

ขอบเขตของงาน (Terms of Reference : TOR) (ซื้อขาย)
โครงการซื้อระบบตรวจสอบและป้องกันไวรัส สำหรับเครื่องคอมพิวเตอร์
จำนวน ๕๒๐๐ License
ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

ความเป็นมา

สำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์ มีภารกิจหลักในการวางโครงสร้างพื้นฐาน และให้บริการด้านระบบสารสนเทศ ระบบคอมพิวเตอร์ และเครือข่ายแก่นิสิต อาจารย์ บุคลากร และให้บริการเครื่องคอมพิวเตอร์เพื่อสนับสนุนการเรียนการสอนและการปฏิบัติงานของบุคลากรหน่วยงานในสังกัด มหาวิทยาลัยเกษตรศาสตร์ การใช้งานเครื่องคอมพิวเตอร์ดังกล่าวจำเป็นต้องติดตั้งซอฟต์แวร์ป้องกันการถูกโจมตีจากไวรัสคอมพิวเตอร์

ดังนั้นจึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการดำเนินการจัดหาระบบตรวจสอบและป้องกันไวรัสเพื่อติดตั้งในเครื่องคอมพิวเตอร์ที่ใช้ในห้องปฏิบัติการคอมพิวเตอร์การเรียนการสอนและการดำเนินงานต่าง ๆ ของมหาวิทยาลัยเกษตรศาสตร์ อีกทั้งเพื่อรองรับการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

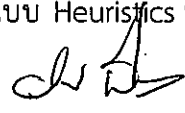
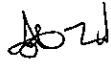
วัตถุประสงค์

๑. เพื่อให้บริการระบบตรวจสอบและป้องกันไวรัสได้อย่างต่อเนื่อง
๒. เพื่อให้เครื่องคอมพิวเตอร์ที่ให้บริการห้องการเรียนการสอนและเจ้าหน้าที่ปฏิบัติงานของหน่วยงานในมหาวิทยาลัยเกษตรศาสตร์สามารถปฏิบัติงานได้อย่างต่อเนื่องไม่ติดขัดจากการถูกโจมตีหรือบุกรุกจากไวรัสคอมพิวเตอร์

รายละเอียดข้อกำหนดของระบบตรวจสอบและป้องกันไวรัส สำหรับเครื่องคอมพิวเตอร์ เป็นดังนี้

๑. โปรแกรมป้องกันไวรัสสำหรับเครื่องแม่ข่าย (จำนวนอย่างน้อย ๒๐๐ License)

- ๑.๑. สนับสนุนการทำงานบนระบบปฏิบัติการ Microsoft Windows Server ๒๐๐๘ R๒ SP๑ /Server ๒๐๑๒/Server ๒๐๑๒/Server ๒๐๑๔ ได้เป็นอย่างน้อย
- ๑.๒. สามารถป้องกัน Malware ต่าง ๆ ได้แบบ Proactive ซึ่งได้แก่ Viruses, Ransomware, Rootkits, Worms และ Spyware โดยไม่ขัดขวางประสิทธิภาพของระบบหรือรบกวนคอมพิวเตอร์
- ๑.๓. สามารถป้องกันและกำจัด Malware ต่าง ๆ ได้ทั้งแบบ Real-time file system protection และแบบ On-demand computer scan
- ๑.๔. ใช้วิธีการตรวจสอบ Malware โดยวิธีดังนี้
 - ๑.๔.๑. ตรวจสอบโดยอาศัยการอ้างอิงจากฐานข้อมูลแบบ Definition หรือ Signatures
 - ๑.๔.๒. ตรวจสอบโดยอาศัยการวิเคราะห์พฤติกรรมแบบ Heuristics หรือ Machine Learning หรือ AI



 ๒๖๓๐

๑.๕. สามารถตรวจจับ Potentially Unwanted Applications และ Potentially Unsafe Applications ได้

