ขอบเขตการดำเนินงาน
โครงการจัดหาโปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์
กรมการแพทย์
(Term of Reference: TOR)

โดย

กรมการแพทย์ กระทรวงสาธารณสุข
ถนนติวานนท์ อำเภอเมือง จังหวัดนนทบุรี 11000

โครงการจัดหาโปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์
กรมการแพทย์

---

1. <u>ความเป็นมา</u>

ด้วยกรมการแพทย์มีเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่ายจำนวนมากที่ติดตั้งและเชื่อมโยงกันเพื่อการใช้งานบนระบบเครือข่ายอินทราเน็ตและอินเตอร์เน็ต จึงจำเป็นต้องมีโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ที่มีประสิทธิภาพและมีความเหมาะสมในการใช้งานเพื่อลดผลกระทบจากโปรแกรมไวรัสคอมพิวเตอร์และเพิ่มความปลอดภัยให้กับระบบสารสนเทศของกรมการแพทย์

2. <u>วัตถุประสงค์</u>

เพื่อให้กรมการแพทย์มีเครื่องมือในการป้องกันและกำจัดไวรัสคอมพิวเตอร์ที่มีประสิทธิภาพรวมทั้งมีความสามารถในการตรวจจับผู้บุกรุกและการป้องกันการโจมตีต่างๆ ให้กับเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่ายได้อย่างอัตโนมัติ โดยสามารถบริหารจัดการควบคุมตรวจสอบระบบจากส่วนกลางได้อย่างสะดวก รวดเร็ว และทันต่อเหตุการณ์

3. <u>ความต้องการจัดหา</u>

3.1 โปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายพร้อมสิทธิการใช้งานที่ถูกต้องตามกฎหมายจำนวน 20 ชุด พร้อมติดตั้งและการUpdate Software เป็นเวลาไม่น้อยกว่า1 ปี

3.2 โปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายพร้อมสิทธิการใช้งานที่ถูกต้องตามกฎหมายจำนวน 430 ชุด พร้อมติดตั้ง และการUpdate Software เป็นเวลาไม่น้อยกว่า1 ปี

3.3 โปรแกร มบริหารจัดการระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์จากส่วนกลาง 1 ชุด พร้อมติดตั้ง และการ Update Software เป็นเวลาไม่น้อยกว่า 1 ปี

4. <u>คุณสมบัติของผู้เสนอราคา</u>

4.1 ผู้เสนอราคาต้องเป็นนิติบุคคลที่จดทะเบียนในประเทศไทยและประกอบธุรกิจเกี่ยวกับการจำหน่ายอุปกรณ์คอมพิวเตอร์หรือพัฒนาระบบคอมพิวเตอร์ (แนบสำเนาเอกสารหลักฐานยื่นมาพร้อมการเสนอราคา)

4.2 บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญาต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับ รายจ่าย หรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ

4.3 บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญากับหน่วยงานของรัฐซึ่งได้ดำเนินการจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์ (e-Government Procurement : e-GP) ต้องลงทะเบียนในระบบอิเล็กทรอนิกส์ของกรมบัญชีกลางที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐ

4.4 คู่สัญญาต้องรับจ่ายเงินผ่านบัญชีเงินฝากกระแสรายวัน เว้นแต่การรับจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจรับจ่ายเป็นเงินสดก็ได้

4.5 ผู้เสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการ หรือห้ามติดต่อหรือห้ามเข้าเสนอราคากับทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคล หรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ

4.6 ผู้เสนอราคาต้องเป็นผู้ผลิต หรือเป็นตัวแทนจำหน่ายที่ได้รับการแต่งตั้งจากบริษัทผู้ผลิตโดยตรง หรือสาขาของบริษัทผู้ผลิตประจำประเทศไทย สำหรับโปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์ โดยแนบเอกสารหลักฐานการแต่งตั้งเป็นตัวแทนจำหน่ายซอฟต์แวร์ที่ออกให้สำหรับโครงการนี้

