

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย
ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)
ในการจัดซื้อจัดจ้างที่มีใช้งานก่อสร้าง

1. ชื่อโครงการ การเช่าใช้บริการระบบ Cloud Service สำหรับโครงการ SmartEase-EXIM



2. หน่วยงานเจ้าของโครงการ ฝ่ายบริหารและพัฒนาเทคโนโลยีสารสนเทศ

3. วงเงินงบประมาณที่ได้รับจัดสรร 1,000,000.00 บาท (หนึ่งล้านบาทถ้วน)

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) **16 มิ.ย. 2569**
เป็นเงิน 999,000.00 บาท (เก้าแสนเก้าหมื่นเก้าพันบาทถ้วน)

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
บริษัท พีวชั่น โซลูชั่น จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายศिला	กอบประเสริฐ	ผู้เชี่ยวชาญ 2 (เทียบเท่าผู้บริหารส่วน)-ฝ่ายบริหารและพัฒนาเทคโนโลยีสารสนเทศ
6.2 นายณัฐพงษ์	มะลาเวช	ผู้บริหารส่วนพัฒนาระบบสารสนเทศบริการ 2 / ฝ่าย พส. 
6.3 นายสุรพงศ์	เพียรบัณฑิต	ผู้บริหารส่วนพัฒนาระบบสารสนเทศบริการ 1 / ฝ่าย พส. 

ผนวก 1
ขอบเขตการดำเนินงาน
การเข้าใช้บริการระบบ Cloud Service สำหรับโครงการ SmartEase-EXIM

1. ขอบเขตการดำเนินงาน

ผู้ยื่นข้อเสนอจะต้องดำเนินการตามขอบเขตของงานที่กำหนดอย่างน้อย ดังต่อไปนี้

1.1. ข้อกำหนดความต้องการใน Environment Non-Production

- 1.1.1. ผู้ยื่นข้อเสนอจะต้องจัดหาและติดตั้ง Cloud Service สำหรับรองรับสภาพแวดล้อม Non-Production และพร้อมใช้งาน โดยมีระยะเวลาตั้งแต่วันที่ 18 มิถุนายน 2569 ถึง วันที่ 17 มกราคม 2570
- 1.1.2. ต้องมีการแยก Environment อย่างชัดเจนระหว่าง Non-Production และ Production เพื่อป้องกันผลกระทบข้ามระบบ และรองรับการควบคุมความมั่นคงปลอดภัยตามหลักการกำกับดูแลที่เหมาะสม
- 1.1.3. รองรับการบริหารจัดการสิทธิ์การเข้าถึง (Access Control) ตามระดับการใช้งานของผู้พัฒนา ผู้ทดสอบ และผู้ใช้งานที่เกี่ยวข้อง พร้อมบันทึกการใช้งาน (Audit Trail) เพื่อการตรวจสอบย้อนหลัง
- 1.1.4. มีระบบ Monitoring และ Logging สำหรับติดตามการทำงานของระบบ รวมถึงรองรับการวิเคราะห์ปัญหา การตรวจสอบ Incident และการทดสอบการแก้ไขปัญหาก่อนนำขึ้น Production
- 1.1.5. รองรับการทำ Vulnerability Assessment (VA), Security Testing และการทดสอบด้าน Performance เพื่อประเมินความพร้อมของระบบก่อนเข้าสู่ Production
- 1.1.6. ผู้ยื่นข้อเสนอจะต้องสนับสนุนการจัดเตรียม Test Data, Deployment Pipeline และ Release Process เพื่อให้การพัฒนาและทดสอบเป็นไปอย่างต่อเนื่องและมีประสิทธิภาพ
- 1.1.7. ต้องรองรับการสำรองข้อมูล (Backup) และการกู้คืนข้อมูล (Recovery) ในระดับที่เหมาะสมสำหรับ Environment Non-Production เพื่อป้องกันความเสียหายจากความผิดพลาดในการพัฒนาและทดสอบ
- 1.1.8. ผู้ยื่นข้อเสนอจะต้องจัดทำเอกสาร Environment Design, Deployment Guideline, Operation Procedure

1.2. ข้อกำหนดความต้องการใน Environment Production

- 1.2.1. จัดหาและติดตั้ง Cloud Service สำหรับรองรับระบบงานในสภาพแวดล้อม Production ที่มีความมั่นคงปลอดภัย และพร้อมใช้งานตลอดเวลา โดยมีระยะเวลาตั้งแต่วันที่ 1 ตุลาคม 2569 ถึง วันที่ 17 มกราคม 2570
- 1.2.2. รองรับการดำเนินงานของระบบงานหลักที่เกี่ยวข้อง เช่น Online Application, SmartEase-EXIM, Forward Contract Service และระบบเชื่อมต่อภายใน/ภายนอกธนาคาร ผ่านสถาปัตยกรรมที่สามารถขยายตัวได้ (Scalability) และรองรับปริมาณธุรกรรมที่เพิ่มขึ้นในอนาคต
- 1.2.3. รองรับการเชื่อมต่อกับระบบงานภายในธนาคาร (On-Premise Systems) และระบบภายนอกที่เกี่ยวข้องผ่านช่องทางที่มีความปลอดภัย และเป็นไปตามมาตรฐานด้านการเชื่อมต่อข้อมูลของธนาคาร
- 1.2.4. มีระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ เช่น Identity and Access Management (IAM), Encryption, Logging, Monitoring, Backup และ Disaster Recovery เพื่อให้เป็นไปตามข้อกำหนดของธนาคารและข้อกำหนดของธนาคารแห่งประเทศไทย (ธปท.)
- 1.2.5. รองรับการจัดเก็บ Log และ Audit Trail เพื่อให้สามารถตรวจสอบย้อนหลังได้ตามข้อกำหนดด้าน Compliance และ Regulatory Requirement
- 1.2.6. มีระบบ Monitoring และ Alert สำหรับติดตามสถานะการทำงานของระบบแบบ Real-time พร้อมรองรับการแจ้งเตือนเมื่อเกิดเหตุผิดปกติ