๑.๖. สามารถตรวจสอบภัยคุกคามจากทางอินเทอร์เน็ตและอีเมลผ่านทาง Protocol HTTP, HTTPS, POP๓, POP๓S, IMAP และ IMAPS

๑.๗. สามารถตรวจจับภัยคุกคามผ่าน Media ดังนี้ Local Drives, Removable Media, Networks Drives

๑.๘. มีระบบปิดกั้นการโจมตีโดยใช้ช่องโหว่ของโปรแกรมประยุกต์ (Exploit Blocker)

๑.๙. มีระบบป้องกันบ็อตเน็ต (Botnet Protection)

๑.๑๐. มีระบบป้องกันการโจมตีทางช่องโหว่ของระบบเครือข่าย (Network Attack Protection)

๑.๑๑. มีระบบป้องกันแรนซัมแวร์ (Ransomware Shield)

๑.๑๒. มีระบบ Host Intrusion Prevention System และระบบ Self-defense เพื่อป้องกันภัยคุกคามโจมตีระบบได้

๑.๑๓. มีเครื่องมือในการสร้างแผ่น Bootable CD,DVD และ USB เพื่อสแกนและกำจัดไวรัสบนระบบปฏิบัติการได้

๑.๑๔. มีเทคโนโลยีในการตรวจสอบ Process ที่รันอยู่ในระบบว่ามีความเสี่ยงในระบบการรักษาความปลอดภัยในระดับใด โดยตรวจสอบจากฐานข้อมูลของผู้ผลิตโปรแกรมป้องกันไวรัส (Cloud-powered scanning)

๑.๑๕. สามารถตั้งค่าการห้ามผ่านในการถือการตั้งค่าโปรแกรมได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปลี่ยนแปลงการตั้งค่าโปรแกรม

๑.๑๖. สามารถอัปเดตฐานข้อมูลไวรัสของโปรแกรมได้โดยอัตโนมัติ และสามารถอัปเดตส่วนประกอบต่าง ๆ ของโปรแกรมได้

๑.๑๗. โปรแกรมป้องกันไวรัสสามารถตั้งค่าแยกเว้นไฟล์ หรือโฟลเดอร์จากการสแกนได้

๑.๑๘. โปรแกรมป้องกันไวรัสสามารถตั้งค่าแยกเว้นการสแกนของไฟล์ที่เกี่ยวข้องกับ Microsoft Windows Server ได้แบบอัตโนมัติ

๑.๑๙. สามารถป้องกัน Phishing ได้

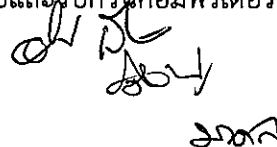
๑.๒๐. สามารถควบคุมการใช้งานอุปกรณ์ที่ถอดเข้าออกได้ โดยสามารถระบุประเภท, หมายเลขอุปกรณ์ และกำหนดสิทธิ์ความสามารถที่ผู้ใช้สามารถเข้าถึงและการทำงานกับอุปกรณ์ที่กำหนด

๑.๒๑. สามารถตรวจสอบชื่อเสียงของไฟล์จากคลาวด์ (Cloud-based protection)

๒. โปรแกรมป้องกันไวรัสสำหรับเครื่องลูกข่าย (จำนวน ๕๐๐๐ License)

๒.๑. เป็นโปรแกรมป้องกันไวรัสที่สนับสนุนการทำงานบนระบบปฏิบัติการดังต่อไปนี้ Microsoft Windows ๗ SP๑ /๘/๘.๑/๑๐ ได้เป็นอย่างดี

๒.๒. สามารถป้องกัน Malware ต่างๆ ได้แบบ Proactive ซึ่งได้แก่ Viruses, Spyware, Trojan, Worms, Adware และ Rootkits โดยไม่ขัดขวางประสิทธิภาพของระบบและระบบงานคอมพิวเตอร์



๒.๓. สามารถป้องกันและกำจัด Malware ต่างๆ ได้ทั้งแบบ Real-time file system protection และแบบ On-demand computer scan

