มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

**รายละเอียดคุณลักษณะเฉพาะครุภัณฑ์ (Spec)**

**ชื่อครุภัณฑ์ :** ค่าลิขสิทธิ์ Anti Virus **จำนวน** 1 ชุด

**หน่วยงาน** สำนักวิทยบริการฯ มทร.ศรีวิชัย **วงเงิน** 790,000 **บาท**

☑ **เงินงบประมาณรายได้ ประจำปี 2563** ☐ **เงินงบประมาณประจำปี 2563**

| ลำดับที่ | รายละเอียด | หมายเหตุ |
|---|---|---|
| 1. | **ค่าลิขสิทธิ์ Anti Virus** 1 ชุด<br>รายละเอียดคุณสมบัติดังต่อไปนี้<br>1. คุณสมบัติผู้เสนอราคา<br>1.1. เสนอราคาต้องเป็นนิติบุคคลที่ได้จดทะเบียนในประเทศถูกต้องตามกฎหมาย และประกอบธุรกิจเกี่ยวกับโปรแกรมคอมพิวเตอร์<br>1.2. ผู้เสนอราคาต้องมีผลงานในการขายผลิตภัณฑ์ลิขสิทธิ์ซอฟต์แวร์กับมหาวิทยาลัยของรัฐและเอกชนที่เป็นที่ยอมรับมาก่อน<br>1.3. ผู้เสนอราคาต้องส่งมอบงานภายในระยะเวลาไม่เกิน 60 วัน นับตั้งแต่วันที่ลงนามในสัญญา<br><br>2. ข้อกำหนดทางเทคนิค<br>โปรแกรมป้องกันไวรัสสำหรับเครื่องลูกข่าย จำนวน 2,500 เครื่อง<br>2.1. สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่าง ๆ เช่น Windows 7, Windows 8, และWindows 10 ทั้งแบบ 32 bit และ 64 bit ได้เป็นอย่างน้อย<br>2.2. สามารถป้องกันจาก Malware แบบ Proactive (Virus, Spyware, Trojans, Adware, Worms, Phishing และ Root kits) ได้หรือดีกว่า<br>2.3. สามารถป้องกันและกำจัด Malware ต่าง ๆ ได้ทั้งแบบ Real-time file system protection และแบบ On-demand computer scan หรือดีกว่า<br>2.4. ตรวจสอบโดยอาศัยการอ้างอิงจากฐานข้อมูลแบบ Definition หรือ Signatures หรือดีกว่า<br>2.5. ตรวจสอบภัยคุกคามจากทางอินเทอร์เน็ตและอีเมลผ่านทาง Protocol HTTP, HTTPS, POP3, POP3S, IMAP และ IMAPS ได้เป็นอย่างน้อย<br>2.6. สามารถตรวจจับภัยคุกคามผ่าน Media ประเภท Local drives, Removable media, Networks drives ได้เป็นอย่างน้อย<br>2.7. สามารถตรวจสอบไฟล์ที่สร้างขึ้นใหม่จำพวกไฟล์บีบอัดได้ ซึ่งได้แก่ Archives, Self-extracting files และ Runtime packers หรือดีกว่า<br>2.8. มีระบบปิดกั้นการโจมตีโดยใช้ช่องโหว่ของโปรแกรมประยุกต์ (Exploit Blocker) หรือดีกว่า<br>2.9. มีมอดูลในการสแกนอีเมลไวรัสที่สามารถรวมเข้ากับ Microsoft Outlook Express, Windows Mail และ Mozilla Thunderbird ได้ที่ตัวเครื่องลูกข่ายโดยตรงหรือดีกว่า | |

2.10. มีระบบ Host Intrusion Prevention System และระบบ Self-defense เพื่อป้องกันภัยคุกคามโจมตีระบบได้หรือดีกว่า

2.11. มีเครื่องมือในการสร้างแผ่น Boot CD เพื่อสแกนและกำจัดไวรัสนอกระบบปฏิบัติการได้หรือดีกว่า

2.12. มีเทคโนโลยีในการตรวจสอบ Process ที่รันอยู่ในระบบว่ามีความเสี่ยงในระบบความรักษาความปลอดภัยในระดับใด โดยตรวจสอบจากฐานข้อมูลของผู้ผลิตโปรแกรมป้องกันไวรัส (Cloud-powered scanning) หรือดีกว่า

2.13. สามารถทำ Web Filtering ได้โดยกำหนด URL ที่ต้องการ Allow หรือ Block ให้กับผู้ใช้งาน และสามารถ Exclude URL ที่ไม่ต้องการให้โปรแกรมป้องกันไวรัสสแกนได้หรือดีกว่า

