แบบ บก. 06 เลขที่ 30/65
ลงวันที่ 2 มีนาคม 2565

**ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย**
**การจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง**

1. ชื่อโครงการ ซื้อระบบรักษาความปลอดภัย Firewall พร้อมติดตั้ง จำนวน 1 ระบบ (รายละเอียดตามเอกสารแนบท้าย)
   หน่วยงานเจ้าของโครงการ สังกัดฝ่ายเทคนิคและวิศกรรม
   สถาบันวิจัยแสงซินโครตรอน (องค์การมหาชน)

2. วิธีจัดซื้อจัดจ้าง ○ วิธีประกาศเชิญชวน ⊘ วิธีคัดเลือก ○ วิธีเฉพาะเจาะจง

3. วงเงินงบประมาณที่ได้รับจัดสรร **3,800,000.00** บาท (ตามใบขอซื้อ/จ้าง พท 21/65 ลว. 7 ธ.ค. 64)

4. วันที่กำหนดราคากลาง ราคาอ้างอิง **2 มีนาคม 2565** เป็นเงิน **3,799,784.00** บาท

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   1. ใบเสนอราคา บริษัท ไอ - ซีเคียว จำกัด
   2. ใบเสนอราคา บริษัท ไซเทค ซิสเต็ม จำกัด
   3. ใบเสนอราคา บริษัท เวิลด์ อินฟอร์เมชั่น เทคโนโลยี่ จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน
   6.1 นายมงคล ผานาค เจ้าหน้าที่ผู้กำหนดราคากลาง
   6.2 นายกิตติรัชต์ ฤกษ์บุรี เจ้าหน้าที่ผู้กำหนดราคากลาง
   6.3 นางสาวอธิการ ทองวัฒน์ เจ้าหน้าที่ผู้กำหนดราคากลาง

**หมายเหตุ :**

แหล่งที่มาของราคากลาง (ราคาอ้างอิง) ได้มาจากมติในที่ประชุมของเจ้าหน้าที่ผู้กำหนดราคากลาง โดยพิจารณาจากใบเสนอราคาตามท้องตลาดซึ่งมีผู้เสนอราคา จำนวน 3 ราย โดยผู้เสนอราคามีคุณสมบัติตรงตามสถาบันฯ กำหนด

# ตารางราคากลาง

| ลำดับ | รายการ | จำนวน | หน่วยนับ | ราคา/หน่วย (บาท) | ภาษีมูลค่าเพิ่ม 7% | ราคารวม/หน่วย (บาท) | ราคารวมทั้งสิ้น (บาท) |
|---|---|---|---|---|---|---|---|
| 1 | ระบบรักษาความปลอดภัย Firewall พร้อมติดตั้ง | 1 | ระบบ | 3,551,200.00 | 248,584.00 | 3,799,784.00 | 3,799,784.00 |
| **ราคากลางรวมทั้งสิ้น** | | | | | | 3,799,784.00 | |

# ขอบเขตงานและรายละเอียดคุณสมบัติของพัสดุ
# ระบบรักษาความปลอดภัย Firewall พร้อมติดตั้ง สถาบันวิจัยแสงซินโครตรอน (องค์การมหาชน) จำนวน 1 ระบบ

## 1. หลักการและเหตุผล

สถาบันวิจัยแสงซินโครตรอน (องค์การมหาชน) ได้มีการติดตั้งใช้งานระบบรักษาความปลอดภัย Firewall หลักและ Firewall สำรองคู่กันแบบ High Availability ภายในศูนย์คอมพิวเตอร์ของ สซ. เพื่อทำหน้าที่ป้องกันและรักษาความมั่นคงปลอดภัยให้แก่ระบบสารสนเทศของ สซ. อย่างต่อเนื่องตั้งแต่ปี 2557 จนถึงปัจจุบัน อย่างไรก็ตามระบบรักษาความปลอดภัย Firewall ดังกล่าว ผู้ผลิตได้มีการกำหนดระยะเวลาที่จะสิ้นสุดการสนับสนุนทางด้าน Hardware และ Software จากเจ้าของผลิตภัณฑ์ แล้ว

ดังนั้น เพื่อให้ระบบเครือข่ายของ สซ. มีความมั่นคงปลอดภัย สามารถให้บริการได้อย่างต่อเนื่องและรองรับการเชื่อมต่อ แบบ 10 Gbps สซ. มีความจำเป็นต้องจัดหาระบบรักษาความปลอดภัยเครือข่าย Firewall เพื่อทดแทนระบบเดิมให้สามารถรองรับกับเทคโนโลยีที่ก้าวหน้ามากขึ้น และเหมาะสมในเรื่องของการแบ่งขอบเขตของเครือข่าย รวมถึงความคงทนของการให้บริการของระบบสารสนเทศ เพื่อให้การป้องกันเครือข่ายทั้งหมดเป็นไปอย่างมีประสิทธิภาพ และเป็นประโยชน์สูงสุดกับ สซ.

## 2. วัตถุประสงค์

เพื่อทดแทนระบบรักษาความปลอดภัยของระบบเครือข่ายเดิมในการป้องกันภัยคุกคามทางระบบสารสนเทศ การปิดช่องโหว่ และการป้องกันการโจมตีระบบเครือข่าย และป้องกันการโจมตีระบบเครือข่ายในรูปแบบใหม่ที่เกิดขึ้นในปัจจุบันและอนาคต รวมถึงรองรับการเชื่อมต่อเครือข่าย แบบ 10 Gbps ได้อย่างมีประสิทธิภาพ

## 3. ข้อกำหนดทั่วไป

คำนิยาม ในรายการข้อกำหนดฉบับนี้ได้กำหนดให้

3.1. **สซ.** หมายถึง สถาบันวิจัยแสงซินโครตรอน (องค์การมหาชน) หรือผู้แทนที่ สซ. แต่งตั้งและมอบหมายให้ดำเนินการคัดเลือก ควบคุม ตรวจสอบ กำกับดูแล การปฏิบัติงานของผู้ขายให้เป็นไปตามสัญญาและรายการข้อกำหนดนี้

