ขอบเขตของงาน (Terms of Reference : TOR)

จ้างเหมาบริการตรวจสอบความปลอดภัยของระบบหลังจากการย้ายไปคลาวด์ เฟสที่ 1

---

1. ความเป็นมา

ตามที่สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) (สขญ.) ดำเนินการและพัฒนาระบบการเชื่อมต่อข้อมูลสุขภาพจากหน่วยบริการต่างๆ ผ่านโครงการ Health Link หรือ โครงการจัดทำระบบดิจิทัลและเทคโนโลยีเพื่อเชื่อมโยงข้อมูลสุขภาพทั่วประเทศ สขญ. ได้ดำเนินการเชื่อมโยงประวัติการรักษาระหว่างสถานพยาบาลในพื้นที่กรุงเทพมหานครแล้วกว่า 1,568 แห่ง และต้องการขยายการเชื่อมต่อให้ครอบคลุมหน่วยบริการทั่วประเทศจำนวนอีกกว่า 10,000 แห่ง ปัจจุบัน สขญ. ได้ดำเนินการจัดจ้างเพื่อย้ายระบบโครงสร้างพื้นฐานและพัฒนาระบบ Health Link ให้รองรับปริมาณการใช้งานที่เพิ่มขึ้น เพิ่มประสิทธิภาพการทำงานของบุคลากร และยกระดับความปลอดภัยของระบบ Health Link อย่างเป็นรูปธรรม โดยย้ายจากระบบคลาวด์เดิมไปยังระบบคลาวด์ใหม่

เนื่องจากระบบ Health Link เป็นระบบที่มีข้อมูลสุขภาพ ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวสูง และมีความเสี่ยงต่อการถูกโจมตีจากผู้ไม่หวังดี การย้ายระบบไปยังคลาวด์จึงจำเป็นต้องดำเนินการตรวจสอบความปลอดภัยขั้นพื้นฐาน เพื่อให้มั่นใจว่าระบบมีความมั่นคงปลอดภัยเพียงพอในการปกป้องข้อมูล โครงการ Health Link จึงได้จ้างเหมาบริการตรวจสอบความปลอดภัยของระบบหลังจากการย้ายระบบไปยังคลาวด์ในเฟสที่ 1 เพื่อประเมินความเสี่ยง ค้นหาช่องโหว่ และดำเนินการจัดการกับช่องโหว่เหล่านั้นอย่างเหมาะสม

2. วัตถุประสงค์

2.1 เพื่อให้ได้รายงานผลการทดสอบและจำนวนช่องโหว่ที่ตรวจพบภายหลังจากการย้ายระบบไปยังโครงสร้างพื้นฐานใหม่

2.2 เพื่อให้สามารถพิจารณาแนวทางและวิธีการในการจัดการกับช่องโหว่เหล่านั้นได้อย่างมีประสิทธิภาพ

3. คุณสมบัติของผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพตามที่ประกาศ

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่น หรือกระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกันซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

4. ขอบเขตของงาน

ขอบเขตของงานจ้างเหมาบริการตรวจสอบความปลอดภัยของระบบหลังจากการย้ายไปคลาวด์ เฟสที่ 1 (ครั้งที่ 1 และ 2 บริการตรวจสอบความปลอดภัยของระบบหลังจากการย้ายไปคลาวด์) โดยมีรายละเอียดดังนี้

4.1 Gray-box Penetration Test website ที่ใช้สำหรับแสดงข้อมูลการรักษา 1 เป้าหมาย

4.1.1 Role บุคลากรทางการแพทย์

4.1.1.1 1 หน้า Login

4.1.1.2 1 หน้า จัดการ Profile (Read-Write)

4.1.1.3 9 หน้า แสดงข้อมูลการรักษา (Read-Only)

4.1.2 Role Hospital Admin

4.1.2.1 1 หน้า Login

4.1.2.2 4 หน้า Read-Write

4.1.2.3 5 หน้า Read-Only

4.2 Gray-box Penetration Test API ที่ใช้สำหรับรับส่งข้อมูลการรักษา จำนวน 1 เป้าหมาย , 120 endpoints

4.3 Gray-box Penetration Test website https://healthlink.go.th/ (Wordpress) จำนวน 1 เป้าหมาย

4.4 Security Roadmap สำหรับเฟสที่ 2

5. กำหนดระยะเวลาส่งมอบงาน

ผู้รับจ้างจะต้องส่งมอบงานทั้งหมดภายในระยะเวลา 120 วัน นับถัดจากวันลงนามในสัญญา โดยมีรายละเอียด ดังนี้

