# ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง) ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

๑. ชื่อโครงการ ซื้อโปรแกรมป้องกันไวรัส (Antivirus) ประจำปีงบประมาณ พ.ศ. ๒๕๖๒

/หน่วยงานเจ้าของโครงการ สำนักบริหาร

๒. วงเงินงบประมาณที่ได้รับจัดสรร ๒๓๕,๐๐๐ บาท

๓. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ๓๐ สิงหาคม ๒๕๖๒

เป็นเงิน ๒๓๔,๓๓๐ บาท ราคา/หน่วย (ถ้ามี) บาท

๔. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

๑. บริษัท ไทยทรานสมิชชั่น อินดัสทรี จำกัด

๒. บริษัท ทีโออาร์ คอมพิวติ้ง จำกัด

๓. บริษัท เอ็นต้าซอร์ส จำกัด

๕. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

๑. นายประชารักษ์ บุญประกอบ

๒.

๓.

# วิธีคำนวณราคากลาง

## ซื้อโปรแกรมป้องกันไวรัส (Antivirus) ประจำปีงบประมาณ พ.ศ. ๒๕๖๒

| | | | |
|---|---|---|---|
| ๑. บริษัท ไทยทรานสมิชชั่น อินดัสทรี จำกัด | เสนอราคา | ๒๓๔,๓๓๐.๐๐ | บาท |
| ๒. บริษัท ทีโออาร์ คอมพิวติ้ง จำกัด | เสนอราคา | ๒๓๙,๙๘๔.๙๕ | บาท |
| ๓. บริษัท เอ็นต้าซอร์ส จำกัด | เสนอราคา | ๒๕๓,๐๐๑.๕๐ | บาท |

**ขอบเขตของงาน (Term of Reference : TOR)**
**โครงการจัดซื้อโปรแกรมป้องกันไวรัส (Antivirus) ปีงบประมาณ พ.ศ. ๒๕๖๒**
**สถาบันเพื่อการยุติธรรมแห่งประเทศไทย**

**๑. หลักการและเหตุผล**

ด้วยปัจจุบันสถาบันได้นำระบบเครือข่ายคอมพิวเตอร์เข้ามาใช้งาน ทำให้เครื่องคอมพิวเตอร์สามารถเชื่อมต่อถึงกัน ซึ่งคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายของสถาบันก็สามารถเชื่อมต่อถึงกันได้ ทำให้สะดวกและเกิดประโยชน์ในการทำงานสามารถใช้บริการ Internet และ Intranet และบริการอื่น ๆ บนเครือข่ายทำให้ผู้ใช้งานสะดวก นั้น

ดังนั้นเมื่อนำระบบดังกล่าวมาใช้งานปัญหาไวรัสคอมพิวเตอร์ จึงเป็นปัญหาที่ทุกคนต้องตระหนักและให้ความสำคัญ ส่วนงานเทคโนโลยีสารสนเทศจึงต้องหาทางป้องกันไม่ให้เครื่องคอมพิวเตอร์ แม่ข่าย(Server) และคอมพิวเตอร์ลูกข่าย(Client) ติดไวรัส

**๒.วัตถุประสงค์ของการจัดหา**

เพื่อจัดหาโปรแกรม Antivirus สำหรับเครื่อง แม่ข่ายคอมพิวเตอร์ (Server Computer ) และเครื่องลูกข่าย (Client) เป็นระยะเวลา ๓ ปี

**๓. คุณสมบัติผู้รับจ้าง**

๓.๑ เป็นนิติบุคคลหรือผู้ร่วมการงาน (Consortium) หรือกิจการร่วมค้า (Joint Venture) ที่จดทะเบียนตั้งขึ้นตามกฎหมายประเทศไทย ซึ่งมีวัตถุประสงค์ในการประกอบธุรกิจทางด้านการออกแบบ ติดตั้ง หรือพัฒนาระบบเทคโนโลยีสารสนเทศ

๓.๒ ไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการ และได้แจ้งเวียนชื่อแล้วหรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ

๓.๓ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

๓.๔ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่นที่เข้าเสนอราคาให้แก่กระทรวงยุติธรรม ณ วันประกาศสอบราคา หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างไม่เป็นธรรมในการสอบราคาซื้อครั้งนี้

๓.๕ ผู้เสนอราคา ต้องไม่เป็นผู้ที่ถูกระบุชื่อว่าเป็นคู่สัญญาที่ไม่ได้แสดงบัญชีรายรับรายจ่ายหรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญตามประกาศคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ เรื่องหลักเกณฑ์และวิธีการจัดทำและแสดงบัญชีรายการรับจ่ายของโครงการที่บุคคลหรือนิติบุคคลเป็นคู่สัญญากับหน่วยงานของรัฐ พ.ศ. ๒๕๕๔ (แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ.๒๕๕๔ และ (ฉบับที่ ๓) พ.ศ. ๒๕๕๕)

สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (องค์การมหาชน) THAILAND INSTITUTE OF JUSTICE

**๔. ขอบเขตงานที่จ้าง**

๔.๑ ระบบตรวจสอบและป้องกันไวรัสคอมพิวเตอร์ แบบ Server จำนวน ๑๕ Licenses ระยะเวลาการใช้งาน ๓๖ เดือน มีคุณลักษณะอย่างน้อย ดังนี้

๔.๑.๑ สามารถติดตั้ง (Agent) และใช้งานได้อย่างถูกต้องบนระบบปฏิบัติการ เช่น Windows Server ๒๐๐๘R๒, Windows Server ๒๐๑๒, Windows Server ๒๐๑๖, Windows Server ๒๐๑๙ ทั้งแบบ ๓๒ บิต และ ๖๔ บิต และ Linux ได้เป็นอย่างน้อย

๔.๑.๒ มีระบบบริหารจัดการนโยบายจากส่วนกลาง (Policy Management) ผ่าน web console หรือ GUI ได้

๔.๑.๓ มีระบบบริหารจัดการนโยบายจากส่วนกลาง (Policy Management) เป็น Cloud Base Management

๔.๑.๔ สามารถทำการป้องกันอันตรายที่มาจากทางเว็บไซต์ต่าง ๆ (Web Threats) โดยใช้ Web Reputation ได้

๔.๑.๕ สามารถบริหารจัดการ Endpoint ได้ทั้ง Windows, Linux ผ่าน Cloud Dashboard เดียวกันได้

๔.๑.๖ สามารถดูแลระบบสาขาที่อยู่ต่างวงเครือข่าย ได้โดย Web-bases Management เพียงตัวเดียวกัน

๔.๑.๗ สามารถทำการป้องกันภัยคุกคามจาก Viruses, Worms, Trojans, Spyware , Greyware ได้

๔.๑.๘ สามารถตรวจจับแอนตี้ไวรัสที่ใช้งานอยู่ก่อนการติดตั้งใหม่ ได้ เพื่อการถอดถอนแอนตี้ไวรัส ก่อนการติดตั้งโดยอัตโนมัติ

๔.๑.๙ สามารถตรวจพบไวรัสคอมพิวเตอร์ได้อย่างน้อย โดยวิธีการตรวจสอบข้อมูลจาก Definition หรือ Signature ของไวรัส นอกจากนั้นสามารถใช้เทคนิคการตรวจจับไวรัสหรือมัลแวร์ได้หลากหลายวิธีเช่น Signature Database, Live protection, HIPS และ Malicious Traffic Detection หรือ ระบบอื่นเพิ่มเติมเพื่อทำงานเทียบเท่าได้หรือดีกว่า

๔.๑.๑๐ มีระบบการติดตั้งใช้งานและปรับปรุงข้อมูลไวรัสคอมพิวเตอร์ให้ทันสมัยซึ่งสามารถทำงานได้ในลักษณะผ่าน cloud หรือผ่านเครื่องบริหารจัดการส่วนกลางกับเครื่องคอมพิวเตอร์ลูกข่าย

๔.๑.๑๑ มีระบบส่งหรือวิธีส่งไฟล์ที่ต้องสงสัยว่าเป็นไวรัสตรวจพบใหม่ไปยังทาง Lab ของผู้ผลิตโปรแกรมได้

๔.๑.๑๒ สามารถทำงานยกเว้นการตรวจสอบ (Scan) ไวรัส โดยกำหนดในรูปแบบ Drive, Folder, Website และ ระบุชื่อ File ได้เป็นอย่างน้อย

๔.๑.๑๓ สามารถกำหนดการเข้าใช้งานแอพพลิเคชั่น โดยระบบบริหารจัดการการเข้าใช้งานแอพพลิเคชั่น สามารถตั้งค่าได้แบบ Category หรือ Path List

๔.๑.๑๔ สามารถอนุญาต/ไม่อนุญาต ใช้งานอุปกรณ์ต่อพ่วง ได้ หรือกำหนดให้ใช้งานได้เฉพาะอ่านไฟล์จากอุปกรณ์ต่อพ่วงได้อย่างเดียว

๔.๑.๑๕ สามารถป้องกันการแก้ไขค่า และการถอนการติดตั้งโปรแกรมป้องกันไวรัสโดยใช้รหัสผ่านได้

๔.๑.๑๖ มีเทคโนโลยีที่ทำการเพิ่มประสิทธิภาพในการตรวจสอบ (Scan) ไวรัสคอมพิวเตอร์ โดยสามารถกำหนดให้ตรวจสอบเฉพาะไฟล์ใหม่หรือไฟล์ที่มีการแก้ไขได้ เป็นอย่างน้อย

