EXIM THAILAND

ประกาศราคากลาง

ลำดับ	รายการ/ชื่อเรื่อง	วิธี	ราคากลาง	ประเภทไฟล์	วันที่ประกาศ
1	ประกาศราคากลาง การจ้างผู้ให้บริการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและโปรแกรมสำเร็จรูปด้านฐานข้อมูลของระบบงานหลัก (Oracle Sparc T5-2) (/getattachment/e05e1c17-7232-4a3a-81da-5dfeb6a5e18d/ประกาศราคากลาง-การ	วิธีพิเศษ	1,412,400.00	PDF (/getattachment/e05e1c17-7232-4a3a-81da-	25 กรกฎาคม 2568
2	ประกาศราคากลาง การจ้างผู้ให้บริการสิทธิการใช้งานระบบป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็บไซต์ (/getattachment/4f57d529-ef22-4904-b992-4a37d79eca12/ประกาศราคากลาง-การจางผใหบรการสทธการใชงานระบบปองกนภยคกคาม-DDOS-และ	วิธีพิเศษ	1,318,000.00	PDF (/getattachment/4f57d529-ef22-4904-b992-	24 กรกฎาคม 2568
3	ประกาศราคากลาง การเช่าอุปกรณ์เครือข่าย Network Equipment Service (/getattachment/4579ff7b-0766-427d-8ba2-b1e94a7a4295/ประกาศราคากลาง-การเชาอปกรณเครอขาย-Network-Equipment-Service.aspx)	วิธีพิเศษ	2,461,000.00	PDF (/getattachment/4579ff7b-0766-427d-8ba2-	21 กรกฎาคม 2568
4	ประกาศราคากลางจ้างที่ปรึกษาสำหรับการนำ Fund Transfer Pricing (FTP) มาใช้ในองค์กร (/getattachment/f0891df6-006d-4524-92bb-e11701fe273a/ประกาศราคากลางจางทปรกษาสำหรบการนำ-Fund-Transfer-Pricing-(FTP)-มาใชในองคกร.aspx)	วิธีคัดเลือก	8,125,480.40	PDF (/getattachment/f0891df6-006d-4524-92bb-	21 กรกฎาคม 2568
5	ประกาศราคากลาง การเช่าระบบสำรองข้อมูล Backup as a Service (/getattachment/76772169-3e53-44b7-8488-1cf47e098619/ประกาศราคากลาง-การเชาระบบสำรองขอมล-Backup-as-a-Service.aspx)	วิธีพิเศษ	2,136,400.00	PDF (/getattachment/76772169-3e53-44b7-8488-	17 กรกฎาคม 2568
6	ประกาศราคากลาง การจ้างจัดทำของที่ระลึกสำหรับพนักงานเกษียณอายุการทำงานประจำปี 2568 (/getattachment/5ddebd45-1ced-4fc0-a933-1c8615505060/ประกาศราคากลาง-การจางจดทำของทระลกสำหรบพนกงานเกษยณอายการทำงานประจำป-2568.aspx)	วิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)	789,802.00	PDF (/getattachment/5ddebd45-1ced-4fc0-a933-	14 กรกฎาคม 2568
7	ประกาศราคากลาง การเช่าศูนย์สำรองระบบคอมพิวเตอร์ ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉิน (/getattachment/11e4b388-1507-4328-a005-7d1df7405904/ประกาศราคากลาง-การเชาศนยสำรองระบบคอมพวเตอร-ตามแผนกอบกธรกจกรณเกดเหตฉกเฉน.aspx)	วิธีพิเศษ	3,696,000.00	PDF (/getattachment/11e4b388-1507-4328-a005-	09 กรกฎาคม 2568
8	ประกาศราคากลาง การจ้างผู้ให้บริการ Security Operation Center (SOC) (/getattachment/717a9589-f989-4b20-88a2-46571fbb9085/ประกาศราคากลาง-การจางผใหบรการ-Security-Operation-Center-(SOC).aspx)	วิธีประกาศเชิญชวน	3,181,700.00	PDF (/getattachment/717a9589-f989-4b20-88a2-	04 กรกฎาคม 2568
9	ประกาศราคากลาง จ้างผู้ให้บริการพัฒนาระบบ LOS ฝ่ายงาน RM และ CA ของสายงาน SME (/getattachment/6feb1b97-7ffb-415c-b371-286765ac147f/ประกาศราคากลาง-จางผใหบรการพฒนาระบบ-LOS-ฝายงาน-RM-และ-CA-ของสายงาน-SME.aspx)	วิธีพิเศษ	3,353,432.00	PDF (/getattachment/6feb1b97-7ffb-415c-b371-	25 มิถุนายน 2568
10	ประกาศราคากลาง การจ้างผู้ให้บริการพัฒนา Database Upgrade ระบบ Kastle (/getattachment/4d5fb8e5-8a0a-43a6-9c89-a23fe3c7855e/ประกาศราคากลาง-การจางผใหบรการพฒนา-Database-Upgrade-ระบบ-Kastle.aspx)	วิธีพิเศษ	3,366,656.87	PDF (/getattachment/4d5fb8e5-8a0a-43a6-9c89-	23 มิถุนายน 2568

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ การจ้างผู้ให้บริการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและโปรแกรมสำเร็จรูปด้านฐานข้อมูลของระบบงานหลัก (Oracle Sparc T5-2)
2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
3. วงเงินงบประมาณที่ได้รับจัดสรร 1,600,000.00 บาท (หนึ่งล้านหกแสนบาทถ้วน)
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) /วันที่ 25 ก.ค. 2568
   เป็นเงิน ทั้งสิ้น 1,412,400.00 บาท (หนึ่งล้านสี่แสนหนึ่งหมื่นสองพันสี่ร้อยบาทถ้วน)
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   บริษัท นีโอพลัส จำกัด
6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายศรณรินทร์	ยศสุพรม	ผู้ช่วยผู้บริหารส่วนบริหารจัดการโครงสร้างพื้นฐานและระบบเครือข่าย /ฝ่าย ปส.
6.2 นายกิตติ์ธเนศ	วงศ์ประสิทธิ์	ผู้ช่วยผู้บริหารส่วนบริการและปฏิบัติการเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.3 นางสาวจิตรา	ขันแก้ว	เจ้าหน้าที่ธุรการส่วนจัดซื้อเทคโนโลยีสารสนเทศ /ฝ่าย จธ.

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่าย

และโปรแกรมสำเร็จรูปด้านฐานข้อมูลของระบบงานหลัก (Oracle Sparc T5-2)

---

1. **ขอบเขตการดำเนินงาน**

ผู้ยื่นข้อเสนอต้องเสนอบริการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและโปรแกรมสำเร็จรูปด้านฐานข้อมูลของระบบงานหลัก (Oracle Sparc T5-2) Server Serial No : AK00220255 ที่ตั้งอยู่ ณ ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

2. **การให้บริการสนับสนุนตลอดระยะเวลาการใช้บริการ (Support)**

2.1 ต้องจัดให้มีเจ้าหน้าที่ประสานงานพร้อมเบอร์โทรศัพท์ที่สามารถรับแจ้งเหตุขัดข้องและให้คำปรึกษาแก้ไขปัญหาต่างๆ เกี่ยวกับการใช้งานระบบงาน ในวันจันทร์ถึงวันศุกร์ ระหว่างเวลา 8.30 น. - 17.00 น. และจัดให้มีช่องทางอื่นที่สามารถติดต่อขอรับคำปรึกษาจากผู้ให้บริการนอกวันและเวลาทำการของธนาคารได้ตลอดเวลา

2.2 ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการแก้ไขปัญหาให้แล้วเสร็จภายในกำหนดระยะเวลา ตามระดับผลกระทบที่มีต่อธุรกิจ หรือการทำงาน (Severity) ซึ่งให้เป็นไปตามดุลยพินิจของธนาคาร ดังนี้

ระดับผลกระทบ (Severity)	ระยะเวลาติดต่อกลับ	ระยะเวลาการแก้ไขปัญหาเสร็จสิ้น นับจากที่ได้รับแจ้ง
ปัญหาเร่งด่วน ธนาคารไม่สามารถใช้ระบบได้	30 นาที	4 ชั่วโมง
ปัญหาสำคัญ ระบบทำงานผิดพลาดในเรื่องสำคัญ หรือใช้งานได้บางส่วน	2 ชั่วโมง	24 ชั่วโมง
ปัญหาไม่เร่งด่วน ระบบทำงานผิดพลาดแบบไม่มีสาระสำคัญ	4 ชั่วโมง	72 ชั่วโมง

2.3 ต้องนำส่งรายละเอียดและขั้นตอนการแก้ไขปัญหา เหตุขัดข้อง และ/หรือความชำรุดบกพร่องของระบบงานอย่างละเอียดให้แก่ธนาคารในทันทีที่สามารถดำเนินการได้และผู้ยื่นข้อเสนอที่ได้รับคัดเลือกตกลงเป็นผู้รับผิดชอบชำระค่าใช้จ่ายที่เกิดขึ้นจากการเข้าดำเนินการทั้งจำนวน

2.4 จัดให้มีเจ้าหน้าที่เข้าตรวจสอบและบำรุงรักษา (Preventive Maintenance: PM) ไม่น้อยกว่า 4 ครั้ง/ปี พร้อมทั้งจัดทำรายละเอียดและขั้นตอนการตรวจเช็ครวมทั้งข้อเสนอแนะที่เป็นประโยชน์ต่อธนาคารเป็นลายลักษณ์อักษรทุกครั้งที่ให้บริการ โดยผู้ให้บริการจะต้องแจ้งกำหนดวันเวลาแน่นอน ก่อนการเข้ามาให้บริการล่วงหน้าไม่น้อยกว่า 1 วัน ดังนี้

ครั้งที่ 1 ภายในเดือนพฤศจิกายน 2568 ครั้งที่ 2 ภายในเดือนกุมภาพันธ์ 2569
ครั้งที่ 3 ภายในเดือนพฤษภาคม 2569 ครั้งที่ 4 ภายในเดือนสิงหาคม 2569

2.5 กรณีธนาคารตรวจพบช่องโหว่การจ้างผู้ให้บริการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและโปรแกรมสำเร็จรูปด้านฐานข้อมูลของระบบงานหลัก (Oracle Sparc T5-2) หรือ ช่องโหว่ของระบบปฏิบัติการที่ส่งผลกระทบต่อการจ้างผู้ให้บริการบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายและโปรแกรมสำเร็จรูปด้านฐานข้อมูลของระบบ

งานหลัก (Oracle Sparc T5-2) ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการแก้ไขปิดช่องโหว่ให้แล้วเสร็จ โดยไม่มีค่าใช้จ่ายเพิ่มเติม โดยมีรายละเอียดดังนี้

2.5.1 ช่องโหว่ระดับ High ดำเนินการภายใน 30 วัน นับจากได้รับแจ้งจากธนาคาร

2.5.2 ช่องโหว่ระดับ Medium ดำเนินการภายใน 60 วัน นับจากได้รับแจ้งจากธนาคาร

2.5.3 ช่องโหว่ระดับ Low หรือ อื่นๆ ดำเนินการภายใน 120 วัน นับจากได้รับแจ้งจากธนาคาร

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ การจ้างผู้ให้บริการสิทธิการใช้งานระบบป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์
2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
3. วงเงินงบประมาณที่ได้รับจัดสรร 1,500,000.00 บาท (หนึ่งล้านห้าแสนบาทถ้วน)
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 24/7/2025

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

   บริษัท อาสค์โฟร์คีย์ จำกัด (สำนักงานใหญ่)
6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

   6.1 นายชานนท์ แท่นทองจันทร์ ผู้ช่วยผู้บริหารส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ / ฝ่ายปส.

   6.2 นางสาววิลาสินี คำเพ็ง ผู้ช่วยผู้บริหารส่วนบริหารจัดการโครงสร้างพื้นฐานและระบบเครือข่าย / ฝ่ายปส.

   6.3 นางสาวอรพรรณ แสงศิริกุลชัย เจ้าหน้าที่ธุรการส่วนจัดซื้อเทคโนโลยีสารสนเทศ / ฝ่ายจธ.

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการสิทธิการใช้งานระบบป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์

ผู้ยื่นข้อเสนอต้องจัดหาบริการสิทธิการใช้งานระบบป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ โดยมีขอบเขตการดำเนินงานดังต่อไปนี้

1. **ข้อกำหนดความต้องการทั่วไป**
   - 1.1 ต้องเสนอบริการสิทธิการใช้งานระบบป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ที่มีคุณสมบัติที่สามารถใช้งานร่วมกับระบบเครือข่าย และระบบคอมพิวเตอร์ที่ธนาคารใช้งานอยู่ในปัจจุบันได้ เป็นระยะเวลา 1 ปี เริ่มตั้งแต่วันที่ 1 พฤศจิกายน 2568 – 31 ตุลาคม 2569
   - 1.2 สามารถแจ้งเตือนเหตุการณ์ที่เกิดขึ้นได้ตามเงื่อนไขที่ได้กำหนดไว้ ผ่านทาง SNMP หรือ Syslog หรือ Email หรือ SMS ได้
   - 1.3 สามารถบริหารจัดการผ่าน Web Browser ได้
   - 1.4 หากมีส่วนประกอบเพิ่มเติมใดที่มิได้ระบุไว้ในเอกสารรายละเอียดของคุณลักษณะเฉพาะและขอบเขตการดำเนินงาน แต่มีความจำเป็นต่อการใช้งานของระบบป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ เพื่อให้งานแล้วเสร็จ สามารถใช้งานระบบป้องกันภัยคุกคาม 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 ประเภทวีดิโอ

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. ระยะเวลาการให้บริการ

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะต้องจัดให้มีบริการงานจ้างดังกล่าวเป็นระยะเวลา 1 ปี เริ่มตั้งแต่วันที่ 1 พฤศจิกายน 2568 – 31 ตุลาคม 2569

4. การให้บริการสนับสนุนตลอดระยะเวลาการใช้บริการ (Support)

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

4.2 จัดให้มีเจ้าหน้าที่เข้าตรวจสอบสถานะการทำงานของระบบ (Preventive Maintenance) ไม่น้อยกว่า 4 ครั้ง/ปี พร้อมจัดทำรายงานสรุปการดำเนินการ และสถานะของระบบ รวมถึงเหตุการณ์ที่น่าสนใจ โดยต้องแจ้งให้ธนาคารทราบล่วงหน้าในการเข้าดำเนินการไม่น้อยกว่า 1 วัน และต้องได้รับความเห็นชอบจากธนาคารก่อนเข้าดำเนินการ พร้อมส่งมอบรายงานให้ธนาคาร ภายใน 15 วัน ของเดือนถัดไป 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 2569
ครั้งที่ 2 ภายในเดือนเมษายน 2569
ครั้งที่ 3 ภายในเดือนกรกฎาคม 2569
ครั้งที่ 4 ภายในเดือนตุลาคม 2569

