ข้อกำหนดการจัดซื้อโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์
ประจำปีงบประมาณ พ.ศ.2562

1. คุณสมบัติผู้เสนอราคา

1.1 ต้องเป็นตัวแทนจำหน่ายของผลิตภัณฑ์ที่เสนอ และจะต้องได้รับการรับรองจากทางเจ้าของผลิตภัณฑ์ หรือผู้แทนจำหน่ายผลิตภัณฑ์ประจำประเทศไทย โดยมีหนังสือที่ออกโดยเจ้าของผลิตภัณฑ์ หรือตัวแทนของเจ้าของผลิตภัณฑ์ในประเทศไทย โดยนำเอกสารมาแสดงประกอบการพิจารณา

1.2 ไม่เป็นผู้ถูกแจ้งเวียนชื่อเป็นผู้ทิ้งงาน หรือไม่เป็นผู้ได้รับผลของการสั่งให้นิติบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการหรือห้ามติดต่อหรือห้ามเข้าเสนอราคาหรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม

2. คุณลักษณะเทคนิคเฉพาะ

2.1 โปรแกรมป้องกันไวรัสคอมพิวเตอร์ โดยต้องมีคุณสมบัติทั่วไปอย่างน้อย ดังนี้

2.1.1 โปรแกรมป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่ายจำนวนไม่น้อยกว่า 1,500 (License)

2.1.2 สามารถติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่มีระบบปฏิบัติการ อย่างน้อยดังนี้

- สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่าง ๆ เช่น Windows Server 2003, Windows Server 2008, Windows server 2008 R2, Windows server 2012 หรือ Windows server เวอร์ชั่นล่าสุด ทั้งแบบ 32 และ 64 bits ได้เป็นอย่างน้อย

2.1.3 สามารถติดตั้งบนเครื่องคอมพิวเตอร์ลูกข่ายที่มีระบบปฏิบัติการ อย่างน้อยดังนี้

- Windows XP SP3, Windows Vista SP2, Windows 7 SP1, Windows 8, Windows 10 ทั้งแบบ 32 และ 64 bits ได้ พร้อมรองรับระบบปฏิบัติการในปัจจุบัน หรือระบบปฏิบัติการรุ่นใหม่ล่าสุดได้

2.1.4 สามารถติดตั้งบน ระบบปฏิบัติการ **Mac Osx** อย่างใดอย่างหนึ่งหรือมากกว่า รายการที่กำหนด ดังนี้

- 10.4 Tiger
- 10.5 Leopard
- 10.6 Snow Leopard
- 10.7 Lion
- 10.8 Mountain Lion
- 10.9 Mavericks
- 10.10 Yosemite
- 10.11 El Capitan
- 10.12 Mac OS® Sierra

2.2 โปรแกรมป้องกันไวรัสสำหรับเครื่องลูกข่าย โดยต้องมีคุณสมบัติทั่วไปอย่างน้อย ดังนี้

2.2.1 สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่าง ๆ เช่น Windows XP SP3, Windows Vista SP2, Windows 7 SP1, Windows 8 และ Windows 10 ทั้งแบบ 32 และ 64 bits ได้ พร้อมรองรับระบบปฏิบัติการในปัจจุบัน หรือระบบปฏิบัติการรุ่นใหม่ล่าสุดได้

2.2.2 สามารถป้องกันจาก Malware (Virus, Spyware, Bots, Backdoors, Key loggers, Root kits, Dialers, Adware, Trojans, Phishing และ Worm) แบบ Real time protection หรือเทคโนโลยีอื่น ที่เทียบเท่าหรือดีกว่า

2.2.3 มีเทคโนโลยีในการตรวจจับ Malware แบบ Signature base, Proactive, Cloud Technology หรือเทคโนโลยีอื่น ที่เทียบเท่าหรือดีกว่า

2.2.4 มีระบบในการรันไฟล์ที่ไม่รู้จักเพื่อเอาพฤติกรรมมาตรวจสอบกับฐานข้อมูลว่าเป็นภัยคุกคามต่ออุปกรณ์หรือไม่ และ สามารถแจ้งเตือนช่องโหว่ของแต่ละ Application ที่อยู่ ภายในเครื่องลูกข่ายพร้อมทั้งออกเป็นรายงานได้

2.2.5 สามารถทำงานแบบ Personal firewall และสามารถทำการตรวจจับการโจมตีผ่านทางระบบเครือข่าย พร้อมทั้งแสดงถึงแหล่งที่มา ประเภท และการแพร่ของการโจมตีเหล่านั้นได้

