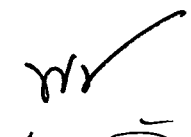
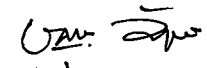
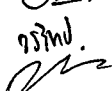


ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่ายการจ้างที่ปรึกษา

๑. ชื่อโครงการ แผนงาน โครงการจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบข้อเท็จจริงและทดสอบบุญกรูกระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล ประจำปี ๒๕๖๗
๒. หน่วยงานเจ้าของโครงการ ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่
๓. วงเงินงบประมาณที่ได้รับจัดสรร ๕๐๐,๐๐๐.- บาท (ห้าแสนบาทถ้วน)
๔. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ 24 เม.ย. 2567
เป็นเงิน ๔๗๘,๓๗๐.๒๕ บาท (สี่แสนเจ็ดหมื่นแปดพันสามร้อยเจ็ดสิบบาทยี่สิบห้าสตางค์)
(รวมภาษีมูลค่าเพิ่มแล้ว)
๕. ค่าตอบแทนบุคลากร ๔๗๘,๓๗๐.๒๕ บาท (สี่แสนเจ็ดหมื่นแปดพันสามร้อยเจ็ดสิบบาทยี่สิบห้าสตางค์)
 - ๕.๑ ประเภทที่ปรึกษากลุ่มวิชาชีพเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)
 - ๕.๒ คุณสมบัติที่ปรึกษาต้องประกอบธุรกิจด้านการให้คำปรึกษา ต้องเป็นผู้ที่มีความรู้ ความชำนาญ และประสบการณ์ด้านมาตรฐานความปลอดภัยสารสนเทศ
 - ๕.๓ จำนวนที่ปรึกษาไม่น้อยกว่า ๓ คน
๖. ค่าวัสดุอุปกรณ์ บาท
๗. ค่าใช้จ่ายในการเดินทางไปต่างประเทศ (ถ้ามี)บาท
๘. ค่าใช้จ่ายอื่นๆบาท
๙. รายชื่อผู้รับผิดชอบในการกำหนดค่าใช้จ่าย/ดำเนินการ/ขอบเขตดำเนินการ (TOR)
(ตามบันทึกข้อความที่ ศม.๐๔๖/๒๕๖๗ ลว. ๒๗ มี.ค. ๒๕๖๗)

๙.๑ นายพัลลภ ม่วงไหมทอง	ประธานกรรมการ	    
๙.๒ นายธีระชัย วิสุทธิพันธ์	กรรมการ	
๙.๓ นายวรวิทย์ วงศ์รัตนวัฒน์	กรรมการ	
๙.๔ นายชัยวัชร รัชญาอิสรานิ	กรรมการ	
๙.๕ นางสาวธนาภรณ์ พูลเลิศ	กรรมการและเลขานุการ	
๑๐. ที่มาของการกำหนดราคากลาง (ราคาอ้างอิง)
 - ๑๐.๑ หนังสือเลขที่ กค(กวจ)๐๔๐๕.๓/ว๑๒๐๓ ของกรมบัญชีกลาง
เรื่อง แนวทางการจ้างที่ปรึกษา ลว. ๒๗ กันยายน ๒๕๖๕

ขอบเขตงาน (Terms of Reference : TOR)

โครงการจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบงานบริการดิจิทัล
ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล ประจำปี 2567

เลขที่ 102-083/67

1. ความเป็นมา/เหตุผลและความจำเป็น

ด้วยศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ มีความประสงค์จะขอจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล โดยมีวงเงินงบประมาณ 500,000.00 บาท (ห้าแสนบาทถ้วน) เพื่อสร้างความน่าเชื่อถือ ด้านความมั่นคงปลอดภัยระบบสารสนเทศ จากลูกค้าธนาคาร และสอดคล้องตามมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 และประกาศธนาคารแห่งประเทศไทย ที่ สนส.21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน

2. วัตถุประสงค์

ธนาคารอาคารสงเคราะห์ ซึ่งต่อไปนี้จะเรียกว่า "ธนาคาร" มีความประสงค์จะจัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล โดยวัตถุประสงค์เพื่อทำการตรวจสอบและค้นหาจุดอ่อนที่สำคัญของระบบการรักษาความมั่นคงปลอดภัย และเพื่อให้ธนาคารทราบถึงข้อบกพร่อง และข้อเสนอแนะ ในการปรับปรุงแก้ไขระบบให้มีประสิทธิภาพและความปลอดภัยที่ดีตามมาตรฐานสากล

