

**รายละเอียดขอบเขตของงาน**  
**การจัดซื้อโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ จำนวน 1 ชุด**  
**ประจำปีงบประมาณ พ.ศ.2564**

**1. หลักการและเหตุผล**

การเข้าถึงและใช้ประโยชน์จากเทคโนโลยีดิจิทัล และข้อมูลข่าวสาร เป็นฐานรากในการพัฒนา การสร้างความเจริญเติบโตทางเศรษฐกิจ การเพิ่มขีดความสามารถในการให้บริการ และการพัฒนาทางสังคมในด้านต่าง ๆ ควบคู่กันไป ความก้าวหน้าและนวัตกรรมของเทคโนโลยีดิจิทัล ยังส่งผลต่อการเปลี่ยนแปลง ทั้งรูปแบบ กระบวนการ โครงสร้าง ทางด้านกิจกรรมทางเศรษฐกิจและสังคมอย่างหลีกเลี่ยงไม่ได้ โดยที่การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นกลไกสำคัญในการขับเคลื่อนการปฏิรูปกระบวนการผลิต การบริการ การศึกษา การบริหารราชการแผ่นดิน รวมถึงกิจกรรมทางเศรษฐกิจและสังคมอื่น ๆ ที่ส่งผลต่อการพัฒนาพัฒนาคุณภาพชีวิตของคนในสังคมไทย ตามมาตรการด้านความมั่นคงปลอดภัยในการใช้ระบบสารสนเทศภาครัฐ ของสถาบันบัณฑิตพัฒนศิลป์ ได้กำหนดแนวทางการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศ ต้องมีโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ ติดตั้งใช้งานในเครื่องคอมพิวเตอร์ทุกเครื่องที่ใช้งานในระบบเครือข่ายเดียวกันของสถาบันบัณฑิตพัฒนศิลป์ และเพื่อให้เป็นมาตรฐานเดียวกันทั้งสถาบันบัณฑิตพัฒนศิลป์ อันจะก่อให้เกิดประสิทธิภาพในการควบคุม ดูแล บริหารจัดการ ระบบรักษาความมั่นคงปลอดภัย ในภาพรวมของหน่วยงาน จำเป็นต้องจัดซื้อโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ จากส่วนกลาง เพื่อบริหารจัดการแบบรวมศูนย์ในครั้งนี้

**2. วัตถุประสงค์**

- 2.1 เพื่อจัดหาโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์ที่ใช้งานภายในระบบเครือข่ายของสถาบันบัณฑิตพัฒนศิลป์
- 2.2 เพื่อให้การบริหารจัดการ ควบคุม ดูแล ระบบรักษาความมั่นคงปลอดภัย เป็นมาตรฐานเดียวกัน การใช้งานระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ มีประสิทธิภาพ มั่นคงปลอดภัย เป็นไปอย่างต่อเนื่อง

**3. เป้าหมาย**

จัดสรรโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์ของสถาบัน จำนวน 1,500 ลิขสิทธิ์ สำหรับเครื่องคอมพิวเตอร์ทุกเครื่อง ของทุกหน่วยงานในสังกัดสถาบันบัณฑิตพัฒนศิลป์ ส่งผลให้เครื่องคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์ สามารถใช้ประโยชน์ ได้อย่างมีประสิทธิภาพ

**4. คุณสมบัติของผู้ยื่นข้อเสนอ**

- 4.1 มีความสามารถตามกฎหมาย
- 4.2 ไม่เป็นบุคคลล้มละลาย
- 4.3 ไม่อยู่ระหว่างเลิกกิจการ
- 4.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนด ตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

4.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

4.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

4.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพจำหน่ายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

4.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอแก่สถาบันบัณฑิตพัฒนศิลป์ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางแข่งขันอย่างเป็นทางการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

4.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นนั้น

4.10 ต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

4.11 ต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทย โดยให้ยื่นหนังสือแสดงการแต่งตั้งตัวแทนจำหน่ายดังกล่าวพร้อมกับการเสนอราคา

