ร่างขอบเขตงาน

โครงการจ้างบริการตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ

---

1. **หลักการและเหตุผล**

ปัจจุบันเทคโนโลยีมีความเจริญก้าวหน้าและเข้ามามีบทบาทในวิถีชีวิตของคน การเข้าถึงอินเทอร์เน็ตสามารถทำได้ทุกที่ทุกเวลา ทำให้สถาบันบัณฑิตพัฒนบริหารศาสตร์เกิดความเสี่ยงต่อภัยคุกคามทางไซเบอร์ จำเป็นต้องมีความพร้อมในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์หลายด้าน อาทิ งานโครงสร้างพื้นฐาน การเฝ้าระวัง ป้องกันและแก้ปัญหา การตรวจสอบช่องโหว่ของระบบสารสนเทศ รวมถึงเว็บไซต์ซึ่งมักจะเป็นเป้าถูกโจมตีอยู่บ่อยครั้ง นอกจากนี้ การแพร่ระบาดของภัยไซเบอร์ในรูปแบบต่าง ๆ มีเพิ่มมากขึ้น ขณะที่การวางแผนรับมือและซักซ้อมทั้งก่อนเกิดเหตุ ขณะเกิดเหตุ และหลังเกิดเหตุ ที่สถาบันมีอยู่ไม่เพียงพอ จึงจำเป็นต้องเสริมสร้างขีดความสามารถในการรับมือกับไซเบอร์ของสถาบันให้มีประสิทธิภาพยิ่งขึ้นกว่าเดิม

2. **วัตถุประสงค์**:

2.1. เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามด้านไซเบอร์และเตรียมความพร้อมในการรับมือกับภัยคุกคาม

2.2. เพื่อวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศ ทำการทดสอบการเจาะระบบเครือข่ายจากภายใน และภายนอกสถาบัน พร้อมทั้งรับข้อเสนอแนะในการปรับปรุงระบบความปลอดภัยที่เกี่ยวข้อง

3. **คุณสมบัติของผู้เสนอราคา**

3.1. เป็นนิติบุคคลที่ประกอบธุรกิจเกี่ยวกับการเป็นที่ปรึกษาด้านความมั่นคงปลอดภัยสารสนเทศ หรือดำเนินการทดสอบความปลอดภัยของระบบเทคโนโลยีสารสนเทศมาแล้วไม่น้อยกว่า 2 ปีนับจนถึงวันยื่นเอกสาร

3.2. ต้องมีประสบการณ์ในการทดสอบความปลอดภัยของระบบเทคโนโลยีสารสนเทศให้กับหน่วยงานภาครัฐหรือรัฐวิสาหกิจหรือหน่วยงานเอกชนต่าง ๆ มาแล้วไม่น้อยกว่า 2 หน่วยงาน

3.3. ต้องจัดบุคลากรซึ่งเป็นพนักงานประจำอย่างน้อย 1 ปี และเป็นผู้มีที่มีความเชี่ยวชาญ ด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ เข้าปฏิบัติงานจริงในโครงการ อย่างน้อย 2 คน พร้อมหลักฐานอ้างอิง รวมถึงแสดงรายละเอียดประวัติ และประสบการณ์การทำงานกับบริษัท ในวันยื่นเอกสารประกวดราคาโดยมีคุณสมบัติ ดังนี้

3.3.1. มีใบรับรองมาตรฐาน (Certification) ความรู้ความสามารถทางด้านความปลอดภัยคอมพิวเตอร์โดยหน่วยงานระดับสากล อย่างน้อย 1 รายการ จากการรับรองมาตรฐานดังต่อไปนี้ CEH (Certified Ethical Hacker), OSCP(Offensive Security Certified

Professional), GPEN (GIAC Penetration Tester) ใบรับรองมาตรฐาน (Certificate) จะต้องไม่หมดอายุ

3.3.2. ต้องมีการแจ้งชื่อบุคลากรทั้งหมด ที่ทำโครงการนี้ให้สถาบันทราบก่อนเริ่มโครงการ หากมีการเปลี่ยนแปลงในภายหลังจะต้องได้รับอนุญาต จากสถาบันก่อนเท่านั้น

