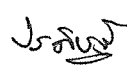
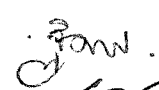


ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่ายการจ้างที่ปรึกษา

1. ชื่อโครงการ แผนงานจ้างที่ปรึกษาสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3
ให้มีความปลอดภัย ตามเกณฑ์มาตรฐานสากล ประจำปี 2566
2. หน่วยงานเจ้าของโครงการ ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่
3. วงเงินงบประมาณที่ได้รับจัดสรร 500,000.- บาท (ห้าแสนบาทถ้วน)
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ ...-...19 ก.ค. 2566.....
เป็นเงิน 498,960.- บาท (สี่แสนเก้าหมื่นแปดพันเก้าร้อยหกสิบบาทถ้วน) (รวมภาษีมูลค่าเพิ่มแล้ว)
5. ค่าตอบแทนบุคลากร.. 498,960.- บาท (สี่แสนเก้าหมื่นแปดพันเก้าร้อยหกสิบบาทถ้วน)
 - 5.1 ประเภทที่ปรึกษากลุ่มวิชาชีพเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)
 - 5.2 คุณสมบัติที่ปรึกษาต้องประกอบธุรกิจด้านการให้คำปรึกษา ต้องเป็นผู้ที่มีความรู้ ความชำนาญ
และประสบการณ์ด้านมาตรฐานความปลอดภัยสารสนเทศ
 - 5.3 จำนวนที่ปรึกษาไม่น้อยกว่า 4 คน
6. ค่าวัสดุอุปกรณ์-..... บาท
7. ค่าใช้จ่ายในการเดินทางไปต่างประเทศ (ถ้ามี)-.....บาท
8. ค่าใช้จ่ายอื่นๆ-.....บาท
9. รายชื่อผู้รับผิดชอบในการกำหนดค่าใช้จ่าย/ดำเนินการ/ขอบเขตดำเนินการ (TOR)
(ตามบันทึกข้อความที่ ศม.075/2566 ลว. 27 เม.ย.2566)

9.1 นายพัลลภ ม่วงไหมทอง	ประธานกรรมการ	
9.2 นายประดิษฐ์ นิธิคุณไชย	กรรมการ	
9.3 นางสาวฐิมาพร โชติวิจิณชัย	กรรมการ	
9.4 นายศศิศ ตระกูลวรานนท์	กรรมการ	
9.5 นางสาวธนาภรณ์ พูลเลิศ	กรรมการและเลขานุการ	สมร พูลเลิศ
10. ที่มาของการกำหนดราคากลาง (ราคาอ้างอิง)
 - 10.1 หนังสือจากสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร.0506/ว 128 ลว.8 สิงหาคม 2556

ร่างเอกสารขอบเขตงาน (Terms of Reference : TOR)

โครงการจ้างที่ปรึกษาสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3

ให้มีความปลอดภัยตามเกณฑ์มาตรฐานสากล ประจำปี 2566

เลขที่ 102-124/66

1. ความเป็นมา/เหตุผลและความจำเป็น

ด้วยศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ มีความประสงค์จะขอจ้างที่ปรึกษาเพื่อสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล โดยมีวงเงินงบประมาณ 500,000.00 บาท (ห้าแสนบาทถ้วน) เพื่อสร้างความน่าเชื่อถือ ด้านความมั่นคงปลอดภัยระบบสารสนเทศ จากลูกค้าธนาคาร และสอดคล้องตามมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2013 และประกาศธนาคารแห่งประเทศไทย ที่ สนส.21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน

2. วัตถุประสงค์

ธนาคารอาคารสงเคราะห์ ซึ่งต่อไปนี้จะเรียกว่า "ธนาคาร" มีความประสงค์จะจัดจ้างที่ปรึกษาเพื่อสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 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 หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการประกวดราคาค้างนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

