มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

รายละเอียดคุณลักษณะเฉพาะครุภัณฑ์ (Spec)

ชื่อครุภัณฑ์ : Anti Virus จำนวน 1 ชุด

หน่วยงาน สำนักวิทยบริการฯ มทร.ศรีวิชัย วงเงิน 800,000.- บาท

☑ เงินงบประมาณรายได้ ประจำปี 2560 ☐ เงินงบประมาณประจำปี 2560

ลำดับที่	รายละเอียด	หมายเหตุ
1.	Anti Virus 1 ชุด รายละเอียดคุณสมบัติดังต่อไปนี้ 1. คุณสมบัติผู้เสนอราคา 1.1 ผู้เสนอราคาต้องเป็นนิติบุคคลที่ได้จดทะเบียนในประเทศถูกต้องตามกฎหมาย และประกอบธุรกิจเกี่ยวกับโปรแกรมคอมพิวเตอร์ 1.2 ผู้เสนอราคาต้องมีผลงานในการขายผลิตภัณฑ์ลิขสิทธิ์ซอฟแวร์กับมหาวิทยาลัยของรัฐและเอกชนที่เป็นที่ยอมรับมาก่อน 1.3 ผู้เสนอราคาต้องส่งมอบงานภายในระยะเวลาไม่เกิน 60 วัน นับตั้งแต่วันที่ลงนามในสัญญา 2. ข้อกำหนดทางเทคนิค โปรแกรมป้องกันไวรัสสำหรับเครื่องลูกข่าย จำนวน 2,500 เครื่อง 2.1 สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่างๆ เช่น Windows XP, Windows Vista, Windows 7, Windows 8, และWindows 10 ทั้งแบบ 32 และ 64 bits ได้ 2.2 สามารถป้องกันจาก Malware แบบ Proactive (Virus, Spyware, Trojans, Adware, Worms, Phishing และ Root kits ได้ 2.3 สามารถป้องกันและกำจัด Malware ต่างๆ ได้ทั้งแบบ Real-time file system protection และแบบ On-demand computer scan 2.4 ตรวจสอบโดยอาศัยการอ้างอิงจากฐานข้อมูลแบบ Definition หรือ Signatures 2.5 ตรวจสอบโดยอาศัยการวิเคราะห์พฤติกรรมแบบ Heuristics และ Advanced Heuristics 2.6 สามารถตรวจจับ Potentially Unwanted Applications และ Potentially Unsafe Applications ได้ 2.7 สามารถตรวจสอบภัยคุกคามจากทางอินเตอร์เน็ตและอีเมล์ผ่านทาง Protocol HTTP, HTTPS, POP3, POP3S, IMAP และ IMAPS 2.8 สามารถตรวจจับภัยคุกคามผ่าน Media ได้ดังนี้ Local drives, Removable media, Networks drives 2.9 สามารถตรวจสอบไฟล์ที่สร้างขึ้นใหม่จำพวกไฟล์บีบอัดได้ ซึ่งได้แก่ Archives, Self-extracting files และ Runtime packers	

2.10 สามารถกู้คืนความเสียหายที่เกิดขึ้นจากพฤติกรรมของไวรัสได้ (Roll back Malicious Activity)

2.11 มีระบบปิดกั้นการโจมตีโดยใช้ช่องโหว่ของโปรแกรมประยุกต์ (Exploit Blocker)

2.12 มีโมดูลในการสแกนอีเมล์ไวรัสที่สามารถรวมเข้ากับ Microsoft Outlook, Outlook Express, Windows Mail และ Windows Live Mail ได้ที่ตัวเครื่องลูกข่ายโดยตรง

2.13 มีระบบ Host Intrusion Prevention System และระบบ Self-defense เพื่อป้องกันภัยคุกคามโจมตีระบบได้

2.14 มีโมดูล Document Protection เพื่อป้องกันไวรัสติดไฟล์เอกสาร Microsoft Office

2.15 มีเครื่องมือในการสร้างแผ่น Boot CD เพื่อสแกนและกำจัดไวรัสนอกระบบปฏิบัติการได้