๒.๔. ใช้วิธีการตรวจสอบ Malware โดยวิธีดังนี้

๒.๔.๑. ตรวจสอบโดยอาศัยการอ้างอิงจากฐานข้อมูลแบบ Definition หรือ Signatures

๒.๔.๒. ตรวจสอบโดยอาศัยการวิเคราะห์พฤติกรรมแบบ Heuristics หรือ Machine Learning หรือ AI

๒.๕. สามารถตรวจจับ Potentially Unwanted Applications และ Potentially Unsafe Applications ได้

๒.๖. สามารถตรวจสอบภัยคุกคามจากทางอินเทอร์เน็ตและอีเมลผ่านทาง Protocol HTTP, HTTPS, POP๓, POP๓S, IMAP และ IMAPS

๒.๗. สามารถตรวจจับภัยคุกคามผ่าน Media ดังนี้ Local Drives, Removable Media, Networks Drives

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

๒.๙. มีระบบปิดกั้นการโจมตีโดยใช้ช่องโหว่ของโปรแกรมประยุกต์ (Exploit Blocker)

๒.๑๐. สามารถป้องกัน Phishing ได้

๒.๑๑. มีโมดูลในการสแกนอีเมลไวรัสและอีเมลขยะที่สามารถรวมเข้ากับ Microsoft Outlook, Outlook Express, Windows Mail และ Windows Live Mail ได้ที่ตัวเครื่องลูกข่ายโดยตรง

๒.๑๒. มีระบบ Host Intrusion Prevention System และระบบ Self-defense เพื่อป้องกันภัยคุกคามโจมตีระบบได้

๒.๑๓. มีเครื่องมือในการสร้างแผ่น Bootable CD,DVD และ USB เพื่อสแกนและกำจัดไวรัสบนระบบปฏิบัติการได้

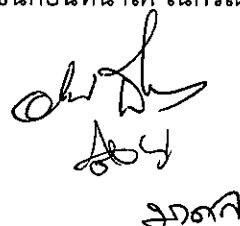
๒.๑๔. สามารถตั้งค่ารหัสผ่านในการล็อคการตั้งค่าโปรแกรมได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปลี่ยนแปลงการตั้งค่าโปรแกรม

๒.๑๕. สามารถอัปเดตฐานข้อมูลไวรัสของโปรแกรมได้โดยอัตโนมัติ และสามารถอัปเดตส่วนประกอบต่างๆ ของโปรแกรมได้

๒.๑๖. โปรแกรมป้องกันไวรัสสามารถตั้งค่ายกเว้นไฟล์ แอปพลิเคชัน และไฟล์เตอร์จากการสแกนได้

๒.๑๗. สามารถควบคุมการใช้งานอุปกรณ์ที่ถอดเข้าออกได้ โดยสามารถระบุประเภท, หมายเลขอุปกรณ์ และกำหนดสิทธิ์ความสามารถที่ผู้ใช้สามารถเข้าถึงและการทำงานกับอุปกรณ์ที่กำหนด

๒.๑๘. สามารถทำการย้อนกลับฐานข้อมูลไวรัสไปยังเวอร์ชันก่อนหน้าได้ ในกรณีที่เกิดผลกระทบในการทำงานจากการปรับปรุงฐานข้อมูลไวรัส



๖๖๓

๒.๑๙. มีเครื่องมือในการตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์ เช่น Drivers, Applications, Network Connection, Registry รวมถึงการประเมินความเสี่ยงของแต่ละ Components อยู่ในโปรแกรมป้องกันไวรัสเอง เพื่อการวิเคราะห์ข้อมูลได้

๒.๒๐. มีความสามารถในการสแกน Unified Extensible Firmware Interface (UEFI)

๒.๒๑. มีความสามารถในการตรวจสอบ Patch ของ Windows ที่ยังไม่ได้ติดตั้งอัปเดต และแจ้งเตือน Patch ที่ในโปรแกรมป้องกันไวรัสได้

