ประกาศ
สหกรณ์ออมทรัพย์กรมป่าไม้ จำกัด
เรื่อง เสนอราคาโปรแกรมป้องกันไวรัส

สหกรณ์ออมทรัพย์กรมป่าไม้ จำกัด มีความประสงค์จะซื้อโปรแกรมป้องกันไวรัส จำนวน 70 Licenses รายละเอียดคุณสมบัติให้เป็นไปตามรายละเอียดแนบท้ายประกาศนี้

<u>คุณสมบัติของผู้เสนอราคา</u>

1. เป็นผู้มีอาชีพขายพัสดุที่สอบราคาซื้อดังกล่าว
2. เป็นนิติบุคคลที่จดทะเบียนในราชอาณาจักรไทยและต้องมีสำเนาแสดงหลักฐานการเป็นนิติบุคคลจดทะเบียนในประเทศไทย และหนังสือแสดงหลักฐานผู้มีอำนาจลงนาม ส่งมาพร้อมซองเสนอราคา
3. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่นที่เข้าเสนอราคาให้แก่สหกรณ์ออมทรัพย์กรมป่าไม้ จำกัด ณ วันประกาศเสนอราคา หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการเสนอราคาครั้งนี้

<u>การยื่นซองเสนอราคา</u>

1. ให้ผู้ประสงค์เสนอราคายื่นซองเสนอราคาได้ระหว่างวันที่ 20 เมษายน – 13 พฤษภาคม 2564 ณ สำนักงานสหกรณ์ออมทรัพย์กรมป่าไม้ จำกัด
2. ในการยื่นซองเสนอราคาให้ผู้เสนอราคา จัดเตรียมซอง จำนวน 3 ซอง ดังนี้
   2.1 ซองเสนอราคาโปรแกรมป้องกันไวรัส <u>โดยให้ปิดผนึกซองพร้อมประทับตราผู้เสนอราคา</u>
   2.2 ซองรายละเอียดคุณลักษณะเฉพาะและประสิทธิภาพของโปรแกรมป้องกันไวรัส
   2.3 ซองสำเนาแสดงหลักฐานการเป็นนิติบุคคลจดทะเบียนในประเทศไทย และหนังสือแสดงหลักฐานผู้มีอำนาจลงนาม

สหกรณ์ออมทรัพย์กรมป่าไม้ จำกัด จะเปิดซองตามข้อ 2.2 และข้อ 2.3 เมื่อมีการยื่นเอกสารเพื่อพิจารณารายละเอียดคุณลักษณะเฉพาะ และหลักฐานเอกสารประกอบ

<u>การเปิดซองเสนอราคา</u>

สหกรณ์ออมทรัพย์กรมป่าไม้ จำกัด จะทำการเปิดซอง ณ สำนักงานสหกรณ์ออมทรัพย์กรมป่าไม้ จำกัด ในวันจันทร์ที่ 17 พฤษภาคม 2564 เวลา 09.30 น. เป็นต้นไป

ทั้งนี้ สหกรณ์ออมทรัพย์กรมป่าไม้ จำกัด ขอสงวนสิทธิ์ในการพิจารณา ดังนี้

1. สหกรณ์ออมทรัพย์กรมป่าไม้ จำกัด มีเอกสิทธิ์ในการพิจารณาคัดเลือกผู้เสนอราคารายใดก็ได้ หรืออาจยกเลิกการสอบราคาครั้งนี้ หากพิจารณาแล้วเห็นว่าข้อเสนอที่เสนอมานั้นยังไม่เหมาะสม
2. สหกรณ์ออมทรัพย์กรมป่าไม้ จำกัด อาจไม่พิจารณาคัดเลือกผู้เสนอราคาต่ำสุด