- 1.2.7. ผู้ยื่นข้อเสนอจะต้องจัดทำเอกสาร Architecture Design, Security Design, Network Diagram และ Operation Runbook สำหรับการบริหารจัดการระบบในระยะยาว
- 1.2.8. สามารถกำหนดสิทธิ์การเข้าถึง (Access Control) การแยกหน้าที่ (Segregation of Duties: SoD) และการบริหารจัดการสิทธิ์ของผู้ใช้งานตามหลักการกำกับดูแลที่เหมาะสม
- 1.2.9. สามารถรองรับการตรวจสอบด้าน Vulnerability Assessment (VA), Penetration Test (Pentest) และการปฏิบัติตามข้อกำหนดด้าน Cybersecurity ของธนาคารได้อย่างครบถ้วน
- 1.2.10. ผู้ยื่นข้อเสนอจะต้องสนับสนุนการส่งมอบระบบ การทดสอบความพร้อมก่อนใช้งานจริง (Production Readiness) และการถ่ายทอดองค์ความรู้ (Knowledge Transfer) ให้แก่เจ้าหน้าที่ของธนาคารอย่างครบถ้วน
- 1.3. เอกสารที่ต้องดำเนินการส่งมอบเอกสารประกอบ
 - 1.3.1. เอกสาร Architecture Design
 - 1.3.2. เอกสาร Security Design
 - 1.3.3. เอกสาร Network Diagram
 - 1.3.4. เอกสาร Deployment Guide
 - 1.3.5. เอกสาร Incident Handling Procedure
 - 1.3.6. เอกสาร Backup and Recovery Procedure
 - 1.3.7. เอกสาร Access Control Matrix และสิทธิ์การเข้าถึงระบบ
 - 1.3.8. เอกสาร Security Assessment ที่เกี่ยวข้อง
 - 1.3.9. ผลการทดสอบระบบใน Environment Non-Production และ Production Readiness Test
 - 1.3.10. ผลการทดสอบด้าน Performance และ Scalability
 - 1.3.11. ผลการทดสอบ Disaster Recovery (DR Drill) และการกู้คืนระบบ
- 1.4. การถ่ายทอดองค์ความรู้
 - 1.4.1. ต้องจัดทำคู่มือการใช้งาน คู่มือการปฏิบัติงาน และเอกสารประกอบการอบรมอย่างครบถ้วน
 - 1.4.2. ต้องมีการจัดประชุม Workshop / Hands-on Session พร้อมสรุปผลการถ่ายทอดองค์ความรู้ที่ได้รับการลงนามรับรองการส่งมอบงาน และใบรายชื่อผู้เข้ารับการอบรม อย่างน้อย 1 รอบ

2. การให้บริการสนับสนุนตลอดระยะเวลาการใช้บริการ

2.1. กรณีที่การให้คำปรึกษา/แก้ไขปัญหาผ่านทางโทรศัพท์หรือช่องทางอื่น ยังไม่สามารถแก้ไขปัญหาได้ ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกต้องจัดส่งพนักงานเพื่อแก้ไขปัญหาหรือเหตุขัดข้องที่ธนาคาร ซึ่งให้เป็นไปตามดุลพินิจของธนาคาร ดังนี้

ระดับผลกระทบ (Severity)	ระยะเวลาติดต่อกลับ	ระยะเวลาการแก้ไขปัญหาเสร็จสิ้นนับจากที่ได้รับแจ้ง
ปัญหาเร่งด่วน ธนาคารไม่สามารถใช้ระบบได้	4 ชั่วโมง	12 ชั่วโมง
ปัญหาสำคัญ ระบบทำงานผิดพลาดในเรื่องสำคัญ หรือใช้งานได้บางส่วน	4 ชั่วโมง	24 ชั่วโมง
ปัญหาไม่เร่งด่วน ระบบทำงานผิดพลาดแบบไม่มีสาระสำคัญ	4 ชั่วโมง	7 วัน

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องนำส่งรายละเอียดและขั้นตอนการแก้ไขปัญหาเหตุขัดข้อง และ/หรือความชำรุดบกพร่องของระบบ ให้แก่ธนาคาร ในทันทีที่สามารถดำเนินการได้ ภายหลังจากวันที่ได้ดำเนินการขั้นตอนการแก้ไขปัญหา

เหตุขัดข้อง และ/หรือความชำรุดบกพร่องของระบบแล้วเสร็จในแต่ละคราว และรับผิดชอบชำระค่าใช้จ่ายที่เกิดขึ้นจากการเข้าดำเนินการทั้งจำนวน

- 2.2 หากธนาคารพบว่าระบบมีช่องโหว่ที่เสี่ยงต่อการถูกโจมตี ผู้ยื่นข้อเสนอต้องดำเนินการแก้ไขและป้องกันไม่ให้มีช่องโหว่เกิดขึ้นในระบบ โดยผู้ยื่นข้อเสนอต้องไม่คิดค่าใช้จ่ายดำเนินการใด ๆ เพิ่มเติม ผู้ยื่นข้อเสนอจะต้องสนับสนุนการตรวจสอบด้าน Vulnerability Assessment (VA), Penetration Test (Pentest), Audit และ Compliance Review ที่เกี่ยวข้อง รวมถึงดำเนินการแก้ไขประเด็นที่ตรวจพบในระดับสถาปัตยกรรมภายในระยะเวลาที่ธนาคารกำหนด