามข้อ 3.12.1 – ข้อ 3.12.4 ไม่ใช้บังคับกับกรณีดังต่อไปนี้

3.12.5.1 กรณีผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

3.12.5.2 นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติ ล้มละลาย พ.ศ. 2483 และที่แก้ไขเพิ่มเติม

3.13 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลที่มีผลงานเกี่ยวกับระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ หรือระบบป้องกันการสูญหายและการรั่วไหลของข้อมูล หรือระบบเครือข่ายคอมพิวเตอร์ โดยเป็นผลงานที่เสร็จสมบูรณ์แล้วอย่างน้อย 1 สัญญา และมีวงเงินต่อสัญญาไม่น้อยกว่า 8.5 ล้านบาท รวมภาษีมูลค่าเพิ่มแล้ว และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับส่วนราชการ หน่วยงานตามกฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น รัฐวิสาหกิจ หน่วยงานอื่นของรัฐ หรือหน่วยงานเอกชนที่น่าเชื่อถือและตรวจสอบได้ โดยผู้เสนอราคาต้องแนบหนังสือรับรองผลงานและสำเนาสัญญา โดยให้ยื่นขณะเข้าเสนอราคา

3.14 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นขณะเข้าเสนอราคา ตามรายการครุภัณฑ์ ข้อ 4

4. รายการครุภัณฑ์

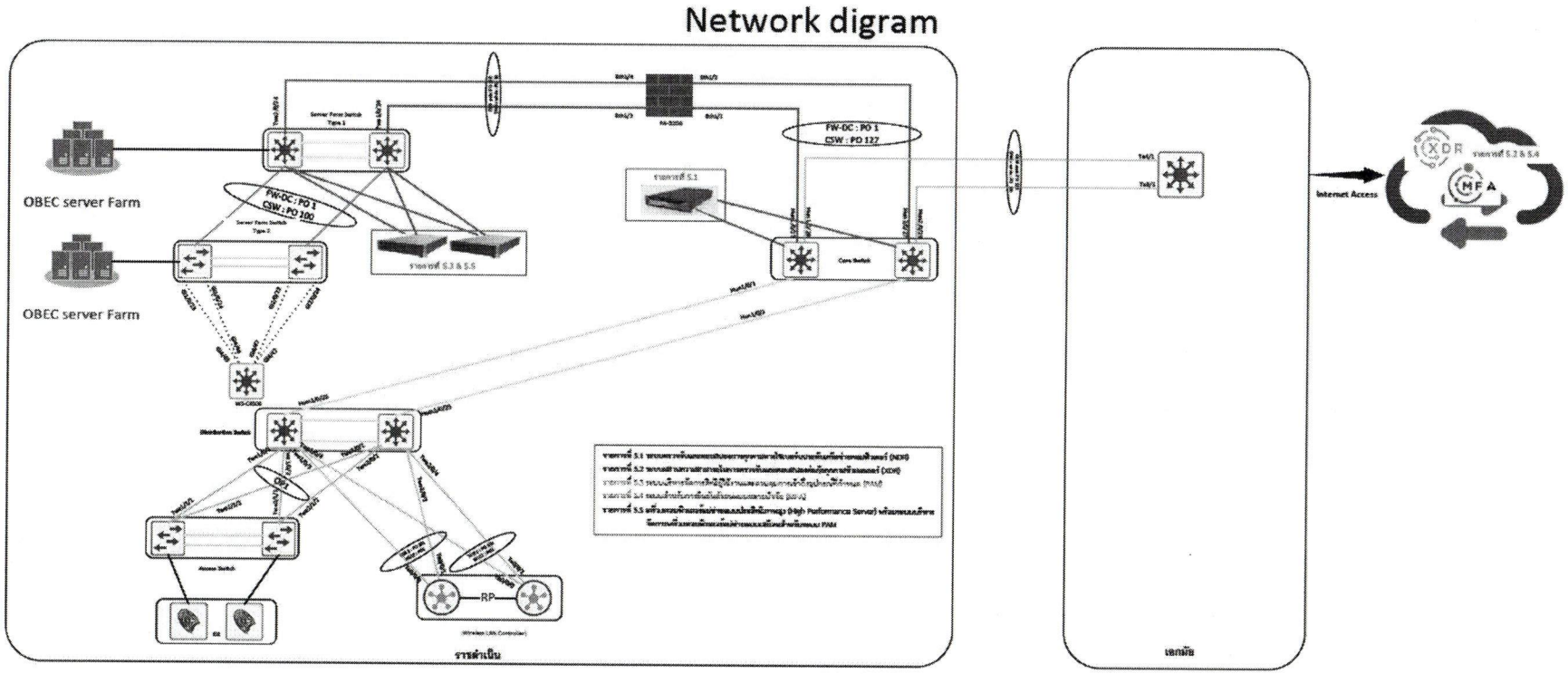
ลำดับ	รายการและคุณลักษณะ	จำนวน/หน่วยนับ	ราคาต่อหน่วย	ราคารวม
4.1	ระบบตรวจจับและตอบสนองการคุกคามทางไซเบอร์บนระดับเครือข่ายคอมพิวเตอร์ (Network Detection and Response: NDR)	1 ระบบ	10,190,000	10,190,000
4.2	ระบบผสานความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคามข้ามเลเยอร์ (Extended Detection and Response: XDR)	1 ระบบ	6,370,000	6,370,000

