ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจัดซื้ออุปกรณ์โครงข่าย** External Firewall

2. หน่วยงานเจ้าของโครงการ **ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ**

3. วงเงินงบประมาณที่ได้รับจัดสรร 11,500,000.- **บาท (สิบเอ็ดล้านห้าแสนบาทถ้วน)**

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 24 ก.ย. 2567

   เป็นเงิน 11,499,243.75 **บาท (สิบเอ็ดล้านสี่แสนเก้าหมื่นเก้าพันสองร้อยสี่สิบสามบาทเจ็ดสิบห้าสตางค์)**

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   บริษัท แทนเจอรีน จำกัด

   บริษัท ดาต้าโปร คอมพิวเตอร์ ซิสเต็มส์ จำกัด

   บริษัท แอ็ดวานซ์อินฟอร์เมชั่นเทคโนโลยี จำกัด (มหาชน)

   บริษัท เดอะแพรคทิเคิลโซลูชั่น จำกัด (มหาชน)

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายฉัตรชัย	อาศรมเงิน	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.2 นายจรัส	ขวัญพิเชษฐ์สกุล	ผู้บริหารส่วนรักษาความปลอดภัยเทคโนโลยีสารสนเทศ /ฝ่าย ปส.
6.3 นายกิตติ์ธเนศ	วงศ์ประสิทธิ์	ผู้ช่วยผู้บริหารส่วนบริการและปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่าย ปส.

ผนวก 1

ข้อกำหนดด้านเทคนิคและขอบเขตของงาน

ผู้ยื่นข้อเสนอต้องจัดหาอุปกรณ์ External Firewall พร้อม Implementation ตามขอบเขตงานที่ธนาคารกำหนด โดยมีขอบเขตการดำเนินงานดังต่อไปนี้

1. ข้อกำหนดความต้องการทั่วไป

1.1 ต้องเสนอบริการอุปกรณ์โครงข่าย External Firewall ที่มีคุณสมบัติที่สามารถใช้งานร่วมกับระบบเครือข่ายและระบบคอมพิวเตอร์ที่ธนาคารใช้งานอยู่ในปัจจุบันได้

1.2 อุปกรณ์จะต้องเป็นของใหม่และไม่เคยผ่านการใช้งานมาก่อน ไม่เป็นของเก่าเก็บ หรือสินค้าที่นำกลับมาใช้ใหม่ (Refurbished)

1.3 ต้องดำเนินการทดสอบตามเกณฑ์ที่ธนาคารกำหนด และต้องแก้ไขปัญหาจนกระทั่งการติดตั้งและปรับปรุงเสร็จสมบูรณ์โดยไม่มีค่าใช้จ่ายเพิ่มเติม

1.4 ต้องดำเนินการติดตั้งอุปกรณ์โครงข่าย External Firewall ทดแทนอุปกรณ์เดิม และดำเนินการ Migration อุปกรณ์โครงข่าย External Firewall ปัจจุบัน ไปยัง อุปกรณ์โครงข่าย External Firewall ชุดใหม่

1.5 สามารถแจ้งเตือนเหตุการณ์ที่เกิดขึ้นได้ตามเงื่อนไขที่ได้กำหนดไว้ ผ่านทาง SNMP หรือ Syslog หรือ Email หรือ SMS ได้

1.6 มีระบบ Centralized Management และสามารถบริหารจัดการผ่าน Web Browser หรือ Management Application ได้

1.7 หากมีส่วนประกอบเพิ่มเติมใดที่มิได้ระบุไว้ในเอกสารรายละเอียดของคุณลักษณะเฉพาะและขอบเขตการดำเนินงาน แต่มีความจำเป็นต่อการใช้งานของอุปกรณ์โครงข่าย External Firewall เพื่อให้งานแล้วเสร็จสามารถใช้งานอุปกรณ์โครงข่าย External Firewall ถูกต้อง ผู้ยื่นข้อเสนอต้องจัดหาหรือจัดทำมาให้เพียงพอต่อการใช้งานของธนาคาร และต้องส่งมอบให้เป็นกรรมสิทธิ์ หรือสิทธิ์ หรือลิขสิทธิ์ของธนาคารทั้งหมด โดยไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติม

2. ข้อกำหนดคุณสมบัติเฉพาะของอุปกรณ์โครงข่าย External Firewall

2.1 อุปกรณ์โครงข่าย External Firewall จำนวน 2 ชุด โดยแต่ละชุดมีคุณสมบัติขั้นต่ำดังนี้

2.1.1 อุปกรณ์แบบ Hardware Appliance ที่ออกแบบมาเพื่อทำหน้าที่ Next Generation Firewall โดยเฉพาะ

2.1.2 มี Firewall Throughput ไม่น้อยกว่า 35 Gbps ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

2.1.3 มี Threat prevention Throughput ไม่น้อยกว่า 20 Gbps ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix และจำนวน Max Sessions ได้ไม่น้อยกว่า 3,000,000 sessions และ New Sessions ไม่น้อยกว่า 268,000 ต่อวินาที

2.1.4 มีช่องเชื่อมต่อ Network Interface แบบ 1G/2.5G/5G/10G แบบ RJ45 หรือดีกว่าไม่ต่ำกว่า 6 พอร์ต

2.1.5 มีช่องเชื่อมต่อ Network Interface แบบ 1G/10G SFP/SFP+ หรือดีกว่าไม่ต่ำกว่า 10 พอร์ต พร้อมทั้งเสนอ Transceiver Module 10G SFP+ SR จำนวนไม่น้อยกว่า 10 Transceivers

2.1.6 มีช่องเชื่อมต่อ Network Interface แบบ 25G SFP28 หรือดีกว่าไม่ต่ำกว่า 2 พอร์ต

2.1.7 มีช่องเชื่อมต่อ Network Interface แบบ 40G/100G QSFP/QSFP28 หรือดีกว่าไม่ต่ำกว่า 2 พอร์ต

2.1.8 มีช่องเชื่อมต่อ Management Interface แบบ 100/1000 หรือดีกว่า แยกออกมาจาก Network Interface ข้างต้น

2.1.9 เสนอ Transceiver Module ยี่ห้อ Cisco รุ่น SFP-10G-SR-S จำนวนไม่น้อยกว่า 4 Transceivers

2.1.10 อุปกรณ์ที่นำเสนอต้องสามารถทำ Client VPN (Remote Access) ได้ไม่ต่ำกว่า 2,000 tunnels หรือมี VPN Throughput หรือ IPsec VPN Throughput ไม่น้อยกว่า 14 Gbps รวมทั้งสามารถทำงานกับระบบปฏิบัติการ Windows (ทั้ง 32 และ 64 bits) ได้เป็น อย่างน้อย

2.1.11 อุปกรณ์ต้องมี SSD สำหรับเก็บข้อมูลระบบไม่ต่ำกว่า 480 GB

2.1.12 สามารถติดตั้งในรูปแบบ Transparent, Non-Inline Monitoring (Tap), L2 และ L3 หรือเทียบเท่าได้

2.1.13 สามารถทำ Dynamic Routing Protocol ได้แก่ RIP, OSPF และ BGP เป็นอย่างน้อย

2.1.14 สามารถรับ Syslog จากระบบที่มีอยู่ได้ เพื่อใช้ในการยืนยันตัวตน ของ User ที่ใช้งาน โดยรองรับทั้ง User Log-in และ User Log-out โดยสามารถทำได้บนตัวอุปกรณ์ Firewall หรือเสนอระบบอื่นเพิ่มเติมเพื่อให้สามารถทำงานได้

2.1.15 สามารถทำการตรวจสอบทราฟฟิคที่เข้ารหัส SSL ด้วยการทำ SSL decryption (ทั้งแบบ Inbound และ Outbound) และสามารถทำ SSL Orchestrator หรือ SSL Security Service Chain หรือ SSL Decryption Broker ได้ โดยสามารถเสนอระบบเพิ่มเติมเพื่อให้ทำได้ตามข้อกำหนด

2.1.16 สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication System) ได้แก่ Active Directory, LDAP และ RADIUS เพื่อทำการติดตามผู้ใช้ได้เป็นอย่างน้อย

2.1.17 มีระบบเรียกดูสรุปข้อมูลรายงานของ Data ในรูปแบบของกราฟฟิคได้ โดยสามารถ ปรับแต่งรายงานตามความต้องการ (Custom Report) และส่งออก (Export) ให้อยู่ในรูปแบบ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลา ส่งรายงานผ่านทาง Email แบบอัตโนมัติได้ และสามารถทำรายงานต่าง ๆ ได้

