

รายละเอียดคุณลักษณะเฉพาะ
ระบบบริหารจัดการไวรัสคอมพิวเตอร์ ชนิดควบคุมจากส่วนกลาง
แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพมหานคร 1 ระบบ

1. ความเป็นมา

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมส่งเสริมอุตสาหกรรม มีบทบาทภารกิจในการดูแลและให้บริการระบบคอมพิวเตอร์และเครือข่ายแก่เจ้าหน้าที่กรมส่งเสริมอุตสาหกรรม ทำให้ต้องมีการบริหารจัดการคอมพิวเตอร์และเครือข่ายให้พร้อมใช้งานและมีความปลอดภัยอยู่เสมอโดยมีภาระงานที่เกี่ยวข้องกับการจัดการระบบคอมพิวเตอร์ที่หลากหลาย เช่น การแก้ปัญหาการใช้งานระบบคอมพิวเตอร์ให้กับผู้ใช้ การตรวจสอบและบันทึกการรายการอุปกรณ์และซอฟต์แวร์ภายในเครื่องคอมพิวเตอร์ทั้งหมดเพื่อป้องกันไวรัสแปลกปลอมเข้ามาต่อเชื่อมติดตั้งในเครื่องคอมพิวเตอร์ขององค์กร ซึ่งเสี่ยงต่อการแก้ปัญหาการใช้งานระบบให้กับผู้ใช้และก่อให้เกิดความเสียหายต่าง ๆ กับเครื่องคอมพิวเตอร์ อีกทั้งสามารถแพร่กระจายตัวเองจากไฟล์หนึ่งไปยังไฟล์อื่น ๆ ภายในเครื่องคอมพิวเตอร์ แต่ไม่สามารถแพร่กระจายข้ามเครื่องคอมพิวเตอร์ได้ด้วยตัวเอง อย่างไรก็ตามเมื่อเวลาผ่านไปไวรัสได้รับการพัฒนา รูปแบบ เทคนิคแพร่กระจาย ความสามารถ รวมถึงความรุนแรงในการก่อความเสียหายให้ระบบคอมพิวเตอร์ที่แตกต่างไปจากเดิมมาก ซึ่งปัจจุบันคำว่า “ไวรัสคอมพิวเตอร์” มีการบัญญัติคำศัพท์ใหม่ว่า “มัลแวร์ (Malware)” จึงจำเป็นต้องพัฒนาโครงสร้างด้านระบบเครือข่ายของกรมส่งเสริมอุตสาหกรรมให้มีความทันสมัย มีประสิทธิภาพ และเพิ่มระดับการรักษาความปลอดภัยของระบบเครือข่ายและข้อมูลสารสนเทศของกรมส่งเสริมอุตสาหกรรมให้มีมาตรฐานด้านความปลอดภัย

2. วัตถุประสงค์

2.1 เพื่อเพิ่มประสิทธิภาพของระบบโครงสร้างพื้นฐานด้านระบบเครือข่ายและคอมพิวเตอร์ลูกข่ายของกรมส่งเสริมอุตสาหกรรม

2.2 เพื่อป้องกันระบบเครือข่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ลูกข่ายของกรมส่งเสริมอุตสาหกรรมจากไวรัสคอมพิวเตอร์

3. สถานที่ส่งมอบ

กรมส่งเสริมอุตสาหกรรม ถนนพระรามที่ 6 กรุงเทพฯ

4. ระยะเวลาดำเนินการ

ภายใน 60 วัน นับถัดจากวันลงนามในสัญญา

5. รายละเอียดคุณลักษณะเฉพาะของพัสดุ

ระบบบริหารจัดการไวรัสคอมพิวเตอร์ ชนิดควบคุมจากส่วนกลาง 1 ระบบ มีคุณลักษณะอย่างน้อยดังนี้

5.1 ระบบบริหารจัดการจากส่วนกลางของโปรแกรมป้องกันไวรัส มีคุณลักษณะอย่างน้อยดังนี้

5.1.1 ผลิตภัณฑ์ป้องกันไวรัสต้องสามารถควบคุมและบริหารจัดการจากส่วนกลางซึ่งเป็นการทำงานภายใต้สถาปัตยกรรมแบบ Cloud Console และ บริหารจัดการผ่าน Web Management ได้