๒.๒๒. โปรแกรมป้องกันไวรัสสามารถส่งอีเมลแจ้งเตือนเหตุการณ์ต่าง ๆ ไปยังผู้ดูแลระบบได้โดยอัตโนมัติ

๒.๒๓. โปรแกรมสามารถ Diagnostics เพื่อสร้าง Application crash dump เพื่อใช้ในการตรวจสอบปัญหาได้

๒.๒๔. มีระบบสแกนหน่วยความจำขั้นสูง (Advanced Memory Scanner) เพื่อตรวจจับมัลแวร์ที่ใช้เทคนิคการโจมตีที่ซับซ้อน

๒.๒๕. มีฟังก์ชัน Presentation mode เพื่อปิดการทำงานของหน้าต่างป๊อป-อัพ เมื่อใช้งานแอปพลิเคชันแบบเต็มจอ

๒.๒๖. สามารถตั้งค่าให้สแกนอัตโนมัติ เมื่อคอมพิวเตอร์อยู่ในสถานะ Screen Saver, Computer lock, User logoff

๒.๒๗. มีระบบป้องกันบ็อตเน็ต (Botnet Protection)

๒.๒๘. โปรแกรมสามารถติดตั้งและใช้งานเป็นภาษาไทย (GUI)

๒.๒๙. มีระบบป้องกันการโจมตีทางช่องโหว่ของระบบเครือข่าย (Network Attack Protection)

๒.๓๐. มีระบบป้องกันแรนซัมแวร์ (Ransomware Shield)

๒.๓๑. มีโมดูล Personal Firewall ที่สามารถควบคุมการรับส่งข้อมูลเครือข่ายทั้งหมดทั้งขาเข้าและขาออก

๒.๓๒. มี Secure Browser เพื่อรักษาความปลอดภัยขณะทำธุรกรรมออนไลน์

๒.๓๓. สามารถตรวจสอบชื่อเสียงของไฟล์จากคลาวด์ (Cloud-based protection)

๒.๓๔. สามารถทำ Web Filtering ได้โดยกำหนด Web Category ที่ต้องการ Allow หรือ Block ให้กับผู้ใช้งาน และสามารถ Exclude URL ที่ไม่ต้องการให้โปรแกรมป้องกันไวรัสสแกนได้

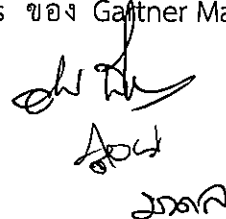
๒.๓๕. มีเครื่องมือการถอนการติดตั้งโปรแกรมป้องกันไวรัสรายอื่นรวมอยู่ในตัวติดตั้ง

๒.๓๖. มีโมดูล Document Protection เพื่อป้องกันไวรัสติดไฟล์เอกสาร Microsoft Office

๒.๓๗. รองรับการดำเนินงานร่วมกับเทคโนโลยี Cloud Sandbox

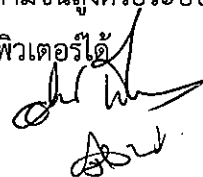
๒.๓๘. ได้รับรางวัลจาก Vb100 ไม่น้อยกว่า ๑๒๐ ครั้ง

๒.๓๙. ผลิตภัณฑ์ที่นำเสนอต้องอยู่ในกลุ่ม Challengers ของ Gartner Magic Quadrant ของ Endpoint Protection Platforms ปี ๒๐๑๙