ผู้สนใจติดต่อสอบถามรายละเอียดเพิ่มเติมได้ที่ สำนักงานสหกรณ์ออมทรัพย์กรมป่าไม้ จำกัด เลขที่ 61 ถนนพหลโยธิน เขตจตุจักร กรุงเทพมหานคร (ภายในบริเวณกรมป่าไม้) โทรศัพท์ 0 2579 4899 ในวันและเวลาทำการ หรือดูรายละเอียดได้ที่ www.025798899.com

ประกาศ ณ วันที่ 20 เมษายน พ.ศ. 2564

(นายวิชิต สนธิวณิช)
ประธานกรรมการดำเนินการ
สหกรณ์ออมทรัพย์กรมป่าไม้ จำกัด

รายละเอียดแนบท้ายประกาศ

โปรแกรมป้องกันไวรัส จำนวน 70 Licenses โดยมีคุณลักษณะเฉพาะและมีประสิทธิภาพไม่น้อยกว่ารายการดังต่อไปนี้

คุณสมบัติสำหรับโปรแกรมบริหารจัดการกลาง

1. โปรแกรมบริหารจัดการต้องรองรับการใช้งานกับ Database Microsoft SQL Server 2014 Express SP2 (64bit) หรือดีกว่า และรองรับการใช้งาน MySQL Standard Edition 5.7 32-bit/64-bit หรือดีกว่า
2. โปรแกรมบริหารจัดการกลางต้องรองรับการใช้งานกับ Microsoft Windows 8, 8.1 windows 10, windows server 2012, 2012 r2, windows server 2016(64bit) All edition, windows server 2019 (64bit) All edition
3. โปรแกรมการบริหารจัดการต้องสามารถทำได้ทั้งรูปแบบของ On-Cloud และ On-Premise และทั้งสองอย่างต้องสามารถเชื่อมต่อถึงกันในรูปแบบ (Master-Slave)
4. สามารถจัดตั้งเครื่องควบคุมส่วนกลางได้หลายเครื่องเพื่อส่งข้อมูลและสั่งงานกันได้ระหว่างเครื่องจัดการและบริหารโปรแกรมป้องกันไวรัสจากศูนย์กลางกันเองและเครื่องลูกข่าย
5. สามารถตั้งค่าตัวบริหารจัดการแบบจำลอง (Virtual administration server) ภายในตัวบริหารจัดการหลักได้
6. สามารถกำหนดสิทธิ์ให้กับผู้ดูแลระบบในการใช้งานตัวบริหารจัดการที่แตกต่างกัน
7. มีโปรแกรมที่ใช้เข้าถึงตัวบริหารจัดการแบบ On-Premise โดยไม่จำเป็นต้องผ่านการใช้ Remote-Desktop เช่น administration console, Web console
8. สามารถแสดงรายงานของไฟล์ที่ถูกสำรองข้อมูลไว้หากถูกลบไป (backup) หรือ โดนกักกัน (quarantine) ไว้ได้จากส่วนกลาง หรือ สามารถสั่งคืนค่าไฟล์ดังกล่าวได้จากส่วนกลาง
9. สามารถทำการกู้คืนและสำรองฐานข้อมูลของเครื่องแม่ข่ายเพื่อป้องกันในกรณีระบบเกิดการเสียหาย (Backup copying and restoration)
10. โปรแกรมการบริหารจัดการ On-Cloud ต้องสามารถกำหนดการเข้าได้ในรูปแบบการทำ (Two-step verification) ได้
11. โปรแกรมบริหารจัดการต้องสามารถควบคุมบริหารจัดการแอนตี้ไวรัสได้ดังต่อไปนี้ในโปรแกรมบริหารจัดการเดียว เช่น Virtual, Windows, Linux Mac OS, Mobile devices, Embedded Systems
12. สามารถทำการ Update โดยกำหนดให้เครื่องลูกอื่น ๆ เป็นแหล่งของการเข้ามา update ได้ (Agent Distribution points)
13. สามารถทำการเก็บรายละเอียด (Inventory) ของ Software และ Hardware ทั้งเครื่องแม่ข่ายและเครื่องลูกข่ายได้
14. โปรแกรมบริหารจัดการสามารถออก Report ในรูปแบบ PDF, Microsoft Excel, HTML
15. สามารถกำหนด User name, Password เพื่อสามารถแก้ไขหรือ Uninstall โปรแกรมได้จากโปรแกรมบริหารจัดการ Anti – Virus ได้
16. สามารถกำหนดการยกเว้นการ Scan โดยระบุเป็นนามสกุลไฟล์ได้สามารถทำการสั่ง Scan โดย On-Demand ได้ (Trusted Zone)
17. มีฟีเจอร์การสั่งลบไฟล์ที่เครื่องลูกข่ายโดยสั่งผ่านตัวบริหารจัดการกลาง (Wipe data) โดยต้องสามารถระบุเป็น Folders ,Predefined folders , File by extension
18. มีเทคโนโลยีตรวจสอบช่องโหว่ (Vulnerabilities) ของ Software ภายในเครื่องแม่ข่ายและเครื่องลูกข่าย