3.10 ผู้เสนอราคาต้องมีบุคลากรภายในทีมงานที่จะเข้ามาดำเนินการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ไม่น้อยกว่า 2 ท่าน ที่มีประกาศนียบัตรที่เกี่ยวข้องด้านความมั่นคงปลอดภัย OSCP หรือ GPEN อย่างใดอย่างหนึ่ง หรือมีทั้ง 2 Certificate

3.11 ผู้เสนอราคาต้องมีประสบการณ์ทดสอบช่องโหว่ให้กับองค์กรหรือหน่วยงาน ไม่น้อยกว่า 1 หน่วยงาน และผู้เสนอราคาต้องแจ้งชื่อองค์กรหรือหน่วยงานดังกล่าวนั้น พร้อมสถานที่ติดตั้งหมายเลขโทรศัพท์ 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 หนังสือบริคณห์สนธิบัญชีรายการกรรมการผู้จัดการ ผู้มีอำนาจควบคุม และบัญชีผู้ถือหุ้นรายใหญ่ พร้อมรับรองสำเนาถูกต้อง

(2) ในกรณีผู้เสนอราคาเป็นบุคคลธรรมดาหรือคณะบุคคลที่มีโชตินิติบุคคล ให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้ยื่น สำเนาข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน พร้อมทั้งรับรองสำเนาถูกต้อง

(3) ในกรณีผู้เสนอราคาเป็นผู้เสนอราคาร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า สำเนาบัตรประจำตัวประชาชนของผู้ร่วมค้า และในกรณีที่ผู้เข้าร่วมค้าฝ่ายใดเป็นบุคคลธรรมดาที่มีเชื้อสายชาติไทย 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 ผู้เสนอราคาจะต้องเสนอรูปแบบการทดสอบบุกรุกระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 แก่ธนาคาร

- มีกระบวนการขั้นตอนในการทดสอบ
- มีมาตรฐานอ้างอิงในการทดสอบ เช่น SANS , OSCP , OWASP หรือมาตรฐานสากลอื่นๆที่เกี่ยวข้อง

5.2 รายละเอียดของ Proposal ควรประกอบด้วยหัวข้อ ดังต่อไปนี้

- ตารางเปรียบเทียบคุณลักษณะเฉพาะของการสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ให้มีความปลอดภัย ตามเกณฑ์มาตรฐานสากลตามที่ธนาคารกำหนด (ตามภาคผนวก 1)
- แผนการดำเนินงานทั้งหมด โดยต้องแบ่งแยกแผนการทำงานแต่ละงาน รายละเอียดงาน ช่วงเวลาและผู้รับผิดชอบในการเข้าปฏิบัติงาน และเบอร์ดติดต่อ (ตามภาคผนวก 1)
- เอกสารอื่นๆ (ถ้ามี) ที่ผู้เสนอราคาเห็นว่าจะเป็นประโยชน์ต่อการพิจารณาของธนาคาร

6. ระยะเวลาดำเนินการ/ส่งมอบงาน และการตรวจรับ

การดำเนินงานสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ของธนาคาร ให้มีความปลอดภัยตามเกณฑ์มาตรฐานสากล มีระยะเวลาดำเนินงานทั้งสิ้น 180 วัน ตลอดระยะเวลาโครงการ นับถัดจากวันที่ลงนามในสัญญา โดยการดำเนินการจะแบ่งเป็น 2 ครั้ง ดังนี้