๓. โปรแกรมบริหารจัดการโปรแกรมป้องกันไวรัสคอมพิวเตอร์

- ๓.๑. สามารถติดตั้งทำงานบนระบบปฏิบัติการดังต่อไปนี้ Microsoft Windows Server ๒๐๑๒/ Server ๒๐๑๖/ Server ๒๐๑๙ และระบบปฏิบัติการ Linux เช่น Ubuntu/CentOS/OpenSUSE ได้เป็นอย่างดีน้อย
- ๓.๒. สามารถบริหารจัดการได้ผ่านเว็บเบราว์เซอร์ (Web Console) และ สามารถบริหารจัดการได้ผ่านเว็บเบราว์เซอร์ (Web Console) โดยใช้งานผ่านคลาวด์ของผู้ผลิต
- ๓.๓. สามารถตรวจสอบ Hardware Inventory และ Installed Application ของเครื่องลูกข่ายได้เป็นอย่างดีน้อย
- ๓.๔. สามารถตรวจสอบเวอร์ชันของฐานข้อมูลไวรัส เวอร์ชันของโปรแกรมป้องกันไวรัสที่ติดตั้งอยู่ที่เครื่องลูกข่าย และลิขสิทธิ์ที่ใช้งานได้เป็นอย่างดีน้อย
- ๓.๕. สามารถเรียกดูการตั้งค่าโปรแกรมของเครื่องลูกข่ายได้
- ๓.๖. สามารถกำหนดนโยบายของเครื่องลูกข่ายตาม Group ได้
- ๓.๗. สามารถสั่งงานไปยังเครื่องลูกข่ายได้ เช่น อัปเดตฐานข้อมูลไวรัส, สแกน, รีสตาร์ท และปิดคอมพิวเตอร์
- ๓.๘. สามารถรองรับการเก็บข้อมูลบนฐานข้อมูล MSSQL และ MYSQL ได้
- ๓.๙. สามารถกำหนดสิทธิ์ให้ผู้ใช้เข้าถึงได้หลายระดับ เช่น Read, Use และ Write
- ๓.๑๐. สามารถแจ้งเตือนเมื่อเกิดเหตุการณ์ต่าง ๆ ไปยังผู้ดูแลระบบได้ ผ่านทางอีเมล และ SNMP Trap
- ๓.๑๑. สามารถเชื่อมต่อกับ Active Directory/Open Directory/LDAP ได้
- ๓.๑๒. มี Dashboard เพื่อมอนิเตอร์สถานะต่าง ๆ ได้
- ๓.๑๓. สามารถทำการบริหารจัดการ Quarantine ของเครื่องลูกข่ายทั้งหมดได้
- ๓.๑๔. สามารถส่งข้อความไปยังอุปกรณ์ต่าง ๆ ได้ (client computer, tablet, mobile)
- ๓.๑๕. สามารถตั้ง Schedule ในการออกรายงานและส่งอีเมลไปยังผู้ดูแลระบบได้
- ๓.๑๖. การจัดทำรายงานสามารถนำเอาข้อมูลออกมาได้ในรูปแบบของ CSV Format หรือ PDF Format
- ๓.๑๗. สามารถส่งข้อมูลออกไปยังระบบเก็บข้อมูลแบบ Syslog และนำข้อมูลออกมาในรูปแบบแบบ Leef และ JSON ได้
- ๓.๑๘. สามารถทำการติดตั้งและถอดถอนโปรแกรม antivirus สำหรับเครื่องลูกข่ายแบบรีโมทจากศูนย์กลางได้
- ๓.๑๙. สามารถตรวจสอบกิจกรรมของ User ที่ Login เข้ามาดำเนินการกับตัวคอนโซลได้
- ๓.๒๐. สามารถสั่งตัดการเชื่อมต่อเน็ตเวิร์คสำหรับเครื่องลูกข่ายแบบรีโมทจากศูนย์กลางได้ (Isolate from network)
- ๓.๒๑. รองรับการทำงานร่วมกับเทคโนโลยีการป้องกันภัยคุกคามขั้นสูงด้วยระบบคลาวด์ได้
- ๓.๒๒. รองรับการทำงานกับโปรแกรมเข้ารหัสไฟล์เครื่องคอมพิวเตอร์ได้



อรรถก

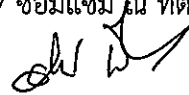
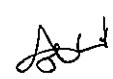
ข้อกำหนดเพิ่มเติม

ผู้สนใจเข้ายื่นข้อเสนอในครั้งนี้จะต้องมีคุณสมบัติเป็นไปตามข้อกำหนดของทางราชการ และข้อกำหนดเพิ่มเติมดังนี้