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

ลำดับ	รายการและคุณลักษณะ	จำนวน/หน่วยนับ	ราคาต่อหน่วย	ราคารวม
4.3	ระบบบริหารจัดการสิทธิ์ผู้ใช้งานและควบคุมการเข้าถึงอุปกรณ์ที่กำหนด (Privileged Access Management: PAM)	1 ระบบ	12,186,000	12,186,000
4.4	ระบบสำหรับการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA)	1 ระบบ	862,900	862,900
4.5	เครื่องคอมพิวเตอร์แม่ข่ายแบบประสิทธิภาพสูง (High Performance Server) พร้อมระบบบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือนสำหรับระบบ PAM	1 ระบบ	4,961,600	4,961,600
รวมทั้งสิ้น				**34,570,500**

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

5. รายละเอียดคุณลักษณะ



การเชื่อมโยงอุปกรณ์ของโครงการกับระบบหรืออุปกรณ์ที่เกี่ยวข้อง

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

5.1 ระบบตรวจจับและตอบสนองการคุกคามทางไซเบอร์บนระดับเครือข่ายคอมพิวเตอร์ จำนวน 1 ระบบ มีคุณลักษณะอย่างน้อยดังต่อไปนี้

5.1.1 เป็นอุปกรณ์แบบ Hardware Appliance ที่สามารถติดตั้งในตู้ Rack ได้

5.1.2 สามารถตรวจจับ ค้นหา แจ้งเตือนและรายงานอันตรายจากภัยต่าง ๆ (Threats) ในระบบเครือข่ายให้กับผู้ดูแลระบบได้

5.1.3 สามารถตรวจสอบข้อมูลที่มีการส่งผ่านในระบบ และพฤติกรรมที่ไม่ปลอดภัย หรือการโจมตีภายในกระแสข้อมูลของระบบได้

5.1.4 สามารถเชื่อมต่อกับระบบเครือข่ายสื่อสารข้อมูลได้ โดยรองรับ Interface 10 Gbps หรือดีกว่า ไม่น้อยกว่า 4 ช่อง พร้อมเสนอโมดูล 10GBASE-SR หรือดีกว่า จำนวนไม่น้อยกว่า 2 โมดูล

5.1.5 มีพอร์ต Management แบบ 10/100/1000 (RJ45) หรือดีกว่า จำนวนไม่น้อยกว่า 1 พอร์ต

5.1.6 รองรับการวิเคราะห์ปริมาณการรับส่งข้อมูล (Traffic Analytics) ได้ไม่น้อยกว่า 4 Gbps

5.1.7 สามารถรับข้อมูลจากระบบเครือข่ายสื่อสารข้อมูลด้วยวิธี Mirror Port หรือ Tap/SPAN ได้ และรองรับการตรวจหากระแสข้อมูล (Traffic) จากโปรโตคอล CIFS/SMB, SMTP, HTTP ได้เป็นอย่างน้อย รวมไปถึงสามารถตรวจค้นการใช้งานโปรแกรมประยุกต์ต่าง ๆ เช่น Instant Messaging, P2P File Sharing และ Streaming Media ได้

5.1.8 สามารถตรวจจับ ค้นหาการโจมตี แบบ APT (Advanced Persistent Threats), Zero-day Exploits, Zero-day Malware และการโจมตีโดยใช้ Document Exploits ได้

5.1.9 สามารถวิเคราะห์พฤติกรรมของไฟล์ด้วย Virtual Analyzer หรือ Sandbox ได้ภายในตัวอุปกรณ์ โดยรองรับไฟล์ตระกูล Executables และ Microsoft Office เป็นอย่างน้อย รวมทั้งสามารถ Custom Sandbox หรือสามารถปรับแต่ง Operating System และ Application ได้ หรือเสนออุปกรณ์เพิ่มเติม เพื่อให้ใช้ความสามารถดังกล่าวได้

5.1.10 สามารถแสดง Top Malware-Infected Hosts, Top Suspicious Behavior Detected และทำการปรับแต่งหน้าจอได้ (Custom Dashboard)

5.1.11 สามารถแสดงผลการตรวจพบ (Detection) ที่รวมถึง Fingerprinting (JA3, JA3S Hash) และ MITRE ATT&CK Tactics and Techniques ได้

5.1.12 สามารถตรวจสอบ Websites หรือ URL ที่ User พยายามเข้าใช้งานโดยใช้ เทคโนโลยีบน Cloud ได้

5.1.13 สามารถทำ Network Analytics ด้วย Machine Learning เพื่อทำ Threat Correlation ในการโจมตี โดยเก็บรวบรวมข้อมูลย้อนหลังได้บนตัวอุปกรณ์ได้ไม่น้อยกว่า 3 เดือน

5.1.14 สามารถค้นหาร่องรอยการโจมตี (Sweeping / Hunting) จากข้อมูลที่บันทึก โดยมี Threat Intelligence จากเจ้าของผลิตภัณฑ์ หรือสามารถเพิ่มแหล่งข้อมูลจาก STIX File หรือ TAXII Feeds ได้

5.1.15 สามารถค้นหา Log แบบกำหนดเวลาได้ และกำหนดเงื่อนไข เช่น ชนิดของการตรวจสอบ (Detection Type), IP Address, Mac Address ได้เป็นอย่างน้อย

5.1.16 สามารถตรวจจับ ค้นหา ภัยคุกคามประเภท Ransomware, Bot, Trojan, Worm และ Key Logger ได้