4.3 ตลอดระยะเวลาการให้บริการจะต้องจัดให้มีทีมงานที่มีความรู้ความชำนาญเกี่ยวกับระบบป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ พร้อมหมายเลขโทรศัพท์ที่สามารถติดต่อได้เพื่อให้คำปรึกษาและให้ความช่วยเหลือเบื้องต้น (On Phone Support) ทุกวันตลอด 24 ชั่วโมง (7x24)

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

ระดับผลกระทบ (Severity)	ระยะเวลาติดต่อกลับ	ระยะเวลาการแก้ไขปัญหาเสร็จสิ้น นับจากที่ได้รับแจ้ง
ปัญหาเร่งด่วน ธนาคารไม่สามารถใช้ระบบได้	30 นาที	4 ชั่วโมง
ปัญหาสำคัญ ระบบทำงานผิดพลาดในเรื่องสำคัญ หรือใช้งานได้บางส่วน	2 ชั่วโมง	24 ชั่วโมง
ปัญหาไม่เร่งด่วน ระบบทำงานผิดพลาดแบบไม่มีสาระสำคัญ	4 ชั่วโมง	72 ชั่วโมง

4.5 ในกรณีที่ธนาคารประสงค์ให้ติดตั้ง Sub-domain เพิ่มเติม ทางผู้ยื่นข้อเสนอจะต้องดำเนินการติดตั้ง แก้ไขปัญหา และทดสอบความพร้อมใช้งานของระบบป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ โดยไม่มีค่าใช้จ่ายเพิ่มเติม

4.6 จัดทำรายละเอียดและขั้นตอนการเข้ามาดำเนินการแก้ไขปัญหาหรือเหตุขัดข้องหรือความชำรุดบกพร่องของระบบป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ให้กับธนาคารในทันทีที่สามารถดำเนินการได้

4.7 ดำเนินการ Review Policy ตาม Best Practice เพื่อปรับปรุงระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ตามที่ธนาคารได้มีการร้องขอ โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

4.8 ดำเนินการ Configure ระบบป้องกันภัยคุกคาม DDOS และเพิ่มประสิทธิภาพของเว็ปไซต์ ตามที่ธนาคารได้มีการร้องขอ โดยไม่มีค่าใช้จ่ายเพิ่มเติม

5. การ Upgrade โปรแกรม

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

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การเช่าอุปกรณ์เครือข่าย Network Equipment Service**

2. หน่วยงานเจ้าของโครงการ **ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ**

3. วงเงินงบประมาณที่ได้รับจัดสรร **3,000,000.00 บาท (สามล้านบาทถ้วน)**

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ...2..1..มี.ค..2568..
   เป็นเงิน **2,461,000.00 บาท (สองล้านสี่แสนหกหมื่นหนึ่งพันบาทถ้วน)**

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   บริษัท ดาต้าโปร คอมพิวเตอร์ ซิสเต็มส์ จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายชานนท์	แท่นทองจันทร์	ผู้ช่วยผู้บริหารส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ / ฝ่ายปส.
6.2 นางสาวศรัญญา	แวงวรรณ์	ผู้บริหารส่วนจัดซื้อเทคโนโลยีสารสนเทศ / ฝ่ายจธ.
6.3 นายจเร	บุญกร	ผู้ช่วยผู้บริหารส่วนบริหารจัดการโครงสร้างพื้นฐานและระบบเครือข่าย / ฝ่ายปส.

ผนวก 1

ขอบเขตการดำเนินงาน

การเช่าอุปกรณ์เครือข่าย Network Equipment Service

1. ความต้องการทั่วไป

1.1 ต้องเสนออุปกรณ์เครือข่ายที่มีคุณสมบัติสามารถทำงานร่วมกับระบบคอมพิวเตอร์และระบบ เครือข่ายของธนาคารที่ใช้งานอยู่ในปัจจุบันได้

1.2 หากอุปกรณ์ หรือโปรแกรม หรือสิทธิการใช้งาน หรือส่วนประกอบเพิ่มเติมที่ธนาคารไม่ได้กำหนด และมีความจำเป็นต้องนำมาใช้งานร่วมกันเพื่อให้เกิดประสิทธิภาพสูงสุดผู้เสนอราคาจะต้องจัดหาและส่ง มอบให้กับธนาคารได้อย่างครบถ้วน

1.3 อุปกรณ์ที่เสนอและส่งมอบต้องสามารถทำงานร่วมกันได้ทั้งระบบทั้งแบบมีสาย (Wired) และแบบไร้สาย (Wireless)

1.4 มีระบบการจัดการยืนยันตัวตนของผู้ใช้งานเพื่อเข้าถึงระบบเครือข่าย และของผู้บริหารเครือข่าย เพื่อเข้าไปบริหารจัดการอุปกรณ์ และต้องสามารถจัดการผ่านระบบการจัดการแบบศูนย์กลางเดียว (Single Centralized Authentication System) โดยสามารถควบคุมและกำหนดนโยบายการเชื่อมต่อเครือข่ายได้

1.5 สามารถทำงานบน IPv4 และ IPv6 ได้

1.6 โปรแกรมที่เกี่ยวข้องกับการให้บริการ ผู้ให้เช่าจะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย โดยไม่ละเมิดสิทธิ์ของผู้อื่น รวมทั้งรับผิดชอบในกรณีที่มีการกล่าวหา ฟ้องร้อง หรือเรียกค่าเสียหายใดๆ จากเจ้าของลิขสิทธิ์หรือผู้เรียกร้องอื่นใด

2. รายการอุปกรณ์ที่ต้องการเช่า รายละเอียดตามเอกสารแนบท้าย ก.

2.1 อุปกรณ์กระจายสัญญาณหลักเพื่อรองรับ Fiber Optic (Core Switch Fiber Optic) จำนวน 2 ชุด (N9K-C93180YC-EX)

2.2 อุปกรณ์กระจายสัญญาณหลักเพื่อรองรับ UTP (Core Switch UTP) จำนวน 3 ชุด (N2K-C2248TP-E)

2.3 อุปกรณ์กระจายสัญญาณเพื่อรองรับ Server Farm (Stack Switch Server Farm) จำนวน 2 ชุด (WS-C3650-48TD-L)

2.4 อุปกรณ์กระจายสัญญาณเพื่อรองรับ Server farm ชนิด 10 Gigabit จำนวน 2 ชุด (N3K-C3172TQ-XL)

2.5 อุปกรณ์กระจายสัญญาณ ขนาด 48 Port ประเภทที่ 1 (Access Switch 48 Port Type 1) จำนวน 10 ชุด (WS-C2960X-48FPD-L)

2.6 อุปกรณ์กระจายสัญญาณ ขนาด 48 Port ประเภทที่ 2 (Access Switch 48 Port Type 2) จำนวน 17 ชุด (WS-C2960X-48LPD-L)

2.7 อุปกรณ์กระจายสัญญาณขนาด 48 Port ประเภทที่ 3 (Access Switch 48 Port Type 3) จำนวน 2 ชุด (WS-C2960X-48LPS-L)

2.8 อุปกรณ์กระจายสัญญาณขนาด 24 Port ประเภทที่ 1 (Access Switch 24 Port Type 1) จำนวน 5 ชุด (WS-C2960X-24PD-L)

2.9 อุปกรณ์กระจายสัญญาณขนาด 24 Port ประเภทที่ 2 (Access Switch 24 Port Type 2) จำนวน 5 ชุด (WS-C2960X-24PS-L)

2.10 อุปกรณ์เชื่อมต่อเครือข่ายโมดูลสัญญาณใยแก้วนำแสง จำนวน 60 ชุด (SFP-10G-SR)

2.11 อุปกรณ์กระจายสัญญาณขนาด 24 Port สำหรับสาขา (Access Switch 24 Port for Branch) จำนวน 16 ชุด (WS-C2960X-24TS-L)

2.12 อุปกรณ์ควบคุมเครือข่ายไร้สาย (Wireless LAN Controller) จำนวน 2 ชุด (AIR-CT5520-K9)

2.13 อุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) จำนวน 65 ชุด (AIR-AP2802I-S-K9)

2.14 ระบบบริหารจัดการเครือข่าย จำนวน 1 ชุด (R-MGMT3X-N-K9)

2.14.1 สามารถบริหารจัดการอุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) ได้ไม่น้อยกว่า 90 ตัว

2.14.2 สามารถบริหารจัดการอุปกรณ์กระจายสัญญาณ (Switch) ได้ทั้งโครงการ

2.15 เครื่องคอมพิวเตอร์แม่ข่าย (Server) (UCSC-C240-M4S)

2.16 ระบบควบคุมและกำหนดนโยบายการเชื่อมต่อเครือข่าย จำนวน 1 ชุด (R-ISE-VM-K9, L-ISE-TACACS)

2.17 สายสัญญาณใยแก้วนำแสงที่ใช้ในการเดินข้ามระหว่างชั้น (Fiber Optic) ตามตำนวนการใช้งาน

2.17.1 สายสัญญาณใยแก้วนำแสง (Fiber Optic)

2.17.2 กล่องเก็บสายใยแก้วนำแสง (Fiber Optic Distribution Unit)

2.17.3 หัวต่อสายใยแก้วนำแสง (Fiber Optic Connector)

2.17.4 ชุดเชื่อมต่อสายใยแก้วนำแสง (Fiber Optic Adapter)

2.17.5 สายเชื่อมต่อสายใยแก้วนำแสง (Fiber Optic Patch Cord)

2.17.6 หัวต่อสายใยแก้วนำแสงแบบ Pigtail

2.18 สายสัญญาณ UTP (Unshielded Twisted Pair) CAT 6 ตามตำนวนการใช้งาน

2.19 แผงกระจายสาย (Patch Panel) CAT 6 ตามตำนวนการใช้งาน

2.20 เต้ารับสายสัญญาณตัวเมีย CAT 6 (RJ 45 modular Jack) ตามตำนวนการใช้งาน

2.21 สายต่อ CAT 6 (Patch Cord) ตามตำนวนการใช้งาน

2.22 ตู้สำหรับจัดเก็บอุปกรณ์ (Rack) ขนาด 9U จำนวน 3 ชุด

2.23 อุปกรณ์กระจายสัญญาณ ขนาด 48 ช่อง ประเภทที่ 1 (Access Switch 48 Port Type 1) จำนวน 6 ชุด (WS-C2960X-48FPD-L)

2.24 อุปกรณ์กระจายสัญญาณ ขนาด 48 ช่อง ประเภทที่ 1 (Access Switch 48 Port Type 1) จำนวน 2 ชุด (WS-C2960X-48FPD-L)

2.25 อุปกรณ์กระจายสัญญาณ ขนาด 48 ช่อง ประเภทที่ 2 (Access Switch 48 Port Type 2) จำนวน 1 ชุด (WS-C2960X-48LPD-L)

2.26 อุปกรณ์กระจายสัญญาณเพื่อรองรับ Server Farm (Stack Switch Server Farm) จำนวน 2 ชุด (WS-C3650-48TD-L)

2.27 อุปกรณ์กระจายสัญญาณ ขนาด 48 ช่อง ประเภทที่ 3 (Access Switch 48 Port Type 3) จำนวน 2 ชุด (WS-C2960X-48TD-L)

2.28 อุปกรณ์กระจายสัญญาณขนาด 24 ช่อง ประเภทที่ 1 (Access Switch 24 Port Type 1) จำนวน 2 ชุด (WS-C2960X-48TS-L)

2.29 อุปกรณ์ Stack Module Catalyst 2960X series พร้อมเสนอสาย จำนวน 18 ชุด

2.30 อุปกรณ์เชื่อมต่อเครือข่ายโมดูลสัญญาณใยแก้วนำแสง จำนวน 32 ชุด (SFP-10G-SR)

2.31 อุปกรณ์เชื่อมต่อเครือข่ายโมดูลสัญญาณใยแก้วนำแสง GLC-TE จำนวน 8 ชุด (GLC-TE)

2.32 อุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) 25 ชุด (AIR-AP2802I-S-K9)

2.33 อุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) จำนวน 2 ชุด (Catalyst 9100AX-Series)

2.34 อุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) เพิ่มเติม จำนวน 4 ชุด (อุปกรณ์ใหม่ไม่เคยผ่านการใช้งานมาก่อน)

2.35 บริการดูแล บำรุงรักษา รวมถึงการเคลม (Claim) อุปกรณ์ ให้อยู่ในสภาพพร้อมใช้งานตลอดเวลา (Maintenance Service Agreement) / MA

#	Host-Name	Serial Number	Model
1	SWITCH_TBP-LOSCRM	FOC1452Z2D5	Cisco Catalyst WS-C3560G-48PS
2	Exim_SW19_EXAC_1	FOC1452W3C0	Cisco Catalyst WS-C3560G-48PS-S
3	Exim_MGMT_2	FOC1245W15V	Cisco Catalyst WS-C3560G-48TS-S
4	EXIM_SW_EXAC	FOC1452W3FB	Cisco Catalyst WS-C3560G-48PS-S
5	Exim_SW16_2	FOC1452W3E0	Cisco Catalyst WS-C3560G-48PS-S
6	Exim_SW22_2	FOC1445Z4NL	Cisco Catalyst WS-C3560G-48PS-S
7	Rama2_SW2_COVID-Temp.exim.go.th	FOC1448Y3JC	Cisco Catalyst WS-C3560G-48TS-S
8	EXIM_SW15_3ExTm	FOC1447Z6BU	Cisco Catalyst WS-C2960G-24TC-L
9	Exim_SW19_COVID-1.exim.go.th	FOC1052Z1X3	Cisco Catalyst WS-C2960-48TC-L
10	Serithai_SW_4_Covid.exim.go.th	FOC1052X1JM	Cisco Catalyst WS-C2960-48TC-L
11	EXIM_SW22_3	FOC1501Y2QH	Cisco Catalyst WS-C2960G-24TC-L

3. การให้การสนับสนุนตลอดระยะเวลาการใช้บริการ (Support)

3.1 ในกรณีอุปกรณ์เครือข่ายภายใน Network Equipment Service เกิดเหตุขัดข้องชำรุด หรือมีข้อบกพร่องที่ไม่สามารถใช้งานได้ ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกจะต้องจัดส่งเจ้าหน้าที่เข้ามาให้บริการ ตรวจสอบ และแก้ไขปัญหาให้กับทางธนาคาร ณ สถานที่ตั้ง รวมทั้งต้องดำเนินการตรวจสอบแก้ไขหรือปรับปรุงให้แล้วเสร็จภายในกำหนดระยะเวลานับถัดจากที่ได้รับแจ้งเหตุขัดข้องหรือความชำรุดบกพร่องจากธนาคาร ตามระดับผลกระทบที่มีต่อธุรกิจ หรือการทำงาน (Severity) ซึ่งให้เป็นไปตามดุลยพินิจของธนาคาร ดังนี้