2.2.6 สามารถป้องกันตนเอง (self-Defense) การปิด Service ของโปรแกรม Antivirus ได้ ถึงแม้ว่าจะมีสิทธิเป็น Administrator ของระบบก็ตาม

1) สามารถกำหนด User Name และ Password ซึ่งกำหนดจาก Server ในการป้องกันการตั้งค่าตัวโปรแกรม เพื่อไม่ให้ User สามารถ แก้ไข และ Uninstall โปรแกรมได้

2.2.7 สามารถทำการตรวจสอบและป้องกันไฟล์สร้างใหม่หรือมีการเปลี่ยนแปลงโดยใช้เทคโนโลยี iSwift, iChecker พร้อมทั้งมีเทคโนโลยี Behavior Analysis และ Exploit Prevention เพื่อป้องกันภัยคุกคามที่เข้ามาทางช่องโหว่

2.2.8 สามารถกำหนดการยกเว้นการ Scan โดยระบุเป็นนามสกุลไฟล์ได้สามารถทำการสั่ง Scan โดย On-Demand ได้ และสามารถทำการ Exclusion ในรูปแบบ Trusted System Certificate Store

2.2.9 สามารถส่งอีเมล์ หรือ Alert Message ไปยังผู้ดูแลระบบได้ เมื่อเครื่อง Server ตรวจพบไวรัส สามารถนำ Alert Message ออกรายงานในรูปแบบ HTML หรือ Text ได้

2.2.10 สามารถกู้คืนความเสียหายที่เกิดขึ้นจากพฤติกรรมของไวรัสได้ (Roll back Malicious Activity)

2.2.12 สามารถกำหนด อนุญาต/ไม่อนุญาต/แจ้งเตือน การเข้าใช้งาน Website ของ user แต่ละคนได้

2.2.12 สามารถอนุญาต/ไม่อนุญาต โปรแกรมที่ใช้อยู่ในเครื่องได้ และ สามารถทำ Application Control เพื่อทำ Black List กับ White List ของแต่ละ Application ได้

2.2.13 สามารถอนุญาต/ไม่อนุญาตการใช้งานอุปกรณ์พกพาจำพวก flash drive memory, CD-DVD drive, Bluetooth ของแต่ละ User และสามารถกำหนด Logging Control ในอุปกรณ์ Removable Drive ได้ โดยสามารถดูข้อมูลว่า Delete, Copy ไฟล์อะไรจาก Removable Drive ลงที่เครื่องลูกข่าย

2.2.14 สามารถตรวจสอบถึงพฤติกรรมอันตรายของไฟล์เพื่อเป็นการยับยั้งการแพร่ระบาดของโปรแกรมที่ มีความร้ายแรงได้ (System Watcher) รวมไปถึงวิเคราะห์พฤติกรรมของไฟล์นั้น ๆ ว่าอันตรายหรือไม่ หากเป็นอันตรายต้องสามารถห้ามไม่ให้ไฟล์ดังกล่าวสามารถใช้งานได้

2.3 โปรแกรมป้องกันไวรัสสำหรับเครื่องแม่ข่าย โดยต้องมีคุณสมบัติทั่วไปอย่างน้อย ดังนี้

2.3.1 สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่าง ๆ เช่น Windows Server 2003, Windows Server 2008, Windows server 2008 R2 , Windows server 2012 หรือ Windows server เวอร์ชันล่าสุด ทั้งแบบ 32 และ 64 bits ได้เป็นอย่างน้อย

2.3.2 สามารถป้องกันจาก Malware (Virus, Spyware, Bots, Backdoors, Key loggers, Root kits, Dialers, Adware, Trojans, Phishing และ Worm) แบบ Real time protection หรือเทคโนโลยีอื่น ที่เทียบเท่าหรือดีกว่า

2.3.3 มีเทคโนโลยีในการตรวจจับ Malware แบบ Signature base, Proactive, Cloud Technology

2.3.4 สามารถทำงานแบบ Personal firewall และสามารถทำการตรวจจับการโจมตีผ่านทางระบบเครือข่าย พร้อมทั้งแสดงถึงแหล่งที่มาประเภท และการแพร่ ของการโจมตีเหล่านั้นได้ และสามารถแจ้งรายงานช่องโหว่ทุก Application ในเครื่องแม่ข่ายได้ (Vulnerabilities)