๑. ผู้ยื่นข้อเสนอจะต้องเสนอผลิตภัณฑ์ดังกล่าวซึ่งเป็นเวอร์ชันล่าสุด ยังอยู่ในสายการผลิต และต้องเป็นผลิตภัณฑ์ที่ผลิตออกมาเป็นชุดภายใต้เครื่องหมายการค้าจดทะเบียนที่ถูกต้อง ผลิตภัณฑ์ที่เสนอต้องมีคุณสมบัติไม่ด้อยกว่าข้อกำหนด ผู้ยื่นข้อเสนอต้องจัดทำรายการข้อเสนอเปรียบเทียบระหว่าง “ข้อกำหนด” และ “ข้อเสนอ” ให้ครบถ้วน ชัดเจน โดยระบุเครื่องหมายการค้าและรุ่นที่เสนอ และจัดทำหมายเลขอ้างอิงในตารางเปรียบเทียบกับแค็ตตาล็อก ที่เสนอทุกรายการ พร้อมทั้งแนบเอกสารยืนยันในรูปแค็ตตาล็อก คู่มือ หรือภาพถ่าย สำนักบริการคอมพิวเตอร์สแกนสิทธิ์ที่จะไม่พิจารณาเอกสารเสนอราคาที่ไม่มีการเปรียบเทียบที่ชัดเจน หรือมีการเปรียบเทียบที่ระบุเพียง “ตรงตามข้อกำหนด” หรือ การนำเสนอข้อความที่มีในลักษณะทำนองเดียวกัน
๒. ผู้ยื่นข้อเสนอต้องเป็นตัวแทนจำหน่ายที่ได้รับการแต่งตั้งจากบริษัทผู้ผลิต พร้อมแนบสำเนาเอกสารการแต่งตั้งเอกสารเสนอราคา เพื่อประกอบการพิจารณาให้แนบเอกสารแสดงรายการคุณลักษณะของผลิตภัณฑ์ที่เป็นฉบับจริง เพื่อประกอบการพิจารณา
๓. ผู้ยื่นข้อเสนอต้องส่งรายชื่อ สถานที่และเบอร์โทรศัพท์ที่ติดต่อได้ง่ายและสะดวกของทีมงาน ผู้ประสานงาน และผู้เชี่ยวชาญให้กับทางมหาวิทยาลัยพิจารณา
๔. ผู้ยื่นข้อเสนอต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานของสำนักงาน หรือทางราชการและได้แจ้งเวียนชื่อแล้วหรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคล หรือบุคคลอื่นเป็นผู้ทำงานตามระเบียบราชการ
๕. ผู้ยื่นข้อเสนอต้องมีเอกสารรายละเอียดของซอฟต์แวร์แอนตี้ไวรัสแต่ละรุ่นว่ารองรับระบบปฏิบัติการและฮาร์ดแวร์ขั้นต่ำ
๖. ผู้ยื่นข้อเสนอต้องมีผลงานการจำหน่ายพัสดุประเภทเดียวกันกับที่จะซื้อให้กับมหาวิทยาลัยหรือสถาบันการศึกษาที่อยู่ในประเทศไทย ในวงเงินไม่น้อยกว่า ๔๔๐,๐๐๐.- บาท ในสัญญาเดียว ภายในเวลาไม่เกิน ๑ ปี นับถัดจากวันทีลงนามในสัญญาหรือใบสั่งซื้อ อย่างน้อย ๑ ผลงาน และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับมหาวิทยาลัยสถาบันการศึกษาที่อยู่ในประเทศไทย โดยต้องแนบสำเนาสัญญาและหนังสือรับรองผลงานเสนอพร้อมการยื่นเสนอราคา