## 5. รายละเอียดคุณลักษณะเทคนิคเฉพาะ

5.1 โปรแกรมป้องกันไวรัสคอมพิวเตอร์ โดยต้องมีคุณสมบัติทั่วไปอย่างน้อย ดังนี้

5.1.1 โปรแกรมป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่ายจำนวนไม่น้อยกว่า 1,500 (License)

5.1.2 สามารถติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่มีระบบปฏิบัติการ อย่างน้อยดังนี้

- สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่าง ๆ เช่น Windows Server 2003, Windows Server 2008 SP2, Windows server 2008 R2 SP1, Windows server 2012, Windows server 2016 Windows server 2019, หรือ Windows server เวอร์ชันล่าสุด ทั้งแบบ 32 และ 64 bits ได้

5.1.3 สามารถติดตั้งบนเครื่องคอมพิวเตอร์ลูกข่ายที่มีระบบปฏิบัติการ อย่างน้อยดังนี้

- Windows 7 SP1, Windows 8, Windows 10 ทั้งแบบ 32 และ 64 bits ได้ พร้อมรองรับระบบปฏิบัติการในปัจจุบัน หรือระบบปฏิบัติการรุ่นใหม่ล่าสุดได้

5.1.4 สามารถติดตั้งบน ระบบปฏิบัติการ Mac Osx อย่างใดอย่างหนึ่งหรือมากกว่า รายการที่กำหนด ดังนี้

- 10.12 Mac OS® Sierra
- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15

5.2 โปรแกรมป้องกันไวรัสสำหรับเครื่องลูกข่าย โดยต้องมีคุณสมบัติทั่วไปอย่างน้อย ดังนี้

5.2.1 สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่าง ๆ เช่น Windows 7 SP1, Windows 8 และ Windows 10 ทั้งแบบ 32 และ 64 bits ได้ พร้อมรองรับ ระบบปฏิบัติการในปัจจุบัน หรือระบบปฏิบัติการรุ่นใหม่ล่าสุดได้

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

5.2.3 มีเทคโนโลยีในการตรวจจับ Malware แบบ Signature base, Proactive, Cloud Technology Behavior Detection, Machine Learning, Exploit Prevention, Host-Based Intrusion Prevention System อย่างใดอย่างหนึ่ง หรือเทคโนโลยีอื่น ที่เทียบเท่าหรือดีกว่า

5.2.4 มีระบบในการรันไฟล์ที่ไม่รู้จักเพื่อเอาพฤติกรรมมาตรวจสอบกับฐานข้อมูลว่าเป็นภัยคุกคามต่ออุปกรณ์หรือไม่ และสามารถแจ้งเตือนช่องโหว่ของแต่ละ Application ที่อยู่ ภายในเครื่องลูกข่ายพร้อมทั้งออกเป็นรายงานได้

5.2.5 สามารถทำงานแบบ Personal firewall และสามารถทำการตรวจจับการโจมตีผ่านทางระบบเครือข่าย พร้อมทั้งแสดงถึงแหล่งที่มา ประเภท และการแพร่ของการโจมตีเหล่านั้นได้

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

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

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

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

5.2.9 สามารถส่งอีเมล หรือ Alert Message ไปยังผู้ดูแลระบบได้ เมื่อเครื่อง Server ตรวจพบไวรัส สามารถนำ Alert Message ออกรายงานในรูปแบบ HTML หรือ Text ได้

5.2.10 สามารถกู้คืนความเสียหายที่เกิดขึ้นจากพฤติกรรมของไวรัสได้ (Roll back Malicious Activity)

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

5.2.12 สามารถอนุญาต/ไม่อนุญาต โปรแกรมที่ใช้อยู่ในเครื่องได้ และสามารถทำ Application Control เพื่อทำ Black List กับ White List ของแต่ละ Application ได้

