EXIM THAILAND

ประกาศราคากลาง

ลำดับ	รายการ/ชื่อเรื่อง	วิธี	ราคากลาง	ประเภทไฟล์	วันที่ประกาศ
1	ประกาศราคากลาง การจ้างผู้ให้บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็บไซต์ (/getattachment/7f190647-05ae-4abd-827c-c75a0f7a2a23/ประกาศราคากลาง-การจางผใหบรการปองกนภยคกคาม-DDOS-และเพมประสทธภาพของเวปไซต.aspx)	วิธีพิเศษ	1,318,000.00	PDF (/getattachment/7f190647-05ae-4abd-827c-	30 กรกฎาคม 2567
2	ประกาศราคากลางเช่ารถยนต์ประจำตำแหน่งสำหรับผู้บริหารฝ่าย (/getattachment/968d426d-2312-4543-afcc-0b680f561352/ประกาศราคากลางเชารถยนตประจำตำแหนงสำหรบผบรหารฝาย.aspx)	วิธีคัดเลือก	6,480,000.00	PDF (/getattachment/968d426d-2312-4543-afcc-	24 กรกฎาคม 2567
3	ประกาศราคากลางงานจ้างผู้ให้บริการเช่าระบบสำรองข้อมูล Backup as a Service (/getattachment/d67ae886-b507-455a-8879-35fc73441d25/ประกาศราคากลางงานจางผใหบรการเชาระบบสำรองขอมล-Backup-as-a-Service.aspx)	วิธีพิเศษ	2,136,400.00	PDF (/getattachment/d67ae886-b507-455a-8879-	24 กรกฎาคม 2567
4	ประกาศราคากลาง การจัดซื้อแบตเตอรี่เครื่องสำรองไฟฟ้า (UPS) (/getattachment/321d2013-1a1d-4c56-af0a-bde8708b952f/ประกาศราคากลาง-การจดซอแบตเตอรเครองสำรองไฟฟา-(UPS).aspx)	วิธีเฉพาะเจาะจง	1,498,856.00	PDF (/getattachment/321d2013-1a1d-4c56-af0a-	23 กรกฎาคม 2567
5	ประกาศราคากลาง การจ้างผู้ให้บริการเช่าใช้บริการ Security Operation Center (SOC) (/getattachment/30008d30-eead-4501-b5a3-984817576db7/ประกาศราคากลาง-การจางผใหบรการเชาใชบรการ-Security-Operation-Center-(SOC).aspx)	วิธีพิเศษ	3,265,661.40	PDF (/getattachment/30008d30-eead-4501-b5a3-	08 กรกฎาคม 2567
6	ประกาศราคากลาง งานจ้างผู้ให้บริการบำรุงรักษา WAF and Network Traffic Management (/getattachment/286be717-a7b2-4371-83c1-53315c42ce28/ประกาศราคากลาง-งานจางผใหบรการบำรงรกษา-WAF-and-Network-Traffic-Management.aspx)	วิธีพิเศษ	1,471,250.00	PDF (/getattachment/286be717-a7b2-4371-83c1-	08 กรกฎาคม 2567
7	ประกาศราคากลาง การจ้างผู้ให้บริการศูนย์สำรองระบบคอมพิวเตอร์ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉิน (/getattachment/139b5309-30a0-4568-95c4-b6ca813333d9/ประกาศราคากลาง-การจางผใหบรการศนยสำรองระบบคอมพวเตอรตามแผนกอบกธรกจก	วิธีพิเศษ	3,695,352.00	PDF (/getattachment/139b5309-30a0-4568-95c4-	05 กรกฎาคม 2567
8	ประกาศราคากลาง การจัดซื้อข้อมูลคดีความในระบบรวมศูนย์การตรวจสอบข้อมูลคดีความและข้อมูลภาครัฐ (/getattachment/638d2ace-8287-4198-b813-445fae3df7a1/ประกาศราคากลาง-การจดซอขอมลคดความในระบบรวมศนยการตรวจสอบขอมลคดความและขอมล	วิธีพิเศษ	1,001,520.00	PDF (/getattachment/638d2ace-8287-4198-b813-	01 กรกฎาคม 2567
9	ประกาศราคากลาง การจ้างผู้ให้บริการบำรุงรักษาเครื่องแม่ข่ายแบบเสมือน 6 เครื่อง (/getattachment/b82a4ad7-0d65-4498-8166-1b725ab5272a/ประกาศราคากลาง-การจางผใหบรการบำรงรกษาเครองแมขายแบบเสมอน-6-เครอง.aspx)	วิธีประกาศเชิญชวน	1,458,493.00	PDF (/getattachment/b82a4ad7-0d65-4498-8166-	26 มิถุนายน 2567
10	ประกาศราคากลาง การจ้างผู้ให้บริการเช่าระบบป้องกันการบุกรุก Firewall for Internet Zone (/getattachment/1a0e27a4-78c7-4213-a7fb-09be171bd720/ประกาศราคากลาง-การจางผใหบรการเชาระบบปองกนการบกรก-Firewall-for-Internet-Zone.aspx)	วิธีพิเศษ	2,337,950.00	PDF (/getattachment/1a0e27a4-78c7-4213-a7fb-	25 มิถุนายน 2567

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจัดซื้อข้อมูลคดีความในระบบรวมศูนย์การตรวจสอบข้อมูลคดีความและข้อมูลภาครัฐ**

   หน่วยงานเจ้าของโครงการ **ฝ่ายบริหารหนี้**

2. วงเงินงบประมาณที่ได้รับจัดสรร **1,008,000.- บาท (หนึ่งล้านแปดพันบาทถ้วน)**

3. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 1/7/2567

   เป็นเงิน 1,001,520.- บาท (หนึ่งล้านหนึ่งพันห้าร้อยยี่สิบบาทถ้วน)

   ราคา/หน่วย (ถ้ามี) - บาท

4. แหล่งที่มาของราคากลาง (ราคาอ้างอิง) : บริษัท ดาต้า มาร์ท จำกัด

5. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง)

   5.1 นายวิวัฒน์ แซ่ตั้ง ผู้ช่วยผู้บริหารฝ่ายบริหารหนี้

   5.2 นางสาวทวินุช กลิ่นสุคนธ์ ผู้จัดการประจำฝ่ายทรัพยากรบุคคล

   5.3 นางวิจุฬา ทองสิมา ผู้ช่วยผู้บริหารส่วนจัดซื้อทั่วไป

ผนวก 1

ขอบเขตการดำเนินงาน

การจัดซื้อข้อมูลคดีความในระบบรวมศูนย์การตรวจสอบข้อมูลคดีความและข้อมูลภาครัฐ

ผู้เสนอราคา ต้องให้บริการข้อมูลคดีความและข้อมูลภาครัฐ (ข้อมูลคดีล้มละลายและคดีขายทอดตลาดทรัพย์) ตามขอบเขตงานที่ธนาคารกำหนด ดังนี้

1. ให้สิทธิ์ธนาคารใช้งานข้อมูลคดีความและข้อมูลภาครัฐ (ข้อมูลคดีล้มละลายและคดีขายทอดตลาดทรัพย์) รวมถึงข้อมูลที่จะมีการเพิ่มเติมรายเดือนตลอดระยะเวลาการให้บริการ

2. ให้บริการข้อมูลคดีล้มละลายและคดีขายทอดตลาดทรัพย์ ที่เป็นข้อมูลจากกรมบังคับคดี กระทรวงยุติธรรม ซึ่งเป็นข้อมูลคดีล้มละลายทั้งประเทศ และมีข้อมูลย้อนหลัง ตั้งแต่ปี พ.ศ.2527 จนถึงปัจจุบัน ให้อยู่ในรูปแบบ Text File หรือ DBF File โดยธนาคารจะเป็นผู้พัฒนาระบบที่สามารถ Convert ข้อมูล Text File หรือ DBF File ได้เอง และสามารถดูประวัติคดีแดงและข้อมูลทรัพย์ย้อนหลังของแต่ละคดีได้ทั้งหมด และสามารถติดตามความคืบหน้าได้อย่างรวดเร็วจากการได้รับข้อมูลที่ทันสมัยและเป็นปัจจุบัน ทั้งคดีแดงใหม่ การเปลี่ยนแปลงทางคดีของแต่ละจำเลยรวมทั้งทรัพย์ใหม่และทรัพย์เดิมที่รอขายทุกสัปดาห์ ให้เป็นไปตามที่กรมบังคับคดีมีการปรับปรุงข้อมูล โดยข้อมูลจะต้องประกอบด้วยรายละเอียดดังนี้

2.1 ข้อมูลคดีล้มละลาย ประกอบด้วย เลขคดีแดง เลขคดีดำ (ถ้ามี) รหัสศาล ชื่อศาล ชื่อโจทก์ เลขบัตรประชาชน/เลขทะเบียนนิติบุคคลของจำเลย ภูมิลำเนาที่อยู่ของผู้ล้มละลาย จำเลยที่ ลำดับที่ของจำเลย ประเภทจำเลย (นิติบุคคล/บุคคลธรรมดา) ชื่อจำเลย เลขบัตรประชาชน/เลขทะเบียนนิติบุคคลของจำเลย ที่อยู่จำเลย สถานะคดีของจำเลย เรื่อง (เช่น พิทักษ์ทรัพย์เด็ดขาด,ล้มละลาย) วันที่ประกาศตามคำสั่งศาล วันที่ประกาศเจ้าพนักงาน วันที่ประกาศโฆษณาในหนังสือพิมพ์ วันที่ประกาศโฆษณาในราชกิจจานุเบกษา เป็นอย่างน้อย

ในกรณีกรมบังคับคดี มีการระบุเลขบัตรประจำตัวประชาชนหรือเลขทะเบียนนิติบุคคลในเอกสารกรมบังคับคดี ซึ่งผู้ให้บริการได้มีการบันทึกข้อมูลจากเอกสารที่ได้รับจากกรมบังคับคดี ผู้ให้บริการจะปรับปรุงข้อมูลให้ทันสมัยและเป็นปัจจุบัน

2.2 ข้อมูลคดีขายทอดตลาดทรัพย์ ประกอบด้วย เลขคดี ชื่อโจทก์ ชื่อจำเลย ชื่อศาล ประเภททรัพย์ รายละเอียดทรัพย์ สถานที่ตั้งทรัพย์ ชื่อผู้ครอบครองทรัพย์/เจ้าของกรรมสิทธิ์ วันที่นัดประมูล สถานที่นัด ราคาประเมิน(ถ้ามี) ประเภทการขาย วันที่ขายทรัพย์ ชื่อสำนักบังคับคดีจังหวัด

3. ดำเนินการในการนำส่งข้อมูลส่วนเพิ่มเติมรวมทั้งข้อมูลที่มีการ Update รายละเอียดเพิ่มเติมหรือข้อมูลที่มีการแก้ไขจากต้นทางให้แก่ธนาคาร ไม่น้อยกว่า 3 ครั้งต่อเดือน โดยนำส่งข้อมูลคดีล้มละลายและคดีขายทอดตลาดทรัพย์ทั้งหมดที่ทางบริษัทฯ เก็บรวบรวม ในรูปแบบของ Text File นำส่งทาง Link ที่ธนาคารกำหนด

4. ให้มีการรับประกันและเงื่อนไขการบำรุงรักษา อย่างน้อยดังนี้

4.1 ในกรณีข้อมูลที่ทางธนาคารได้รับจากผู้ให้บริการมีข้อผิดพลาด ไม่ถูกต้อง ผู้ให้บริการตกลงที่จะดำเนินการแก้ไขข้อผิดพลาดดังกล่าว และ/หรือจัดส่งข้อมูลใหม่ที่ถูกต้อง

4.2 ในการจัดส่ง และ/หรือแก้ไขข้อมูลให้ถูกต้องดังกล่าว หากมีค่าใช้จ่ายใด ๆ เกิดขึ้นทางผู้ให้บริการ ตกลงเป็นผู้รับผิดชอบค่าใช้จ่ายดังกล่าวเองทั้งสิ้น

4.3 จะต้องให้คำปรึกษา แนะนำ กรณีที่เกิดปัญหาหรือข้อผิดพลาดในการนำเข้าชุดข้อมูลในระหว่างเวลา 8:30 – 17:30 น. ของวันทำการของธนาคาร โดยไม่คิดค่าใช้จ่าย

4.4 จะต้องรับประกันความชำรุดบกพร่องหรือข้อขัดข้องของการบันทึกข้อมูล (การนำเข้าข้อมูล) ที่ไม่สามารถใช้งานได้ไม่ว่าทั้งหมดหรือบางส่วนและยอมรับที่จะดำเนินการแก้ไขความชำรุดบกพร่องนั้นภายใน 3 วันหลังจากได้รับแจ้งจากธนาคาร

5. ระยะเวลาการให้บริการข้อมูล

ระยะเวลาดำเนินงาน 1 ปี (ตั้งแต่วันที่ 1 สิงหาคม 2567 ถึงวันที่ 31 กรกฎาคม 2568)

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างผู้ให้บริการศูนย์สำรองระบบคอมพิวเตอร์ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉิน**

2. หน่วยงานเจ้าของโครงการ **ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ**

3. วงเงินงบประมาณที่ได้รับจัดสรร 3,700,000.00 บาท **(สามล้านเจ็ดแสนบาทถ้วน)**

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 05 ก.ค. 2567

   เป็นเงิน 3,695,352.00 บาท **(สามล้านหกแสนเก้าหมื่นห้าพันสามร้อยห้าสิบสองบาทถ้วน)**

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   บริษัท ดาต้าโปร คอมพิวเตอร์ ซิสเต็มส์ จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายฉัตรชัย	อาศรมเงิน	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่ายปส.
6.2 นายจรินทร์	เบญจรงคพันธ์	ผู้ช่วยผู้บริหารส่วนพัฒนาระบบสารสนเทศบริการ 1 / ฝ่ายพส.
6.3 นายกิตติ์ธเนศ	วงศ์ประสิทธิ์	ผู้ช่วยผู้บริหารส่วนบริการและปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่ายปส.

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการศูนย์สำรองระบบคอมพิวเตอร์ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉิน

ผู้ยื่นข้อเสนอต้องจัดให้มีศูนย์สำรองระบบคอมพิวเตอร์ ซึ่งประกอบด้วยเครื่องคอมพิวเตอร์ ระบบสื่อสัญญาณ ระบบ Internet ระบบกระแสไฟฟ้า ระบบกระแสไฟฟ้าสำรอง (UPS/Generator) ไฟฟ้าส่องสว่าง ระบบปรับอากาศ รวมถึงบุคลากร ซึ่งมีคุณลักษณะ มีมาตรฐานและมีคุณสมบัติตามที่ธนาคารกำหนด สำหรับให้ธนาคารใช้ปฏิบัติงานเมื่อเกิดเหตุฉุกเฉิน ในกรณีสถานที่ทำงาน เครื่องใช้อุปกรณ์คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ของธนาคารได้รับความเสียหายไม่สามารถใช้งานได้ไม่ว่าทั้งหมดหรือบางส่วน หรือเป็นเหตุให้เจ้าหน้าที่ของธนาคารไม่สามารถเข้าไปปฏิบัติงานในสถานที่ทำงานได้ตามปกติ ทั้งนี้ผู้ยื่นข้อเสนอจะต้องจัดเตรียมศูนย์สำรองระบบคอมพิวเตอร์พร้อมส่วนประกอบต่าง ๆ สำหรับให้บริการแก่ธนาคารอย่างน้อยดังต่อไปนี้

1. **ห้องปฏิบัติงาน**

จำนวน 1 ห้อง พร้อมติดตั้งเครื่องคอมพิวเตอร์ลูกข่าย อุปกรณ์คอมพิวเตอร์รวมทั้งโต๊ะ เก้าอี้ และอุปกรณ์เครื่องใช้สำนักงานเพื่อรองรับการปฏิบัติงานของเจ้าหน้าที่ธนาคาร จำนวน 3 ที่นั่ง โดยผู้ยื่นข้อเสนอจะต้องทำการเชื่อมโยงระบบเครือข่ายระหว่างเครื่องคอมพิวเตอร์ลูกข่ายกับเครื่องคอมพิวเตอร์แม่ข่ายที่ติดตั้งภายในห้องศูนย์สำรองระบบคอมพิวเตอร์

2. **ระบบ Internet และ VPN**

2.1. ความเร็วไม่น้อยกว่า 200/100 Mbps. (Domestic/Inter) เพื่อรองรับการใช้งานจากเครื่องคอมพิวเตอร์ของธนาคารผ่านทาง Internet มายังเครื่องคอมพิวเตอร์แม่ข่ายที่ห้องศูนย์สำรองระบบคอมพิวเตอร์ ได้อย่างมีประสิทธิภาพ

2.2. มีระบบ VPN เพื่อรองรับการใช้งานจากเครื่องคอมพิวเตอร์ของธนาคารผ่านทาง Internet มายังศูนย์สำรองระบบคอมพิวเตอร์ไม่น้อยกว่า 100 บัญชีผู้ใช้งาน

3. **บุคลากร**

ผู้ยื่นข้อเสนอต้องจัดให้มีบุคลากรซึ่งเป็นพนักงานประจำของผู้ยื่นข้อเสนอเท่านั้น เพื่อทำหน้าที่เป็นผู้ประสานงานหรือผู้ดำเนินงานให้บริการระบบคอมพิวเตอร์อย่างน้อย ดังต่อไปนี้

3.1. ผู้จัดการโครงการ (Project Manager) จำนวน 1 คน เพื่อปฏิบัติงาน ดังต่อไปนี้

3.1.1. ร่วมกับทางธนาคารในการจัดทำแผนการดำเนินงาน (Project Plan) สำหรับแผนการกู้คืนระบบคอมพิวเตอร์ Disaster Recovery Action Plan (DRP) ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉินของทางธนาคาร Business Continuity Plan (BCP) (เฉพาะส่วนที่ผู้ให้บริการเกี่ยวข้อง)

3.1.2. ติดตามและประเมินผลการดำเนินงานให้คำแนะนำเพื่อให้การกู้คืนระบบคอมพิวเตอร์ Disaster Recovery Action Plan (DRP) ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉินของทางธนาคาร Business Continuity Plan (BCP) (เฉพาะส่วนที่ผู้ให้บริการเกี่ยวข้อง)

3.1.3. ร่วมกับทางธนาคารในการดำเนินการทดสอบตามแผนการกู้คืนระบบคอมพิวเตอร์ Disaster Recovery Action Plan (DRP) ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉินของทางธนาคาร Business Continuity Plan (BCP)

3.1.4. รายงานความเรียบร้อยในการทดสอบให้ธนาคารทราบ

3.1.5. ให้ความร่วมมือและสนับสนุนธนาคารในการให้บริการศูนย์สำรองระบบคอมพิวเตอร์ ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉินของทางธนาคาร Business Continuity Plan (BCP)

3.2. วิศวกรระบบ (System Engineer) จำนวนอย่างน้อย 2 คน เพื่อปฏิบัติงานดังต่อไปนี้

3.2.1. ประสานงานกับเจ้าหน้าที่ด้านเทคนิคและโปรแกรมคอมพิวเตอร์ของธนาคารในการดำเนินการติดตั้งโปรแกรมระบบคอมพิวเตอร์ที่จำเป็นในการใช้งานและเชื่อมโยงสัญญาณระบบเครือข่ายคอมพิวเตอร์