- ครั้งที่ 1 : เวลาดำเนินงานทั้งสิ้น 90 วัน (นับถัดจากวันที่ลงนามในสัญญา)
 - ดำเนินการตรวจสอบ วิเคราะห์ อุปกรณ์ความมั่นคงปลอดภัยและเครื่องแม่ข่ายในระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ของธนาคาร (รายละเอียดตามภาคผนวก 1: วิธีการดำเนินงาน ข้อ 4.1)
 - ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ที่ธนาคารกำหนด จำนวนไม่เกิน 10 หมายเลขไอพี (รายละเอียดตามภาคผนวก 1: วิธีการดำเนินงาน ข้อ 4.2)
 - ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) จากระบบจากภายนอกแบบ Black-Box Penetration Testing และทำการทดสอบเจาะระบบจากภายในธนาคารแบบ White-Box Penetration Testing ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 หรือที่ธนาคารกำหนด จำนวนไม่เกิน 10 หมายเลขไอพี (รายละเอียดตามภาคผนวก 1: วิธีการดำเนินงาน ข้อ 4.3)
- ครั้งที่ 2 : เวลาดำเนินงานทั้งสิ้น 180 วัน (นับถัดจากวันที่ลงนามในสัญญา)
 - ดำเนินการทดสอบบุกรุกและประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 หรือเมื่อธนาคารมีการพัฒนา Module ใหม่ หรือเมื่อธนาคารมีความต้องการให้ทำการทดสอบด้านความปลอดภัยในระบบบริการดิจิทัลและระบบงาน GHB ALL GEN ตามที่ธนาคารกำหนด เป็นจำนวนทั้งสิ้น 1 ครั้ง (รายละเอียดตามภาคผนวก 1: วิธีการดำเนินงาน ข้อ 4.4)

เมื่อธนาคารได้ตรวจรับมอบผลการสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ให้มีความปลอดภัยตามเกณฑ์มาตรฐานสากล ถูกต้องครบถ้วนตามสัญญาจ้างแล้ว ธนาคารจะออกหลักฐานการรับมอบไว้เป็นหนังสือ เพื่อผู้เสนอราคานำมาใช้เป็นหลักฐานประกอบการขอรับเงินค่าจ้างสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 หรือให้มีความปลอดภัยตามเกณฑ์มาตรฐานสากล

7. การทำสัญญา

ผู้ได้รับการคัดเลือกจะต้องติดต่อธนาคารเพื่อทำสัญญาภายใน 7 วัน นับถัดจากวันที่ได้รับแจ้ง และจะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละ 5 ของมูลค่าสัญญา และให้ธนาคารยึดถือไว้ในขณะทำสัญญา โดยใช้หลักประกันอย่างหนึ่งอย่างใด ดังต่อไปนี้

7.1 เงินสด

7.2 เช็คหรือตราพดที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือตราพดที่ลงวันที่ที่ใช้เช็คหรือตราพดนั้นชำระต่อเจ้าหนี้ หรือก่อนหน้านั้นไม่เกิน 3 วัน ทำการ

7.3 หนังสือค้ำประกันของธนาคารภายในประเทศตามตัวอย่างที่คณะกรรมการนโยบายกำหนด โดยอาจเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนดก็ได้

7.4 หนังสือค้ำประกันของบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

7.5 พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้โดยไม่มีดอกเบี้ย ภายใน 15 วัน นับถัดจากวันที่คู่สัญญาพ้นจากข้อผูกพันตามสัญญาแล้ว

ทั้งนี้ หากผู้ได้รับการคัดเลือกไม่ดำเนินการภายในระยะเวลาดังกล่าวข้างต้น ธนาคารสงวนสิทธิ์ที่จะยกเลิกการจ้าง และพิจารณาแจ้งเป็นผู้ทิ้งงาน

8. เงื่อนไขการชำระเงิน

โครงการจัดจ้างที่ปรึกษาสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ให้มีความปลอดภัยตามเกณฑ์มาตรฐานสากล จะแบ่งการชำระออกเป็น 2 งวด โดยมีรายละเอียดดังนี้