2.1.18 มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

2.1.19 สามารถติดตั้งเพื่อทำ High Availability (HA) แบบ Active/Passive หรือ Active/Active ได้

2.1.20 สามารถบริหารจัดการอุปกรณ์แบบ Web-based Management (HTTPS) หรือ Command Line Interface ได้

2.1.21 สามารถทำการคัดกรอง log (log filtering) และส่ง log ผ่าน HTTP-based API ไปยังอุปกรณ์ 3rd party ได้

2.1.22 มีระบบป้องกันภัยคุกคาม Intrusion Prevention (IPS) เพื่อป้องกันภัยคุกคาม โดย มีคุณสมบัติอย่างน้อยดังต่อไปนี้

2.1.22.1 สามารถป้องกัน Malware แบบ Stream-Based ป้องกัน malware ด้วยการตรวจสอบ signature อ้างอิง payload ได้

2.1.22.2 สามารถตรวจจับและป้องกัน Virus บนโปรโตคอล HTTP, FTP, IMAP, POP3, SMTP, SMB และ SSL รวมถึง Virus ที่ฝังตัวมากับ PDF, Web Content, Microsoft® Office documents และ Compressed Files ได้

2.1.23 มีระบบตรวจจับ Advanced Malware แบบ Cloud-Based และใช้เทคโนโลยีแบบ Sandbox เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero-day Malware) ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้ รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ และมี report พฤติกรรมการทำงานของ malware ดังกล่าวได้

2.1.24 มีเครื่องมือในการทำ Firewall Policy Optimization โดยวิเคราะห์ Log และแนะนำการสร้าง Security Policy ใหม่จาก Traffic logs ที่เรียนรู้ภายในองค์กร หรือเสนอระบบเพิ่มเติมเพื่อให้ทำได้ตามข้อกำหนด

2.1.25 อุปกรณ์ที่นำเสนอต้องสามารถส่ง log ไปยังระบบ SIEM ของธนาคารฯได้

2.1.26 ผลิตภัณฑ์ที่นำเสนอจะต้องอยู่ใน Leader Quadrant ของ Gartner Magic Quadrant ด้าน Enterprise Network Firewalls ปีล่าสุด โดยนับจากปี 2022 เป็นต้นไป

2.1.27 ต้องรับประกันอุปกรณ์เป็นเวลาอย่างน้อย 3 ปี โดยระบบต้องสามารถแสดงวันที่สิ้นสุดได้ในระบบหรือตัวอุปกรณ์ที่นำเสนอ

2.1.28 ผู้เสนอราคาต้องได้รับการแต่งตั้งจากเจ้าของผลิตภัณฑ์โดยตรงในการยื่นข้อเสนอสำหรับโครงการ

2.1.29 อุปกรณ์จะต้องเป็นของใหม่และไม่เคยผ่านการใช้งานมาก่อนไม่เป็นของเก่าเก็บหรือสินค้าที่นำกลับมาใช้ใหม่ (Refurbished)

2.2 ข้อกำหนดคุณสมบัติเฉพาะของอุปกรณ์ Centralized Management สำหรับอุปกรณ์โครงข่าย External Firewall จำนวน 1 ชุด มีคุณสมบัติขั้นต่ำดังนี้

2.2.1 เป็นอุปกรณ์แบบ Virtual Appliance ทำหน้าที่บริหารจัดการแบบรวมศูนย์ (Centralized Management) ยี่ห้อเดียวกับอุปกรณ์โครงข่าย External Firewall ข้อ 2.1 โดยมีคุณสมบัติดังต่อไปนี้

2.2.2 สามารถบริหารจัดการอุปกรณ์ Firewall จากศูนย์กลาง (Centralized Management) ได้ไม่น้อยกว่า 25 อุปกรณ์ (Licensed) และสามารถเพิ่ม License ให้รองรับได้ไม่น้อยกว่า 1,000 อุปกรณ์ในอนาคต