3.2.2. ให้ความร่วมมือและสนับสนุนธนาคารในการดำเนินการทดสอบแผนการกู้คืนระบบคอมพิวเตอร์ Disaster Recovery Action Plan (DRP) ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉินของทางธนาคาร Business Continuity Plan (BCP)

3.2.3. ให้ความร่วมมือและสนับสนุนธนาคารในการให้บริการศูนย์สำรองระบบคอมพิวเตอร์ ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉินของทางธนาคาร Business Continuity Plan (BCP)

3.3. **บุคคลอื่นๆ** ซึ่งผู้ยื่นข้อเสนอเห็นว่ามีความจำเป็นหรือเป็นประโยชน์ต่อการให้บริการ

ทั้งนี้ ผู้ยื่นข้อเสนอต้องแจ้งรายละเอียดเกี่ยวกับชื่อ ที่อยู่ วุฒิการศึกษา ตำแหน่งงาน และประสบการณ์ของบุคลากรดังกล่าวข้างต้นให้ธนาคารทราบก่อนวันที่เริ่มต้นการให้บริการ รวมทั้งแจ้งให้ธนาคารทราบทุกครั้งโดยเร็วเมื่อมีการเปลี่ยนแปลง

4. ระยะเวลาการให้บริการ

ผู้ยื่นข้อเสนอต้องให้บริการศูนย์สำรองระบบคอมพิวเตอร์ ตามขอบเขตการให้บริการที่ระบุไว้ในผนวก 1 มีกำหนดระยะเวลา 1 ปี ตั้งแต่วันที่ 25 กรกฎาคม 2567 – 24 กรกฎาคม 2568

5. การให้บริการตามแผนการกู้คืนระบบคอมพิวเตอร์ Disaster Recovery Action Plan (DRP) เมื่อธนาคารเกิดเหตุฉุกเฉิน

ผู้ยื่นข้อเสนอจะต้องดำเนินการให้ธนาคารสามารถใช้บริการศูนย์สำรองระบบคอมพิวเตอร์ เมื่อธนาคารเกิดเหตุฉุกเฉินได้เป็นระยะเวลาไม่น้อยกว่า 30 วันติดต่อกันต่อการเกิดเหตุฉุกเฉินแต่ละคราวโดยไม่จำกัดจำนวนคราว และในกรณีที่ธนาคารจำเป็นต้องใช้ศูนย์สำรองติดต่อกันเกินกว่าระยะเวลาที่ได้ตกลงร่วมกัน เมื่อธนาคารได้แจ้งผู้ให้ยื่นข้อเสนอทราบล่วงหน้าก่อนสิ้นสุดระยะเวลาดังกล่าว ผู้ยื่นข้อเสนอจะต้องให้ธนาคารใช้ศูนย์สำรองต่อไปได้ไม่น้อยกว่า 180 วัน โดยผู้ยื่นข้อเสนอมีสิทธิคิดค่าใช้จ่ายจากธนาคารตามจำนวนวันที่ใช้บริการในส่วนที่เกินกว่าระยะเวลาที่ได้ตกลงร่วมกันเป็นรายวันตามอัตราที่ผู้ยื่นข้อเสนอ เสนอต่อธนาคาร ทั้งนี้ผู้ยื่นข้อเสนอต้องพร้อมที่จะให้บริการทันทีในระยะไม่เกิน 4 ชั่วโมง นับจากเวลาที่ธนาคารนำเทประบบงาน AS/400 ไปถึงศูนย์สำรองระบบคอมพิวเตอร์

6. การทดสอบตามแผนการกู้คืนระบบคอมพิวเตอร์ Disaster Recovery Action Plan (DRP)

ตลอดระยะเวลาการให้บริการ ผู้ยื่นข้อเสนอต้องจัดให้ธนาคารได้ซ้อมหรือทดสอบแผนการกู้คืนระบบคอมพิวเตอร์ตามที่ธนาคารกำหนดอย่างน้อยปีละ 1 ครั้ง โดยในการซ้อมแผนดังกล่าวแต่ละครั้งจะต้องดำเนินการตามแผนงานการกู้คืนระบบคอมพิวเตอร์และตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉินของทางธนาคาร Business Continuity Plan (BCP) ตามที่ได้มีการกำหนดแผนร่วมกัน ทั้งนี้จำนวนวันในการทดสอบการกู้คืนระบบคอมพิวเตอร์ให้เป็นไปตามที่ธนาคารกำหนดแต่สูงสุดไม่เกิน 10 วันทำการ

7. ข้อกำหนดความต้องการทั่วไป

7.1. สามารถทำงานร่วมกับระบบคอมพิวเตอร์และระบบเครือข่ายของธนาคารในปัจจุบันได้

7.2. ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องจัดให้มีบริการแบบ On-Site Service (24x7) พร้อมให้การสนับสนุน ตามข้อ 22

8. คุณลักษณะเฉพาะขั้นต่ำของเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบ AS/400 จำนวน 1 เครื่อง

8.1 เป็นเครื่องคอมพิวเตอร์แม่ข่ายฯ แบบติดตั้งบน Rack มาตรฐาน 19 นิ้ว พร้อมอุปกรณ์

8.2 เป็นเครื่อง POWER9 รุ่น 41A (S914) แบบ CBU

8.3 มีหน่วยประมวลผลกลาง (CPU) รุ่น EP10 (4-core Typical 2.3 to 3.8 GHz (max) POWER9 Processor)

8.4 มีหน่วยความจำหลัก (RAM) ไม่น้อยกว่า 32 GB

8.5 มี hard disk แบบ SAS ความเร็ว 15k rpm ที่มีความจุไม่น้อยกว่า 283 GB จำนวน 2 หน่วย

8.6 มีหน่วยจ่ายไฟและ Redundant ขนาดต่อหน่วยไม่น้อยกว่า 1400 W จำนวนไม่น้อยกว่า 2 หน่วย

8.7 มี Network Port แบบ 1 Gigabit Ethernet จำนวนไม่น้อยกว่า 4 Port

อรินทร์

8.8 มี FC Adapter ขนาดไม่น้อยกว่า 16 Gbps จำนวนรวมไม่น้อยกว่า 4 Port สำหรับเชื่อมต่อกับ SAN Switch

8.9 มี software สำหรับใช้งานบนระบบ AS/400 ดังต่อไปนี้

8.9.1 มีระบบปฏิบัติการ (OS) สำหรับ iSeries (i/OS) เวอร์ชั่น V7R3 (5770-SS1) จำนวน 1-core license (5770-SSA)

8.9.2 มี user สำหรับใช้งาน OS (5770-SSC) จำนวน 5 หน่วย

8.9.3 มีสิทธิ์การใช้ IBM i Access Family (5770-XW1) แบบไม่จำกัด

8.9.4 มี PowerVM Enterprise Edition (5765-PVE) จำนวน 4-core license

9. คุณลักษณะเฉพาะขั้นต่ำของเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบ AIX จำนวน 1 เครื่อง

9.1 เป็นเครื่องคอมพิวเตอร์แม่ข่ายฯ แบบติดตั้งบน Rack มาตรฐาน 19 นิ้ว พร้อมอุปกรณ์

9.2 เป็นเครื่อง POWER9 รุ่น 22A (S922)

9.3 มีหน่วยประมวลผลกลาง (CPU) รุ่น EP16 (4-core Typical 2.3 to 3.8 GHz (max) POWER9 Processor)

9.4 มีหน่วยความจำหลัก (RAM) ไม่น้อยกว่า 64 GB

9.5 มี hard disk แบบ SAS ความเร็ว 15k rpm ที่มีความจุไม่น้อยกว่า 300 GB จำนวน 2 หน่วย

9.6 มีหน่วยจ่ายไฟและ Redundant ขนาดต่อหน่วยไม่น้อยกว่า 1400 W จำนวนไม่น้อยกว่า 2 หน่วย

9.7 มี Network Port แบบ 1 Gigabit Ethernet จำนวนไม่น้อยกว่า 4 Port

9.8 มี FC Adapter ขนาดไม่น้อยกว่า 16 Gbps จำนวนรวมไม่น้อยกว่า 4 Port สำหรับเชื่อมต่อกับ SAN Switch

9.9 สามารถทำ logical partition ได้

9.10 มี software สำหรับใช้งานบนระบบ AIX ดังต่อไปนี้

9.11 มีระบบปฏิบัติการ (OS) สำหรับ AIX เวอร์ชั่น 7.1 Standard จำนวน 2-core license

10. คุณลักษณะเฉพาะขั้นต่ำของเครื่องควบคุมการทำงานของระบบ AS/400 (HMC) จำนวน 1 เครื่อง

10.1 เป็นอุปกรณ์แบบติดตั้งบน Rack มาตรฐาน 19 นิ้ว พร้อมอุปกรณ์

10.2 เป็นอุปกรณ์ รุ่น 7063-CR1

10.3 รองรับการเชื่อมต่อกับเครื่องแม่ข่ายในข้อ 8

10.4 มีจอรุ่น 7316-TF4 เพื่อเชื่อมต่อกับ HMC และสามารถติดตั้งบน Rack มาตรฐาน 19 นิ้วได้

11. คุณลักษณะเฉพาะขั้นต่ำของเครื่องคอมพิวเตอร์แม่ข่าย VMware (Guest) จำนวน 22 เครื่อง

Item	Server Name	Operating System	Hardware Spec		
			vCPU (Core)	Memory (GB)	Disk (GB)
1	Zigma	Win 2012 R2 Std	2	8	90
2	KTLEAPPPRD	Win 2019	4	16	300
3	SFTP_PRD	Red Hat Enterprise Linux 5	4	4	200
4	OPER	Win 10	8	16	720
5	APIWEBWSPRD	Win 2019	4	16	180
6	Web-Portal_APP_PRD	Win 2003 Ent. R2 SP2	12	16	130
7	MY_WS_PRD	Win 2012 R2 Std	8	8	90
8	MY_WEB_PRD	Win 2019	6	8	170
9	MY_DB_PRD	Win 2008 Std R2	8	8	170
10	MY_APP_PRD	Win 2008 Std R2	8	8	110
11	MYAPPPRD	Win 2019	4	4	160
12	GL_DB1_PRD-N	Win 2008 Std R2	4	10	700

13	GL_APP1_PRD	Win 2008 Std R2	16	8	160
14	GL_APP1_PRD-N	Win 2008 Std R2	4	8	160
15	GLINFWEBPRD	Win 2016	4	16	130
16	T4DWEBPRD	Win 2012 R2 Std	8	16	90
17	T4DAPDBPRD	Win 2012 R2 Std	8	30	190
18	DTS_APP_PRD	Linux 7	2	20	350
19	SpoolAllBackup_PRD	Win 2008	16	2	400
20	NTP-Production	Oracle Solaris 10 - Linux	8	8	240
21	SKLMServerPRD	Win 2016	4	5	87
22	CIRFAPP01PRD	Red Hat Enterprise Linux 7	8	32	540

12. **คุณลักษณะเฉพาะขั้นต่ำของเครื่องคอมพิวเตอร์แม่ข่ายสำหรับ Backup Server จำนวน 1 เครื่อง**

12.1 เป็นเครื่องคอมพิวเตอร์แม่ข่ายฯ แบบติดตั้งบน Rack มาตรฐาน 19 นิ้ว พร้อมอุปกรณ์

12.2 มีหน่วยประมวลผลกลาง (CPU) รุ่น Intel Xeon-Silver 4108 (1.8GHz/8-core) จำนวน 1 หน่วยเป็นอย่างน้อย

12.3 มีหน่วยความจำหลัก (RAM) ไม่น้อยกว่า 32 GB

12.4 มี hard disk แบบ SAS ความเร็ว 10k rpm ที่มีความจุไม่น้อยกว่า 900GB จำนวน 2 หน่วย

12.5 มี Network Port แบบ 1 Gigabit Ethernet จำนวนไม่น้อยกว่า 4 Port

12.6 มี FC Adapter ขนาดไม่น้อยกว่า 16 Gbps จำนวนรวมไม่น้อยกว่า 2 Port สำหรับเชื่อมต่อกับ SAN Switch

12.7 มีระบบปฏิบัติการ Windows Server 2016 พร้อมลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย

13. **คุณลักษณะเฉพาะขั้นต่ำของอุปกรณ์จัดเก็บข้อมูล (Storage) จำนวน 1 เครื่อง**

13.1 เป็นอุปกรณ์จัดเก็บข้อมูลแบบ External Storage

13.2 มีหน่วยความจำ cache ไม่น้อยกว่า 16 GB

13.3 มี hard disk แบบ SSD ขนาด 1.92 TB จำนวนไม่น้อยกว่า 4 หน่วย

13.4 มี hard disk แบบ SAS ขนาด 900 GB จำนวนไม่น้อยกว่า 20 หน่วย

13.5 มี Fiber Port แบบ 16 Gbps จำนวนไม่น้อยกว่า 4 Port

14. **คุณลักษณะเฉพาะขั้นต่ำของอุปกรณ์ SAN switch จำนวน 2 เครื่อง**

14.1 เป็นอุปกรณ์ขนาด 1U แบบติดตั้งบน Rack มาตรฐาน 19 นิ้วพร้อมอุปกรณ์

14.2 เป็นอุปกรณ์ Fiber Channel Switch สำหรับระบบ Storage Area Network (SAN) โดยเฉพาะ

14.3 สามารถเชื่อมต่อด้วยเทคโนโลยี Fiber Channel (FC) แบบ Autosensing ที่ความเร็ว 4 Gbps, 8 Gbps และ 16 Gbps ได้ และมีจำนวนพอร์ตรวมทั้งสิ้นไม่น้อยกว่า 12 พอร์ต

14.4 มีอุปกรณ์ Optical Transceiver ชนิด Short Wave ความเร็วไม่น้อยกว่า 16 Gbps จำนวน 12 หน่วย

14.5 มีสาย Fiber Optic ประเภท LC-LC แบบ OM3 ความยาวไม่น้อยกว่า 10 เมตร จำนวน 12 เส้น

14.6 สามารถเชื่อมต่อได้ทั้ง AS/400, UNIX-Base Server และ Intel-Base Server

15. **คุณลักษณะเฉพาะขั้นต่ำของอุปกรณ์จัดเก็บข้อมูล (Tape)**

15.1. อุปกรณ์จัดเก็บข้อมูล (Tape) สำหรับระบบงาน AS/400 จำนวน 1 หน่วย

15.1.1 เป็นเทป library รุ่น TS4300 หรือดีกว่า

15.1.2 มี tape drive แบบ LTO Ultrium 8 Half high แบบ fiber จำนวน 1 หน่วย

15.1.3 สามารถเขียนและอ่านม้วนเทปชนิด Ultrium 8, Ultrium 7 ได้

15.1.4 Ultrium Cleaning Cartridge จำนวน 1 ม้วน

15.1.5 Tape library ต้องสามารถทำ encryption ได้ และต้องมี IBM Security Key Lifecycle Manager software (5641-SKM)

15.2 อุปกรณ์จัดเก็บข้อมูล (Tape) สำหรับระบบงานอื่นๆ จำนวน 1 หน่วย

15.2.1 เป็นเทป library รุ่น TS4300 หรือดีกว่า

15.2.2 มี tape drive แบบ LTO Ultrium 7 Half high แบบ fiber จำนวน 3 หน่วย

15.2.3 สามารถเขียนและอ่านม้วนเทปชนิด Ultrium 7, Ultrium 6 ได้

16. อุปกรณ์กระจายสัญญาณหลักเพื่อรองรับ Fiber Optic (Core Switch Fiber Optic) จำนวน 1 ชุด

16.1 มีหน่วยประมวลผล (CPU) ชนิด 4 Cores และมีหน่วยความจำ (Memory) ในตัวไม่น้อยกว่า 24 GB หรือเทียบเท่า

16.2 มีหน่วยเก็บข้อมูลชนิด SSD Drive ขนาดไม่น้อยกว่า 64 GB หรือเทียบเท่า

16.3 มีแหล่งจ่ายไฟ Power supply จำนวนไม่น้อยกว่า 2 หน่วย รองรับการทำงานแบบ Hot-swap และแบบ Redundant ได้

16.4 มี Port เชื่อมต่อแบบ 100M/1/10GBASE-T จำนวนไม่น้อยกว่า 48 Port

16.5 รองรับ Port เชื่อมต่อระบบเครือข่ายแบบ QSFP+ จำนวนไม่น้อยกว่า 6 Port ได้ในอนาคต

16.6 สามารถรองรับ Bandwidth ได้ไม่น้อยกว่า 2.16 Tbps และมี Forwarding rate ไม่น้อยกว่า 1.5 bpps

16.7 สามารถเชื่อมต่อกับ Switch ลูกผ่าน Fabric Extenders ได้ไม่น้อยกว่า 16 ชุด

16.8 รองรับ VLAN ID ได้ไม่น้อยกว่า 3,967 VLAN

16.9 รองรับ Mac Address ได้ไม่น้อยกว่า 256,000 Mac Address

16.10 รองรับ Multicast Route ได้ไม่น้อยกว่า 32,000 และรองรับการทำ Virtual Routing and Forwarding (VRF) ได้ไม่น้อยกว่า 16,000

16.11 รองรับ IP host entries ได้ไม่น้อยกว่า 896,000

16.12 สามารถทำงานในรูปแบบดังต่อไปนี้ได้หรือเทียบเท่า

16.12.1 VXLAN

16.12.2 EIGRP

16.12.3 OSPF

16.12.4 BGP

16.13 สามารถบริหารจัดการผ่านโปรโตคอล SNMP

16.14 อุปกรณ์ต้องผ่านมาตรฐานความปลอดภัย และคลื่นแม่เหล็กไฟฟ้า UL, EN, VCCI และ KN22

16.15 เป็นอุปกรณ์แบบติดตั้งบน Rack มาตรฐาน 19 นิ้วพร้อมอุปกรณ์

17. อุปกรณ์รักษาความปลอดภัยเครือข่าย จำนวน 1 ชุด

17.1. Firewall Appliance มี Firewall throughput (64 byte UDP packets) ไม่น้อยกว่า 27.9 Gbps

17.2. มี NGFW throughput ไม่น้อยกว่า 2.5 Gbps ในรูปแบบ Enterprise Traffic mix หรือ Appmix หรือ enterprise testing conditions

17.3. สามารถรองรับ concurrent sessions อย่างน้อย 3,000,000 sessions และมี new sessions per second ไม่น้อยกว่า 124,000 new session per second

17.4. รองรับ SSL-VPN throughput ไม่น้อยกว่า 1.4 Gbps

17.5. รองรับการใช้งาน SSL-VPN 200 concurrent users

17.6. มี Network Interface แบบ10/100/1000 จำนวนอย่างน้อย 8 พอร์ท หรือดีกว่า

17.7. มีช่องรองรับการเชื่อมต่ออุปกรณ์ต่อพ่วงประเภท 10GE/GE SFP+/ SFP ไม่น้อยกว่า 2 ช่อง หรือ Network Interface แบบ 10/5/2.5/GE RJ45 ไม่น้อยกว่า 2 ช่อง