3.2. **ผู้เสนอราคา** หมายถึง บุคคลหรือนิติบุคคลที่ยื่นข้อเสนอและราคาต่อ สซ. เพื่อขอรับการคัดเลือกเป็นผู้ขายดำเนินการตามรายการข้อกำหนดนี้

3.3. **ผู้ขาย หรือ ผู้รับจ้าง** หมายถึง บุคคลหรือนิติบุคคลที่ สซ. ตกลงว่าจ้างเป็นหนังสือให้ดำเนินการตามรายการข้อกำหนดฉบับนี้ และให้รวมถึงบุคคลที่อยู่ภายใต้ความรับผิดชอบของผู้ขาย หรือ ผู้รับจ้าง ทุกกรณีด้วย

4. <u>ขอบเขตการดำเนินงาน</u>

ผู้ขายต้องดำเนินการจัดหาและติดตั้งระบบรักษาความปลอดภัย Firewall บนระบบเครือข่ายภายในให้สามารถใช้งานได้ดีตามหลักวิธีปฏิบัติที่ดีและมาตรฐานวิชาชีพที่เกี่ยวข้องโดยมีขอบเขตของการดำเนินงานภายใต้ความรับผิดชอบและค่าใช้จ่ายของผู้ขายทั้งหมดไม่น้อยกว่าที่กำหนดดังต่อไปนี้

4.1. อุปกรณ์ทั้งหมดที่จัดหาในครั้งนี้ต้องเป็นของใหม่ ไม่เคยใช้งานมาก่อน ผลิตจากผู้ผลิตที่เชื่อถือได้ เป็นผลิตภัณฑ์ที่ใช้งานอย่างแพร่หลายโดยมีผู้ใช้งานแล้วภายในประเทศไทยไม่น้อยกว่า 1 ราย โดยมีเอกสาร Customer list ประกอบและมีคุณลักษณะเฉพาะ (Specification) ไม่ต่ำกว่าที่กำหนดในข้อ 5

4.2. ผู้ขายต้องทำการติดตั้งระบบรักษาความปลอดภัย Firewall พร้อมซอฟต์แวร์ที่เกี่ยวข้องจำนวน 2 ชุด โดยใช้วิธีตัวตายตัวแทน หากระบบรักษาความปลอดภัย Firewall เครื่องหนึ่งไม่ทำงาน ระบบรักษาความปลอดภัย Firewall อีกเครื่องจะสามารถทำงานทดแทนได้ทันที โดยมีเงื่อนไขในการติดตั้งดังรายละเอียด ในข้อ 6

4.3. ผู้ขาย ต้องทำการทดสอบการติดตั้ง และ/หรือการใช้งานของระบบรักษาความปลอดภัย Firewall ที่ส่งมอบ พร้อมทั้งแนะนำการใช้งานในลักษณะ On the Job Training ให้แก่ผู้ปฏิบัติงาน ของ สซ. รายละเอียดเพิ่มเติมได้กำหนดไว้ในข้อที่ 7

4.4. ผู้ขาย จะต้องรับผิดชอบดำเนินการบำรุงรักษา (Maintenance: MA) อุปกรณ์ดังกล่าวเป็นระยะเวลา 3 ปีติดต่อกันนับจากวันที่ สซ. ตรวจรับงานงวดสุดท้าย รายละเอียดเพิ่มเติมได้กำหนดไว้ในข้อที่ 8

4.5. ผู้ขาย จะต้องรับประกันการชำรุดเสียหาย ใช้งานไม่ได้ของระบบรักษาความปลอดภัย Firewall บางส่วนหรือทั้งหมดที่ส่งมอบให้ สซ. เป็นระยะเวลาตามที่กำหนดนับจากวันที่ สซ. ตรวจรับงานงวดสุดท้าย รายละเอียดเพิ่มเติมได้กำหนดไว้ในข้อ 9

4.6. ผู้ขายต้องมีทีมงาน และต้องยื่นหลักฐานแสดงคุณสมบัติผู้ที่มีความรู้หรือความเชี่ยวชาญเกี่ยวกับระบบและการติดตั้ง รวมทั้งบริการหลังการขายเป็นอย่างดี โดยมีบุคลากรที่ได้รับวุฒิการศึกษาด้านวิศวกรรมคอมพิวเตอร์ หรือวิทยาศาสตร์คอมพิวเตอร์ ที่ได้รับประกาศนียบัตรทางด้านระบบรักษาความปลอดภัยสารสนเทศหรือด้านเครือข่าย และต้องเป็นพนักงานประจำของผู้ประกอบการที่เสนอราคา โดยให้แนบประวัติ วุฒิบัตร พร้อมใบประกาศนียบัตรจำนวนไม่น้อยกว่า 2 ท่าน ณ วันที่ส่งมอบ

5. <u>รายละเอียดคุณลักษณะเฉพาะของระบบรักษาความปลอดภัย Firewall พร้อมซอฟต์แวร์ที่เกี่ยวข้อง จำนวน 2 ชุด</u>

ผู้ขายหรือผู้รับจ้าง ต้องจัดหาระบบรักษาความปลอดภัย Firewall ใหม่ ยี่ห้อ Palo alto พร้อมซอฟต์แวร์ที่เกี่ยวข้อง จำนวน 2 ชุดที่เป็นผลิตภัณฑ์รุ่นเดียวกันและมีผู้ผลิตรายเดียวกัน โดยมีคุณสมบัติไม่น้อยกว่า ดังต่อไปนี้

5.1. รายละเอียดคุณสมบัติเฉพาะทางเทคนิคของอุปกรณ์ Firewall โดยมีคุณสมบัติไม่น้อยกว่าดังต่อไปนี้

5.1.1. เป็นอุปกรณ์ Appliance Firewall หรือ Chassis ที่สร้างขึ้นเพื่อทำหน้าที่ตรวจจับและควบคุม Application, User และ Content โดยแยก หน่วยประมวลผลสำหรับบริหารจัดการ Management/Control Plane และ หน่วยประมวลผลสำหรับข้อมูล (Data Plane) ออกจากกัน หรือนำเสนอ Appliance สำหรับทำ Management แยกออกจากตัวอุปกรณ์