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

5.1.17 มีความสามารถตรวจสอบภัยคุกคามแบบต่อเนื่องขั้นสูงภายในกระแสข้อมูลของระบบอย่างน้อยดังนี้

5.1.17.1 Network Content Inspection Engine หรือเทียบเท่า

5.1.17.2 Network Content Correlation Engine หรือเทียบเท่า

5.1.17.3 Advance Threat Scan Engine หรือเทียบเท่า

5.1.17.4 Retro scan หรือเทียบเท่า

5.1.18 สามารถทำงานร่วมกับระบบผสานความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคามข้ามเลเยอร์ (Extended Detection and Response) ตามรายการครุภัณฑ์ ข้อ 4.2 ที่เสนอในโครงการได้ เพื่อป้องกันและตรวจจับภัยคุกคามข้ามเลเยอร์ โดยสามารถกำหนดให้ระบบส่งค่า Threat Intelligence เช่น File Hash และ IP Address ได้ หรือเสนออุปกรณ์เพิ่มเติม เพื่อให้ใช้ความสามารถดังกล่าวได้

5.1.19 มีลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย เป็นระยะเวลาไม่น้อยกว่า 3 ปี นับถัดจากวันตรวจรับงานงวดสุดท้าย โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์หรือสาขาของเจ้าของผลิตภัณฑ์ในประเทศไทย

5.1.20 ผลิตภัณฑ์ที่เสนอต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ The Forrester Wave ในกลุ่มผลิตภัณฑ์ Network Analysis and Visibility ปี 2023 หรือปีล่าสุด

5.2 ระบบผสานความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคามข้ามเลเยอร์ (XDR) จำนวน 1 ระบบ มีคุณลักษณะอย่างน้อยดังต่อไปนี้

5.2.1 มีระบบตรวจจับและโต้ตอบต่อภัยคุกคามข้ามเลเยอร์ (Extended Detection and Response) เพื่อการค้นหาและวิเคราะห์ภัยคุกคามที่มาจากหลายทิศทางแบบเชิงลึก

5.2.2 รองรับการตรวจสอบสิ่งที่เกิดขึ้น เช่น File, Process, Network Activity, Registry และ User Account Activity ได้

5.2.3 ค้นหาข้อมูลของภัยคุกคามเชิงรุก (Threat Hunting หรือ Proactively Search) โดยอาศัยข้อมูลจาก EndpointID, EndpointName, DomainName, IPv4, IPv6, URL, Port, UserAccount, UserDomain, FileName, FileFullPath, FileSHA, FileMD, ProcessFullPath, CLICommand, RegistryKey, RegistryValue, RegistryValueData, Technique และ Tactic ได้เป็นอย่างน้อย

5.2.4 แสดงการแจ้งเตือนที่สอดคล้องกับ Detection Models เพื่อทำการวิเคราะห์หาต้นเหตุ (Root Cause Analysis & Analysis Chain)

5.2.5 รองรับการดำเนินการโต้ตอบต่อ Event หรือ Object ด้วยฟังก์ชัน เช่น Collect File, Add to Block List, Isolate Endpoint, Restore Connection, Start Remote Shell Session, Run Remote Custom Script และ Submit for Sandbox Analysis ได้

5.2.6 มีหน้าจอแสดงการจัดลำดับความสำคัญและแจ้งเตือน (Workbench) ดังนี้ ดูรายละเอียด การดำเนินการเพิ่มเติม (Execution Profile), ระบุขอบเขตของผลกระทบ (Identify the Scope of Impact) และดำเนินการโต้ตอบ (Response Actions)

5.2.7 สามารถแสดงข้อมูลการเชื่อมต่อกับ MITRE ATT&CK หรือ Cyber Kill Chain หรือ Diamond Model of Intrusion Analysis เพื่อตรวจสอบ Tactic และ Technique ที่ถูกตรวจพบได้

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

5.2.8 สามารถทำการเก็บข้อมูลหลักฐานของเครื่องคอมพิวเตอร์ (Telemetry หรือ Forensic Analysis) เพื่อตรวจสอบเหตุการณ์ย้อนหลังได้ไม่น้อยกว่า 30 วัน

5.2.9 มี Public API เพื่อทำงานร่วมกับ SIEM และ SOAR ได้

5.2.10 มีลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย เป็นระยะเวลาไม่น้อยกว่า 3 ปี นับถัดจากวันตรวจรับงานงวดสุดท้าย โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์หรือสาขาของเจ้าของผลิตภัณฑ์ในประเทศไทย

5.2.11 ผลิตภัณฑ์ที่เสนอต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leaders หรือ Strong Performers ของ The Forrester Wave ในกลุ่มผลิตภัณฑ์ Extended Detection and Response Platforms ปี 2024 หรือปีล่าสุด

5.3 ระบบบริหารจัดการสิทธิ์ผู้ใช้งานและควบคุมการเข้าถึงอุปกรณ์ที่กำหนด (Privilege Access Management: PAM) จำนวน 1 ระบบ โดยมีคุณสมบัติอย่างน้อยดังนี้

5.3.1 ระบบที่เสนอต้องเป็นแบบ Virtual Appliance หรือ Software ที่สามารถทำหน้าที่ในการบริหารจัดการสิทธิ์ผู้ใช้งานและควบคุมการเข้าถึงอุปกรณ์ที่กำหนด โดยทำการ Hardening OS แล้วจากผู้ผลิต