3. คุณสมบัติของผู้เสนอราคา

- 3.1 มีความสามารถตามกฎหมาย
- 3.2 ไม่เป็นบุคคลล้มละลาย
- 3.3 ไม่อยู่ระหว่างเลิกกิจการ
- 3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพตามที่จ้าง

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ธนาคาร ณ วันประกาศประกวดราคา หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคารั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น*

3.10 ผู้เสนอราคาต้องมีบุคลากรภายในทีมงานที่จะเข้ามาดำเนินการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล ไม่น้อยกว่า 2 ท่าน ที่มีประกาศนียบัตรที่เกี่ยวข้องด้านความมั่นคงปลอดภัย OSCP หรือ GPEN อย่างใดอย่างหนึ่ง หรือมีทั้ง 2 Certificate

3.11 ผู้เสนอราคาต้องมีประสบการณ์ทดสอบช่องโหว่ให้กับองค์กรหรือหน่วยงาน ไม่น้อยกว่า 1 หน่วยงาน และผู้เสนอราคาต้องแจ้งชื่อองค์กรหรือหน่วยงานดังกล่าวไว้ พร้อมสถานที่ติดตั้ง หมายเลขโทรศัพท์ ผู้ติดต่อ ให้ธนาคารทราบ เพื่อให้สามารถติดต่อได้

3.12 ผู้เสนอราคาต้องมีความรู้ความสามารถด้านเทคนิคและความชำนาญพิเศษเฉพาะด้าน และขึ้นทะเบียนที่ปรึกษาของสำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง

3.13 ผู้เสนอราคาจะต้องเก็บรักษาข้อมูลที่เกี่ยวข้องทั้งหมดของธนาคารไว้เป็นความลับ จะไปเผยแพร่ที่อื่นมิได้

4. หลักฐานการเสนอราคา

ผู้เสนอราคาจะต้องเสนอเอกสารหลักฐานยื่นมาพร้อมกับซองใบเสนอราคา โดยแยกไว้นอกซองใบเสนอราคาเป็น 2 ส่วน คือ

4.1 ส่วนที่ 1 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) ในกรณีผู้เสนอราคาเป็นนิติบุคคล

(ก) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล บัญชีรายชื่อหุ้นส่วนผู้จัดการ ผู้มีอำนาจควบคุม พร้อมรับรองสำเนาถูกต้อง

(ข) บริษัทจำกัดหรือบริษัทมหาชนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล หนังสือบริคณห์สนธิบัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุม และบัญชีผู้ถือหุ้นรายใหญ่ พร้อมรับรองสำเนาถูกต้อง

(2) ในกรณีผู้เสนอราคาเป็นบุคคลธรรมดาหรือคณะบุคคลที่มีโชตินิติบุคคล ให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้ยื่น สำเนาข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน พร้อมทั้งรับรองสำเนาถูกต้อง

(3) ในกรณีผู้เสนอราคาเป็นผู้เสนอราคาร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า สำเนาบัตรประจำตัวประชาชนของผู้ร่วมค้า และในกรณีที่ผู้เข้าร่วมค้าฝ่ายใดเป็นบุคคลธรรมดาที่มีโชติสัญชาติไทย ก็ให้ยื่นสำเนาหนังสือเดินทาง หรือผู้ร่วมค้าฝ่ายใดเป็นนิติบุคคลให้ยื่นเอกสารตามที่ระบุไว้ใน (1)

(4) บัญชีเอกสารส่วนที่ 1 ทั้งหมดที่ได้ยื่นพร้อมกับซองใบเสนอราคา

4.2 ส่วนที่ 2 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) แค็ตตาล็อกและหรือแบบรูปรายการละเอียดคุณลักษณะเฉพาะ

(2) หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมายในกรณีที่ผู้เสนอราคามอบอำนาจให้บุคคลอื่นลงนามในใบเสนอราคาแทน