งวดที่ 1: ชำระเงินเป็นจำนวน 50% ของมูลค่าโครงการจัดจ้างที่ปรึกษาสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ให้มีความปลอดภัยตามเกณฑ์มาตรฐานสากล เป็นจำนวนเงินทั้งสิ้น (.....) บาท(.....) (รวมภาษีมูลค่าเพิ่มแล้ว) เมื่อผู้เสนอราคาได้ทำการส่งมอบงานงวดที่ 1 (ตามภาคผนวก 1: ระยะเวลาของโครงการ ข้อ 5.1) ภายในระยะเวลา 90 วัน ให้แก่ธนาคาร และคณะกรรมการตรวจรับ ได้ตรวจสอบคุณสมบัติถูกต้องครบถ้วนตามที่ระบุไว้ในสัญญาจ้าง และกรรมการตรวจรับเห็นว่าถูกต้องตรงตามเงื่อนไขของสัญญาจ้าง



งวดที่ 2: ชำระเงินเป็นจำนวน 50% ของมูลค่าโครงการจัดจ้างที่ปรึกษาสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ให้มีความปลอดภัยตามเกณฑ์มาตรฐานสากล เป็นจำนวนเงินทั้งสิ้น (.....) บาท(.....) (รวมภาษีมูลค่าเพิ่มแล้ว) เมื่อผู้เสนอราคาได้ทำการส่งมอบงานงวดที่ 2 (ตามภาคผนวก 1: ระยะเวลาของโครงการ ข้อ 5.2) ภายในระยะเวลา 180 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

ธนาคารจะพิจารณาคัดสินโดยใช้เกณฑ์ราคา

11. อัตราค่าปรับ

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

12. การรับประกันความชำรุดบกพร่อง

ผู้ได้รับการคัดเลือกซึ่งได้ทำสัญญากับธนาคาร จะต้องรับประกันความชำรุดบกพร่องของสิ่งของงานจ้างที่เกิดขึ้นภายในระยะเวลาไม่น้อยกว่า 120 วัน นับถัดจากวันที่ธนาคารได้รับมอบงาน

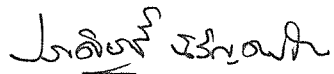
13. หน่วยงานที่รับผิดชอบ

ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์ (สำนักงานใหญ่)

63 ถนนพระราม 9 ห้วยขวาง กรุงเทพฯ 10310 โทร. 022021735

()

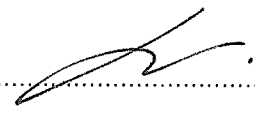
นายพัลลภ ม่วงไหมทอง
หัวหน้าส่วนดูแลมาตรฐานความมั่นคงปลอดภัยฯ
ประธานกรรมการ

()

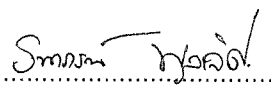
นายประติษฐ์ นิรัตดอนไชย
ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย
เทคโนโลยีสารสนเทศ
กรรมการ

()

นางสาวสุวิมาพร ไชติวินิจัย
พนักงานคอมพิวเตอร์อาวุโส
กรรมการ

()

นายศศิ์ ตระกูลวรานนท์
นักพัฒนาระบบ
กรรมการ

()

นางสาวธนาภรณ์ พูลเลิศ
พนักงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
กรรมการและเลขานุการ

ผนวก 1.

รายละเอียดและคุณลักษณะเฉพาะโครงการจ้างที่ปรึกษาสอบทานระบบบริการดิจิทัลและระบบงาน
GHB ALL GEN Phase 3 ให้มีความปลอดภัยตามเกณฑ์มาตรฐานสากล ประจำปี 2566