๔.๑.๑๗ สามารถป้องกันการโอนย้ายข้อมูลออกจากเครื่องคอมพิวเตอร์ (Data Loss Prevention - DLP) โดยสามารถระบุเงื่อนไขได้ ๒ รูปแบบ คือ File Matching rules และ Content rules เป็นอย่างน้อย โดยไม่ต้องซื้อไลเซ่นส์เพิ่มเติมและอยู่ภายใต้ Agent เดียวกันกับระบบป้องกันไวรัส

๔.๑.๑๘ สามารถทำการแจ้งเตือนการพบไวรัสคอมพิวเตอร์ผ่านทาง Desktop messaging, Email alerting และ Event logging ได้เป็นอย่างน้อย

๔.๑.๑๙ ผลิตภัณฑ์ที่เสนอต้องจัดอยู่ในกลุ่ม Leader Gartner ของ Magic Quadrant for Endpoint Protection ปี ๒๐๑๘

**๔.๒ ระบบตรวจสอบและป้องกันไวรัสคอมพิวเตอร์ แบบ Endpoint จำนวน ๘๕ Licenses ระยะเวลาการใช้งาน ๓๖ เดือน มีคุณลักษณะอย่างน้อย ดังนี้**

๔.๒.๑ สามารถติดตั้ง (Agent) และใช้งานได้อย่างถูกต้องบนระบบปฏิบัติการ เช่น Windows ๗, Windows ๘ , Windows ๑๐ ทั้งแบบ ๓๒ บิต และ ๖๔ บิต และ MAC OS ได้เป็นอย่างน้อย

๔.๒.๒ มีระบบบริหารจัดการนโยบายจากส่วนกลาง (Policy Management) ผ่าน web console หรือ GUI ได้

๔.๒.๓ มีระบบบริหารจัดการนโยบายจากส่วนกลาง (Policy Management) เป็น Cloud Base Management

๔.๒.๔ สามารถทำการป้องกันอันตรายที่มาจากทางเว็บไซต์ต่างๆ (Web Threats) โดยใช้ Web Reputation ได้

๔.๒.๕ สามารถบริหารจัดการ Endpoint ได้ทั้ง Windows, Mac ผ่าน Cloud Dashboard เดียวกันได้

๔.๒.๖ สามารถดูแลระบบสาขาที่อยู่ต่างวงเครือข่าย ได้โดย Web-bases Management เพียงตัวเดียวกัน

๔.๒.๗ สามารถทำการป้องกันภัยคุกคามจาก Viruses, Worms, Trojans, Spyware , Greyware ได้

๔.๒.๘ สามารถตรวจจับแอนตี้ไวรัสที่ใช้งานอยู่ก่อนการติดตั้งใหม่ ได้ เพื่อการถอดถอนแอนตี้ไวรัส ก่อนการติดตั้งโดยอัตโนมัติ

๔.๒.๙ สามารถตรวจพบไวรัสคอมพิวเตอร์ได้อย่างน้อย โดยวิธีการตรวจสอบข้อมูลจาก Definition หรือ Signature ของไวรัส นอกจากนั้นสามารถใช้เทคนิคการตรวจจับไวรัสหรือมัลแวร์ได้หลากหลายวิธีเช่น Signature Database, Live protection, HIPS และ Malicious Traffic Detection หรือ ระบบอื่นเพิ่มเติมเพื่อทำงานเทียบเท่าได้หรือดีกว่า

๔.๒.๑๐ มีการ update signature แบบ Genotype Technology เพื่อเพิ่มประสิทธิภาพในการ Update ฐานข้อมูลการป้องกันไวรัสอย่างมีประสิทธิภาพ

๔.๒.๑๑ มีระบบการติดตั้งใช้งานและปรับปรุงข้อมูลไวรัสคอมพิวเตอร์ให้ทันสมัยซึ่งสามารถทำงานได้ในลักษณะผ่าน cloud หรือผ่านเครื่องบริหารจัดการส่วนกลางกับเครื่องคอมพิวเตอร์ลูกข่าย

๔.๒.๑๒ มีระบบส่งหรือวิธีส่งไฟล์ที่ต้องสงสัยว่าเป็นไวรัสตรวจพบใหม่ไปยังทาง Lab ของผู้ผลิตโปรแกรมได้

๔.๒.๑๓ สามารถทำงานยกเว้นการตรวจสอบ (Scan) ไวรัส โดยกำหนดในรูปแบบ Drive, Folder, Website และ ระบุชื่อ File ได้เป็นอย่างน้อย

๔.๒.๑๔ สามารถกำหนดการเข้าใช้งานแอพพลิเคชั่น โดยสามารถกำหนดเป็นกลุ่มหรือราย User ได้ โดยระบบบริหารจัดการการเข้าใช้งานแอพพลิเคชั่น สามารถตั้งค่าได้แบบ Category หรือ Path List