2.2.3 สามารถส่ง log ที่ได้ไปยังอุปกรณ์ภายนอกในรูปแบบของ UDP หรือ TCP หรือ SSL พร้อมทั้งสามารถส่งข้อมูลหรือคำสั่ง ไปยังอุปกรณ์ภายนอกที่มี HTTP-based API เช่นระบบ ticketing service ได้ สามารถทำการ correlate ข้อมูลเพื่อตรวจจับหาเครื่องที่ถูก compromise ได้

2.2.4 สามารถกำหนดสิทธิที่ต่างกันให้กับผู้ดูแลระบบแต่ละคนได้ (Role-based Administration)

2.2.5 สามารถทำการอัพเดท software, license และ contents ของ Firewall ที่ควบคุมอยู่ได้

2.2.6 สามารถบริหารจัดการและปรับเปลี่ยนค่าต่าง ๆ จากส่วนกลาง เช่น Policies, Object และ Security Profile แล้วทำการส่งผ่านการตั้งค่าไปยังอุปกรณ์รักษาความปลอดภัยได้

2.2.7 สามารถแสดงหน้า dashboard จากการประมวลผลจาก log ที่มาจาก firewall ในรูปแบบ graphical เช่น data files, URLs, threats และสามารถ customize เองได้

2.2.8 สามารถสร้างรายงาน (Report) ต่างๆ เช่น User Activity Report, Application Report, SaaS Report, Threat/Attack Report, AntiVirus Report, URL Filtering Report หรือสามารถสร้างรายงาน(Report) ดังนี้ MITRE ATT&CK Report, Threat Prevention Report, Application and URL Filtering Report ได้เป็นอย่างน้อย โดยสามารถทำการปรับแต่งรายงาน (Custom Report) และส่งออก (Export) ให้อยู่ในรูปแบบ PDF หรือ CSV

2.2.9 ผู้เสนอราคาต้องได้รับการแต่งตั้งจากเจ้าของผลิตภัณฑ์โดยตรงในการยื่นข้อเสนอสำหรับโครงการ

2.2.10 อุปกรณ์ Virtual Appliance จะต้องเป็นของใหม่และไม่เคยผ่านการใช้งานมาก่อนไม่เป็นของเก่าเก็บ หรือสินค้าที่นำกลับมาใช้ใหม่ (Refurbished)

2.3 ข้อกำหนดคุณสมบัติเฉพาะของอุปกรณ์กระจายสัญญาณ สำหรับอุปกรณ์โครงข่าย External Firewall จำนวน 2 ชุด มีคุณสมบัติขั้นต่ำดังนี้

2.3.1 มี Switching capacity ขนาดไม่น้อยกว่า 128 Gbps.

2.3.2 มีประสิทธิภาพในการส่งผ่านข้อมูล Forwarding Rate ไม่น้อยกว่า 95 Mpps.

2.3.3 มีพอร์ต Gigabit Ethernet แบบ 100/1000 แบบ RJ45 จำนวนไม่น้อยกว่า 24 พอร์ต

2.3.4 มีพอร์ต Gigabit Ethernet แบบ SFP+ จำนวนไม่น้อยกว่า 4 พอร์ต พร้อมเสนอ Transceiver Modules แบบ 10 Gbps. ชนิด 10GBase-SR หรือเทียบเท่า จำนวนไม่น้อยกว่า 4 โมดูล

2.3.5 อุปกรณ์กระจายสัญญาณ รองรับการทำ Stack ได้ไม่น้อยกว่า 8 Switches

2.3.6 รองรับ Stacking bandwidth ต่อชุดไม่น้อยกว่า 160 Gbps พร้อมเสนอสาย Stack โดยมีความยาวไม่น้อยกว่า 50 เซนติเมตร หรือ ดีกว่า

2.3.7 สามารถทำ ตามมาตรฐาน IEEE802.1p และ IEEE802.1q

2.3.8 สามารถทำงาน ทั้ง IP Version 4 และ IP Version 6

2.3.9 สามารถทำ Spanning tree ตามมาตรฐาน IEEE802.1D, IEEE802.1w และ IEEE802.1s

2.3.10 สามารถทำ Port Aggregation ตามมาตรฐาน IEEE802.3ad ได้

2.3.11 รองรับการสร้าง VLAN ได้ไม่น้อยกว่า 4000 VLANs

2.3.12 รองรับ MAC address ได้ไม่น้อยกว่า 13,000 MAC addresses

2.3.13 รองรับการทำ IP Routing ได้แก่ Static, Policy-Based Routing, OSPF และ EIGRP ได้