1. วัตถุประสงค์ของโครงการ

- 1.1 เพื่อทำการตรวจสอบและค้นหาจุดอ่อนที่สำคัญของระบบการรักษาความมั่นคงปลอดภัยของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3
- 1.2 เพื่อทำการตรวจสอบและค้นหาจุดอ่อนที่สำคัญของอุปกรณ์ความมั่นคงปลอดภัยและเครือข่ายของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3
- 1.3 เพื่อให้ธนาคารทราบถึงข้อบกพร่อง และข้อเสนอแนะ ในการปรับปรุงแก้ไขระบบให้มีประสิทธิภาพและความปลอดภัยที่ดีตามมาตรฐานสากล
- 1.4 เพื่อเพิ่มประสิทธิภาพการทำงาน และให้ธนาคารมีแนวทางการปฏิบัติงานตามเกณฑ์มาตรฐานสากล เป็นที่ยอมรับจากสถาบันที่มีหน้าที่กำกับและตรวจสอบธนาคาร ตลอดจนพัฒนาบุคลากรให้ได้รับความรู้ความเข้าใจเกี่ยวกับการปฏิบัติงาน และการป้องกันระบบงานสารสนเทศ

2. เป้าหมายของโครงการ

- 2.1 เพื่อให้ธนาคารทราบข้อมูลจุดอ่อนที่สำคัญของระบบการรักษาความมั่นคงปลอดภัยของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3
- 2.2 เพื่อให้ธนาคารทราบถึงข้อบกพร่อง และข้อเสนอแนะ ในการปรับปรุงแก้ไข ระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ให้มีประสิทธิภาพและความปลอดภัยที่ดีตามมาตรฐานสากล
- 2.3 ธนาคารมีกระบวนการจัดการด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ จะสามารถช่วยทีม IT ของธนาคารเพิ่มประสิทธิภาพในการให้บริการและการดำเนินงาน ลดปัญหาของการเกิดการละเมิดความมั่นคงปลอดภัยสารสนเทศและการเกิด Incident ได้



3. ขอบเขตการดำเนินงาน

ขอบเขตของการดำเนินงานสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ให้มีความปลอดภัยตามเกณฑ์มาตรฐานสากล ประกอบด้วย

- ระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ของธนาคาร
- อุปกรณ์ความมั่นคงปลอดภัยและเครื่องแม่ข่าย ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ของธนาคาร
- เป้าหมายการดำเนินงานทั้งหมดจะเป็นระบบงานของธนาคารเท่านั้น โดยอุปกรณ์คอมพิวเตอร์ หรือ Software ที่นำมาใช้ในการดำเนินงานตามขอบเขตงาน บริษัทผู้รับงานจะต้องเป็นผู้จัดหา มาทั้งสิ้น

4. วิธีการดำเนินงาน

4.1 ดำเนินการตรวจสอบ วิเคราะห์ อุปกรณ์ความมั่นคงปลอดภัยและเครื่องแม่ข่าย ในระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ของธนาคาร โดยมีรายละเอียดดังนี้

- ต้องทำการตรวจสอบและวิเคราะห์การตั้งค่าของอุปกรณ์ไฟร์วอลล์ (Policy Firewall) ตามขอบเขตของโครงการจำนวนไม่เกิน 1 อุปกรณ์
- ต้องทำการตรวจสอบและวิเคราะห์การตั้งค่าเครื่องแม่ข่ายตามเอกสาร (Hardening) ที่กำหนด โดยจำนวนเครื่องแม่ข่ายไม่เกิน 5 อุปกรณ์

4.2 ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ที่ธนาคารกำหนด จำนวนไม่เกิน 10 หมายเลขไอพี โดยจะต้องดำเนินการ ดังต่อไปนี้

- ใช้เครื่องมือตรวจสอบช่องโหว่ (Scanning Tool) จำนวน 1 ชนิด ซึ่งต้องเป็นเครื่องมือที่เป็น Commercial มีการใช้งานแพร่หลาย เช่น Nessus หรือ Nexpose
- จัดทำผลสรุปภาพรวมการทดสอบสำหรับผู้บริหาร (Executive Summary) รวมถึงเสนอ แผนในการแก้ไขระยะสั้น และระยะยาว วิเคราะห์ผลสำหรับผู้ดูแลระบบ โดยมีรายละเอียดดังนี้
 - จัดลำดับความเสี่ยงที่ต้องเร่งดำเนินการแก้ไข แยกตามประเภทอุปกรณ์ เครือข่าย/เครื่องแม่ข่าย และเรียงตามลำดับหมายเลขไอพี ที่ตรวจพบความเสี่ยงมากที่สุดไปน้อยที่สุด