5.2.13 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

5.2.14 สามารถตรวจสอบถึงพฤติกรรมอันตรายของไฟล์เพื่อเป็นการยับยั้งการแพร่ระบาดของโปรแกรมที่มีความร้ายแรงได้ (Behavior Detection) รวมไปถึงวิเคราะห์พฤติกรรมของไฟล์นั้น ๆ ว่าอันตรายหรือไม่ หากเป็นอันตรายต้องสามารถห้ามไม่ให้ไฟล์ดังกล่าวสามารถใช้งานได้

5.3 โปรแกรมป้องกันไวรัสสำหรับเครื่องแม่ข่าย โดยต้องมีคุณสมบัติทั่วไปอย่างน้อย ดังนี้

5.3.1 สามารถติดตั้งบนระบบปฏิบัติการ Windows รุ่นต่าง ๆ เช่น Windows Server 2003, Windows Server 2008 SP2, Windows server 2008 R2 SP1, Windows server 2012, Windows server 2016, Windows server 2019 หรือ Windows server เวอร์ชันล่าสุด ทั้งแบบ 32 และ 64 bits ได้เป็นอย่างน้อย

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

5.3.3 มีเทคโนโลยีในการตรวจจับ Malware แบบ Signature base, Proactive, Cloud Technology Behavior Detection, Machine Learning, Exploit Prevention, Host-Based Intrusion Prevention System อย่างใดอย่างหนึ่ง หรือเทคโนโลยีอื่น ที่เทียบเท่าหรือดีกว่า

5.3.4 สามารถทำงานแบบ Personal firewall และสามารถทำการตรวจจับการโจมตีผ่านทางระบบเครือข่าย พร้อมทั้งแสดงถึงแหล่งที่มาประเภท และการแพร่ ของการโจมตีเหล่านั้นได้ และสามารถแจ้งรายงาน ช่องโหว่ทุก Application ในเครื่องแม่ข่ายได้ (Vulnerabilities)

5.3.5 สแกนไฟล์ในรูปแบบ Compressed, Installation packages, OLE objects ได้

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

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

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

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

5.3.10 สามารถส่งอีเมล หรือ Alert Message ไปยังผู้ดูแลระบบได้ เมื่อเครื่อง Server ตรวจพบไวรัสสามารถนำ Alert Message ออกรายงานในรูปแบบ HTML หรือ Text ได้

5.4 โปรแกรมบริหารจัดการสำหรับเครื่องลูกข่ายและเครื่องแม่ข่าย โดยต้องมีคุณสมบัติทั่วไปอย่างน้อย ดังนี้

5.4.1 รองรับระบบปฏิบัติการ Windows Server 2008 R2 SP1, VMWare ESX, Windows 7 SP1, Windows 8 และ Windows 10 ทั้งแบบ 32 และ 64 bits ได้ พร้อมรองรับ ระบบปฏิบัติการในปัจจุบัน หรือระบบปฏิบัติการรุ่นใหม่ล่าสุดได้ หรือรองรับการบริหารจัดการผ่านระบบ Cloud-Base Console ได้

5.4.2 รองรับการใช้งานกับ Database Microsoft SQLServer 2012 เทียบเท่าหรือดีกว่า รองรับ My SQL 5.7 เทียบเท่าหรือดีกว่า

5.4.3 สามารถบริหารจัดการความปลอดภัยบนเครื่องคอมพิวเตอร์สำหรับองค์กรที่ประกอบไปด้วย เทคโนโลยีทางด้าน Anti-Malware, Personal Firewall, Intrusion Detection และ Device, Web and Application Control ได้ หรืออย่างใดอย่างหนึ่ง ได้เป็นอย่างน้อย และสามารถควบคุมโปรแกรมป้องกันไวรัสได้

5.4.4 มีเทคโนโลยีตรวจจับหา Malware ที่เครื่องแม่ข่ายในรูปแบบ Real Time ใช้เทคโนโลยีแบบ Cloud - assisted security intelligence และทำการตรวจสอบช่องโหว่ (Vulnerabilities) ของ Software ภายในเครื่องแม่ข่ายและเครื่องลูกข่ายได้ทั้งหมดจากโปรแกรมบริหารจัดการ