2.14. สามารถตั้งค่ารหัสผ่านในการล็อคการตั้งค่าโปรแกรมได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปลี่ยนแปลงการตั้งค่าโปรแกรม

2.15. สามารถปรับปรุงฐานข้อมูลไวรัสของโปรแกรมได้โดยอัตโนมัติ และสามารถปรับปรุงส่วนประกอบต่าง ๆ ของโปรแกรมได้

2.16. โปรแกรมป้องกันไวรัสสามารถตั้งค่ายกเว้นไฟล์หรือโฟลเดอร์จากการสแกนได้

2.17. สามารถควบคุมการใช้งานอุปกรณ์ที่ถอดเข้าออกได้ โดยสามารถระบุประเภท, หมายเลขอุปกรณ์ และกำหนดสิทธิ์ความสามารถที่ผู้ใช้สามารถเข้าถึงและการทำงานกับอุปกรณ์ที่กำหนด

2.18. ทำการย้อนกลับฐานข้อมูลไวรัสไปยังเวอร์ชันก่อนหน้าได้ ในกรณีที่เกิดผลกระทบในการทำงานจากการปรับปรุงฐานข้อมูลไวรัส

2.19. โปรแกรมต้องสามารถสร้าง Application memory dump เพื่อใช้ในการตรวจสอบปัญหาได้หรือดีกว่า

2.20. โปรแกรมป้องกันไวรัสสามารถส่งอีเมลแจ้งเตือนเหตุการณ์ต่าง ๆ ไปยังผู้ดูแลระบบได้โดยอัตโนมัติ

2.21. สามารถทำงานแบบ Personal firewall และ สามารถทำการตรวจจับการโจมตีผ่านทางระบบเครือข่าย พร้อมทั้งแสดงถึงแหล่งที่มาของการโจมตีเหล่านั้นได้ (Intrusion Detection System)

3. <u>โปรแกรมป้องกันไวรัสสำหรับเครื่องแม่ข่าย</u>

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 ได้เป็นอย่างน้อย

3.2. สามารถป้องกันจาก Malware แบบ Proactive (Virus, Spyware, Trojans, Adware, Worms, Phishing และ Root kits) ได้เป็นอย่างน้อย

3.3. สามารถป้องกันและกำจัด Malware ต่าง ๆ ได้ทั้งแบบ Real-time file system protection และแบบ On-Demand Scanning หรือดีกว่า

3.4. ตรวจสอบโดยอาศัยการอ้างอิงจากฐานข้อมูลแบบ Definition หรือ Signatures หรือดีกว่า

3.5. ตรวจจับภัยคุกคามผ่านทาง Protocal HTTP, HTTPS, POP3, POP3S, IMAP และ IMAPS ได้เป็นอย่างน้อย

3.6. สามารถตรวจจับภัยคุกคามผ่าน Media ประเภท Local drives, Removable media, Networks drives ได้เป็นอย่างน้อย

3.7. สามารถตรวจสอบไฟล์ที่สร้างขึ้นใหม่จำพวกไฟล์บีบอัดได้ ซึ่งได้แก่ Archives, Self-extracting files และ Runtime packers หรือดีกว่า

3.8. มีระบบปิดกั้นการโจมตีโดยใช้ช่องโหว่ของโปรแกรมประยุกต์ (Exploit Blocker) หรือดีกว่า

3.9. มีระบบ Host Intrusion Prevention System และระบบ Self-defense เพื่อป้องกันภัยคุกคามโจมตีระบบได้หรือดีกว่า

3.10. มีเครื่องมือในการสร้างแผ่น Boot CD เพื่อสแกนและกำจัดไวรัสนอกระบบปฏิบัติการได้หรือดีกว่า

3.11. มีเทคโนโลยีในการตรวจสอบ Process ที่รันอยู่ในระบบว่ามีความเสี่ยงในระบบความรักษาความปลอดภัยในระดับใด โดยตรวจสอบจากฐานข้อมูลของผู้ผลิตโปรแกรมป้องกันไวรัส (Cloud-powered scanning) หรือดีกว่า

3.12. สามารถตั้งค่ารหัสผ่านในการล็อคการตั้งค่าโปรแกรมได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปลี่ยนแปลงการตั้งค่าโปรแกรม

3.13. สามารถปรับปรุงฐานข้อมูลไวรัสของโปรแกรมได้โดยอัตโนมัติ และสามารถปรับปรุงส่วนประกอบต่างๆ ของโปรแกรมได้