- รายละเอียดช่องโหว่ที่ตรวจพบในแต่ละอุปกรณ์เครือข่าย/เครื่องแม่ข่าย พร้อมทั้งให้คำแนะนำการปรับปรุงระบบหรือการแก้ไขช่องโหว่ที่ตรวจพบหรือแนวทางในการลดความเสี่ยงที่เกิดขึ้น
- รายละเอียดช่องโหว่ที่ตรวจพบ แบ่งตามประเภทช่องโหว่และระดับความรุนแรง (Critical, High) โดยอธิบายรายละเอียดช่องโหว่, ระดับความรุนแรง, CVSS Score Detail, แนวทางการแก้ไข และอุปกรณ์เครือข่าย/เครื่องแม่ข่ายที่ได้รับผลกระทบ
- ดำเนินการตรวจสอบซ้ำ จากผลการแก้ไข เพื่อยืนยันความถูกต้องของการแก้ไข และรายงานผลให้ธนาคารรับทราบ

4.3 ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) จากระบบจากภายนอกแบบ Black-Box Penetration Testing และทำการทดสอบเจาะระบบจากภายในธนาคารแบบ White-Box Penetration Testing ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ที่ธนาคารกำหนด จำนวนไม่เกิน 10 หมายเลขไอพี โดยจะต้องดำเนินการดังต่อไปนี้

- ทดสอบเจาะระบบจากภายนอกแบบ Black-Box Penetration Testing และทำการทดสอบเจาะระบบจากภายในธนาคารแบบ White-Box Penetration Testing ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) การดำเนินงานจะต้องครอบคลุมการทดสอบหาเป้าหมายทั้งแบบทางตรงและทางอ้อม
- จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก เปรียบเทียบภาพรวมและผลกระทบของช่องโหว่ที่ตรวจพบ จากการทำ Black-Box พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางการแก้ไข ประเมินและจัดลำดับความเสี่ยง แยกตามประเภทของอุปกรณ์เครือข่าย และเครื่องแม่ข่าย โดยวิเคราะห์ผลจะต้องสอดคล้องหรือต้องอ้างอิงตาม OWASP หรือมาตรฐานสากลอ้างอิงอื่น ๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ
- ดำเนินการตรวจสอบซ้ำ จากผลการแก้ไข เพื่อยืนยันความถูกต้องของการแก้ไข และรายงานผลให้ธนาคารรับทราบ

4.4 ดำเนินการทดสอบบุกรุกและประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 เมื่อธนาคารมีการพัฒนา Module ใหม่ หรือเมื่อธนาคารมีความต้องการให้ทำการทดสอบด้านความปลอดภัยในระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ตามที่ธนาคารกำหนด เป็นจำนวน 1 ครั้ง โดยมีรายละเอียดดังนี้

- การดำเนินการทดสอบบุกรุกและประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ของธนาคาร จะต้องแจ้งให้ทราบล่วงหน้าอย่างน้อยเป็นเวลา 7 วันก่อนเริ่มทำการทดสอบ เพื่อให้บริษัทผู้รับจ้างเตรียมความพร้อมก่อนเข้าดำเนินการ
- จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก ภาพรวมและผลกระทบ ของช่องโหว่ที่ตรวจพบ พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง โดยวิเคราะห์ผลจะต้องสอดคล้อง หรือต้องอ้างอิงตาม OWASP หรือมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ และส่งมอบให้กับธนาคารเพื่อให้ธนาคารนำข้อมูลช่องโหว่ที่ตรวจพบไปดำเนินการแก้ไขปรับปรุงให้มีความปลอดภัย และรายงานผลให้ธนาคารรับทราบ
- ดำเนินการตรวจสอบซ้ำ จากผลการแก้ไข เพื่อยืนยันความถูกต้องของการแก้ไข และรายงานผลให้ธนาคารรับทราบ