4.7 ผู้เสนอราคาต้องเคยมีผลงานในการติดตั้งหรือบำรุงรักษาระบบโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ให้กับส่วนราชการ หรือรัฐวิสาหกิจ หรือองค์กรที่รู้จักกันโดยทั่วไปมาแล้วภายในเวลา 3 ปี (แนบสำเนาหนังสือรับรองผลงานที่อ้างถึงมาด้วย โดยมีหัวหน้างานหรือผู้กระทำการแทนของหน่วยงานนั้นเป็นผู้ลงนามรับรอง)

4.8 ผู้เสนอราคาต้องสามารถจัดหาบุคลากรผู้เชี่ยวชาญซึ่งเป็นทีมปฏิบัติงานของผู้เสนอราคา ซึ่งอย่างน้อยต้องประกอบด้วย

4.8.1 ผู้จัดการโครงการ (Project Manager)

4.8.2 บุคลากรที่มีความรู้ประสบการณ์หรือเชี่ยวชาญด้านระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์(แนบเอกสารหลักฐานที่น่าเชื่อถือประกอบ)

5. คุณลักษณะเฉพาะ

5.1 คุณสมบัติของโปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์บนเครื่องลูกข่าย

5.1.1 เป็นโปรแกรมป้องกันไวรัสที่สนับสนุนการทำงานบนระบบปฏิบัติการดังต่อไปนี้ Microsoft Windows XP/Vista/7/8/8.1/10 ได้เป็นอย่างน้อย

5.1.2 สามารถป้องกัน Malware ต่างๆ ได้แบบ Proactive ซึ่งได้แก่ Viruses, Spyware, Trojans, Worms, Adware และ Root kits โดยใช้ ThreatSense Technology

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

5.1.4 ใช้วิธีการตรวจสอบ Malware โดยวิธีดังนี้

5.4.1.1 อาศัยการอ้างอิงจากฐานข้อมูลแบบ Definition หรือ Signatures

5.4.1.2 อาศัยการวิเคราะห์พฤติกรรมแบบ Heuristics และ Advanced Heuristics

5.1.5 สามารถตรวจจับ Potentially Unwanted Applications และ Potentially Unsafe Applications ได้

5.1.6 สามารถตรวจสอบภัยคุกคามจากทางอินเตอร์เน็ตและอีเมล์ผ่านทาง Protocol HTTP, HTTPS, POP3, POP3S, IMAP และ IMAPS

5.1.7 สามารถตรวจจับภัยคุกคามผ่าน Media ดังนี้ Local Drives, Removable Media, Networks Drives

5.1.8 สามารถตรวจสอบไฟล์ที่สร้างขึ้นใหม่จำพวกไฟล์บีบอัดได้ ซึ่งได้แก่ Self-extracting files และ Runtime packers

5.1.9 มีระบบปิดกั้นการโจมตีโดยใช้ช่องโหว่ของโปรแกรมประยุกต์ (Exploit Blocker)

5.1.10 มีระบบป้องกันบ็อตเน็ต (Botnet Protection)

5.1.11 สามารถป้องกัน Phishing ได้

5.1.12 มีระบบสแกนหน่วยความจำ เพื่อตรวจจับมัลแวร์ที่ใช้เทคนิคการโจมตีที่ซับซ้อน (Advanced Memory Scanner)

5.1.13 มีระบบป้องกันการโจมตีทางช่องโหว่ของระบบเครือข่าย (Vulnerabilities Shield)

5.1.14 มีโมดูล Personal Firewall สามารถตั้งค่าเข้มงวดหรือเปิดให้แชร์ไฟล์กับระบบเครือข่ายที่เชื่อมต่อใหม่

5.1.15 มีโมดูล Personal Firewall จะต้องมีระบบ IDS ภายในตัว ที่มีความสามารถในการป้องกันการโจมตีจากระบบเครือข่ายในแบบต่างๆ

