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 ก.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 เริ่มนับจากเวลาที่อุปกรณ์ของธสน. 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) ที่ยังมีผลบังคับใช้ของบุคลากรพร้อมกับการยื่นข้อเสนอในครั้งนี้ 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) หรือส่งมอบแล้วแต่ไม่ถูกต้องไม่ครบถ้วน 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 ธนาคารขอสงวนสทธิที่จะปรับเปลี่ยนข้อความในสัญญาบางประการตามที่เห็นสมควร

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