5.1.2. มี Firewall Throughput ไม่น้อยกว่า 4 Gbps และ Threat prevention Throughput ไม่น้อยกว่า 2 Gbps ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix และจำนวน Max Sessions ได้ไม่น้อยกว่า 1,000,000 sessions และ New Sessions ไม่น้อยกว่า 52,800 ต่อวินาที

5.1.3. มี Network Interface แบบ 10/100/1000 Copper ไม่ต่ำกว่า 12 พอร์ต, ช่องเชื่อมต่อแบบ 1G SFP ไม่ต่ำกว่า 4 พอร์ต และช่องเชื่อมต่อแบบ 1G/10G SFP/SFP+ ไม่ต่ำกว่า 4 พอร์ต

5.1.4. มี Interface แบบ 10/100/1000 ไม่ต่ำกว่า 2 พอร์ต และ Interface แบบ 10G SFP+ ไม่ต่ำกว่า 1 พอร์ต สำหรับการทำ High Availability (HA) โดย Interface ดังกล่าวแยกออกมาจาก Network Interface (Dedicate interface HA)

5.1.5. อุปกรณ์ที่นำเสนอต้องสามารถทำ Client VPN (Remote Access) บนโปรโตคอล IPSec และ SSL ได้ไม่ต่ำกว่า 1,024 tunnels รวมทั้งสามารถทำงานกับระบบปฏิบัติการ Windows (ทั้ง 32 และ 64 bits) ได้เป็น อย่างน้อย

5.1.6. อุปกรณ์ต้องมี SSD สำหรับเก็บข้อมูลระบบไม่ต่ำกว่า 240GB หรือเสนออุปกรณ์เก็บ log เพิ่มเติมที่มีขนาด disk ขนาด 240GB ที่เป็นยี่ห้อเดียวกับ Firewall ที่นำเสนอ

5.1.7. สามารถทำ NAT (Network Address Translation) และ PAT (Port Address Translation) หรือ Port Translation ได้

5.1.8. สามารถใช้กับระบบเครือข่ายแบบ VLAN ผ่าน Protocol 802.1Q ได้

5.1.9. สามารถทำงานแบบ Route Mode (Layer 3) และ Transparent Mode Firewall (Bridge Mode) ได้

5.1.10. สามารถทำ Dynamic Routing Protocol ได้แก่ RIP, OSPF และ BGP เป็นอย่างน้อย

5.1.11. สามารถรับ Syslog จากระบบที่มีอยู่ได้ เพื่อใช้ในการยืนยันตัวตน ของ User ที่ใช้งาน โดยสามารถทำได้บนตัวอุปกรณ์ Firewall ไม่ต้องมีระบบใด ๆ เพิ่มเติม

5.1.12. สามารถทำการตรวจสอบทราฟฟิคที่เข้ารหัส SSL ด้วยการทำ SSL decryption (ทั้งแบบ Inbound และ Outbound )

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

5.1.14. สามารถเรียกดูรายงานสรุปข้อมูลของ Data ในรูปแบบของกราฟฟิคได้ และสามารถส่งรายงานผ่านทาง Email แบบอัตโนมัติได้ โดยสามารถทำรายงานใน Category ต่าง ๆ อย่างน้อย ดังนี้

5.1.14.1. Application

5.1.14.2. Traffic

5.1.14.3. Threats

5.1.14.4. URL Filtering

5.1.15. สามารถปรับแต่งรายงานตามความต้องการ (Custom Report) และส่งออก (Export) ให้อยู่ในรูปแบบ PDF ได้เป็นอย่างน้อย

5.1.16. มี Power Supply แบบ Redundant หรือ Hot Swap

5.1.17. สามารถรองรับการติดตั้งเพื่อทำ High Availability (HA) แบบ Active/Passive และ Active/Active ได้

5.1.18. สามารถบริหารจัดการอุปกรณ์แบบ Web-based Management (HTTPS) และ Command Line Interface ได้

5.1.19. สามารถทำส่ง log (Forward Log) ด้วย HTTP-based API ไปยังอุปกรณ์ 3rd party หรือนำเสนอระบบอื่นเพิ่มเติมได้

5.1.20. สามารถขยาย Virtual Systems เพิ่มเติมได้สูงสุดถึง 6 System ในอนาคต

5.1.21. ผลิตภัณฑ์ที่นำเสนอจะต้องอยู่ใน Leader Quadrant ของ Gartner Magic Quadrant ด้าน Enterprise Network Firewalls ในปีล่าสุด

5.1.22. ต้องรับประกันอุปกรณ์เป็นเวลาอย่างน้อย 3 ปี โดยระบบต้องสามารถแสดงวันที่สิ้นสุดได้ในระบบ หรือตัวอุปกรณ์ที่นำเสนอ

5.1.23. ผู้เสนอราคาต้องแสดงหลักฐานการมีสิทธิ์เสนอราคาสำหรับโครงการนี้ โดยต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจาก บริษัทเจ้าของผลิตภัณฑ์ (เอกสารแนบตอนเสนอราคา)

5.2. รายละเอียดคุณลักษณะระบบป้องกันภัยคุกคาม (Threat Prevention Subscriptions) โดยเมื่อเปิดการใช้งาน Intrusion Prevention (IPS), Command-and-Control protection (Antispyware) และ Malware protection พร้อมกัน จะต้องรองรับ Throughput ไม่น้อยกว่า 2.6 Gbps และมีคุณสมบัติอย่างน้อยดังต่อไปนี้

5.2.1. มีสถาปัตยกรรมการตรวจสอบภัย คุกคามแบบ Single-Pass (Single-pass scanning architecture)

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

5.2.3. สามารถตรวจจับและป้องกันport Scans, buffer Overflows, remote code execution, protocol fragmentation and obfuscation และ Non-RFC Compliant ได้เป็นอย่างน้อย รวมทั้งสามารถปรับแต่งรูปแบบของภัยคุกคาม (Custom Vulnerability signatures) ได้ตาม ความต้องการ

5.2.4. สามารถตรวจจับและป้องกัน Virus บนโปรโตคอล HTTP, FTP, IMAP, POP3, SMTP และ SMB รวมถึง Virus ที่ฝัง ตัวมากับ PDF, yeb Content, Microsoft Office documents และ Compressed Files ได้

