กองทุนบำเหน็จบำนาญข้าราชการ

ขอบเขตของงาน (Terms of Reference : TOR)

การจ้างผู้ให้บริการประเมินประสิทธิภาพและการรักษาความปลอดภัยด้านแอพพลิเคชั่น

(Application Security)

---

1. หลักการและเหตุผล

กองทุนบำเหน็จบำนาญข้าราชการ (กบข.) มีความประสงค์จะตรวจสอบและประเมินความมั่นคงปลอดภัยข้อมูลส่วนบุคคลและการรักษาความปลอดภัยด้านแอพพลิเคชั่นของ โมบายแอพพลิเคชั่น และเว็บแอพพลิเคชั่น เพื่อพัฒนาและปรับปรุงระบบและมาตรการรักษาความมั่นคง ปลอดภัยของระบบสารสนเทศที่มีลักษณะเป็นโมบายแอพพลิเคชั่น และเว็บแอพพลิเคชั่นให้ได้ตาม มาตรฐานสากล ซึ่งจะทำให้การดำเนินธุรกิจของ กบข. และการให้บริการด้านระบบสารสนเทศแก่สมาชิกของ กบข. มีความมั่นคงปลอดภัยและน่าเชื่อถือ และเพื่อให้เป็นไปตามข้อกำหนดในระเบียบกองทุนบำเหน็จบำนาญข้าราชการว่าด้วยนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พ.ศ. 2561 และกฎหมายอื่นๆที่เกี่ยวข้อง

2. วัตถุประสงค์

เพื่อจัดหาผู้ยื่นข้อเสนอตรวจสอบและประเมินความมั่นคงปลอดภัยข้อมูลส่วนบุคคลและการรักษาความปลอดภัยด้านแอพพลิเคชั่น ของโมบายแอพพลิเคชั่น และเว็บแอพพลิเคชั่น โดยวิเคราะห์ ประเมินความเสี่ยง/ช่องโหว่/จุดอ่อน ตามมาตรฐาน OWASP Application Security Verification Standard 4.0 โดเมน V8: Data Protection Verification Requirements เพื่อเป็นแนวทางให้สำนักงานพิจารณาปรับเพิ่มประสิทธิภาพระบบและมาตรการรักษาความมั่นคงปลอดภัยโมบายแอพพลิเคชั่นและเว็บแอพพลิเคชั่นให้ได้ตามมาตรฐานระดับสากลและการให้บริการด้านสารสนเทศต่อสมาชิก กบข. ที่น่าเชื่อถือ เพื่อให้สอดคล้องกับกฎหมายอื่นๆที่เกี่ยวข้อง

คุณสมบัติผู้ยื่นข้อเสนอ

ผู้ยื่นข้อเสนอต้องมีคุณสมบัติตามมาตรฐานที่ระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic GovernmentProcurement : e-GP) กำหนด

3. รายการรายละเอียดของงานจ้าง

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องนำเสนอแผนและ ดำเนินการตรวจสอบและประเมินความมั่นคงปลอดภัยข้อมูลส่วนบุคคลและการรักษาความปลอดภัยด้านแอพพลิเคชั่น ของโมบายแอพพลิเคชั่น และเว็บแอพพลิเคชั่น ให้สอดคล้องตามมาตรฐาน OWASP Application Security Verification Standard โดเมน V8: Data Protection Verification Requirements โดยดำเนินการตรวจสอบ จำนวน 3 ระบบ ดังต่อไปนี้

(1) My GPF My Web My Way (https://mygpf.gpf.or.th/)

(2) My GPF (Mobile Application for iOS & Android)

(3) GPF Web (https://www.gpf.or.th)

โดยผู้ยื่นข้อเสนอต้องทำการนำเสนอวิธีการ ตรวจสอบและประเมินความมั่นคงปลอดภัยข้อมูลส่วนบุคคลและการรักษาความปลอดภัยของแอพพลิเคชั่นที่ระบุ แจงแจงตาม โดเมนย่อย V8.1, V8.2 และ V8.3 เพื่อวัตถุประสงค์ดังต่อไปนี้เป็นอย่างน้อย