5.1.16 มีโมดูลในการสแกนอีเมล์ไวรัสและอีเมล์ขยะที่สามารถรวมเข้ากับ Microsoft Outlook, Outlook Express และ Windows Mail ได้ที่ตัวเครื่องลูกข่ายโดยตรง

5.1.17 มีระบบ Host Intrusion Prevention System และระบบ Self-defense เพื่อป้องกันภัยคุกคามโจมตีระบบได้

5.1.18 มีโมดูล Document Protection เพื่อป้องกันไวรัสติดไฟล์เอกสาร Microsoft Office

5.1.19 มีเครื่องมือในการสร้างแผ่น Boot CD เพื่อสแกนและกำจัดไวรัสนอกระบบปฏิบัติการได้

5.1.20 สามารถทำ Web Filtering ได้โดยสามารถกำหนดประเภทของเว็บไซต์หรือ URL ที่ต้องการ Block ไม่ต้องการให้ผู้ใช้งานเข้าถึงได้ และสามารถ Exclude URL ที่ไม่ต้องการให้โปรแกรมป้องกันไวรัสสแกนได้

5.1.21 สามารถตั้งค่ารหัสผ่านในการล็อคการตั้งค่าโปรแกรมได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปลี่ยนแปลงการตั้งค่าโปรแกรม

5.1.22 สามารถอัพเดทฐานข้อมูลไวรัสและส่วนประกอบของโปรแกรมได้โดยอัตโนมัติ และสามารถตั้งค่าอัพเดทฐานข้อมูลไวรัสแบบ Pre-release เพื่อตรวจจับไวรัสได้เร็วยิ่งขึ้นได้

5.1.23 สามารถทำการสแกนไฟล์ที่กักไว้ในQuarantine หลังจากอัพเดท เพื่อตรวจสอบไฟล์ที่กักเก็บไว้อีกครั้ง

5.1.24 สามารถกำหนดการใช้งาน Removable Media ได้ โดยสามารถระบุ Device ID ของ Removable Media และทำการ Blocked, Read-only และ Read-write ได้

5.1.25 สามารถทำการ Rollback ฐานข้อมูลไวรัสได้ในกรณีที่เกิดปัญหาเกี่ยวกับฐานข้อมูลไวรัส

5.1.26 มีฟังก์ชั่นเพื่อปิดการทำงานของหน้าต่างป๊อบ-อัพ เมื่อใช้งานแอพพลิเคชั่นแบบเต็มจอ

5.1.27 มีเครื่องมือในการตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์ในโปรแกรมป้องกันไวรัสเอง เพื่อการวิเคราะห์ข้อมูลได้ (Diagnostic tool)

5.1.28 มีความสามารถในการตรวจสอบ Patch ของ Windows ที่ยังไม่ได้ติดตั้งอัพเดท และแจ้งเตือน Patch ที่ในโปรแกรมป้องกันไวรัสได้

5.1.29 โปรแกรมต้องสามารถสร้าง Application memory dump เพื่อใช้ในการตรวจสอบปัญหาได้

5.1.30 สามารถทำ Update Server เพื่อให้บริการการอัพเดทผ่าน HTTP/HTTPS และสามารถทำ Authentication เครื่องที่จะเข้ามาอัพเดทได้

5.1.31 มีระบบการติดตั้งใช้งานในระบบเครือข่าย และปรับปรุงข้อมูลไวรัสคอมพิวเตอร์ให้ทันสมัย ซึ่งสามารถทำงานได้ในลักษณะติดตั้งเครื่องแม่ข่ายส่วนกลางโดยสามารถกำหนดให้เครื่องแม่ข่ายหรือเครื่องลูกข่ายที่จะติดตั้ง หรือปรับปรุงข้อมูลขึ้นตรงกับเครื่องแม่ข่ายส่วนกลาง โดยมีคุณสมบัติด้านการติดตั้งใช้งานระบบเครือข่าย ดังนี้

5.1.31.1 สามารถทำงานได้เป็นอย่างดีบนระบบเครือข่ายโดยไม่กระทบต่อประสิทธิภาพของระบบเครือข่าย