ระดับผลกระทบ (Severity)	ระยะเวลาติดต่อกลับ	ระยะเวลาการแก้ไขปัญหาเสร็จสิ้น นับจากที่ได้รับแจ้ง
ปัญหาเร่งด่วน ธนาคารไม่สามารถใช้ระบบได้	30 นาที	4 ชั่วโมง
ปัญหาสำคัญ ระบบทำงานผิดพลาดในเรื่องสำคัญ หรือใช้งานได้บางส่วน	2 ชั่วโมง	24 ชั่วโมง
ปัญหาไม่เร่งด่วน ระบบทำงานผิดพลาดแบบไม่มีสาระสำคัญ	4 ชั่วโมง	72 ชั่วโมง

3.2 ต้องจัดทำรายละเอียดและขั้นตอนการเข้ามาดำเนินการแก้ไขปัญหาหรือเหตุขัดข้องหรือความชำรุดบกพร่องของอุปกรณ์ระบบเครือข่ายที่ทางธนาคารเช่าในทันทีที่สามารถดำเนินการได้

3.3 จัดให้มีเจ้าหน้าที่เข้าตรวจสอบสถานะสถานะการทำงานของระบบ (Preventive Maintenance) ไม่น้อยกว่า 4 ครั้ง/ปี พร้อมจัดทำรายงานสรุปการดำเนินการ และสถานะของระบบ รวมถึงเหตุการณ์ที่น่าสนใจ

โดยต้องแจ้งให้ธนาคารทราบล่วงหน้าในการเข้าดำเนินการไม่น้อยกว่า 1 วันทำการ และต้องได้รับความเห็นชอบจากธนาคารก่อนเข้าดำเนินการพร้อมส่งมอบ ดังต่อไปนี้

- รายงานสรุปผลการตรวจสอบสถานะของระบบ (Health Check Report) สรุปผลการตรวจสอบ และสถานะของอุปกรณ์เครือข่าย Network Equipment Service รายงานสรุปเหตุการณ์ที่น่าสนใจ (Events Report) ซึ่งได้ตรวจพบจาก Traffic log บน Dashboard ของอุปกรณ์เครือข่ายภายใน Network Equipment Service

การตรวจสอบสถานะของระบบ (Preventive Maintenance) มีจำนวน 4 ครั้ง ดังนี้

ครั้งที่ 1 ภายในเดือนพฤศจิกายน 2568
ครั้งที่ 2 ภายในเดือนกุมภาพันธ์ 2569
ครั้งที่ 3 ภายในเดือนพฤษภาคม 2569
ครั้งที่ 4 ภายในเดือนสิงหาคม 2569

3.4 ในกรณีที่ธนาคารมีความต้องการเปลี่ยนแปลงปรับปรุงแก้ไขอุปกรณ์เครือข่ายภายใน Network Equipment Service ต้องจัดให้มีเจ้าหน้าที่ที่มีความรู้ความชำนาญเกี่ยวกับอุปกรณ์เครือข่ายภายใน Network Equipment Service เข้ามาสนับสนุนช่วยเหลือตลอดระยะเวลาการใช้บริการ โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

3.5 ในระหว่างสัญญาการใช้งาน หากพบว่าอุปกรณ์เครือข่าย Network Equipment Service สิ้นสุดการรับประกันคุณภาพหรือการสนับสนุนการให้บริการจากเจ้าของผลิตภัณฑ์ ผู้ให้เช่าจะต้องทำการเปลี่ยนอุปกรณ์เครือข่าย Network Equipment Service ให้กับธนาคารใหม่ โดยอุปกรณ์ฯ ที่เปลี่ยนจะต้องมีคุณสมบัติไม่ด้อยกว่าเดิม ภายใน 1 วัน

3.6 ในกรณีที่สัญญาณของอุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) ไม่ครอบคลุมพื้นที่การใช้งาน (Out of Coverage Area) ทางผู้ยื่นข้อเสนอต้องดำเนินการจัดหาอุปกรณ์กระจายสัญญาณไร้สายให้ครอบคลุมพื้นที่การใช้งาน โดยไม่มีค่าใช้จ่ายเพิ่มเติม

3.7 ดำเนินการ Upgrade firmware อุปกรณ์เครือข่าย Network Equipment Service firmware เพื่อปรับปรุงระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ตามที่ธนาคารได้มีการร้องขอ โดยไม่คิดค่าใช้จ่ายเพิ่มเติม

4. การสิ้นสุดสัญญาและการบอกเลิกสัญญา

4.1 ในกรณีอุปกรณ์เช่าดังกล่าวสิ้นอายุสัญญา ผู้ยื่นข้อเสนอสามารถเก็บอุปกรณ์ได้ภายหลัง 60 วัน นับจากวันที่หมดอายุสัญญา

No.	Type	Part ID	Product Description	Serial Number
2.1	Switch	N9K-C93180YC-EX	Nexus 9300 with 48p 10/25G SFP+ and 6p 100G QSFP28	FDO210805UH
		N9K-C93180YC-EX	Nexus 9300 with 48p 10/25G SFP+ and 6p 100G QSFP28	FDO210721P1
2.2	Switch	N2248TP-E-FA-BUN	Standard Airflow pack:N2K-C2248TP-E-1GE, 2 AC PS, 1Fan	FOX2108PCH1
		N2248TP-E-FA-BUN	Standard Airflow pack:N2K-C2248TP-E-1GE, 2 AC PS, 1Fan	FOX2108PCJ0
		N2248TP-E-FA-BUN	Standard Airflow pack:N2K-C2248TP-E-1GE, 2 AC PS, 1Fan	FOX2108PCMJ
2.3	Switch	WS-C3650-48TD-L	Cisco Catalyst 3650 48 Port Data 2x10G Uplink LAN Base	FDO2112E0CR
		C3650-STACK	Cisco Catalyst 3650 Stack Module	FDO21111K27
		C3650-STACK	Cisco Catalyst 3650 Stack Module	FDO21111GH1
		WS-C3650-48TD-L	Cisco Catalyst 3650 48 Port Data 2x10G Uplink LAN Base	FDO2109Q11E
		C3650-STACK	Cisco Catalyst 3650 Stack Module	FDO21111GH5
		C3650-STACK	Cisco Catalyst 3650 Stack Module	FDO21111J9B
2.4	Switch	N3K-C3172TQ-XL	Nexus 3172TQ, 48 x 10GT & 6 QSFP+ ports, extended memory	FOC2125R239
		N3K-C3172TQ-XL	Nexus 3172TQ, 48 x 10GT & 6 QSFP+ ports, extended memory	FOC2118R0RB
2.5	Switch	WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FCW2130B29L
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21296HF9
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2132T3Z4
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21296G14
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2132T3YW
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21314AAF
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2132T3YR
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21296FXW

		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2131T3ZA
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21296EF4
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2132T3Z3
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21314BP2
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2132T3ZC
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21319B19
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2132T3Z7
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21314AB9
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2132T3Z9
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21296GVV
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2131S3XT
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21312P82
2.6	Switch	WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FOC2110S32G
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21306WED
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FCW2110E1TB
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21314BC6
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FCW2110A4SZ
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21306SHS
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+, LAN Base	FOC2110S327
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21306VQC

		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FOC2110S31S
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21314AQJ
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FCW2110A4RM
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21306W9P
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FCW2110A4RZ
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21314AGZ
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+, LAN Base	FOC2110V1YS
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21314AEN
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FOC2110S309
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC213199K9
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FCW2110A4SJ
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21319TWZ
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FOC2110V1YJ
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21314AA4
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FCW2110A4T3
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21319BG7
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FOC2110S31J
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21306WEE
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FCW2110A4SQ
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21312PRC

		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FOC2110S302
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21312QMS
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FOC2110V1Z0
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21314BC9
		WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FCW2110A4S5
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC21319SGC
2.7	Switch	WS-C2960X-48LPS-L	Catalyst 2960-X 48 GigE PoE 370W, 4 x 1G SFP, LAN Base	FCW2109A5JX
		WS-C2960X-48LPS-L	Catalyst 2960-X 48 GigE PoE 370W, 4 x 1G SFP, LAN Base	FCW2109B5WW
2.8	Switch	WS-C2960X-24PD-L	Catalyst 2960-X 24 GigE PoE 370W, 2 x 10G SFP+, LAN Base	FOC2111S15K
		WS-C2960X-24PD-L	Catalyst 2960-X 24 GigE PoE 370W, 2 x 10G SFP+, LAN Base	FCW2111B0JQ
		WS-C2960X-24PD-L	Catalyst 2960-X 24 GigE PoE 370W, 2 x 10G SFP+, LAN Base	FCW2111E0A1
		WS-C2960X-24PD-L	Catalyst 2960-X 24 GigE PoE 370W, 2 x 10G SFP+, LAN Base	FCW2111E09Z
		WS-C2960X-24PD-L	Catalyst 2960-X 24 GigE PoE 370W, 2 x 10G SFP+, LAN Base	FOC2111S15L
2.9	Switch	WS-C2960X-24PS-L	Catalyst 2960-X 24 GigE PoE 370W, 4 x 1G SFP, LAN Base	FCW2110A489
		WS-C2960X-24PS-L	Catalyst 2960-X 24 GigE PoE 370W, 4 x 1G SFP, LAN Base	FCW2110A48V
		WS-C2960X-24PS-L	Catalyst 2960-X 24 GigE PoE 370W, 4 x 1G SFP, LAN Base	FCW2110A48H
		WS-C2960X-24PS-L	Catalyst 2960-X 24 GigE PoE 370W, 4 x 1G SFP, LAN Base	FCW2110A48C
		WS-C2960X-24PS-L	Catalyst 2960-X 24 GigE PoE 370W, 4 x 1G SFP, LAN Base	FCW2110A0Y6
2.10	SFP	SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DFP
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DSH
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21090WRZ
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21090WR8
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	OPM21290UZA

		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	OPM21290UZX
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	OPM21290UZN
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	OPM21290UZM
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091EG2
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091EGV
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091EH8
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091EGR
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091EH4
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CFV
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CGB
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CFT
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CHJ
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CGJ
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CH2
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CGX
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21090WT6
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DY4
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DW4
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DXY
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DXV
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DXP
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DEV
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091ELE
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21090WRN
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21090WTM
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CFX
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CGG
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CGL
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CHL
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CHU
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise Class	FNS21091CHV
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CHX
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091CJ1
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DA6
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DAW
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DCN
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DE6
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DEH
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091DF4
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091E16

		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091E1A
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091E1D
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091E1S
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091E2K
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091E37
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091EHC
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091EHZ
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091EK4
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	FNS21091EK7
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	OPM21290UXF
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	OPM21290UXG
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	OPM21290UXJ
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	OPM21290UXK
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	OPM21290UXL
		SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	OPM21290UZS
2.11	Switch	WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6G2
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6EP
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6DE
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6DB
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6J0
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6J7
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6F3
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6DZ
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6JN
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6GL
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6G1
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6JA
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6FP

		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6ES
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6G3
		WS-C2960X-24TS-L	Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base	FCW2110B6EC
2.12	WLC	AIR-CT5520-K9	Cisco 5520 Wireless Controller w/rack mounting kit	FCH2128V2U4
		C1-AIR-CT5520-K9	Cisco ONE - 5520 Wireless Controller w/rack mounting kit	FCH2131V0KU
2.13	AP	AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XA
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YY
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9X5
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9X8
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131AA8Z
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XU
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YG
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9X9
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YD
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9WH
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9X0
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9X7
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9WT
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9Z1
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XR

		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9ZB
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9Z9
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9X4
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9X6
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9WP
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9X3
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9ZC
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XG
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9X1
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XM
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9WG
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9WU
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9WJ
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9WB
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YB
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YX
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XS
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YN
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YR
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XQ

		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XL
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XT
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XD
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XB
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9WA
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9W7
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XH
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XE
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XC
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9WN
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9WW
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XP
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9ZA
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YS
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9Z5
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YC
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YU
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9Z2
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YF
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9Z6

		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YM
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9YT
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XK
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XJ
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XF
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9XN
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9X2
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9W9
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9WZ
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2131A9WK
2.14	Management System	R-MGMT3X-N-K9	Cisco Ent MGMT: Lic For PI 3.x And APIC EM Solution Apps	
2.15	Server	UCSC-C240-M4S	UCS C240 M4 SFF 8 HD w/o xpdr,CPU,mem,HD,PCIe,PS,railkt	FCH2204V180
2.16	Policy Management	R-ISE-VM-K9,L-ISE-TACACS	Cisco ISE Device Admin License	
2.22	Cabinet Rack	Rack 9U		
2.23	Switch	WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2344L414
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455NVB
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2344L40U
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455N9R
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2344L412
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455P5E

		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2344L40T
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455NZ1
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FOC2344L40C
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455N5P
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2344L3Z6
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455NFG
2.24	Switch	WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FOC2344L40Q
		WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	FOC2344L40J
2.25	Switch	WS-C2960X-48LPD-L	Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base	FOC2346L64P
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23456J57
2.26	Switch	WS-C3650-48TD-L	Cisco Catalyst 3650 48 Port Data 2x10G Uplink LAN Base	FDO2352M4GK
		C3650-STACK	Cisco Catalyst 3650 Stack Module	FDO23500Y60
		C3650-STACK	Cisco Catalyst 3650 Stack Module	FDO23500Y62
		WS-C3650-48TD-L	Cisco Catalyst 3650 48 Port Data 2x10G Uplink LAN Base	FDO2352M4B9
		C3650-STACK	Cisco Catalyst 3650 Stack Module	FDO23500X06
		C3650-STACK	Cisco Catalyst 3650 Stack Module	FDO235010CU
2.27	Switch	WS-C2960X-48TD-L	Catalyst 2960-X 48 GigE, 2 x 10G SFP+, LAN Base	FOC2347L1R1
		WS-C2960X-48TD-L	Catalyst 2960-X 48 GigE, 2 x 10G SFP+, LAN Base	FOC2347L1P9
2.28	Switch	WS-C2960X-48TS-L	Catalyst 2960-X 48 GigE, 4 x 1G SFP, LAN Base	FOC2351L2EF
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455N1H
		WS-C2960X-48TS-L	Catalyst 2960-X 48 GigE, 4 x 1G SFP, LAN Base	FOC2351L2EK
		C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455NVA

2.29	Stacking Module	C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23456J69
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455P6L
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455NHG
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455NS4
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455P6G
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455NDG
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455Q0F
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455N5R
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455NS3
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455PTB
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455N55
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455NDE
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455Q43
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455PB8
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455P76
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455N1V
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455MRG
		C2960X-STACK=	Catalyst 2960-X FlexStack Plus Stacking Module	FOC23455NUP
2.30	SFP	SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430T9H
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430U3Q
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430UR0
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430KL5
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430JHK

		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430T9J
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430SCR
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430U3W
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430T8Y
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430K9V
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430JNT
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430K3M
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430U7T
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430TVA
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430UGC
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430KLV
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430KLM
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430UFD
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430R58
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430T77
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430TR6
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430HSP
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430TXF
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430STE
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430URL
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430UMK
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430TJV
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430TJD
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430T05
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430UG9
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430K5W
		SFP-10G-SR=	10GBASE-SR SFP Module, Enterprise-Class	ACW23430HQJ
2.31		GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	ACW23490PRQ
		GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	ACW23490PRU
		GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	ACW23490PS5
		GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	ACW23490PS9
		GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	ACW23490PRP
		GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	ACW23490PRY
		GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	ACW23490PRW

		GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	ACW23490PS1
2.32	AP	AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQZ
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQW
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQJ
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQB
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQ0
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQK
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQN
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQH
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQR
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQS
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQM
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQQ
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQ1
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMPS
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMPX
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQC
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQ4
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMPT
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQ6

		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQ9
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQ8
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQU
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMQT
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMR3
		AIR-AP2802I-S-K9	802.11ac W2 AP w/CA; 4x4:3; Int Ant; 2xGbE S Domain	FGL2351LMPW
2.33	AP	C9120AXI-S		FGL2806L61G
		C9120AXI-S		FGL2806L61F
2.34			Wireless Access Point 4 ชุด	

ตารางแสดงวงเงินงบประมาณที่รับจัดสรรและรายละเอียดค่าใช้จ่ายการจ้างที่ปรึกษา

1. **ชื่อโครงการ** จัดจ้างที่ปรึกษาสำหรับการนำ Fund Transfer Pricing (FTP) มาใช้ในองค์กร
2. **หน่วยงานเจ้าของโครงการ** ฝ่ายบริหารเงิน
3. **วงเงินงบประมาณที่ได้รับจัดสรร** 10,000,000.00 บาท (สิบล้านบาทถ้วน)
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ 21 กค 2568

   เป็นเงิน 8,125,480.40 บาท (แปดล้านหนึ่งแสนสองหมื่นห้าพันสี่ร้อยแปดสิบบาทสี่สิบสตางค์)
5. **ค่าตอบแทนบุคลากร** 7,315,440.00 บาท

   5.1 ประเภทที่ปรึกษา กลุ่มวิชาชีพเฉพาะ (การเงิน)

   5.2 คุณสมบัติที่ปรึกษา

5.2.1 ผู้จัดการโครงการ	ไม่ต่ำกว่าวุฒิปริญญาโท	มีประสบการณ์ในการทำงานไม่น้อยกว่า 15 ปี มีประสบการณ์ในการบริหารโครงการไม่น้อยกว่า 10 ปี มีประสบการณ์การทำงานเกี่ยวข้องกับ FTP ไม่น้อยกว่า 10 ปี
5.2.2 ผู้เชี่ยวชาญ	ไม่ต่ำกว่าวุฒิปริญญาโท	มีประสบการณ์ในการทำงานไม่น้อยกว่า 10 ปี มีประสบการณ์การทำงานเกี่ยวข้องกับ FTP ไม่น้อยกว่า 10 ปี
5.2.3 ทีมงาน	ไม่ต่ำกว่าวุฒิปริญญาโท	มีประสบการณ์ในการทำงานไม่น้อยกว่า 5 ปี มีประสบการณ์การทำงานเกี่ยวข้องกับ FTP หรือ การบริหารสินทรัพย์และหนี้สิน (ALM) ไม่น้อยกว่า 3 ปี
5.2.4 ทีมงาน	ไม่ต่ำกว่าวุฒิปริญญาตรี	มีประสบการณ์ในการทำงานไม่น้อยกว่า 5 ปี ประสบการณ์การทำงานเกี่ยวข้องกับ FTP หรือ การบริหารสินทรัพย์และหนี้สิน (ALM) หรือการเงิน หรือการบัญชีการธนาคาร ไม่น้อยกว่า 1 ปี

   5.3 จำนวนที่ปรึกษา

   5.3.1 ผู้จัดการโครงการ ไม่น้อยกว่า 1 คน
   5.3.2 ผู้เชี่ยวชาญ ไม่น้อยกว่า 1 คน
   5.3.3 ทีมงาน ไม่น้อยกว่า 4 คน
6. **ค่าวัสดุอุปกรณ์** 112,500.00 บาท
7. **ค่าใช้จ่ายในการเดินทางไปต่างประเทศ (ถ้ามี)** -
8. **ค่าใช้จ่ายอื่นๆ** 697,540.40 บาท
9. **รายชื่อผู้รับผิดชอบกำหนดราคากลาง**

   9.1 นางชลิสา ดานุสวัสดิ์ ผู้ช่วยผู้บริหารฝ่ายบริหารเงิน
   9.2 นายรชตพงศ สุขสงวน ผู้บริหารฝ่ายกลยุทธ์องค์กร
   9.3 นายเดชา ปริญญาสุข รักษาการผู้บริหารฝ่ายจัดซื้อและธุรการ
10. **ที่มาของการกำหนดราคากลาง (ราคาอ้างอิง)**

    10.1 ตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) 0405.3/ว 1203 ลงวันที่ 27 กันยายน 2565

    10.2 ค่าใช้จ่ายตรง ใช้ราคาที่ได้มาจากการสืบราคาจากท้องตลาด จำนวน 4 ราย

    10.2.1 บริษัท เคพีเอ็มจี ภูมิไชย ที่ปรึกษาธุรกิจ จำกัด
    10.2.2 บริษัท ดีลอยท์ แพลนเนอร์ จำกัด
    10.2.3 บริษัท อีวาย คอร์ปอเรท เซอร์วิสเซส จำกัด
    10.2.4 บริษัท ไพร้ซวอเตอร์เฮาส์คูเปอร์ส เอบีเอเอส จำกัด

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างที่ปรึกษาสำหรับการนำ Fund Transfer Pricing (FTP) มาใช้ในองค์กร

ผู้เสนอราคาต้องเสนอการให้คำปรึกษาสำหรับการนำ Fund Transfer Pricing (FTP) มาใช้ในองค์กร โดยครอบคลุมตามขอบเขตงานที่ธนาคารกำหนดอย่างน้อยดังต่อไปนี้

1. จัดทำแผนการดำเนินงานโครงการและแผนรองรับการปฏิบัติงานในสถานการณ์ที่ไม่ปกติ และภายใต้ข้อจำกัดต่างๆ ที่อาจเกิดขึ้นจากสถานการณ์ที่ไม่ปกติดังกล่าว เช่น การเกิดโรคระบาดร้ายแรง การเกิดภัยพิบัติทางธรรมชาติ การเกิดเหตุการจลาจล เป็นต้น
2. ศึกษาโครงสร้างการบริหารจัดการ การกำกับดูแล ด้านการบริหารสินทรัพย์และหนี้สิน และการจัดสรรต้นทุนของธนาคาร ตลอดจนบทบาท ภาระหน้าที่ และความรับผิดชอบ ของหน่วยงานที่สนับสนุนการบริหารสินทรัพย์และหนี้สิน และการจัดสรรต้นทุนของธนาคารในปัจจุบัน เพื่อวิเคราะห์ความแตกต่าง (Gap Analysis) ระหว่างวิธีการบริหารจัดการ การกำกับดูแล วิธีการจัดสรรต้นทุนของธนาคารในปัจจุบันกับแนวปฏิบัติที่ดี (Best Practice) เพื่อประเมินความพร้อมในการนำ FTP มาใช้ในองค์กร
3. ประเมินผลกระทบของการนำ FTP มาใช้ในองค์กรต่อโครงสร้าง กระบวนการทำงาน ความพร้อมของข้อมูล ระบบงาน และเครื่องมือในการกำหนดราคาโอน/การจัดสรรต้นทุน
4. นำเสนอวิธีการ/แนวทางการจัดทำ FTP ที่เหมาะสมกับธนาคาร โดยเปรียบเทียบกับวิธีปฏิบัติทั่วไปในอุตสาหกรรม พร้อมจัดทำแบบจำลอง (FTP Model) ที่ครอบคลุมการสร้างเส้นราคาโอน (FTP Curve) และเครื่องมือรองรับการคำนวณตามแบบจำลองที่นำเสนอ (Pilot FTP Model) ซึ่งสามารถแสดงตัวอย่างการคำนวณอัตราราคาโอน (FTP Rate) สำหรับแต่ละกลุ่มผลิตภัณฑ์หรือธุรกรรมที่เกี่ยวข้องของธนาคาร ให้ธนาคารภายในระยะเวลา 6 เดือน นับถัดจากวันที่ลงนามในสัญญา
5. นำเสนอกรอบการวิเคราะห์กำไรในแต่ละระดับ เช่น ระดับสาขา หน่วยธุรกิจ ผลิตภัณฑ์ และประเภทลูกค้า รวมถึงการเสนอแนะผลกระทบต่อการปันส่วนต้นทุนและค่าใช้จ่ายในการดำเนินงานของธนาคาร
6. ทดสอบการใช้งาน FTP Model และ Pilot FTP Model เพื่อทดสอบความถูกต้อง ความเหมาะสมของโมเดล และประเมินผลลัพธ์ พร้อมให้คำปรึกษาและคำแนะนำทางเทคนิคเกี่ยวกับการคำนวณ FTP และวิธีการใช้โมเดล รวมถึงนำเสนอวิธีการแก้ไขปัญหาที่อาจพบในการนำมาปฏิบัติใช้จริง
7. จัดอบรมเพื่อให้ความรู้ความเข้าใจแก่ผู้บริหารและพนักงาน พร้อมจัดทำเอกสารประกอบการอบรม จำนวนอย่างน้อย 3 ครั้ง ดังนี้
   7.1 อบรมความรู้พื้นฐานเกี่ยวกับ FTP เพื่อสร้างการตระหนักรู้ให้กับพนักงานของธนาคาร
   7.2 อบรมเชิงลึกเกี่ยวกับ FTP Model ให้กับฝ่ายงานที่เกี่ยวข้อง ได้แก่ ฝ่ายบริหารเงิน ฝ่ายกลยุทธ์องค์กร ฝ่ายงานด้านการตลาด ฝ่ายบัญชี ฝ่ายบริหารความเสี่ยงองค์กร ฝ่ายบริหารความเสี่ยงด้านเครดิต ฝ่ายพัฒนาผลิตภัณฑ์
   7.3 อบรมขั้นตอนการใช้งาน Pilot FTP Model ให้กับฝ่ายงานที่เกี่ยวข้อง ได้แก่ ฝ่ายบริหารเงิน ฝ่ายกลยุทธ์องค์กร ฝ่ายงานด้านการตลาด ฝ่ายบัญชี ฝ่ายบริหารความเสี่ยงองค์กร ฝ่ายบริหารความเสี่ยงด้านเครดิต ฝ่ายพัฒนาผลิตภัณฑ์
8. ให้การสนับสนุน/คำปรึกษาเกี่ยวกับการใช้งาน FTP Model และ Pilot FTP Model เป็นระยะเวลา 3 เดือน หลังจากส่งมอบ FTP Model และ Pilot FTP Model และผ่านการตรวจรับงานจากธนาคารเป็นที่เรียบร้อยแล้ว เช่น ให้คำแนะนำในการแก้ไขปัญหา ปรับปรุงโมเดล เป็นต้น พร้อมจัดทำรายงานสรุปการให้การสนับสนุน/คำปรึกษา

9. นำเสนอแนวทางการกำกับดูแล FTP โดยจัดทำนโยบายและคู่มือการดำเนินการ FTP ที่ครอบคลุมทั้งกระบวนการทำงาน ความรับผิดชอบของฝ่ายงานต่างๆที่เกี่ยวข้อง และข้อกำหนดต่างๆ
10. นำเสนอแนวทางในการพัฒนา/จัดหาระบบ FTP ที่เหมาะสมกับธนาคาร พร้อมทั้งเปรียบเทียบข้อดีข้อเสีย พร้อมจัดทำร่างขอบเขตความต้องการ เพื่อให้ธนาคารนำไปใช้ประโยชน์ในการพัฒนา/จัดหาระบบ FTP
11. ให้การสนับสนุนข้อมูลและนำเสนอผลสรุปการประเมินความพร้อมของธนาคารและแนวทางการนำ FTP Model ที่เหมาะสมในการนำ Fund Transfer Pricing (FTP) มาใช้ในองค์กรต่อคณะทำงานหรือคณะกรรมการที่เกี่ยวข้อง

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ การเช่าระบบสำรองข้อมูล Backup as a Service
2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
3. วงเงินงบประมาณที่ได้รับจัดสรร 2,163,400.00 (สองล้านหนึ่งแสนหกหมื่นสามพันสี่ร้อยบาทถ้วน)
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) /วันที่ 17 ก.ค. 2568
   เป็นเงิน ทั้งสิ้น 2,136,400.00 บาท (สองล้านหนึ่งแสนสามหมื่นหกพันสี่ร้อยบาทถ้วน)
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   บริษัท เมโทรซิสเต็มส์คอร์ปอเรชั่น จำกัด (มหาชน)
6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายจรัส	ขวัญพิเชษฐ์สกุล	ผู้บริหารส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.2 นางสาวศรัญญา	แวงวรรณ์	ผู้บริหารส่วนจัดซื้อเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.3 นางสาววิลาสินี	คำเพ็ง	ผู้ช่วยผู้บริหารส่วนบริหารจัดการโครงสร้างพื้นฐานและระบบเครือข่าย /ฝ่าย จธ.