17.8. รองรับการใช้งาน Virtual Domain หรือ Virtual system ได้ไม่น้อยกว่า 10 virtual

17.9. สามารถตรวจสอบและป้องกันการโจมตี โดยใช้ IPS , Anti-malware Protection และ Mobile Malware ได้

17.10. อุปกรณ์สามารถจัดเก็บ Log ได้ 90 วันย้อนหลังโดยสามารถเสนออุปกรณ์เพิ่มเติมโดยอยู่ภายใต้ยี่ห้อผลิตภัณฑ์เดียวกันในรูปแบบ Virtual appliance

17.11. ผลิตภัณฑ์ที่นำเสนอต้องอยู่ใน Gartner Leader Quadrant ด้าน Enterprise Network Firewalls ปี 2023 หรือใหม่กว่า

17.12. อุปกรณ์ต้องได้รับการรับรองมาตรฐาน FCC, ICES และ VCCI เป็นอย่างน้อย

17.13. ผู้ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองการบริการหลังการขายจากเจ้าของผลิตภัณฑ์หรือเป็นตัวแทนที่ได้รับการแต่งตั้ง

18. **คุณลักษณะเฉพาะขั้นต่ำของ software replicate data สำหรับระบบ AS/400 จำนวน 1 ชุด**

18.1 ใช้เทคนิคการทำเจอนัล (Journaling) ของ IBM เพื่อให้มั่นใจว่าข้อมูลจะถูกส่งผ่านได้สมบูรณ์ที่สุด

18.2 สามารถปรับขนาดความต้องการของปริมาณการรองรับการใช้งานและการปฏิบัติงานหลายๆ กระบวนการในเวลาเดียวกัน

18.3 การส่งผ่านข้อมูลไปถึงที่หมายขณะที่ระบบงานทั้ง 2 ฝั่งถูกเปิดใช้งานอยู่ ได้อย่างรวดเร็วเกือบจะสมบูรณ์ หรือ near zero downtime

18.4 สามารถส่งผ่านข้อมูลระหว่างกันได้หลากหลายรุ่นของเครื่องคอมพิวเตอร์แม่ข่าย, ระบบการจัดเก็บข้อมูลความเร็วสูง (storage), ระบบปฏิบัติงาน (OS Version) บนเครื่องคอมพิวเตอร์แม่ข่าย AS/400

18.5 รองรับการขยายระบบการเชื่อมต่อที่ซับซ้อนกับ ระบบ Backup server ที่มีมากกว่า 1 Servers เช่น การทำ HA หรือ DR

18.6 ให้สิทธิ์เข้าถึงการส่งผ่านข้อมูล สำหรับการทำสืบค้นข้อมูล (Queries), แสดงรายงานผล, การทำสำรองข้อมูล และการซ่อมบำรุง

18.7 รูปแบบการรับส่งข้อมูลสามารถรองรับทั้ง 1 ต่อ 1 หรือจะเป็นการกระจายของข้อมูลจาก 1 ไปยังหลายๆที่

18.8 สามารถส่งผลวิเคราะห์ข้อมูลตามแผนหลักของ RPO/RTO และ แจ้งประสิทธิภาพของการสลับไปใช้ระบบสำรอง (HA) ที่ผ่านมาได้

18.9 สามารถตรวจสอบความถูกต้องของข้อมูลจากการส่งผ่านข้อมูล โดยผ่านระบบตรวจสอบได้ด้วยตัวเอง

18.10 สามารถตรวจดูข้อมูลบนระบบคอมพิวเตอร์สำรองเพื่อตรวจจับผู้ไม่มีสิทธิ์และแก้ไขให้ถูกต้องอยู่ตลอดเวลา

18.11 ให้สิทธิ์การทำทดสอบความพร้อมของ HA/DR โดยไม่กระทบต่อเครื่องคอมพิวเตอร์แม่ข่ายหลักหรือการดำเนินการทางธุรกิจ

18.12 สามารถทำการติดตั้ง ใช้งาน และตรวจสอบดูแล software ได้โดยสามารถใช้งานได้ทั้งหน้าจอ 5250 และแบบกราฟฟิกซ์ (GUI)

18.13 สามารถแสดงผลของสถานะการทำงานของ software ผ่านทางหน้าจอและมีสีต่างๆที่แสดงความหมาย ทำให้เข้าใจง่าย

18.14 มีเครื่องมือ (Tools) เพื่ออำนวยความสะดวกในการจัดการการส่งผ่านข้อมูลไปยังเครื่องสำรอง

18.15 สามารถตรวจสอบและแจ้งเตือนผ่านทางอีเมล หรือ การทำงานผ่านทางหน้าจอคอนโซล

18.16 ให้สิทธิ์การตรวจดูและควบคุมการทำงานของ software ที่อยู่ในหลายๆแห่ง รวบรวมไว้ในหน้าจอเดียวกัน

18.17 สามารถตั้งคำสั่งอัตโนมัติ, และสามารถแก้ไขเพิ่มเติมขั้นตอนให้เป็นไปตามความต้องการ

18.18 สามารถกำหนดสิทธิ์ในการเข้าถึงซอฟท์แวร์ได้หลายระดับ ตั้งแต่สิทธิ์สำหรับระดับปฏิบัติการถึงระดับการจัดการขั้นสูงขึ้น

18.19 สนับสนุนทั้งระบบความปลอดภัยของซอฟแวร์และควบคุมสิทธิ์ของ user

19. คุณลักษณะเฉพาะขั้นต่ำของ link สำหรับการ replicate ข้อมูลสำหรับระบบ AS/400 จำนวน 1 ชุด

19.1 กรณีมีการทดสอบหรือเมื่อเกิดเหตุฉุกเฉิน ต้องจัดให้มีระบบสื่อสารข้อมูลความเร็วสูง ที่เชื่อมต่อระหว่างศูนย์ข้อมูลหลักของธนาคาร (Data Center) และศูนย์สำรองข้อมูล (DRC) โดยมี Bandwidth ขนาดไม่น้อยกว่า 50 Mbps แบบ Full Duplex เพื่อ Replicate ข้อมูล ทั้งนี้ ในกรณีเหตุการณ์ปกติ ต้องให้มีระบบสื่อสารข้อมูล โดยมี Bandwidth ความเร็วไม่น้อยกว่า 20 Mbps

19.2 ต้องสามารถเชื่อมต่อกับผู้ให้บริการอินเทอร์เน็ตในประเทศไทย และเชื่อมต่อกับระบบเครือข่ายได้ทุกประเภทไม่ว่าจะเป็น Leased Line หรือ MPLS

20. คุณสมบัติของสถานที่ศูนย์สำรองข้อมูล (DR site)

20.1 ผู้ยื่นข้อเสนอต้องไม่เช่าช่วงจากผู้ให้บริการดาต้าเซ็นเตอร์รายอื่น

20.2 ผู้ยื่นข้อเสนอต้องให้บริการด้าน DR มาไม่น้อยกว่า 10 ปี

20.3 ทำเลที่ตั้งอาคารของศูนย์สำรองคอมพิวเตอร์ ต้องอยู่ห่างจากธนาคาร EXIM Bank สำนักงานใหญ่ ไม่น้อยกว่า 12 ก.ม. และสามารถเดินทางไปถึงได้โดยสะดวก

20.4 ทำเลที่ต้องของศูนย์สำรองคอมพิวเตอร์ ต้องอยู่ในพื้นที่ซึ่งสามารถรองรับการบริการระบบสื่อสารข้อมูลจากผู้รับจ้างอื่น ได้อย่างน้อย 4 ราย ประกอบไปด้วย TRUE, UIH, SYMPHONY, NT เป็นต้น

20.5 ภายในศูนย์คอมพิวเตอร์ต้องมีการติดตั้งอุปกรณ์เพื่ออำนวยความสะดวกสำหรับระบบสายสัญญาณ (Cabling system)

20.6 ภายในศูนย์คอมพิวเตอร์ต้องมีการติดตั้งระบบพื้นยกระดับ (Raised Floor System) ที่มีระดับความสูงหรือมีพื้นที่เพียงพอต่อการระบายอากาศให้อุปกรณ์คอมพิวเตอร์ต่างๆ

20.7 ระบบไฟฟ้าต้องสามารถจ่ายกระแสไฟฟ้าเข้าตู้อุปกรณ์คอมพิวเตอร์ โดยต้องมีการออกแบบให้สามารถจ่ายไฟเข้าตู้ได้ 2 เส้นทาง จาก UPS ข้างละไม่ต่ำกว่า 16 amp ระบบไฟฟ้าต้องมีการติดตั้งวงจรสำหรับป้องกันไฟกระชาก (Surge Protection)

20.8 ระบบสำรองไฟฟ้าฉุกเฉินอัตโนมัติ (UPS) ต้องมีการออกแบบให้ทำงานในลักษณะอย่างน้อย 2N เพื่อให้ระบบคอมพิวเตอร์และเครือข่ายภายในศูนย์คอมพิวเตอร์ได้รับไฟฟ้าที่มีการควบคุมและการสำรองไฟฟ้าโดยอัตโนมัติปลอดภัยจากสภาวะไฟฟ้าผิดปกติในทุกรูปแบบ และเพื่อให้แน่ใจว่าระบบสามารถทำงานได้อย่างต่อเนื่องในกรณีระบบสำรองไฟฟ้าตัวใดตัวหนึ่งเสียหายหรือหยุดทำงาน (มีระบบตรวจสอบการทำงานของ UPS และแบตเตอรี่)

20.9 กรณีแหล่งจ่ายไฟฟ้าหลัก จากการไฟฟ้าขัดข้อง ต้องมีระบบเครื่องกำเนิดไฟฟ้าสำรองที่สามารถทำงานโดยอัตโนมัติ และต้องสามารถจ่ายไฟฟ้าสำรองได้ไม่น้อยกว่า 8 ชั่วโมง

20.10 มีระบบควบคุมอุณหภูมิและความชื้น สำหรับอุปกรณ์คอมพิวเตอร์ โดยระบบปรับอากาศ ภายในพื้นที่ศูนย์คอมพิวเตอร์ต้องควบคุมโดยระบบ Precision air conditioning และมีการติดตั้งระบบควบคุมสำรอง เพื่อควบคุมอุณหภูมิให้เป็นไปอย่างมีประสิทธิภาพ สามารถทำความเย็น ลดความชื้น เพิ่มความชื้น และกรองฝุ่นละออง เพื่อให้สภาวะอุณหภูมิภายในศูนย์คอมพิวเตอร์อยู่ในระดับที่คงที่ตลอดเวลา พร้อมระบบปรับอากาศเป็นแบบ N+1

20.11 มีระบบดับเพลิงอัตโนมัติ (Fire Suppression System) ภายในพื้นที่ศูนย์สำรองคอมพิวเตอร์ต้องได้รับการออกแบบให้สามารถป้องกันอัคคีภัยด้วยระบบสารพิเศษในการดับเพลิงที่ต้องไม่เกิดปัญหากับอุปกรณ์อิเล็กทรอนิกส์ มีการวางระบบหัวฉีดทั่วพื้นที่ ซึ่งสามารถตั้งค่าการดับเพลิงในแบบอัตโนมัติ (Auto) และแบบปกติด้วยมือได้ (Manual)

20.12 มีระบบตรวจจับควันด้วยเครื่องตรวจจับควันด้วยเครื่องจับความไวสูงภายในพื้นที่ศูนย์สำรองคอมพิวเตอร์ โดยต้องสามารถตรวจจับเหตุเพลิงไหม้ได้ตั้งแต่สถานะก่อนเกิดควัน และส่งสัญญาณเตือนล่วงหน้า (Pre-alert) เพื่อให้เจ้าหน้าที่ดำเนินการใดๆ ก่อนที่จะเกิดการลุกลามขึ้น อุปกรณ์ตรวจจับควันจะต้องสามารถเริ่มต้นนับเวลาเพื่อทำการปล่อยสารพิเศษในการดับเพลิงทันทีที่เกินกว่าระดับที่กำหนด

20.13 การแบ่งโซนป้องกันไฟ (Separate Fire Zones) ภายในพื้นที่ศูนย์คอมพิวเตอร์ต้องติดตั้งผนังทนไฟเพื่อชะลอและป้องกันเพลิงจากภายนอกพื้นที่ได้ อย่างน้อย 2 ชั่วโมง

20.14 ระบบตรวจจับน้ำรั่วซึม (Water leak detection system) ภายในพื้นที่ศูนย์สำรองคอมพิวเตอร์ ควรมีการออกแบบและติดตั้งระบบตรวจจับน้ำรั่วซึม เพื่อให้สามารถตรวจจับและแจ้งเตือนให้ทราบถึงปัญหารั่วซึมของน้ำเข้ามายังภายศูนย์คอมพิวเตอร์ได้อย่างรวดเร็ว

20.15 มีระบบควบคุมการเข้า-ออก ประตูอัตโนมัติ (Access Control) เช่น ระบบสแกนนิ้วมือหรือระบบสแกนขนาดรูปร่างของฝ่ามือ หรือระบบตรวจสอบอื่นๆที่ได้มาตรฐาน (Three factor authentication)

20.16 มีระบบรักษาความปลอดภัยด้วยเจ้าหน้าที่ Security guards เพื่อควบคุมการเข้า-ออก ของบุคคลภายนอกที่ได้รับการอนุญาตให้เข้าพื้นที่เท่านั้น

20.17 มีระบบบันทึกภาพกล้องวงจรปิด (CCTV) ซึ่งทำการบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่มีความเคลื่อนไหวตามจุดที่ติดตั้งอุปกรณ์ที่ธนาคาร
ใช้เช่า โดยสามารถบันทึกภาพในที่มืด จัดเก็บข้อมูล และตรวจดูความเคลื่อนไหวย้อนหลังได้อย่างน้อย 30 วัน

20.18 มีเจ้าหน้าที่ Network Operation Center (NOC) คอยเฝ้าระวังอยู่ตลอด 24 ชั่วโมง ตลอดปี (24 x7) มีด้านหน้าของศูนย์คอมพิวเตอร์ เพื่อให้บริการลูกค้า เช่น การ Reboot เซิร์ฟเวอร์ การเปลี่ยนใส่เทป หรือแผ่นซีดี เพื่อการสำรองข้อมูลประจำวัน การปิด/เปิดอุปกรณ์ต่างๆ หรือช่วยตรวจดูไฟสถานะต่างๆของอุปกรณ์ภายในตู้อุปกรณ์ และสามารถติดต่อประสานงานได้โดยสะดวก หากอุปกรณ์ที่ศูนย์สำรองเกิดเหตุขัดข้อง หรือชำรุดบกพร่องจนไม่สามารถใช้งานได้เป็นปกติ บริษัทฯ ต้องรีบแจ้งธนาคารให้ทราบโดยทันที

21. การให้บริการ DR

มีเจ้าหน้าที่คอย Monitoring ระบบงาน AS/400 และซอฟต์แวร์ในการส่งข้อมูล ตลอด 24 ชั่วโมง ณ ศูนย์สำรอง พร้อมทั้งตรวจสอบระบบ Network ที่เชื่อมต่อระหว่างศูนย์คอมพิวเตอร์หลัก มาที่ศูนย์คอมพิเตอร์สำรอง

21.1 มีเจ้าหน้าที่สำหรับลงข้อมูลจากเทป (restore data) สำหรับระบบงานอื่นๆ ทุกเดือน ณ ศูนย์สำรอง

21.2 ผู้ยื่นข้อเสนอต้องจัดทำรายงานรายเดือนเกี่ยวกับผลการ Monitoring ระบบงาน AS/400 และผลการลงข้อมูลจากเทป (restore data) สำหรับระบบงานอื่นๆ และจัดทำรายงานความผิดปกติที่เกิดขึ้นรายเดือน (กรณีเกิดเหตุผิดปกติ)

22. การให้การสนับสนุน

22.1 ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องจัดให้มีเจ้าหน้าที่ประสานงานที่มีความรู้ความชำนาญเกี่ยวกับระบบ AS/400 server, VMware, NetBackup, Software replicate data ที่ให้บริการพร้อมหมายเลขโทรศัพท์ที่สามารถติดต่อได้สะดวกเพื่อรับแจ้งเหตุขัดข้อง ให้คำปรึกษา ตอบข้อซักถาม ให้ความช่วยเหลือหรือแก้ไขปัญหาเบื้องต้น (on Phone Support) รวมถึงช่องทางอื่นได้ทุกวันตลอด 24 ชั่วโมง

22.2 ให้คำปรึกษาด้านการออกแบบ การใช้งาน และกำหนดค่าพารามิเตอร์ของอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายสำหรับ DR solution

22.3 ในกรณีที่อุปกรณ์ที่ศูนย์สำรองเกิดเหตุขัดข้อง หรือชำรุดบกพร่องจนไม่สามารถใช้งานได้เป็นปกติ ในระหว่างธนาคารใช้งาน และทางธนาคารได้แจ้งให้บริษัทฯ ทราบถึงเหตุขัดข้องดังกล่าวแล้ว โดยหากไม่สามารถแก้ไขปัญหา หรือให้ความช่วยเหลือในการแก้ไขปัญหาผ่านทางโทรศัพท์ได้ทันที บริษัทฯ ตกลงติดต่อกลับธนาคารภายใน 30 นาที นับจากที่ได้รับแจ้งจากธนาคาร และดำเนินการแก้ไขเหตุขัดข้อง หรือชำรุดบกพร่องให้เสร็จสิ้นจนอุปกรณ์ที่ศูนย์สำรองสามารถใช้งานได้ตามปกติภายใน 4 ชั่วโมง นับจากที่ได้รับแจ้งจากธนาคาร

22.4 ผู้รับจ้างจะต้องนำส่งรายละเอียดและขั้นตอนการเข้ามาดำเนินการแก้ไขปัญหาหรือเหตุขัดข้องหรือความชำรุดบกพร่อง ให้กับธนาคารในทันทีที่สามารถดำเนินการได้

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ การจ้างผู้ให้บริการบำรุงรักษา WAF and Network Traffic Management

2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ

3. วงเงินงบประมาณที่ได้รับจัดสรร 2,600,000.00 บาท (สองล้านหกแสนบาทถ้วน)

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 08 ก.ค. 2567

เป็นเงิน 1,471,250.00 บาท (หนึ่งล้านสี่แสนเจ็ดหมื่นหนึ่งพันสองร้อยห้าสิบบาทถ้วน)

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

บริษัท ตาต้าโปร คอมพิวเตอร์ ซิสเต็มส์ จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายฉัตรชัย	อาศรมเงิน	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่ายปส.
6.2 นายจรัส	ขวัญพิเชษฐ์สกุล	ผู้บริหารส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ / ฝ่ายปส.
6.3 นายกิตติ์ธเนศ	วงศ์ประสิทธิ์	ผู้ช่วยผู้บริหารส่วนบริการและปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่ายปส.