5.4.5 สามารถบริหารจัดการโปรแกรมป้องกันไวรัสคอมพิวเตอร์ได้ทั้ง Windows, Mac OSX, Smart Phone, Linux, VMware, Hyper V, Citrix, KVM ได้ภายในโปรแกรมบริหารจัดการเดียว

5.4.6 สามารถทำการ update virus/spyware pattern แบบ incremental update หรือ เทคโนโลยีอื่นที่เทียบเท่าหรือดีกว่า เพื่อลดภาระในระบบเครือข่ายได้

5.4.7 สามารถแสดงรายงานของไฟล์ที่ถูกสำรองข้อมูลไว้หากถูกลบไป (backup) หรือ โดนกักกัน (quarantine) ไว้ได้จากส่วนกลางและสามารถส่งคืนค่าไฟล์ดังกล่าวได้จากส่วนกลาง

5.4.8 สามารถตรวจสอบโปรแกรมต่าง ๆ ที่ติดตั้งอยู่บนเครื่องลูกข่าย และระบบเครื่องแม่ข่าย (Inventory) ในระบบได้ พร้อมทั้งแจ้งช่องโหว่ในแต่ละ Application ของเครื่องลูกข่าย, เครื่องแม่ข่าย และสามารถออกรายงานของช่องโหว่ของโปรแกรมต่าง ๆ ที่เครื่องลูกข่าย และ เครื่องแม่ข่ายได้

5.4.9 สามารถทำการกู้คืนและสำรองฐานข้อมูลของเครื่องแม่ข่ายเพื่อป้องกันในกรณีระบบเกิดการเสียหาย

5.4.10 สามารถดึง (import) เอรายละเอียดกลุ่มที่ได้สร้างเอาไว้จาก Active Directory เพื่อนำมาแบ่งกลุ่มการใช้งานตัวโปรแกรมบริหารจากส่วนกลางได้

5.4.11 สามารถบริหารจัดการ และกำหนดนโยบายให้กับ Mobile device ที่ติดตั้งโปรแกรมป้องกันไวรัสลงไปได้ (Mobile Device Management)

5.4.12 สามารถสร้างรายงาน ในรูปแบบ PDF, Microsoft Excel, HTML ได้

5.4.13 สามารถย้อนคืนค่าการทำงานใน Operation System ที่ Malware สร้างความเสียหายได้ (Remediation Engine) หรือ สามารถย้อนคืนค่าการทำงานใน Operation System กรณี Malware สร้างความเสียหายใน Operation System (Roll back action)

5.4.14 สามารถกำหนด User name, Password เพื่อสามารถแก้ไขหรือ Uninstall โปรแกรมได้จากตัวโปรแกรม Anti - Virus เอง หรือ จากโปรแกรมบริหารจัดการ Anti - Virus ได้

5.4.15 สามารถเข้าถึงเครื่องควบคุมส่วนกลางได้หลายเครื่องหลายผู้ใช้งานตามที่สถาบันบัณฑิตพัฒนศิลป์กำหนดเพื่อส่งข้อมูลและสั่งงานกันได้ระหว่างหน่วยงาน และบริหารโปรแกรมป้องกันไวรัสจากศูนย์กลางกันเองและเครื่องลูกข่าย

## 6. การส่งมอบและการรับประกัน

### 6.1 การส่งมอบ

ผู้ขายต้องส่งมอบพัสดุให้แล้วเสร็จ ภายใน 90 วัน นับตั้งแต่วันที่ 1 เมษายน 2564 โดยการติดตั้งโปรแกรมฯ มีรายละเอียดดังนี้

6.1.1 ผู้ขายต้องดำเนินการติดตั้งโปรแกรมบริหารจัดการสำหรับเครื่องลูกข่ายและเครื่องแม่ข่ายให้กับสถาบันบัณฑิตพัฒนศิลป์ ในส่วนกลาง ตั้งแต่วันที่ 1 เมษายน 2564 ให้แล้วเสร็จภายใน 30 วัน หากมีการให้ดำเนินการติดตั้งในภายหลัง ผู้ขายต้องดำเนินการติดตั้งให้กับสถาบันฯ โดยไม่มีค่าใช้จ่ายเพิ่ม