กำหนดการส่งมอบ

๑. ผู้ชนะการเสนอราคาจะต้องจัดส่งพร้อมติดตั้งซอฟต์แวร์ให้สามารถใช้งานได้ตามคุณลักษณะที่กำหนด ณ สถานที่ที่มหาวิทยาลัยกำหนด ภายในเวลา ๓๐ วัน นับถัดจากวันทีลงนามในสัญญา หรือเร็วกว่า
๒. ผู้ชนะการเสนอราคาจะต้องจัดส่งพร้อมติดตั้งซอฟต์แวร์ให้สามารถใช้งานตามคุณลักษณะที่กำหนด ณ มหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตกำแพงแสน, วิทยาเขตศรีราชา, วิทยาเขตเฉลิมพระเกียรติ จ.สกลนคร อย่างน้อยวิทยาเขตละ ๑๐๐๐ License
๓. ผู้ชนะการเสนอราคาจะต้องรับประกันถึงความเสียหายและดูแลรักษาระบบซอฟต์แวร์ทั้งหมดเป็นระยะเวลา ๑ ปี นับจากวันที่ส่งมอบของโครงการเป็นที่เรียบร้อยแล้ว ซึ่งหากเกิดความเสียหายใด ๆ ผู้ชนะการเสนอราคาจะต้องติดต่อกลับภายใน ๔ ชั่วโมงนับจากที่ มหาวิทยาลัยเกษตรศาสตร์แจ้งให้ทราบผ่านทางโทรศัพท์ หรือทางโทรสาร หรือทางจดหมายอิเล็กทรอนิกส์ และดำเนินการเข้าทำการแก้ไข / ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site



 ๒๕๖๓

Service) เพื่อให้ระบบสามารถใช้งานได้ตามปกติให้แล้วเสร็จภายใน ๓ วัน นับจากที่แจ้งให้ทราบผ่านทางโทรศัพท์ หรือทางโทรสาร หรือทางจดหมายอิเล็กทรอนิกส์ โดยไม่คิดค่าใช้จ่ายใด ๆ ในการดำเนินการ ตลอดจนซอฟต์แวร์ จะต้องมิลิซสิทธิ์ใช้งานและการอัปเดตรุ่นตลอดระยะเวลารับประกัน

๔. ผู้ชนะการเสนอราคาจะต้องมีการอบรมการใช้งานผลิตภัณฑ์ที่เสนอให้แก่เจ้าหน้าที่ของสำนักบริการ คอมพิวเตอร์จำนวน ๕ ท่าน พร้อมคู่มือประกอบการใช้งาน อย่างน้อย ๓ ชั่วโมง ณ อาคารสำนักบริการคอมพิวเตอร์ โดยผู้ยื่นข้อเสนอเป็นผู้รับผิดชอบค่าใช้จ่าย

๕. มหาวิทยาลัยมีสิทธิ์ในการอัปเดตและดาวน์โหลดชุดซอฟต์แวร์ทั้งหมดให้เป็นเวอร์ชันล่าสุด เป็น ระยะเวลาอย่างน้อย ๑ ปี โดยไม่มีค่าใช้จ่ายเพิ่มเติมใด ๆ

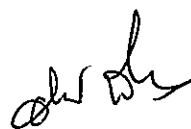
งบประมาณในการจัดซื้อ

งบประมาณในการจัดซื้อชุดระบบตรวจสอบและป้องกันไวรัส สำหรับเครื่องคอมพิวเตอร์ จำนวน ๕,๒๐๐ License จำนวนเงิน ๘๘๔,๖๗๖.- บาท (แปดแสนแปดหมื่นสี่พันหกกร้อยเจ็ดสิบบาทถ้วน)

เกณฑ์การพิจารณา

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ มหาวิทยาลัยเกษตรศาสตร์ จะพิจารณา ตัดสินโดยใช้เกณฑ์ราคา (ใช้ราคาต่ำสุด)

- กำหนดยื่นราคา๔๐..... วัน
- รับประกันความชำรุดบกพร่อง๑.....ปี
- ซ่อมแซมแก้ไขให้ติดตั้งเดิมภายใน.....๓.....วัน


 ๕๐ ๗
 ๕๐๗