



รายละเอียดคุณลักษณะเฉพาะครุภัณฑ์(Spec.)

ชื่อครุภัณฑ์ค่าลิขสิทธิ์ Anti Virus.....จำนวน1 ชุด.....

หน่วยงานสำนักวิทยบริการฯ มทร.ศรีวิชัย..... วงเงินวงเงิน749,000.-... บาท


 เงินงบประมาณรายได้ ประจำปี 2562 เงินงบประมาณประจำปี 2562

ลำดับที่	รายละเอียด	หมายเหตุ
1.	<p>ค่าลิขสิทธิ์ Anti Virus 1 ชุด</p> <p>รายละเอียดคุณสมบัติดังต่อไปนี้</p> <p>1. คุณสมบัติผู้เสนอราคา</p> <p>1.1. เสนอราคาต้องเป็นนิติบุคคลที่ได้จดทะเบียนในประเทศถูกต้องตามกฎหมาย และประกอบธุรกิจเกี่ยวกับโปรแกรมคอมพิวเตอร์</p> <p>1.2. ผู้เสนอราคาต้องมีผลงานในการขายผลิตภัณฑ์ลิขสิทธิ์ซอฟต์แวร์กับมหาวิทยาลัยของรัฐและเอกชนที่เป็นที่ยอมรับมาก่อน</p> <p>1.3. ผู้เสนอราคาต้องส่งมอบงานภายในระยะเวลาไม่เกิน 60 วัน นับตั้งแต่วันที่ลงนามในสัญญา</p> <p>2. ข้อกำหนดทางเทคนิค</p> <p>โปรแกรมป้องกันไวรัสสำหรับเครื่องลูกข่าย จำนวน 2,500 เครื่อง</p> <p>2.1. สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่างๆ เช่น Windows7, Windows 8, และWindows 10 ทั้งแบบ 32 bit และ 64 bit ได้เป็นอย่างดี</p> <p>2.2. สามารถป้องกันจาก Malware แบบ Proactive (Virus, Spyware, Trojans, Adware, Worms, Phishing และ Root kits) ได้หรือดีกว่า</p> <p>2.3. สามารถป้องกันและกำจัด Malware ต่าง ๆ ได้ทั้งแบบ Real-time file system protection และแบบ On-demand computer scan หรือดีกว่า</p> <p>2.4. ตรวจสอบโดยอาศัยการอ้างอิงจากฐานข้อมูลแบบ Definition หรือ Signatures หรือดีกว่า</p> <p>2.5. ตรวจสอบภัยคุกคามจากทางอินเทอร์เน็ตและอีเมลผ่านทาง Protocol HTTP, HTTPS, POP3, POP3S, IMAP และ IMAPS ได้เป็นอย่างดี</p> <p>2.6. สามารถตรวจจับภัยคุกคามผ่าน Media ประเภท Local drives, Removable media, Networks drives ได้เป็นอย่างดี</p> <p>2.7. สามารถตรวจสอบไฟล์ที่สร้างขึ้นใหม่จำพวกไฟล์บีบอัดได้ ซึ่งได้แก่ Archives, Self-extracting files และ Runtime packers หรือดีกว่า</p> <p>2.8. มีระบบปิดกั้นการโจมตีโดยใช้ช่องโหว่ของโปรแกรมประยุกต์ (Exploit Blocker) หรือดีกว่า</p> <p>2.9. มีมอดูลในการสแกนอีเมลไวรัสที่สามารถรวมเข้ากับ Microsoft Outlook Express, Windows Mail และ Mozilla Thunderbird ได้ที่ตัวเครื่องลูกข่าย โดยตรงหรือดีกว่า</p>	

[Handwritten signature]

ก.พ.พ.ก.