Handwritten signature and initials

- 5.1.2 มีระบบบริหารจัดการจากส่วนกลางสามารถควบคุมเครื่องลูกข่ายที่เป็นแบบ Physical , Laptop, Server, Virtualization และสามารถที่จะบริหารจัดการภายใต้ Management เดียวกันได้ แบบ Single Agent และ Single Console
- 5.1.3 ระบบจะต้องสามารถสร้างผู้ดูแลระบบได้มากกว่า 1 ชื่อบัญชีและมีประวัติการเข้าใช้งานของแต่ละชื่อบัญชี และสามารถกำหนดสิทธิ์ได้ว่าผู้ดูแลระบบสามารถบริหารจัดการเฉพาะกลุ่มที่ให้สิทธิ์ได้
- 5.1.4 ระบบจะต้องสามารถแจ้งเตือนไปยังผู้ดูแลระบบโดยผ่านช่องทางอีเมล มากกว่า 1 อีเมลตามข้อมูลดังต่อไปนี้ได้เป็นอย่างดี
- (1) Malware outbreak
 - (2) Update Available
 - (3) License Expires
 - (4) Antiphishing event
 - (5) Outdated Update Server
- 5.1.5 บริหารจัดการได้ผ่านทางเว็บเบราว์เซอร์ในรูปแบบ HTTPS โพรโทคอล รองรับการทำงานกับ Browser ดังต่อไปนี้ Internet Explorer, Mozilla Firefox, Google Chrome, Safari
- 5.1.6 สามารถทำการ Submission File แบบ Manual ไปยัง Cloud Sandbox เพื่อทำการตรวจสอบว่าเป็น Malware หรือไม่
- 5.1.7 สามารถออกรายงานเกี่ยวกับ Sandbox Analyzer ได้
- 5.1.8 ระบบต้องสามารถส่งรูปแบบรายงานได้โดยอัตโนมัติตามช่วงเวลาที่กำหนดได้ และรายงานดังกล่าวจะต้องส่งมาในรูปแบบของการบีบอัดแบบ zip ไฟล์ซึ่งมีไฟล์ PDF และ CSV ถูกบีบอัดอยู่ใน Zip ได้
- 5.2 ระบบป้องกันไวรัสสำหรับเครื่องลูกข่าย จำนวน 1,500 สิทธิ์ มีคุณลักษณะอย่างน้อยดังนี้
- 5.2.1 เป็นโปรแกรมป้องกันไวรัสที่สนับสนุนการทำงานบนระบบปฏิบัติการดังต่อไปนี้ Microsoft Windows 10, Windows 8.1, Windows 8, Windows 7 ได้เป็นอย่างดี
- 5.2.2 รองรับการติดตั้งโปรแกรมผ่านโปรแกรมบริหารจัดการจากส่วนกลาง (Network Discovery) หรือแบบส่งเป็น e-mail หรือ ติดตั้งเอง โดยใช้ไฟล์ติดตั้งด้วยไฟล์เดียวได้
- 5.2.3 สามารถทำการตรวจจับ Malware ประเภทดังต่อไปนี้ได้ ไวรัส, โทรจัน, Worm, Rootkit, Phishing, Adware และ Keylogger เป็นอย่างน้อย
- 5.2.4 มีฟังก์ชันในการเฝ้าระวังการทำงานของ Ransomware เพื่อป้องกันไม่ให้สร้างความเสียหายกับเครื่องได้ (Ransomware Vaccine)
- 5.2.5 สามารถกำหนดนโยบายการรักษาความปลอดภัย เพื่อนำไปใช้โดยผู้ใช้อย่างไม่สามารถยกเลิกหรือแก้ไขนโยบายได้เอง
- 5.2.6 สามารถสั่งสแกน/อัปเดตทันทีหรือกำหนดช่วงเวลาการ สแกน/อัปเดต ได้จาก Management Console พร้อมทั้งสามารถสั่งปิดเครื่องหลังจากการ สแกนได้
- 5.2.7 ผู้ดูแลระบบ สามารถเลือกที่จะทำการลบไฟล์ (Delete) ที่ต้องสงสัยว่าเป็นไวรัส หรือ