ผนวก 1
ขอบเขตการดำเนินงาน
การเช่าระบบสำรองข้อมูล Backup as a Service

---

1. ข้อกำหนดขั้นต่ำด้านเทคนิค/ขอบเขตการดำเนินงาน

1.1 คุณลักษณะขั้นต่ำของเครื่องคอมพิวเตอร์แม่ข่าย Backup Server จำนวน 2 เครื่อง โดยมีรายละเอียดดังนี้

1.1.1 ยี่ห้อ Huawei รุ่น 2288H Serial No. 2102311XBHP0L3000004

1.1.2 ยี่ห้อ Huawei รุ่น 2288H Serial No. 2102311XBHP0L3000005

- มีหน่วยประมวลผลกลาง (CPU) แบบ 64-bit มีความเร็ว (Clock Speed)ไม่น้อยกว่า 2.2 GHz มีจำนวนแกนหลัก (Core) ไม่น้อยกว่า 10 แกน มีจำนวนไม่น้อยกว่า 1 หน่วย
- มีหน่วยความจำหลัก (Main Memory) ชนิด DDR4 หรือดีกว่า ความเร็วไม่น้อยกว่า 2933 MHz ขนาดรวมไม่น้อยกว่า 64 GB
- มีหน่วยเก็บข้อมูล (Hard disk) แบบ Solid State Drive(SSD) หรือดีกว่า และมีความจุไม่น้อยกว่า 900 GB จำนวน 2 หน่วย และรองรับการเปลี่ยน แบบ Hot-swap
- มีระบบควบคุมการจัดเก็บข้อมูล (Controller) แบบ SAS / SATA หรือดีกว่า ซึ่งสนับสนุนการทำ RAID 0,1,5 ได้ โดยมีหน่วยความจำไม่น้อยกว่า 2 GB
- มี DVD-ROM Drive หรือดีกว่า จำนวนอย่างน้อย 1 หน่วย
- มี Network Interface แบบ 1 Gigabit Ethernet หรือดีกว่า จำนวนพอร์ตรวมไม่น้อยกว่า 2 พอร์ต
- มี Network Interface แบบ 10 Gigabit Ethernet Base-T หรือดีกว่า จำนวนพอร์ตรวมไม่น้อยกว่า 2 พอร์ต
- มี HBA (Host Bus Adapter) ชนิด Fiber Channel หรือดีกว่า ที่สามารถรับ-ส่ง ข้อมูลที่ความเร็วไม่น้อยกว่า 16 Gbps จำนวน รวมไม่น้อยกว่า 2 พอร์ต สำหรับเชื่อมต่อกับ SAN Switch
- มี Power Supplies ขนาดไม่น้อยกว่า 770 Watts จำนวนไม่น้อยกว่า 2 หน่วย และรองรับการถอดเปลี่ยนแบบ Hot Plug หรือ Hot Swap ได้
- รองรับการทำงานร่วมกับ Windows 2012R2 Server (64-bit) / Windows Server 2016/ Window Server 2019 , Red Hat Enterprise Linux, SUSE Linux Enterprise Server, หรือ VMware ได้
- สามารถติดตั้งบน Rack มาตรฐาน 19 นิ้ว พร้อมอุปกรณ์

1.2 คุณลักษณะขั้นต่ำของอุปกรณ์สำรองข้อมูล (Backup Storage) จำนวน 1 หน่วย พื้นที่สำหรับใช้งานไม่น้อยกว่า 210 TB โดยมีรายละเอียดดังนี้

1.2.1 ยี่ห้อ Huawei รุ่น Oceanstore 2200 Serial No. 2102350SHW10L2000014

- เป็นอุปกรณ์ที่ทำหน้าที่จัดเก็บข้อมูลภายนอกแบบ SAN มี 10 Gigabit Ethernet Base-T หรือ 10 Gigabit SFP+ จำนวนไม่น้อยกว่า 2 พอร์ต
- มี Controller จำนวนไม่น้อยกว่า 2 หน่วย
- มีช่องสัญญาน Host Interface แบบ FC ความเร็วไม่น้อยกว่า 16 Gbps มีจำนวนไม่น้อยกว่า 2 ช่อง ต่อ 1 หน่วย Controller

- รองรับการเชื่อมต่อแบบ Fiber Channel หรือ ISCSI
- มีการทำงานของ Harddisk แบบ RAID เพื่อป้องกันการเสียหายของ Harddisk
- สามารถเปลี่ยน Hard Drive ที่เสียได้ โดยไม่ต้องหยุดการทำงานของระบบ (Hot Plug)
- มีหน่วยจัดเก็บข้อมูล (Hard Drive) ชนิด NL-SAS มีความเร็วรอบไม่น้อยกว่า 7,200 rpm ต่อลูก และมีขนาดความจุรวมกันแล้วไม่น้อยกว่า 210 TB (หลังการทำ RAID)
- สามารถบริหารจัดการจากศูนย์กลางผ่านทาง Web Browse หรือ Agent
- มี Power Supplies จำนวนไม่น้อยกว่า 2 หน่วย และรองรับการถอดเปลี่ยนแบบ Hot Plug หรือ Hot Swap ได้
- สามารถติดตั้งบน Rack มาตรฐาน 19 นิ้ว พร้อมอุปกรณ์

1.3 คุณลักษณะขั้นต่ำของเทปสำรองข้อมูล (Tape Library) จำนวน 2 หน่วย โดยมีรายละเอียดดังนี้

1.3.1 ยี่ห้อ HPE รุ่น MSL3040 Serial No. DEC00204KU

1.3.2 ยี่ห้อ HPE รุ่น MSL3040 Serial No. DEC00204KR

- LTO: รองรับเทคโนโลยี LTO-9, LTO-8, LTO-7, และ LTO-6
- Drive Interface: 8 Gb/sec Fibre Channel
- จำนวนไดรฟ์: สูงสุด 48 ไดรฟ์ Half Height
- สามารถติดตั้งบน Rack มาตรฐาน 19 นิ้ว พร้อมอุปกรณ์

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

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 ต้องจัดทำรายงานสรุปรายละเอียดของระบบสำรองข้อมูลและอุปกรณ์ที่ใช้สำรองข้อมูลทั้งหมดส่งให้ธนาคารนำส่งแต่ละรายเดือน ทุกๆ วันสิ้นเดือน

2.2 ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการแก้ไขปัญหาให้แล้วเสร็จภายในกำหนดระยะเวลา ตามระดับผลกระทบที่มีต่อธุรกิจ หรือ การทำงาน (Severity) ซึ่งให้เป็นไปตามดุลยพินิจของธนาคาร ดังนี้

ระดับผลกระทบ (Severity)	ระยะเวลาติดต่อกลับ	ระยะเวลาการแก้ไขปัญหาเสร็จสิ้น นับจากที่ได้รับแจ้ง
ปัญหาเร่งด่วน ธนาคารไม่สามารถใช้ระบบได้	30 นาที	4 ชั่วโมง
ปัญหาสำคัญ ระบบทำงานผิดพลาดในเรื่องสำคัญ หรือใช้งานได้บางส่วน	2 ชั่วโมง	24 ชั่วโมง
ปัญหาไม่เร่งด่วน ระบบทำงานผิดพลาดแบบไม่มีสาระสำคัญ	4 ชั่วโมง	72 ชั่วโมง

2.3 ต้องนำส่งรายละเอียดและขั้นตอนการแก้ไขปัญหา เหตุขัดข้อง และ/หรือความชำรุดบกพร่องของระบบสำรองข้อมูล อย่างละเอียดให้แก่ธนาคารในทันทีที่สามารถดำเนินการได้ และผู้ให้บริการตกลงเป็นผู้รับผิดชอบชำระค่าใช้จ่ายที่เกิดขึ้นจากการเข้าดำเนินการทั้งจำนวน

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

2.5 จัดให้มีเจ้าหน้าที่เข้า "ตรวจสอบและบำรุงรักษา (Preventive Maintenance: PM)" ไม่น้อยกว่า 4 ครั้ง/ปี พร้อมทั้งจัดทำรายละเอียดและขั้นตอนการตรวจเช็ครวมทั้งข้อเสนอแนะที่เป็นประโยชน์ต่อธนาคารเป็นลายลักษณ์อักษรทุกครั้งที่ให้บริการ และนำส่งรายงานผลการตรวจสอบและบำรุงรักษา

(Preventive Maintenance: PM) ภายในวันที่ 12 ของเดือนถัดไป นับถัดจากเดือนที่ดำเนินการตรวจสอบและบำรุงรักษาระบบงานในแต่ละรอบการให้บริการ โดยผู้ให้บริการจะต้องแจ้งกำหนดวันเวลาแน่นอน ก่อนการเข้ามาให้บริการล่วงหน้าไม่น้อยกว่า 1 วันทำการ ดังนี้

ครั้งที่ 1 ภายในเดือนตุลาคม 2568 ครั้งที่ 2 ภายในเดือนมกราคม 2569
ครั้งที่ 3 ภายในเดือนเมษายน 2569 ครั้งที่ 4 ภายในเดือนกรกฎาคม 2569

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

2.6.1 ระดับ High แก้ไขปิดช่องโหว่ภายใน 5 วัน นับจากได้รับแจ้งจากธนาคาร

2.6.2 ระดับ Medium แก้ไขปิดช่องโหว่ภายใน 10 วัน นับจากได้รับแจ้งจากธนาคาร

2.6.3 ระดับ Low หรือ อื่นๆ ภายใน 30 วัน นับจากได้รับแจ้งจากธนาคาร

3. การสิ้นสุดสัญญาและการบอกเลิกสัญญา

3.1 ในกรณีอุปกรณ์เช่าใช้ดังกล่าวสิ้นอายุสัญญา เนื่องจากธนาคารไม่ได้มีการต่ออายุของสัญญาและอยู่ระหว่างดำเนินการตรวจสอบและจัดเก็บข้อมูลที่เกี่ยวข้องกับอุปกรณ์ดังกล่าว เพื่อให้การดำเนินงานเป็นไปอย่างเรียบร้อยและสมบูรณ์ ผู้ให้บริการต้องยินยอมให้ธนาคารเก็บอุปกรณ์ดังกล่าวไว้เป็นระยะเวลา 60 วัน นับจากวันที่หมดอายุสัญญา ทั้งนี้เพื่อประโยชน์ในการตรวจสอบ ติดตาม หรือดำเนินการอื่นใดที่จำเป็น โดยผู้ให้บริการตกลงจะเข้ามารับอุปกรณ์ ที่สำนักงานใหญ่ ที่ให้บริการคืนจากธนาคาร ในสภาพที่เป็นอยู่ ณ ขณะนั้น รวมทั้งกรณีที่เกิดการชำรุดหรือเสื่อมสภาพอันเนื่องมาจากการใช้งานใดๆ และต้องปรับสภาพพื้นที่ให้พร้อมใช้งานให้แล้วเสร็จเมื่อสิ้นสุดระยะเวลาดังกล่าว โดยไม่มีค่าใช้จ่ายเพิ่มเติม

3.2 เมื่อครบกำหนดการติดตั้งและส่งมอบอุปกรณ์ตามสัญญา แล้วปรากฏว่าผู้ขายไม่สามารถปฏิบัติตามข้อกำหนดตามที่เสนอในโครงการ ธนาคารมีสิทธิ์บอกเลิกสัญญาทั้งหมดหรือบางส่วนได้ โดยไม่มีค่าใช้จ่ายเพิ่มเติม

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างจัดทำของที่ระลึกสำหรับพนักงานเกษียณอายุการทำงานประจำปี 2568**
/หน่วยงานเจ้าของโครงการ **ฝ่ายทรัพยากรบุคคล**

2. วงเงินงบประมาณที่ได้รับจัดสรร 850,000.00 บาท **(แปดแสนห้าหมื่นบาทถ้วน)**

3. วันที่กำหนดราคากลาง (ราคาอ้างอิง) .....
เป็นเงิน 789,802.00 บาท (เจ็ดแสนแปดหมื่นเก้าพันแปดร้อยสองบาทถ้วน)

4. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
ใช้ราคาที่สืบจากผู้ให้บริการ จำนวน 3 ราย
4.1 บริษัท วัชรินทรโกลด์ จำกัด (สำนักงานใหญ่)
4.2 บริษัท ค้าทองโชวเซ่งเฮง จำกัด
4.3 บริษัท ชายนิ่ง โกลด์ จำกัด

5. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

5.1	นางสาว เสาวนีย์ ธารีพุฒ	ผู้ช่วยผู้บริหารส่วน HR Shared Service 2 ฝ่ายทรัพยากรบุคคล
5.2	นางสาว ณัฐธยาน์ บวรพงษ์สกุล	ผู้ช่วยผู้บริหารส่วน HR Strategic and Execution ฝ่ายทรัพยากรบุคคล
5.3	นางสาว พิชามญชุ์ โต๊ะชื่นดี	พนักงานบุคคลส่วน HR Strategic and Execution ฝ่ายทรัพยากรบุคคล

รายละเอียดและขอบเขตงาน
การจ้างจัดทำของที่ระลึกสำหรับพนักงานเกษียณอายุการทำงานประจำปี 2568

---

1. ข้อกำหนดและขอบเขตของงาน

ผู้เสนอราคาต้องเสนอจ้างจัดทำของที่ระลึกทำด้วยแผ่นทองคำเพื่อมอบให้แก่พนักงานเกษียณอายุการทำงานประจำปี 2568 ตามรายละเอียดและขอบเขตงานที่ธนาคารกำหนด ดังนี้

รูปแบบและรายละเอียดการจัดทำ

1. แผ่นทองคำ	: ค่าความบริสุทธิ์ไม่ต่ำกว่า 96.5% น้ำหนัก 25 กรัม
2. จำนวน	: 8 ชิ้น
3. รูปทรง	: สี่เหลี่ยมผืนผ้า
4. ด้านหน้า	: ขอบพ่นทราย
	: พื้นเรียบ
	: มีโลโก้ธนาคารนูนเงาและข้อความที่ระลึกเกษียณอายุการทำงาน ตรงกลางแผ่นทอง (ธนาคารเป็นผู้จัดหา Block ในการจัดทำ)
5. ด้านหลัง	: พื้นเรียบ
	: ระบุชื่อร้าน/ โลโก้ร้าน น้ำหนักทอง และค่าความบริสุทธิ์
6. บรรจุภัณฑ์	: กล่องกำมะหยี่ สีแดงแบบเจาะช่อง (1 ชิ้น/กล่อง)
7. เอกสารการรับประกันคุณภาพ	: ระบุน้ำหนักทอง ค่าความบริสุทธิ์ ชื่อร้าน/โลโก้ร้าน และช่องทางการติดต่อโดยใส่ในกล่องบรรจุภัณฑ์ กล่องละ 1 ฉบับ

ข้อความบนแผ่นทอง (ด้านหน้า)

2. การส่งมอบงาน

2.1 ต้องส่งมอบแผ่นทองคำที่ระลึกเกษียณประจำปี 2568 ตามแบบที่ระบุในเอกสารแนบท้าย 1.1 (ข้อ 1) ที่ตกลงว่าจ้างได้อย่างถูกต้องครบถ้วนทั้งหมด ณ ที่ทำการสำนักงานใหญ่ของธนาคารภายใน 30 วันนับถัดจากวันลงนามในสัญญาจ้าง

2.2 หากธนาคารตรวจสอบแล้วพบว่าแผ่นทองคำที่ระลึกเกษียณประจำปี 2568 ที่ส่งมอบไม่ตรงตามแบบที่ระบุในเอกสารแนบท้าย 1.1 ที่ธนาคารตกลงว่าจ้างประการหนึ่งประการใด ธนาคารสงวนสิทธิ์ที่จะไม่รับมอบทั้งหมด หรือเพียงบางส่วน หรือให้ผู้รับจ้างดำเนินการเปลี่ยนแปลง และ/หรือปรับปรุง แก้ไขให้ถูกต้อง ตามคำชี้ขาดของธนาคารด้วยค่าใช้จ่ายของผู้รับจ้างเองทั้งสิ้น ทั้งนี้ระยะเวลาที่เสียไปเพราะเหตุดังกล่าว ไม่เป็นเหตุให้ผู้รับจ้างมีสิทธิขยายระยะเวลาการส่งมอบเกินกำหนดเวลาที่ระบุในใบสั่งจ้าง หรือ ขอยกเว้นหรือ ลดค่าปรับได้

3. การชำระเงิน

ธนาคารจะจ่ายเงินค่าจ้างซึ่งรวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงแล้วให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้รับจ้าง ภายในระยะเวลา 7 วันทำการ นับจากวันที่ส่งมอบแผ่นทองคำที่ระลึกเกษียณประจำปี 2568 ถูกต้อง ครบถ้วน ตามข้อกำหนด (ผนวก 1) และผ่านการตรวจรับจากคณะกรรมการตรวจรับของธนาคารเป็นที่เรียบร้อยแล้ว