3.4. ผู้ปฏิบัติงานในโครงการต้องมีประสบการณ์การทดสอบเจาะระบบ มาแล้วไม่น้อยกว่า 2 ปี อย่างน้อย 3 โครงการ

4. ข้อเสนอด้านเทคนิค และขอบเขตการดำเนินงาน

4.1. จัดทำแผนดำเนินงานอย่างละเอียด โดยต้องเสนอแผนดำเนินงานดังกล่าวให้สถาบันเห็นชอบก่อนเข้าดำเนินการล่วงหน้า

4.2. ดำเนินการประเมินความเสี่ยงและเจาะระบบเพื่อหาช่องโหว่ (Vulnerability Assessment & Penetration Testing : Gray box) ให้ครอบคลุมทั้งระบบ ระบบที่ทำการตรวจสอบ มีดังต่อไปนี้

4.2.1. ระบบทะเบียนนักศึกษา (REG) Web Application

4.2.2. ระบบฐานข้อมูลงานวิจัย (RMS) Web Application

4.2.3. ระบบฐานข้อมูลบริหารจัดการงานฝึกอบรม/สัมมนา (TMS) Web Application

4.2.4. ระบบสารสนเทศการบริหารทรัพยากรบุคคล (HRIS) Web Application

4.2.5. ระบบทะเบียนนักศึกษาส่วน Back Office (Client/Server Application)

4.3. ดำเนินการเจาะระบบ ให้สอดคล้องตามมาตรฐานต่างๆ เช่น OWASP (Open Web Application Security Project) โดยครอบคลุมอย่างน้อยตาม OWASP Top 10 Application Security version ล่าสุด หรืออื่นๆที่เกี่ยวข้อง หรือเกี่ยวเนื่องกับเซอร์วิสนั้นๆ

4.4. ดำเนินการทดสอบการเจาะระบบเครือข่ายภายใน ในรูปแบบของผู้บุกรุกที่เป็นผู้ใช้งาน

4.5. ดำเนินการหาข้อมูลหมายเลขไอพี เซอร์วิสการให้บริการ และเครือข่ายที่เกี่ยวข้องเพื่อส่งให้สถาบันพิจารณาในการดำเนินการทดสอบเจาะระบบ ต่อไป

4.6. ดำเนินการโดยใช้เครื่องมือ หรือโปรแกรมสำหรับการตรวจสอบค้นหาช่องโหว่ในระบบเครือข่ายหรือวิธีการอื่นๆ ร่วมกับการตรวจสอบโดยผู้เชี่ยวชาญ โดยหลีกเลี่ยงการดำเนินการที่จะทำให้ระบบเกิดปัญหา

4.7. การจัดทำรายงาน และสรุปผลการทดสอบเจาะระบบ

4.7.1. จุดอ่อนหรือช่องโหว่ที่พบ

4.7.2. รายละเอียดของจุดที่พบ เช่นรายละเอียดทางด้านเทคนิค

4.7.3. ระดับความเสี่ยง

4.7.4. วิธีการตรวจสอบหรือวิธีการโจมตีจุดที่พบ

4.7.5. วิธีการแก้ไขจุดอ่อนหรือช่องโหว่ที่พบ

4.7.6. ข้อแนะนำในการปรับปรุงระบบการรักษาความปลอดภัย

4.7.7. ข้อเสนอแนะอื่นๆ

4.8. การประชุมสรุปผลการทดสอบเจาะระบบ โดยมีรายละเอียดดังต่อไปนี้

4.8.1. การประชุมสรุปสำหรับผู้บริหาร (Executive) เป็นการประชุมสรุปผลการทดสอบการเจาะระบบให้กับผู้บริหารด้านเทคโนโลยีสารสนเทศ และผู้พัฒนาโปรแกรม เพื่อชี้แจงสิ่งที่พบและวิธีการดำเนินการแก้ไขต่อไป รวมทั้งชี้ให้เห็นถึงข้อมูลสาคัญๆ ของระบบที่สามารถเข้าถึงได้จากการทดสอบเจาะระบบ