(3) บัญชีเอกสารส่วนที่ 2 ทั้งหมดที่ได้ยื่นพร้อมกับซองใบเสนอราคา

5. คุณสมบัติเฉพาะ / รายละเอียดของงานจ้าง

5.1 ผู้เสนอราคาจะต้องเสนอรูปแบบการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบงานบริการดิจิทัล แก่ธนาคาร

(1) มีกระบวนการขั้นตอนในการทดสอบ

(2) มีมาตรฐานอ้างอิงในการทดสอบ เช่น SANS , OSCP , OWASP หรือมาตรฐานสากลอื่นๆ ที่เกี่ยวข้อง

5.2 รายละเอียดของ Proposal ควรประกอบด้วยหัวข้อ ดังต่อไปนี้

(1) ตารางเปรียบเทียบคุณสมบัติเฉพาะของการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากลตามที่ธนาคารกำหนด (ตามภาคผนวก 1)

(2) แผนการดำเนินงานทั้งหมด โดยต้องแบ่งแยกแผนการทำงานแต่ละงาน รายละเอียดงาน ช่วงเวลา และผู้รับผิดชอบในการเข้าปฏิบัติงาน และเบอร์ดิตต่อ (ตามภาคผนวก 1)

(3) เอกสารอื่นๆ (ถ้ามี) ที่ผู้เสนอราคาเห็นว่าจะประโยชน์ต่อการพิจารณาของธนาคาร

6. ระยะเวลาดำเนินการ/ส่งมอบงาน และการตรวจรับ

การดำเนินงานโครงการจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุญกรูกระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล มีระยะเวลาดำเนินงานทั้งสิ้น 200 วัน ตลอดระยะเวลาโครงการ นับถัดจากวันที่ลงนามในสัญญา ธนาคารจะแบ่งชำระเงินค่าจ้างบริการ โดยแบ่งการชำระออกเป็น 2 งวด มีรายละเอียด ดังนี้

งวดที่ 1: ชำระเงินเป็นจำนวน 50% ของมูลค่าโครงการ ฯ เมื่อผู้ได้รับการคัดเลือกได้ส่งมอบงานงวดที่ 1 ภายในระยะเวลา 90 วัน นับถัดจากวันลงนามในสัญญา และเมื่อคณะกรรมการตรวจรับ ตรวจรับงานถูกต้องครบถ้วนตรงตามเงื่อนไขของสัญญาจ้าง ตามที่ระบุไว้ในผนวก 1.

งวดที่ 2: ชำระเงินเป็นจำนวน 50% ของมูลค่าโครงการ ฯ เมื่อผู้ได้รับการคัดเลือกได้ส่งมอบงานงวดที่ 2 ภายในระยะเวลา 200 วัน นับถัดจากวันลงนามในสัญญา และเมื่อคณะกรรมการตรวจรับ ตรวจรับงานถูกต้องครบถ้วนตรงตามเงื่อนไขของสัญญาจ้าง ตามที่ระบุไว้ในผนวก 1.

เมื่อธนาคารได้ตรวจรับมอบการสอบทานการตรวจสอบช่องโหว่และทดสอบบุญกรูกระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากลถูกต้องครบถ้วนตามสัญญาจ้าง แล้วธนาคารจะออกหลักฐานการรับมอบไว้เป็นหนังสือ เพื่อยืนยันข้อเสนอแนะมาใช้เป็นหลักฐานประกอบการขอรับเงินค่าจ้างโครงการจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุญกรูกระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล

7. การทำสัญญา

ผู้ได้รับการคัดเลือกจะต้องติดต่อธนาคารเพื่อทำสัญญาภายใน 7 วัน นับถัดจากวันที่ได้รับแจ้ง และจะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละ 5 ของมูลค่าสัญญา และให้ธนาคารยึดถือไว้ในขณะทำสัญญา โดยใช้หลักประกันอย่างหนึ่งอย่างใด ดังต่อไปนี้

7.1 เงินสด

7.2 เช็คหรือตราพดที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือตราพดที่ลงวันที่ที่ใช้เช็คหรือตราพดนั้น ชำระต่อเจ้าหน้าที่ หรือก่อนหน้านั้นไม่เกิน 3 วันทำการ

