รายละเอียดคุณลักษณะเฉพาะ
จัดซื้อสิทธิ์การใช้งานชุดซอฟต์แวร์ระบบรักษาความปลอดภัย
สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล

1. ความเป็นมา

ตามที่ฝ่ายเทคโนโลยีสารสนเทศ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) ดำเนินการจัดซื้อชุดสิทธิ์การใช้งานชุดซอฟต์แวร์ระบบรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล เพื่อป้องกันการโจมตีหรือภัยคุกคามต่างๆ ที่จะเกิดขึ้นกับเครื่องคอมพิวเตอร์ส่วนบุคคล จำนวน 360 เครื่อง สำหรับควบคุมการใช้งานอุปกรณ์ต่อพ่วงตามนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ โดยต้องมีระบบตรวจจับและตอบสนองต่อเหตุภัยคุกคามไซเบอร์ บริหารจัดการด้วยผ่านระบบบริหารจัดการส่วนกลาง (Centralized Management Console)

2. วัตถุประสงค์

เพื่อจัดหาสิทธิ์การใช้งานชุดซอฟต์แวร์ระบบรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล จำนวน 1 สิทธิ์ สามารถใช้งานร่วมกับเครื่องคอมพิวเตอร์ส่วนบุคคล ได้ไม่น้อยกว่า 360 เครื่อง

3. คุณสมบัติผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงาน ของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการ ผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดาเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและ การบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคล ผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวาง การแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของ ผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) ที่ ๐๔๐๕.๒ /ว๑๒๔ ลงวันที่ ๑ มีนาคม ๒๕๖๖

3.11 ผู้ยื่นข้อเสนอต้องมีผลงานจำหน่ายระบบหรือซอฟต์แวร์ที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ จำนวน 1 ผลงาน วงเงินรวมกันไม่น้อยกว่า 250,000 บาท (สองแสนห้าหมื่นบาทถ้วน) ในระยะเวลาไม่เกิน 5 ปี จนถึงวันที่ยื่นข้อเสนอ และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงานเอกชนที่ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) เชื่อถือ โดยยื่นสำเนาหนังสือรับรองผลงานและสำเนาสัญญาหรือใบสั่งซื้อ ซึ่งเป็นงานเดียวกัน

3.12 ผู้ยื่นข้อเสนอต้องจัดทำรายการวัสดุหรือครุภัณฑ์ที่ใช้ในงานจ้างซึ่งเป็นพัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างนี้ (ถ้ามี)

4. คุณสมบัติผู้ยื่นข้อเสนอเพิ่มเติม

ผู้ยื่นข้อเสนอต้องมีเอกสารแต่งตั้งเป็นตัวแทนจำหน่ายซอฟต์แวร์ ที่ประกาศประกวดราคาอิเล็กทรอนิกส์ในครั้งนี้ จากบริษัทผู้ผลิตซอฟต์แวร์หรือสาขาของผู้ผลิตซอฟต์แวร์ในประเทศไทย

5. คุณลักษณะเฉพาะ

5.1 โปรแกรมป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ (Antivirus) โดยต้องมีคุณลักษณะดังต่อไปนี้

1. เป็นโปรแกรมป้องกันไวรัสที่สนับสนุนการทำงานบนระบบปฏิบัติการ Microsoft Windows 10/11 และสามารถป้องกันและกำจัดมัลแวร์ได้ทั้งแบบ Real-time และ On-demand โดยไม่กระทบต่อประสิทธิภาพของระบบ
2. ใช้วิธีการตรวจจับมัลแวร์ทั้งจากฐานข้อมูล Signatures, Heuristics, Advanced Heuristics และ Machine Learning รวมถึงสามารถตรวจจับโปรแกรมที่ไม่พึงประสงค์ (PUA/PUP) ได้
3. สามารถตรวจจับภัยคุกคามจากอินเทอร์เน็ต อีเมล และสื่อบันทึกข้อมูล เช่น Local Drive, Removable Media และ Network Drive ได้
4. สามารถตรวจสอบและสแกนไฟล์ประเภท Archives, Self-extracting files และ Runtime packers ได้
5. มีระบบป้องกันภัยขั้นสูง เช่น Exploit Blocker, Host Intrusion Prevention, Advanced Memory Scanner, Network Attack Protection, Botnet Protection และ Ransomware Shield
6. มีระบบ Web Control และ Anti-Phishing เพื่อป้องกันเว็บไซต์อันตรายและเว็บไซต์หลอกลวง
7. มี Microsoft Outlook Toolbar สำหรับการสแกนอีเมลไวรัสโดยตรงบนเครื่องลูกข่าย
8. สามารถตั้งรหัสผ่านเพื่อป้องกันการเปลี่ยนค่าการติดตั้งโปรแกรม และสามารถตั้งค่า Exclusion สำหรับไฟล์ โฟลเดอร์ หรือ Hash file ได้

