ขอบเขตของงาน (Term of Reference: TOR)

จ้างเหมาการทดสอบความปลอดภัยของระบบสารสนเทศ (Information Security Testing)

ประจำปี 2566 ศูนย์คุณธรรม (องค์การมหาชน)

---

1. หลักการและเหตุผล

ปีงบประมาณ 2566 ศูนย์คุณธรรม (องค์การมหาชน) กำหนดให้มีการทดสอบความปลอดภัยของระบบสารสนเทศ เพื่อเป็นการสร้างความมั่นใจในการป้องกันภัยคุกคามทางไซเบอร์ โดยทำการทดสอบ วิเคราะห์ ประเมินความเสี่ยง จุดอ่อน หรือจุดที่อาจก่อให้เกิดความเสียหายต่อข้อมูลสารสนเทศ เพื่อสามารถช่วยให้ ศูนย์คุณธรรม (องค์การมหาชน) มีการบริหารจัดการความเสี่ยงของระบบสารสนเทศได้อย่างมีประสิทธิภาพ พร้อมทั้งสามารถนำความรู้ที่ได้รับ มาประยุกต์ใช้เพื่อปรับปรุงระบบงานต่าง ๆ ให้มีประสิทธิภาพและมีความปลอดภัยอย่างเพียงพอ

2. วัตถุประสงค์

2.1 เพื่อประเมินสถานะความเสี่ยงด้านความปลอดภัยของระบบสารสนเทศ

2.2 เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

2.3 เพื่อนำความรู้ที่ได้รับมาประยุกต์ใช้เพื่อรักษาความปลอดภัยของระบบสารสนเทศ

3. คุณสมบัติของผู้เสนอราคา

3.1 ผู้เสนอราคาต้องมีความสามารถตามกฎหมาย

3.2 ผู้เสนอราคาต้องไม่เป็นบุคคลล้มละลาย

3.3 ผู้เสนอราคาต้องไม่อยู่ระหว่างเลิกกิจการ

3.4 ผู้เสนอราคาต้องไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอ หรือ ทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากไม่เป็นผู้ที่ผ่านเกณฑ์ประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของ กรมบัญชีกลาง

3.5 ผู้เสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการ ผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 ผู้เสนอราคาต้องมีคุณสมบัติ และ ไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

ประธาน

กรรมการ

กรรมการและเลขานุการ

3.7 ผู้เสนอราคาต้องเป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ผู้เสนอราคาต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ศูนย์คุณธรรม ณ วันประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม

3.9 ผู้เสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้เสนอราคาต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง ตามที่คณะกรรมการ ป.ป.ช. กำหนด

3.11 ผู้เสนอราคาต้องเป็นนิติบุคคลที่มีประสบการณ์ในการทำงานในหัวข้อที่สัมพันธ์กับงานที่ประกาศ จ้าง โดยมีมูลค่าของผลงานไม่น้อยกว่า 200,000 บาท (สองแสนบาทถ้วน) และเป็นผลงานที่เป็นคู่สัญญาเดียวและทำสัญญาโดยตรงกับส่วนราชการหรือหน่วยงานเอกชน ไม่น้อยกว่า 3 ปี จำนวน 1 ผลงาน จนถึงวันที่ประกาศประกวดราคาหรือวันที่ยื่นข้อเสนอ แล้วแต่วิธีการจัดจ้างที่กำหนด โดยผู้เสนอราคาจะต้องส่งเอกสารหนังสือรับรองผลงานหรือสำเนาสัญญาหรือสำเนาใบสั่งซื้อ/สั่งจ้าง มาประกอบการพิจารณาในการยื่นข้อเสนอโครงการด้วย

3.12 ผู้เสนอราคาเสนอโครงสร้างทีมงาน โดยมีรายละเอียดคุณสมบัติ และเอกสารรับรอง (Certificate) ดังนี้

(1) Project Manager อย่างน้อย 1 ท่าน และมีใบรับรองตามที่ระบุ ดังนี้

- CISSP (CERTIFIED INFORMATION SYSTEM SECURITY PROFESSIONAL)
- GPEN (GIAC PENETRATION TESTER)
- OSCP (OFFENSIVE SECURITY CERTIFIED PROFESSIONAL)
- GWAPT (GIAC WEB APPLICATION PENETRATION TESTER)