- ตรวจสอบการทำงานของแอพพลิเคชั่นและอุปกรณ์ที่เกี่ยวข้องเกี่ยวกับการเก็บข้อมูลส่วนบุคคลบนหน่วยความจำแคช (Cache Memory)
- ตรวจสอบการจัดเก็บข้อมูลส่วนบุคคลชั่วคราวหรือที่ถูกจัดเก็บบนหน่วยความจำแคชในฝั่งแอพพลิเคชั่น เซิร์ฟเวอร์จากการเข้าถึงโดยผู้ที่ไม่มีสิทธิ์
- ตรวจสอบมาตรการความปลอดภัยของแอพพลิเคชั่นในการแสดงจำนวนผู้ใช้งานหรือตรวจจับพฤติกรรมการใช้งานที่มากเกินไป
- ตรวจสอบแผนการสำรองและกู้ข้อมูลสำคัญและข้อมูลที่สำรองต้องถูกจัดเก็บไว้อย่างปลอดภัย
- ตรวจสอบการทำงานและความสามารถของแอพพลิเคชั่นเพื่อตอบสนองต่อการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (เช่น สิทธิการขอเข้าถึง ขอรับสำเนา ลบหรือทำลายข้อมูล เป็นต้น) รวมถึงตรวจสอบมาตรการการรักษาความมั่นคงปลอดภัยเพื่อป้องกันการสูญหาย เข้าถึง เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

เอกสารและผลงานที่ต้องส่งมอบ

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะต้องจัดส่งมอบรายงานต่างๆ(ภาษาไทย) ตามกำหนดเวลา ในรูปแบบรายงาน Soft file และ Hard copy เป็นอย่างน้อย โดยเอกสารจะต้องมีรายละเอียดดังต่อไปนี้

(ก) รายละเอียดแผนการตรวจสอบและประเมินความมั่นคงปลอดภัยข้อมูลส่วนบุคคลและการรักษาความปลอดภัยของแอพพลิเคชั่นทั้งหมดตามที่ระบุ

(ข) รายละเอียดผลการตรวจสอบและประเมินความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

(ค) รายงานสรุปผู้บริหาร (Management Summary Report) พร้อมกับเป็นผู้รายงานผลการดำเนินการให้แก่ผู้บริหารและผู้ที่เกี่ยวข้อง ตามที่สำนักงานกำหนด

4. หลักฐานการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องเสนอเอกสารหลักฐานยื่นมาพร้อมการเสนอราคาโดยแยกเป็น 2 ส่วน ดังต่อไปนี้

4.1 ส่วนที่ 1 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) ในกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคล

(ก) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคลที่มีระยะเวลาไม่เกิน 90 วัน นับถึงวันที่ยื่นข้อเสนอ บัญชีรายชื่อหุ้นส่วนผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี) พร้อมรับรองสำเนาถูกต้อง

(ข) บริษัทจำกัดหรือบริษัทมหาชนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคลที่มีระยะเวลาไม่เกิน 90 วัน นับถึงวันที่ยื่นข้อเสนอ หนังสือบริคณห์สนธิ บัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุม(ถ้ามี) บัญชีผู้ถือหุ้นรายใหญ่ (ถ้ามี) พร้อมรับรองสำเนาถูกต้อง

(2) ในกรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาหรือคณะบุคคลที่ไม่ใช่นิติบุคคลให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้นั้น สำเนาข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน หรือสำเนาหนังสือเดินทางของผู้เป็นหุ้นส่วนที่มิได้ถือสัญชาติไทย พร้อมทั้งรับรองสำเนาถูกต้อง