5.2.5. สามารถทำ DNS Sinkhole เพื่อป้องกันการเข้าถึง malicious domain, เพื่อป้องกันการจารกรรมข้อมูลออกจากระบบ (preventing exfiltration)

5.2.6. มีระยะเวลารับประกันและการบำรุงรักษาเป็นระยะเวลาไม่น้อยกว่า 3 ปี

5.3. รายละเอียดคุณลักษณะระบบป้องกัน Advanced Persistent Threats (Wildfire Subscriptions) ระบบตรวจจับ Malware, exploit แบบ Cloud-Based เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero-day Malware ) ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติโดยมีคุณสมบัติอย่างน้อยดังนี้

5.3.1. สามารถทำ Static Analysis, Dynamic Analysis, Machine Learning และBare metal Analysis ได้

5.3.2. สามารถตรวจจับได้ในหลายๆ Protocol เช่น SMTP, POP3, SMB, FTP, IMAP,HTTP และ HTTPS

5.3.3. สามารถตรวจสอบและป้องกัน zero-day malware จากไฟล์ชนิดต่าง ๆ อย่างน้อยดังนี้ EXE, DLL, all Microsoft Office file types, PDF, Java applets, including JAR and CLASS; RAR and 7 ZIP archive files, Linux ELFs, Mach-O, DMG, PKG, JScript, VBScript, PowerShell, Shell Script, APKs ไฟล์และลิงค์ที่แนบมากับอีเมล์ได้

5.3.4. มี report แสดงรายละเอียดการทำงานของ malware ที่ตรวจจับได้ทั้ง host-base และ network-base activity

5.3.5. สามารถสร้าง signature ขึ้นมาเพื่อป้องกันได้หลังจากตรวจพบ malware ภายในระยะเวลาไม่ถึง 5 นาที

5.3.6. มีระยะเวลารับประกันและการบำรุงรักษาเป็นระยะเวลาไม่น้อยกว่า 3 ปี

5.4. รายละเอียดคุณลักษณะระบบการตรวจสอบ DNS security (DNS Security Subscriptions) หรือ DNS Filtering ที่สามารถป้องกันระบบ DNS จากการโจมตีของ Command-and-Control และการจารกรรมข้อมูล (Data Theft) โดยมีคุณสมบัติอย่างน้อยต่อไปนี้

5.4.1. สามารถทำนายและหยุดการเข้าถึง malicious domains จาก domain generation algorithm-based (DGA) โดยการใช้ Machine learning ได้

5.4.2. มีระบบ Machine Learning ที่สามารถตรวจจับ traffic Command and Control และ Data Theft ที่ฝังมากับ DNS tunneling โดยการใช้ Algorithm ดังต่อไปนี้ query rate and patterns, entropy, n-gram frequency analysis

5.4.3. มีระยะเวลารับประกันและการบำรุงรักษาเป็นระยะเวลาไม่น้อยกว่า 3 ปี

5.5. รายละเอียดคุณลักษณะระบบกลั่นกรอง URL website (URL Filtering Subscriptions) ระบบกลั่นกรองการเข้าถึง website (URL Filtering) โดยมีคุณสมบัติอย่างน้อยต่อไปนี้

5.5.1. สามารถกำหนดนโยบายการเข้าถึง website (URL Filtering หรือ Web Filtering), สามารถติดตามและควบคุมการเข้าถึงเว็บได้ตาม Category รวมทั้งสามารถปรับแต่ง Custom Category ได้ตามต้องการ

5.5.2. สามารถป้องกันการเข้าถึง website ที่ไม่อนุญาตโดยทางอ้อม ผ่านทาง Search Engine Cache (เช่น Google cache) และ Translation Site (เช่น Google translate) ได้

5.5.3. มีความสามารถในการป้องกันการรั่วไหลของชื่อผู้ใช้และรหัสผ่านขององค์กร ผ่านการใช้งาน website ที่เข้าข่ายเป็น Phishing page ได้ (Credential Phishing Prevention)

5.5.4. มีระยะเวลารับประกันและการบำรุงรักษาเป็นระยะเวลาไม่น้อยกว่า 3 ปี

## 6. เงื่อนไขการติดตั้ง

6.1. ในระหว่างการติดตั้งอุปกรณ์ตามโครงการนั้น จะต้องไม่มีผลกระทบต่อการทำงานของระบบงานต่าง ๆ หรือก่อให้เกิดความเสียหายแก่ สซ. และในส่วนการติดตั้งอุปกรณ์เพิ่มเติมในส่วนของส่วนเทคโนโลยีสารสนเทศและสื่อสาร หากเกิดผลกระทบหรือความเสียหายและต้องติดตั้งอุปกรณ์เพิ่มเติมต่าง ๆ ผู้ขายต้องเป็นผู้ดำเนินการแก้ไขให้สามารถใช้งานได้ตามปกติและรับผิดชอบค่าใช้จ่ายในการแก้ไขและอุปกรณ์ต่าง ๆ ที่ต้องติดตั้งเพิ่มเติมที่เกิดขึ้นทั้งสิ้น

6.2. ผู้ขายต้องดำเนินการติดตั้งและกำหนดค่าต่าง ๆ ของอุปกรณ์ทั้งหมด ให้สามารถใช้งานกับระบบต่าง ๆ ในเครือข่ายของ สซ. ได้ตามปกติ

## 7. เงื่อนไขการฝึกอบรมและการถ่ายทอดความรู้

7.1. ผู้ขายจะต้องดำเนินการจัดหาหลักสูตรการฝึกอบรมให้แก่ผู้ดูแลระบบของส่วนงานเทคโนโลยีสารสนเทศในการดูแลติดตั้งและการใช้งานอุปกรณ์ โดยมีรายละเอียดดังต่อไปนี้

7.1.1. ผู้ขายต้องเสนอแผนการฝึกอบรมการดูแล ติดตั้ง และการใช้งานสำหรับผู้ดูแลระบบ ของส่วนงานเทคโนโลยีสารสนเทศ พร้อมการส่งมอบและทดสอบการใช้งานให้แล้วเสร็จตามระยะเวลาที่กำหนด