9. มีระบบควบคุมการใช้งานอุปกรณ์เชื่อมต่อภายนอก (Device Control) โดยสามารถกำหนดประเภท หมายเลขอุปกรณ์ และสิทธิ์ในการเข้าถึงได้
10. มีเครื่องมือวิเคราะห์ข้อมูลของเครื่อง เช่น Drivers, Applications, Network Connection และ Registry เพื่อประเมินความเสี่ยงของแต่ละองค์ประกอบได้
11. สามารถสแกนภัยคุกคามในระดับระบบและหน่วยความจำ เช่น Unified Extensible Firmware Interface (UEFI) และ RAM ได้
12. สามารถเข้าสู่โหมดการทำงานเงียบ (Presentation Mode) และสแกนอัตโนมัติเมื่อเครื่องอยู่ในสถานะ Screen Saver, Lock หรือ Logoff ได้
13. มีระบบป้องกันภัยบนคลาวด์ (Cloud-based Sandbox and Reputation System) เพื่อวิเคราะห์ไฟล์ที่ไม่เคยรู้จักภายใน 5 นาที และป้องกันการโจมตีแบบ Zero-day
14. รองรับการใช้งานในเมนูภาษาไทย (Thai GUI) และมีเครื่องมือถอนการติดตั้งโปรแกรมป้องกันไวรัสรายอื่นในตัวติดตั้ง
15. สามารถป้องกันการโจมตีแบบ Brute-force ได้
16. รองรับการอัปเดตฐานข้อมูลไวรัสและโปรแกรมโดยอัตโนมัติ
17. สามารถสำรองและกู้คืนไฟล์ที่ถูกแก้ไขโดยแรนซัมแวร์ได้
18. สำหรับเครื่องแม่ข่าย (Server) โปรแกรมสามารถยกเว้นไฟล์ระบบของ Windows Server ได้อัตโนมัติ และสามารถสแกนไฟล์ที่จัดเก็บไว้บน OneDrive ได้

5.2 ระบบตรวจสอบและตอบสนองการโจมตีขั้นสูง (Endpoint Detection and Response - EDR)

สามารถตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามสมัยใหม่ที่โปรแกรมป้องกันไวรัส ไม่สามารถตรวจพบได้ อีกทั้งยังสนับสนุนการดำเนินการตามประกาศของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อให้สามารถรับมือและกู้คืนจากเหตุภัยคุกคามได้อย่างมีประสิทธิภาพและทันท่วงที โดยต้องมีคุณลักษณะดังต่อไปนี้

1. รองรับการติดตั้ง Agent บนระบบปฏิบัติการ Microsoft Windows 10/11
2. มีระบบบริหารจัดการผ่าน Web Console บนคลาวด์ของเจ้าของผลิตภัณฑ์ พร้อม Dashboard แสดงภาพรวม เช่น Incidents, Detections และ Executables
3. สามารถแสดงระดับความรุนแรงของภัยคุกคามได้ (Threats, Warnings, Informational)
4. สามารถสร้างกฎการตอบสนองต่อเหตุการณ์ความปลอดภัย เช่น Block Executables, Kill Process, หรือ Isolate Endpoint ได้ทั้งแบบอัตโนมัติและด้วยตนเอง
5. สามารถตรวจสอบรายละเอียดไฟล์ที่เกี่ยวข้อง เช่น Hash SHA1, Signature Type, File Description, File Version, Company Name และ File Size ได้
6. มีระบบ Reputation/Popularity จากคลาวด์เพื่อใช้ประเมินความน่าเชื่อถือของไฟล์