5.1.31.2 สามารถติดตั้งชุดซอฟต์แวร์โดยการ Download, การติดตั้งผ่านสื่อต่างๆ เช่น Diskette CD-ROM, Flash Drive

5.1.31.3 สามารถปรับปรุงข้อมูลไวรัสคอมพิวเตอร์บนเครื่องแม่ข่าย และเครื่องลูกข่าย จากเครื่องแม่ข่ายส่วนกลางได้โดยรองรับทั้งแบบ Manual หรือ Automatic (ตั้งเวลา)

5.1.31.4 ในการปรับปรุงข้อมูลไวรัสคอมพิวเตอร์ต้องสามารถทำงานบนเครือข่ายของกรมการแพทย์ได้เป็นอย่างดี

5.1.31.5 เครื่องลูกข่ายสามารถปรับปรุงข้อมูลไวรัสคอมพิวเตอร์และซอฟต์แวร์จากเครื่องแม่ข่ายส่วนกลางได้โดยไม่ขัดแย้งกับ Configuration ของระบบเครือข่ายกรมการแพทย์ในปัจจุบัน

5.1.32 ผลิตภัณฑ์หรือผู้ผลิตชุดโปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์ต้องมีใบรับรองตามมาตรฐานจาก ICSA Labs, Virus Bulletin และ West Coast Labs

5.2 <u>คุณสมบัติของโปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์บนเครื่องแม่ข่ายสำหรับระบบปฏิบัติการ Microsoft Windows Server</u>

5.2.1 เป็นโปรแกรมป้องกันไวรัสที่สนับสนุนการทำงานบนระบบปฏิบัติการ Microsoft Windows Server /Server 2003/Server 2008/Server 2012 ได้เป็นอย่างน้อย

5.2.2 สามารถป้องกัน Malware ต่างๆ ได้แบบ Proactive ซึ่งได้แก่ Viruses, Spyware, Trojans, Worms, Adware และ Root kits โดยใช้ ThreatSense Technology

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

5.2.4 ใช้วิธีการตรวจสอบ Malware โดยวิธีดังนี้

5.2.4.1 ตรวจสอบโดยอาศัยการอ้างอิงจากฐานข้อมูลแบบ Definition หรือ Signatures

5.2.4.2 ตรวจสอบโดยอาศัยการวิเคราะห์พฤติกรรมแบบ Heuristics และ Advanced Heuristics

5.2.5 สามารถตรวจจับ Potentially Unwanted Applications และ Potentially Unsafe Applications ได้เป็นอย่างน้อย

5.2.6 สามารถตรวจจับภัยคุกคามผ่าน Local Drives, Removable Media, Networks Drivesได้เป็นอย่างน้อย

5.2.7 สามารถตรวจสอบไฟล์ที่สร้างขึ้นใหม่จำพวกไฟล์บีบอัดได้ ซึ่งได้แก่ Self-extracting files และ Runtime packers

5.2.8 มีระบบการป้องกันฟิชชิ่ง

5.2.9 มีโมดูล Document Protection เพื่อป้องกันไวรัสติดไฟล์เอกสาร Microsoft Office

5.2.10 สามารถตั้งค่า Exclude การสแกนของไฟล์ที่เกี่ยวข้องกับ Microsoft Windows Server ได้อัตโนมัติ

5.2.11 สามารถตั้งค่ารหัสผ่านในการล็อคการตั้งค่าโปรแกรมได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปลี่ยนแปลงการตั้งค่าโปรแกรม

5.2.12 สามารถอัพเดทฐานข้อมูลไวรัสและส่วนประกอบของโปรแกรมได้โดยอัตโนมัติ

5.2.13 สามารถทำการสแกนไฟล์ที่กักไว้ใน Quarantine หลังจากอัพเดท เพื่อตรวจสอบไฟล์ที่กักเก็บไว้อีกครั้ง

5.2.14 สามารถกำหนดการใช้งาน Removable Media ได้ เช่นการบล็อคการใช้งาน USB Flash Drive