7.2. ผู้ขายต้องจัดทำคู่มือภาษาไทย สำหรับเจ้าหน้าที่เรียนรู้ด้วยตนเอง ประกอบไปด้วยคู่มือการดูแล ติดตั้ง และการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall) จำนวนไม่น้อยกว่า 3 ชุด พร้อมไฟล์เอกสารบันทึกลงใน CD-ROM หรือ Flash Drive

8. การบำรุงรักษา (Maintenance)

ผู้ขายต้องทำการบำรุงรักษา ซ่อมแซม แก้ไข ปรับปรุง และ/หรือเปลี่ยนทดแทนระบบให้อยู่ในสภาพที่ใช้งานได้ดีตลอดระยะเวลา 3 ปีติดต่อกันนับจากวันที่ สซ. ตรวจรับงานงวดสุดท้าย ตามหลักวิธีปฏิบัติที่ดีและมาตรฐานวิชาชีพที่เกี่ยวข้อง โดยขอบเขตของงานบำรุงรักษาต้องประกอบด้วย

1) การบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) เพื่อให้ระบบอยู่ในสภาพที่ใช้งานได้ดีเป็นปกติและมีประสิทธิภาพตลอดเวลา

2) แก้ไขข้อขัดข้องต่าง ๆ ที่เกิดขึ้นกับระบบ

3) ซ่อมแซม แก้ไข และ/หรือเปลี่ยนทดแทนส่วนที่ใช้งานไม่ได้ หรือใช้งานได้แต่ไม่เป็นไปตามสภาพปกติของระบบ

4) ปรับแต่งประสิทธิภาพ (Performance Tuning) ระบบเพื่อเพิ่มประสิทธิผลการบำรุงรักษา ประกอบด้วยงาน 2 ส่วนย่อย ดังนี้

8.1. การบำรุงรักษาซอฟต์แวร์ระบบ

ผู้ขายจะต้องรับผิดชอบดำเนินการไม่น้อยกว่าที่กำหนดตามรายละเอียดดังนี้

ในสภาพการทำงานตามปกติของระบบ ผู้ขายต้องทำการตรวจสอบและบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ณ สถานที่ติดตั้งเพื่อให้แน่ใจได้ว่าระบบจะสามารถทำงานได้อย่างถูกต้องอย่างน้อย 6 เดือน ต่อครั้ง โดยต้องทำการแจ้งให้เจ้าหน้าที่ทราบกำหนดการเข้าตรวจสอบระบบล่วงหน้าอย่างน้อย 5 วันทำการ โดยผู้ขายต้องแจ้งข้อมูลให้ทราบไม่น้อยกว่า ดังนี้

ก. งวดงานการบำรุงรักษา

ข. ชื่อรายการที่ทำการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance)

ค. วิธีการ และขั้นตอนการทำงาน

ง. วัน เวลาที่ทำการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance)

จ. วิธีการทดสอบการทำงานของระบบคอมพิวเตอร์หลังการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) เพื่อให้มั่นใจได้ว่าระบบสามารถทำงานได้ดีดังเดิม

รายละเอียดของงานบำรุงรักษาและซ่อมแซมจะต้องไม่น้อยกว่าดังนี้

- ตรวจสอบการทำงานของ Software ต่าง ๆ ให้สามารถใช้งานได้ดีตามปกติ และอย่างมีประสิทธิภาพ
- ตรวจสอบฐานข้อมูลให้อยู่ในสภาพสมบูรณ์
- ตรวจสอบข้อผิดพลาดที่เกิดขึ้นจากไฟล์ (Log File)
- ทำการ Apply patch กรณีมีความจำเป็นเพื่อแก้ไขปัญหา หรือ ข้อบกพร่อง และหากมีเหตุการณ์ที่จะต้องทำการตัดสินใจอย่างใดอย่างหนึ่งที่มีผลกระทบกับระบบฐานข้อมูลและ/หรือข้อมูล ผู้ขายจะต้องขอความเห็นชอบจาก สซ. ก่อนที่จะดำเนินการใด ๆ
- ผู้ขายจะต้องทำการติดตั้ง Version ใหม่ให้ ถ้าหากมีการปรับปรุงโปรแกรมเพิ่มเติม และหากมีเหตุการณ์ที่จะต้องทำการตัดสินใจอย่างใดอย่างหนึ่งที่มีผลกระทบกับระบบฐานข้อมูลและ/หรือข้อมูล ผู้ขายจะต้องขอความเห็นชอบจาก สซ. ก่อนที่จะดำเนินการใด ๆ

- ในกรณีที่ผู้ดูแลระบบต้องการคำปรึกษาในการดูแลระบบ ผู้ขายต้องให้คำปรึกษาได้ทั้งทางโทรศัพท์ โทรสาร และจดหมายอิเล็กทรอนิกส์ โดยมีระยะเวลาตอบสนองไม่ช้ากว่า 1 วัน หลังจากได้รับคำร้องขอ

- ในกรณีที่ระบบมีการใช้งานที่ผิดปกติ เกิดการชำรุดบกพร่องหรือใช้งานไม่ได้บางส่วนหรือทั้งหมด ผู้ขายต้องรับเรื่องทันทีเมื่อมีปัญหา โดยใช้สายด่วนสอบถาม และให้คำปรึกษาแนะนำทางโทรศัพท์เพื่อแก้ปัญหาเฉพาะหน้าทันทีที่ได้รับแจ้ง ทางโทรศัพท์ พร้อมทั้งตรวจสอบการแจ้งปัญหาจากทางระบบ E-mail การแก้ไขปัญหาระบบเบื้องต้นจะต้องสามารถกระทำผ่าน Online ภายในระยะเวลา 4 ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้ง และหากการแก้ไขปัญหาผ่าน Online ไม่สำเร็จ ผู้ขายจะต้องจัดส่งพนักงานมาทำการแก้ไขซ่อมแซมระบบภายในวันทำการถัดไป (Next Business Day; NBD)