๔.๒.๑๕ สามารถอนุญาต/ไม่อนุญาต ใช้งานอุปกรณ์ต่อพ่วง ได้ หรือกำหนดให้ใช้งานได้เฉพาะอ่านไฟล์จากอุปกรณ์ต่อพ่วงได้อย่างเดียว โดยสามารถกำหนดเป็นกลุ่มหรือราย User ได้

๔.๒.๑๖ สามารถป้องกันการแก้ไขค่า และการถอนการติดตั้งโปรแกรมป้องกันไวรัสโดยใช้รหัสผ่านได้

๔.๒.๑๗ สามารถป้องกันการแก้ไข Registry โปรแกรมป้องกันไวรัสได้

๔.๒.๑๘ มีเทคโนโลยีที่ทำการเพิ่มประสิทธิภาพในการตรวจสอบ (Scan) ไวรัสคอมพิวเตอร์ โดยสามารถกำหนดให้ตรวจสอบเฉพาะไฟล์ใหม่หรือไฟล์ที่มีการแก้ไขได้ เป็นอย่างน้อย

๔.๒.๑๙ สามารถป้องกันการโอนย้ายข้อมูลออกจากเครื่องคอมพิวเตอร์ (Data Loss Prevention - DLP) โดยสามารถระบุเงื่อนไขได้ ๒ รูปแบบ คือ File Matching rules และ Content rules เป็นอย่างน้อย โดยไม่ต้องซื้อไลเซ่นส์เพิ่มเติม

๔.๒.๒๐ สามารถทำการแจ้งเตือนการพบไวรัสคอมพิวเตอร์ผ่านทาง Desktop messaging, Email alerting และ Event logging ได้เป็นอย่างน้อย

๔.๒.๒๑ ผลิตภัณฑ์ที่เสนอต้องจัดอยู่ในกลุ่ม Leader Gartner ของ Magic Quadrant for Endpoint Protection ปี ๒๐๑๘

**๕. ระยะเวลาในการดำเนินงาน**

ใช้ระยะเวลาในการดำเนินการ ๓๐ วัน นับตั้งแต่ลงนามในสัญญา

สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (องค์การมหาชน) THAILAND INSTITUTE OF JUSTICE

**๖. งบประมาณในการดำเนินงาน**

งบประมาณในการจัดซื้อโปรแกรมป้องกันไวรัส (Antivirus) ตาม TOR นี้ อยู่ในวงเงิน ๒๓๕,๐๐๐ บาท (สองแสนสามหมื่นห้าพันบาทถ้วน) โดยเบิกจ่ายจากเงินงบประมาณรายจ่ายประจำปี พ.ศ. ๒๕๖๒ ค่าใช้จ่ายในการดำเนินงาน ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น และค่าใช้จ่ายทั้งปวงแล้ว

**๗. เงื่อนไขการเบิกจ่าย**

กำหนดการจ่ายเงินค่าจ้างทั้งหมด เมื่อผู้รับจ้างส่งมอบลิขสิทธิ์การใช้บริการโปรแกรมป้องกันไวรัส (Antivirus) และทำการติดตั้งระบบบริหารจัดการนโยบายจากส่วนกลาง (Policy Management) เป็น Cloud Base Management ตามที่ได้สรุปกับทางสถาบันฯ และตามรายละเอียดและข้อกำหนดในข้อ ๔ แก่สถาบันฯ เสร็จเรียบร้อยแล้ว

**๘. ลิขสิทธิ์ความเป็นเจ้าของ**

สิ่งต่าง ๆ ที่ผู้ให้บริการนำมาใช้ในการทำงาน ให้บริการ และส่งมอบให้แก่ สถาบัน ตาม TOR นี้ จะต้องมีความเหมาะสมตามหลักวิชาการ รวมทั้งไม่ขัดต่อกฎหมายและศีลธรรมอันดี และไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาของบุคคลใด ถ้าหากสิ่งใดที่ผู้ให้บริการนำมาใช้ในการทำงานเป็นงานอันมีทรัพย์สินทางปัญญา ผู้ให้บริการจะต้องจัดให้ สถาบันมีสิทธิใช้ประโยชน์ได้อย่างไม่มีข้อจำกัดตามเงื่อนไขที่กำหนดใน TOR นี้ และไม่มีค่าใช้จ่ายใด ๆ เพิ่มเติม และในกรณีที่มีบุคคลใดกล่าวอ้างว่า สถาบันละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาของบุคคลนั้น ผู้ให้บริการจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายและค่าเสียหายในเรื่องดังกล่าวทั้งสิ้น

สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (องค์การมหาชน) THAILAND INSTITUTE OF JUSTICE