2.3.5 สแกนไฟล์ในรูปแบบ Compressed, Installation packages ,OLE objects ได้

2.3.6 สามารถป้องกันตนเอง (self-Defense) การปิด Service ของโปรแกรม Antivirus ได้ ถึงแม้ว่าจะมีสิทธิเป็น Administrator ของระบบก็ตาม

2.3.7 มี User Name และ Password ซึ่งกำหนดจาก Server ในการป้องกันการตั้งค่าตัวโปรแกรม เพื่อไม่ให้ User สามารถแก้ไข และ Uninstall โปรแกรมได้

2.3.8 สามารถทำการ scan โดยไม่ไป scan หรือตรวจสอบไฟล์เดิมซ้ำที่ใช้เทคโนโลยี iSwift และ iChecker พร้อมทั้งมีเทคโนโลยี Behavior Analysis และ Exploit Prevention เพื่อป้องกันภัยคุกคามที่เข้ามาทางช่องโหว่

2.3.9 สามารถกำหนดการยกเว้นการ Scan โดยระบุเป็น นามสกุลไฟล์ได้สามารถทำการสั่ง Scan โดย On-Demand ได้ และสามารถทำการ Exclusion ในรูปแบบ Trusted System Certificate Store

2.3.10 สามารถส่งอีเมล์ หรือ Alert Message ไปยังผู้ดูแลระบบได้ เมื่อเครื่อง Server ตรวจพบไวรัส สามารถนำ Alert Message ออกรายงานในรูปแบบ HTML หรือ Text ได้

3. โปรแกรมบริหารจัดการสำหรับเครื่องลูกข่ายและเครื่องแม่ข่าย โดยต้องมีคุณสมบัติทั่วไปอย่างน้อย ดังนี้

รองรับระบบปฏิบัติการ Windows Server 2008 R2, VMWare ESX, Windows 7, Windows 8 และ Windows 10 ทั้งแบบ 32 และ 64 bits ได้ พร้อมรองรับ ระบบปฏิบัติการในปัจจุบัน หรือระบบปฏิบัติการรุ่นใหม่ล่าสุดได้ หรือรองรับการบริหารจัดการผ่านระบบ Cloud-Base Console ได้

3.1 รองรับการใช้งานกับ Database Microsoft SQLServer 2005, 2008 เทียบเท่าหรือดีกว่า รองรับ My SQl 5.0 เทียบเท่าหรือดีกว่า

3.2 สามารถบริหารจัดการความปลอดภัยบนเครื่องคอมพิวเตอร์สำหรับองค์กรที่ประกอบไปด้วยเทคโนโลยีทางด้าน Anti-Malware, Personal Firewall, Intrusion Detection และ Device, Web and Application Control ได้ หรืออย่างใดอย่างหนึ่ง ได้เป็นอย่างน้อย และสามารถควบคุมโปรแกรมป้องกันไวรัสได้ทั้

3.3 สามารถบริหารจัดการโปรแกรมป้องกันไวรัสคอมพิวเตอร์ได้ทั้ง Windows, Mac OSX, Smart Phone, Linux, Vmware, Hyper V, Citrix, KVM ได้ภายในโปรแกรมบริหารจัดการเดียว

3.4 สามารถทำการ update virus/spyware pattern แบบ incremental update หรือเทคโนโลยีอื่นที่เทียบเท่าหรือดีกว่า เพื่อลดภาระในระบบเครือข่ายได้

3.5 สามารถแสดงรายงานของไฟล์ที่ถูกสำรองข้อมูลไว้หากถูกลบไป (backup) หรือ โดนกักกัน (quarantine) ไว้ได้จากส่วนกลางและสามารถสั่งคืนค่าไฟล์ดังกล่าวได้จากส่วนกลาง

3.6 สามารถตรวจสอบโปรแกรมต่าง ๆ ที่ติดตั้งอยู่บนเครื่องลูกข่าย และ ระบบเครื่องแม่ข่าย (Inventory) ในระบบได้ พร้อมทั้งแจ้งช่องโหว่ในแต่ละ Application ของเครื่องลูกข่าย, เครื่องแม่ข่าย และ สามารถออกรายงานของช่องโหว่ของโปรแกรมต่าง ๆ ที่เครื่องลูกข่าย และ เครื่องแม่ข่ายได้

3.7 สามารถทำการกู้คืนและสำรองฐานข้อมูลของเครื่องแม่ข่ายเพื่อป้องกันในกรณีระบบเกิดการเสียหาย