ผนวก 1

คุณลักษณะขั้นต่ำด้านเทคนิค/ขอบเขตของงานบริการ

การจ้างผู้ให้บริการบำรุงรักษา WAF and Network Traffic Management

---

1. รายการอุปกรณ์ระบบ WAF and Network Traffic Management สำหรับการบำรุงรักษา (Preventive Maintenance) มีดังนี้

   1.1 อุปกรณ์ที่ต่ออายุรับประกัน

   1.1.1 HPE Proliant DL380 Gen10 Server for Imperva (Serial no. SGH014X705)

   1.1.2 HPE Proliant DL380 Gen10 Server for Imperva (Serial no. SGH014X706)

   ระยะเวลาตั้งแต่วันที่ 29 สิงหาคม 2567 ถึง 28 สิงหาคม 2568

   1.2 ลิขสิทธิ์ซอฟแวร์ 1 ปี (License)

   1.2.1 FlexProtect Plus for Application Security, 20 Mbps Base Plan, Annual Enhanced Subscription x1 Unit

   1.2.2 Add Applications to FlexProtect Plus for Application Security, Annual Enhanced Subscription x10 Units

   ระยะเวลาตั้งแต่วันที่ 29 สิงหาคม 2567 ถึง 28 สิงหาคม 2568

2. ขอบเขตการดำเนินงาน

   ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก ต้องให้การสนับสนุนธนาคารตลอดระยะเวลา 1 ปี นับถัดจากวันรับมอบงาน ดังนี้

   2.1 จัดให้มีเจ้าหน้าที่ประสานงานที่มีความรู้ความชำนาญเกี่ยวกับระบบ WAF and Network Traffic Management พร้อมหมายเลขโทรศัพท์ที่สามารถติดต่อได้สะดวกเพื่อรับแจ้งเหตุขัดข้อง ให้คำปรึกษา ตอบข้อซักถาม ให้ความช่วยเหลือหรือแก้ไขปัญหาเบื้องต้น (On Phone Support) รวมถึงช่องทางอื่นได้ทุกวันตลอด 24 ชั่วโมง

   2.2 ในกรณีที่ระบบ WAF and Network Traffic Management เกิดเหตุขัดข้องหรือความชำรุดบกพร่อง และธนาคารเห็นว่าการให้ความช่วยเหลือ ตามข้อ 2.1 ไม่อาจแก้ปัญหาได้ต้องจัดส่งพนักงานเข้ามายังสถานที่ติดตั้งเพื่อดำเนินการแก้ไขเหตุขัดข้องหรือความชำรุดบกพร่องแบบ Onsite Service รวมทั้งหากต้องมีการเปลี่ยนอุปกรณ์ของระบบ WAF and Network Traffic Management ต้องจัดอุปกรณ์ฯ ที่มีคุณลักษณะเทียบเท่า หรือดีกว่าให้ธนาคาร ให้แล้วเสร็จและสามารถใช้งานได้เป็นปกติภายในระยะเวลา 4 ชั่วโมงนับจากได้รับแจ้งเหตุขัดข้องจากธนาคาร

   2.3 จัดทำรายละเอียดและขั้นตอนการเข้ามาดำเนินการแก้ไขปัญหาหรือเหตุขัดข้องหรือความชำรุดบกพร่องของระบบ WAF and Network Traffic Management ในทันทีที่สามารถดำเนินการได้

2.4 ต้องจัดให้มีเจ้าหน้าที่ตรวจสอบ และบำรุงรักษาระบบ WAF and Network Traffic Management ไม่น้อยกว่า 4 ครั้ง/ปี พร้อมทั้งจัดทำรายละเอียด และขั้นตอนการตรวจสอบ รวมทั้งข้อเสนอแนะที่เป็นประโยชน์ต่อธนาคารเป็นลายลักษณ์อักษรทุกครั้งที่ให้บริการ โดย ผู้ให้บริการจะต้องแจ้งกำหนดวันเวลาแน่นอน ก่อนการเข้ามาบริการล่วงหน้าไม่น้อยกว่า 1 วันและธนาคารเห็นชอบ ดังนี้

ครั้งที่ 1 ภายในเดือนพฤศจิกายน 2567
ครั้งที่ 2 ภายในเดือนกุมภาพันธ์ 2568
ครั้งที่ 3 ภายในเดือนพฤษภาคม 2568
ครั้งที่ 4 ภายในเดือนสิงหาคม 2568

2.5 ในกรณีที่ธนาคารมีความต้องการเปลี่ยนแปลง ปรับปรุงแก้ไขระบบ WAF and Network Traffic Management ต้องจัดให้มีเจ้าหน้าที่ที่มีความรู้ความชำนาญเกี่ยวกับระบบ WAF and Network Traffic Management เข้ามาสนับสนุนช่วยเหลือ และเข้าถึงเครือข่ายตามความยินยอมของธนาคารตลอดระยะเวลาการรับประกัน 1 ปี โดยธนาคารจะแจ้งให้ทราบล่วงหน้าอย่างน้อย 1 วัน ก่อนให้เข้ามาดำเนินการ และต้องได้รับความเห็นชอบจากธนาคารก่อนดำเนินการ พร้อมทั้งต้องดำเนินการให้แล้วเสร็จภายใน 1 วัน นับจากได้รับแจ้งจากธนาคาร

2.6 ต้องดำเนินการ Update Software / firmware และสิทธิการใช้งานระบบ WAF and Network Traffic Management ตลอดระยะเวลาให้บริการ

2.7 ในกรณีระบบ WAF and Network Traffic Management เกิดเหตุขัดข้องชำรุด หรือมีข้อบกพร่องที่ไม่สามารถใช้งานได้ ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกจะต้องจัดส่งเจ้าหน้าที่เข้ามาให้บริการตรวจสอบ และแก้ไขปัญหาให้กับทางธนาคาร ณ สถานที่ตั้ง รวมทั้งต้องดำเนินการตรวจสอบแก้ไขหรือปรับปรุงให้แล้วเสร็จภายในกำหนดระยะเวลานับถัดจากที่ได้รับแจ้งเหตุขัดข้องหรือความชำรุดบกพร่องจากธนาคาร ตามระดับผลกระทบที่มีต่อธุรกิจ หรือการทำงาน (Severity) ดังนี้

ระดับผลกระทบ (Severity)	ระยะเวลาคิดต่อกลับ	ระยะเวลาการแก้ไขปัญหาเสร็จสิ้นนับจากที่ได้รับแจ้ง
Urgent ระบบ WAF and Network Traffic Management ไม่สามารถใช้งานได้	30 นาที	4 (สี่) ชั่วโมง
High ระบบ WAF and Network Traffic Management ทำงานผิดพลาดซึ่งเป็นส่วนสำคัญที่ส่งผลกระทบต่อการดำเนินงานของธนาคาร	1 ชั่วโมง	8 (แปด) ชั่วโมง
Medium ระบบ WAF and Network Traffic Management ทำงานผิดพลาดซึ่งไม่เป็นส่วนสำคัญที่กระทบต่อการดำเนินงานของธนาคาร	2 ชั่วโมง	48 (สี่สิบแปด) ชั่วโมง
Low ระบบ WAF and Network Traffic Management ทำงานผิดพลาด ซึ่งไม่เป็นส่วนสำคัญที่ไม่กระทบต่อการดำเนินงานของธนาคาร	4 ชั่วโมง	96 (เก้าสิบหก) ชั่วโมง

2.8 ดำเนินการ Review Policy (WAF) ตาม Best Practice เพื่อปรับปรุงระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ตามที่ธนาคารได้มีการร้องขอ โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

2.9 ดำเนินการ Configure ระบบ WAF and Network Traffic Management ตามที่ธนาคารได้มีการร้องขอ

2.10 การ Upgrade Program / Firmware ในระหว่างระยะเวลารับประกัน หาก Application Software หรือ Firmware หรือ Patch หรือระบบ WAF and Network Traffic Management มีการออก Version ใหม่ หรือพัฒนาปรับปรุง (Upgrade) ผู้ยื่นข้อเสนอที่ได้รับเลือกจะต้องแจ้งรายละเอียดการเปลี่ยนแปลงและผลกระทบที่เกิดขึ้นจากการเปลี่ยนแปลงดังกล่าวให้ธนาคารทราบ เพื่อใช้เป็นข้อมูลประกอบการตัดสินใจของธนาคาร และหากธนาคารประสงค์จะดำเนินการพัฒนาปรับปรุง (Upgrade) ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการพัฒนาปรับปรุง (Upgrade) ให้กับธนาคารโดยไม่คิดค่าใช้จ่ายเพิ่มเติม และดำเนินการให้แล้วเสร็จภายใน 7 วันนับจากได้รับแจ้งจากธนาคาร

2.11 ดำเนินการจัดทำ System Architecture โดยระบุรายละเอียดของอุปกรณ์ ตลอดจนรูปแบบและวิธีการเชื่อมต่อทั้งหมด

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างผู้ให้บริการเช่าใช้บริการ Security Operation Center (SOC)**
2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
3. วงเงินงบประมาณที่ได้รับจัดสรร **5,000,000.00 บาท (ห้าล้านบาทถ้วน)**
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 08 ก.ค. 2567

   เป็นเงิน 3,265,661.40 บาท (สามล้านสองแสนหกหมื่นห้าพันหกร้อยหกสิบเอ็ดบาทสี่สิบสตางค์)
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด
6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายฉัตรชัย	อาศรมเงิน	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.2 นายจรัส	ขวัญพิเชษฐ์สกุล	ผู้บริหารส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.3 นายจเร	บุญกร	ผู้ช่วยผู้บริหารส่วนบริหารจัดการโครงสร้างพื้นฐานและระบบเครือข่าย /ฝ่าย ปส.

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการเช่าใช้บริการ Security Operation Center (SOC)

ผู้ยื่นข้อเสนอต้องเสนอบริการ โดยมีขอบเขตการดำเนินงานดังนี้

1. **ข้อกำหนดความต้องการทั่วไป**

   1.1 ผู้ยื่นข้อเสนอต้องเป็นผู้ให้บริการการบริหารจัดการระบบความปลอดภัยสารสนเทศ (Managed Security Service Provider: MSSP) หรือ ประกอบกิจการศูนย์เฝ้าระวังด้านความปลอดภัยสารสนเทศ หรือความปลอดภัยไซเบอร์แบบครบวงจร ที่มีศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Security Operations Center: SOC) ตั้งอยู่ในประเทศไทย

   1.2 ศูนย์ปฏิบัติการ Security Operations Center (SOC) ของผู้ยื่นข้อเสนอ ต้องได้รับมาตรฐานสากล ISO/ICE 27001 และมีความพร้อมในการให้บริการเฝ้าระวังและแจ้งเตือนเหตุการณ์ภัยคุกคามให้แก่ธนาคารตลอด 7 วัน 24 ชั่วโมง (7 x 24)

   1.3 ผลิตภัณฑ์ที่ให้บริการทั้งหมด ผู้ยื่นข้อเสนอต้องมีสิทธิความเป็นเจ้าของหรือสิทธิการใช้งานอย่างถูกต้อง เพื่อให้บริการกับธนาคาร

   1.4 ต้องเสนออุปกรณ์, โปรแกรมต่างๆ, บริการ, การดำเนินการส่ง log จากอุปกรณ์หรือระบบงานของทางธนาคารไปประมวลผลที่ศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ และส่วนประกอบเพิ่มเติมที่จำเป็นต่อการให้บริการให้ครบถ้วน หากบริการใดที่ธนาคารไม่ได้กำหนดและมีความจำเป็นต้องนำมาใช้งานร่วมกันเพื่อให้สามารถใช้บริการได้อย่างมีประสิทธิภาพ ผู้ยื่นข้อเสนอจะต้องจัดหาและส่งมอบให้กับธนาคารได้อย่างครบถ้วน

<u>ส่วนที่ 1 การเตรียมระบบ</u>

2. **ความต้องการด้านเทคนิค**

   2.1 ต้องจัดเตรียมระบบเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ ซึ่งสามารถจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร ระบบจะต้องประกอบด้วยการทำงานดังต่อไปนี้

   - สามารถวิเคราะห์และหาความสัมพันธ์ของข้อมูล เพื่อหาเหตุการณ์ผิดปกติได้
   - สามารถปรับแต่งรูปแบบความสัมพันธ์หรือเงื่อนไข (Custom Rule) ได้
   - สามารถแจ้งเตือนให้ผู้ดูแลระบบทราบ เมื่อตรวจพบข้อมูลที่สอดคล้องกับเงื่อนไขที่ได้ตั้งไว้
   - สามารถจัดทำรายงาน หรือสรุปรายงานประจำเดือนได้
   - สามารถบริการจัดการผ่าน Web Interface หรือ GUI ได้เป็นอย่างน้อย
   - สามารถกำหนดสิทธิ์การเข้าถึงระบบ ตามระดับสิทธิ์การเข้าถึงได้ (Role Base Access Control)

2.2 ระบบเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ จะต้องสามารถรองรับข้อมูลจราจรทางคอมพิวเตอร์ได้ 100 GB/Day และจะต้องรองรับการทำงานหรือการเฝ้าระวัง ตามอุปกรณ์ดังต่อไปนี้ เป็นอย่างน้อย

- Firewall : Checkpoint, Paloalto, Juniper, Fortinet, Cisco
- OS : Windows Server, RedHat, AS400
- Database : Oracle, Microsoft Sql, My Sql
- Network : Cisco, F5 SSL VPN, F5-Load Balance, Radware, Huawei, Forescout
- IPS : Tippingpoint
- WAF : Imperva, Cloudflare
- Antivirus : Trendmicro
- Secure Internet Gateway : Zscaler
- Cloud : INET, MS-Azure, AWS or Etc.

2.3 ต้องมี Disaster Recovery Site (DR Site) ที่ทำหน้าที่เป็นศูนย์ปฏิบัติการสำรอง ในกรณีที่ศูนย์ปฏิบัติการหลักของผู้ยื่นข้อเสนอไม่สามารถให้บริการได้ หรือ ระบบการเฝ้าระวังของผู้ยื่นข้อเสนอไม่สามารถให้บริการได้

2.4 ต้องจัดหาระบบเครือข่ายเชื่อมโยงศูนย์เทคโนโลยีสารสนเทศของธนาคาร และศูนย์ปฏิบัติหลักและศูนย์ปฏิบัติการสำรองของผู้ยื่นข้อเสนอ จำนวนอย่างน้อย 2 วงจร เพื่อใช้เป็นช่องทางหลัก 1 ช่องทาง และช่องทางสำรอง 1 ช่องทาง ในการส่งข้อมูลจราจรทางคอมพิวเตอร์โดยเฉพาะ ซึ่งต้องมีความเร็วของการส่งข้อมูลเพียงพอกับปริมาณข้อมูลจราจรทางคอมพิวเตอร์ที่ธนาคารจะส่งไปยังศูนย์ปฏิบัติการของผู้ยื่นข้อเสนอ และต้องเข้ารหัสข้อมูลจราจรทางคอมพิวเตอร์ก่อนที่จะส่งไปยังศูนย์ปฏิบัติการ

2.5 ต้องดำเนินการดูแลรักษาซอฟต์แวร์ (Log Collector) ที่ได้ติดตั้งไว้ที่ธนาคารซึ่งซอฟต์แวร์ดังกล่าวจะต้องมีคุณสมบัติดังต่อไปนี้

- สามารถทำหน้าที่ รับข้อมูลจราจรจากเครื่องต้นทาง มายังอุปกรณ์ดังกล่าวได้
- สามารถทำหน้าที่ ในการคัดกรอง Log ก่อนทำการส่งให้ระบบด้านความมั่นคงปลอดภัยเพื่อวิเคราะห์ต่อได้ เช่น SIEM เป็นต้น
- สามารถทำหน้าที่ ในการเก็บข้อมูลจราจรคอมพิวเตอร์ ได้ที่บนอุปกรณ์ ในกรณีที่ เครือข่ายเชื่อมโยง ไม่สามารถใช้งานได้ หรือ ข้อมูลจราจรไม่สามารถส่งไปที่ศูนย์ปฏิบัติการของผู้ยื่นข้อเสนอได้ เป็นเวลาอย่างน้อย 1 วัน นับจากเวลาที่ไม่สามารถส่งข้อมูลไปที่ศูนย์ปฏิบัติการของผู้ยื่นข้อเสนอได้
- สามารถทำหน้าที่ ในการแจ้งเตือนในกรณีที่ ข้อมูลจราจร ไม่ส่งมายังตัวอุปกรณ์ได้
- สามารถรองรับปริมาณข้อมูลจราจรทางคอมพิวเตอร์ได้อย่างน้อย 150 GB/Day
- สามารถติดตั้งบนระบบ Virtual Machine (VMware) ได้

2.6 ต้องดำเนินการดูแลรักษาซอฟต์แวร์ Syslog Server ที่ได้ติดตั้งไว้ที่ธนาคารซึ่งซอฟต์แวร์ ดังกล่าวจะต้องมีคุณสมบัติดังต่อไปนี้

- สามารถจัดเก็บ Log File ในรูปแบบของ Syslog หรือ SNMP หรือ sFlow หรือ NetFlow หรือ OPSEC ได้เป็นอย่างน้อย
- สามารถจัดเก็บ Log File ได้อย่างน้อย 100 GB/Day เป็นเวลาอย่างน้อย 120 วัน
- สามารถค้นหาข้อมูลได้ โดยสามารถค้นหาข้อมูลได้ดังต่อไปนี้ เช่น Syslog, SNMP traps หรือ Windows event logs เป็นต้น
- สามารถสร้างรายงาน และจัดส่งผ่านช่องทางอีเมลโดยอัตโนมัติและสามารถออกรายงานในรูปแบบ PDF หรือ CSV หรือ HTML
- สามารถตั้งระยะเวลาในการเก็บข้อมูลหรือ สั่งลบข้อมูลได้
- สามารถทำหน้าที่ ในการทำ Hashing เพื่อตรวจสอบความถูกต้องของ Logs หากถูกแก้ไขเปลี่ยนแปลงได้ ตามมาตรฐาน MD5 หรือ SHA1 หรือ SHA-256
- สามารถทำหน้าที่ในการบีบอัดข้อมูลของ Log ได้
- สามารถติดตั้งบนระบบ Virtual Machine (VMware) ได้

2.7 จัดให้มีผู้เชี่ยวชาญเข้าทำกระบวนการเตรียมพร้อมและส่งผ่านข้อมูลจราจรทางคอมพิวเตอร์ เพื่อใช้ในการเฝ้าระวังฯ (On-boarding process) ดังนี้

2.7.1 ตรวจสอบความพร้อมใช้ของระบบและอุปกรณ์ต้นกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ที่จะใช้ในการ เฝ้าระวังร่วมกับเจ้าหน้าที่ของธนาคาร และให้คำแนะนำในการตั้งค่าอุปกรณ์เพื่อให้สามารถส่งข้อมูลจราจรทางคอมพิวเตอร์ได้

2.7.2 ระบุแหล่งที่มาของข้อมูลจราจรทางคอมพิวเตอร์และจัดหมวดหมู่ของอุปกรณ์ต้นกำเนิด

2.7.3 ระบุและวิเคราะห์ความเสี่ยงรูปแบบการโจมตี และจัดระดับของผลกระทบต่อระบบของทางธนาคารรวมทั้งกำหนดประเภทข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่ต้องใช้ในการวิเคราะห์ร่วมกับธนาคาร