7.3 หนังสือค้ำประกันของธนาคารภายในประเทศตามตัวอย่างที่คณะกรรมการนโยบายกำหนด โดยอาจเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนดก็ได้

7.4 หนังสือค้ำประกันของบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

7.5 พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้โดยไม่มีดอกเบี้ย ภายใน 15 วัน นับถัดจากวันที่คู่สัญญาพ้นจากข้อผูกพันตามสัญญาแล้ว

ทั้งนี้ หากผู้ได้รับการคัดเลือกไม่ดำเนินการภายในระยะเวลาดังกล่าวข้างต้น ธนาคารสงวนสิทธิ์ที่จะยกเลิกการจ้าง และพิจารณาแจ้งเป็นผู้ทำงาน

8. เงื่อนไขการชำระเงิน

โครงการจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุญคุณระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล จะแบ่งการชำระออกเป็น 2 งวด โดยมีรายละเอียดดังนี้

งวดที่ 1: ชำระเงินเป็นจำนวน 50% ของมูลค่าโครงการจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุญคุณระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล เป็นจำนวนเงินทั้งสิ้น (.....) บาท (.....) (รวมภาษีมูลค่าเพิ่มแล้ว) เมื่อผู้เสนอราคาได้ทำการส่งมอบงานงวดที่ 1 (ตามภาคผนวก 1: ระยะเวลาของโครงการ ข้อ 5.1) ภายในระยะเวลา 90 วัน ให้แก่ธนาคาร และคณะกรรมการตรวจรับ ได้ตรวจสอบคุณสมบัติถูกต้องครบถ้วนตามที่ระบุไว้ในสัญญาจ้าง และกรรมการตรวจรับเห็นว่าถูกต้องตรงตามเงื่อนไขของสัญญาจ้าง

งวดที่ 2: ชำระเงินเป็นจำนวน 50% ของมูลค่าโครงการจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุญคุณระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล เป็นจำนวนเงินทั้งสิ้น (.....) บาท (.....) (รวมภาษีมูลค่าเพิ่มแล้ว) เมื่อผู้เสนอราคาได้ทำการส่งมอบงานงวดที่ 2 (ตามภาคผนวก 1: ระยะเวลาของโครงการ ข้อ 5.2) ภายในระยะเวลา 200 วัน ให้แก่ธนาคาร และคณะกรรมการตรวจรับ ได้ตรวจสอบคุณสมบัติถูกต้องครบถ้วนตามที่ระบุไว้ในสัญญาจ้าง และกรรมการตรวจรับเห็นว่าถูกต้องตรงตามเงื่อนไขของสัญญาจ้าง

การชำระเงิน ดังกล่าวข้างต้น ต้องรับจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การรับจ่ายเงินแต่ละครั้ง ซึ่งมีมูลค่าไม่เกิน 30,000 บาท อาจรับจ่ายเป็นเงินสดได้

9. วงเงินในการจัดหา

วงเงินงบประมาณ 500,000.00 บาท (ห้าแสนบาทถ้วน) (เฉพาะที่ใช้ในการจัดซื้อ จัดจ้างครั้งนี้)

10. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ธนาคารจะพิจารณาตัดสินโดยใช้เกณฑ์ราคา

11. อัตราค่าปรับ

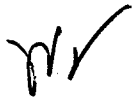
ค่าปรับตามแบบสัญญาจ้าง ให้คิดเป็นรายวันในอัตราร้อยละ 0.10 ของราคางานจ้าง
เศษของวันให้คิดเป็นรายชั่วโมง โดย 1 วัน เท่ากับ 24 ชั่วโมง แต่จะต้องไม่ต่ำกว่าวันละ 100.- บาท

12. การรับประกันความชำรุดบกพร่อง

ผู้ได้รับการคัดเลือกซึ่งได้ทำสัญญากับธนาคาร จะต้องรับประกันความชำรุดบกพร่อง
ของสิ่งของงานจ้างที่เกิดขึ้นภายในระยะเวลาไม่น้อยกว่า 120 วัน นับถัดจากวันที่ธนาคารได้รับมอบงาน