5.3.2 มีลิขสิทธิ์ของผู้ใช้งานไม่น้อยกว่า 30 Users โดยเป็นแบบ Perpetual License

5.3.3 สามารถทำงานได้โดยไม่ต้องติดตั้ง Software บนอุปกรณ์ปลายทาง (Agentless)

5.3.4 สามารถทำงานในรูปแบบ Single Sign-On (SSO) โดยที่ไม่ต้องเปิดเผยรหัสผ่านของอุปกรณ์ปลายทางให้ผู้ใช้งานรับทราบ

5.3.5 สามารถรองรับการเข้าถึงอุปกรณ์ปลายทางด้วยโปรโตคอล อย่างน้อยดังนี้ SSH, RDP, VNC, SFTP Telnet, Rlogin และ Raw TCP/IP

5.3.6 สามารถใช้งานผ่าน Client Software เช่น PuTTY, FileZilla และ Terminal Server Client ได้

5.3.7 มีการใช้ Session Probe ในการเก็บข้อมูล Metadata บน RDP Session เพื่อเก็บ Activity ของผู้ใช้งานได้

5.3.8 สามารถเลือกกำหนดให้อุปกรณ์บันทึกกิจกรรมการทำงานของผู้ใช้งานในรูปแบบภาพเคลื่อนไหวเฉพาะบางอุปกรณ์ปลายทางที่ต้องการได้

5.3.9 สามารถแสดงรายการภาพวิดีโอตัวอย่าง (Screenshot List) ของแต่ละช่วงเวลาตั้งแต่เริ่มต้นจนถึงสิ้นสุดการใช้งาน เพื่อให้เจ้าหน้าที่สามารถเรียกดูกิจกรรมการทำงานในรูปแบบภาพเคลื่อนไหวในช่วงเวลาดังกล่าวได้

5.3.10 สามารถทำ Session Sharing และ Remote Control บน RDP Session ขณะที่ผู้ใช้งานกำลังใช้งานอยู่ได้

5.3.11 สามารถให้เจ้าหน้าที่เรียกดูเซสชั่น (Session) ที่ผู้ใช้งานกำลังปฏิบัติงานแบบ Real Time และสามารถตัดสิทธิ์ (Terminate) การใช้งานของผู้ใช้งานที่กำลังใช้งานอยู่ได้

5.3.12 สามารถตัดสิทธิ์ (Terminate) การใช้งาน เมื่อมีการเรียกใช้คำสั่ง (Command) ที่ไม่อนุญาตบนอุปกรณ์ปลายทางที่ใช้งานด้วยโปรโตคอล SSH ได้

5.3.13 สามารถเข้าถึงอุปกรณ์ปลายทางผ่าน Web Browser ได้ โดยไม่ต้องติดตั้งโปรแกรมหรือ Extension ของ Web Browser เพิ่มเติม

5.3.14 สามารถกำหนดให้มีการทำ Approval Workflow ในลักษณะ Request Approve ได้

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

5.3.15 มีการเข้ารหัส (Encrypt) ด้วยอัลกอริทึม AES 256 สำหรับข้อมูลรหัสผ่านของอุปกรณ์ปลายทาง

5.3.16 สามารถกำหนดหรือไม่กำหนด การจัดเก็บไฟล์บันทึกกิจกรรมการทำงานของผู้ใช้งาน (Video Recording) ในรูปแบบเข้ารหัสข้อมูล (Encrypt)

5.3.17 สามารถสำรองข้อมูลรหัสผ่านของอุปกรณ์ปลายทางผ่านช่องทาง E-mail Encryption ได้

5.3.18 สามารถเชื่อมต่อกับอุปกรณ์จัดเก็บข้อมูลภายนอกผ่านโปรโตคอล Network File System (NFS) หรือ Server Message Block (SMB) เพื่อใช้ในการเก็บบันทึกไฟล์บันทึกกิจกรรมการทำงานของผู้ใช้งาน (Video Recording) ได้เป็นอย่างน้อย

5.3.19 สามารถเก็บบันทึก Log โดยแสดงรายละเอียดการใช้งานอย่างน้อยดังนี้

5.3.19.1 วันและเวลาที่เริ่มต้นใช้งาน

5.3.19.2 วันและเวลาที่สิ้นสุดการใช้งาน

5.3.19.3 ระยะเวลาที่ใช้งาน

5.3.19.4 ชื่อผู้ใช้งาน

5.3.19.5 โปรโตคอล

5.3.19.6 อุปกรณ์ปลายทางที่ถูกเรียกใช้งาน

5.3.20 สามารถบริหารจัดการอุปกรณ์ผ่านทาง HTTPS และ SSH ได้

5.3.21 สามารถกำหนดสิทธิ์ในการบริหารจัดการอุปกรณ์ของเจ้าหน้าที่ Administrator ได้

5.3.22 สามารถทำงานในลักษณะ High Available หรือ Replication ได้โดยไม่มีค่าใช้จ่ายเพิ่ม

5.3.23 มีลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย เป็นระยะเวลาไม่น้อยกว่า 3 ปี นับถัดจากวันตรวจรับงานงวดสุดท้าย โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์หรือสาขาของเจ้าของผลิตภัณฑ์ในประเทศไทย