2.3.14 มี Console Port เพื่อกำหนดค่าการทำงานของอุปกรณ์

2.3.15 สามารถทำงานตามมาตรฐาน SSH, NTP, SNMPv3 ได้

2.3.16 อุปกรณ์ที่นำเสนอ ต้องมี Rack Mount สามารถติดตั้งบน Rack 19" ได้

2.3.17 ผ่านการรับรองตามมาตรฐานความปลอดภัย UL หรือ EN หรือ IEC หรือ เทียบเท่า ได้

2.3.18 มี Redundant Power Supply ในตัวอุปกรณ์โดยสามารถใช้กับระบบไฟฟ้าในประเทศไทยแบบ 220 VAC 50Hz ได้ และแหล่งจ่ายไฟนี้จะต้องทำงานได้ในลักษณะ Hot-Swappable ได้

2.3.19 อุปกรณ์ที่นำเสนอ ต้องสามารถทำงานร่วมกันได้กับ ระบบบริหารและจัดการเครือข่าย Network Access Control ที่ทางธนาคารฯใช้อยู่

2.3.20 อุปกรณ์ที่นำเสนอต้องสามารถส่ง Log ไปยังระบบ SIEM ของธนาคารฯได้

2.3.21 ผู้เสนอราคาต้องได้รับการแต่งตั้งจากเจ้าของผลิตภัณฑ์โดยตรงในการยื่นข้อเสนอสำหรับโครงการ

2.3.22 อุปกรณ์จะต้องเป็นของใหม่และไม่เคยผ่านการใช้งานมาก่อนไม่เป็นของเก่าเก็บ หรือสินค้าที่นำกลับมาใช้ใหม่ (Refurbished)

3 ขอบเขตการดำเนินการ

3.1 จัดประชุมโครงการ (Kick-off) โดยมีรายละเอียดในการดำเนินโครงการประกอบด้วย

3.1.1 วัตถุประสงค์และแผนดำเนินงาน

3.1.2 ขั้นตอนการดำเนินโครงการ

3.1.3 บทบาท หน้าที่และความรับผิดชอบของผู้เกี่ยวข้องระยะเวลาการดำเนินโครงการ

3.2 นำเสนอ Configuration Design ของระบบส่งให้กับธนาคาร โดยต้องให้รายละเอียดของระบบตลอดจนรูปแบบและวิธีการเชื่อมต่อของอุปกรณ์ทั้งโครงการ

3.3 จัดเตรียมสายสัญญาณ และอุปกรณ์เชื่อมโยงต่างๆ (ถ้ามี) เพื่อเชื่อมโยงกับอุปกรณ์โครงข่าย External Firewall ของธนาคารให้สามารถใช้งานร่วมกันได้อย่างมีประสิทธิภาพ โดยผลิตภัณฑ์ และสีของสายต่อต้องเป็นไปตามที่ธนาคารกำหนด และเป็นผลิตภัณฑ์ยี่ห้อชนิดเดียวกับที่ธนาคารมีใช้งานอยู่เดิมดังนี้

3.3.1 สีแดง เชื่อมต่อจาก Server ไปยัง Switch

3.3.2 สีเหลือง เชื่อมต่อระหว่าง Switch และ Switch

3.3.3 สีเขียว เชื่อมต่ออุปกรณ์ภายในตู้เก็บอุปกรณ์ (Rack Cabinet)

3.3.4 สีเทา เชื่อมต่อระหว่าง Patch Panel และ Patch Panel

3.4 จัดเตรียมสายสัญญาณ Fiber optic patch cord (Multi-mode) ความยาว 5 เมตร จำนวน 20 เส้น และความยาว 15 เมตร จำนวน 20 เส้น

3.5 ต้องดำเนินการทดสอบอุปกรณ์ระบบโครงข่าย External Firewall ตามเกณฑ์ที่ธนาคารกำหนด และต้องแก้ไขปัญหาจนกระทั่งการติดตั้งและปรับปรุงเสร็จสมบูรณ์โดยไม่มีค่าใช้จ่ายเพิ่มเติม