สามารถกักกันไฟล์ (Quarantine) ที่ต้องสงสัยได้

- 5.2.8 ต้องสามารถกำหนดพาสเวิร์ดในการป้องกันการถอนการติดตั้งโปรแกรมได้
- 5.2.9 สามารถอัปเดตฐานข้อมูลแอนตี้ไวรัส ผ่านทาง Web Management Console ได้หรืออัปเดตผ่านทางเครื่องที่อยู่ในระบบเครือข่ายเดียวกันได้ โดยสามารถเลือกกำหนดได้เพียงช่องทางเดียวหรือได้ทั้งสองช่องทาง
- 5.2.10 สามารถกำหนดให้เครื่องลูกข่ายทำหน้าที่รับข้อมูลการอัปเดตจากทาง Management Console และเครื่องดังกล่าวสามารถกระจายข้อมูลการ Update ต่อไปยังเครื่องลูกข่ายอื่น ๆ ได้
- 5.2.11 เมื่อตรวจพบเจอไวรัสสามารถทำการแจ้งเตือนไปยังผู้ดูแลระบบผ่านทางอีเมลได้ โดยอัตโนมัติ โดยสามารถกำหนดให้ส่งได้มากกว่า 1 อีเมล
- 5.2.12 สามารถทำการคืนไฟล์ (Restore) ไฟล์ที่ถูกกักกัน (Quarantine) กลับไปยังตำแหน่งเดิมได้โดยผ่านทาง Management Console หรือผ่านทางเครื่องลูกข่าย หรือกำหนดโพลเดอร์ปลายทางที่ต้องการใหม่ได้
- 5.2.13 สามารถบล็อกเว็บหลอกลวงหรือเว็บที่อาจเป็นอันตรายได้ (Anti-Phishing)
- 5.2.14 มีไฟล์วอลล์ที่สามารถป้องกันภัยคุกคามที่เข้ามาโจมตี ทั้งขาเข้าและขาออก ได้ พร้อมทั้งแจ้งเตือนหากมีโปรแกรมหรือโปรเซสใดพยายามจะเชื่อมต่อมาใช้งานกับ Port ภายในเครื่องได้
- 5.2.15 สามารถตั้งค่าให้เครื่องคอมพิวเตอร์ มีการเปลี่ยนใช้ policy อันโดยอัตโนมัติตามเงื่อนไขที่กำหนดไว้ได้อย่างน้อยดังต่อไปนี้
 - (1) IP address ของเครื่องลูกข่ายมีการเปลี่ยนแปลง
 - (2) Gateway address ของเครื่องลูกข่ายมีการเปลี่ยนแปลง
 - (3) DNS server ของเครื่องลูกข่ายมีการเปลี่ยนแปลง
 - (4) รูปแบบการเชื่อมต่อระบบเครือข่ายมีการเปลี่ยนแปลง เช่น เปลี่ยนจาก LAN ไปใช้งาน Wireless LAN เป็นต้น
- 5.2.16 สามารถตรวจจับแอนตี้ไวรัสที่ใช้งานอยู่ก่อนการติดตั้งใหม่ ได้ไม่น้อยกว่า 10 ชนิดเพื่อการถอดถอนแอนตี้ไวรัส ก่อนการติดตั้ง
- 5.2.17 สามารถทำการสแกนอุปกรณ์ต่อพ่วง (Removable device) และ Network drive ได้
- 5.2.18 มีเทคโนโลยีการสแกนอย่างน้อยดังต่อไปนี้
 - (1) Local scan: การสแกนโดยใช้ทรัพยากรที่มีอยู่ในเครื่องคอมพิวเตอร์เท่านั้น
 - (2) Hybrid scan: การสแกนโดยอาศัยทรัพยากรเพียงส่วนหนึ่งในเครื่องและใช้ Cloud security ในการช่วยสแกน
 - (3) Central scan: การสแกนโดยทำการส่งไฟล์ต้องสงสัยไปสแกนยังระบบส่วนกลางของทางระบบป้องกันไวรัสที่ได้ติดตั้งอยู่ในระบบ
- 5.2.19 มีเทคโนโลยีตรวจสอบไฟล์เพื่อไม่ทำการสแกนซ้ำไฟล์เดิม แต่จะทำการสแกนไฟล์ที่เป็นไฟล์ใหม่และไฟล์ที่มีการอัปเดตหรือไฟล์ติดไวรัส
- 5.2.20 สามารถ อนุญาตให้ใช้งานหรือไม่ให้ใช้งานอุปกรณ์ต่อพ่วงจำพวก External storage,