13. หน่วยงานที่รับผิดชอบ

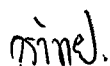
ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์ (สำนักงานใหญ่)
63 ถนนพระราม 9 ห้วยขวาง กรุงเทพฯ 10310 โทร. 022021735



นายพัลลภ ม่วงไหมทอง

หัวหน้าส่วนดูแลมาตรฐานความมั่นคงปลอดภัย
กฎข้อบังคับและประเมินความเสี่ยงระบบสารสนเทศ

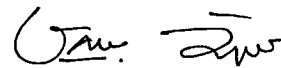
ประธานกรรมการ



นายวรวิทย์ วงศ์รัตนวัฒน์

พนักงานคอมพิวเตอร์อาวุโส

กรรมการ



นายธีระชัย วิสุทธิพันธ์

ผู้ช่วยหัวหน้าส่วนฯ

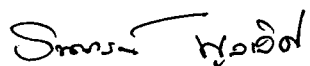
กรรมการ



นายชัยวัชร รัชญาอิสราณี

พนักงานคอมพิวเตอร์

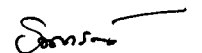
กรรมการ



นางสาวธนาภรณ์ พูลเลิศ

พนักงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

กรรมการและเลขานุการ



ผนวก 1.

รายละเอียดและคุณลักษณะเฉพาะของโครงการจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล ประจำปี 2567

1. วัตถุประสงค์ของโครงการ

- 1.1 เพื่อทำการตรวจสอบและค้นหาจุดอ่อนที่สำคัญของระบบการรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่ายระบบงาน และ Mobile Application ในโครงการจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล ของธนาคาร
- 1.2 เพื่อให้ธนาคารทราบถึงข้อบกพร่อง และข้อเสนอแนะ ในการปรับปรุงแก้ไขระบบ ให้มีประสิทธิภาพและความปลอดภัยที่ดีตามมาตรฐานสากล
- 1.3 เพื่อเพิ่มประสิทธิภาพการทำงาน และให้ธนาคารมีแนวทางการปฏิบัติงานตามเกณฑ์มาตรฐานสากล เป็นที่ยอมรับจากสถาบันที่มีหน้าที่กำกับและตรวจสอบธนาคาร ตลอดจนพัฒนาบุคลากรให้ได้รับความรู้ความเข้าใจเกี่ยวกับการปฏิบัติงาน และการป้องกันระบบงานสารสนเทศ

2. เป้าหมายของโครงการ

- 2.1 เพื่อให้ธนาคารทราบข้อมูลจุดอ่อนที่สำคัญของระบบการรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัลของธนาคาร
- 2.2 เพื่อให้ธนาคารทราบถึงข้อบกพร่อง และข้อเสนอแนะ ในการปรับปรุงแก้ไข เครื่องแม่ข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัลของธนาคาร ให้มีประสิทธิภาพและความปลอดภัยที่ดีตามมาตรฐานสากล
- 2.3 ธนาคารมีกระบวนการจัดการด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ จะสามารถช่วยทีม IT ของธนาคารเพิ่มประสิทธิภาพในการให้บริการและการดำเนินงาน ลดปัญหาของการเกิด การละเมิดความมั่นคงปลอดภัยสารสนเทศและการเกิด Incident ได้

3. ขอบเขตการดำเนินงาน

ขอบเขตของการดำเนินงานโครงการจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล ประกอบด้วย

- (1) เครื่องแม่ข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัลของธนาคาร
- (2) Module ใหม่ที่พัฒนาเพิ่มเติม ใน Mobile Application และระบบงานบริการดิจิทัลของธนาคาร ภายในระยะเวลา 200 วัน นับถัดจากวันที่ลงนามในสัญญาและอยู่ในขอบเขตระยะเวลาของโครงการ
- (3) เป้าหมายการดำเนินงานทั้งหมดจะเป็นระบบงานของธนาคารเท่านั้น โดยอุปกรณ์คอมพิวเตอร์ หรือ Software ที่นำมาใช้ในการดำเนินงานตามขอบเขตงาน บริษัทผู้รับงานจะต้องเป็นผู้จัดหา มาทั้งสิ้น