- ในกรณีที่ระบบมีการใช้งานที่ผิดปกติ เกิดการชำรุดบกพร่องเล็กน้อยซึ่งไม่มีผลกระทบต่อการทำงานหลักตามปกติ ผู้ขายจะต้องให้คำปรึกษาแนะนำทางโทรศัพท์ หรือทำการแก้ไขปัญหาที่ได้รับแจ้งผ่าน Online ภายในระยะเวลาวันทำการ 3 วันนับแต่เวลาที่ได้รับแจ้ง และหากการแก้ไขปัญหาผ่าน Online ไม่สำเร็จลุล่วง ผู้ขายจะต้องจัดส่งพนักงานมาทำการแก้ไขซ่อมแซมระบบภายในระยะเวลาวันทำการ 7 วันนับตั้งแต่ที่ได้รับแจ้ง

- ในกรณีที่ระบบเกิดการชำรุดเสียหายและต้องเปลี่ยนอุปกรณ์ ผู้ขายจะต้องเข้าดำเนินการช่วยเหลือในการเปลี่ยนอุปกรณ์ หลังจากได้รับอุปกรณ์จากเจ้าของผลิตภัณฑ์

- ในกรณีที่มีปัญหาที่เกิดจากโปรแกรม เช่น Bug เป็นต้นผู้ขายจะต้องทำการเปิดเคสซัพพอร์ตไปยังผู้ผลิตเพื่อทำการแก้ไขในอนาคต

- การซ่อมแซมระบบงานดังกล่าวข้างต้น เมื่อผู้ขายดำเนินการแล้วเสร็จจะต้องแจ้งเจ้าหน้าที่ สซ. ที่รับผิดชอบหรือได้รับมอบหมายทราบทันที และจัดทำรายงานการซ่อมแซม แก้ไข ให้กับ สซ. ภายในระยะเวลา 3 วันนับแต่เวลาที่ดำเนินการแล้วเสร็จผ่านจดหมายอิเล็กทรอนิกส์ (E-Mail)

- การบำรุงรักษาและซ่อมแซมระบบจะต้องกระทำในเวลาทำการตั้งแต่เวลา 09.00 น. ถึง 16.30 น. ของวันจันทร์ถึงวันศุกร์ และ/หรือวันและเวลาที่ สซ. ตกลงกันเป็นอย่างอื่น (ยกเว้นวันเสาร์ วันอาทิตย์ และวันหยุดนักขัตฤกษ์)

- ผู้ขายจะต้องจัดให้มีการรับประกันคุณภาพการให้บริการของระบบ

8.2. การบำรุงรักษาฮาร์ดแวร์ระบบ

ผู้ขายจะต้องรับผิดชอบดำเนินการไม่น้อยกว่าที่กำหนดตามรายละเอียดดังนี้

1) การบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ในสภาพการทำงานตามปกติของระบบ ผู้ขายต้องทำการตรวจสอบและบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ณ สถานที่ติดตั้งเพื่อให้แน่ใจได้ว่าระบบจะสามารถทำงานได้อย่างถูกต้องอย่างน้อย 6 เดือน ต่อครั้ง โดยต้องทำการแจ้งให้เจ้าหน้าที่ทราบกำหนดการเข้าตรวจสอบระบบล่วงหน้าอย่างน้อย 5 วันทำการ โดยผู้ขายต้องแจ้งข้อมูลให้ทราบไม่น้อยกว่า ดังนี้

ก. งวดงานการบำรุงรักษา

ข. ชื่อรายการที่ทำการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance)

ค. วิธีการ และขั้นตอนการทำงาน

ง. วัน เวลาที่ทำการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance)

จ. วิธีการทดสอบการทำงานของระบบคอมพิวเตอร์หลังการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) เพื่อให้มั่นใจได้ว่าระบบสามารถทำงานได้ดีดังเดิม

รายละเอียดของงานบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ไม่น้อยกว่าดังนี้

- ตรวจสภาพและทำความสะอาดภายนอกและภายในของอุปกรณ์ฮาร์ดแวร์ให้สะอาดเรียบร้อยและอยู่ในสภาพที่ใช้งานได้ดีตามปกติ
- ทำความสะอาดและตรวจสอบแผงวงจรหลักและ Connector ต่าง ๆ ให้สะอาดเรียบร้อย แน่นหนาและไม่ชำรุด โดยให้อยู่ในสภาพที่ใช้งานได้ดีตามปกติ
- การบำรุงรักษาและซ่อมแซมระบบจะต้องกระทำในเวลาทำการตั้งแต่เวลา 09.00 น. ถึง 16.30 น. ของวันจันทร์ถึงวันศุกร์ และ/หรือวันและเวลาที่ สซ. ตกลงกันเป็นอย่างอื่นโดยจะต้องหลีกเลี่ยงผลกระทบต่อการปฏิบัติงานของผู้ใช้งานระบบคอมพิวเตอร์ให้น้อยที่สุด (ยกเว้นวันเสาร์ วันอาทิตย์ และวันหยุดนักขัตฤกษ์)

2) การบำรุงรักษาเชิงซ่อมแซม (Corrective Maintenance) ผู้ขายต้องรับผิดชอบ จัดการดำเนินการ ซ่อมแซมแก้ไขอุปกรณ์ป้องกันเครือข่ายให้อยู่ในสภาพใช้งานได้ดีตามปกติตลอดระยะเวลาที่กำหนด หากอุปกรณ์ป้องกันเครือข่ายขัดข้องบางส่วนหรือทั้งหมดจะต้องดำเนินการดังนี้