(3) ในกรณีผู้ยื่นข้อเสนอเป็นผู้ยื่นข้อเสนอร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า และเอกสารตามที่ระบุไว้ใน (1) หรือ (2) ของผู้ร่วมค้า แล้วแต่กรณี

(4) เอกสารเพิ่มเติมอื่น ๆ ได้แก่ สำเนาใบทะเบียนพาณิชย์ สำเนาทะเบียนภาษีมูลค่าเพิ่ม พร้อมทั้งรับรองสำเนาถูกต้อง

4.2 ส่วนที่ 2 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) ในกรณีที่ผู้ยื่นข้อเสนอมอบอำนาจให้บุคคลอื่นกระทำการแทนให้แนบหนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมาย จะต้องระบุในหนังสือมอบอำนาจให้ชัดเจนว่ามีอำนาจในการเสนอราคาแทนหรือทำการในเรื่องใด โดยมีหลักฐานแสดงตัวตนของผู้มอบอำนาจและผู้รับมอบอำนาจ (แนบสำเนาบัตรประจำตัวประชาชนผู้มอบอำนาจและผู้รับมอบอำนาจพร้อมรับรองสำเนาถูกต้อง) ทั้งนี้ หากผู้รับมอบอำนาจเป็นบุคคลธรรมดาต้องเป็นผู้ที่บรรลุนิติภาวะตามกฎหมายแล้วเท่านั้น

(2) ผู้ยื่นข้อเสนอต้องจัดทำตารางเปรียบเทียบคุณสมบัติของผู้ยื่นเสนอราคา รายละเอียดคุณลักษณะเฉพาะที่ กบข. ต้องการ และการรับประกัน (ถ้ามี) ตาม TOR นี้ กับข้อเสนอของผู้ยื่นข้อเสนอ ซึ่งคุณลักษณะเฉพาะจะต้องระบุหัวข้อให้ถูกต้องตรงกันกับเอกสารหรือแคตตาล็อกที่เสนอโดยให้จัดทำในรูปแบบดังต่อไปนี้

ลำดับ	ข้อกำหนดตาม TOR	ความสอดคล้อง	รายละเอียดข้อเสนอ	เอกสารอ้างอิง
	▪ คัดลอกคุณสมบัติของผู้ยื่นข้อเสนอ ▪ คัดลอกข้อกำหนดรายละเอียดคุณลักษณะเฉพาะของงานตามที่กำหนดใน TOR ▪ คัดลอกการรับประกัน	▪ ตรงหรือดีกว่าข้อกำหนดตาม TOR	▪ ระบุคุณสมบัติผู้ยื่นข้อเสนอราคา ▪ ระบุรายการและรายละเอียดคุณลักษณะเฉพาะของงานที่เสนอมาให้พิจารณา ▪ ระบุรายละเอียดการรับประกันงานที่เสนอมาให้พิจารณา	▪ ระบุเลขหน้าของเอกสารอ้างอิงหรือแคตตาล็อก

5. การเสนอราคา

5.1 ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอและเสนอราคาโดยไม่มีเงื่อนไขใด ๆ ทั้งสิ้น

5.2 ราคาที่เสนอจะต้องเป็นราคาที่รวมภาษีมูลค่าเพิ่ม ภาษีอื่น (ถ้ามี) รวมค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว

5.3 ผู้ยื่นข้อเสนอต้องยืนราคาเป็นเวลาไม่น้อยกว่า 90 วัน นับตั้งแต่วันที่เสนอราคา โดยภายในกำหนดยืนราคา ผู้ยื่นข้อเสนอจะต้องรับผิดชอบราคาที่ตนเสนอไว้และถอนการเสนอราคามิได้

5.4 ผู้ยื่นข้อเสนอจะต้องดำเนินการให้แล้วเสร็จภายใน 120 วันนับตั้งแต่วันที่ลงนามในสัญญา