2.16 มีเทคโนโลยีในการตรวจสอบ Process ที่รันอยู่ในระบบว่ามีความเสี่ยงในระบบความรักษาความปลอดภัยในระดับใด โดยตรวจสอบจากฐานข้อมูลของผู้ผลิตโปรแกรมป้องกันไวรัส (Cloud-powered scanning)

2.17 สามารถทำ Web Filtering ได้โดยกำหนด URL ที่ต้องการ Allow หรือ Block ให้กับผู้ใช้งาน และสามารถ Exclude URL ที่ไม่ต้องการให้โปรแกรมป้องกันไวรัสสแกนได้

2.18 สามารถตั้งค่ารหัสผ่านในการล็อคการตั้งค่าโปรแกรมได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปลี่ยนแปลงการตั้งค่าโปรแกรม

2.19 สามารถอัพเดทฐานข้อมูลไวรัสของโปรแกรมได้โดยอัตโนมัติ และสามารถอัพเดทส่วนประกอบต่างๆ ของโปรแกรมได้

2.20 โปรแกรมป้องกันไวรัสสามารถตั้งค่ายกเว้นไฟล์หรือโฟลเดอร์จากการสแกนได้

2.21 สามารถควบคุมการใช้งานอุปกรณ์ที่ถอดเข้าออกได้ โดยสามารถระบุประเภท, หมายเลขอุปกรณ์ และกำหนดสิทธิ์ความสามารถที่ผู้ใช้สามารถเข้าถึงและการทำงานกับอุปกรณ์ที่กำหนด

2.22 สามารถทำการย้อนกลับฐานข้อมูลไวรัสไปยังเวอร์ชั่นก่อนหน้าได้ ในกรณีที่เกิดผลกระทบในการทำงานจากการปรับปรุงฐานข้อมูลไวรัส

2.23 มีเครื่องมือในการตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์ในโปรแกรมป้องกันไวรัสเอง เพื่อการวิเคราะห์ข้อมูลได้

2.24 สามารถสนับสนุนการทำงานร่วมกับ Microsoft NAPได้

2.25 มีความสามารถในการตรวจสอบ Patch ของ Windows ที่ยังไม่ได้ติดตั้งอัพเดท และแจ้งเตือน Patch ที่ในโปรแกรมป้องกันไวรัสได้

2.26 โปรแกรมต้องสามารถสร้าง Application memory dump เพื่อใช้ในการตรวจสอบปัญหาได้

2.27 โปรแกรมป้องกันไวรัสสามารถส่งอีเมลแจ้งเตือนเหตุการณ์ต่าง ๆ ไปยังผู้ดูแลระบบได้โดยอัตโนมัติ

2.28 มีระบบสแกนหน่วยความจำขั้นสูง (Advanced Memory Scanner) เพื่อตรวจจับมัลแวร์ที่ใช้เทคนิคการโจมตีที่ซับซ้อน

2.29 มีฟังก์ชั่น Presentation mode เพื่อปิดการทำงานของหน้าต่างป๊อบ-อัพ เมื่อใช้งานแอพพลิเคชั่นแบบเต็มจอ

2.30 สามารถตั้งค่าให้สแกนอัตโนมัติ เมื่อคอมพิวเตอร์อยู่ในสถานะ Screen Saver, Computer lock, User logoff

3. <u>โปรแกรมป้องกันไวรัสสำหรับเครื่องแม่ข่าย</u>

3.1 สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่างๆ เช่น Windows Server 2003, Windows Server 2008, Windows server 2008 R2, Windows server 2012 และ Windows server 2016 ทั้งแบบ 32 และ 64 bits ได้

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

3.3 สามารถป้องกันและกำจัด Malware ต่างๆ ได้ทั้งแบบ Real-time file system protection และแบบ On-Demand Scanning

3.4 ตรวจสอบโดยอาศัยการอ้างอิงจากฐานข้อมูลแบบ Definition หรือ Signatures

3.5 ตรวจสอบโดยอาศัยการวิเคราะห์พฤติกรรมแบบ Heuristics และ Advanced Heuristics

3.6 สามารถตรวจจับ Potentially Unwanted Applications และ Potentially Unsafe Applications ได้