- ผู้ขายต้องจัดหาและใช้อุปกรณ์ อะไหล่แท้ที่ผู้ผลิตเลือกใช้หรือที่ สซ. เห็นชอบสำหรับใช้ในการซ่อมแซมเปลี่ยนทดแทน
- ในกรณีที่ผู้ดูแลระบบต้องการคำปรึกษาในการดูแลระบบ ผู้ขายต้องให้คำปรึกษาได้ทั้งทางโทรศัพท์ โทรสาร และจดหมายอิเล็กทรอนิกส์ โดยมีระยะเวลาตอบสนองไม่ช้ากว่า 1 วัน หลังจากได้รับคำร้องขอ
- ในกรณีที่อุปกรณ์เครือข่ายมีการใช้งานที่ผิดปกติ เกิดการชำรุดบกพร่องหรือใช้งานไม่ได้บางส่วนหรือทั้งหมด ผู้ขายต้องรับเรื่องทันทีเมื่อมีปัญหา โดยใช้สายด่วนสอบถาม และให้คำปรึกษาแนะนำทางโทรศัพท์ เพื่อแก้ปัญหาเฉพาะหน้าทันทีที่ได้รับแจ้ง ทางโทรศัพท์ พร้อมทั้งตรวจสอบการแจ้งปัญหาจากทางระบบ E-mail การแก้ไขปัญหาระบบเบื้องต้นจะต้องสามารถกระทำผ่าน Online ภายในระยะเวลา 4 ชั่วโมง นับตั้งแต่เวลาที่ได้รับแจ้ง และหากการแก้ไขปัญหาผ่าน Online ไม่สำเร็จ ผู้ขายจะต้องจัดส่งพนักงานมาทำการแก้ไขซ่อมแซมระบบภายในวันทำการถัดไป (Next Business Day; NBD)
- ในกรณีที่อุปกรณ์เครือข่ายมีการใช้งานที่ผิดปกติ เกิดการชำรุดบกพร่องเล็กน้อยซึ่งไม่มีผลกระทบต่อการทำงานหลักตามปกติ ผู้ขายจะต้องให้คำปรึกษาแนะนำทางโทรศัพท์ หรือทำการแก้ไขปัญหาที่ได้รับแจ้งผ่าน Online ภายในระยะเวลาวันทำการ 3 วันนับแต่เวลาที่ได้รับแจ้ง และหากการแก้ไขปัญหาผ่าน Online ไม่สำเร็จลุล่วง ผู้ขายจะต้องจัดส่งพนักงานมาทำการแก้ไขซ่อมแซมระบบภายในระยะเวลาวันทำการ 7 วัน นับตั้งแต่ที่ได้รับแจ้ง

- การซ่อมแซมอุปกรณ์เครือข่ายดังกล่าวข้างต้น เมื่อผู้ขายดำเนินการแล้วเสร็จจะต้องแจ้งเจ้าหน้าที่ สซ. ที่รับผิดชอบหรือได้รับมอบหมายทราบทันที และจัดทำรายงานการซ่อมแซม แก้ไข ให้กับ สซ. ภายในระยะเวลา 3 วันนับแต่เวลาที่ดำเนินการแล้วเสร็จผ่านจดหมายอิเล็กทรอนิกส์ (E-Mail)
- การบำรุงรักษาและซ่อมแซมระบบจะต้องกระทำในเวลาทำการตั้งแต่เวลา 09.00 น. ถึง 16.30 น. ของวันจันทร์ถึงวันศุกร์ และ/หรือวันและเวลาที่ สซ. ตกลงกันเป็นอย่างอื่น (ยกเว้นวันเสาร์ วันอาทิตย์ และวันหยุดนักขัตฤกษ์)

**9. <u>การรับประกันการชำรุดเสียหาย</u>**

9.1. ผู้ขายหรือผู้รับจ้าง ต้องรับประกันการชำรุดเสียหายหรือการใช้งานไม่ได้บางส่วนหรือทั้งหมดของอุปกรณ์เครือข่าย (Hardware) เป็นระยะเวลา 3 ปี (36 เดือน) ติดต่อกันนับตั้งแต่วันถัดจากวันที่ สซ. ตรวจรับมอบงาน

9.2. ผู้ขายหรือผู้รับจ้าง ต้องรับประกันการชำรุดเสียหายหรือการใช้งานไม่ได้บางส่วนหรือทั้งหมดของโปรแกรมและซอฟต์แวร์ (Software) เป็นระยะเวลา 3 ปี (36 เดือน) ติดต่อกันนับตั้งแต่วันถัดจากวันที่ สซ. ตรวจรับมอบงาน

**10. การส่งมอบงาน**

ผู้ขายจะต้องดำเนินการและส่งมอบผลงานให้ สซ. ตามเงื่อนไขและเวลาที่กำหนดดังนี้

10.1. ผู้ขายจะต้องดำเนินการส่งมอบอุปกรณ์โดยมีรายละเอียดตามข้อ 4.1 ให้ครบถ้วนภายใน 90 วันนับถัดวันที่ลงนามในสัญญา

10.2. ผู้ขายจะต้องดำเนินการตามข้อ 4.2 - 4.3 แล้วเสร็จพร้อมทั้งจัดส่งรายงานผลการดำเนินงานภายใน 120 วันนับถัดวันที่ลงนามในสัญญา

**11. <u>การจ่ายเงิน</u>**

สซ. จะจ่ายเงินค่างานเป็นงวดซึ่งแต่ละงวดจะถึงกำหนดชำระเมื่อผู้ขายได้ดำเนินงานตามเงื่อนไขและรายละเอียดแล้วเสร็จในแต่ละขั้นตอน โดยผู้ขายจะต้องแจ้งขอส่งมอบงานที่ได้ดำเนินการแล้วเสร็จให้ สซ. เป็นลายลักษณ์อักษร ไม่น้อยกว่า 3 วันทำการ เพื่อให้คณะกรรมการตรวจรับพัสดุได้ตรวจสอบ พิจารณาให้ความเห็นชอบ และใช้เป็นหลักฐานในการเบิกจ่ายเงินค่างาน โดยจะจ่ายเงินค่างานหลักจากตรวจรับงานในแต่ละงวดเรียบร้อยแล้ว โดยแบ่งจ่ายค่างานออกเป็น 2 งวดดังนี้

**งวดที่ 1** จ่ายให้ร้อยละ 70 ของมูลค่าของสัญญา เมื่อผู้ขายได้ดำเนินการตามข้อ 10.1 แล้วเสร็จและ สซ. ตรวจรับแล้ว

**งวดที่ 2** จ่ายให้ร้อยละ 30 ของมูลค่าของสัญญา เมื่อผู้ขายได้ดำเนินการตามข้อ 10.2 แล้วเสร็จครบถ้วนและ สซ. ตรวจรับแล้ว

12. การปรับเนื่องจากการไม่ปฏิบัติตามสัญญา

12.1. ในกรณีที่ผู้ขายไม่สามารถปฏิบัติตามสัญญาโดยไม่สามารถส่งมอบอุปกรณ์ทั้งหมดหรือบางส่วนได้ตามกำหนดจะต้องชำระค่าปรับเป็นรายวันในอัตราร้อยละ 0.2 ของราคาค่างานทั้งหมด นอกจากนี้ผู้เสนอราคายินยอมให้ สช. เรียกค่าเสียหายอันเกิดจากการที่ผู้เสนอราคาทำให้เกิดความเสียหายแก่งานของ สช.