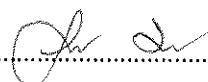
๒๓/๑๒/๖๒

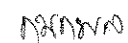
ลำดับที่	รายละเอียด	หมายเหตุ
	<p>2.10. มีระบบ Host Intrusion Prevention System และระบบ Self-defense เพื่อป้องกันภัยคุกคามโจมตีระบบได้หรือดีกว่า</p> <p>2.11. มีเครื่องมือในการสร้างแผ่น Boot CD เพื่อสแกนและกำจัดไวรัสบนระบบปฏิบัติการได้หรือดีกว่า</p> <p>2.12. มีเทคโนโลยีในการตรวจสอบ Process ที่รันอยู่ในระบบว่ามีความเสี่ยงในระบบการรักษาความปลอดภัยในระดับใด โดยตรวจสอบจากฐานข้อมูลของผู้ผลิตโปรแกรมป้องกันไวรัส (Cloud-powered scanning) หรือดีกว่า</p> <p>2.13. สามารถทำ Web Filtering ได้โดยกำหนด URL ที่ต้องการ Allow หรือ Block ให้กับผู้ใช้งาน และสามารถ Exclude URL ที่ไม่ต้องการให้โปรแกรมป้องกันไวรัสสแกนได้หรือดีกว่า</p> <p>2.14. สามารถตั้งค่ารหัสผ่านในการถือการตั้งค่าโปรแกรมได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปลี่ยนแปลงการตั้งค่าโปรแกรม</p> <p>2.15. สามารถปรับปรุงฐานข้อมูลไวรัสของโปรแกรมได้โดยอัตโนมัติ และสามารถปรับปรุงส่วนประกอบต่าง ๆ ของโปรแกรมได้</p> <p>2.16. โปรแกรมป้องกันไวรัสสามารถตั้งค้ายกเว้นไฟล์หรือโฟลเดอร์จากการสแกนได้</p> <p>2.17. สามารถควบคุมการใช้งานอุปกรณ์ที่ถอดเข้าออกได้ โดยสามารถระบุประเภท, หมายเลขอุปกรณ์ และกำหนดสิทธิ์ความสามารถที่ผู้ใช้สามารถเข้าถึงและการทำงานกับอุปกรณ์ที่กำหนด</p> <p>2.18. ทำการย้อนกลับฐานข้อมูลไวรัสไปยังเวอร์ชันก่อนหน้าได้ ในกรณีที่เกิดผลกระทบในการทำงานจากการปรับปรุงฐานข้อมูลไวรัส</p> <p>2.19. โปรแกรมต้องสามารถสร้าง Application memory dump เพื่อใช้ในการตรวจสอบปัญหาได้หรือดีกว่า</p> <p>2.20. โปรแกรมป้องกันไวรัสสามารถส่งอีเมลแจ้งเตือนเหตุการณ์ต่าง ๆ ไปยังผู้ดูแลระบบได้โดยอัตโนมัติ</p> <p>2.21. สามารถทำงานแบบ Personal firewall และสามารถทำการตรวจจับการโจมตีผ่านทางระบบเครือข่าย พร้อมทั้งแสดงถึงแหล่งที่มาของการโจมตีเหล่านั้นได้ (Intrusion Detection System)</p> <p>3. <u>โปรแกรมป้องกันไวรัสสำหรับเครื่องแม่ข่าย</u></p> <p>3.1. สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่าง ๆ เช่น Windows Server 2003, Windows Server 2008, Windows server 2008 R2, Windows server 2012 และ Windows server 2016 ทั้งแบบ 32 และ 64 bits ได้เป็นอย่างดี</p> <p>3.2. สามารถป้องกันจาก Malware แบบ Proactive (Virus, Spyware, Trojans, Adware, Worms, Phishing และ Root kits) ได้เป็นอย่างดี</p> <p>3.3. สามารถป้องกันและกำจัด Malware ต่าง ๆ ได้ทั้งแบบ Real-time file system protection และแบบ On-Demand Scanning หรือดีกว่า</p>	<p></p> <p>พทททท.</p> <p>๒๗๕๐๐</p>

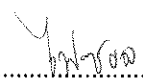
ลำดับที่	รายละเอียด	หมายเหตุ
	<p>3.4. ตรวจสอบโดยอาศัยการอ้างอิงจากฐานข้อมูลแบบ Definition หรือ Signatures หรือดีกว่า</p> <p>3.5. ตรวจสอบภัยคุกคามผ่านทาง Protocol HTTP, HTTPS, POP3, POP3S, IMAP และ IMAPS ได้เป็นอย่างดี</p> <p>3.6. สามารถตรวจภัยคุกคามผ่าน Media ประเภท Local drives, Removable media, Networks drives ได้เป็นอย่างดี</p> <p>3.7. สามารถตรวจสอบไฟล์ที่สร้างขึ้นใหม่จำพวกไฟล์บีบอัดได้ ซึ่งได้แก่ Archives, Self-extracting files และ Runtime packers หรือดีกว่า</p> <p>3.8. มีระบบปิดกั้นการโจมตีโดยใช้ช่องโหว่ของโปรแกรมประยุกต์ (Exploit Blocker) หรือดีกว่า</p> <p>3.9. มีระบบ Host Intrusion Prevention System และระบบ Self-defense เพื่อป้องกันภัยคุกคามโจมตีระบบได้หรือดีกว่า</p> <p>3.10. มีเครื่องมือในการสร้างแผ่น Boot CD เพื่อสแกนและกำจัดไวรัสบนระบบปฏิบัติการได้หรือดีกว่า</p> <p>3.11. มีเทคโนโลยีในการตรวจสอบ Process ที่รันอยู่ในระบบว่ามีความเสี่ยงในระบบการรักษาความปลอดภัยในระดับใด โดยตรวจสอบจากฐานข้อมูลของผู้ผลิตโปรแกรมป้องกันไวรัส (Cloud-powered scanning) หรือดีกว่า</p> <p>3.12. สามารถตั้งค่ารหัสผ่านในการถือการตั้งค่าโปรแกรมได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปลี่ยนแปลงการตั้งค่าโปรแกรม</p> <p>3.13. สามารถปรับปรุงฐานข้อมูลไวรัสของโปรแกรมได้โดยอัตโนมัติ และสามารถปรับปรุงส่วนประกอบต่างๆ ของโปรแกรมได้</p> <p>3.14. สามารถทำการย้อนกลับฐานข้อมูลไวรัสไปยังเวอร์ชันก่อนหน้าได้ ในกรณีที่เกิดผลกระทบในการทำงานจากการปรับปรุงฐานข้อมูลไวรัส</p> <p>3.15. มีเครื่องมือในการตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์ในโปรแกรมป้องกันไวรัส เพื่อการวิเคราะห์ข้อมูลได้</p> <p>3.16. โปรแกรมต้องสามารถสร้าง Application memory dump เพื่อใช้ในการตรวจสอบปัญหาได้หรือดีกว่า</p> <p>3.17. โปรแกรมป้องกันไวรัสสามารถส่งอีเมลแจ้งเตือนเหตุการณ์ต่าง ๆ ไปยังผู้ดูแลระบบได้โดยอัตโนมัติ</p>	
	<p>4. <u>โปรแกรมบริหารจัดการสำหรับเครื่องลูกข่ายและเครื่องแม่ข่าย</u></p> <p>4.1. สามารถติดตั้งโปรแกรมบริหารจัดการได้บนเครื่อง Windows Server 2008, Windows Server 2012, Windows Server 2016, Microsoft Small Business Server 2008 และ Microsoft Small Business Server 2011 ทั้งแบบ 32 และ 64 bits ได้เป็นอย่างดี</p> <p>4.2. สามารถบริการจัดการได้ผ่านเว็บเบราว์เซอร์ (Web Console) ได้เป็น อย่างน้อย</p> <p>4.3. สามารถตรวจสอบ Inventory ของเครื่องลูกข่ายได้ดังนี้ Computer Name, IP Address, MAC Address และ Operating System ได้เป็นอย่างดี</p>	<p><i>(Handwritten signature)</i></p> <p><i>(Handwritten initials)</i></p> <p><i>(Handwritten initials)</i></p>