3.8 สามารถดึง (import) เอารายละเอียดกลุ่มที่ได้สร้างเอาไว้จาก Active Directory เพื่อนำมาแบ่งกลุ่มการใช้งานตัวโปรแกรมบริหารจากส่วนกลางได้

3.9 สามารถบริหารจัดการ และกำหนดนโยบายให้กับ Mobile device ที่ติดตั้งโปรแกรมป้องกันไวรัสลงไปได้ (Mobile Device Management)

3.10 สามารถสร้างรายงาน ในรูปแบบ PDF, Microsoft Excel, HTML ได้

3.11 สามารถเข้าถึงเครื่องควบคุมส่วนกลางได้หลายเครื่องหลายผู้ใช้งานตามที่สถาบันบัณฑิตพัฒนศิลป์กำหนดเพื่อส่งข้อมูลและสั่งงานกันได้ระหว่างหน่วยงาน และบริหารโปรแกรมป้องกันไวรัสจากศูนย์กลางกันเองและเครื่องลูกข่าย

4. การส่งมอบและการรับประกัน

4.1 การส่งมอบ

4.1.1 ผู้ขายต้องส่งมอบพัสดุให้แล้วเสร็จ ภายใน 90 วัน นับตั้งแต่วันที่ 1 เมษายน 2562 โดยการติดตั้งโปรแกรมฯ มีรายละเอียดดังนี้

4.1.1.1 ผู้ขายต้องดำเนินการติดตั้งโปรแกรมบริหารจัดการสำหรับเครื่องลูกข่ายและเครื่องแม่ข่ายให้กับสถาบันบัณฑิตพัฒนศิลป์ ในส่วนกลาง ตั้งแต่วันที่ 1 เมษายน 2562 ให้แล้วเสร็จภายใน 30 วัน หากมีการให้ดำเนินการติดตั้งในภายหลัง ผู้ขายต้องดำเนินการติดตั้งให้กับสถาบันฯ โดยไม่มีค่าใช้จ่ายเพิ่ม

4.1.1.2 ผู้ขายต้องจัดทำโปรแกรมการติดตั้งโปรแกรมป้องกันไวรัสเพื่อจัดส่งให้กับหน่วยงานในสังกัดสถาบันบัณฑิตพัฒนศิลป์ เพื่อใช้ในการติดตั้ง จำนวน 18 ชุด ให้แล้วเสร็จภายใน 60 วัน นับตั้งแต่วันที่ 1 เมษายน 2562

4.1.1.3 โปรแกรมป้องกันและกำจัดไวรัส ต้องสามารถติดตั้งหน่วยงานในสังกัดสถาบันบัณฑิตพัฒนศิลป์ทั้ง 19 หน่วยงานได้ ทั้งในเครือข่ายเดียวกันและต่างเครือข่าย โดยต้องจัดส่งเอกสารคู่มือการติดตั้งและการใช้งานโปรแกรมป้องกันและกำจัดไวรัส จำนวน 20 ชุด ภายใน 60 วัน นับตั้งแต่วันที่ 1 เมษายน 2562 รายการดังนี้

1) จัดส่งคู่มือสำหรับการติดตั้งและการใช้งานสำหรับเครื่องลูกข่าย จำนวน 20 เล่ม

2) จัดส่งคู่มือสำหรับการติดตั้งและการใช้งานสำหรับเครื่องแม่ข่าย รวมถึงการกำหนดค่าการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย ที่ต้องการติดตั้งโปรแกรมบริหารจัดการโปรแกรมป้องกันไวรัสจากศูนย์กลาง จำนวน 2 เล่ม

4.1.1.4 จัดส่งแผ่นโปรแกรม Installation CD\DVD ที่มีสิขสิทธิ์ถูกต้องตามกฎหมาย สำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวน 1 ชุด สำหรับเครื่องคอมพิวเตอร์แม่ข่ายจำนวน 1 ชุด และโปรแกรมสำหรับการบริหารจัดการโปรแกรมป้องกันไวรัส จำนวน 1 ชุด

4.1.1.5 จัดส่งเอกสาร License Support Certificate สำหรับเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่าย จำนวน 1,500 License

4.1.1.6 จัดทำรายงานผลการดำเนินการติดตั้งโปรแกรมบริหารจัดการสำหรับเครื่องลูกข่ายและเครื่องแม่ข่าย ซึ่งแสดงความพร้อมใช้งาน ในรูปแบบเอกสาร อย่างน้อย จำนวน 2 เล่ม ภายใน 60 วัน นับตั้งแต่วันที่ 1 เมษายน 2562