7. สามารถตรวจสอบพฤติกรรมของ Executables และ Script เช่น PowerShell หรือ Visual Basic Script รวมถึงการเปลี่ยนแปลงของ File และ Registry ได้
8. สามารถแสดงเทคนิคของภัยคุกคามโดยเทียบเคียงกับ MITRE ATT&CK Framework
9. สามารถแสดง Timeline ของเหตุการณ์เพื่อใช้ในการสืบสวนทางดิจิทัล (Forensic Investigation) ได้

5.3 ระบบบริหารจัดการส่วนกลาง (Centralized Management Console) ต้องมีคุณลักษณะดังต่อไปนี้

1. สามารถบริหารจัดการผ่าน Web Console บนคลาวด์ของเจ้าของผลิตภัณฑ์ การเชื่อมต่อระหว่างเครื่องลูกข่ายกับคอนโซลต้องเข้ารหัสด้วยโปรโตคอล TLS ขึ้นไป 2.1
2. สามารถตรวจสอบรายละเอียดเครื่องลูกข่าย เช่น Hardware Inventory, Installed Applications, Virus DB Version และการตั้งค่าโปรแกรมได้
3. สามารถกำหนดนโยบาย (Policy) และการสั่งงานจากศูนย์กลาง เช่น อัปเดตฐานข้อมูลไวรัส, สแกนเครื่อง, ปิดเครื่อง, ส่งข้อความ หรือสั่งออกจากระบบได้
4. สามารถกำหนดสิทธิ์ผู้ใช้งานหลายระดับ เช่น Read, Use และ Write (Role-based Access Control)
5. รองรับการเชื่อมต่อกับระบบ Active Directory เพื่อดึงโครงสร้างผู้ใช้และกลุ่มคอมพิวเตอร์อัตโนมัติ
6. มี Dashboard แสดงภาพรวมสถานะการป้องกันของระบบ เช่น เครื่องที่ปลอดภัย เครื่องที่มีปัญหา และภัยคุกคามที่ตรวจพบ
7. สามารถแจ้งเตือนเหตุการณ์ผ่านอีเมลเมื่อพบภัยคุกคามหรือสถานะผิดปกติ
8. สามารถบริหารจัดการ Quarantine ของเครื่องลูกข่ายจากศูนย์กลางได้
9. สามารถตั้งเวลาออกรายงานและส่งอีเมลรายงานในรูปแบบ CSV หรือ PDF ได้
10. รองรับการส่งข้อมูล Log ออกไปยังระบบ SIEM ผ่าน Syslog และสามารถ Export ข้อมูลในรูปแบบ Leef, JSON หรือ CEF ได้
11. สามารถติดตั้งหรือถอนการติดตั้งโปรแกรมป้องกันไวรัสจากศูนย์กลางได้
12. สามารถตรวจสอบกิจกรรมของผู้ดูแลระบบ (Admin Audit Log) ได้อย่างน้อยย้อนหลัง 12 เดือน
13. สามารถสั่งตัดการเชื่อมต่ออินเทอร์เน็ตของเครื่องลูกข่ายจากศูนย์กลาง (Isolate from Network) ได้
14. รองรับการสั่งงานเข้ารหัสทั้งดิสก์ (Full Disk Encryption) ผ่านคอนโซลได้

คุณสมบัติเพิ่มเติม

ผู้เสนอราคาจะต้องจัดอบรมแนะนำผู้ใช้งาน ให้กับบุคลากร สสวท. ไม่น้อยกว่า 1 ชั่วโมง จำนวน 1 ครั้ง และผู้ดูแลระบบ ไม่น้อยกว่า 1 ชั่วโมง จำนวน 1 ครั้ง พร้อมคู่มือการใช้งาน ในรูปแบบไฟล์ PDF จำนวน 1 ชุด

6. หลักเกณฑ์และสิทธิ์ในการพิจารณาราคา

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จะพิจารณาตัดสิน โดยใช้หลักเกณฑ์ราคาเพียงอย่างเดียว และ การพิจารณาผู้ชนะการยื่นข้อเสนอ สสวท. จะพิจารณาจาก ราคารวม (รวมภาษีมูลค่าเพิ่มแล้ว) ที่เสนอราคาต่ำสุด