3.14. สามารถทำการย้อนกลับฐานข้อมูลไวรัสไปยังเวอร์ชันก่อนหน้าได้ ในกรณีที่เกิดผลกระทบในการทำงานจากการปรับปรุงฐานข้อมูลไวรัส

3.15. มีเครื่องมือในการตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์ในโปรแกรมป้องกันไวรัส เพื่อการวิเคราะห์ข้อมูลได้

3.16. โปรแกรมต้องสามารถสร้าง Application memory dump เพื่อใช้ในการตรวจสอบปัญหาได้หรือดีกว่า

3.17. โปรแกรมป้องกันไวรัสสามารถส่งอีเมลแจ้งเตือนเหตุการณ์ต่าง ๆ ไปยังผู้ดูแลระบบได้โดยอัตโนมัติ

4. <u>โปรแกรมบริหารจัดการสำหรับเครื่องลูกข่ายและเครื่องแม่ข่าย</u>

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 ได้เป็นอย่างน้อย

4.2. สามารถบริการจัดการได้ผ่านเว็บเบราว์เซอร์ (Web Console) ได้เป็นอย่างน้อย

4.3. สามารถตรวจสอบ Inventory ของเครื่องลูกข่ายได้ดังนี้ Computer Name, IP Address, MAC Address และ Operating System ได้เป็นอย่างน้อย

4.4. สามารถมอนิเตอร์ เพื่อดูแลการทำงานของเครื่องลูกข่ายแบบ Real Time ได้ดังนี้ เวอร์ชันของฐานข้อมูลไวรัส, ระยะเวลาที่เครื่องลูกข่ายเข้ามาเชื่อมต่อครั้งสุดท้าย, ชื่อและเวอร์ชันของโปรแกรมป้องกันไวรัสที่ติดตั้งอยู่ที่เครื่องลูกข่าย

| | | |
|---|---|---|
| | และปัญหาที่เกิดขึ้นกับเครื่องลูกข่ายได้เป็นอย่างน้อย<br>4.5. สามารถเรียกดูการตั้งค่าโปรแกรมของเครื่องลูกข่ายได้หรือดีกว่า<br>4.6. สามารถกำหนดนโยบายของเครื่องลูกข่ายตาม Group ได้หรือดีกว่า<br>4.7. สามารถสั่งงานไปยังเครื่องลูกข่าย เช่น ปรับปรุงฐานข้อมูลไวรัส, สแกน, รีสตาร์ท และปิดคอมพิวเตอร์ได้เป็นอย่างน้อย<br>4.8. สามารถกำหนดสิทธิ์ในการเข้าถึงได้หลายระดับ เช่น แบบผู้ดูแลระบบ และแบบอ่านได้อย่างเดียวเป็นอย่างน้อย<br>4.9. สามารถแจ้งเตือนเมื่อเกิดเหตุการณ์ต่าง ๆ ไปยังผู้ดูแลระบบผ่านทางอีเมล์ หรือ SNMP Trap ได้<br>4.10. สามารถเชื่อมต่อกับ Active Directory หรือ สามารถค้นหาเครื่องที่อยู่ในเครือข่ายเดียวกับตัวโปรแกรมบริหารจัดการได้<br>4.11. มี Dashboard เพื่อมอนิเตอร์สถานะต่าง ๆ ได้เป็นอย่างน้อย<br>4.12. สามารถทำการบริหารจัดการ Backup หรือ Quarantine ของเครื่องลูกข่ายและเครื่องแม่ข่ายทั้งหมดได้<br>4.13. สามารถส่งข้อความไปยังอุปกรณ์ต่าง ๆ ได้ ( Client Computer, Server, Notebook )<br>4.14. สามารถตั้ง Schedule ในการออกรายงานและส่งอีเมลไปยังผู้ดูแลระบบได้หรือดีกว่า<br>4.15. สามารถตั้งค่า SMTP เพื่อใช้ในการส่งอีเมล์ไปยังผู้ดูแลระบบได้<br>4.16. สามารถทำการติดตั้งและถอดถอนโปรแกรม antivirus สำหรับเครื่องลูกข่ายแบบควบคุมจากศูนย์กลางได้ | |

**ผู้ออกรายละเอียด**

1. ..... (ผศ.สุวิพล มหศักดิสกุล)

2. ..... (นายพีรพงษ์ ขุนทอง)

3. ..... (นายภานุวัฒน์ หนูนคง)