5.2.15 มีเครื่องมือในการตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์ในโปรแกรมป้องกันไวรัสเอง เพื่อการวิเคราะห์ข้อมูลได้ (Diagnostic tool)

5.2.16 สามารถรองรับการใช้งานแบบ Clustering ได้

5.2.17 ผลิตภัณฑ์หรือผู้ผลิตชุดโปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์ต้องมีใบรับรองตามมาตรฐานจาก ICSA Labs, Virus Bulletin และ West Coast Labs

5.3 <u>คุณสมบัติของโปรแกรมบริหารจัดการระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์</u>

5.3.1 สามารถติดตั้งทำงานบนระบบปฏิบัติการดังต่อไปนี้ Microsoft Windows Server 2003/Server 2008/Server 2012 ได้เป็นอย่างน้อย

5.3.2 สามารถบริการจัดการได้ผ่านเว็บเบราว์เซอร์ (Web Console)

5.3.3 สามารถตรวจสอบ Inventory ของเครื่องลูกข่ายได้ดังนี้ Computer Name, IP Address, MAC Address, Operating System และ Hardware Platform

5.3.4 สามารถมอนิเตอร์ เพื่อดูแลการทำงานของเครื่องลูกข่ายแบบ Real Time ได้ดังนี้ เวอร์ชั่นของฐานข้อมูลไวรัส , ระยะเวลาที่เครื่องลูกข่ายเข้ามาเชื่อมต่อครั้งสุดท้าย , สถานะของ Protection status, ชื่อและเวอร์ชั่นของโปรแกรมป้องกันไวรัสที่ติดตั้งอยู่ที่เครื่องลูกข่าย

5. 3.5 สามารถเรียกดูและปรับแต่งการตั้งค่าโปรแกรมของเครื่องลูกข่ายได้

5.3.6 สามารถกำหนดนโยบายของเครื่องลูกข่ายตาม Group ได้

5.3.7 สามารถสั่งงานในการอัพเดทฐานข้อมูลไวรัสและสั่งงาน On-Demand Scan ไปยังเครื่องลูกข่ายได้

5.3.8 สามารถส่งข้อมูลไปเก็บไว้บนฐานข้อมูล MSSQL และ MYSQL ได้

5.3.9 สามารถกำหนดสิทธิ์ในการเข้าถึงได้หลายระดับ เช่น แบบผู้ดูแลระบบ และแบบอ่านได้อย่างเดียว

5.3.10 สามารถแจ้งเตือนเมื่อเกิดเหตุการณ์ต่างๆไปยังผู้ดูแลระบบได้ ผ่านทางอีเมล และ SNMP Trap

5.3.11 สามารถเชื่อมต่อกับ Active Directory โดยใช้โปรโตคอล LDAPได้

5.3.12 มี Dashboard เพื่อมอนิเตอร์สถานะต่างๆได้

5.3.13 สามารถทำการบริหารจัดการ Quarantine ของเครื่องลูกข่ายทั้งหมดได้

5.3.14 สามารถออกรายงานอันดับไวรัส หรือเครื่องที่ติดไวรัสมากที่สุด เป็นต้น ได้

5.3.15 สามารถตั้ง Schedule ในการออกรายงานและส่งอีเมล์ไปยังผู้ดูแลระบบได้

5.3.16 การจัดทำรายงานสามารถนำเอาข้อมูลออกมาได้ในรูปแบบของ CSV Format, PDF Format

5.3.17 สามารถตั้งค่า SMTP เพื่อใช้ในการส่งอีเมล์ไปยังผู้ดูแลระบบ

5.3.18 สามารถทำการติดตั้งและถอดถอนโปรแกรม Antivirus สำหรับเครื่องลูกข่ายแบบรีโมทจากศูนย์กลางได้

5.3.19 เครื่องมือบริหารจัดการสามารถสั่งงานเครื่องลูกข่ายให้รัน Command ตามพารามิเตอร์ที่กำหนดได้