4.8.2. การประชุมสรุปผลในเชิงเทคนิค เป็นการประชุมสรุปผลการทดสอบเจาะระบบให้กับผู้ดูแลระบบเทคโนโลยีสารสนเทศโดยตรง ซึ่งเนื้อหาจะเน้นไปเกี่ยวกับ ข้อมูลทางเทคนิคเชิงลึก รวมถึงการแก้ไข และป้องกัน ทั้งในระยะสั้น และระยะยาว

4.9. ทำการตรวจสอบช่องโหว่ และทดสอบเจาะระบบซ้ำ 1 ครั้ง (Revisit VA Scan & Pentest) ภายในเวลาที่สถาบันกำหนด

5. การรักษาความลับ

5.1. ผู้เสนอราคาต้องตกลงจะไม่เปิดเผยรายละเอียดเกี่ยวกับงาน และจะเก็บรักษาข้อมูล และหรือเอกสารอื่นใดที่เกี่ยวข้องกับโครงการนี้ไว้เป็นความลับ เว้นแต่เป็นการเปิดเผยเพื่อประโยชน์หรือความจำเป็นในการปฏิบัติงานตามสัญญา หรือเป็นกรณีจำเป็นต้องเปิดเผยตามกฎหมายหรือคำสั่งศาล หรือได้รับความยินยอมจากผู้ว่าจ้างเป็นลายลักษณ์อักษรหรือเป็นข้อมูลและหรือเอกสารที่ได้เปิดเผยต่อสาธารณชนแล้ว

5.2. ผู้เสนอราคาต้องตกลงว่าบรรดาข้อมูล เอกสาร และความลับทางธุรกิจของผู้ว่าจ้างทั้งปวง ที่ติดต่อสื่อสารมาจากผู้ว่าจ้างไม่ว่าลักษณะใด ๆ ที่เกี่ยวพันกับโครงการนี้ ไม่ว่าก่อนหรือหลังจากวันที่ลงนามในสัญญาฯ ถือว่าเป็นข้อมูลความลับของผู้ว่าจ้าง ซึ่งผู้เสนอราคาจะต้องนำข้อมูลดังกล่าวไปใช้เพื่อให้บรรลุวัตถุประสงค์ตามสัญญาฯ ผู้เสนอราคามีหน้าที่รับผิดชอบในการควบคุมดูแลพนักงาน ลูกจ้าง ตัวแทนหรือบุคคลากรของผู้เสนอราคา ไม่ให้เปิดเผยข้อมูลความลับของผู้ว่าจ้างให้แก่บุคคลที่สาม โดยปราศจากความยินยอมล่วงหน้าเป็นลายลักษณ์อักษรจากผู้ว่าจ้าง

5.3. ผู้เสนอราคาเข้าใจและยอมรับว่าข้อมูลหรือเอกสารใด ๆ ที่เกี่ยวข้องกับการปฏิบัติงานตามสัญญาฉบับนี้ เป็นทรัพย์สินของผู้ว่าจ้าง ผู้เสนอราคาจะใช้ข้อมูลและหรือเอกสารดังกล่าว ในการปฏิบัติงานให้เป็นไปตามวัตถุประสงค์ของสัญญาฯ นี้เท่านั้น และจะต้องเก็บรักษาข้อมูลและหรือเอกสารดังกล่าวไว้เป็นความลับ โดยจะเปิดเผยต่อบุคคลอื่นไม่ได้เป็นอันขาด เว้นแต่จะได้รับความยินยอมจากผู้ว่าจ้างเป็นลายลักษณ์อักษรและตกลงจะควบคุมดูแลให้บุคลากร พนักงาน ลูกจ้าง และหรือตัวแทนของผู้รับจ้างปฏิบัติเช่นเดียวกันกับผู้เสนอราคาด้วย ในกรณีที่สัญญานี้สิ้นสุดลงไม่ว่าด้วยเหตุใด ๆ ผู้เสนอราคาต้องตกลงส่งมอบบรรดาข้อมูลและเอกสารดังกล่าวคืนให้แก่ผู้ว่าจ้างทันที

5.4. ผู้เสนอราคาตกลงจะเก็บรักษาข้อมูลใด ๆ ที่ได้รับมา เนื่องจากการปฏิบัติงานตามสัญญาฯ ไว้เป็นความลับตลอดไป แม้ว่าสัญญาฯ จะสิ้นสุดลงไม่ว่าด้วยเหตุใด ๆ ก็ตาม