4. ข้อกำหนดอื่นๆ

4.1 ธนาคารเป็นผู้ทรงสิทธิ์ในรูปแบบของแผ่นทองคำที่ระลึกเกษียณประจำปี 2568 ที่ธนาคารคัดเลือกแล้ว และห้ามบุคคลหรือนิติบุคคลทำซ้ำ ดัดแปลง เผยแพร่ ให้เช่า ขาย มีไว้เพื่อขาย หรือทำการอื่นใดอันเป็นการละเมิดสิทธิ์โดยตรงหรือโดยอ้อม โดยไม่ได้รับอนุญาตจากธนาคาร

4.2 กรณีมีความจำเป็นที่ธนาคารต้องงดการดำเนินการไม่ว่าขั้นตอนใดๆ อันเนื่องมาจากการแพร่ระบาดของโรคติดต่ออันตราย หรือสถานการณ์หนึ่งสถานการณ์ใดที่เป็นอุปสรรคหรือความเสี่ยงต่อการมาปฏิบัติงานของพนักงานธนาคาร ธนาคารขอสงวนสิทธิ์ในการเปลี่ยนแปลงระยะเวลาดำเนินการหรือยกเลิกการจัดซื้อจัดจ้าง หรือบอกเลิกการสั่งซื้อสั่งจ้าง

4.3 ผู้เสนอราคาที่ได้รับการคัดเลือกจะต้องดำเนินงานให้สอดคล้องเป็นไปตามกฎหมาย รวมถึงหลักเกณฑ์ภายในธนาคารที่เกี่ยวข้อง เพื่อให้การดำเนินงาน ไม่ขัดหรือแย้งต่อกฎหมายและหลักเกณฑ์ภายใน

4.4 ผู้เสนอราคาที่ได้รับการคัดเลือกต้องใช้พัสดุประเภทวัสดุหรือครุภัณฑ์ที่จะใช้ในงานจ้างเป็นพัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานทั้งหมดตามสัญญา

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การเช่าศูนย์สำรองระบบคอมพิวเตอร์ ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉิน**

2. หน่วยงานเจ้าของโครงการ **ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ**

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

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 9 ก.ค. 2568
   เป็นเงิน **3,696,000.00 บาท (สามล้านหกแสนเก้าหมื่นหกพันบาทถ้วน)**

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   บริษัท ดาต้าโปร คอมพิวเตอร์ ซิสเต็มส์ จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายฉัตรชัย	อาศรมเงิน	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่ายปส.
6.2 นางสาวศรัญญา	แวงวรรณ์	ผู้บริหารส่วนจัดซื้อเทคโนโลยีสารสนเทศ / ฝ่ายจธ.
6.3 นายพงษ์เทพ	เลขะกุล	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่ายปส.

ผนวก 1

ขอบเขตการดำเนินงาน

การเช่าศูนย์สำรองระบบคอมพิวเตอร์ ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉิน

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 (ถ้ามี)** ซึ่งผู้ยื่นข้อเสนอเห็นว่ามีความจำเป็นหรือเป็นประโยชน์ต่อการให้บริการ

ทั้งนี้ ผู้ยื่นข้อเสนอต้องแจ้งรายละเอียดเกี่ยวกับชื่อ ที่อยู่ วุฒิการศึกษา ตำแหน่งงาน และประสบการณ์ของบุคลากรดังกล่าวข้างต้นให้ธนาคารทราบก่อนวันที่เริ่มต้นการให้บริการ รวมทั้งแจ้งให้ธนาคารทราบทุกครั้งโดยเร็วเมื่อมีการเปลี่ยนแปลง

4. ระยะเวลาการให้บริการ

ผู้ยื่นข้อเสนอต้องให้บริการเช่าศูนย์สำรองระบบคอมพิวเตอร์ ตามแผนกอบกู้ธุรกิจกรณีเกิดเหตุฉุกเฉิน ตามขอบเขตการดำเนินงานที่ระบุไว้ในผนวก 1 มีกำหนดระยะเวลา 1 ปี ตั้งแต่วันที่ 25 กรกฎาคม 2568 ถึง 24 กรกฎาคม 2569

5. การให้บริการตามแผนการกู้คืนระบบคอมพิวเตอร์ Disaster Recovery Action Plan (DRP) เมื่อธนาคารเกิดเหตุฉุกเฉิน

5.1 เมื่อธนาคารเกิดเหตุฉุกเฉิน ผู้ยื่นข้อเสนอจะต้องดำเนินการให้ธนาคารสามารถใช้บริการศูนย์สำรองระบบคอมพิวเตอร์ ตามเวลาที่ธนาคารกำหนดแต่ทั้งนี้ไม่เกิน 30 วันติดต่อกันต่อการเกิดเหตุฉุกเฉินแต่ละคราวโดยไม่จำกัดจำนวนคราว

5.2 ในกรณีที่ธนาคารจำเป็นต้องใช้ศูนย์สำรองติดต่อกันเกินกว่าระยะเวลาที่ได้ตกลงร่วมกัน เมื่อธนาคารได้แจ้งผู้ให้ยื่นข้อเสนอทราบล่วงหน้าก่อนสิ้นสุดระยะเวลาดังกล่าว ผู้ยื่นข้อเสนอจะต้องให้ธนาคารใช้ศูนย์สำรองต่อไปได้ ไม่เกิน 180 วัน โดยผู้ยื่นข้อเสนอมีสิทธิคิดค่าใช้จ่ายจากธนาคารตามจำนวนวันที่ใช้บริการในส่วนที่เกินกว่าระยะเวลาที่ได้ตกลงร่วมกันเป็นรายวันตามอัตราที่ผู้ยื่นข้อเสนอ เสนอต่อธนาคาร

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

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 จำนวน 1 เครื่อง**

11.1 เป็นเครื่องคอมพิวเตอร์แม่ข่ายฯ แบบติดตั้งบน Rack มาตรฐาน

11.2 มีหน่วยประมวลผลกลางแบบ Intel Xeon-Silver 4116 (2.1GHz / 12-core) อย่างน้อย จำนวน 2 หน่วย

11.3 มีหน่วยความจำหลัก (RAM) ไม่น้อยกว่า 322 GB.

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

11.5 มี Network Port แบบ 1 Gigabit Ethernet จำนวนไม่น้อยกว่า 4 Port

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

11.7 มีระบบปฏิบัติการ VMware vSphere standard edition พร้อมลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย

11.8 รองรับ VM ได้ดังนี้

Item	Server Name	Operating System	Hardware Spec		
			vCPU (Core)	Memory (GB)	Disk (GB)
1	Zigma	Win 2012 R2 Std	2	8	80
2	KTLEAPPPRD	Win 2019	4	16	300
3	DTS-APP-PRD	Red Hat 7	2	20	320
4	GL_DB1_PRD-N	Win 2012 R2 Std	4	10	790
5	GL_APP1_PRD	Win 2012 R2 Std	16	8	150
6	GLINFWEBPRD	Win 2016	4	16	110
7	GL_APP1_PRD-N	Win 2012 R2 Std	4	8	150
8	Web-Portal_APP_PRD	Win 2003 Ent. R2 SP2	12	16	115
9	STMT4DAP1	Win 2022	4	8	100
10	MY_APP_PRD	Win 2008 Std R2	8	8	100
11	SpoolAllBackup_PRD	Win 2008	16	8	400
12	CIRFAPPPRD	Red Hat 7	8	32	500
13	APIWEBWSPRD	Win 2019	4	16	160
14	MYWEBPRD	Win 2019	6	8	160
15	MYDBPRD	Win 2019	4	8	120
16	SFS-APP-PRD	Win 2019	2	4	460
17	Oper_EOD_2024	Win 2019	4	8	500
18	NTP-Production-DR	Oracle Solaris 10 - Linux	8	8	110
19	SKLMServerPRD	Win 2016	4	16	80
20	ESVOBPRD	Win 2016	4	16	320
21	e-servicesapp1PRD	Win 2016 & SQL Express	8	32	180
22	e-servicesapp2PRD	Win 2016 & SQL Express	4	32	860
23	MailAPPRD	Red Hat Enterprise Linux 8	2	8	60
24	SDRSTDDP1	Win 2022	4	8	250

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 เป็นอุปกรณ์ Firewall Appliance โดยมี Firewall throughput ไม่น้อยกว่า 55 Gbps และมี NGFW throughput ไม่น้อยกว่า 18.6 Gbps

17.2 อุปกรณ์มี Threat Prevention throughput ไม่น้อยกว่า 4.95 Gbps และมี IPS throughput ไม่น้อยกว่า 25.7 Gbps

17.3 อุปกรณ์สามารถรองรับ Concurrent Connections ได้อย่างน้อย 7,270,000 Connections และมี Connections per second ไม่น้อยกว่า 190,000 ต่อวินาที

17.4 อุปกรณ์สามารถรองรับ VPN throughput ไม่น้อยกว่า 22.1 Gbps

17.5 อุปกรณ์มี Network Interface แบบ RJ45 โดยมีความเร็ว 1 GbE หรือดีกว่า จำนวนไม่น้อยกว่า 8 พอร์ต

17.6 อุปกรณ์มี Storage บนตัวอุปกรณ์ ขนาดไม่น้อยกว่า 480 GB SSD

17.7 อุปกรณ์ต้องมี Memory อย่างน้อย 32 GB

17.8 มีแหล่งจ่ายไฟจำนวนไม่น้อยกว่า 2 หน่วย

17.9 สามารถใช้งาน Routing Static route และแบบ Dynamic Routing ได้แก่ OSPFv2 และ v3 , BGP, RIP, IGMP v2 และv3 ได้เป็นอย่างน้อย

17.10 สามารถรองรับการใช้งานไม่น้อยกว่า VPN 200 concurrent users

17.11 สามารถตรวจสอบและควบคุม Applications ได้อย่างน้อย 4,500 Applications

17.12 อุปกรณ์ต้องสามารถใช้งาน Intrusion Prevention System (IPS) ได้ โดยสามารถระบุการโจมตีล้อตามช่องโหว่ตาม CVE ได้

17.13 สามารถกำหนดทำงานของ IPS ในลักษณะของ Bypass Under load เมื่อระดับการทำงานของ CPU และ Memory ของอุปกรณ์เกินค่า Threshold ที่กำหนด

17.14 อุปกรณ์ต้องสามารถตรวจจับ Virus โดยป้องกันการดาวโหลดไฟล์ที่มีมัลแวร์ และสามารถตรวจจับและป้องกัน Virus บนโปรโตคอล HTTP, FTP, SMB ได้

17.15 สามารถตรวจจับ Bot, Command & Control (C&C) หรือ Spyware ได้เป็นอย่างน้อย

17.16 สามารถป้องกันการโจมตีผ่านโปรโตคอล DNS ในรูปแบบ DGA (Domain Generation Algorithm) และ DNS Tunneling ได้

17.17 สามารถทำงานแบบ URL Filtering เพื่อเพิ่มความปลอดภัยในการใช้งาน Web site ได้ โดยมีการจัดประเภทของ Content ได้ทั้งแบบ category และ custom ได้ พร้อมทั้งสามารถ Update ฐานข้อมูลได้อย่างสม่ำเสมอ

17.18 มีความสามารถในป้องกันการโจมตี โดยใช้เทคโนโลยี Sandbox ในการตรวจสอบได้

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) ซึ่งทำการบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่มีความเคลื่อนไหวตามจุดที่ติดตั้งอุปกรณ์ที่ธนาคารใช้เช่า 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 หรือแผ่นซีดีเพื่อการสำรองข้อมูลประจำวัน การปิด/เปิดอุปกรณ์ต่างๆ หรือช่วยตรวจดูไฟสถานะต่างๆของอุปกรณ์ภายในตู้อุปกรณ์ และสามารถติดต่อประสานงานได้โดยสะดวก หากอุปกรณ์ที่ศูนย์สำรองเกิดเหตุขัดข้อง หรือชำรุดบกพร่องจนไม่สามารถใช้งานได้เป็นปกติ บริษัทฯ ต้องรีบแจ้งธนาคารให้ทราบโดยทันที

21. การให้บริการ DR

มีเจ้าหน้าที่คอย Monitoring ระบบงาน AS/400 และซอฟต์แวร์ในการส่งข้อมูล ตลอด 24 ชั่วโมง ณ ศูนย์สำรองพร้อมทั้งตรวจสอบระบบ Network ที่เชื่อมต่อระหว่างศูนย์คอมพิวเตอร์หลัก มาที่ศูนย์คอมพิวเตอร์สำรอง

21.1 สามารถกู้คืนระบบงาน AS/400 ภายใน 4 ชั่วโมง (RTO 4) นับจากได้รับแจ้งการเกิดเหตุการณ์ (Downtime) อย่างเป็นทางการจากทางธนาคารฯ เพื่อดำเนินการ Recovery

21.2 มีเจ้าหน้าที่สำหรับลงข้อมูลจากเทป (restore data) สำหรับระบบงานอื่นๆ ทุกเดือน ณ ศูนย์สำรอง

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

22. การให้บริการสนับสนุนตลอดระยะเวลาการใช้บริการ (Support)

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 ในกรณีที่อุปกรณ์ที่ศูนย์สำรองระบบคอมพิวเตอร์เกิดเหตุขัดข้อง หรือชำรุดบกพร่องจนไม่สามารถใช้งานได้ ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกจะต้องดำเนินการแก้ไขเหตุขัดข้องหรือความชำรุดบกพร่องให้แล้วเสร็จและสามารถใช้งานได้เป็นปกติ นับถัดจากที่ได้รับแจ้งเหตุขัดข้องหรือความชำรุดบกพร่องจากธนาคาร ตามระดับผลกระทบที่มีต่อธุรกิจ หรือการทำงาน (Severity) ดังนี้

ระดับผลกระทบ (Severity)	ระยะเวลาติดต่อกลับ	ระยะเวลาการแก้ไขปัญหาเสร็จสิ้น นับจากที่ได้รับแจ้ง
ปัญหาเร่งด่วน ธนาคารไม่สามารถใช้ระบบได้	30 นาที	4 ชั่วโมง
ปัญหาสำคัญ ระบบทำงานผิดพลาดในเรื่องสำคัญ หรือใช้งานได้บางส่วน	2 ชั่วโมง	24 ชั่วโมง
ปัญหาไม่เร่งด่วน ระบบทำงานผิดพลาดแบบไม่มีสาระสำคัญ	4 ชั่วโมง	72 ชั่วโมง

ต้องนำส่งรายละเอียดและขั้นตอนการเข้ามาดำเนินการแก้ไขปัญหาหรือเหตุขัดข้องหรือความชำรุดบกพร่อง ให้กับธนาคารในทันทีที่สามารถดำเนินการได้และผู้ยื่นข้อเสนอที่ได้รับคัดเลือกตกลงเป็นผู้รับผิดชอบชำระค่าใช้จ่าย ที่เกิดขึ้นจากการเข้าดำเนินการทั้งจำนวน

12/25

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ การจ้างผู้ให้บริการ Security Operation Center (SOC)

2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ

3. วงเงินงบประมาณที่ได้รับจัดสรร 3,500,000.00 บาท (สามล้านห้าแสนบาทถ้วน)

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 04 มี.ค. 2568

   เป็นเงิน 3,181,700.00 บาท (สามล้านหนึ่งแสนแปดหมื่นหนึ่งพันเจ็ดร้อยบาทถ้วน)

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   บริษัท ซีเคียว ดี เซ็นเตอร์ จำกัด
   บริษัท อี-ซี.โอ.พี (ประเทศไทย) จำกัด
   บริษัท แบงคอค เอ็มเอสพี จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายพงษ์เทพ	เลขะกุล	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.2 นายจรัส	ขวัญพิเชษฐ์สกุล	ผู้บริหารส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ / ฝ่าย ปส.
6.3 นางสาวศรัญญา	แวงวรรณ์	ผู้บริหารส่วนจัดซื้อเทคโนโลยีสารสนเทศ / ฝ่าย จธ.