2.7.4 วิเคราะห์และสร้างแบบจำลองของภัยคุกคาม เพื่อหาวิธีและเครื่องมือในการเฝ้าระวังที่เหมาะสม (Threat Model)

2.7.5 จัดทำ Monitoring Use case ให้สอดคล้องกับ Threat Model และตั้งค่าระบบที่ใช้เฝ้าระวังฯ (SIEM) ตามที่กำหนดไว้ใน Monitoring Use case

2.7.6 จัดทำ Dashboard และ Alert ให้สอดคล้องกับ Monitoring Use case เพื่อใช้ในการแจ้งเตือนและรายงานต่างๆ

2.7.7 จัดทำแผนการทำงานร่วมกันในกระบวนการ Incident Management รวมถึงแผนการดำเนินการตอบโต้ภัยคุกคามร่วมกันกับทางธนาคาร

2.8 ให้คำแนะนำและประเมินกระบวนการตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response) ในปัจจุบันของธนาคาร เพื่อปรับปรุงกระบวนการตอบสนองต่อเหตุการณ์ผิดปกติให้มีประสิทธิภาพดีขึ้น

2.9 ให้คำแนะนำและประเมินกระบวนจำแนกชั้นข้อมูลและการป้องกันข้อมูลรั่วไหล

2.10 ดำเนินการ Upgrade new firmware / Patch / IOS อุปกรณ์ที่ทางผู้ให้บริการนำมาวางที่ธนาคาร สำหรับโครงการ SOC เช่น Firewall หรือ อุปกรณ์อื่นๆ

2.11 ให้คำแนะนำในการออกแบบระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) เพื่อจัดเก็บข้อมูล ณ ศูนย์เทคโนโลยีของธนาคาร ให้สอดคล้องตามนโยบายหรือข้อบังคับที่ทางธนาคารต้องปฏิบัติตาม

<u>ส่วนที่ 2 การให้บริการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ ระยะเวลาให้บริการ 12 เดือน</u>

2.12 ให้บริการ Security Awareness โดยการจัดทำ Phishing Simulation อย่างน้อย 2 ครั้งต่อปี

2.13 บริการจัดเก็บและสืบค้นข้อมูลจราจรคอมพิวเตอร์ (Log Management)

2.13.1 จัดเก็บข้อมูลจราจรคอมพิวเตอร์ เป็นระยะเวลา 120 วัน ณ. ศูนย์เฝ้าระวังฯของผู้ให้บริการ และทำการสืบค้นข้อมูลจราจรคอมพิวเตอร์ ตามที่ธนาคารร้องขอ โดยมี SLA ดังนี้

Log ที่ร้องขอ	การสืบค้นข้อมูล
น้อยกว่า 30 วัน	ภายใน 24 ชั่วโมง
30 - 120 วัน	ภายใน 7 วันทำการ

2.13.2 ดำเนินการแยกประเภทข้อมูลจราจรทางคอมพิวเตอร์ ในกรณีที่จำเป็นต้องส่งข้อมูลจราจรทางคอมพิวเตอร์บางส่วนไปยังศูนย์ปฏิบัติการของผู้ยื่นข้อเสนอ และบางส่วนที่ต้องเก็บไว้ที่ศูนย์เทคโนโลยีของธนาคาร

2.13.3 บริการตรวจสอบสถานะการส่งจราจรทางคอมพิวเตอร์ พร้อมแจ้งเตือนไปยังเจ้าหน้าที่ที่เกี่ยวข้องของผู้ใช้บริการผ่านทางระบบอีเมล์ หรือช่องทางตามที่ตกลงกัน ในกรณีที่ตรวจพบว่าอุปกรณ์ทั้งหมดของธนาคารไม่สามารถส่งข้อมูลมายังศูนย์ปฏิบัติการของผู้ยื่นข้อเสนอ ผู้ยื่นข้อเสนอจะต้องแก้ไขให้สามารถส่งข้อมูลจราจรทางคอมพิวเตอร์ได้ภายในระยะเวลา 1.5 ชั่วโมง (90 นาที) เริ่มนับจากเวลาที่อุปกรณ์ของ ธสน. สำหรับใช้ในการส่งข้อมูลจราจรทางคอมพิวเตอร์ (log) ตามที่ได้ตกลงกับผู้เสนอราคาฯ ไม่สามารถดำเนินการได้

2.14 ดำเนินการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์เหตุการณ์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ ให้แก่ธนาคาร ณ ศูนย์ปฏิบัติการของผู้รับจ้าง โดยให้บริการแบบตลอดเวลา 24 ชั่วโมงของทุกวัน ไม่มีวันหยุด (7 x 24) ตลอดระยะเวลาของสัญญา หากบริการการเฝ้าระวังความมั่นคงปลอดภัยของผู้ยื่นข้อเสนอไม่สามารถทำงานได้ ผู้ยื่นข้อเสนอจะต้องแก้ไขให้บริการเฝ้าระวังความความมั่นคงปลอดภัยสามารถใช้บริการได้ภายในระยะเวลา 1.5 ชั่วโมง (90 นาที) เริ่มนับจากเวลาที่บริการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์วิเคราะห์เหตุการณ์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ของผู้เสนอราคาฯ ไม่สามารถดำเนินการได้

2.15 แจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยจะต้องแจ้งเตือนผ่านทาง Email หรือทางโทรศัพท์ หรือช่องทางอื่นใด ตามที่จะตกลงร่วมกันกับธนาคาร ตาม Severity Level Agreement (SLA) อย่างน้อย เริ่มนับจากเวลาที่ผู้เสนอราคาฯ ตรวจพบภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

ระดับความรุนแรง	แจ้งเตือนผู้รับบริการ	ให้คำแนะนำในการแก้ไข
วิกฤติ	ภายใน 0.5 ชั่วโมง (30 นาที)	ภายใน 1 ชั่วโมง (60 นาที)
สูง	ภายใน 1 ชั่วโมง (60 นาที)	ภายใน 2 ชั่วโมง (120 นาที)
กลาง	ภายใน 1.5 ชั่วโมง (90 นาที)	ภายใน 3 ชั่วโมง (180 นาที)
ต่ำ	ภายใน 2 ชั่วโมง (120 นาที)	ภายใน 4 ชั่วโมง (240 นาที)

2.16 การแจ้งเตือนจะต้องมีรายละเอียด อย่างน้อยดังนี้

- ระบุประเภทของภัยคุกคาม
- วัน-เวลา เริ่มต้นของภัยคุกคาม
- ระบุต้นทาง (Attacker) และปลายทาง (Target)
- ระบุระดับความรุนแรง (Severity)
- รายละเอียดเหตุการณ์และพฤติกรรมทั้งหมด
- ภาพการเชื่อมโยงเหตุการณ์ภัยคุกคามที่เกิดขึ้น
- คำแนะนำและขั้นตอนการดำเนินการแก้ไขด้านเทคนิค Action & Recommendation

2.17 ให้คำปรึกษาเกี่ยวกับบริการวิเคราะห์เฝ้าระวังภัยคุกคามต่างๆ ที่เกิดขึ้น และสนับสนุนการทำงานเกี่ยวกับการแก้ไข ป้องกันและรับมือกับภัยคุกคามได้ตลอด 24 ชั่วโมง

2.18 ดำเนินการวิเคราะห์แบบรวมศูนย์และจัดทำเงื่อนไขการโจมตี (Use case Management) เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคามด้วยรูปแบบและมาตรฐานของผู้รับจ้าง (Standard Use case) รวมทั้งปรับปรุงและจัดทำการแจ้งเตือนภัยคุกคามด้วยรูปแบบเงื่อนไขเฉพาะ หรือเงื่อนไขอื่นๆ เพิ่มเติม (Custom Usecase) ให้เหมาะสมกับ ธนาคารฯ

2.19 สามารถตรวจจับเหตุการณ์การคุกคามครอบคลุมในเรื่องดังนี้ เป็นอย่างน้อย

2.19.1 Unauthorized Access

2.19.2 Malicious code

2.19.3 Inappropriate usage

2.19.4 Multiple component

2.19.5 Denial of service

2.19.6 Information Gathering

2.19.7 Malware

2.19.8 Suspicious Traffic

2.19.9 Vulnerability Scan

2.19.10 Lateral movement

2.20 ให้บริการทีมงานสำหรับการรวบรวมข้อมูลภัยคุกคามทางไซเบอร์ที่มีการปรับปรุงให้ทันสมัยอยู่เสมอจากแหล่งต่างๆ จากทั่วทุกมุมโลก (Threat Intelligence) เพื่อการวิเคราะห์ข้อมูลภัยคุกคามร่วมกับระบบ SIEM หรือ SOC Technology เพิ่มเติม เพื่อทำให้ ธนาคารฯ สามารถรับมือกับภัยคุกคามไซเบอร์ได้ อย่างมีประสิทธิภาพมากยิ่งขึ้น

2.21 จัดให้มีบริการแจ้งข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความมั่นคงปลอดภัย ระบบคอมพิวเตอร์และระบบเครือข่ายที่เกิดขึ้น ผ่านทางอีเมล์ เช่น

- รายชื่อ และคุณลักษณะของมัลแวร์ (Malware)
- ช่องโหว่ใหม่ (Vulnerability) ของอุปกรณ์ในระบบเครือข่าย (Network Equipment)
- ช่องโหว่ใหม่ (Vulnerability) ของระบบปฏิบัติการ (Operating System)
- ช่องโหว่ใหม่ (Vulnerability) ของระบบฐานข้อมูลหลัก (Database)
- ช่องโหว่ใหม่ (Vulnerability) ของโปรแกรมต่างๆ ที่ผู้รับจ้างเห็นว่าจะก่อให้เกิดผล เสียหายต่อการดำเนินงานของ ธนาคารฯ

โดยข่าวสารดังกล่าวประกอบด้วยเนื้อหาที่สำคัญ เช่น คำอธิบายอย่างคร่าวๆ (Overview), คำอธิบายอย่างละเอียด (Description), ผลกระทบ (Impact), ระบบที่ได้รับผลกระทบ (System Affected), ทางแก้ไข (Solution) (ถ้ามี), อ้างอิง (Reference) เป็นต้น

2.22 จัดเตรียมหน่วยปฏิบัติการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ (CSIRT) พร้อมที่จะปฏิบัติหน้าที่ในการตอบสนองต่อภัยคุกคามหรือการบุกรุกระบบอย่างทันท่วงที หรือเข้าดำเนินการสืบสวนและวิเคราะห์หาสาเหตุของปัญหา ภัยคุกคามที่เกิดขึ้น รวมถึงการตรวจพิสูจน์พยานหลักฐานทาง Digital เมื่อมีการร้องขอบริการจากทางธนาคารภายในระยะเวลา 4 ชั่วโมง นับตั้งแต่ที่ธนาคารร้องขอ ไม่เกินกว่า 15 เหตุการณ์ พร้อมจัดทำรายงานผลการดำเนินงานสรุปข้อมูลหลักฐานต่างๆ ที่ได้จากการตอบสนองต่อเหตุการณ์ภัยคุกคาม รวมถึงแนวทางในการป้องกันการเกิดซ้ำในอนาคต (Incident Response and Recommendations Report) ทันทีที่สามารถดำเนินการได้

2.23 จัดทำรายงานสรุปสถิติภัยคุกคามประจำเดือน (Monthly Report) ภายในรูปแบบที่ธนาคารเห็นชอบ และ มีหัวข้อของรายงาน อย่างน้อยดังนี้

- สรุปเหตุการณ์ตามประเภทและระดับความรุนแรง (Incident Report)
- สรุป 10 อันดับสูงสุดของการโจมตี
- สรุป 10 อันดับสูงสุดของเป้าหมายที่โดยโจมตี

- สรุป 10 อันดับสูงสุดของผู้เข้ามาโจมตี
- สรุป 10 อันดับสูงสุดของช่องทางที่ถูกใช้โจมตี
- สรุปปริมาณและสถานะการใช้งานข้อมูลจราจรทางคอมพิวเตอร์ประจำเดือนแยกตามอุปกรณ์
- บทวิเคราะห์แนวโน้มของภัยคุกคามต่างๆ ที่เกิดขึ้นในเดือนที่ผ่านมา
- บทวิเคราะห์ประเมินความเสี่ยงในเดือนที่ผ่านมา เพื่อพัฒนาแนวทางการเฝ้าระวังให้ครอบคลุมกับภัยคุกคามใหม่ (Use Cases Development)
- สรุปคำแนะนำ

2.24 บริการเข้าร่วมประชุมประจำเดือน ทั้งแบบประชุมทางไกล (Video Conference Monthly Meeting) หรือเข้าประชุม ณ. ที่ทำการธนาคารฯ สำนักงานใหญ่ (On-Site Monthly Meeting) โดยผู้ยื่นข้อเสนอจะต้องเข้าร่วมประชุมเพื่อสรุปให้คำแนะนำและประเมินกระบวนจำแนกชั้นข้อมูลและการป้องกันข้อมูลรั่วไหลและเฝ้าระวังภัยคุกคามต่างๆ ที่เกิดขึ้นกับธนาคาร ทุกๆ เดือน ตลอดสัญญาของการให้บริการ

2.25 ผู้ยื่นข้อเสนอต้องดำเนินการจัดการซ้อมแผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ในรูปแบบการฝึกซ้อมแผนบนโต๊ะ (Tabletop Exercise) จำนวนอย่างน้อย 2 แผน ต่อปี โดยมีเจ้าหน้าที่ที่เกี่ยวข้องของธนาคาร เข้าร่วมการฝึกซ้อมด้วย

3. บุคลากรในการดำเนินโครงการ

ผู้ยื่นข้อเสนอจะต้องมีผู้เชี่ยวชาญและเจ้าหน้าที่ที่ปฏิบัติงานในศูนย์เฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ พนักงานประจำที่มีประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ที่ได้รับการรับรองความรู้ความสามารถ และมีประกาศนียบัตรรับรอง (Certificate) ที่ยังไม่หมดอายุ จนถึงวันที่ยื่นข้อเสนอดังต่อไปนี้

3.1 CISSP (Certified Information System Security Professional) หรือ GIAC GCFA (GIAC Certified Forensic Analyst) หรือ GIAC GCIH (GIAC Certified Incident Handler) หรือ CISM (Certified Information Security Manager) หรือ CISA (Certified Information System Auditor) อย่างน้อย 1 คน

3.2 OSCP (Offensive Security Certified Professional) หรือ CEH (Certified Ethical Hacker) หรือ CHFI (Computer Hacking Forenic Investigator) อย่างน้อย 1 คน

3.3 CompTIA CySA+ หรือ CompTIA Security+ อย่างน้อย 4 คน

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจัดซื้อแบตเตอรี่เครื่องสำรองไฟฟ้า (UPS)**

2. หน่วยงานเจ้าของโครงการ **ฝ่ายธุรการ**

3. วงเงินงบประมาณที่ได้รับจัดสรร 1,500,000.- **บาท (หนึ่งล้านห้าแสนบาทถ้วน)**

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 23 ก.ค. 2567

เป็นเงิน 1,498,856.- **บาท (หนึ่งล้านสี่แสนเก้าหมื่นแปดพันแปดร้อยห้าสิบหกบาทถ้วน)**

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

สืบราคาจาก บริษัท ซินเนอร์ไจซ์ เอ็นจิเนียริ่ง จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง)

1. นายฉัตรชัย อาศรมเงิน	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
2. นายพุทธิพงษ์ สุกิตติวงศ์	ผู้ช่วยผู้บริหารส่วนอาคาร ฝ่ายธุรการ
3. นายชัยพร รัตนา	เจ้าหน้าที่ธุรการ ส่วนอาคาร ฝ่ายธุรการ

ผนวก 1

ข้อกำหนดและขอบเขตการดำเนินงาน

การจัดซื้อแบตเตอรี่เครื่องสำรองไฟฟ้า (UPS)

ผู้เสนอราคาต้องเสนอแบตเตอรี่เครื่องสำรองไฟฟ้าที่มีคุณลักษณะตามรายละเอียดที่ธนาคารกำหนดให้ธนาคารพิจารณา ดังต่อไปนี้

1. **รายละเอียดคุณลักษณะทั่วไป**
   - 1.1 ดำเนินการรื้อถอนแบตเตอรี่ของเดิม และติดตั้งของใหม่
   - 1.2 แบตเตอรี่ได้รับมาตรฐาน ISO 9001 และ ISO 14001 เป็นอย่างน้อย โดยต้องมีเอกสารยืนยัน
   - 1.3 แบตเตอรี่ต้องได้รับมาตรฐาน IEC60896-21 & 22 เป็นอย่างน้อย โดยต้องมีเอกสารยืนยัน
   - 1.4 ต้องเป็นของใหม่ที่มีคุณภาพดีและไม่เคยผ่านการใช้งานมาก่อน และจะต้องไม่มีการดัดแปลงแก้ไขใดๆ ทั้งสิ้น
   - 1.5 ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการติดตั้ง หรือความเสียหายใดที่เกิดขึ้นอันเนื่องมาจากการปฏิบัติงาน และต้องซ่อมแซมแก้ไขให้สามารถใช้งานได้โดยเร็ว
2. **รายละเอียดคุณลักษณะด้านเทคนิค**
   - 2.1 แบตเตอรี่ขนาด 12V/84Ah จำนวน 68 ลูก โดยมีจำนวน 6 เซลล์ต่อลูก
   - 2.2 ต้องสำรองกระแสไฟฟ้าได้ไม่น้อยกว่า 15 นาที ที่ Full Load, Power Factor 0.9 (ในการคำนวณเลือกแบตเตอรี่ ให้ใช้ค่า End of discharge voltage ของแบตเตอรี่เท่ากับ 1.75V/Cell ที่อุณหภูมิ 25 องศาเซลเซียส) โดยต้องแสดงเอกสารการคำนวณประกอบ
   - 2.3 แบตเตอรี่ชนิดตะกั่วกรด ควบคุมแรงดันด้วยวาล์ว (Valve Regulated lead-acid, VRLA) และเป็นแบบ Maintenance free ที่ถูกออกแบบมาให้ใช้กับเครื่องสำรองกระแสไฟฟ้า (UPS) มีความสามารถในการคายประจุสูง
   - 2.4 อายุในการออกแบบ (Design life) ไม่น้อยกว่า 10 ปี ที่อุณหภูมิ 25 องศาเซลเซียส
   - 2.5 ตัวถังและฝาปิดต้องทำจากวัสดุ Durable Polypropylene เพื่อป้องกันอันตรายจากการระเบิด และต้องไม่เป็นเชื้อเพลิง หรือเรียกว่า Flame Retardant ที่เป็นตามมาตรฐาน UL94-V0
   - 2.6 ขั้วต่อ (Terminal) เป็นชนิดขั้วฝัง (Insert Terminal) และสามารถรองรับอัตราการคายประจุสูงได้เป็นอย่างดี
   - 2.7 แผ่นกั้นระหว่างแผ่นธาตุ (Separator) ต้องเป็นชนิดใยแก้ว Absorbent Glass Mat (AGM) technology
   - 2.8 แผ่นธาตุ (Plate Grid Alloy) เป็นประเภท Radius Grid ผลิตจากโลหะผสม Lead, low calcium alloy grid เพื่อลดอัตราการเกิดก๊าซ (Reduce Gassing) และช่วยยืดอายุของแบตเตอรี่ โดยแผ่นธาตุทุกแผ่นต้องสามารถจ่ายกระแสไฟฟ้าได้สูงและสม่ำเสมอตลอดทั้งแผ่น และต้องมีเอกสารยืนยันจากผู้ผลิต