5.3.20 เครื่องมือบริหารจัดการสามารถตรวจสอบ Application ที่ติดตั้งบนเครื่องลูกข่ายได้

5.3.21 สามารถกำหนดสิทธิ์ในการบริหารจัดการเครื่องลูกข่ายแต่ละ Group ได้

5.4 การจัดการฝึกอบรม ดังนี้

5.4.1 จัดฝึกอบรมการใช้โปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์บนเครื่องลูกข่ายเครื่องแม่ข่าย จำนวน 4 รุ่น รุ่นละไม่น้อยกว่า 50 คน

5.4.2 จัดฝึกอบรมการใช้ โปรแกรมบริหารจัดการระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์ 1 รุ่น ไม่น้อยกว่า 10 คน

5.4.3 ผู้เสนอราคาต้องรับผิดชอบค่าใช้จ่ายทั้งหมดที่เกิดขึ้นในการจัดฝึกอบรมตามข้อ 5.4.1 และ 5.4.2

6 <u>เงื่อนไขอื่นๆ</u>

6.1 ผู้เสนอราคาต้องสาธิตการติดตั้ง การปรับแต่ง โปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์ทั้งส่วน Client, Server และManagement Serverและโปรแกรมระบบตรวจสอบสิทธิการใช้งานระบบเครือข่ายคอมพิวเตอร์ พร้อมทั้งทดสอบการใช้งานเพื่อให้สามารถทำงานร่วมกันระบบงานคอมพิวเตอร์ของกรมการแพทย์ให้แล้วเสร็จภายในกำหนดเวลาส่งมอบ

6.2 ผู้เสนอราคาต้องให้การสนับสนุนแก่กรมการแพทย์ในการดูแลรักษาโปรแกรมตลอดระยะเวลาของสัญญา

6.3 หากเจ้าของผลิตภัณฑ์มีการปรบปรุง Version ของโปรแกรมภายในระยะเวลาของสัญญา ผู้เสนอราคาจะต้องปรับปรุง Version ของโปรแกรมดังกล่าวให้กรมการแพทย์ให้แล้วเสร็จทั้งหมดภายใน ๓๐ วันนับถัดจากวันที่ผลิตภัณฑ์ออกวางตลาด

7. <u>เงื่อนไขการชำระเงิน</u>

ชำระเงิน 100% ของมูลค่าสัญญา เมื่อได้มีการส่งมอบ และตรวจรับพัสดุเสร็จสิ้นแล้ว

8. <u>เงื่อนไขการให้บริการช่วงระยะเวลาการรับประกัน</u>

8.1 ผู้เสนอราคาต้องมีเจ้าหน้าที่ทางเทคนิคหรือผู้เชี่ยวชาญเฉพาะเพื่อให้คำปรึกษาตลอดระยะเวลาในสัญญา

8.2 ในกรณีที่มีความจำเป็นเร่งด่วน ผู้เสนอราคาจะต้องส่งเจ้าหน้าที่เข้ามาดำเนินการ ณ สถานที่ติดตั้ง

8.3 โปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์สำหรับเครื่องแม่ข่ายจำนวน 20 ชุด และโปรแกรมระบบป้องกันและกำจัดไวรัสคอมพิวเตอร์สำหรับเครื่องลูกข่ายจำนวน 430 ชุด พร้อมโปรแกรมบริหารจัดการจากส่วนกลาง ต้องสามารถ Upgrade ได้โดยไม่เสียค่าใช้จ่ายเพิ่มและไม่มีเงื่อนไข และรับประกันอย่างน้อย1 ปีนับถัดจากวันที่ส่งมอบงานเสร็จสิ้น แบบ On Site Service ภายใน 3 วัน

9. <u>ระยะเวลาที่ส่งมอบพัสดุและติดตั้ง</u>

ส่งมอบและติดตั้งครุภัณฑ์คอมพิวเตอร์ตามรายละเอียดของเอกสาร พร้อมลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย ให้แล้วเสร็จภายใน 30 วัน นับถัดจากวันที่ลงนามในสัญญา