5.4 ระบบสำหรับการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) จำนวน 1 ระบบ โดยมีคุณสมบัติอย่างน้อยดังนี้

5.4.1 สามารถทำงานในลักษณะ On-Premises หรือ Cloud หรือ Hybrid ได้

5.4.2 รองรับการยืนยันตัวตนหลายรูปแบบ เช่น การใช้รหัส OTP การยืนยันผ่าน Mobile Application หรือ โทรศัพท์ หรือ SMS ได้เป็นอย่างน้อย

5.4.3 สามารถแจ้งเตือนผ่าน Mobile Application

5.4.4 สามารถตรวจสอบและอนุญาตการเข้าถึงตามเงื่อนไข (Conditional Access) เช่น ตรวจสอบอุปกรณ์ (Device Trust) และพฤติกรรมการใช้งาน (User Behavior)

5.4.5 รองรับการตรวจสอบการอัปเดตซอฟต์แวร์ สถานะของอุปกรณ์ (Device Health Check)

5.4.6 ควบคุมการเข้าถึง (Access Control) สำหรับแอปพลิเคชันต่าง ๆ เช่น Microsoft 365, Google Workspace, VPNs และแอปพลิเคชันอื่น ๆ

5.4.7 สามารถกำหนดนโยบายเฉพาะสำหรับกลุ่มผู้ใช้หรืออุปกรณ์ เช่น จำกัดการเข้าถึงจากอุปกรณ์ที่ไม่ได้รับอนุญาต

5.4.8 รองรับการเชื่อมต่อกับระบบต่าง ๆ เช่น Active Directory, LDAP, หรือ SAML-based Applications เป็นอย่างน้อย

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

5.4.9 การตรวจสอบความเสี่ยงอัจฉริยะ (Risk-Based Authentication) ที่สามารถเพิ่มระดับการยืนยันตัวตนเมื่อพบความเสี่ยง

5.4.10 มีฟังก์ชันการตรวจสอบและรายงานการเข้าถึง เช่น การวิเคราะห์ความปลอดภัยของผู้ใช้งานและอุปกรณ์

5.4.11 การตรวจสอบความเสี่ยงอัจฉริยะ (Risk-Based Authentication) ที่สามารถเพิ่มระดับการยืนยันตัวตนเมื่อพบความเสี่ยง

5.4.12 รองรับการใช้งานร่วมกับ VPN, ระบบ Remote Desktop และระบบบริหารจัดการสิทธิ์ผู้ใช้งานและควบคุมการเข้าถึงอุปกรณ์ที่กำหนดได้

5.4.13 มีลิขสิทธิ์การใช้งานได้ไม่น้อยกว่า 50 Users

5.4.14 มีลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย เป็นระยะเวลาไม่น้อยกว่า 3 ปี นับถัดจากวันตรวจรับงานงวดสุดท้าย โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์หรือสาขาของเจ้าของผลิตภัณฑ์ในประเทศไทย

5.5 เครื่องคอมพิวเตอร์แม่ข่ายแบบประสิทธิภาพสูง (High Performance Server) พร้อมระบบบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือนสำหรับระบบ PAM จำนวน 1 ระบบ ประกอบด้วย

5.5.1 เครื่องคอมพิวเตอร์แม่ข่ายแบบประสิทธิภาพสูง (High Performance Server) จำนวน 2 ชุด โดยแต่ละชุดมีคุณสมบัติอย่างน้อยดังนี้

5.5.1.1 เป็นเครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบติดตั้งบน Rack โดยเฉพาะที่มีความสูงไม่เกิน 2U ตามมาตรฐาน EIA พร้อมรางเลื่อน

5.5.1.2 มีหน่วยประมวลผลกลางแบบ 16 แกนหลัก (16 Core) หรือดีกว่า โดยมีความเร็วสัญญาณนาฬิกาไม่ต่ำกว่า 3.6 GHz จำนวนไม่น้อยกว่า 2 หน่วย

5.5.1.3 มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันไม่น้อยกว่า 45 MB

5.5.1.4 มีหน่วยความจำหลัก (RAM) ชนิด DDR5 RDIMM หรือดีกว่า ขนาดรวมไม่น้อยกว่า 256 GB โดยตัวเครื่องต้องมี RDIMM Slot ไม่น้อยกว่า 32 ช่อง โดยรองรับการขยายได้รวมสูงสุดไม่น้อยกว่า 8 TB

5.5.1.5 มีDriver, Firmware, Software Management tools มาพร้อมกับตัวเครื่องคอมพิวเตอร์โดยทำการติดตั้งบน NAND Storage ที่อยู่บนเมนบอร์ดจากโรงงาน

5.5.1.6 มีช่องขยายแบบ PCIe 5.0 หรือดีกว่า ไม่น้อยกว่า 2 ช่องและรองรับการขยายเพิ่มรวมได้สูงสุดไม่น้อยกว่า 3 ช่อง

5.5.1.7 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10GBASE-T (RJ-45) หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง

5.5.1.8 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10 Gb SFP+ หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง พร้อม Transceiver ชนิด 10GBASE-SR (SFP+) จำนวนไม่น้อยกว่า 2 โมดูล

5.5.1.9 มีหน่วยจัดเก็บข้อมูลชนิด SSD หรือดีกว่า จำนวนไม่น้อยกว่า 2 หน่วย โดยแต่ละหน่วยจะต้องมีความจุไม่น้อยกว่า 960 GB รองรับการถอดเปลี่ยนแบบ Hot-Plug หรือ Hot-swap ได้

