

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย
ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่มีชิ้นงานก่อสร้าง

1. ชื่อโครงการ การเช่าระบบป้องกันการบุกรุก Firewall For Internet Zone
2. หน่วยงานเจ้าของโครงการ ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ
3. วงเงินงบประมาณที่ได้รับจัดสรร 2,400,000.00 บาท (สองล้านสี่แสนบาทถ้วน)
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ 6/6/2025
เป็นเงิน 2,337,950.00 บาท (สองล้านสามแสนสามหมื่นเจ็ดพันเก้าร้อยห้าสิบบาทถ้วน)
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
บริษัท ดาต้าโปร คอมพิวเตอร์ ซิสเต็มส์ จำกัด
6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน
 - 6.1 นายชานนท์ แทนทองจันทร์ ผู้ช่วยผู้บริหารส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ / ฝ่าย ปส. 
 - 6.2 นางสาวศรัณญา แวงวรรณ ผู้บริหารส่วนจัดซื้อเทคโนโลยีสารสนเทศ / ฝ่าย จธ. 
 - 6.3 นายจเร บุญกร ผู้ช่วยผู้บริหารส่วนบริหารจัดการโครงสร้างพื้นฐานและระบบเครือข่าย / ฝ่าย ปส. 

ผนวก 1
ขอบเขตการดำเนินงาน
การเข้าระบบป้องกันการบุกรุก Firewall For Internet Zone

1. ขอบเขตการดำเนินงาน

ผู้ยื่นข้อเสนอต้องให้บริการการเข้าระบบป้องกันการบุกรุก Firewall For Internet Zone ตามรายการอุปกรณ์และรายละเอียดคุณลักษณะอุปกรณ์ รวมถึงขอบเขตงานที่ธนาคารกำหนด ดังต่อไปนี้

1.1 รายการอุปกรณ์

ลำดับ	อุปกรณ์	จำนวน	หน่วยนับ
1	Firewall Palo-Alto (PA-5220)	2	Units
2	Threat Prevention License	2	Licenses
3	Advance URL Filtering License	2	Licenses

1.2 รายละเอียดคุณลักษณะอุปกรณ์

- 1.2.1 เป็น Firewall Appliance โดยมี Firewall throughput ในรูปแบบ Appmix ไม่น้อยกว่า 15 Gbps
- 1.2.2 มี Threat Protection Throughput ในรูปแบบ Appmix ไม่น้อยกว่า 8.8 Gbps
- 1.2.3 มี IPsec VPN Throughput ไม่น้อยกว่า 9.5 Gbps
- 1.2.4 มีจำนวน New session per second ไม่น้อยกว่า 150,000 sessions
- 1.2.5 สามารถใช้งาน Routing แบบ Dynamic Routing ได้แก่ OSPF, BGP, RIP ได้เป็นอย่างดี

2. การให้บริการสนับสนุนตลอดระยะเวลาการให้บริการ (Support)

- 2.1 จัดให้มีเจ้าหน้าที่ประสานงานที่มีความรู้ความชำนาญเกี่ยวกับระบบป้องกันการบุกรุก Firewall For Internet Zone พร้อมหมายเลขโทรศัพท์ที่สามารถติดต่อได้สะดวกเพื่อรับแจ้งเหตุขัดข้อง ให้คำปรึกษาตอบข้อซักถาม ให้ความช่วยเหลือหรือแก้ไขปัญหาเบื้องต้น (On Phone Support) รวมถึงช่องทางอื่นได้ทุกวันตลอด 24 ชั่วโมง
- 2.2 ในกรณีระบบป้องกันการบุกรุก Firewall For Internet Zone เกิดเหตุขัดข้องซ้ำชุด หรือมีข้อบกพร่องที่ไม่สามารถใช้งานได้ ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกจะต้องจัดส่งเจ้าหน้าที่เข้ามาให้บริการ ตรวจสอบและแก้ไขปัญหาให้กับทางธนาคาร ณ สถานที่ตั้ง รวมทั้งต้องดำเนินการตรวจสอบแก้ไขหรือปรับปรุงให้แล้วเสร็จภายในกำหนดระยยะเวลานับถัดจากที่ได้รับแจ้งเหตุขัดข้องหรือความชำรุดบกพร่องจากธนาคารตามระดับผลกระทบที่มีต่อธุรกิจ หรือการทำงาน (Severity) ดังนี้

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

ต้องนำส่งรายละเอียดและขั้นตอนการแก้ไขปัญหา เหตุขัดข้อง และ/หรือความชำรุดบกพร่องของระบบ
สำรองข้อมูล อย่างละเอียดให้แก่ธนาคารในทันทีที่สามารถดำเนินการได้ และผู้ให้บริการตกลงเป็น
ผู้รับผิดชอบชำระค่าใช้จ่ายที่เกิดขึ้นจากการเข้าดำเนินการทั้งจำนวน