7. วงเงินงบประมาณ

จำนวน 600,000 บาท (หกแสนบาทถ้วน) รวมภาษีมูลค่าเพิ่ม

8. ระยะเวลาการใช้สิทธิ์

ระยะเวลา 12 เดือน นับตั้งแต่ สสวท. ได้รับสิทธิ์การใช้งาน

9. การส่งมอบและการชำระเงิน

สสวท. ชำระเงิน 100% เมื่อ ได้รับสิทธิ์การใช้งาน และ กรรมการตรวจรับเรียบร้อยแล้ว ดังนี้

9.1 ส่งมอบแผนการทำงานตลอดระยะเวลาตามสัญญา ภายใน 14 วัน นับถัดจากวันลงนามในสัญญา

9.2 จัดอบรมแนะนำผู้ใช้งาน ให้กับบุคลากร สสวท. ไม่น้อยกว่า 1 ชั่วโมง จำนวน 1 ครั้ง และผู้ดูแลระบบไม่น้อยกว่า 1 ชั่วโมง จำนวน 1 ครั้ง พร้อมเอกสารการฝึกอบรม ในรูปแบบไฟล์เอกสารอิเล็กทรอนิกส์ (PDF) ภายใน 60 วัน นับถัดจากลงนามในสัญญา

9.3 ต้องแจ้งกำหนดเวลาส่งมอบงาน โดยทำหนังสือแจ้ง สสวท. ก่อนวันส่งมอบงาน ไม่น้อยกว่า 7 วันทำการ และ ดำเนินการส่งมอบสิทธิ์การใช้งาน ภายใน 60 วัน นับถัดจากลงนามในสัญญา

10. การรับประกัน

10.1 ผู้ยื่นข้อเสนอต้องรับประกัน 12 เดือน นับถัดจากวันส่งมอบงาน และ ในกรณีที่ตรวจสอบพบความผิดพลาดของซอฟต์แวร์ ต้องดำเนินการแก้ไขให้ถูกต้องภายใน 1 วันทำการ

10.2 ผู้ยื่นข้อเสนอ ต้องมีการให้บริการถึงสถานที่ติดตั้ง (On-Site Service) แบบ 8x5x4 พร้อมให้บริการใน 8 ชั่วโมง ตลอด 5 วันทำการ วันจันทร์ถึงศุกร์ และมีการตอบสนอง (Response Time) ภายในระยะเวลา 4 ชั่วโมง หลังจากได้รับแจ้งเหตุผิดปกติ ตลอดระยะเวลาการรับประกัน

10.3 สสวท. จะต้องมีสิทธิ์ได้รับการปรับปรุงผลิตภัณฑ์ (Upgrade) ให้เป็น Version หรือ Release ใหม่เพื่อการใช้งานซอฟต์แวร์ที่ปรับให้ทันสมัยอย่างครอบคลุมทุกฟังก์ชันการใช้งาน โดยการปรับปรุงต้องไม่มีผลกระทบต่อการทำงานของระบบทั้งหมดที่เกี่ยวข้องและไม่คิดค่าใช้จ่ายเพิ่ม

11. การรับผิดชดใช้ค่าเสียหาย

กรณีผู้ขายไม่ปฏิบัติตามสัญญาจนเป็นเหตุให้เกิดความเสียหายแก่ สสวท. ผู้ขายต้องชดใช้ค่าเสียหายให้แก่ สสวท. ภายในกำหนด 30 วัน นับถัดจากวันที่ได้รับแจ้งจาก สสวท.

12. สิทธิ์ของ สสวท.

สสวท. มีสิทธิ์ทำสำเนาโปรแกรมคอมพิวเตอร์ได้ 1 ชุด เพื่อป้องกันการสูญหาย โดยบรรจุโปรแกรมคอมพิวเตอร์ ลงในเครื่องคอมพิวเตอร์แม่ข่าย ชื่อว่า File Server

13. ค่าปรับ

กรณีที่ผู้ขายส่งมอบงานเกินระยะเวลาที่กำหนด ผู้ขายจะต้องชำระค่าปรับเป็นรายวันให้แก่ สสวท. เป็นรายวัน ในอัตราร้อยละ 0.2 ของราคาซอฟต์แวร์ที่ยังไม่ได้รับมอบ นับแต่วันถัดจากวันครบกำหนด ตามสัญญา จนถึงวันที่ผู้ขายได้นำซอฟต์แวร์มาส่งมอบให้แก่ สสวท. จนถูกต้องครบถ้วน