5.5.1.10 มีหน่วยจัดเก็บข้อมูลชนิด SSD หรือดีกว่า จำนวนไม่น้อยกว่า 9 หน่วย โดยแต่ละหน่วยจะต้องมีความจุไม่น้อยกว่า 1.92 TB รองรับการถอดเปลี่ยนแบบ Hot-Plug หรือ Hot-swap ได้

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

5.5.1.11 มีระบบควบคุมการจัดเก็บข้อมูล (Storage Controller) แบบ Hardware RAID รองรับการทำ RAID ชนิด RAID 0, 1, 5 ได้เป็นอย่างน้อย โดยมีหน่วยความจำไม่น้อยกว่า 4 GB

5.5.1.12 มี Power Supplies ขนาดไม่น้อยกว่า 1,500 Watts จำนวน 2 หน่วย และรองรับการถอดเปลี่ยนแบบ Hot Plug หรือ Hot Swap ได้โดยมีมาตรฐานประสิทธิภาพการใช้พลังงานไม่ต่ำกว่า 80 plus

5.5.1.13 มีพอร์ตเชื่อมต่ออุปกรณ์ชนิด USB 3.0 หรือดีกว่า จำนวนไม่น้อยกว่า 2 พอร์ต

5.5.1.14 มี Remote Management Port อย่างน้อย 1 พอร์ต เพื่อช่วยในการจัดการกับ Server จากระยะไกลผ่าน Web Base Application สามารถสั่ง Power On, Power OFF, Restart เครื่อง Server และตั้งค่าใน BIOS ได้และสามารถทำ Virtual KVM Remote Graphical Console, Virtual Power Button Control, Virtual Media และ Virtual Folder ได้ รองรับการสั่งการสั่งงานระยะไกล (Remote) ได้เป็นอย่างน้อย

5.5.1.15 สามารถบริหารจัดการเครื่องผ่าน Management Port ชนิด USB ที่ติดตั้งอยู่ด้านหน้าเครื่องได้

5.5.1.16 มีเมนูคำสั่งกำหนดการทำงาน เพื่อเพิ่มประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย ให้ตรงกับลักษณะของงาน (Workload Profile)

5.5.1.17 มีระบบรักษาความปลอดภัยสำหรับ Firmware (UEFI Secure Boot) และสามารถกู้คืน Firmware ที่มีปัญหาได้โดยอัตโนมัติ อีกทั้งรองรับมาตรฐานความปลอดภัยอื่นๆ ได้แก่ FIPS 140-2, AES, 3DES และ CNSA เป็นต้น

5.5.1.18 มีระบบบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายผ่านบริการแบบ Cloud Service ที่ให้บริการโดยตรงจากเจ้าของผลิตภัณฑ์ เพื่อบริหารจัดการอัพเดต Firmware และ Monitor Firmware Compliance ได้ โดยสามารถแจ้งเตือนเกี่ยวกับฮาร์ดแวร์ผ่านทาง email และรองรับการเชื่อม Multi-Factor Authentication (MFA) สำหรับแต่ละ User ได้เป็นอย่างน้อย

5.5.1.19 รองรับการทำงานร่วมกับ Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Canonical Ubuntu, Oracle Linux และ VMware ได้เป็นอย่างน้อย

5.5.1.20 เครื่องคอมพิวเตอร์แม่ข่ายที่เสนอมา ได้รับการรับรองตามมาตรฐานอย่างน้อย ดังนี้

1) มาตรฐานการผลิต/บริการตาม ISO 9001 Series
2) มาตรฐานระบบการจัดการสิ่งแวดล้อม ISO 14001
3) มาตรฐานการแพร่กระจายคลื่นแม่เหล็กไฟฟ้าตาม FCC หรือ EN หรือ VCCI หรือ CE
4) มาตรฐานความปลอดภัยด้านไฟฟ้าตาม UL หรือ EN หรือ TUV หรือ CSA หรือ IEC

5.5.2 ระบบบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายแบบเสมือน จำนวน 1 ชุด โดยมีคุณสมบัติอย่างน้อย ดังต่อไปนี้

5.5.2.1 สามารถบริหารจัดการแบบรวมศูนย์ (Unified Management) ได้

5.5.2.2 รองรับการทำ High Availability (HA) โดยทำการเปิดคอมพิวเตอร์เสมือนใหม่ได้โดยอัตโนมัติกรณีที่เครื่องคอมพิวเตอร์แม่ข่าย หรือ Operating System มีปัญหา

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

5.5.2.3 สามารถย้ายคอมพิวเตอร์เสมือนระหว่างเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์จัดเก็บข้อมูลในขณะทำงาน (Live Migration หรือ V-motion) โดยไม่ส่งผลกระทบต่อการให้บริการ

5.5.2.4 สามารถกระจายโหลดงานระหว่างเครื่องคอมพิวเตอร์แม่ข่าย (Distributed Workload)

5.5.2.5 รองรับการใช้งานร่วมกับอุปกรณ์จัดเก็บข้อมูลภายนอก (External Storage Support) ด้วยการเชื่อมต่อแบบ iSCSI, NFS และ Fiber Channel

5.5.2.6 รองรับการทำงานร่วมกับ Storage Array Base Snapshot โดยตรงจากอุปกรณ์จัดเก็บข้อมูล