(2) Tester อย่างน้อย 2 ท่าน และมีใบรับรองตามที่ระบุ ดังนี้

- CEH (CERTIFIED ETHICAL HACKER)
- OSCP (OFFENSIVE SECURITY CERTIFIED PROFESSIONAL)
- GWAPT (GIAC WEB APPLICATION PENETRATION TESTER)

3.13 ผู้เสนอราคาต้องจัดทำขอบเขตการดำเนินงานเป็นตารางเปรียบเทียบคุณสมบัติตามรูปแบบดังนี้

.....ประธาน
.....กรรมการ
.....กรรมการและเลขานุการ

ขอบเขตการดำเนินงาน ศคธ. กำหนด	*ขอบเขตการดำเนินงานที่ผู้รับจ้างเสนอ*	*เปรียบเทียบขอบเขตการดำเนินงานที่ผู้เสนอราคาเสนอ*	*เอกสารอ้างอิง*
ให้ระบุขอบเขตการดำเนินงานที่สำนักงานกำหนด	ให้ระบุขอบเขตการดำเนินงานที่ผู้เสนอราคาเสนอ	ให้ระบุจุดที่ดีกว่า หรือเทียบเท่า หรือตามข้อกำหนด	ให้ระบุเอกสารอ้างอิงหรืออ้างอิงข้อตามเอกสารข้อกำหนด

4. ขอบเขตการดำเนินงาน

4.1 ผู้รับจ้างต้องดำเนินการจัดทำแผนการดำเนินงานทดสอบความปลอดภัยของระบบสารสนเทศ ดังนี้

4.1.1 จัดประชุมกับศูนย์คุณธรรม เพื่อนำเสนอแผนการดำเนินงานทดสอบระบบฯ

4.1.2 จัดทำแผนปฏิบัติการงานทดสอบระบบฯ ประกอบด้วย การทดสอบหาช่องโหว่ของระบบ Vulnerability assessment และ การทดสอบเจาะระบบ (Web Application Penetration Testing) จำนวน 2 ครั้ง โดยมีรายละเอียดหัวข้อต่างๆ ดังนี้

(1) ขอบเขตการดำเนินงานทดสอบ

(2) วิธีการทดสอบ

(3) ระยะเวลาการทดสอบ

(4) ทีมผู้ทดสอบ

(5) เครื่องมือที่ใช้ในการทดสอบ

4.1.3 ดำเนินการทดสอบหาช่องโหว่ของระบบ Vulnerability assessment ครั้งที่ 1 ดังนี้

(1) ทดสอบระบบฯ ไม่น้อยกว่า 10 IP

(2) ทดสอบระบบฯ แบบมี Credential (User และ Password)

(3) ทดสอบระบบฯ โดยใช้เครื่องมือทดสอบ ไม่น้อยกว่า 1 เครื่องมือ ทั้ง Commercial และ Open Source

4.1.4 ดำเนินการทดสอบเจาะระบบ (Web Application Penetration Testing) ครั้งที่ 1 ดังนี้

(1) ทดสอบระบบฯ จำนวน 1 Domain

(2) ทดสอบระบบฯ Website ที่อยู่ภายใต้ moralcenter.or.th

(3) ทดสอบระบบฯ รูปแบบ Grey-Box Penetration testing

ประธาน
กรรมการ
กรรมการและเลขานุการ

(4) ทดสอบระบบฯ ตามรูปแบบการทดสอบ (Framework) เช่น OWASP Web Security Testing Guide v.4.2, OWASP Top 10 Application Risk เป็นต้น

4.1.5 สรุปผลการทดสอบหาช่องโหว่ของระบบ Vulnerability assessment และ การทดสอบเจาะระบบ (Web Application Penetration Testing) ครั้งที่ 1 ตามขอบเขตงานข้อ 4.1.3 และ 4.1.4 โดยระบุรายละเอียดผลการทดสอบอย่างน้อย ดังนี้

(1) เป้าหมายการทดสอบ

(2) วิธีการทดสอบ

(3) เครื่องมือที่ใช้

(4) ชื่อช่องโหว่/ข้อตรวจพบ

(5) URL/IP address ที่มีช่องโหว่/ข้อตรวจพบ

(6) ผลกระทบ

(7) วิธีการแก้ไขช่องโหว่/ข้อตรวจพบ

4.2 ผู้รับจ้างต้องดำเนินการทดสอบหาช่องโหว่ (Vulnerability Assessment) และ ทดสอบเจาะระบบ (Penetration test) ครั้งที่ 2 ภายใน 60 วัน