3:6 ต้องดำเนินการติดตั้งอุปกรณ์ระบบโครงข่าย External Firewall ให้พร้อมใช้งาน ณ สำนักงานใหญ่ ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

3.7 ต้องดำเนินการ Migration อุปกรณ์ระบบโครงข่าย External Firewall ปัจจุบัน ไปยัง อุปกรณ์ระบบโครงข่าย External Firewall ชุดใหม่ ให้พร้อมใช้งาน ณ สำนักงานใหญ่ ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

3.8 ต้องให้บริการอุปกรณ์โครงข่าย External Firewall ระยะเวลา 3 ปี นับถัดจากธนาคารตรวจรับมอบงานเรียบร้อยแล้ว

4 การฝึกอบรม และจัดทำเอกสารคู่มือ

4.1 จัดหลักสูตรการฝึกอบรมเชิงปฏิบัติการให้กับผู้ดูแลระบบจำนวนไม่น้อยกว่า 4 คน โดยเนื้อหาของการฝึกอบรมจะต้องครอบคลุม วิธีการใช้งานและบำรุงรักษาอุปกรณ์โครงข่าย External Firewall

4.2 จัดหลักสูตรการฝึกอบรม Official Class จำนวนไม่น้อยกว่า 3 ท่าน พร้อมทั้งจัดทำคู่มือการใช้งาน/การทำงานของระบบ ในรูปแบบสื่อ Electronics ดังนี้

4.2.1 คู่มือการติดตั้งระบบ (Installation & Configuration Manual)

4.2.2 คู่มือการใช้งานระบบสำหรับผู้ใช้ระบบงานระบบ (User Manual)

4.2.3 คู่มือการใช้งานระบบสำหรับผู้ดูแลระบบ (Operation Manual Administrator)

4.2.4 คู่มือการแก้ไขปัญหาเบื้องต้น (Trouble Shooting Manual)

4.2.5 คู่มือตรวจสอบการทำงานของระบบ (Monitoring Manual)

4.2.6 คู่มือการทำงานของระบบ (System Detail & Diagram)

5 การรับประกันคุณภาพ (Warranty)

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะต้องรับประกันคุณภาพ เป็นระยะเวลาไม่น้อยกว่า 3 ปี นับถัดจากวันที่คณะกรรมการตรวจรับมอบงานและลงนามเป็นที่เรียบร้อยแล้ว

6. การให้บริการสนับสนุนของการใช้บริการตลอดระยะเวลาการใช้บริการ (Support)

6.1 ดำเนินการดูแลพร้อมให้บริการแก้ไขปัญหาเกี่ยวกับอุปกรณ์โครงข่าย External Firewall ตลอด Warranty period ตามข้อ 5

6.2 จัดให้มีเจ้าหน้าที่เข้าตรวจสอบสถานะการทำงานของระบบ (Preventive Maintenance) ไม่น้อยกว่า 4 ครั้ง/ปี พร้อมจัดทำรายงานสรุปการดำเนินการ และสถานะของระบบ รวมถึงเหตุการณ์ที่น่าสนใจ โดยต้องแจ้งให้ธนาคารทราบล่วงหน้าในการเข้าดำเนินการไม่น้อยกว่า 1 วันทำการ และต้องได้รับความเห็นชอบจากธนาคารก่อนเข้าดำเนินการ และส่งมอบรายงานให้ธนาคารภายใน 15 วันนับถัดจากวันที่เข้าดำเนินการตามรายละเอียด ดังต่อไปนี้

6.2.1 รายงานสรุปผลการตรวจสอบสถานะของระบบ (Health Check Report) สรุปผลการตรวจสอบและสถานะของอุปกรณ์โครงข่าย External Firewall รายงานสรุปเหตุการณ์ที่น่าสนใจ (Events Report) ซึ่งได้ตรวจพบจาก Traffic log บน Dashboard ของอุปกรณ์โครงข่าย External Firewall

6.3 ในกรณีอุปกรณ์โครงข่าย External Firewall เกิดเหตุขัดข้องชำรุด หรือมีข้อบกพร่องที่ไม่สามารถใช้งานได้ ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกจะต้องจัดส่งเจ้าหน้าที่เข้ามาให้บริการ ตรวจสอบ และแก้ไขปัญหาให้กับทางธนาคาร ณ สถานที่ตั้ง รวมทั้งต้องดำเนินการตรวจสอบแก้ไขหรือปรับปรุงให้แล้วเสร็จภายในกำหนดระยะเวลานับถัดจากที่ได้รับแจ้งเหตุขัดข้องหรือความชำรุดบกพร่องจากธนาคาร ตามระดับผลกระทบที่มีต่อธุรกิจ หรือการทำงาน (Severity) ดังนี้