4. วิธีการดำเนินงาน

4.1 ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของเครื่องแม่ข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัลของธนาคาร ในภาพรวมครั้งแรก ภายในระยะเวลา 90 วัน นับถัดจากวันที่ลงนามในสัญญา เพื่อให้ธนาคารรับทราบความเสี่ยง หรือช่องโหว่ในสภาพปัจจุบัน โดยมีรายละเอียดดังนี้

- (1) ทดสอบบุกรุกระบบ (Penetration Testing) เครื่องแม่ข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัลของธนาคาร โดยการทำงานจะต้องครอบคลุมการทดสอบหาเป้าหมายทั้งแบบทางตรงและทางอ้อม
- (2) จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก ภาพรวมและผลกระทบ ของช่องโหว่ที่ตรวจพบ พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง โดยวิเคราะห์ผลจะต้องสอดคล้อง หรือต้องอ้างอิงตาม OWASP หรือมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ และส่งมอบให้กับธนาคารเพื่อให้ธนาคารนำข้อมูลช่องโหว่ที่ตรวจพบไปดำเนินการแก้ไขปรับปรุงให้มีความปลอดภัย และรายงานผลให้ธนาคารรับทราบ
- (3) ดำเนินการตรวจสอบซ้ำ จากผลการแก้ไขในครั้งแรก เพื่อยืนยันความถูกต้องของการแก้ไข และรายงานผลให้ธนาคารรับทราบ
- (4) จัดส่งรายงานผลการทดสอบฉบับสมบูรณ์ให้กับธนาคาร

4.2 ดำเนินการทดสอบบุกรุกระบบเครื่องแม่ข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัลของธนาคาร เมื่อธนาคารมีการพัฒนา Module ใหม่ หรือเมื่อธนาคารมีความ

ต้องการให้ทำการทดสอบด้านความปลอดภัยเครื่องมือข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัลตามที่ธนาคารกำหนด เป็นจำนวนทั้งสิ้น 1 ครั้ง ภายในระยะเวลา 200 วัน นับถัดจากวันที่ลงนามในสัญญา โดยมีรายละเอียดดังนี้

- (1) การดำเนินการทดสอบบุกรุกระบบ เครื่องข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัลของธนาคาร จะแจ้งให้ทราบล่วงหน้าอย่างน้อยเป็นเวลา 7 วัน ก่อนเริ่มทำการทดสอบ เพื่อให้บริษัทผู้รับจ้างเตรียมความพร้อมก่อนเข้าดำเนินการ
- (2) จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก ภาพรวมและผลกระทบ ของช่องโหว่ที่ตรวจพบ พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง โดยวิเคราะห์ผลจะต้องสอดคล้องหรือต้องอ้างอิงตาม OWASP หรือมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ และส่งมอบให้กับธนาคารเพื่อให้ธนาคารนำข้อมูลช่องโหว่ที่ตรวจพบไปดำเนินการแก้ไขปรับปรุงให้มีความปลอดภัย และรายงานผลให้ธนาคารรับทราบ
- (3) ดำเนินการตรวจสอบซ้ำ จากผลการแก้ไขใน เพื่อยืนยันความถูกต้องของการแก้ไข และรายงานผลให้ธนาคารรับทราบ

5. ระยะเวลาของโครงการ

การดำเนินงานโครงการจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบงานบริการดิจิทัล ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล มีระยะเวลาดำเนินงานทั้งสิ้น 200 วัน ตลอดระยะเวลาโครงการ นับถัดจากวันที่ลงนามในสัญญา โดยการดำเนินการจะแบ่งเป็น 2 ครั้ง ดังนี้

5.1 ครั้งที่ 1 : เวลาดำเนินงานทั้งสิ้น 90 วัน (นับถัดจากวันที่ลงนามในสัญญา)

ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของเครื่องมือข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัลของธนาคาร ในภาพรวมครั้งแรก เพื่อให้ธนาคารรับทราบความเสี่ยง หรือช่องโหว่ในสภาพปัจจุบัน โดยมีรายละเอียดดังนี้