6. **ระยะเวลาดำเนินการ** 150 วัน นับจากวันที่ลงนามในสัญญา

6.1. งวดที่ 1 ระยะเวลาดำเนินการภายใน 60 วัน เมื่อดำเนินการตามข้อ 4.1 ถึง 4.8

6.2. งวดที่ 2 ระยะเวลาดำเนินการภายใน 150 วัน เมื่อดำเนินการตามข้อ 4.9

7. **เอกสารการส่งมอบงาน**

ผู้ชนะการเสนอราคาต้องจัดทำเอกสารรายงานตามที่เสนออย่างน้อย 2 ชุด ในรูปแบบเอกสาร (hard copy) และไฟล์ (Soft copy) ในรูปแบบ Microsoft Word หรือ Portable Document Format (.pdf) ลงบนสื่อ CD-ROM หรือดีกว่าอย่างน้อย 2 ชุด โดยจัดทำเป็นภาษาไทย และ/หรือภาษาอังกฤษ โดยลักษณะของเอกสาร ต้องเป็นทางการจัดทำรูปเล่มอย่างเหมาะสม มีสารบัญ เลขหน้า เพื่อให้เจ้าหน้าที่ของสถาบัน สะดวกในการค้นหาใช้งานและใช้อ้างอิงกับบริษัท

7.1. แผนการดำเนินงานอย่างละเอียด

7.2. รายงานผลการประเมิน

7.3. รายงานการประชุม

7.4. เอกสารอ้างอิงอื่น ๆ ที่เกี่ยวข้องทั้งหมด

8. **วงเงินงบประมาณ จำนวน** 1,300,000.00 **บาท (หนึ่งล้านสามแสนบาทถ้วน) รวมภาษีมูลค่าเพิ่ม**

สถาบันจะทำการเบิกชำระเงินให้ผู้รับจ้าง จำนวน 2 งวด โดยจะแบ่งการชำระเงิน ดังนี้

8.1. สถาบันจะชำระเงินร้อยละ 70 ของมูลค่ารวมทั้งสิ้น
เมื่อคณะกรรมการตรวจรับได้ทำการตรวจรับงานในงวดที่ 1 เรียบร้อยแล้ว

8.2. สถาบันจะชำระเงินร้อยละ 30 ของมูลค่ารวมทั้งสิ้น
เมื่อคณะกรรมการตรวจรับได้ทำการงานในงวดที่ 2 ตรวจรับเรียบร้อยแล้ว

ภาคผนวก ก ตารางเปรียบเทียบคุณสมบัติระหว่างข้อกำหนดและข้อเสนอ

ตารางเปรียบเทียบคุณสมบัติระหว่างข้อกำหนดและข้อเสนอ				
ข้อกำหนด	**ข้อกำหนดของสถาบันบันบัณฑิตพัฒนบริหารศาสตร์**	**ข้อเสนอของบริษัท**		**เอกสารอ้างอิงถึง**
		ตรงตามข้อกำหนด	ดีกว่าข้อกำหนด	((Reference

หมายเหตุ :

สำหรับเอกสารอ้างอิง ถ้าเป็นแคตตาล็อก ต้องมีการขีดเส้นใต้หรือลงสีสะท้อนแสงแสดงคุณลักษณะเฉพาะตามข้อกำหนดของสถาบัน เป็นข้อ ๆ โดยระบุเลขข้อให้ชัดเจนด้วย

<u>สถานที่ติดต่อสอบถามข้อมูลเพิ่มเติมหรือเสนอแนะวิจารณ์</u>

ขอทราบข้อมูลเพิ่มเติมได้ที่ กลุ่มงานพัสดุ กองคลังและพัสดุ สถาบันบัณฑิตพัฒนบริหารศาสตร์ เลขที่ 118 ถนนเสรีไทย แขวงคลองจั่น เขตบางกะปิ กรุงเทพฯ 10240

หรือ ทาง e-mail ที่ kasima@nida.ac.th

หรือสอบถามทางโทรศัพท์หมายเลข 02-727-3422 โทรสาร 02-374-9825 ในวันและเวลาราชการ