ระดับผลกระทบ (Severity)	ระยะเวลาติดต่อกลับ	ระยะเวลาการแก้ไขปัญหาเสร็จสิ้นนับจากที่ได้รับแจ้ง
Urgent อุปกรณ์โครงข่าย External Firewall ไม่สามารถใช้งานได้	30 minutes	4 (สี่) hours
High อุปกรณ์โครงข่าย External Firewall ทำงานผิดพลาด ซึ่งเป็นส่วนสำคัญที่ส่งผลกระทบต่อการดำเนินงานของธนาคาร	1 hour	8 (แปด) hours
Medium อุปกรณ์โครงข่าย External Firewall ทำงานผิดพลาด ซึ่งไม่เป็นส่วนสำคัญที่กระทบต่อการดำเนินงานของธนาคาร	2 hours	48 (สี่สิบแปด) hours
Low อุปกรณ์โครงข่าย External Firewall ทำงานผิดพลาด ซึ่งไม่เป็นส่วนสำคัญที่ไม่กระทบต่อการดำเนินงานของธนาคาร	4 hours	96 (เก้าสิบหก) hours

รวมถึงต้องจัดให้มีเจ้าหน้าที่ประสานงานพร้อมเบอร์โทรศัพท์และ/หรือช่องทางอื่น เพื่อบริการให้คำปรึกษา ตอบข้อซักถาม และให้ความช่วยเหลือในการแก้ไขปัญหาต่างๆ เกี่ยวกับอุปกรณ์โครงข่าย External Firewall ในวันและเวลาทำการของธนาคาร และจัดให้มีช่องทางอื่นที่สามารถติดต่อขอรับคำปรึกษานอกวันและเวลาทำการของธนาคารได้ตลอด 24 ชั่วโมง

6.4 มีการดำเนินการ Review Policy ตาม Best Practice และ Upgrade firmware เพื่อปรับปรุงระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ตามที่ธนาคารได้มีการร้องขอ

6.5 ดำเนินการ Configure อุปกรณ์โครงข่าย External Firewall ตามที่ธนาคารได้มีการร้องขอ

6.6 ต้องดำเนินการจัดทำรายละเอียด และขั้นตอนของการเข้ามาดำเนินการแก้ไขปัญหาหรือเหตุขัดข้องหรือความชำรุดบกพร่องของระบบฯ ให้กับธนาคารภายใน 7 วันนับถัดจากวันที่สามารถแก้ไขปัญหาเหตุขัดข้อง และ/หรือความชำรุดบกพร่องของระบบเสร็จสิ้นเป็นที่เรียบร้อยแล้ว และผู้ยื่นข้อเสนอที่ได้รับคัดเลือกต้องเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นจากการเข้าดำเนินการทั้งจำนวน

7. **การ Upgrade โปรแกรม**

ในระหว่างดำเนินการติดตั้งหรือภายในระยะเวลารับประกัน หาก Application Software หรือ Firmware หรือ Patch หรือระบบปฏิบัติการของอุปกรณ์โครงข่าย External Firewall มีการออก Version ใหม่ หรือพัฒนาปรับปรุง (Upgrade) ผู้ยื่นข้อเสนอที่ได้รับเลือกจะต้องแจ้งรายละเอียดการเปลี่ยนแปลงและผลกระทบที่เกิดขึ้นจากการเปลี่ยนแปลงดังกล่าวให้ธนาคารทราบ เพื่อใช้เป็นข้อมูลประกอบการตัดสินใจของธนาคาร และหากธนาคารประสงค์จะดำเนินการพัฒนาปรับปรุง (Upgrade) ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องดำเนินการพัฒนาปรับปรุง (Upgrade) ให้กับธนาคารโดยไม่คิดค่าใช้จ่ายเพิ่มเติม และดำเนินการให้แล้วเสร็จภายใน 7 วันนับจากได้รับแจ้งจากธนาคาร