- 2.3 จัดให้มีเจ้าหน้าที่เข้าตรวจสอบสถานะการทำงานของระบบ (Preventive Maintenance: PM) ไม่น้อยกว่า
4 ครั้ง/ปี พร้อมจัดทำรายงานสรุปการดำเนินการ ของระบบ (Health Check Report) สรุปผลการ
ตรวจสอบ และสถานะของอุปกรณ์โครงข่าย Firewall For Internet Zone (Events Report) ซึ่งได้ตรวจ
พบจาก Traffic log บน Dashboard ของระบบป้องกันการบุกรุก Firewall For Internet Zone รวมถึง
เหตุการณ์ที่น่าสนใจ โดยต้องแจ้งให้ธนาคารทราบล่วงหน้าในการเข้าดำเนินการไม่น้อยกว่า 1 วันทำการ
และต้องได้รับความเห็นชอบจากธนาคารก่อนเข้าดำเนินการ และส่งมอบรายงานให้ธนาคารภายใน 15 วัน
นับถัดจากวันที่เข้าดำเนินการตามรายละเอียด ดังต่อไปนี้

ครั้งที่ 1 ภายในเดือนตุลาคม 2568

ครั้งที่ 2 ภายในเดือนมกราคม 2569

ครั้งที่ 3 ภายในเดือนเมษายน 2569

ครั้งที่ 4 ภายในเดือนกรกฎาคม 2569

- 2.4 ในระหว่างสัญญาการใช้งาน หากพบว่าอุปกรณ์ระบบป้องกันการบุกรุก Firewall For Internet Zone
สิ้นสุดการรับประกันคุณภาพหรือการสนับสนุนการให้บริการจากเจ้าของผลิตภัณฑ์ ผู้ให้บริการจะต้องทำการ
เปลี่ยนอุปกรณ์ระบบป้องกันการบุกรุก Firewall For Internet Zone ให้กับธนาคารใหม่ โดยอุปกรณ์ฯ ที่
เปลี่ยนจะต้องมีคุณสมบัติไม่ด้อยกว่าเดิม ภายใน 24 ชั่วโมง
- 2.5 ดำเนินการ Review Policy (Firewall) ตาม Best Practice และ Upgrade firmware เพื่อปรับปรุงระบบ
ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ตามที่ธนาคารได้มีการร้องขอ โดยไม่คิดค่าใช้จ่ายเพิ่มเติม
- 2.6 ดำเนินการ Configure อุปกรณ์โครงข่าย Firewall For Internet Zone ตามที่ธนาคารได้มีการร้องขอ
- 2.7 ในกรณีที่มีการ Upgrade Program / Firmware ในระหว่างระยะเวลาเช่า หาก Application Software
หรือ Firmware หรือ Patch หรือระบบปฏิบัติการของอุปกรณ์โครงข่าย Firewall For Internet Zone มี
การออก Version ใหม่ หรือพัฒนาปรับปรุง (Upgrade) ผู้ยื่นข้อเสนอที่ได้รับเลือกจะต้องแจ้งรายละเอียด
การเปลี่ยนแปลงและผลกระทบที่เกิดขึ้นจากการเปลี่ยนแปลงดังกล่าวให้ธนาคารทราบ เพื่อใช้เป็นข้อมูล
ประกอบการตัดสินใจของธนาคาร และหากธนาคารประสงค์จะดำเนินการพัฒนาปรับปรุง (Upgrade) ผู้ยื่น
ข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการพัฒนาปรับปรุง (Upgrade) ให้กับธนาคารโดยไม่คิดค่าใช้จ่าย
เพิ่มเติม และดำเนินการให้แล้วเสร็จภายใน 7 วันนับจากได้รับแจ้งจากธนาคาร
- 2.8 ในกรณีที่ธนาคารตรวจพบช่องโหว่ของระบบป้องกันการบุกรุก Firewall For Internet Zone หรือช่องโหว่
ของระบบปฏิบัติการที่ส่งผลกระทบต่อระบบป้องกันการบุกรุก Firewall For Internet Zone ผู้ยื่นข้อเสนอ
ที่ได้รับการคัดเลือกต้องดำเนินการแก้ไขปิดช่องโหว่ให้แล้วเสร็จ โดยไม่คิดค่าใช้จ่ายเพิ่มเติม
- 2.9 ในกรณีอุปกรณ์เช่าใช้ดังกล่าวสิ้นอายุสัญญา ผู้ให้บริการสามารถเก็บอุปกรณ์ได้ภายใน 60 วัน นับจาก
วันที่หมดอายุสัญญา