5.5.2.7 สามารถเพิ่มอุปกรณ์ต่าง ๆ ให้กับเครื่องคอมพิวเตอร์เสมือน (Virtual Machine: VM) ขณะเครื่องยังคงทำงานอยู่ โดยคุณสมบัตินี้สามารถใช้ในการเพิ่มหน่วยประมวลผลกลาง (CPU) หน่วยความจำ (Memory) และช่องเชื่อมต่อเคือข่าย (Network Adapter) ได้

5.5.2.8 สามารถบริหารจัดการเครือข่ายเสมือนผ่านระบบศูนย์กลางได้

5.5.2.9 สามารถกำหนดและบริหารจัดการกลุ่มของ IP Address (IP Pools) ที่เชื่อมโยงกับเครือข่ายของคอมพิวเตอร์เสมือนได้

5.5.2.10 รองรับการให้บริการทำงานอัตโนมัติ โดยทำงานร่วมกับสคริปต์ (Scripts) ได้แก่ Bash และ PowerShell ได้

5.5.2.11 มีลิขสิทธิ์ใช้งานถูกต้องตามกฎหมาย ครอบคลุมทรัพยากรเครื่องคอมพิวเตอร์แม่ข่ายที่เสนอในโครงการนี้ เป็นระยะเวลาไม่น้อยกว่า 3 ปี นับถัดจากวันตรวจรับงานงวดสุดท้าย โดยมีหนังสือรับรองจากเจ้าของผลิตภัณฑ์หรือสาขาของเจ้าของผลิตภัณฑ์ในประเทศไทย

6. ขอบเขตการดำเนินงาน

6.1 ผู้ขายมีหน้าที่จัดหา ติดตั้ง กำหนดค่า และส่งมอบอุปกรณ์หรือครุภัณฑ์ที่จัดซื้อในครั้งนี้ให้ครบถ้วนสมบูรณ์ตามข้อกำหนด

6.2 กรณีที่ผู้ขายดำเนินการติดตั้งพร้อมตั้งค่าระบบอุปกรณ์ หากต้องมีการจัดหาอุปกรณ์ส่วนเสริมเพิ่มเติมที่จำเป็นสำหรับติดตั้งอุปกรณ์เพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพ ผู้ขายต้องจัดหาเพิ่มเติมโดยไม่คิดค่าใช้จ่ายเพิ่มเติม

6.3 การดำเนินการใด ๆ ต้องได้รับความเห็นชอบจากสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานก่อนดำเนินการ หากผู้ขายดำเนินการติดตั้งระบบใด ๆ โดยไม่ได้รับความเห็นชอบ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน มีสิทธิ์ที่จะให้ผู้ขายดำเนินการรื้อถอนระบบต่าง ๆ ที่ได้ดำเนินการไปแล้ว

6.4 ผู้ขายต้องรับผิดชอบความเสียหายที่อาจจะเกิดขึ้น เนื่องจากการติดตั้งอุปกรณ์หรือความเสียหายใดที่เกิดขึ้นเนื่องจากการปฏิบัติงานของผู้ขาย โดยจะต้องดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพเดิมโดยเร็วและยินยอมชดใช้ค่าเสียหายที่เกิดขึ้นให้กับสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....

7. เงื่อนไขอื่น ๆ

ผู้ขายต้องจัดทำแผนและหลักสูตรการฝึกอบรมให้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานเห็นชอบ ก่อนการจัดฝึกอบรม และจัดฝึกอบรมให้กับบุคลากรและเจ้าหน้าที่ ตามที่สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานกำหนด จำนวนไม่น้อยกว่า 5 คน โดยผู้ขายเป็นผู้รับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด

8. ระยะเวลาดำเนินงาน

ระยะเวลาในการดำเนินการ 150 วัน นับถัดจากวันลงนามในสัญญา

9. หลักเกณฑ์ในการพิจารณาข้อเสนอ

การพิจารณาผลการยื่นข้อเสนอครั้งนี้ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานจะใช้หลักเกณฑ์พิจารณาตัดสินโดยใช้เกณฑ์ราคา

10. งบประมาณโครงการ

งบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2569 จำนวนทั้งสิ้น 34,570,500 บาท (สามสิบสี่ล้าน-ห้าแสนเจ็ดหมื่นห้าร้อยบาทถ้วน)

11. การส่งมอบงาน และการจ่ายเงิน

11.1 งวดที่ 1 ภายใน 30 วัน นับถัดจากวันที่ลงนามในสัญญา เบิกจ่ายเงินร้อยละ 10 ของวงเงินงบประมาณตามสัญญา และคณะกรรมการตรวจรับพัสดุได้ทำการตรวจรับเรียบร้อยแล้ว โดยผู้ขายต้องส่งมอบเอกสาร อย่างน้อยดังนี้

11.1.1 แผนการบริหารโครงการ (Project Management Plan)

11.1.2 แผนการดำเนินการโครงการ (Implementation Plan)

11.2 งวดที่ 2 ภายใน 120 วัน นับถัดจากวันที่ลงนามในสัญญา เบิกจ่ายเงินร้อยละ 50 ของวงเงินงบประมาณตามสัญญา และคณะกรรมการตรวจรับพัสดุได้ทำการตรวจรับเรียบร้อยแล้ว โดยผู้ขายต้องส่งมอบอุปกรณ์ ตามรายการครุภัณฑ์ ข้อ 4 ครบถ้วนแล้ว