12.2. ในช่วงระยะเวลาบำรุงรักษา หากผู้ขายไม่สามารถปฏิบัติได้ตามกำหนดในข้อ 8 สช. ยินยอมให้มีเวลาที่ระบบหรืออุปกรณ์ใด ๆ ทั้งหมดขัดข้องไม่สามารถใช้งานได้สะสมนับรวมกันไม่เกินเดือนละ 72 ชั่วโมง หรือ ร้อยละ 10 (72 ชั่วโมง คูณด้วย 100 หารด้วย 720 ชั่วโมง) ของเวลาใช้งานทั้งหมดของอุปกรณ์ของเดือนนั้น แล้วแต่ตัวเลขใดจะมากกว่ากัน หากระยะเวลาที่ระบบหรืออุปกรณ์ใด ๆ ทั้งหมด ขัดข้องรวมกันในรอบเดือนมากกว่าเกณฑ์การคำนวณนับดังกล่าวแล้ว ผู้ขายจะต้องชำระค่าปรับในช่วงเวลาส่วนที่เกินที่ไม่สามารถใช้งานระบบหรืออุปกรณ์ใด ๆ ได้ ในอัตราชั่วโมงละ ร้อยละ 0.1 x ราคาค่าระบบ/อุปกรณ์ใด ๆ x ค่าตัวถ่วงของรายการระบบ/อุปกรณ์นั้น ๆ ค่าตัวถ่วงแต่ละอุปกรณ์ได้กำหนดดังนี้

| รายการ | ค่าตัวถ่วง |
|---|---|
| อุปกรณ์ฮาร์ดแวร์ (Hardware) ใด ๆ ของระบบ | 0.80 |
| โปรแกรมหรือซอฟต์แวร์ (Software) ใด ๆ ของระบบ | 0.20 |

13. คุณสมบัติผู้เสนอราคา

13.1 ผู้ประสงค์จะเสนอราคาจะต้องเป็นบุคคลหรือนิติบุคคลที่ได้ลงทะเบียนอิเล็กทรอนิกส์ (e-Government Procurement : e-GP) ของกรมบัญชีกลางที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐ

13.2 ผู้ประสงค์จะเสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ หรือไม่เป็นผู้ที่ถูกระบุชื่อว่า เป็นคู่สัญญาที่ไม่ได้แสดงบัญชีรายรับรายจ่าย หรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ ตามประกาศคณะกรรมการป้องกันและปราบการทุจริตแห่งชาติ เรื่อง หลักเกณฑ์และวิธีการจัดทำและแสดงบัญชีรายการรับจ่ายของโครงการที่บุคคลหรือนิติบุคคลเป็นคู่สัญญากับหน่วยงานของรัฐ พ.ศ. 2555 (แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2554 และ (ฉบับที่ 3) พ.ศ. 2555)

13.3 ผู้ประสงค์จะเสนอราคาต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่น และ/หรือต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันระหว่างผู้ประสงค์จะเสนอราคากับผู้ให้บริการตลาดกลางอิเล็กทรอนิกส์ ณ วันประกาศประกวดราคาซื้อด้วยวิธีการอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการขัดขวางการแข็งขันอย่างเป็นธรรม

13.4 ผู้ประสงค์จะเสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

13.5 ผู้ประสงค์จะเสนอราคาต้องเป็นผู้ผลิต หรือเป็นตัวแทนจำหน่ายที่ได้รับการแต่งตั้งจากบริษัทผู้ผลิตโดยตรง หรือสาขาของผู้ผลิตประจำประเทศไทย พร้อมแนบเอกสารหลักฐานการเป็นผู้ผลิตหรือหลักฐานการแต่งตั้งตัวแทนจำหน่ายที่ออกให้สำหรับโครงการนี้

13.6 ผู้ประสงค์จะเสนอราคาต้องมีทุนจดทะเบียนทำธุรกิจด้านระบบเครือข่ายคอมพิวเตอร์ในประเทศไทยไม่น้อยกว่า 7 ปี และมีทุนจดทะเบียนไม่น้อยกว่า 5 ล้านบาท

13.7 ผู้ประสงค์จะเสนอราคาต้องมีผลงานในการติดตั้งอุปกรณ์ และอัพเกรดเฟิร์มแวร์ ของอุปกรณ์ป้องกันเครือข่ายคอมพิวเตอร์ (Firewall) ให้กับสถาบันการศึกษาระดับอุดมศึกษา หน่วยงานราชการ,รัฐวิสาหกิจ หรือเอกชน โดยผู้ประสงค์จะเสนอราคาต้องเป็นคู่สัญญาหลักในสัญญาที่มีวงเงินไม่ต่ำกว่า 2 ล้านบาท (สัญญาเดียว) และเป็นผลงานที่เคยทำไว้ระหว่างปี พ.ศ. 2560 ถึง ณ วันที่ยื่นข้อเสนอ (สำเนาหนังสือรับรองผลงานหรือสำเนาสัญญาจากหน่วยงานมาพร้อมเอกสารเสนอราคา)

**14.** <u>วงเงินในการจัดหา</u>

งบประมาณ พ.ศ. 2565 จำนวน 3,800,000.- (สามล้านแปดแสนบาทถ้วน)

ลงชื่อ.....

(นางสาวอธิการ ทองวัฒน์)

ผู้กำหนดขอบขตงานและรายละเอียดของคุณลักษณะของพัสดุ