Internal storage, Bluetooth, Network adaptor, Imaging device ได้

5.2.21 มีเทคโนโลยีการป้องกันการโจมตีประเภท Fileless attacks และ Script-based attacks

5.2.22 มีเทคโนโลยี Hyper detect สำหรับการตรวจสอบไฟล์ ก่อนทำการ Run File (PreExecution Stage) ได้ดังนี้

- (1) Targeted Attack
- (2) Suspicious files and network traffic
- (3) Exploits
- (4) Ransomware
- (5) Grayware

5.2.23 มีเทคโนโลยี Sandbox Analyzer สำหรับการตรวจสอบวิเคราะห์พฤติกรรมของไฟล์ ที่ต้องสงสัยแบบอัตโนมัติ และแบบส่งไฟล์ไปวิเคราะห์บน Cloud ได้ด้วยตนเอง

5.2.24 ผู้ยื่นข้อเสนอต้องมีหนังสือสนับสนุนทางด้านเทคนิคและการให้บริการจากบริษัท เจ้าของผลิตภัณฑ์หรือบริษัทสาขาเจ้าของผลิตภัณฑ์ในประเทศไทยโดยตรงในการ เสนอครั้งนี้เพื่อรับรองว่าผู้เสนอราคาสามารถให้คำปรึกษาทางด้านเทคนิครวมถึงการ ติดตั้งให้เป็นไปตามวัตถุประสงค์ของโครงการและการให้บริการอย่างมีประสิทธิภาพ ตลอดระยะเวลารับประกัน

6. คุณสมบัติของผู้เสนอราคา

6.1 มีความสามารถตามกฎหมาย

6.2 ไม่เป็นบุคคลล้มละลาย

6.3 ไม่อยู่ระหว่างเลิกกิจการ

6.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการ กระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

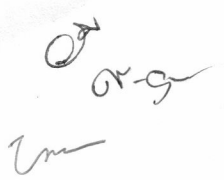
6.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงาน ของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

6.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่ คณะกรรมการนโยบายการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

6.7 เป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

6.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ กรมส่งเสริมอุตสาหกรรม วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการ ประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

6.9 ไม่เป็นผู้ได้รับเอกสิทธิ์ หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาล ของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น



6.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e - GP) ของกรมบัญชีกลาง

6.11 ผู้เสนอราคาต้องมีผลงานและประสบการณ์ในการจำหน่ายหรือในงานลักษณะเดียวกันกับงานที่จัดซื้อครั้งนี้ให้กับหน่วยงานราชการหรือรัฐวิสาหกิจ พร้อมแนบเอกสารประกอบ

7. วงเงินในการจัดหา

จำนวน 1,050,000 บาท (หนึ่งล้านห้าหมื่นบาทถ้วน)

8. หลักเกณฑ์และสิทธิในการพิจารณาเสนอราคา

8.1 ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ กรมจะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา

8.2 ในกรณีที่ไม่สามารถคัดเลือกผู้ดำเนินการที่มีคุณสมบัติและราคาที่เหมาะสมได้ กรมส่งเสริมอุตสาหกรรม ขอสงวนสิทธิ์ที่จะยกเลิกการประกวดราคา ทั้งนี้ ผู้เสนอราคาจะเรียกร้องค่าใช้จ่ายใด ๆ ทั้งสิ้น ไม่ได้