คุณสมบัติสำหรับโปรแกรมป้องกันไวรัสเครื่องแม่ข่าย

19. โปรแกรมป้องกันไวรัสสำหรับเครื่องแม่ข่าย สามารถติดตั้งในระบบปฏิบัติการ Windows Server 2008 64 Bit SP2, 2008 R2 SP1 64 Bit, 2012 (64 Bit), 2012 R2 Standard (64Bit), 2016 (64 Bit), 2019 (64Bit)

20. สามารถป้องกันเครื่องที่ติด Ransomware ทำการเข้ารหัสบน Share Folders, Map drive ได้และกำหนดเวลาในการเข้าใช้งาน Share Folders หลังจากทาการป้องกันแล้ว (Anti-Cryptor)

21. มีฟีเจอร์คุณสมบัติป้องกันดังนี้ Exploit Prevention, Behavior Detection,

22. มีฟีเจอร์กันป้องกันการโจมตีทางระบบเน็ตเวิกค์ (Network-Attack) โดยจะต้องสามารถออกรายงานเกี่ยวกับการโจมตีทางระบบเน็ตเวิกค์และสามารถทำการ (Block) การถูกโจมตีได้โดยอัตโนมัติ

23. สแกนไฟล์ในรูปแบบ Compound files, Installation packages และ OLE objects ได้

24. สามารถทำการเก็บรายละเอียด (Inventory) ของ Software และ Hardware เครื่องแม่ข่ายได้

25. สามารถป้องกันแอนตี้ไวรัสในตัวเองได้ (self – Defense) จากโปรแกรมที่เป็นอันตรายรวมถึงมัลแวร์ที่พยายามบล็อกการทำงาน หรือ แม้กระทั่งลบออกจากคอมพิวเตอร์

26. สามารถทำการ scan โดยไม่ไป scan หรือตรวจสอบไฟล์เดิมซ้ำที่ใช้เทคโนโลยี iSwift และ iChecker เพื่อเก็บค่าการสแกนของไฟล์ต่างๆ เป็นการลดเวลาในการตรวจสอบไฟล์

27. สามารถทำงานแบบ Personal firewall ได้

28. สามารถกำหนดและควบคุมการใช้งานของโปรแกรมบนเครื่องแม่ข่ายได้โดยใช้ฟังก์ชั่น Applications Launch Control

29. สามารถกำหนดค่าเพื่อป้องกันการใช้งานอุปกรณ์ที่มาเชื่อมต่อกับเครื่องข่ายได้โดยฟังก์ชั่น Device Control ได้

คุณสมบัติสำหรับโปรแกรมป้องกันไวรัสเครื่องลูกข่าย

30. สามารถติดตั้งโปรแกรมบริหารจัดการได้ในเครื่อง Windows 10, 8.1, 8, 7sp1, Windows Server 2008 R2 SP1(64 Bit), 2012 R2 (64Bit), 2016(64Bit), 2019(64Bit)