6.1.2 ผู้ขายต้องจัดทำโปรแกรมการติดตั้งโปรแกรมป้องกันไวรัสเพื่อจัดส่งให้กับหน่วยงานในสังกัดสถาบันบัณฑิตพัฒนศิลป์ เพื่อใช้ในการติดตั้ง จำนวน 18 ชุด ให้แล้วเสร็จภายใน 60 วัน นับตั้งแต่วันที่ 1 เมษายน 2564

6.1.3 โปรแกรมป้องกันและกำจัดไวรัส ต้องสามารถติดตั้งสำหรับหน่วยงานในสังกัดสถาบันบัณฑิตพัฒนศิลป์ทั้ง 19 หน่วยงานได้ ทั้งในเครือข่ายเดียวกันและต่างเครือข่าย โดยต้องจัดส่งเอกสารคู่มือการติดตั้งและการใช้งานโปรแกรมป้องกันและกำจัดไวรัส จำนวน 20 ชุด ภายใน 60 วัน นับตั้งแต่วันที่ 1 เมษายน 2564 รายการดังนี้

- 1) จัดส่งคู่มือสำหรับการติดตั้งและการใช้งานสำหรับเครื่องลูกข่าย จำนวน 20 เล่ม
- 2) จัดส่งคู่มือสำหรับการติดตั้งและการใช้งานสำหรับเครื่องแม่ข่าย รวมถึงการกำหนดค่าการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย ที่ต้องการติดตั้งโปรแกรมบริหารจัดการโปรแกรมป้องกันไวรัสจากศูนย์กลาง จำนวน 2 เล่ม

6.1.4 จัดส่งแผ่นโปรแกรม Installation CD\DVD สำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวน 1 ชุด สำหรับเครื่องคอมพิวเตอร์แม่ข่ายจำนวน 1 ชุด และโปรแกรมสำหรับการบริหารจัดการโปรแกรมป้องกันไวรัส จำนวน 1 ชุด

6.1.5 จัดส่งเอกสาร License Support Certificate สำหรับเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่าย จำนวน 1,500 License

6.1.6 ผู้รับจ้างต้องอบรมการติดตั้งและบริหารจัดการให้กับผู้ดูแลระบบส่วนกลางของสถาบันบัณฑิตพัฒนศิลป์ จำนวนไม่น้อยกว่า 5 คน ณ สถานที่ วันและเวลา ตามที่สถาบันบัณฑิตพัฒนศิลป์กำหนด (ภายใน 30 วัน นับตั้งแต่วันที่ 1 เมษายน 2564) โดยผู้รับจ้างต้องเป็นผู้รับผิดชอบค่าใช้จ่ายในการจัดอบรมประกอบด้วย เอกสารการอบรม ค่าอาหารกลางวัน ค่าอาหารว่างและเครื่องดื่ม

## 6.2 การรับประกัน

การ Update Version หรือ Patch โปรแกรม ผู้รับจ้างต้องดำเนินการดังกล่าวให้กับสถาบันบัณฑิตพัฒนศิลป์โดยไม่เสียค่าใช้จ่ายใด ๆ ตลอดระยะเวลาไม่น้อยกว่า 1 ปี นับจากวันที่ผู้ขายส่งมอบสิ่งของไว้ถูกต้องครบถ้วนตามสัญญา และคณะกรรมการมีการตรวจรับงานเรียบร้อยแล้ว

## 7. งบประมาณและราคากลาง

7.1 วงเงินงบประมาณในการจัดซื้อ เป็นเงินทั้งสิ้น 600,000 บาท (หกแสนบาทถ้วน) โดยเบิกจ่ายจากงบประจำปีงบประมาณ พ.ศ.2564 ซึ่งเป็นราคารวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น ค่าติดตั้ง ค่าขนส่ง และค่าใช้จ่ายที่พึงปวงแล้ว