3.7 สามารถตรวจจับภัยคุกคามผ่าน Media ได้ดังนี้ Local drives, Removable media, Networks drives

3.8 สามารถตรวจสอบไฟล์ที่สร้างขึ้นใหม่จำพวกไฟล์บีบอัดได้ ซึ่งได้แก่ Archives, Self-extracting files และ Runtime packers

3.9 มีระบบปิดกั้นการโจมตีโดยใช้ช่องโหว่ของโปรแกรมประยุกต์ (Exploit Blocker)

3.10 มีโมดูลในการสแกนอีเมล์ไวรัสที่สามารถรวมเข้ากับ Microsoft Outlook, Outlook Express, Windows Mail และ Windows Live Mailได้ที่ตัวเครื่องลูกข่ายโดยตรง

3.11 มีระบบ Host Intrusion Prevention System และระบบ Self-defense เพื่อป้องกันภัยคุกคามโจมตีระบบได้

3.12 มีโมดูล Document Protection เพื่อป้องกันไวรัสติดไฟล์เอกสาร Microsoft Office

3.13 มีเครื่องมือในการสร้างแผ่น Boot CD เพื่อสแกนและกำจัดไวรัสนอกระบบปฏิบัติการได้

3.14 มีเทคโนโลยีในการตรวจสอบ Process ที่รันอยู่ในระบบว่ามีความเสี่ยงในระบบความรักษาความปลอดภัยในระดับใด โดยตรวจสอบจากฐานข้อมูลของผู้ผลิตโปรแกรมป้องกันไวรัส (Cloud-powered scanning)

3.15 สามารถทำ Web Filtering ได้โดยกำหนด URL ที่ต้องการ Allow หรือ Block ให้กับผู้ใช้งาน และสามารถ Exclude URL ที่ไม่ต้องการให้โปรแกรมป้องกันไวรัสสแกนได้

3.16 สามารถตั้งค่ารหัสผ่านในการล็อคการตั้งค่าโปรแกรมได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปลี่ยนแปลงการตั้งค่าโปรแกรม

3.17 สามารถอัพเดทฐานข้อมูลไวรัสของโปรแกรมได้โดยอัตโนมัติ และสามารถอัพเดทส่วนประกอบต่างๆ ของโปรแกรมได้

3.18 โปรแกรมป้องกันไวรัสสามารถตั้งค่ายกเว้นการสแกนของไฟล์ที่เกี่ยวข้องกับ Microsoft Windows Server ได้อัตโนมัติ

3.19 สามารถควบคุมการใช้งานอุปกรณ์ที่ถอดเข้าออกได้ โดยสามารถระบุประเภท, หมายเลขอุปกรณ์ และกำหนดสิทธิ์ความสามารถที่ผู้ใช้สามารถเข้าถึงและการทำงานกับอุปกรณ์ที่กำหนด

3.20 สามารถทำการย้อนกลับฐานข้อมูลไวรัสไปยังเวอร์ชั่นก่อนหน้าได้ ในกรณีที่เกิดผลกระทบในการทำงานจากการปรับปรุงฐานข้อมูลไวรัส

3.21 มีเครื่องมือในการตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์ในโปรแกรมป้องกันไวรัสเอง เพื่อการวิเคราะห์ข้อมูลได้

3.22 มีความสามารถในการตรวจสอบ Patch ของ Windows ที่ยังไม่ได้ติดตั้งอัพเดท และแจ้งเตือน Patch ที่ในโปรแกรมป้องกันไวรัสได้

3.23 โปรแกรมต้องสามารถสร้าง Application memory dump เพื่อใช้ในการตรวจสอบปัญหาได้

3.24 โปรแกรมป้องกันไวรัสสามารถส่งอีเมล์แจ้งเตือนเหตุการณ์ต่าง ๆ ไปยังผู้ดูแลระบบได้โดยอัตโนมัติ

3.25 มีระบบสแกนหน่วยความจำขั้นสูง (Advanced Memory Scanner) เพื่อตรววจับมัลแวร์ที่ใช้เทคนิคการโจมตีที่ซับซ้อน