31. สามารถกำหนด อนุญาต/ไม่อนุญาต/แจ้งเตือน การเข้าใช้งาน website ของ user แต่ละคนได้

32. สามารถเลือกการใช้งานของโปรแกรม (Application Control) โดยเลือกเป็น Black List, White list ของ Application ได้

33. สามารถป้องกันเครื่องที่ติด Ransomware ทำการเข้ารหัสบน Share Folders, Map drive ได้และกำหนดเวลาในการเข้าใช้งาน Share Folders หลังจากทำการป้องกันแล้ว (Protection of share folders against external encryption)

34. มีฟังก์ชั่น AMSI Protection Providerที่ทาการ ตรวจจับ script malware ที่มากับMS office file, Archives, Distribution packages

35. มีฟังก์ชั่น Anti-Bridging เพื่อกำหนดการเชื่อมต่อเครือข่าย เช่น LAN, Wi-Fi ให้ใช้ช่องทางการเชื่อมต่อได้เพียงอย่างเดียว โดยไม่จำเป็นต้อง block ประเภทของอุปกรณ์แทน

36. สามารถอนุญาต/ไม่อนุญาต การใช้งานอุปกรณ์พกพาจำพวก Removable Drive, CD/DVD drives, Smart card readers, External network adapters, Portable devices, Cameras and และสามารถทำการเก็บข้อมูลการใช้งานไฟล์ เช่น ลบไฟล์, สร้างไฟล์ใหม่ บนอุปกรณ์ Removable Drive และออกรายงาน (Report) ได้

37. มีฟีเจอร์คุณสมบัติป้องกันดังนี้ Exploit Prevention, Behavior Detection, Ransomware, PowerShell & script-based attacks

38. มีฟีเจอร์ป้องกันการโจมตีทางระบบเน็ตเวิกค์ (Network-Attack) โดยจะต้องสามารถออกรายงานเกี่ยวกับการโจมตีทางระบบเน็ตเวิกค์และสามารถทาการ (Block) การถูกโจมตีได้โดยอัตโนมัติ

39. มีฟังก์ชั่นการป้องกันการถูกปลอมแมคแอดเดรส (MAC spoofing protection) ซ้ำเข้ามาในระบบ

40. สแกนไฟล์ในรูปแบบ Compound files, Installation packages และ OLE objects ได้

41. สามารถป้องกันแอนตี้ไวรัสในตัวเองได้ (self – Defense) จากโปรแกรมที่เป็นอันตรายรวมถึงมัลแวร์ที่พยายามบล็อกการทางาน หรือ แม้กระทั่งลบออกจากคอมพิวเตอร์

42. สามารถทำการ scan โดยไม่ไป scan หรือตรวจสอบไฟล์เดิมซ้ำที่ใช้เทคโนโลยี iSwift และ iChecker เพื่อเก็บค่าการสแกนของไฟล์ต่างๆ เป็นการลดเวลาในการตรวจสอบไฟล์

43. สามารถทำงานแบบ Personal firewall

44. มีเทคโนโลยีตรวจสอบช่องโหว่ (Vulnerabilities) ของ Software ภายในเครื่องแม่ข่ายและเครื่องลูกข่ายได้ทั้งหมดจากโปรแกรมบริหารจัดการ

45. รวบรวมข้อมูลเกี่ยวกับกิจกรรมที่น่าสงสัยโดยมัลแวร์เพื่อคืนค่าในระบบปฏิบัติการ (Remediation Engine) หรือ สามารถย้อนคืนค่าการทำงานใน Operation System กรณี Malware สร้างความเสียหายใน Operation System (Roll back action)

ผู้เสนอราคาจะต้องทำการติดตั้งโปรแกรมให้พร้อมใช้งานได้