2.9 งานติดตั้งทางไฟฟ้าทั้งหมดต้องเป็นไปตามมาตรฐานการติดตั้งทางไฟฟ้าอย่างเคร่งครัด หากตรวจพบข้อผิดพลาดอันเนื่องมาจากการติดตั้งที่ผิดไปจากมาตรฐานด้านความปลอดภัยของผู้ผลิต ผู้เสนอราคาต้องดำเนินการแก้ไขให้ถูกต้องโดยเร็ว และไม่มีสิทธิ์เรียกร้องค่าใช้จ่ายใดๆ เพิ่มเติมจากธนาคาร

2.10 ผู้เสนอราคาต้องตรวจสอบค่าทางไฟฟ้าของแบตเตอรี่ทุกลูกให้ถูกต้องตามมาตรฐานของผู้ผลิตให้ธนาคารพิจารณาก่อนดำเนินการติดตั้ง โดยต้องจัดทำรายงานผล Initial Charge แบตเตอรี่ ซึ่งแสดงค่าแรงดันแบตเตอรี่ และค่าความนำหรือค่าความต้านทานภายในของแบตเตอรี่ทุกลูก หากลูกใดมีปัญหาต้องนำแบตเตอรี่ใหม่มาเปลี่ยนทดแทน

3. **การรับประกัน**

ผู้เสนอราคาที่ได้รับการคัดเลือกต้องรับประกันสินค้าเป็นระยะเวลาไม่น้อยกว่า 2 ปี นับจากวันที่คณะกรรมการได้ตรวจรับงานเป็นที่เรียบร้อยแล้ว โดยต้องมีเอกสารที่แสดงถึงการรับประกันมาตรฐานจากโรงงานผู้ผลิตโดยตรง

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การเช่ารถยนต์ประจำตำแหน่งสำหรับผู้บริหารฝ่าย จำนวน 4 คัน ระยะเวลา 5 ปี**

2. /หน่วยงานเจ้าของโครงการ **ฝ่ายธุรการ**

3. วงเงินงบประมาณที่ได้รับจัดสรร **6,600,000.- บาท (หกล้านหกแสนบาทถ้วน)**

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 24 ต.ค. 2567

   กำหนดราคากลาง **เป็นจำนวนเงินทั้งสิ้น 6,480,000.- บาท (หกล้านสี่แสนแปดหมื่นบาทถ้วน)**

   ยี่ห้อ HONDA รุ่น Accord e:HEV E จำนวน 4 คัน อัตราค่าเช่า/คัน ไม่เกิน 27,000.- บาท/เดือน

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง) จำนวน 6 ราย

   5.1 บจก.อาคเนย์ แคปปิตอล

   5.2 บจก.ทรู ลีสซิ่ง

   5.3 บมจ.กรุงไทยคาร์เร้นท์ แอนด์ ลีส

   5.4 บจก.เค คาร์เรนทอล

   5.5 บจก.เวิลด์คลาส เรนท์ อะ คาร์

   5.6 บจก.มาสเตอร์ ไดรฟเวอร์ แอนด์ เซอร์วิสเซส (ประเทศไทย)

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายเดชา	ปริญญาสุข	ผู้ช่วยผู้บริหารฝ่ายธุรการ
6.2 นายชวัลณัฐ	มาตุเรศ	ผู้บริหารส่วนพนักงานสัมพันธ์/ ฝ่ายทรัพยากรบุคคล
6.3 นายพุทธิพงษ์	สุกิตติวงศ์	ผู้ช่วยผู้บริหารส่วนอาคาร/ฝ่ายธุรการ

ผนวก 1
ขอบเขตการดำเนินงาน
การเช่ารถยนต์ประจำตำแหน่งสำหรับผู้บริหารฝ่าย

ผู้เสนอราคาต้องเสนอการเช่ารถยนต์ประจำตำแหน่งตามขอบเขตงานที่ธนาคารกำหนด ดังนี้

1. **รายการและจำนวนของรถยนต์ที่จะเช่า**
   รถยนต์ประจำตำแหน่งผู้บริหารฝ่าย ยี่ห้อ HONDA รุ่น Accord e:HEV E จำนวน 4 คัน

2. **คุณลักษณะและเงื่อนไข**
   - 2.1 คุณลักษณะทั่วไป
     - 2.1.1 รถยนต์ที่เสนอให้เช่าต้องมีคุณสมบัติ รายละเอียดและอุปกรณ์เป็นไปตามแคตตาล็อกและเอกสารหรือโฆษณาส่งเสริมการขายของบริษัทผู้ผลิตรถยนต์ โดยห้ามลดอุปกรณ์คุณภาพหรือประสิทธิภาพในส่วนใด ๆ ของรถยนต์
     - 2.1.2 รถยนต์ที่เสนอให้เช่าต้องเป็นรถยนต์ใหม่ที่ไม่เคยผ่านการใช้งานมาก่อนและเป็นรถยนต์โฉมใหม่ล่าสุดที่มีจำหน่ายในขณะที่ยื่นเสนอราคา
     - 2.1.3 สีตัวถังรถยนต์เป็นไปตามที่ธนาคารกำหนด
   - 2.2 อุปกรณ์เพิ่มเติม/คันอย่างน้อยมีดังต่อไปนี้
     - 2.2.1 ติดฟิล์มกรองแสงเซรามิค ยี่ห้อ V - KOOL หรือ LAMINA หรือ 3M กระจกบานหน้าเต็มบานและกระจกรอบคัน พร้อมใบรับประกันคุณภาพ ไม่น้อยกว่า 5 ปี โดยความเข้มของฟิล์มกรองแสงเป็นไปตามที่ธนาคารกำหนดในภายหลัง
     - 2.2.2 แผ่นปูพื้นแบบเก็บฝุ่นที่มีคุณภาพดีตามมาตรฐานของผู้ผลิตรถยนต์หรือเทียบเท่า จำนวน 1 ชุด (ต้องเสนอให้ธนาคารเห็นชอบก่อนส่งมอบ)
     - 2.2.3 แผ่นพรมปูพื้นที่มีคุณภาพดีตามมาตรฐานของผู้ผลิตรถยนต์หรือเทียบเท่า จำนวน 1 ชุด
     - 2.2.4 ถาดวางของท้ายรถตามมาตรฐานของผู้ผลิตรถยนต์หรือเทียบเท่า
     - 2.2.5 กรอบใส่ป้ายทะเบียนจำนวน 1 คู่
     - 2.2.6 กล้องบันทึกภาพและวีดีโอด้านหน้า-หลัง ความละเอียดไม่น้อยกว่า Full HD (1,080 Pixel) พร้อมหน่วยบันทึกความจำ (SD Card) ขนาดความจุไม่น้อยกว่า 64 GB
     - 2.2.7 ชุดอุปกรณ์ฉุกเฉิน (สายพ่วงแบตเตอรี่/สายลากจูง/ไฟฉาย/ป้ายสะท้อนแสงสามเหลี่ยม ฯลฯ) จำนวน 1 ชุด
     - 2.2.8 เครื่องดับเพลิงสำหรับใช้กับรถยนต์บรรจุสารดับเพลิง DRY CHEMICAL POWDER จำนวน 1 ถัง
     - 2.2.9 เซนเซอร์ช่วยเตือนในการนำรถเข้าจอด (ด้านหลัง) อย่างน้อย 4 จุด จำนวน 1 ชุด
   - 2.3 อื่น ๆ
     - 2.3.1 เครื่องมือมาตรฐานประจำรถยนต์
     - 2.3.2 สมุดคู่มือการใช้รถ
   - 2.4 รถยนต์ประจำตำแหน่งที่เสนอให้เช่าในครั้งนี้ต้องเป็นพัสดุที่ผลิตในประเทศไทย โดยมีเอกสารรับรองจากบริษัทผู้ผลิต หรือตัวแทนจำหน่ายรถยนต์ที่เสนอให้เช่า หรือเอกสารรับรองสินค้า (Made in Thailand) จากสภาอุตสาหกรรมแห่งประเทศไทย

3. เงื่อนไขการส่งมอบและตรวจรับพัสดุ

ก่อนนำรถยนต์มาส่งมอบให้ธนาคาร ผู้เสนอราคาที่ได้รับการคัดเลือก (ผู้ให้เช่า) ต้องจัดทำเป็นหนังสือแจ้งรายละเอียด และกำหนดวันส่งมอบให้ชัดเจนนำส่งถึงประธานคณะกรรมการตรวจรับ โดยมีรายละเอียดการส่งมอบ ดังนี้

3.1 ต้องส่งมอบรถยนต์ที่มีรายละเอียดคุณสมบัติ และจำนวนที่ครบถ้วนถูกต้องตามที่กำหนดในสัญญา ณ ที่ทำการธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย สำนักงานใหญ่ หรือสถานที่ที่ธนาคารกำหนด โดยมีรายละเอียดการส่งมอบ ดังนี้

3.1.1 ส่งมอบรถยนต์ จำนวน 2 คัน ภายในระยะเวลา 60 วัน นับถัดจากวันที่ลงนามในสัญญา

3.1.2 ส่งมอบรถยนต์ จำนวน 2 คัน ภายในระยะเวลา 60 วัน นับถัดจากวันที่ธนาคารมีหนังสือแจ้งความต้องการใช้งานรถยนต์แต่ละคัน

ทั้งนี้ ในการเช่ารถยนต์ตามข้อ 3.1.2 ธนาคารขอสงวนสิทธิ์ในการเช่าเพียงบางส่วน หรือเช่าทั้งหมด หรือยกเลิกการเช่าทั้งหมด โดยธนาคารจะแจ้งความต้องการเช่ารถยนต์ดังกล่าวให้ผู้ให้เช่าทราบ ภายในระยะเวลา 6 เดือน นับถัดจากวันที่ลงนามในสัญญา ซึ่งหากพ้นระยะเวลาดังกล่าว ธนาคารจะยกเลิกการเช่ารถยนต์ในส่วนที่มิได้มีหนังสือแจ้งความต้องการในการเช่าดังกล่าวทั้งหมด

3.2 รถยนต์ที่ส่งมอบทุกคันต้องดำเนินการจดทะเบียน (เป็นรถยนต์นั่งส่วนบุคคล) กับกรมการขนส่งทางบก หรือหน่วยงานที่เกี่ยวข้องให้เป็นที่เรียบร้อยสามารถใช้งานได้อย่างถูกต้องตามกฎหมาย ทั้งนี้ หากธนาคารมีความประสงค์จะใช้รถยนต์ในระหว่างรอการจดทะเบียน ผู้ให้เช่าจะต้องจัดให้มีป้ายแดงพร้อมเอกสารเพื่อให้สามารถใช้งานได้อย่างถูกต้องตามกฎหมายหรือระเบียบของทางราชการ

3.3 รถยนต์ที่ส่งมอบทุกคันต้องจัดทำประกันภัยรถยนต์ตาม พ.ร.บ. คุ้มครองผู้ประสบภัยจากรถ และประกันภัยประเภท 1 (ซ่อมศูนย์) แบบไม่ระบุผู้ขับขี่ และมีเงื่อนไขการชดใช้ความเสียหายแบบไม่จำกัดจำนวนครั้ง โดยผู้ขับขี่ไม่ต้องรับผิดค่าเสียหายส่วนแรกและระบุการใช้รถยนต์เพื่อการพาณิชย์ไม่ใช่รับจ้างสาธารณะ รวมทั้งต้องระบุการคุ้มครองอย่างน้อย ดังต่อไปนี้

3.3.1 ความเสียหายต่อบุคคลภายนอก

3.3.1.1 ความเสียหายต่อชีวิต ความบาดเจ็บ สูงสุดตาม พ.ร.บ. 1,000,000 บาท/คน และไม่เกิน 10,000,000 บาท/ครั้ง

3.3.1.2 ความเสียหายต่อทรัพย์สิน 5,000,000 บาท/ครั้ง (ไม่จำกัดจำนวนครั้ง)

3.3.2 ความคุ้มครองตามเอกสารแนบท้ายกรมธรรม์ (ในรถยนต์ที่เอาประกันภัย)

3.3.2.1 กรณีเสียชีวิต สูญเสียอวัยวะ หรือทุพพลภาพถาวร		
- ผู้ขับขี่	200,000	บาท
- ผู้โดยสารภายในรถ	200,000	บาท/คน
3.3.2.2 ค่ารักษาพยาบาล	200,000	บาท/คน (ไม่จำกัดจำนวนครั้ง)
3.3.2.3 การประกันตัวผู้ขับขี่	200,000	บาท/ครั้ง

3.4 เอกสารที่ต้องส่งมอบ

3.4.1 สำเนาสมุดคู่มือจดทะเบียนรถยนต์ พร้อมป้ายทะเบียน (ป้ายดำ) และป้ายแสดงการชำระภาษีประจำปี หรือสมุดคู่มือประจำรถใช้กับเครื่องหมายพิเศษ พร้อมป้ายทะเบียน (ป้ายแดง) ที่ถูกต้องตามกฎหมาย

3.4.2 สำเนากรมธรรม์ประกันภัยคุ้มครองผู้ประสบภัยจากรถ (พ.ร.บ.)

3.4.3 สำเนากรมธรรม์ประกันภัยรถยนต์ประเภท 1 (ซ่อมศูนย์)

3.5 รถยนต์ที่ส่งมอบทุกคันต้องเติมน้ำมันเชื้อเพลิงเต็มถัง ณ วันที่ส่งมอบ

4. เงื่อนไขการใช้รถยนต์ที่เช่า

4.1 ธนาคารมีสิทธิ์ใช้รถยนต์โดยไม่จำกัดระยะทางวิ่ง

4.2 ธนาคารมีสิทธิ์ใช้รถยนต์โดยผู้ขับขี่เป็นไปตามที่ธนาคารมอบหมาย

4.3 ผู้ให้เช่าต้องเป็นผู้รับผิดชอบในค่าใช้จ่ายต่างๆ ยกเว้นค่าน้ำมันเชื้อเพลิงที่เกิดจากการใช้งานตามปกติของธนาคาร และพนักงานขับรถ ธนาคารจะเป็นผู้รับผิดชอบ (เว้นแต่การนำรถยนต์ที่เช่าไปตรวจสภาพ ซ่อมแซม หรือบำรุงรักษา ผู้ให้เช่ามีหน้าที่ต้องตรวจสอบน้ำมันเชื้อเพลิงในถังว่ามีระดับเท่าใด เมื่อส่งมอบรถยนต์กลับมาให้ธนาคาร น้ำมันเชื้อเพลิงในถังจะต้องอยู่ในระดับเดิม ถ้าต่ำกว่าเดิมผู้ให้เช่าจะต้องเติมให้อยู่ในระดับเดิม)

4.4 ผู้ให้เช่าต้องส่งหลักฐานแสดงรายการชำระภาษีในปีแรกให้กับธนาคาร ณ วันที่ส่งมอบรถยนต์ และจัดส่งหลักฐานแสดงรายการชำระภาษีในปีต่อๆ ไป ให้กับธนาคารล่วงหน้าก่อนวันครบกำหนดการชำระภาษีไม่น้อยกว่า 30 วัน

4.5 ผู้ให้เช่าต้องส่งสำเนากรมธรรม์ประกันภัยในปีแรกให้ธนาคาร ณ วันที่ลงนามสัญญา และจัดส่งสำเนากรมธรรม์ประกันภัยดังกล่าวในปีต่อๆไป ให้กับธนาคารล่วงหน้าก่อนกรมธรรม์เดิมจะสิ้นสุดระยะเวลาความคุ้มครองไม่น้อยกว่า 30 วัน

4.6 ผู้ให้เช่าต้องดำเนินการซ่อมแซม เปลี่ยนอะไหล่ และบำรุงรักษารถยนต์ที่เช่าตามระยะทางหรือระยะเวลาที่กำหนดในคู่มือมาตรฐานของบริษัทผู้ผลิตรถยนต์ รวมทั้งต้องซ่อมบำรุงเปลี่ยนอะไหล่ที่ชำรุดเสียหายจากการใช้งานตามปกติหรือเมื่อรถยนต์เกิดเหตุบกพร่องทั้งเครื่องยนต์และส่วนประกอบของรถยนต์ โดยในกรณีจำเป็นหรือเร่งด่วน ธนาคารมีสิทธิ์นำรถยนต์เข้ารับบริการที่ศูนย์บริการรถยนต์ยี่ห้อนั้นๆ ได้ทั่วประเทศ โดยธนาคารจะแจ้งผู้ให้เช่าทราบล่วงหน้าก่อนเข้ารับบริการและผู้ให้เช่าต้องรับผิดชอบในบรรดาค่าใช้จ่ายต่างๆ ทั้งหมดที่เกิดจากการซ่อมแซม เปลี่ยนอะไหล่ หรือบำรุงรักษา

4.7 ผู้ให้เช่าต้องเปลี่ยนยางใหม่ (4 เส้น) เมื่อครบระยะทางทุกๆ 40,000 กิโลเมตร หรือระยะเวลา 2 ปี แล้วแต่กำหนดใดจะถึงก่อน หรือเมื่อสภาพดอกยางมีความลึกน้อยกว่า 3 มิลลิเมตร หรือด้วยเหตุอื่นใดซึ่งโดยสภาพที่เห็นได้ว่าจะไม่ปลอดภัยหากจะใช้ยางเส้นนั้นต่อไป กรณีมีความจำเป็นเร่งด่วน ธนาคารมีสิทธิ์นำรถยนต์เข้ารับบริการเปลี่ยนยางที่ศูนย์บริการของรถยนต์ยี่ห้อนั้นๆ หรือศูนย์บริการรถยนต์ทั่วไป หรือผู้ให้บริการยางรถยนต์ได้ทั่วประเทศ โดยธนาคารจะแจ้งผู้ให้เช่าทราบล่วงหน้าก่อนเข้ารับบริการและผู้ให้เช่าต้องรับผิดชอบในบรรดาค่าใช้จ่ายต่างๆ ทั้งหมดที่เกิดจากการเปลี่ยนยางนั้น

4.8 ผู้ให้เช่าต้องรับผิดชอบบรรดาค่าใช้จ่ายต่างๆ ทั้งปวง กรณีรถยนต์ที่เช่าเกิดอุบัติเหตุ เสียหาย หรือจำเป็นต้องซ่อมแซมในระหว่างเดินทางเพื่อให้สามารถใช้งานรถยนต์ได้ตามปกติ ซึ่งรวมถึงค่าลากจูงค่ายกรถยนต์จากจุดเกิดเหตุถึงศูนย์บริการรถยนต์ยี่ห้อนั้นๆ หรือถึงธนาคาร หรือถึงบริษัทผู้รับประกันภัย หรือตัวแทน หรือถึงอู่ซ่อมรถของบริษัทผู้รับประกันภัย โดยธนาคารมีสิทธิ์ทำการซ่อมแซมให้รถยนต์เช่าสามารถใช้งานได้ตามปกติภายในวงเงิน ไม่เกิน 10,000 บาท (หนึ่งหมื่นบาทถ้วน) ต่อครั้ง โดยธนาคารจะแจ้งผู้ให้เช่าทราบก่อนซ่อมแซม