งวดที่ 1 ส่งมอบงานภายใน 60 วัน นับถัดจากวันที่ลงนามในสัญญา เมื่อผู้รับจ้างได้ดำเนินงานและทำหนังสือส่งมอบงานงวดที่ 1 จำนวน 1 ชุด และจัดทำสำเนาบรรจุลงในสื่อบันทึกข้อมูลดิจิทัล และคณะกรรมการได้ทำการตรวจรับเรียบร้อยแล้ว โดยผู้รับจ้างจะต้องส่งงานอย่างน้อยดังนี้

- เอกสารรายงานช่องโหว่ครั้งที่ 1 รายละเอียดตามข้อ 4.1 – 4.3

งวดที่ 2 ส่งมอบงานภายใน 120 วัน นับถัดจากวันที่ลงนามในสัญญา เมื่อผู้รับจ้างได้ดำเนินงานและทำหนังสือส่งมอบงานงวดที่ 2 จำนวน 1 ชุด และจัดทำสำเนาบรรจุลงในสื่อบันทึกข้อมูลดิจิทัล และคณะกรรมการได้ทำการตรวจรับเรียบร้อยแล้ว โดยผู้รับจ้างจะต้องส่งงานอย่างน้อยดังนี้

- เอกสารรายงานช่องโหว่ครั้งที่ 2 (ตรวจสอบซ้ำ) รายละเอียดตามข้อ 4.1 – 4.3
- เอกสาร Security Roadmap สำหรับเฟสที่ 2 รายละเอียดตามข้อ 4.4

6. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

เกณฑ์ราคา

7. วงเงินงบประมาณ

งบประมาณประจำปี 2568 เป็นเงินจำนวน 500,000 บาท (ห้าแสนบาทถ้วน) ซึ่งได้รวมภาษีมูลค่าเพิ่มไว้แล้ว

8. งวดงานและการจ่ายเงิน

สขญ. จะชำระเงินจำนวน 2 งวด โดยมีรายละเอียดดังนี้

งวดที่ 1 ผู้ว่าจ้างจะจ่ายค่าจ้าง คิดเป็น ร้อยละ 70 ของวงเงินค่าจ้างเมื่อผู้รับจ้างได้ส่งมอบงานงวดที่ 1 และคณะกรรมการได้ตรวจรับเรียบร้อยแล้ว

งวดที่ 2 ผู้ว่าจ้างจะจ่ายค่าจ้าง คิดเป็น ร้อยละ 30 ของวงเงินค่าจ้างเมื่อผู้รับจ้างได้ส่งมอบงานงวดที่ 2 และคณะกรรมการได้ตรวจรับเรียบร้อยแล้ว

9. อัตราค่าปรับ

หากผู้รับจ้างไม่สามารถส่งมอบงานได้ตามเวลาที่กำหนดไว้ในสัญญา ผู้รับจ้างจะต้องชำระค่าปรับให้แก่ สขญ. เป็นรายวัน ในอัตราร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ของมูลค่าสัญญาจ้าง แต่จะต้องไม่ต่ำกว่าวันละ 100 บาท

10. สถานที่ติดต่อขอรับทราบข้อมูลเพิ่มเติม

สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)
เลขที่ 234/432 ซอยลาดพร้าว 12 ถนนลาดพร้าว
แขวงจอมพล เขตจตุจักร กรุงเทพมหานคร 10900
ไปรษณีย์อิเล็กทรอนิกส์ rinrada.du@bdi.or.th

คณะกรรมการจัดทำรายละเอียดขอบเขตของงาน

ลงชื่อ..... ประธานกรรมการ

(นายณพิภัช ไตรรัตณ์)

ลงชื่อ.....กรรมการ

(นายธัญ รัฐถานาวิน)

ลงชื่อ.....ก รรมการและเลขานุการ

(นายชยนณัฏฐ ทะนะมูล)