4.3 สรุปผลการทดสอบความปลอดภัยระบบสารสนเทศ โดยมีรายละเอียดดังนี้

4.3.1 บทสรุปผู้บริหาร (Executive Summary)

4.3.2 แนวทางการดำเนินงานการทดสอบระบบฯ (Methodologies) ดังนี้

(1) เป้าหมายการทดสอบ

(2) วิธีการทดสอบ

(3) เครื่องมือที่ใช้

(4) การคำนวณความเสี่ยง

4.3.3 สรุปผลการทดสอบระบบฯ (Findings) ดังนี้

(1) ชื่อช่องโหว่/ข้อตรวจพบ

(2) URL/IP address ที่มีช่องโหว่/ข้อตรวจพบ

(3) ผลกระทบ

(4) วิธีการแก้ไขช่องโหว่/ข้อตรวจพบ

ประธาน
กรรมการ
กรรมการและเลขานุการ

(5) ผลการแก้ไขช่องโหว่/ข้อตรวจพบ

5. เงื่อนไขการส่งมอบงาน

การส่งมอบงานในแต่ละงวด ผู้รับจ้างต้องส่งเป็นหนังสือส่งมอบงานพร้อมระบุรายละเอียดของงานที่ส่งมอบทุกรายการให้ครบถ้วน

งวดที่ 1 ผู้รับจ้างจะต้องดำเนินการตามขอบเขตงานข้อ 4.1 ภายใน 30 วัน นับถัดจากวันลงนามสัญญา โดยต้องมีเอกสารที่ส่งมอบ จำนวน 3 ชุด และบันทึกลงแฟลชไดรฟ์ จำนวน 1 ชุด ดังนี้

(1) แผนการดำเนินงานทดสอบความปลอดภัยของระบบสารสนเทศ

(2) ผลการทดสอบหาช่องโหว่ของระบบ Vulnerability assessment และ ผลการทดสอบเจาะระบบ (Web Application Penetration Testing) ครั้งที่ 1 โดยจัดทำเป็นไฟล์ Excel

งวดที่ 2 ผู้รับจ้างจะต้องดำเนินการตามขอบเขตงานข้อ 4.2 และ 4.3 ภายใน 60 วัน นับถัดจากวันลงนามสัญญา โดยต้องมีเอกสารที่ส่งมอบ จำนวน 3 ชุด และบันทึกลงแฟลชไดรฟ์ จำนวน 1 ชุด ดังนี้

(1) ผลการทดสอบหาช่องโหว่ของระบบ Vulnerability assessment และ ผลการทดสอบเจาะระบบ (Web Application Penetration Testing) ครั้งที่ 2 โดยจัดทำเป็นไฟล์ Excel

(2) สรุปผลการทดสอบความปลอดภัยระบบสารสนเทศ ตามข้อ 4.3

6. เงื่อนไขการชำระเงิน

ผู้ว่าจ้างตกลงชำระค่าจ้างให้แก่ผู้รับจ้างเป็นเช็คขีดคร่อม หรือการโอนเงินทางอิเล็กทรอนิกส์ โดยผู้ว่าจ้างจะหักภาษี ค่าธรรมเนียมธนาคาร และค่าธรรมเนียมอื่นๆ ที่เกี่ยวข้องจากมูลค่าของค่าจ้าง ซึ่งผู้รับจ้างจะต้องชำระไว้ตามกฎหมายด้วย โดยมีรายละเอียดการชำระเงินดังนี้

งวดที่ 1 ร้อยละ 50 ของค่าจ้างตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงานงวดที่ 1 ถูกต้องและครบถ้วนตามสัญญา และตรวจรับมอบงานจ้างดังกล่าวเรียบร้อยแล้ว

งวดที่ 2 ร้อยละ 50 ของค่าจ้างตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานและส่งมอบงานงวดที่ 2 ถูกต้องและครบถ้วนตามสัญญา และตรวจรับมอบงานจ้างดังกล่าวเรียบร้อยแล้ว

ประธาน
กรรมการ
กรรมการและเลขานุการ

7. เงื่อนไขการหักค่าจ้างและการปรับ

กรณีที่ผู้รับจ้างไม่สามารถดำเนินการได้ตามข้อกำหนดหรือไม่สามารถส่งมอบงานได้ตามเงื่อนไขที่กำหนดไว้ในเอกสารนี้ ผู้รับจ้างจะต้องชำระค่าปรับในอัตราร้อยละ 0.1 ของมูลค่างานตามสัญญา

