

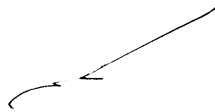


ประกาศ

ด้วยศูนย์สารสนเทศ กรมควบคุมโรค จะดำเนินการจัดซื้อโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ดังรายละเอียดคุณลักษณะตามที่แนบมานี้ จำนวน ๓ แผ่น

ในการนี้ ศูนย์สารสนเทศ จึงใคร่ขอเชิญสาธารณชนเสนอแนะ วิจารณ์ หรือมีความคิดเห็นเป็นลายลักษณ์อักษร โดยส่งถึงศูนย์สารสนเทศ กรมควบคุมโรค อาคาร ๒ ชั้น ๓ ตึกกรมควบคุมโรค ถนนติวานนท์ อำเภอเมือง จังหวัดนนทบุรี หรือทางอีเมล thaiddc.itc@ddc.mail.go.th โดยเปิดเผยตัวในวันที่ ๖ ตุลาคม ๒๕๕๗ เวลา ๑๖.๓๐ น. โทร ๐ ๒๕๕๐ ๓๐๙๓ โทรสาร ๐ ๒๕๖๕ ๙๕๗๖

ประกาศ ณ วันที่ ๓๐ กันยายน ๒๕๕๗



(นายสมศักดิ์ ไชยวัฒน์)

ผู้อำนวยการศูนย์สารสนเทศ

รายละเอียดคุณลักษณะเฉพาะของโปรแกรมป้องกันไวรัสคอมพิวเตอร์

ลิขสิทธิ์โปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ จำนวน 3,000 Licenses สำหรับกรมควบคุมโรค เป็นระยะเวลา ไม่น้อยกว่า 1 ปี นับถัดจากวันที่ส่งมอบ พร้อมคู่มือการติดตั้งใช้งาน และการฝึกอบรม รายละเอียดการทำงานของโปรแกรมดังนี้

ระบบป้องกัน Anti Virus มีคุณสมบัติทั่วไป ดังนี้

สามารถติดตั้งบน ระบบปฏิบัติการ Windows รุ่นต่างๆ ทั้งแบบ 32 และ 64 bits ได้

Server: Windows Server 2003, Windows Server 2008, Windows server 2008 R2

จำนวนอย่างน้อย 100 Licenses

Workstation: Windows XP, Windows Vista , Windows 7, Windows 8

จำนวนอย่างน้อย 3,000 Licenses

คุณสมบัติของโปรแกรมป้องกันไวรัส

1. เป็นโปรแกรมป้องกันไวรัสที่สนับสนุนการทำงานบนระบบปฏิบัติการดังต่อไปนี้ Microsoft Windows 2000/XP/Vista/7/8/Home Server/Server 2003 และ Server 2008
2. สามารถป้องกัน Malware ต่างๆ ได้แบบ Proactive ซึ่งได้แก่ Viruses, Spyware, Trojans, Worms, Adware และ Root kits โดยไม่ทำให้เครื่องคอมพิวเตอร์ช้าลง หรือก่อความรำคาญขณะใช้งานคอมพิวเตอร์
3. สามารถป้องกันและกำจัด Malware ต่างๆ ได้ทั้งแบบ Real-time file system protection และแบบ On-Demand Scanning
4. ใช้วิธีการตรวจสอบ Malware โดยวิธีดังนี้
 - 4.1 ตรวจสอบโดยอาศัยการอ้างอิงจากฐานข้อมูลแบบ Definition หรือ Signatures
 - 4.2 ตรวจสอบโดยอาศัยการวิเคราะห์พฤติกรรมแบบ Heuristics และ Advanced Heuristics
5. สามารถตรวจจับ Potentially Unwanted Applications และ Potentially Unsafe Applications ได้
6. สามารถตรวจสอบภัยคุกคามจากทางอินเทอร์เน็ตและอีเมลผ่านทาง Protocol HTTP, HTTPS, POP3, POP3S, IMAP และ IMAPS
7. สามารถตรวจจับภัยคุกคามผ่าน Media ดังนี้ Local Drives, Removable Media, Networks Drives
8. สามารถตรวจสอบไฟล์ที่สร้างขึ้นใหม่จำพวกไฟล์บีบอัดได้ ซึ่งได้แก่ Self extracting files และ Runtime packers
9. โมดูลในการสแกนอีเมลสามารถรวมเข้ากับ Microsoft Outlook, Outlook Express, Windows Mail Windows Live Mail และ Mozilla Thunderbird ได้ที่ตัวเครื่องถูกถ่ายโดยตรง
10. มีระบบ Host Intrusion Prevention System และระบบ Self-defense เพื่อป้องกันภัยคุกคามโจมตีระบบได้
11. มีโมดูล Document Protection เพื่อป้องกันไวรัสติดไฟล์เอกสาร Microsoft Office
12. โปรแกรมต้องสามารถสร้างแผ่น Boot CD เพื่อสแกนและกำจัดไวรัสบนระบบปฏิบัติการได้
13. สามารถใช้งานแบบ Non-Graphical mode ได้
14. มีเทคโนโลยีในการตรวจสอบ Process ที่รันอยู่ในระบบว่ามีความเสี่ยงในระบบการรักษาความปลอดภัยในระดับใด โดยตรวจสอบจากฐานข้อมูลของผู้ผลิตโปรแกรมป้องกันไวรัส (Cloud-based Technology)
15. สามารถทำ Web Filtering ได้โดยสามารถกำหนด HTTP URL ที่ต้องการ Block ที่ไม่ต้องการให้ผู้ใช้งานเข้าถึงได้ และสามารถ Exclude HTTP URL ที่ไม่ต้องการให้โปรแกรมป้องกันไวรัสสแกนได้
16. สามารถตั้งค่ารหัสผ่านในการถือการตั้งค่าโปรแกรมได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปลี่ยนแปลงการตั้งค่าโปรแกรม