8.3 ในกรณีที่ผู้ผ่านเกณฑ์เพียงรายเดียวให้อยู่ในดุลยพินิจของคณะกรรมการพิจารณาผลการประกวดราคาฯ ที่จะพิจารณาแล้วเห็นว่ามีความเหมาะสมและเป็นประโยชน์สูงสุดต่อราชการ โดยไม่จำเป็นต้องเป็นผู้เสนอราคาต่ำสุด แต่ทั้งนี้จะต้องอยู่ในวงเงินงบประมาณที่ได้รับจัดสรร

8.4 คณะกรรมการ ฯ หรือ กรม มีสิทธิสอบถามข้อเท็จจริงเพิ่มเติมจากผู้เสนอราคารายใดก็ได้

9. ระยะเวลาส่งมอบและการจ่ายเงิน

การชำระเงิน กำหนดการจ่ายเงินเป็นจำนวน 1 งวด เมื่อผู้ขาย ได้ดำเนินการส่งมอบให้แล้วเสร็จภายใน 60 วัน นับถัดจากวันลงนามในสัญญา

10. ค่าปรับ

ผู้ขายจะต้องชำระค่าปรับให้ผู้ซื้อเป็นรายวันในอัตราร้อยละ 0.2 ของราคาส่งของที่ยังไม่ได้รับมอบ นับถัดจากวันครบกำหนดตามสัญญาจนถึงวันที่ผู้ขายได้นำสิ่งของมาส่งมอบให้แก่ผู้ซื้อจนถูกต้องครบถ้วนตามสัญญา

11. การรับประกันความชำรุดบกพร่อง

ผู้ขายตกลงรับประกันความชำรุดบกพร่องหรือข้อบกพร่องของคอมพิวเตอร์และการติดตั้ง ตามสัญญานี้ โดยครุภัณฑ์ตามข้อที่ 5 รับประกันเป็นเวลา 1 ปี นับถัดจากวันที่ผู้ซื้อได้รับมอบสิ่งของโดยถูกต้องครบถ้วนตามสัญญา โดยภายในกำหนดเวลาดังกล่าว หากสิ่งของ ตามสัญญานี้เกิดชำรุดบกพร่องหรือข้อบกพร่องอันเนื่องมาจากการใช้งาน ตามปกติผู้ขายจะต้องจัดการซ่อมแซมหรือแก้ไขให้อยู่ในสภาพที่ใช้การได้ดีดังเดิม ภายใน 2 วัน นับถัดจากวันที่ได้รับแจ้งจากผู้ซื้อ

Handwritten signature and initials at the bottom right of the page.

12. การสงวนสิทธิ์

12.1 การจัดซื้อครั้งนี้จะมีการลงนามในสัญญาหรือข้อตกลงเป็นหนังสือได้ต่อเมื่อพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ.2564 มีผลใช้บังคับ และได้รับจัดสรรงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ.2564 จากสำนักงบประมาณแล้ว และกรณีที่กรมส่งเสริมอุตสาหกรรมไม่ได้รับการจัดสรรงบประมาณเพื่อการจัดซื้อในครั้งนี้ กรมส่งเสริมอุตสาหกรรมสามารถยกเลิกการจัดซื้อได้ โดยผู้ประสงค์จะเสนอราคาไม่สามารถเรียกร้องค่าเสียหายใดๆทั้งสิ้น

12.2 ในกรณีที่ไม่สามารถคัดเลือกผู้ดำเนินการที่มีคุณสมบัติ ราคาที่เหมาะสมได้ กรมส่งเสริมอุตสาหกรรม ขอสงวนสิทธิ์ที่จะยกเลิกการประกวดราคาฯ ทั้งนี้ ผู้เสนอราคาจะเรียกร้องค่าใช้จ่ายใดๆทั้งสิ้นไม่ได้

13. ผู้รับผิดชอบโครงการและผู้ประสานงานโครงการ

กลุ่มระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมส่งเสริมอุตสาหกรรม

- | | |
|------------------------------|------------------------------------|
| ● นายเกียรติพงษ์ อุดมธนะธีระ | นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ |
| โทรศัพท์ 0 2202 4515 | อีเมล kiattiphong@dip.go.th |
| ● นางสาวโชคนิธิ นาคเมธี | นักวิชาการอุตสาหกรรมปฏิบัติการ |
| โทรศัพท์ 0 2202 4516 | อีเมล choknithi@dip.go.th |