4.9 ผู้ให้เช่าต้องรับผิดชอบต่อการสูญหายของรถยนต์เช่าทุกกรณี

4.10 การชดใช้ค่าเสียหายจากการเรียกร้องสิทธิหรือการรบกวนขัดสิทธิ

ในกรณีที่มีบุคคลภายนอกมากล่าวอ้าง และใช้สิทธิเรียกร้องใดๆ ว่าการครอบครองการใช้สอยรถยนต์ที่เช่าของธนาคารเป็นการละเมิด หรือมีบุคคลภายนอกมาก่อการรบกวนขัดสิทธิเกี่ยวกับรถยนต์ที่เช่า ผู้ให้เช่าต้องดำเนินการทั้งปวงเพื่อให้การเรียกร้อง หรือการรบกวนขัดสิทธิดังกล่าวทั้งหมดสิ้นไปโดยเร็ว หากมิอาจดำเนินการดังกล่าวให้ได้และหากการเรียกร้องหรือการรบกวนขัดสิทธิ เป็นเหตุให้ธนาคารเสียค่าใช้จ่ายหรือต้องชดใช้ค่าเสียหายต่อบุคคลภายนอก หรือได้รับความเสียหายจากการถูกรบกวนขัดสิทธิดังกล่าว ผู้ให้เช่าต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่าย รวมทั้งค่าฤชาธรรมเนียมและค่าทนายความแทนธนาคารหรือชดใช้ค่าเสียหายทั้งหมดให้แก่ธนาคารโดยสิ้นเชิง

4.11 การโอนกรรมสิทธิ์ให้บุคคลอื่น

กรณีผู้ให้เช่าจะโอนกรรมสิทธิ์การเช่ารถยนต์แก่บุคคลอื่นจะต้องได้รับความเห็นชอบจากธนาคารเป็นลายลักษณ์อักษรก่อน หากฝ่าฝืนผู้ให้เช่าต้องรับผิดชอบและชดใช้ค่าเสียหาย (ถ้ามี) ให้แก่ธนาคาร

4.12 ผู้ให้เช่าต้องจัดให้มีเจ้าหน้าที่ควบคุม ดูแล และประสานงานพร้อมเบอร์โทรศัพท์หรือช่องทางอื่นที่สามารถติดต่อสื่อสารได้อย่างสะดวก รวดเร็ว ทุกวันตลอด 24 ชั่วโมง เพื่อให้บริการกับธนาคาร อาทิ เช่น การรับแจ้งเมื่อรถยนต์ที่เช่าเกิดเหตุขัดข้อง ชำรุดเสียหาย สูญหาย การเคลมประกัน การจัดส่งรถยนต์เพื่อใช้งานทดแทน เป็นต้น

5. การจัดรถยนต์มาทดแทน

5.1 ในกรณีรถยนต์ที่เช่าเกิดอุบัติเหตุหรือเหตุขัดข้องหรือมีสภาพไม่ปลอดภัยต่อการใช้งาน หรือไม่สามารถใช้งานได้ตามปกติไม่ว่าจะเกิดจากเหตุใด ผู้ให้เช่าจะต้องนำรถยนต์คันใหม่ที่มีรายละเอียดและคุณลักษณะเช่นเดียวกับรถยนต์ที่เช่า หรือเทียบเท่าหรือดีกว่าทั้งในเรื่องความนิยมในยี่ห้อรถยนต์ (brand name) และราคาซื้อขายรถยนต์ (price list) ในท้องตลาดมาเปลี่ยนทดแทนชั่วคราวให้ธนาคาร ณ สถานที่เกิดเหตุหรือสถานที่ที่ธนาคารกำหนดทันทีที่ได้รับแจ้ง

ทั้งนี้ หากรายละเอียดและคุณลักษณะของรถยนต์ที่เช่าที่มาเปลี่ยนทดแทนชั่วคราว ตามข้อ 5.1 มีอายุการใช้งานไม่เกินกว่ารถยนต์ที่เช่าคันเดิม ธนาคารมีสิทธินำรถยนต์คันดังกล่าวมาใช้เป็นการทดแทนแบบถาวรก็ได้

5.2 ในกรณีรถยนต์ที่เช่าเสียหายจนไม่สามารถซ่อมแซมให้ใช้งานได้ดีดังเดิมไม่ว่าจะเกิดจากเหตุใด ผู้ให้เช่าต้องนำรถยนต์คันใหม่ที่มีรายละเอียดและคุณลักษณะเช่นเดียวกับข้อ 5.1 และมีอายุการใช้งานไม่เกินกว่ารถยนต์ที่เช่าคันเดิม รวมทั้งมีสภาพเหมาะสมที่จะใช้งานได้ดีเช่นเดียวกับรถยนต์คันเดิม มาให้ธนาคารใช้งานทดแทนเป็นการถาวร ณ สถานที่ที่ธนาคารกำหนด ภายใน 30 วัน นับจากวันที่ศูนย์บริการรถยนต์ยี่ห้อดังกล่าวหรือบริษัทประกันภัยยืนยันว่ารถยนต์ที่เช่าไม่สามารถซ่อมแซมให้ใช้งานได้ดีดังเดิมอีกต่อไป

5.3 ในกรณีที่รถยนต์ที่เช่าสูญหาย ผู้ให้เช่าจะต้องนำรถยนต์คันใหม่ที่มีรายละเอียดและคุณลักษณะเช่นเดียวกันกับข้อ 5.2 มาเปลี่ยนทดแทนเป็นการถาวรให้ธนาคาร ณ สถานที่เกิดเหตุหรือสถานที่ที่ธนาคารกำหนดทันทีที่ได้รับแจ้ง

กรณีธนาคารมีความจำเป็นเร่งด่วนที่ต้องใช้รถยนต์ทดแทนก่อนผู้ให้เช่านำรถยนต์มาเปลี่ยน หรือผู้ให้เช่าไม่สามารถนำรถยนต์มาเปลี่ยนทดแทนได้ หรือรถยนต์ที่นำมาเปลี่ยนทดแทนมีรายละเอียดและคุณลักษณะไม่เทียบเท่าหรือไม่ดีกว่า ธนาคารมีสิทธิ์เช่ารถยนต์มาใช้งานแทนได้จนกว่าผู้ให้เช่าจะจัดหารถยนต์มาเปลี่ยนทดแทนให้ได้ถูกต้องเป็นไปตามที่กำหนด โดยผู้ให้เช่าต้องรับภาระค่าเช่ารถยนต์ ค่าเดินทาง และค่าใช้จ่ายที่เกี่ยวข้องทั้งหมด โดยไม่จำกัดวงเงิน

กรณีรถยนต์ที่นำมาเปลี่ยนให้ใช้งานชั่วคราว ตามข้อ 5.1 หรือกรณีธนาคารต้องเช่ารถยนต์มาใช้งานทดแทนจะต้องมีระยะเวลาต่อเนื่องกันไม่เกิน 30 วัน นับจากวันที่นำรถยนต์มาเปลี่ยนให้ธนาคารใช้งานทดแทนหรือวันที่ธนาคารเช่ารถยนต์มาใช้งานทดแทน เว้นแต่กรณี ไม่สามารถซ่อมแซมให้ใช้งานได้ดีดังเดิม ตามข้อ 5.2 ซึ่งมีระยะเวลาเกินกว่า 30 วัน เนื่องจากผู้ให้เช่าต้องรอคำยืนยันจากศูนย์บริการรถยนต์ยี่ห้อดังกล่าวหรือบริษัทประกันภัย ผู้ให้เช่าต้องจัดทำเป็นหนังสือแจ้งให้ธนาคารทราบโดยเร็ว แต่อย่างไรก็ตามระยะเวลาดังกล่าวต้องไม่เกินกว่า 60 วัน นับจากวันที่นำรถยนต์มาเปลี่ยนทดแทนหากเกินระยะเวลาดังกล่าวธนาคารมีสิทธิที่จะบอกเลิกสัญญาทั้งหมดหรือแต่บางส่วนได้โดยทำเป็นหนังสือแจ้งไปยังผู้ให้เช่า

อนึ่ง การพิจารณาหรือวินิจฉัยใดๆ เกี่ยวกับการซ่อมแซม การบำรุงรักษา หรือการจัดรถยนต์มาใช้งานทดแทน ธนาคารมีสิทธิ์ที่จะพิจารณานอกเหนือหรือแตกต่างจากที่กำหนดได้ กรณีเป็นประเด็นที่แตกต่างเพียงเล็กน้อยหรือที่เห็นว่าเป็นประโยชน์กับธนาคาร

5.4 ในการจัดหารถยนต์ที่นำมาทดแทนดังกล่าวทุกกรณี ผู้ให้เช่าต้องจัดให้มีป้ายทะเบียน ป้ายแสดงการชำระภาษีประจำปี สำเนาสมุดคู่มือจดทะเบียนรถยนต์ และกรมธรรม์ ตามข้อ 3.4 ที่ยังไม่หมดอายุ รวมทั้งต้องดำเนินการให้ธนาคารใช้งานได้อย่างถูกต้องตามกฎหมาย

6. **ระยะเวลาการเช่า**

กำหนดระยะเวลาการเช่า 5 ปี นับตั้งแต่วันที่ผู้ให้เช่าส่งมอบรถยนต์ถูกต้อง ครบถ้วน ตามเงื่อนไขและระยะเวลาที่ธนาคารกำหนดในข้อ 3.1.1 หรือ 3.1.2 และผ่านการตรวจรับจากคณะกรรมการตรวจรับของธนาคารเรียบร้อย

7. **การชำระเงินค่าใช้จ่ายคืนธนาคาร**

กรณีที่ธนาคารได้ชำระค่าใช้จ่ายที่เกี่ยวกับการเช่ารถยนต์ไปก่อนทุกกรณี ผู้ให้เช่าต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งสิ้นและต้องชำระค่าใช้จ่ายดังกล่าวคืนให้แก่ธนาคารภายใน 7 วัน นับถัดจากวันที่ได้รับแจ้งเป็นลายลักษณ์อักษรจากธนาคาร ทั้งนี้ หากผู้ให้เช่าไม่ชำระค่าใช้จ่ายดังกล่าวคืนให้แก่ธนาคารภายในระยะเวลาที่กำหนด ธนาคารมีสิทธิ์หักค่าใช้จ่ายจากค่าเช่าที่ธนาคารต้องชำระให้แก่ผู้ให้เช่าเพื่อชดใช้ค่าใช้จ่ายดังกล่าว

8. **การใช้ประโยชน์จากรถยนต์**

ธนาคารมีสิทธิ์ติดป้ายโลหะ หรือพ่นตราประทับหรือทำเครื่องหมายอื่นใด หรือติดข้อความหรืออุปกรณ์อื่นใดเพื่อประโยชน์ในการใช้งานของธนาคารหรือดำเนินการใด ๆ บนรถยนต์ที่เช่า โดยไม่ต้องได้รับอนุญาตจากผู้ให้เช่าก่อน และเมื่อสิ้นสุดการเช่ารถยนต์ ผู้ให้เช่ามีหน้าที่ต้องลบข้อความหรือการรื้อถอนการติดตั้งป้าย เครื่องหมาย หรืออุปกรณ์ใด ๆ ตามที่ธนาคารแจ้งให้ดำเนินการด้วยค่าใช้จ่ายของผู้ให้เช่าเองทั้งสิ้น

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างผู้ให้บริการเช่าระบบสำรองข้อมูลBackup as a Service**
2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
3. วงเงินงบประมาณที่ได้รับจัดสรร **2,136,400 บาท (สองล้านหนึ่งแสนสามหมื่นหกพันสี่ร้อยบาทถ้วน)**
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) **24 ก.ค. 2567**

   เป็นเงิน 2,136,400.00 (สองล้านหนึ่งแสนสามหมื่นหกพันสี่ร้อยบาทถ้วน)
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   บริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน)
6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายฉัตรชัย	อาศรมเงิน	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.2 นางสาววิลาสินี	คำเพ็ง	ผู้ช่วยผู้บริหารส่วนบริหารจัดการโครงสร้างพื้นฐานและระบบเครือข่าย /ฝ่าย ปส.
6.3 นายชานนท์	แท่นทองจันทร์	ผู้ช่วยผู้บริหารส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ /ฝ่าย ปส.

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการเช่าระบบสำรองข้อมูล Backup as a Service

ผู้ยื่นข้อเสนอต้องเสนอบริการเช่าระบบสำรองข้อมูล Backup as a Service ตามขอบเขตงานที่ธนาคารกำหนด โดยมีขอบเขตการดำเนินงานดังต่อไปนี้

1. ข้อกำหนดขั้นต่ำด้านเทคนิค/ขอบเขตการดำเนินงาน

1.1 สิทธิการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย Backup Server จำนวน 2 เครื่อง

1.1.1 ยี่ห้อ Huawei รุ่น 2288H Serial No. 2102311XBHP0L3000004

1.1.2 ยี่ห้อ Huawei รุ่น 2288H Serial No. 2102311XBHP0L3000005

1.2 สิทธิการใช้งานอุปกรณ์สำรองข้อมูล (Backup Storage) จำนวน 1 หน่วย

1.2.1 ยี่ห้อ Huawei รุ่น Oceanstore 2200 Serial No. 2102350SHW10L2000014

1.3 สิทธิการใช้งานเทปสำรองข้อมูล (Tape Library) จำนวน 2 หน่วย

1.3.1 ยี่ห้อ HPE รุ่น MSL3040 Serial No. DEC00204KU

1.3.2 ยี่ห้อ HPE รุ่น MSL3040 Serial No. DEC00204KR

1.4 สิทธิการใช้งานซอฟต์แวร์สำรองข้อมูลระบบงาน Veeam License ประกอบด้วย

1.4.1 Veeam Availability Suite Ent Plus + Veeam ONE จำนวน 16 Unit

1.4.2 Veeam Availability Suite Universal จำนวน 2 Unit

1.5 สิทธิการใช้งานซอฟต์แวร์สำรองข้อมูลระบบงาน NETBACKUP License ประกอบด้วย

1.5.1 NETBACKUP ENT Server WLS 1 Server Hardware Tier1 Onpremise STD จำนวน 1 Unit

1.5.2 NETBACKUP ENT Client WLS 1 Server Hardware Tier2 Onpremise STD จำนวน 1 Unit

1.5.3 NETBACKUP Client Application and DB Pack WLS 1 Server Hardware Tier2 Onpremise STD จำนวน 1 Unit

1.5.4 NETBACKUP OPT Library Based Tape drive XPLAT 1 Drive Onpremise STD จำนวน 2 Unit

1.5.5 NETBACKUP Deduplication Data Protection Optimization OPT XPLAT 1 Front End TB Onpremise STD จำนวน 5 Unit

1.6 จัดให้มีเจ้าหน้าที่ในการปฏิบัติงานจำนวนไม่น้อยกว่า 1 คนเพื่อปฏิบัติงานด้านการสำรองข้อมูลในแต่ละวัน ณ สำนักงานใหญ่ของธนาคาร

2. การให้บริการสนับสนุนตลอดระยะเวลาการใช้บริการ (Support)

2.1 ผู้เสนอราคาที่ได้รับคัดเลือกจะต้องให้บริการสนับสนุน เป็นระยะเวลา 1 ปี อย่างน้อยดังต่อไปนี้

2.1.1 ต้องจัดให้มีเจ้าหน้าที่ ที่มีความเชี่ยวชาญเพื่อดูแลรักษาระบบสำรองข้อมูล และตรวจสอบการทำงานของระบบสำรองข้อมูลและกู้คืนข้อมูลให้สามารถทำงานได้อย่างมีประสิทธิภาพทุกวันที่ได้ทำการสำรองข้อมูล ต้องจัดให้มีบุคลากรที่จะให้การสนับสนุนธนาคารในระหว่างดำเนินโครงการจนแล้วเสร็จตามระยะเวลาที่กำหนด โดยแก้ไขปัญหาผ่านทางโทรศัพท์ และ/หรือช่องทางอื่นได้ ตลอด 24 ชั่วโมง

2.1.2 ให้คำแนะนำในการประยุกต์ใช้ และการดำเนินงานอื่น ๆ ที่จำเป็นเพื่อให้ธนาคารสามารถใช้บริการ สำรองข้อมูลและกู้คืนข้อมูล ได้อย่างมีประสิทธิภาพ

2.1.3 จัดให้มีเจ้าหน้าที่ในการปฏิบัติงานจำนวนไม่น้อยกว่า 1 คนเพื่อปฏิบัติงานด้านการสำรองข้อมูลในแต่ละวัน ณ สำนักงานใหญ่ของธนาคาร และนำส่งเทปที่ได้ทำการสำรองข้อมูลหลังจากการสำรองข้อมูลเสร็จสมบูรณ์ของทุกวันไปยังจุดรับเทปของธนาคาร

2.1.4 ต้องจัดทำรายงานสรุปรายละเอียดของระบบสำรองข้อมูลและอุปกรณ์ที่ใช้สำรองข้อมูลทั้งหมดส่งให้ธนาคารนำส่งแต่ละรายเดือน ทุกๆ วันสิ้นเดือน

2.2 ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการแก้ไขปัญหาให้แล้วเสร็จภายในกำหนดระยะเวลา ตามระดับผลกระทบที่มีต่อธุรกิจ หรือ การทำงาน (Severity) ดังนี้

ระดับผลกระทบ (Severity)	ระยะเวลาติดต่อกลับ	ระยะเวลาการแก้ไขปัญหาเสร็จสิ้นนับจากที่ได้รับแจ้ง
Urgent ไม่สามารถใช้งานระบบหรืออุปกรณ์ระบบสำรองข้อมูล Backup as a Service ได้	30 minutes	4 hours
High ระบบหรืออุปกรณ์ระบบสำรองข้อมูล Backup as a Service สามารถทำงานได้เพียงบางส่วน	1 hour	8 hours
Medium ระบบหรืออุปกรณ์ระบบสำรองข้อมูล Backup as a Service ทำงานผิดพลาดซึ่งไม่เป็นส่วนสำคัญ แต่ยังส่งผลบางส่วนต่อการสำรองข้อมูลของธนาคาร	2 hours	48 hours
Low ระบบหรืออุปกรณ์ระบบสำรองข้อมูล Backup as a Service ทำงานผิดพลาดซึ่งไม่เป็นส่วนที่กระทบการการสำรองข้อมูลของธนาคาร	4 hours	96 hours

2.3 ต้องนำส่งรายละเอียดและขั้นตอนการแก้ไขปัญหา เหตุขัดข้อง และ/หรือความชำรุดบกพร่องของระบบสำรองข้อมูล อย่างละเอียดให้แก่ธนาคารในทันทีที่สามารถดำเนินการได้ และผู้ให้บริการตกลงเป็นผู้รับผิดชอบชำระค่าใช้จ่ายที่เกิดขึ้นจากการเข้าดำเนินการทั้งจำนวน