17. สามารถอัปเดตฐานข้อมูลไวรัสและส่วนประกอบของโปรแกรมได้โดยอัตโนมัติ
18. สามารถทำการสแกนไฟล์ที่กักไว้ใน Quarantine หลังจากอัปเดต เพื่อตรวจสอบไฟล์ที่กักเก็บไว้อีกครั้ง
19. สามารถกำหนดการใช้งาน Removable Media ได้ โดยสามารถระบุ Device ID ของ Removable Media และทำการ Blocked, Read-only และ Read-write ได้
20. มีระบบ Gamer-mode เพื่อปิดการทำงานของหน้าต่างبوب-อัฟ เมื่อใช้งานแอปพลิเคชันแบบเต็มจอ
21. สามารถสร้างแผ่น Boot CD จากโปรแกรมป้องกันไวรัสเอง เพื่อสแกนและกำจัดไวรัสบนระบบปฏิบัติการได้
22. มีเครื่องมือในการตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์โน้ตบุ๊กโปรแกรมป้องกันไวรัสเอง เพื่อการวิเคราะห์ข้อมูลได้
23. สามารถทำงานร่วมกับ CISCO NAC และ Microsoft NAPได้
24. สามารถทำ Local Update Server เพื่อให้บริการการอัปเดตผ่าน HTTP/HTTPS และสามารถทำ Authentication เครื่องที่จะเข้ามาอัปเดตได้
25. โปรแกรม Management สามารถตรวจสอบ Inventory ของเครื่องลูกข่ายได้ดังนี้ Computer Name, IP Address, MAC Address, Operating System, Domain และ Hardware Platform
26. โปรแกรม Management สามารถมอนิเตอร์ เพื่อดูผลการทำงานของเครื่องลูกข่ายแบบ Real Time ได้ดังนี้ เวอร์ชันของฐานข้อมูลไวรัส, ระยะเวลาที่เครื่องลูกข่ายเข้ามาเชื่อมต่อครั้งสุดท้าย, รายชื่อไวรัสที่ตรวจพบล่าสุด, สถานะของ Protection status, ชื่อและเวอร์ชันของโปรแกรมป้องกันไวรัสที่ติดตั้งอยู่ที่เครื่องลูกข่าย
27. โปรแกรม Management สามารถเรียกดูและปรับแต่งการตั้งค่าโปรแกรมของเครื่องลูกข่ายได้
28. โปรแกรม Management สามารถกำหนดการตั้งค่าของเครื่องลูกข่ายตาม Group ได้
29. โปรแกรม Management สามารถสั่งงานในการอัปเดตฐานข้อมูลไวรัสและสั่งงาน On-Demand Scan ไปยังเครื่องลูกข่ายได้
30. โปรแกรม Management สามารถรองรับฐานข้อมูล MS Access, MSSQL, MYSQL และ Oracle ได้
31. โปรแกรม Management ต้องมีเครื่องมือที่สามารถสำรองฐานข้อมูล หรือโอนถ่ายฐานข้อมูลได้
32. โปรแกรม Management สามารถกำหนด Policy ให้สำหรับเครื่องลูกข่ายได้
33. โปรแกรม Management สามารถกำหนดสิทธิ์ในการเข้าถึงได้แบบผู้ดูแลระบบ และแบบอ่านได้อย่างเดียว
34. โปรแกรม Management สามารถแจ้งเตือนเมื่อเกิดเหตุการณ์ต่างๆไปยังผู้ดูแลระบบได้ ผ่านทางอีเมล และSNMP Trap
35. โปรแกรม Management สามารถเชื่อมต่อกับ Active Directory โดยใช้โปรโตคอล LDAP ได้
36. มี Real-time Dashboard เพื่อดูสถานะต่างๆได้
37. สามารถออกรายงานอันดับไวรัส หรือเครื่องที่ติดไวรัสมากที่สุด เป็นต้น ได้
38. สามารถตั้ง Schedule ในการออกรายงานและส่งอีเมลไปยังผู้ดูแลระบบได้
39. การจัดทำรายงานสามารถนำเอาข้อมูลออกมาได้ในรูปแบบของ HTML และ CSV
40. สามารถตั้งค่า SMTP ในโปรแกรม Management เพื่อใช้ในการส่งอีเมลไปยังผู้ดูแลระบบ
41. สามารถทำการติดตั้งและถอดถอนโปรแกรม antivirus สำหรับเครื่องลูกข่ายแบบรีโมทจากศูนย์กลางได้
42. สามารถจัดตั้งเครื่องแม่ข่าย Antivirus ได้หลายเครื่อง เพื่อทำการ Replicate ข้อมูลกันได้ระหว่างสาขาและสามารถควบคุมเครื่อง Antivirus ทั้งหมดได้จากศูนย์กลาง
43. สามารถทำการเชื่อมต่อระหว่างเครื่องแม่ข่ายและลูกข่ายได้โดยไม่จำเป็นต้องติดตั้ง Agent หรือ Service ที่ทำหน้าที่เชื่อมต่อใดๆ
44. การเชื่อมต่อระหว่าง Console กับ Server ของโปรแกรม Management มีการเข้ารหัสข้อมูลแบบ AES-256