ผนวก 1

ขอบเขตการดำเนินงาน
การจ้างผู้ให้บริการ Security Operation Center (SOC)

ผู้ยื่นข้อเสนอต้องเสนอบริการ Security Operation Center (SOC) โดยมีขอบเขตการดำเนินงาน ดังนี้

1. **ข้อกำหนดความต้องการทั่วไป**
   1.1 ผู้ยื่นข้อเสนอต้องเป็นผู้ให้บริการการบริหารจัดการระบบความปลอดภัยสารสนเทศ (Managed Security Service Provider: MSSP) หรือ ประกอบกิจการศูนย์เฝ้าระวังด้านความปลอดภัยสารสนเทศหรือความปลอดภัยไซเบอร์แบบครบวงจร 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 ผู้ยื่นข้อเสนอต้องมีสิทธิความเป็นเจ้าของหรือสิทธิการใช้งานอย่างถูกต้องเพื่อให้บริการกับธนาคาร
   1.4 ต้องเสนออุปกรณ์, โปรแกรมต่างๆ, บริการ, การดำเนินการส่ง log จากอุปกรณ์หรือระบบงานของทางธนาคารไปประมวลผลที่ศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ และส่วนประกอบเพิ่มเติมที่จำเป็นต่อการให้บริการให้ครบถ้วน
2. **ความต้องการด้านเทคนิค**
   2.1 ต้องจัดเตรียมระบบเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ ซึ่งสามารถจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร ระบบจะต้องประกอบด้วยการทำงานดังต่อไปนี้
      - สามารถวิเคราะห์และหาความสัมพันธ์ของข้อมูล เพื่อหาเหตุการณ์ผิดปกติได้
      - สามารถปรับแต่งรูปแบบความสัมพันธ์หรือเงื่อนไข (Custom Rule) ได้
      - สามารถแจ้งเตือนให้ผู้ดูแลระบบทราบ เมื่อตรวจพบข้อมูลที่สอดคล้องกับเงื่อนไขที่ได้ตั้งไว้
      - สามารถบริการจัดการผ่าน Web Interface หรือ GUI ได้เป็นอย่างน้อย
      - สามารถกำหนดสิทธิ์การเข้าถึงระบบ ตามระดับสิทธิ์การเข้าถึงได้ (Role Base Access Control)
   2.2 ระบบเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ จะต้องสามารถรองรับข้อมูลจราจรทางคอมพิวเตอร์ได้เฉลี่ยรายเดือนไม่น้อยกว่า 80 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
      - WAF : Cloudflare
      - Antivirus : Trendmicro

- Secure Internet Gateway : Zscaler
- Cloud : INET, MS-Azure, AWS or Etc.

2.3 บริการจัดเก็บและสืบค้นข้อมูล (Log Management)

2.3.1 บริการจัดเก็บ Log เป็นระยะเวลา 365 วัน

2.3.2 บริการสืบค้น Log ที่อยู่ในระยะเวลา 90 วันได้ตามที่ธนาคารร้องขอ ภายใน 7 วัน

2.3.3 บริการตรวจสอบสถานการณ์ส่ง Log พร้อมแจ้งเตือนไปยังเจ้าหน้าที่ที่เกี่ยวข้องของผู้ใช้บริการผ่านทางระบบอีเมล์ หรือช่องทางตามที่ตกลงกัน ในกรณีที่ตรวจพบว่าอุปกรณ์ทั้งหมดของธนาคารไม่สามารถส่งข้อมูล Log มายังศูนย์ปฏิบัติการของผู้ยื่นข้อเสนอ ผู้ยื่นข้อเสนอจะต้องแก้ไขให้สามารถส่งข้อมูล Log ได้ภายในระยะเวลา 4 ชั่วโมง เริ่มนับจากเวลาที่อุปกรณ์ของ ธสน. สำหรับใช้ในการส่งข้อมูล Log ตามที่ได้ตกลงกับผู้เสนอราคาฯ ไม่สามารถดำเนินการได้

2.4 จัดให้มีผู้เชี่ยวชาญเข้าทำกระบวนการเตรียมพร้อมและส่งผ่านข้อมูลจราจรทางคอมพิวเตอร์ เพื่อใช้ในการเฝ้าระวังฯ (On-boarding process) ดังนี้

2.4.1 ตรวจสอบความพร้อมใช้ของระบบและอุปกรณ์ต้นกำเนิดข้อมูลจราจรทางคอมพิวเตอร์ที่จะใช้ในการ เฝ้าระวังร่วมกับเจ้าหน้าที่ของธนาคาร และให้คำแนะนำในการตั้งค่าอุปกรณ์เพื่อให้สามารถส่งข้อมูลจราจรทางคอมพิวเตอร์ได้

2.4.2 ระบุแหล่งที่มาของข้อมูลจราจรทางคอมพิวเตอร์และจัดหมวดหมู่ของอุปกรณ์ต้นกำเนิด

2.4.3 ระบุและวิเคราะห์ความเสี่ยงรูปแบบการโจมตี และจัดระดับของผลกระทบต่อระบบของทางธนาคารรวมทั้งกำหนดประเภทข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่ต้องใช้ในการวิเคราะห์ร่วมกับธนาคาร

2.4.4 วิเคราะห์และสร้างแบบจำลองของภัยคุกคาม เพื่อหาวิธีและเครื่องมือในการเฝ้าระวังที่เหมาะสม (Threat Model)

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

2.4.6 จัดทำ Alert ให้สอดคล้องกับ Monitoring Use case เพื่อใช้ในการแจ้งเตือนและรายงานต่างๆ

2.4.7 จัดทำแผนการทำงานร่วมกันในกระบวนการ Incident Management รวมถึงแผนการดำเนินการตอบโต้ภัยคุกคามร่วมกันกับทางธนาคาร

2.5 ให้คำแนะนำและประเมินกระบวนการตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response) ในปัจจุบันของธนาคาร เพื่อปรับปรุงกระบวนการตอบสนองต่อเหตุการณ์ผิดปกติให้มีประสิทธิภาพดีขึ้น

3. การให้บริการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์

3.1 ให้บริการ Security Awareness โดยการจัดทำ Phishing Simulation อย่างน้อย 2 ครั้งต่อปี (ตามที่ธนาคารกำหนด)

3.2 ดำเนินการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์เหตุการณ์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ให้แก่ธนาคาร ณ ศูนย์ปฏิบัติการของผู้รับจ้าง โดยให้บริการแบบตลอดเวลา 24 ชั่วโมงของทุกวัน ไม่มีวันหยุด (7 x 24) ตลอดระยะเวลาของสัญญา

3.3 แจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัย สำหรับเหตุการณ์ที่อยู่ในขอบข่ายภัยคุกคามทางไซเบอร์ โดยจะต้องแจ้งเตือนผ่านทาง Email หรือทางโทรศัพท์ หรือช่องทางอื่นใด ตามที่จะตกลงร่วมกันกับธนาคาร ตาม Severity Level Agreement (SLA) ดังต่อไปนี้

ระดับ ความรุนแรง	ระยะเวลาแจ้งเตือนผู้รับบริการ (นับจากเวลาที่ผู้เสนอราคาฯ ตรวจพบภัยคุกคามทางไซเบอร์)	ระยะเวลาให้คำแนะนำในการแก้ไขปัญหาเสร็จสิ้น (นับจากเวลาที่ผู้เสนอราคาฯ แจ้งแก่ ธสน.)
วิกฤติ ภัยคุกคามที่ส่งผลกระทบต่อระบบหรือข้อมูลที่สำคัญอย่างมาก ทำให้ระบบหยุดทำงาน หรือไม่สามารถใช้งานได้ และอาจก่อให้เกิดความเสียหายอย่างร้ายแรง	ภายใน 0.5 ชั่วโมง	ภายใน 1 ชั่วโมง
สูง ภัยคุกคามที่อาจส่งผลกระทบต่อระบบหรือข้อมูลที่สำคัญอย่างรุนแรง ทำให้ระบบไม่สามารถทำงานได้ตามปกติ หรืออาจส่งผลกระทบต่อความปลอดภัยของข้อมูล	ภายใน 1 ชั่วโมง	ภายใน 2 ชั่วโมง
กลาง ภัยคุกคามที่อาจส่งผลกระทบต่อระบบหรือข้อมูลบางส่วน แต่ไม่ถึงกับทำให้ระบบหยุดทำงาน หรือไม่สามารถใช้งานได้	ภายใน 1.5 ชั่วโมง	ภายใน 3 ชั่วโมง
ต่ำ ภัยคุกคามที่ไม่ส่งผลกระทบต่อระบบหรือข้อมูลที่สำคัญ หรืออาจส่งผลกระทบเพียงเล็กน้อย	ภายใน 2 ชั่วโมง	ภายใน 4 ชั่วโมง

3.4 การแจ้งเตือนจะต้องมีรายละเอียด อย่างน้อยดังนี้

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

3.5 ให้คำปรึกษาเกี่ยวกับบริการวิเคราะห์เฝ้าระวังภัยคุกคามต่างๆ ที่เกิดขึ้น และสนับสนุนการทำงานเกี่ยวกับการแก้ไข ป้องกันและรับมือกับภัยคุกคามได้ตลอด 24 ชั่วโมง

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

3.7 สามารถตรวจจับเหตุการณ์การคุกคามครอบคลุมในเรื่องดังนี้ เป็นอย่างน้อย

3.7.1 Unauthorized Access

3.7.2 Malicious code

3.7.3 Inappropriate usage

3.7.4 Denial of service

3.7.5 Information Gathering

3.7.6 Malware

3.7.7 Suspicious Traffic

3.7.8 Vulnerability Scan

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

3.9 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), อ้างอิง (Reference) เป็นต้น

3.10 จัดเตรียมหน่วยปฏิบัติการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ (CSIRT) พร้อมที่จะปฏิบัติหน้าที่ในการตอบสนองต่อภัยคุกคามหรือการบุกรุกระบบอย่างทันท่วงที หรือเข้าดำเนินการสืบสวนและวิเคราะห์หาสาเหตุของปัญหา ภัยคุกคามที่เกิดขึ้น รวมถึงการตรวจพิสูจน์พยานหลักฐานทาง Digital เมื่อมีการร้องขอบริการจากทางธนาคารภายในระยะเวลา 4 ชั่วโมง นับตั้งแต่ที่ธนาคารร้องขอ ไม่เกินกว่า 5 เหตุการณ์ พร้อมจัดทำรายงานผลการดำเนินงานสรุปข้อมูลหลักฐานต่างๆ ที่ได้จากการตอบสนองต่อเหตุการณ์ภัยคุกคาม รวมถึงแนวทางในการป้องกันการเกิดซ้ำในอนาคต (Incident Response and Recommendations Report) ทันทีที่สามารถดำเนินการได้

3.11 จัดทำรายงานสรุปสถิติภัยคุกคามประจำเดือน (Monthly Report) ภายในรูปแบบที่ธนาคารเห็นชอบ และมีหัวข้อของรายงาน อย่างน้อยดังนี้

- รายงานสรุประดับความความรุนแรงของเหตุการณ์ที่ตรวจพบรายเดือน
- รายงานสรุประดับความเสี่ยงของเหตุการณ์ที่ตรวจพบรายเดือน
- รายงานสรุปจำนวนของเหตุการณ์ที่ตรวจพบจำแนกตาม Classification type
- รายงานสรุปสถานะของเหตุการณ์ที่ตรวจพบรายเดือน
- รายงานเหตุการณ์ที่ตรวจพบจำแนกตาม Classification type
- รายงานสรุปปริมาณการใช้งานข้อมูลจราจรทางคอมพิวเตอร์ประจำเดือน
- รายงานแสดงสถานะของ Log Source ที่ส่ง Log มา SIEM
- สรุปรายงาน และให้คำแนะนำเพิ่มเติม ในการป้องกันภัยคุกคาม

3.12 บริการเข้าร่วมประชุมประจำเดือน ทั้งแบบประชุมทางไกล (Video Conference Monthly Meeting) หรือเข้าประชุม ณ. ที่ทำการธนาคารฯ สำนักงานใหญ่ (On-Site Monthly Meeting) โดยผู้ยื่นข้อเสนอจะต้องเข้าร่วมประชุมเพื่อสรุปให้คำแนะนำและทุกๆ เดือน ตลอดสัญญาของการให้บริการ

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

4. **บุคลากรในการดำเนินโครงการ**

ผู้ยื่นข้อเสนอจะต้องมีผู้เชี่ยวชาญและเจ้าหน้าที่ที่ปฏิบัติงานในศูนย์เฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ พนักงานประจำที่มีประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ที่ได้รับการรับรองความรู้ความสามารถและมีประกาศนียบัตรรับรอง (Certificate) ที่ยังไม่หมดอายุ จนถึงวันที่ยื่นข้อเสนอ ดังต่อไปนี้

4.1 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

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

4.3 CompTIA CySA+ หรือ CompTIA Security+ อย่างน้อย 4 คน

ผนวก 2

คุณสมบัติผู้ยื่นข้อเสนอและการปฏิบัติตามข้อกำหนด

การจ้างผู้ให้บริการ Security Operation Center (SOC)

ผู้ยื่นข้อเสนอจะต้องมีคุณสมบัติและต้องปฏิบัติตามข้อกำหนด ดังนี้

1. **คุณสมบัติผู้ยื่นข้อเสนอและการปฏิบัติตามข้อกำหนด**

1.1 มีความสามารถตามกฎหมาย

1.2 ไม่เป็นบุคคลล้มละลาย

1.3 ไม่อยู่ระหว่างเลิกกิจการ

1.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบ

1.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

1.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

1.7 ต้องเป็นนิติบุคคลที่มีอาชีพรับจ้างงานตามที่ธนาคารมีความประสงค์จัดหาในครั้งนี้

1.8. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการจัดซื้อ ครั้งนี้

1.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

1.10 ไม่เป็นผู้กระทำการอันเป็นการละเมิดต่อสิทธิมนุษยชน การปฏิบัติด้านแรงงานและสิ่งแวดล้อม ตามหลักการกำกับดูแลกิจการที่ดีและความรับผิดชอบต่อสังคมที่ธนาคารกำหนด