3.26 มีฟังก์ชั่น Presentation mode เพื่อปิดการทำงานของหน้าต่างป๊อบ-อัพ เมื่อใช้งานแอพพลิเคชั่นแบบเต็มจอ

3.27 สามารถตั้งค่าให้สแกนอัตโนมัติ เมื่อคอมพิวเตอร์อยู่ในสถานะ Screen Saver, Computer lock, User logoff

4. <u>โปรแกรมบริหารจัดการสำหรับเครื่องลูกข่ายและเครื่องแม่ข่าย</u>

4.1 สามารถติดตั้งโปรแกรมบริหารจัดการได้บนเครื่อง Windows Server 2003 SP2, Windows Server 2008 R2, Server 2012 Windows XP SP3, Windows 7, Windows Small Business Server 2003, Windows Small Business Server 2008, Windows Small Business Server 2011 ระบบปฏิบัติการ Linux เช่น Ubuntu, CentOS, OpenSUSE ได้

4.2 สามารถบริการจัดการได้ผ่านเว็บเบราว์เซอร์ (Web Console)

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

	4.4 สามารถมอนิเตอร์ เพื่อดูแลการทำงานของเครื่องลูกข่ายแบบ Real Time ได้ดังนี้ เวอร์ชั่นของฐานข้อมูลไวรัส, ระยะเวลาที่เครื่องลูกข่ายเข้ามาเชื่อมต่อครั้งสุดท้าย, ชื่อและเวอร์ชั่นของโปรแกรมป้องกันไวรัสที่ติดตั้งอยู่ที่เครื่องลูกข่าย และปัญหาที่เกิดขึ้นกับเครื่องลูกข่ายได้ 4.5 สามารถเรียกดูการตั้งค่าโปรแกรมของเครื่องลูกข่ายได้ 4.6 สามารถกำหนดนโยบายของเครื่องลูกข่ายตาม Group ได้ 4.7 สามารถสั่งงานไปยังเครื่องลูกข่าย เช่น อัพเดทฐานข้อมูลไวรัส, สแกน, รีสตาร์ท และปิดคอมพิวเตอร์ได้ 4.8 สามารถส่งข้อมูลไปเก็บไว้บนฐานข้อมูล MSSQL และ MYSQL ได้ 4.9 สามารถกำหนดสิทธิ์ในการเข้าถึงได้หลายระดับ เช่น แบบผู้ดูแลระบบ และแบบอ่านได้อย่างเดียว 4.10 สามารถแจ้งเตือนเมื่อเกิดเหตุการณ์ต่างๆ ไปยังผู้ดูแลระบบผ่านทางอีเมล์ และ SNMP Trap ได้ 4.11 สามารถเชื่อมต่อกับ Active Directory/Open Directory/LDAP ได้ 4.12 มี Dashboard เพื่อมอนิเตอร์สถานะต่างๆได้ 4.13 สามารถทำการบริหารจัดการ Quarantine ของเครื่องลูกข่ายทั้งหมดได้ 4.14 สามารถส่งข้อความไปยังอุปกรณ์ต่างๆ ได้ (client computer, tablet, mobile) 4.15 สามารถตั้ง Schedule ในการออกรายงานและส่งอีเมล์ไปยังผู้ดูแลระบบได้ 4.16 การจัดทำรายงานสามารถนำเอาข้อมูลออกมาได้ในรูปแบบของ CSV Format, PDF Format และ PS Format 4.17 สามารถตั้งค่า SMTP เพื่อใช้ในการส่งอีเมล์ไปยังผู้ดูแลระบบ 4.18 สามารถทำการติดตั้งและถอดถอนโปรแกรม antivirus สำหรับเครื่องลูกข่ายแบบรีโมทจากศูนย์กลางได้	

ผู้ออกรายละเอียด

1. .....
(นายกิติศักดิ์ วัฒนกุล)

2. .....
(นายกนกพล เมืองรักษ์)

3. .....
(นายพีรพงษ์ ขุนทอง)