11.3 งวดที่ 3 ภายใน 150 วัน นับถัดจากวันที่ลงนามในสัญญา เบิกจ่ายเงินร้อยละ 40 ของวงเงินงบประมาณตามสัญญา และคณะกรรมการตรวจรับพัสดุได้ทำการตรวจรับเรียบร้อยแล้ว โดยผู้ขายต้องติดตั้งอุปกรณ์ทั้งหมดและทดสอบการทำงานภาพรวม รวมถึงการฝึกอบรม เอกสารการออกแบบติดตั้งและเอกสารคู่มือการใช้งานเป็นภาษาไทย พร้อมจัดส่งแผนการบำรุงรักษาในช่วงการรับประกัน ตามข้อ 13.1

<u>หมายเหตุ</u> ผู้ขายต้องส่งมอบเอกสารในแต่ละงวดงาน ในรูปแบบสื่อสิ่งพิมพ์ อย่างน้อย ๓ ชุด พร้อมไฟล์อิเล็กทรอนิกส์ที่สามารถแก้ไขได้ และ PDF พร้อมบันทึกลงใน Flash Drive หรือ External Hard Disk

1..... 2..... 3..... 4..... 5.....

6..... 7..... 8..... 9..... 10.....

11..... 12..... 13.....

12. อัตราค่าปรับ

12.1 กรณีผู้ขายไม่สามารถส่งมอบงานงวดสุดท้ายให้เป็นไปตามกำหนดระยะเวลาการส่งมอบงาน สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานจะดำเนินการปรับเป็นรายวันในอัตราร้อยละ 0.2 ของมูลค่าตามสัญญานับถัดจากวันที่กำหนดแล้วเสร็จตามสัญญา จนถึงวันที่ผู้ขายปฏิบัติตามสัญญาถูกต้องครบถ้วนและสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานได้ตรวจรับงานแล้ว

12.2 ระหว่างระยะเวลารับประกัน หากมีการชำรุดบกพร่องหรือข้อขัดข้องอันเนื่องมาจากการใช้งานตามปกติ ผู้ขายต้องจัดเจ้าหน้าที่เข้ามาซ่อมแซมและแก้ไขภายใน 2 ชั่วโมงหลังจากที่ได้รับแจ้งจากสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐานและแก้ไขให้แล้วเสร็จภายใน 6 ชั่วโมงโดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น ทั้งนี้ หากไม่สามารถดำเนินการให้แล้วเสร็จภายใน 6 ชั่วโมง ผู้ขายต้องยินยอมให้ผู้ซื้อคิดค่าปรับในอัตราร้อยละ 0.1 ต่อวันของเงินหลักประกันสัญญา

13. รายละเอียดการรับประกัน

13.1 ผู้ขายต้องจัดทำแผนการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance: PM) และการบำรุงรักษาเชิงแก้ไข (Corrective Maintenance: CM) ในช่วงระยะเวลาการรับประกัน พร้อมจัดส่งให้สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน

13.2 ผู้ขายต้องบำรุงรักษา และรับประกันการใช้งานฮาร์ดแวร์และซอฟต์แวร์ที่นำเสนอ ตลอดจนรับผิดชอบดูแลแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นในระบบ รวมทั้งปรับแต่งระบบให้สามารถใช้งานได้อย่างมีประสิทธิภาพ โดยมีระยะเวลาการรับประกันทั้งสิ้น 3 ปี โดยนับถัดจากวันที่คณะกรรมการตรวจรับพัสดุตรวจรับงานงวดสุดท้ายเรียบร้อยแล้ว หากมีการชำรุดบกพร่องหรือข้อขัดข้องอันเนื่องมาจากการใช้งานตามปกติ ผู้ขายต้องจัดเจ้าหน้าที่เข้ามาซ่อมแซมและแก้ไขภายใน 2 ชั่วโมงหลังจากที่ได้รับแจ้งจากผู้ดูแลระบบและแก้ไขให้แล้วเสร็จภายใน 6 ชั่วโมงโดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น ทั้งนี้ หากไม่สามารถดำเนินการให้แล้วเสร็จภายใน 6 ชั่วโมง ผู้ขายต้องยินยอมให้ผู้ซื้อคิดค่าปรับในอัตราร้อยละ 0.1 ต่อวันของเงินหลักประกันสัญญา

13.3 ผู้ขายต้องรักษาความลับและไม่นำเนื้อหาข้อมูล รูปภาพ และข้อมูลใด ๆ ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ไปเผยแพร่

13.4 ผู้ขายต้องจัดให้มีศูนย์บริการ Help Desk ซึ่งสามารถให้บริการช่วยเหลือผู้ใช้งานได้ตลอด 24 ชั่วโมง โดยสามารถติดต่อประสานงาน แจ้งปัญหา ให้คำปรึกษา และแก้ไขปัญหาได้ในวันและเวลาทำการ ยกเว้น กรณีที่เกิดเหตุขัดข้องเร่งด่วนต้องสามารถติดต่อได้นอกเวลาทำการ

14. หน่วยงานที่รับผิดชอบ

สำนักเทคโนโลยีเพื่อการเรียนการสอน สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
อีเมล obecict@obec.go.th
โทรศัพท์ 02-288-5906

1..... 2..... 3..... 4..... 5.....
6..... 7..... 8..... 9..... 10.....
11..... 12..... 13.....