4.5 จัดทำและส่งมอบงานฉบับสมบูรณ์ให้กับธนาคาร

5. ระยะเวลาของโครงการ

การดำเนินงานสอบทานระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ให้มีความปลอดภัยตามเกณฑ์มาตรฐานสากล มีระยะเวลาดำเนินงานทั้งสิ้น 180 วัน ตลอดระยะเวลาโครงการ นับถัดจากวันที่ลงนามในสัญญา โดยการดำเนินการจะแบ่งเป็น 2 ครั้ง ดังนี้

- ครั้งที่ 1 : เวลาดำเนินงานทั้งสิ้น 90 วัน นับถัดจากวันที่ลงนามในสัญญา
- ครั้งที่ 2 : เวลาดำเนินงานทั้งสิ้น 180 วัน นับถัดจากวันที่ลงนามในสัญญา

ประกอบด้วยขั้นตอนการดำเนินงานหลักๆ คือ

5.1 ครั้งที่ 1 : เวลาดำเนินงานทั้งสิ้น 90 วัน (นับถัดจากวันที่ลงนามในสัญญา)

- ดำเนินการตรวจสอบ วิเคราะห์ อุปกรณ์ความมั่นคงปลอดภัยและเครื่องแม่ข่าย ในระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ของธนาคาร โดยมีรายละเอียดดังนี้ (ตามวิธีการดำเนินงานข้อ 4.1)

- ต้องทำการตรวจสอบและวิเคราะห์การตั้งค่าของอุปกรณ์ไฟร์วอลล์ (Policy Firewall) ตามขอบเขตของโครงการจำนวนไม่เกิน 1 อุปกรณ์
- ต้องทำการตรวจสอบและวิเคราะห์การตั้งค่าเครื่องแม่ข่ายตามเอกสาร (Hardening) ที่กำหนด โดยจำนวนเครื่องแม่ข่ายไม่เกิน 5 อุปกรณ์
- ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ที่ธนาคารกำหนด จำนวนไม่เกิน 10 หมายเลขไอพี (ตามวิธีการดำเนินงานข้อ 4.2)
- ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) จากระบบจากภายนอกแบบ Black-Box Penetration Testing และทำการทดสอบเจาะระบบจากภายในธนาคารแบบ White-Box Penetration Testing ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ที่ธนาคารกำหนด จำนวนไม่เกิน 10 หมายเลขไอพี (ตามวิธีการดำเนินงานข้อ 4.3)

5.2 ครั้งที่ 2 : เวลาดำเนินงานทั้งสิ้น 180 วัน (นับถัดจากวันที่ลงนามในสัญญา)

- ดำเนินการทดสอบบุกรุกและประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 เมื่อธนาคารมีการพัฒนา Module ใหม่ หรือเมื่อธนาคารมีความต้องการให้ทำการทดสอบด้านความปลอดภัยในระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ตามที่ธนาคารกำหนด เป็นจำนวนทั้งสิ้น 1 ครั้ง โดยมีรายละเอียดดังนี้
(ตามวิธีการดำเนินงานข้อ 4.4)
 - การดำเนินการทดสอบบุกรุกระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ของธนาคารจะแจ้งให้ทราบล่วงหน้าอย่างน้อยเป็นเวลา 7 วันก่อนเริ่มทำการทดสอบ เพื่อให้บริษัทผู้รับจ้างเตรียมความพร้อมก่อนเข้าดำเนินการ
 - จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก ภาพรวมและผลกระทบ ของช่องโหว่ที่ตรวจพบ พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง โดยวิเคราะห์ผลจะต้องสอดคล้องหรือต้องอ้างอิงตาม OWASP หรือมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ และส่งมอบให้กับธนาคารเพื่อให้ธนาคารนำข้อมูลช่องโหว่ที่ตรวจพบไปดำเนินการแก้ไขปรับปรุงให้มีความปลอดภัย และรายงานผลให้ธนาคารรับทราบ