1.11 ไม่เป็นผู้กระทำการทุจริตในการจัดซื้อจัดจ้าง ตามพระราชบัญญัติประกอบรัฐธรรมนูญ ว่าด้วยการป้องกันและปราบปรามการทุจริต พ.ศ. 2561 มาตรา 176

1.12 ผู้ยื่นข้อเสนอต้องมีบุคลากรผู้ดำเนินงาน โดยต้องมีวุฒิการศึกษาปริญญาตรี และมีประสบการณ์การทำงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) 5 ปี เป็นอย่างน้อยและต้องได้รับรองมาตรฐานความรู้ความสามารถทางด้านความปลอดภัยคอมพิวเตอร์ โดยต้องยื่นเอกสารรับรองวุฒิการศึกษา ประสบการณ์ทำงาน และใบรับรอง (Certificate) ตามข้อ 3 (ผนวก 1) ที่ยังมีผลบังคับใช้ของบุคลากร พร้อมกับการยื่นข้อเสนอในครั้งนี้ ดังต่อไปนี้

1.12.1 ผู้ยื่นข้อเสนอต้องมีบุคลากรที่ได้รับใบรับรอง 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

4. ค่าจ้างและการชำระเงิน

ธนาคารจะชำระเงินค่าบริการ โดยแบ่งชำระเป็น 4 งวด (ราย 3 เดือน) ภายในระยะเวลา 30 วัน เมื่อผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกได้ดำเนินการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ และส่งมอบรายงานประจำเดือน (Monthly Report) ตามระยะเวลาและเงื่อนไขที่กำหนดในสัญญาเป็นที่เรียบร้อยแล้ว ดังนี้

งวดที่	จำนวนเงินร้อยละของมูลค่าการว่าจ้าง	เอกสารประกอบการชำระเงิน
1	25	เอกสารรายงานประจำเดือน (ตั้งแต่วันที่ 30 สิงหาคม 2568 - 30 พฤศจิกายน 2568) รายละเอียดตามข้อ 2.2 ผนวก 2
2	25	เอกสารรายงานประจำเดือน (ตั้งแต่วันที่ 1 ธันวาคม 2568 – 28 กุมภาพันธ์ 2569) รายละเอียดตามข้อ 2.2 ผนวก 2
3	25	เอกสารรายงานประจำเดือน (ตั้งแต่วันที่ 1 มีนาคม 2569 – 31 พฤษภาคม 2569) รายละเอียดตามข้อ 2.2 ผนวก 2
4	25	เอกสารรายงานประจำเดือน (ตั้งแต่วันที่ 1 มิถุนายน 2569 – 29 สิงหาคม 2569) รายละเอียดตามข้อ 2.2 ผนวก 2

5. ค่าปรับ

5.1. กรณีที่ไม่สามารถส่งมอบงานตามที่กำหนดในข้อ 2. (ผนวก 2) หรือส่งมอบแล้วแต่ไม่ถูกต้อง ไม่ครบถ้วน ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกต้องยินยอมให้ธนาคารปรับเป็นรายวัน ในอัตราร้อยละ 0.2 (ศูนย์จุดสอง) ของมูลค่างานทั้งหมด (รวมภาษีมูลค่าเพิ่ม) นับถัดจากวันครบกำหนดการส่งมอบจนถึงวันที่ได้ส่งมอบงานถูกต้องครบถ้วน หรือวันที่ธนาคารบอกเลิกจ้าง

5.2. กรณีที่ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกไม่สามารถดำเนินการได้ตามเงื่อนไขการให้บริการที่กำหนดไว้ในข้อ 3.3 (ผนวก 1) ผู้ยื่นข้อเสนอราคาที่ได้รับการคัดเลือกต้องยินยอมให้ธนาคารปรับเป็นรายชั่วโมงต่อเหตุการณ์ ในอัตราร้อยละ 0.2 (ศูนย์จุดสอง) ของมูลค่างานทั้งหมด (รวมภาษีมูลค่าเพิ่ม) โดยนับถัดจากระยะเวลาที่ครบกำหนดจนถึงระยะเวลาที่สามารถดำเนินการได้เป็นปกติ และระยะเวลาที่ไม่ถึง 1 ชั่วโมง ให้นับเป็น 1 ชั่วโมง โดยธนาคารจะเรียกเก็บค่าปรับเฉพาะกรณีที่คำนวณแล้วมีจำนวนเงินค่าปรับที่สูงสุดเพียงกรณีเดียว

5.3. กรณีที่ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกไม่เข้าดำเนินการสืบสวนและวิเคราะห์สาเหตุของปัญหา ตามข้อ 3.10 (ผนวก 1) ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกต้องยินยอมให้ธนาคารปรับเป็นรายชั่วโมง ในอัตราร้อยละ 0.2 (ศูนย์จุดสอง) ของมูลค่างานทั้งหมด (รวมภาษีมูลค่าเพิ่ม) โดยนับถัดจากระยะเวลาที่ครบกำหนดจนถึงระยะเวลาที่สามารถดำเนินการได้เป็นปกติ โดยระยะเวลาที่ไม่ถึง 1 ชั่วโมง ให้นับเป็น 1 ชั่วโมง

5.4. กรณีที่ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกไม่สามารถให้บริการได้ ตามข้อ 2.3.3 (ผนวก 1) ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกต้องยินยอมให้ธนาคารปรับเป็นรายชั่วโมงในอัตราร้อยละ 0.2 (ศูนย์จุดสอง) ของมูลค่างานทั้งหมด (รวมภาษีมูลค่าเพิ่ม) โดยนับถัดจากระยะเวลาที่ครบกำหนดจนถึงระยะเวลาที่สามารถดำเนินการได้เป็นปกติ โดยระยะเวลาที่ไม่ถึง 1 ชั่วโมง ให้นับเป็น 1 ชั่วโมง

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

1.12.3 ผู้ยื่นข้อเสนอต้องมีบุคลากรที่ได้รับใบรับรอง CompTIA CySA+ หรือ CompTIA Security+ อย่างน้อย 4 คน

2. การส่งมอบงาน

2.1 ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกต้องส่งมอบเอกสารภายในวันที่ 30 สิงหาคม 2568 โดยจัดทำเป็นรูปเล่ม จำนวน 1 ชุด โดยมีเอกสารที่ต้องส่งมอบดังนี้

2.1.1 หนังสือรับรองเพื่อยืนยันต่อธนาคารว่าซอฟต์แวร์ทุกประเภทที่ใช้กับงานของธนาคารไม่มีโปรแกรมแอบแฝงหรือโปรแกรมมุ่งร้ายใดๆ

2.1.2 เอกสารยืนยันการจ้างผู้ให้บริการ Security Operation Center (SOC) ตั้งแต่วันที่ 30 สิงหาคม 2568 – 29 สิงหาคม 2569

2.1.3 เอกสารแสดงสิทธิการใช้งานโปรแกรม (ตามข้อ 2 ผนวก 1)

2.2 ส่งมอบรายงานสรุปสถิติภัยคุกคามประจำเดือน (Monthly Report) ภายใน 15 วัน นับถัดจากวันที่สิ้นสุดการให้บริการในแต่ละเดือน จำนวน 1 ชุด โดยมีหัวข้อของรายงาน อย่างน้อยดังนี้

- รายงานสรุประดับความความรุนแรงของเหตุการณ์ที่ตรวจพบรายเดือน
- รายงานสรุประดับความเสี่ยงของเหตุการณ์ที่ตรวจพบรายเดือน
- รายงานสรุปจำนวนของเหตุการณ์ที่ตรวจพบจำแนกตาม Classification type
- รายงานสรุปสถานะของเหตุการณ์ที่ตรวจพบรายเดือน
- รายงานเหตุการณ์ที่ตรวจพบจำแนกตาม Classification type
- รายงานสรุปปริมาณการใช้งานข้อมูลจราจรทางคอมพิวเตอร์ประจำเดือน
- รายงานแสดงสถานะของ Log Source ที่ส่ง Log มา SIEM
- สรุปคำแนะนำ และให้คำแนะนำเพิ่มเติม ในการป้องกันภัยคุกคาม

หากธนาคารตรวจสอบแล้วพบว่าระบบงานที่ส่งมอบไม่ตรงตามขอบเขตการดำเนินงานที่กำหนดในข้อตกลงหรือสัญญา หรือมีความชำรุดบกพร่องประการหนึ่งประการใด ธนาคารสงวนสิทธิ์ที่จะไม่รับมอบระบบงานดังกล่าวทั้งหมดหรือเพียงบางส่วน หรือให้ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกดำเนินการเปลี่ยนแปลงและ/หรือปรับปรุง แก้ไขให้ถูกต้องตามคำชี้ขาดของธนาคารด้วยค่าใช้จ่ายของผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกเองทั้งสิ้น ทั้งนี้ระยะเวลาที่เสียไปเพราะเหตุดังกล่าว ไม่เป็นเหตุให้ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกมีสิทธิขยายระยะเวลาการส่งมอบเกินกำหนดเวลาที่ระบุในข้อตกลงหรือสัญญา หรือขอยกเว้นหรือลดค่าปรับได้

3. ระยะเวลาการใช้บริการ

ธนาคารจะใช้บริการระบบ SOC เป็นระยะ เริ่มตั้งแต่วันที่ 30 สิงหาคม 2568 – 29 สิงหาคม 2569

5.5. กรณีที่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกนำงานที่รับจ้างไปจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจากธนาคารจะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนเงินร้อยละ 10 ของวงเงินของงานจ้างช่วงนั้น

6. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

6.1 ธนาคารจะพิจารณาข้อเสนอของผู้ยื่นข้อเสนอที่มีคุณสมบัติถูกต้องครบถ้วนตามผนวก 2 และยื่นเอกสารครบถ้วนตามผนวก 8 เว้นแต่เป็นข้อผิดพลาดเพียงเล็กน้อย หรือผิดพลาดในส่วนที่มิใช่สาระสำคัญ ทั้งนี้ เฉพาะในกรณีที่ธนาคารพิจารณาเห็นว่าจะเป็นประโยชน์ต่อธนาคารเท่านั้น

6.2 ขอบเขตการดำเนินงานที่นำเสนอเป็นไปตามที่กำหนดในผนวก 1

6.3 ในการพิจารณาครั้งนี้ ธนาคารจะพิจารณาตัดสินโดยใช้ หลักเกณฑ์ราคา

7. การทำสัญญาและหลักประกันการปฏิบัติตามสัญญา

ในกรณีที่มีมูลค่าการจัดหาครั้งหนึ่งเกิน 5 แสนบาท ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะต้องดำเนินการ ดังนี้

7.1 ลงนามในสัญญากับธนาคารตามแบบที่ธนาคารกำหนดให้แล้วเสร็จภายใน 30 วัน นับถัดจากวันที่ได้รับหนังสือแจ้งจากธนาคาร ทั้งนี้ ธนาคารขอสงวนสิทธิที่จะปรับเปลี่ยนข้อความในสัญญาบางประการตามที่เห็นสมควร

7.2 วางหลักประกันการปฏิบัติตามสัญญาให้ธนาคารก่อน หรือในวันที่ลงนามในสัญญา เป็นจำนวนเงินร้อยละ 5 ของมูลค่าการว่าจ้างทั้งหมด (รวมภาษีมูลค่าเพิ่ม) โดยมีระยะเวลาการค้ำประกันนับตั้งแต่วันที่ลงนามในสัญญาจนถึงวันที่สิ้นสุดภาระผูกพันตามสัญญา โดยใช้หลักประกันอย่างหนึ่งอย่างใดดังนี้

7.2.1 เช็คหรือดราฟท์ที่ธนาคารสั่งจ่าย "ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย" ซึ่งเป็นเช็คหรือดราฟท์ลงวันที่ที่ใช้เช็คหรือดราฟท์นั้น ชำระต่อธนาคาร หรือก่อนวันนั้นไม่เกิน 7 วันทำการ

7.2.2 หนังสือค้ำประกันของธนาคารภายในประเทศไทย ตามที่ธนาคารกำหนด (ผนวก 9)

7.3 การคืนหลักประกันการปฏิบัติตามสัญญา ธนาคารจะคืนให้โดยไม่มีดอกเบี้ยหรือเงินเพิ่มใดๆ เมื่อผู้ให้บริการ พ้นจากข้อผูกพันตามสัญญา

8. ข้อสงวนสิทธิ์ในการเสนอราคาและอื่นๆ

8.1 กรณีมีความจำเป็นที่ธนาคารต้องงดการดำเนินการไม่ว่าในขั้นตอนใดๆ อันเนื่องมาจากการแพร่ระบาดของโรคติดต่ออันตราย หรือสถานการณ์หนึ่งสถานการณ์ใดที่เป็นอุปสรรคหรือความเสี่ยงต่อการปฏิบัติงานของพนักงานธนาคาร หรือการปรับเปลี่ยนนโยบายเพื่อประโยชน์ของธนาคาร ธนาคารขอสงวนสิทธิ์ในการเปลี่ยนแปลงระยะเวลาดำเนินการ หรือยกเลิกการจัดซื้อจัดจ้าง หรือบอกเลิกสัญญาโดยผู้ยื่นข้อเสนอหรือ ผู้ที่ได้รับการคัดเลือกไม่มีสิทธิเรียกร้องค่าใช้จ่าย หรือค่าเสียหายใดๆได้

8.2 ผู้ยื่นข้อเสนอจะต้องดำเนินการให้สอดคล้องเป็นไปตามกฎหมาย รวมถึงหลักเกณฑ์ภายในธนาคารที่เกี่ยวข้อง เพื่อให้การดำเนินงานไม่ขัดแย้งต่อกฎหมายและหลักเกณฑ์ภายใน หากการดำเนินงานไม่ถูกต้องตามหลักเกณฑ์ภายในและกฎหมายที่เกี่ยวข้อง ผู้ยื่นข้อเสนอราคาที่ได้รับการคัดเลือกต้องรับผิดชอบและดำเนินการแก้ไขให้ถูกต้องจนเสร็จสิ้น โดยไม่มีค่าใช้จ่ายเพิ่มเติมแต่อย่างใด

8.3 ผู้ยื่นข้อเสนอราคาที่ได้รับการคัดเลือกต้องยินยอมให้ธนาคารส่งมอบข้อมูลที่เกี่ยวกับการดำเนินงานให้แก่ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอก และ/หรือหน่วยงานอื่นใดที่กำกับดูแลธนาคาร รวมถึงยินยอมให้ธนาคาร พนักงานของธนาคาร และ/หรือบุคคลดังกล่าวเข้าตรวจสอบการดำเนินงานของผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกได้ทันทีที่ได้รับการร้องขอ

8.4 ในการตัดสินคัดเลือกหรือในการทำสัญญา คณะกรรมการดำเนินการจ้าง หรือธนาคาร มีสิทธิ์ให้ผู้ยื่นข้อเสนอชี้แจงข้อเท็จจริง