ลำดับที่	รายละเอียด	หมายเหตุ
	<p>4.4. สามารถมอนิเตอร์ เพื่อดูแลการทำงานของเครื่องลูกข่ายแบบ Real Time ได้ ดังนี้ เวอร์ชันของฐานข้อมูลไวรัส, ระยะเวลาที่เครื่องลูกข่ายเข้ามาเชื่อมต่อครั้ง สุดท้าย, ชื่อและเวอร์ชันของโปรแกรมป้องกันไวรัสที่ติดตั้งอยู่ที่เครื่องลูกข่าย และปัญหาที่เกิดขึ้นกับเครื่องลูกข่ายได้เป็นอย่างดี</p> <p>4.5. สามารถเรียกดูการตั้งค่าโปรแกรมของเครื่องลูกข่ายได้หรือดีกว่า</p> <p>4.6. สามารถกำหนดนโยบายของเครื่องลูกข่ายตาม Group ได้หรือดีกว่า</p> <p>4.7. สามารถสั่งงานไปยังเครื่องลูกข่าย เช่น ปรับปรุงฐานข้อมูลไวรัส, สแกน, รีสตาร์ท และปิดคอมพิวเตอร์ได้เป็นอย่างดี</p> <p>4.8. สามารถกำหนดสิทธิ์ในการเข้าถึงได้หลายระดับ เช่น แบบผู้ดูแลระบบ และ แบบอ่านได้อย่างเดียวเป็นอย่างดี</p> <p>4.9. สามารถแจ้งเตือนเมื่อเกิดเหตุการณ์ต่าง ๆ ไปยังผู้ดูแลระบบผ่านทางอีเมล หรือ SNMP Trap ได้</p> <p>4.10. สามารถเชื่อมต่อกับ Active Directory หรือ สามารถค้นหาเครื่องที่อยู่ใน เครื่องข่ายเดียวกับตัวโปรแกรมบริหารจัดการได้</p> <p>4.11. มี Dashboard เพื่อมอนิเตอร์สถานะต่าง ๆ ได้เป็นอย่างดี</p> <p>4.12. สามารถทำการบริหารจัดการ Backup หรือ Quarantine ของเครื่องลูกข่าย และเครื่องแม่ข่ายทั้งหมดได้</p> <p>4.13. สามารถส่งข้อความไปยังอุปกรณ์ต่าง ๆ ได้ (Client Computer, Server, Notebook)</p> <p>4.14. สามารถตั้ง Schedule ในการออกรายงานและส่งอีเมลไปยังผู้ดูแลระบบได้ หรือดีกว่า</p> <p>4.15. สามารถตั้งค่า SMTP เพื่อใช้ในการส่งอีเมลไปยังผู้ดูแลระบบได้</p> <p>4.16. สามารถทำการติดตั้งและถอดถอนโปรแกรม antivirus สำหรับเครื่องลูกข่าย แบบควบคุมจากศูนย์กลางได้</p>	

ผู้ออกรายละเอียด

1. 
 (นายสุวิพล มหศักดิ์สกุล)

2. 
 (นายกนกพล เมืองรักษ์)

3. 
 (นายไพชอล หมานอิน)