- ดำเนินการตรวจสอบซ้ำ จากผลการแก้ไข เพื่อยืนยันความถูกต้องของการแก้ไข และรายงานผลให้ธนาคารรับทราบ

5.3 จัดทำและส่งมอบงาน ฉบับสมบูรณ์ (ระยะเวลาดำเนินงาน 180 วัน นับถัดจากวันที่ลงนามในสัญญา)

6. งานที่ต้องส่งมอบ

6.1 ครั้งที่ 1 : ส่งมอบงานภายใน 90 วัน นับถัดจากวันที่ลงนามในสัญญา ตามวิธีการดำเนินงาน ข้อ 4.1 – 4.3 เอกสารจะต้องถูกรวบรวมและส่งมอบ (ฉบับภาษาไทย) ในลักษณะของแฟ้มงาน 1 แฟ้ม และจัดทำ Index ของเอกสาร แบ่งแยกเอกสารแต่ละชุดอย่างชัดเจน

- รายงานผลการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ของธนาคาร (ฉบับภาษาไทย)
- รายงานผลการตรวจสอบวิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ของธนาคาร (ฉบับภาษาไทย)
- รายงานผลการทดสอบซ้ำ ผลการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 ของธนาคาร (ฉบับภาษาไทย)
- รายงานผลการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) จากระบบจากภายนอกแบบ Black-Box Penetration Testing และทำการทดสอบเจาะระบบจากภายในธนาคารแบบ White-Box Penetration Testing ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 (ฉบับภาษาไทย)
- รายงานผลการทดสอบซ้ำ ผลการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) จากระบบจากภายนอกแบบ Black-Box Penetration Testing และทำการทดสอบเจาะระบบจากภายในธนาคารแบบ White-Box Penetration Testing ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 (ฉบับภาษาไทย)

- 6.2 ครั้งที่ 2 : ส่งมอบงานภายใน 180 วัน นับถัดจากวันที่ลงนามในสัญญา ตามวิธีการดำเนินงาน ข้อ 4.4 เอกสารจะต้องถูกรวบรวมและส่งมอบ (ฉบับภาษาไทย) ในลักษณะของแฟ้มงาน 1 แฟ้ม และจัดทำ Index ของเอกสาร แบ่งแยกเอกสารแต่ละชุดอย่างชัดเจน
- รายงานผลการทดสอบบุกรุกและประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 (ฉบับภาษาไทย)
 - รายงานผลการทดสอบซ้ำ ผลการทดสอบบุกรุกและประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของระบบบริการดิจิทัลและระบบงาน GHB ALL GEN Phase 3 (ฉบับภาษาไทย)
 - เอกสารคู่มือวิธีการทำ Bypass SSL Certificate Pinning Mobile Application ระบบงาน GHB ALL GEN Phase 3 ทั้งระบบปฏิบัติการ Android และ IOS (ฉบับภาษาไทย)
- 6.3 สิ่งที่ต้องส่งมอบตามวิธีการดำเนินงานข้อ 4.1 - ข้อ 4.4 (ส่งมอบงานภายใน 180 วัน นับถัดจากวันที่ลงนามในสัญญา) เอกสารจะต้องถูกรวบรวมและส่งมอบ (ฉบับภาษาไทย) โดยจัดทำ Index ของเอกสาร แบ่งแยกเอกสารแต่ละชุดอย่างชัดเจน และต้องสามารถเปิดและแก้ไขด้วยชุดโปรแกรมจาก Microsoft office ตั้งแต่ Version 2010 ขึ้นไป บรรจุใน USB Drive รวม 1 ชุด