4.1.1.7 ผู้รับจ้างต้องอบรมการติดตั้งและบริหารจัดการให้กับผู้ดูแลระบบส่วนกลางของสถาบันบัณฑิตพัฒนศิลป์ จำนวนไม่น้อยกว่า 6 คน ณ สถานที่ วันและเวลา ตามที่สถาบันบัณฑิตพัฒนศิลป์กำหนด โดยผู้รับจ้างต้องเป็นผู้รับผิดชอบค่าใช้จ่ายในการจัดอบรมประกอบด้วย เอกสารการอบรม ค่าอาหารกลางวัน ค่าอาหารว่างและเครื่องดื่ม

4.2 การรับประกัน

การ Update Version หรือ Patch โปรแกรม ผู้รับจ้างต้องดำเนินการดังกล่าวให้กับสถาบันบัณฑิตพัฒนศิลป์โดยไม่เสียค่าใช้จ่ายใด ๆ ตลอดระยะเวลาไม่น้อยกว่า 1 ปี นับจากคณะกรรมการมีการตรวจรับงานเรียบร้อยแล้ว

5. การตรวจรับ

5.1 ผู้ขายต้องประสานงานกับเจ้าหน้าที่งานเทคโนโลยีสารสนเทศ สถาบันบัณฑิตพัฒนศิลป์ ก่อนดำเนินการส่งมอบครุภัณฑ์ที่จัดซื้อฯ โดยทำเป็นหนังสือแจ้งกำหนดการส่งมอบก่อนวันส่งมอบไม่น้อยกว่า 5 วันทำการ และต้องดำเนินการ ดังต่อไปนี้

5.1.1 กำหนดสถานที่ตรวจรับและส่งของ ณ สำนักงานอธิการบดี สถาบันบัณฑิตพัฒนศิลป์ 119/19 หมู่ 3 ต.ศาลายา อ.พุทธมณฑล จ.นครปฐม 73170

5.1.2 คณะกรรมการตรวจรับฯ จะทำการตรวจรับ เมื่อผู้ขายดำเนินการให้เป็นไปตามกำหนด ทุกประการ

6. การชำระเงิน

สถาบันบัณฑิตพัฒนศิลป์ จะชำระเงินค่าจัดซื้อครุภัณฑ์และติดตั้งงวดเดียว โดยจะชำระให้หลังจากคณะกรรมการตรวจรับของสถาบันฯ ได้พิจารณาหลักฐานการรายงานผลการตรวจสอบคุณลักษณะของรายการที่ส่งมอบ และประสิทธิภาพการใช้งาน แล้วเห็นว่า ผู้ขายปฏิบัติตามสัญญาเรียบร้อยแล้วเสร็จ ทั้งนี้ การเบิกจ่ายต้องเป็นไปตามระเบียบวิธีปฏิบัติของสถาบันฯ

7. การคุ้มครองและอัตราค่าปรับ

ผู้ขายต้องรับประกันความชำรุดบกพร่องหรือขัดข้องของครุภัณฑ์ที่จัดซื้อ ฯ อันเกิดจากความบกพร่องของอุปกรณ์ และความบกพร่องของผู้ขาย รวมถึงความบกพร่องในการขนส่ง ก่อนส่งมอบให้สถาบัน ฯ

ผู้ขายต้องทำการส่งมอบให้ทันตามกำหนดเวลา และหากผู้ขายไม่สามารถกระทำการดังกล่าวได้อันเนื่องมาจากปัญหาของทางผู้ขายเอง ผู้ขายต้องถูกปรับเป็นรายวันในอัตราร้อยละ 0.2 ของวงเงินตามสัญญานับจากวันถัดจากวันครบกำหนดส่งมอบพัสดุตามสัญญา

8. วงเงินในการจัดหา

ภายในวงเงิน 600,000.- บาท (หกแสนบาทถ้วน) โดยเบิกจ่ายจากงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2562

9. หลักเกณฑ์การพิจารณาคัดเลือก

พิจารณาคัดเลือกข้อเสนอโดยใช้เกณฑ์ราคา ซึ่งราคาที่เสนอต้องเป็นราคารวมภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่นๆ ค่าติดตั้ง ค่าแรงติดตั้ง และค่าใช้จ่ายทั้งปวงแล้ว