- (1) ทดสอบบุกรุกระบบ เครื่องข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัลของธนาคาร ทั้งจากภายนอก และจากภายในธนาคารแบบ White-Box Penetration Testing การดำเนินงานจะต้องครอบคลุมการทดสอบหาเป้าหมายทั้งแบบทางตรงและทางอ้อม
- (2) จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก ภาพรวมและผลกระทบ ของช่องโหว่ที่ตรวจพบ พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง โดยวิเคราะห์ผลจะต้องสอดคล้อง

- หรือต้องอ้างอิงตาม OWASP หรือมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ และส่งมอบให้กับธนาคารเพื่อให้ธนาคารนำข้อมูลช่องโหว่ที่ตรวจพบไปดำเนินการแก้ไขปรับปรุงให้มีความปลอดภัย และรายงานผลให้ธนาคารรับทราบ
- (3) ดำเนินการตรวจสอบซ้ำ จากผลการแก้ไขในครั้งแรก เพื่อยืนยันความถูกต้องของการแก้ไข และรายงานผลให้ธนาคารรับทราบ

5.2 ครั้งที่ 2 : เวลาดำเนินงานทั้งสิ้น 200 วัน (นับถัดจากวันที่ลงนามในสัญญา)

ดำเนินการทดสอบบุกรุกระบบเครื่องแม่ข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัลของธนาคาร เมื่อธนาคารมีการพัฒนา Module ใหม่ หรือเมื่อธนาคารมีความต้องการให้ทำการทดสอบด้านความปลอดภัยเครื่องแม่ข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัล ตามที่ธนาคารกำหนด เป็นจำนวน 1 ครั้ง โดยมีรายละเอียดดังนี้

- (1) การดำเนินการทดสอบบุกรุกเครื่องแม่ข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัลของธนาคาร แต่ละครั้งธนาคารจะแจ้งให้ทราบล่วงหน้าอย่างน้อยเป็นเวลา 7 วันก่อนเริ่มทำการทดสอบ เพื่อให้บริษัทผู้รับจ้างเตรียมความพร้อมก่อนเข้าดำเนินการ
- (2) จัดทำรายงาน ที่แสดงขั้นตอนวิธีการในการบุกรุก ภาพรวมและผลกระทบ ของช่องโหว่ที่ตรวจพบ พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง โดยวิเคราะห์ผลจะต้องสอดคล้องหรือต้องอ้างอิงตาม OWASP หรือมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ และส่งมอบให้กับธนาคาร เพื่อให้ธนาคารนำข้อมูลช่องโหว่ที่ตรวจพบไปดำเนินการแก้ไขปรับปรุงให้มีความปลอดภัย และรายงานผลให้ธนาคารรับทราบ
- (3) ดำเนินการตรวจสอบซ้ำ จากผลการแก้ไขใน เพื่อยืนยันความถูกต้องของการแก้ไข และรายงานผลให้ธนาคารรับทราบ

6. งานที่ต้องส่งมอบ

6.1 ครั้งที่ 1 : ส่งมอบงานภายใน 90 วัน นับถัดจากวันที่ลงนามในสัญญา ตามวิธีการดำเนินงาน ข้อ 4.1

- รายงานผลการวิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของเครื่องแม่ข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัล ของธนาคาร (ฉบับภาษาไทย)

6.2 ครั้งที่ 2 : ส่งมอบงานภายใน 200 วัน นับถัดจากวันที่ลงนามในสัญญา ตามวิธีการดำเนินงาน ข้อ 4.2

- รายงานผลการวิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของเครื่องแม่ข่ายระบบงาน , Mobile Application และระบบงานบริการดิจิทัล ของธนาคาร (ฉบับภาษาไทย)

6.3 สิ่งที่ต้องส่งมอบตามวิธีการดำเนินงานข้อ 4.1 ข้อ 4.2 (ส่งมอบงานภายใน 200 วัน นับถัดจากวันที่ลงนามในสัญญา) ส่งมอบ File เอกสารต่าง ๆ ฉบับสมบูรณ์ ที่ส่งมอบตามข้อ 4.1 ข้อ 4.2 ต้องสามารถเปิดและแก้ไขด้วยชุดโปรแกรมจาก Microsoft office ตั้งแต่ Version 2016 ขึ้นไป บรรจุใน USB Drive อย่างละ 1 ชุด (ฉบับภาษาไทย) แนบมาในแฟ้มงาน