7.2 ราคากลางในการจัดซื้อ เป็นเงิน 552,120 บาท (ห้าแสนห้าหมื่นสองพันหนึ่งร้อยยี่สิบบาทถ้วน) โดยอ้างอิงจากราคาที่เคยจัดซื้อครั้งล่าสุดภายใน 2 ปีงบประมาณ ตามสัญญาซื้อขาย เลขที่ 7/2563 ลงวันที่ 13 มีนาคม 2563

## 8. การตรวจรับ

ผู้ขายต้องประสานงานกับเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ สถาบันบัณฑิตพัฒนศิลป์ก่อนดำเนินการส่งมอบครุภัณฑ์ที่จัดซื้อฯ โดยทำเป็นหนังสือแจ้งกำหนดการส่งมอบก่อนวันส่งมอบไม่น้อยกว่า 3 วันทำการ และต้องดำเนินการ ดังต่อไปนี้

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

8.2 คณะกรรมการตรวจรับฯ จะทำการตรวจรับ เมื่อผู้ขายดำเนินการให้เป็นไปตามกำหนด ทุกประการ

## 9. การชำระเงิน

สถาบันบัณฑิตพัฒนศิลป์ จะชำระเงินค่าจัดซื้อครุภัณฑ์และติดตั้งงวดเดียว โดยจะชำระให้หลังจากคณะกรรมการตรวจรับของสถาบันฯ ได้พิจารณาหลักฐานการรายงานผลการตรวจสอบคุณลักษณะของรายการที่ส่งมอบ และประสิทธิภาพการใช้งานแล้ว และเห็นว่าผู้ขายปฏิบัติตามสัญญาเรียบร้อยแล้วเท่านั้น

## 10. การคุ้มครองและอัตราค่าปรับ

ผู้ขายต้องรับประกันความชำรุดบกพร่องหรือข้อบกพร่องของครุภัณฑ์ที่จัดซื้อฯ อันเกิดจากความบกพร่องของอุปกรณ์ และความบกพร่องของผู้ขาย รวมถึงความบกพร่องในการขนส่ง ก่อนส่งมอบให้สถาบันฯ ผู้ขายต้องทำการส่งมอบให้ทันตามกำหนดเวลา และหากผู้ขายไม่สามารถกระทำการดังกล่าวได้ อันเนื่องมาจากปัญหาของทางผู้ขายเอง ผู้ขายต้องถูกปรับเป็นรายวันในอัตราร้อยละ 0.2 ของราคาส่งของที่สถาบันฯ ยังไม่ได้รับมอบ นับจากวันถัดจากวันครบกำหนดส่งมอบตามสัญญา จนถึงวันที่ผู้ขายส่งมอบสิ่งของถูกต้องและครบถ้วน

## 11. หลักเกณฑ์การพิจารณาคัดเลือก

พิจารณาคัดเลือกข้อเสนอโดยใช้เกณฑ์ราคา

## 12. ข้อกำหนดและเงื่อนไขอื่น ๆ

12.1 รายละเอียดขอบเขตของงาน ตลอดจนเงื่อนไขอื่น ๆ ภายใต้อรายละเอียดขอบเขตของงานนี้ ถือเป็นส่วนหนึ่งของสัญญาหรือข้อตกลง ซึ่งผู้รับจ้างต้องปฏิบัติให้เป็นไปตามเงื่อนไขที่กำหนด ทุกประการ

12.2 การลงนามในสัญญาหรือข้อตกลงจะกระทำต่อเมื่อพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2564 มีผลใช้บังคับและได้รับจัดสรรงบประมาณจากสำนักงบประมาณแล้วเท่านั้น สำหรับกรณีไม่ได้รับการจัดสรรงบประมาณเพื่อการจัดหาครั้งนี้ สถาบันฯ สามารถยกเลิกการจัดหาได้