8. รายละเอียดหลักเกณฑ์ในการพิจารณา

หลักเกณฑ์ด้านราคา

9. ระยะเวลาในการดำเนินงาน

จำนวน 60 วัน นับถัดจากวันลงนามในสัญญา

10. ข้อสงวนสิทธิ์

10.1 ผู้รับจ้างจะต้องไม่จ้างช่วงงาน มอบหมายงาน ถ่ายโอนงาน หรือละทิ้งงานให้ผู้อื่นเป็น ผู้ทำงานแทนไม่ว่าทั้งหมดหรือแต่เพียงบางส่วนด้วยประการใด ๆ

10.2 ผู้รับจ้างจะต้องใช้ความชำนาญ ความระมัดระวัง และความขยันหมั่นเพียรในการปฏิบัติงานและจะต้องปฏิบัติหน้าที่ความรับผิดชอบให้สำเร็จลุล่วง เป็นไปตามมาตรฐานของวิชาชีพที่ยอมรับนับถือโดยทั่วไป

10.3 ในระหว่างระยะเวลาการทำงานจ้างผู้รับจ้างพึงต้องปฏิบัติตามหลักเกณฑ์ที่กฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องได้กำหนดไว้โดยเคร่งครัด

10.4 ข้อมูลเอกสาร ผลการศึกษาและการวิเคราะห์ที่ผู้รับจ้างเป็นผู้ดำเนินการและจัดหามาตามสัญญาจะต้องตกเป็นกรรมสิทธิ์ของศูนย์คุณธรรม โดยผู้รับจ้างจะนำข้อมูลผลการปฏิบัติงานไปใช้ หรือเผยแพร่ในกิจการอื่นนอกเหนือจากที่ระบุไว้ในข้อกำหนดนี้ไม่ได้ เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากศูนย์คุณธรรม

11. การเก็บรักษาข้อมูลที่เป็นความลับ

ผู้รับจ้างจะต้องจัดการเก็บรักษาข้อมูลต่าง ๆ ที่เกี่ยวกับการดำเนินงานตามสัญญานี้ที่ผู้รับจ้างได้รับ จากผู้จ้าง ซึ่งรวมถึงข้อมูลต่างๆ ที่ ผู้จ้างได้จัดทำขึ้นเนื่องจากการดำเนินงานนี้อย่างเป็นความลับ และ/ลงนามผู้กำหนดขอบเขตของงาน หรือความลับทางการค้าของผู้จ้าง และผู้รับจ้างต้องหามาตรการในการจัดเก็บข้อมูลที่เป็นความลับให้ มิดชิด ทั้งนี้ ผู้รับจ้างจะต้องลงนามใน “สัญญาไม่เปิดเผยข้อมูลที่เป็นความลับ” พร้อมสัญญาจ้าง

.....ประธาน
.....กรรมการ
.....กรรมการและเลขานุการ

12. งบประมาณ

จำนวนเงิน 200,000 บาท (สองแสนบาทถ้วน) ราคานี้รวมภาษีมูลค่าเพิ่มแล้ว

13. สอบถามรายละเอียดเพิ่มเติม

กลุ่มงานศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ สำนักพัฒนาองค์ความรู้นวัตกรรมและสื่อสารสนเทศ ศูนย์คุณธรรม (องค์การมหาชน) โทรศัพท์ 02 644 9900 ต่อ 520, 522 อีเมล info@moralcenter.or.th หรือ it@moralcenter.or.th

14. คณะกรรมการกำหนด TOR และกำหนดราคากลาง

ลงชื่อ.....ประธานกรรมการ
(นางสาวปรียาภรณ์ พูลศรี)
ตำแหน่ง ผู้จัดการสำนักพัฒนาองค์ความรู้นวัตกรรม ฯ

ลงชื่อ.....กรรมการ
(นางสาวนันทพร ทาวะระ)
ตำแหน่ง หัวหน้ากลุ่มงานสื่อสารและรณรงค์ทางสังคม

ลงชื่อ.....กรรมการและเลขานุการ
(นางกฤตินิฏฐ์ ประสมพลอย)
ตำแหน่ง นักวิชาการส่งเสริมคุณธรรม