เงื่อนไขอื่นๆ

1 หากมีการ Update Version หรือ Patch โปรแกรมจะต้องดำเนินการดังกล่าวให้กับกรมควบคุมโรค โดยไม่เสียค่าใช้จ่ายใดๆ ตลอดระยะเวลา 1 ปี

2 จะต้องจัดส่งเอกสารคู่มือการใช้งานโปรแกรมที่เป็นเอกสารกระดาษ และ Soft Copy อย่างน้อยจำนวน 1 ชุด ให้กับกรมควบคุมโรค

3 ผู้เสนอราคาต้องจัดหลักสูตรอบรมที่มีประสิทธิภาพโดยเนื้อหาของหลักสูตรจะต้องมีรายละเอียดเกี่ยวกับพื้นฐานของอุปกรณ์และทฤษฎีที่เกี่ยวข้อง และการติดตั้งระบบ ทั้งนี้การอบรมจะจัดให้กับเจ้าหน้าที่ของกรมควบคุมโรคหลังจากได้ทำการส่งมอบสินค้าเรียบร้อยแล้วโดยจัดอบรมในส่วนกลางให้ไม่เกิน 2 ครั้งตลอดระยะเวลาการรับประกัน 1 ปี โดยผู้เสนอราคาจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายในส่วนค่าวิทยากร ค่าอาหารตลอดการอบรม ยกเว้นค่าที่พัก และค่าเดินทางของผู้เข้าร่วมการอบรม


4 ผู้เสนอราคาต้องติดตั้งโปรแกรมสำหรับบริหารจัดการโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ให้กับกรมควบคุมโรค

5 ผู้เสนอราคาต้องติดตั้งโปรแกรมสำหรับป้องกันไวรัสคอมพิวเตอร์ให้ครบตามระยะเวลาและจำนวนเครื่องคอมพิวเตอร์ที่ทางศูนย์สารสนเทศกำหนด


6 ผู้เสนอราคาต้องให้บริการคำแนะนำและวิธีการแก้ไขปัญหาการใช้งานโปรแกรมป้องกันไวรัสคอมพิวเตอร์ รวมทั้งวิธีการกำจัด Malware และวิธีแก้ไขผลกระทบจากการติดหรือกำจัด Malware เมื่อผู้เสนอราคาได้รับแจ้งจากกรมควบคุมโรคในวัน และเวลาราชการทางโทรศัพท์ หรือทาง E-mail

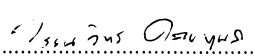
7 ผู้เสนอราคาจะต้องเป็นตัวแทนจำหน่ายของผลิตภัณฑ์ที่เสนอ และจะต้องได้รับการรับรองการให้การสนับสนุนการให้บริการหลังการขายในโครงการนี้จากทางเจ้าของผลิตภัณฑ์ หรือตัวแทนของเจ้าของผลิตภัณฑ์ในประเทศไทย โดยมีหนังสือที่ออกโดยเจ้าของผลิตภัณฑ์ หรือตัวแทนของเจ้าของผลิตภัณฑ์ในประเทศไทย นำมาแสดงประกอบการพิจารณา

8 ผู้เสนอราคาต้องมีประสบการณ์ในการติดตั้งหรือบำรุงรักษาระบบโปรแกรมป้องกันไวรัสให้กับทางราชการ/รัฐวิสาหกิจ/เอกชน สำเร็จมาแล้วไม่น้อยกว่า 1 โครงการ โดยโครงการดังกล่าวจะต้องมีจำนวนในการติดตั้งไม่น้อยกว่า 1,500 License และต้องเป็นหน่วยงานที่น่าเชื่อถือ สามารถตรวจสอบได้โดยมีเอกสารนำมาแสดง

(ลงชื่อ)..........ประธาน

(นายสมชาย เวียงพิทักษ์)
นักวิชาการสาธารณสุขชำนาญการ

(ลงชื่อ)..........กรรมการ
(นางสาวสุพจนา คุ่มวงษ์)
นักวิชาการคอมพิวเตอร์

(ลงชื่อ)..........กรรมการ
(นายวรรณวิทย์ คล้ายบุญส่ง)
นักวิชาการคอมพิวเตอร์