2.4 ต้องจัดทำแผนทดสอบการกู้คืนข้อมูลนำส่งธนาคารภายใน 90 วันนับถัดจากวันเริ่มการให้บริการ และต้องทดสอบกู้คืนข้อมูลไม่น้อยกว่า 1 ครั้ง/ปี ร่วมกับเจ้าหน้าที่ธนาคาร โดยผู้ให้บริการจะต้องแจ้งกำหนดเวลาที่แน่นอนก่อนการเข้ามาให้บริการล่วงหน้าไม่น้อยกว่า 10 วันทำการ และนำส่งรายงานผลการทดสอบการกู้คืนข้อมูล ภายใน 30 วัน นับจากวันที่เข้าดำเนินการ

2.5 ต้องจัดให้มีเจ้าหน้าที่เข้าตรวจสอบและบำรุงรักษาการบริการเซ่าระบบสำรองข้อมูล (Preventive Maintenance) 4 ครั้ง/ปี พร้อมทั้งจัดทำรายละเอียดและขั้นตอนการตรวจเช็ค รวมทั้งข้อเสนอแนะที่เป็นประโยชน์ต่อธนาคารเป็นลายลักษณ์อักษรทุกครั้งที่ให้บริการและนำส่งรายงานภายใน 15 วันทำการนับจากวันที่ให้เข้าบริการ โดยผู้ให้บริการจะต้องแจ้งกำหนดวันเวลาที่แน่นอนก่อนการเข้ามาให้บริการล่วงหน้าไม่น้อยกว่า 1 วันทำการ ดังนี้

ครั้งที่ 1	ภายในเดือนตุลาคม	2567	ครั้งที่ 2	ภายในเดือนมกราคม	2568
ครั้งที่ 3	ภายในเดือนเมษายน	2568	ครั้งที่ 4	ภายในเดือนกรกฎาคม	2568

2.6 กรณีตรวจพบช่องโหว่ระบบปฏิบัติการ (Operating System: OS) หรือ Software ที่เกี่ยวข้องระบบสำรองข้อมูล ต้องจัดให้มีเจ้าหน้าที่ดำเนินการปิดช่องโหว่ตามระยะเวลาที่ธนาคารกำหนดโดยไม่มีค่าใช้จ่ายเพิ่มเติม ดังนี้

2.5.1 ระดับ High แก้ไขปิดช่องโหว่ภายใน 3 วัน นับจากได้รับแจ้งจากธนาคาร

2.5.2 ระดับ Medium แก้ไขปิดช่องโหว่ภายใน 5 วัน นับจากได้รับแจ้งจากธนาคาร

2.5.3 ระดับ Low หรือ อื่นๆ ภายใน 7 วัน นับจากได้รับแจ้งจากธนาคาร

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างผู้ให้บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์**
2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
3. วงเงินงบประมาณที่ได้รับจัดสรร **2,400,000.00 บาท (สองล้านสี่แสนบาทถ้วน)**
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 30 ก.ค. 2567

   เป็นเงิน 1,318,000.00 บาท (หนึ่งล้านสามแสนหนึ่งหมื่นแปดพันบาทถ้วน)
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   บริษัท อาสค์โฟร์คีย์ จำกัด
6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายฉัตรชัย	อาศรมเงิน	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.2 นายจรัส	ขวัญพิเชษฐ์สกุล	ผู้บริหารส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.3 นางสาววิลาสินี	คำเพ็ง	ผู้ช่วยผู้บริหารส่วนบริหารจัดการโครงสร้างพื้นฐานและระบบเครือข่าย /ฝ่าย ปส.

ผนวก 1
ขอบเขตการดำเนินงาน
การจ้างผู้ให้บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์

ผู้ยื่นข้อเสนอต้องจัดหาบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ โดยมีขอบเขตการดำเนินงานดังต่อไปนี้

1. **ข้อกำหนดความต้องการทั่วไป**
   - 1.1 ต้องเสนอบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ที่มีคุณสมบัติที่สามารถใช้งานร่วมกับระบบเครือข่าย และระบบคอมพิวเตอร์ที่ธนาคารใช้งานอยู่ในปัจจุบันได้
   - 1.2 สามารถแจ้งเตือนเหตุการณ์ที่เกิดขึ้นได้ตามเงื่อนไขที่ได้กำหนดไว้ ผ่านทาง SNMP หรือ Syslog หรือ Email หรือ SMS ได้
   - 1.3 สามารถบริหารจัดการผ่าน Web Browser ได้
   - 1.4 หากมีส่วนประกอบเพิ่มเติมใดที่มิได้ระบุไว้ในเอกสารรายละเอียดของคุณลักษณะเฉพาะและขอบเขตการดำเนินงาน แต่มีความจำเป็นต่อการใช้งานของบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ เพื่อให้งานแล้วเสร็จ สามารถใช้งานบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ได้ครบถ้วน ถูกต้อง ผู้ยื่นข้อเสนอต้องจัดหาหรือจัดทำมาให้เพียงพอต่อการใช้งานของธนาคาร และต้องส่งมอบให้เป็นกรรมสิทธิ์ หรือสิทธิ์ หรือลิขสิทธิ์ของธนาคารทั้งหมด โดยไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติม

2. **ข้อกำหนดคุณสมบัติเฉพาะของบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์**
   บริการป้องกันเว็บไซต์ของธนาคารจากการโจมตีในระดับเว็บแอปพลิเคชัน จำนวนไม่น้อยกว่า 1 โดเมน (exim.go.th) และ Sub-domain แบบไม่จำกัดตามที่ธนาคารเป็นผู้กำหนด ต้องมีความสามารถคุณสมบัติขั้นต่ำดังนี้
   - 2.1 ความสามารถในการป้องกันการโจมตีประเภท DDoS (DDoS Protections)
     - 2.1.1 สามารถป้องกันการโจมตีจากในระดับเครือข่าย (DDoS attack) ที่ระดับ Network layer 3, 4 และ 7
     - 2.1.2 สามารถป้องกันการโจมตีในระดับเครือข่าย (DDoS attack) แบบไม่จำกัดจำนวนครั้ง และขนาดของการโจมตี โดยไม่มีค่าใช้จ่ายเพิ่มเติม (Unlimited DDOS protection)
     - 2.1.3 มีเครือข่ายที่มีความสามารถในการป้องกันการโจมตีจากประเภท DDoS ขนาดไม่น้อยกว่า 20 Tbps
     - 2.1.4 มี Node หรือ Point of Presence (PoP) จำนวนไม่น้อยกว่า 250 จุดทั่วโลก และมีจำนวนไม่น้อยกว่า 6 จุด ในประเทศไทยที่มีการเชื่อมต่อกับโครงข่ายอินเทอร์เน็ตระหว่างประเทศ (International Internet Gateway: IIG)
     - 2.1.5 Node หรือ Point of Presence (POP) ที่อยู่ในประเทศไทยจะต้องมีความสามารถในการป้องกัน DDoS, Web Application Firewall (WAF) และ Content Delivery Network (CDN) ได้
     - 2.1.6 เป็นผลิตภัณฑ์ที่ถูกจัดอยู่ในกลุ่ม Leader ของ The Forrester Wave ในหัวข้อของ Web Application Firewall ปี 2022 หรือ ปีล่าสุด
   - 2.2 ความสามารถในการป้องกันเว็บแอพพลิเคชัน (Web Security Functions)
     - 2.2.1 สามารถป้องกันการโจมตีผ่านทาง Website ตามเงื่อนไขของ OWASP Top10 ดังนี้
       - 2.2.1.1 SQL injection
       - 2.2.1.2 Broken Authentication
       - 2.2.1.3 Sensitive Data Exposure

2.2.1.4 XML External Entities (XEE)

2.2.1.5 Broken Access Control

2.2.1.6 Security Misconfiguration

2.2.1.7 Cross-Site Scripting

2.2.1.8 Insecure Deserialization

2.2.1.9 Using Components with Known Vulnerabilities

2.2.1.10 Insufficient Logging and Monitoring

2.2.2 สามารถกำหนดค่าของ Web Application Firewall (WAF) ได้แบบไม่จำกัดจำนวน (Unlimited Custom WAF rules) และตั้งค่าการเปิดปิด WAF Rule ให้มีผลบังคับใช้ (Effective) ภายในระยะเวลาไม่เกิน 30 วินาที

2.2.3 สามารถกำหนดค่า IP Firewall ด้วยเงื่อนไข Source IP address, Source IP address range, Autonomous System Number (ASN) และประเทศได้

2.2.4 สามารถกำหนดค่า Rate Limit Rules ในการป้องกันการเข้าถึง Website ได้ไม่น้อยกว่า 100 rules

2.2.5 สามารถทำการตรวจสอบการออกใบรับรอง SSL (Certificate transparency monitoring) โดยสามารถแจ้งเตือนเมื่อมีผู้ทำการออกใบรับรองภายใต้ชื่อโดเมนเดียวกันกับของธนาคาร

2.2.6 สามารถตรวจจับและระบุการใช้งาน Javascript ได้ด้วยเงื่อนไขว่ามีการใช้งาน Javascript นั้นๆ ครั้งแรกและครั้งล่าสุดเมื่อใด และทำการแจ้งเตือนได้ดังนี้

2.2.6.1 มีการเรียกใช้งาน Javascript ใหม่ที่เกิดขึ้น

2.2.6.2 Javascript ที่ใช้งานอยู่มีการเปลี่ยนแปลง (Page attribution)

2.2.6.3 มีการเรียกใช้งาน Javascript จากโดเมนใหม่

2.2.7 เป็นผลิตภัณฑ์ที่จัดอยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในหัวข้อ Web Application and API Protection (WAAP) ปี 2022 หรือ ปีล่าสุด

2.2.8 สามารถเพิ่มความปลอดภัยให้กับ DNS จากการถูกปลอมแปลงข้อมูลจากผู้ไม่หวังดีผ่านระบบ DNS ด้วยการทำ DNSSEC (DNS Security Extensions) ได้

2.3 ความสามารถในการเพิ่มประสิทธิภาพเว็บแอพพลิเคชัน (Content Delivery Network : CDN & Optimization)

2.3.1 มีบริการ Authoritative DNS services สำหรับโดเมนสาธารณะ และต้องมี Host Domains ทุกภูมิภาคทั่วโลก โดยต้องมี node ในประเทศไทยไม่น้อยกว่า 6 จุด

2.3.2 มีระบบ Caching ในการจัดเก็บเนื้อหาของเว็บไซต์ โดยสามารถทำ Static Content Caching ดังต่อไปนี้ได้

2.3.2.1 ประเภทรูปภาพ

2.3.2.2 ประเภทวีดีโอ

2.3.2.3 ประเภทตัวอักษร

2.3.2.4 ประเภทไฟล์บีบอัด

2.3.3 สามารถลบ Cache (Purge cache) ทั้งหมดได้ทันที หรือกำหนดเงื่อนไขการลบ Cache เฉพาะ URL, Host name และ Tag ได้

2.3.4 สามารถใช้ API ในการอัพเดท Cache ในกรณีที่มีการอัพเดท Content ใหม่

2.3.5 บริการต้องรองรับการใช้ Bandwidth Consumption ได้ไม่น้อยกว่า 7 TB ต่อเดือน

2.3.6 สามารถลดขนาด บีบอัด และลบ Metadata ของไฟล์ ด้วยเทคโนโลยี ดังต่อไปนี้

2.3.6.1 Lossless

2.3.6.2 Lossy

2.3.6.3 WebP

2.3.7 สามารถทำการลบตัวอักษรที่ไม่จำเป็นใน Source code เช่น Whitespace และ Comments ได้

2.3.8 มีระบบ Always-on ที่สามารถทำการแสดง static content ในกรณีที่ Server ต้นทาง ไม่สามารถใช้งานได้

2.3.9 สามารถลด Latency time ให้กับ Dynamic content และแสดงผลในรูปแบบของประสิทธิภาพที่เพิ่มขึ้น และเวลาที่ตอบสนองได้

2.3.10 สามารถทำการเก็บ Payload logging เมื่อมี request traffic ที่ตรงกับ Web Application Firewall Rule ที่ได้ทำการสร้างไว้

2.3.11 สามารถทำ Load Balancing โดยสามารถทำ Automatic Failover, Geographic routing และ Active health check ได้ไม่น้อยกว่า 8 Origins

2.4 ความสามารถในการแสดงรายงาน (Dashboard Functions)

2.4.1 มี Dashboard แสดงรายงานประเภท Security แบบ Real-time หรือ Near Real-time โดยสามารถแสดงถึงข้อมูลแหล่งที่มาของการโจมตี เช่น IP Address, Browser, Country และ Autonomous System Number (ASN) ได้

2.4.2 มี Dashboard แสดงรายงานประเภท Analytic แบบ Real-time หรือ Near Real-time โดยมีรายละเอียด Total Requests, Cached Request, Bandwidth Saved, Threat Sources, Top Threat Origin และ Top Traffic Origin ได้

2.4.3 สามารถส่ง Raw log และ Event log การใช้งาน ไปยังสถานที่เก็บ log ของธนาคารได้

2.4.4 สามารถกำหนดสิทธิผู้ใช้งาน (RBAC) และยืนยันตัวตนด้วยวิธี Two-Factor Authentication ได้

3. การรับประกันคุณภาพ (Warranty)

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะต้องจัดให้มีการรับประกันการอนุญาตให้ใช้สิทธิในโปรแกรมเป็นระยะเวลา 1 ปี เริ่มตั้งแต่วันที่ 1 พฤศจิกายน 2567 – 31 ตุลาคม 2568

4. การให้บริการสนับสนุนของการใช้บริการตลอดระยะเวลาการใช้บริการ (Support)

4.1 ดำเนินการดูแลพร้อมให้บริการแก้ไขปัญหาเกี่ยวกับบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ตลอดระยะเวลา 1 ปี พร้อมจัดทำรายงานสรุปสถิติภัยคุกคามประจำเดือน (Monthly Report)

4.2 จัดให้มีเจ้าหน้าที่เข้าตรวจสอบสถานะการทำงานของระบบ (Preventive Maintenance) ไม่น้อยกว่า 4 ครั้ง/ปี พร้อมจัดทำรายงานสรุปการดำเนินการ และสถานะของระบบ รวมถึงเหตุการณ์ที่น่าสนใจ โดยต้องแจ้งให้ธนาคารทราบล่วงหน้าในการเข้าดำเนินการไม่น้อยกว่า 1 วัน และต้องได้รับความเห็นชอบจากธนาคารก่อนเข้าดำเนินการ และส่งมอบรายงานให้ธนาคารภายใน 15 วันของเดือนถัดไป ตามรายละเอียด ดังต่อไปนี้

4.2.1 รายงานสรุปผลการตรวจสอบสถานะของระบบ (Health Check Report) สรุปผลการตรวจสอบและสถานะของบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์

4.2.2 รายงานสรุปเหตุการณ์ที่น่าสนใจ (Events Report) ซึ่งได้ตรวจพบจาก Traffic log บน Dashboard ของบริการป้องกันภัยคุกคาม WAF DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์

ครั้งที่ 1 ภายในเดือนมกราคม 2568
ครั้งที่ 2 ภายในเดือนเมษายน 2568
ครั้งที่ 3 ภายในเดือนกรกฎาคม 2568

ครั้งที่ 4 ภายในเดือนตุลาคม 2568

4.3 ตลอดระยะเวลาการให้บริการจะต้องจัดให้มีทีมงานที่มีความรู้ความชำนาญเกี่ยวกับบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ พร้อมหมายเลขโทรศัพท์ที่สามารถติดต่อได้เพื่อให้คำปรึกษา และให้ความช่วยเหลือเบื้องต้น (On Phone Support) ทุกวันตลอด 24 ชั่วโมง (7x24)

4.4 ในกรณีที่บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ เกิดเหตุขัดข้องชำรุด หรือมีข้อบกพร่องที่ไม่สามารถใช้งานได้ ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกจะต้องจัดส่งเจ้าหน้าที่เข้ามาให้บริการตรวจสอบ และแก้ไขปัญหาให้กับทางธนาคาร รวมทั้งต้องดำเนินการตรวจสอบแก้ไขหรือปรับปรุงให้แล้วเสร็จภายในกำหนดระยะเวลานับถัดจากที่ได้รับแจ้งเหตุขัดข้องหรือความชำรุดบกพร่องจากธนาคาร ตามระดับผลกระทบที่มีต่อธุรกิจ หรือการทำงาน (Severity) ดังนี้

ระดับผลกระทบ (Severity)	ระยะเวลาติดต่อกลับ	ระยะเวลาการแก้ไขปัญหาเสร็จสิ้นนับจากที่ได้รับแจ้ง
Urgent บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ไม่สามารถใช้งานได้	30 นาที	4 (สี่) ชั่วโมง
High บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ทำงานผิดพลาดซึ่งเป็นส่วนสำคัญที่ส่งผลกระทบต่อการดำเนินงานของธนาคาร	1 ชั่วโมง	8 (แปด) ชั่วโมง
Medium บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ทำงานผิดพลาดซึ่งไม่เป็นส่วนสำคัญที่กระทบต่อการดำเนินงานของธนาคาร	2 ชั่วโมง	48 (สี่สิบแปด) ชั่วโมง
Low บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ทำงานผิดพลาด ซึ่งไม่เป็นส่วนสำคัญที่ไม่กระทบต่อการดำเนินงานของธนาคาร	4 ชั่วโมง	96 (เก้าสิบหก) ชั่วโมง

4.5 ในกรณีที่ธนาคารร้องขอให้ติดตั้ง Sub-domain เพิ่มเติม ทางผู้ยื่นข้อเสนอจะต้องดำเนินการติดตั้ง แก้ไขปัญหา และทดสอบความพร้อมใช้งานของบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ โดยไม่มีค่าใช้จ่ายเพิ่มเติม

4.6 จัดทำรายละเอียดและขั้นตอนการเข้ามาดำเนินการแก้ไขปัญหาหรือเหตุขัดข้องหรือความชำรุดบกพร่องของบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ให้กับธนาคารในทันทีที่สามารถดำเนินการได้

4.7 ดำเนินการ Review Policy ตาม Best Practice เพื่อปรับปรุงระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ตามที่ธนาคารได้มีการร้องขอ โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

4.8 ดำเนินการ Configure บริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ตามที่ธนาคารได้มีการร้องขอ

5. การ Upgrade โปรแกรม

ในระหว่างดำเนินการติดตั้งหรือภายในระยะเวลารับประกัน หาก Application Software หรือ Firmware หรือ Patch หรือระบบปฏิบัติการของบริการป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ มีการออก Version ใหม่ หรือพัฒนาปรับปรุง (Upgrade) ผู้ยื่นข้อเสนอที่ได้รับเลือกจะต้องแจ้งรายละเอียดการเปลี่ยนแปลงและผลกระทบที่เกิดขึ้นจากการเปลี่ยนแปลงดังกล่าวให้ธนาคารทราบ เพื่อใช้เป็นข้อมูลประกอบการตัดสินใจของธนาคาร และหากธนาคารประสงค์จะดำเนินการพัฒนาปรับปรุง (Upgrade) ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการพัฒนาปรับปรุง (Upgrade) ให้กับธนาคารโดยไม่คิดค่าใช้จ่าย