6. **หลักเกณฑ์และสิทธิในการพิจารณา**

การพิจารณาผลการยื่นข้อเสนอครั้งนี้ กบข. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์คะแนนรวมด้านคุณภาพและด้านราคาสูงที่สุด (Price Performance) ในการพิจารณาผู้ชนะการยื่นข้อเสนอ กบข. จะพิจารณาโดยให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนด ดังต่อไปนี้

(1) ราคาที่ยื่นข้อเสนอ (Price) กำหนดน้ำหนักเท่ากับร้อยละ 40

(2) ข้อเสนอด้านเทคนิค กำหนดน้ำหนักเท่ากับร้อยละ 60

โดยแบ่งหัวข้อการพิจารณาออกเป็น 2 หัวข้อย่อย ดังนี้

1) ความน่าเชื่อถือ ผลงาน และความมั่นคงของผู้ยื่นข้อเสนอ (10 คะแนน)

- เอกสารรายละเอียดของผู้ยื่นข้อเสนอ (Company Profile)
- เอกสารแสดง ผลงาน ที่สอดคล้องกับขอบเขตการดำเนินงานตาม TOR นี้

2) แผนประเมินประสิทธิภาพและการรักษาความปลอดภัยด้านแอพพลิเคชั่น (Application Security) (50 คะแนน) โดยแบ่งออกเป็น

- เอกสารการบริหารจัดการโครงการ (10 คะแนน)
- เอกสารแจกแจงรายละเอียดและ Timeline ของโครงการ (10 คะแนน)
- รายละเอียดการจัดเตรียมเจ้าหน้าที่ตามตำแหน่งหน้าที่เพื่อดำเนินการตามแผนงาน (10 คะแนน)
- รายละเอียดเจ้าหน้าที่ประจำผู้มีความชำนาญ ประวัติการศึกษาและประกาศนียบัตรของผู้ดำเนินการที่บอกถึงระดับของความรู้และประสบการณ์ที่เกี่ยวข้อง (20 คะแนน)

7. การทำสัญญาจ้าง

ผู้ยื่นข้อเสนอที่เป็นผู้ชนะการคัดเลือกจะต้องทำสัญญาจ้างตามแบบที่ กบข. กำหนดภายใน 15 วันนัดถัดจากวันที่ได้รับแจ้งจาก กบข. และจะต้องวางหลักประกันสัญญาเป็นเงินเท่ากับร้อยละ 5 ของราคาค่าจ้าง

8. ค่าจ้างและการจ่ายเงิน

กบข. จะจ่ายค่าจ้างซึ่งได้รวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น และค่าใช้จ่ายทั้งปวงด้วยแล้ว ให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้รับจ้างภายใน 30 วัน เมื่อผู้รับจ้างได้ปฏิบัติงานถูกต้องและครบถ้วนตามสัญญาจ้างหรือข้อตกลง และ กบข. ได้ตรวจรับมอบงานจ้างเรียบร้อยแล้วพร้อมทั้ง กบข. ได้รับหนังสือเรียกเก็บเงินจากผู้รับจ้าง

9. อัตราค่าปรับ

ค่าปรับตามสัญญาจ้างหรือข้อตกลงจ้างเป็นหนังสือจะกำหนดไว้ดังต่อไปนี้

9.1 กรณีที่ผู้รับจ้างนำงานที่รับจ้างไปจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจาก กบข. จะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนร้อยละ 10 ของวงเงินของงานจ้างช่วงนั้น

9.2 กรณีที่ผู้รับจ้างปฏิบัติผิดสัญญาจ้างนอกเหนือจากข้อ 10.1 จะกำหนดค่าปรับเป็นรายวันในอัตราร้อยละ 0.1 ของราคาค่าจ้าง แต่จะต้องไม่ต่ำกว่าวันละ 100 บาท

10. การรับประกันความชำรุดบกพร่อง

ผู้ยื่นข้อเสนอที่เป็นผู้ชนะการคัดเลือกจะต้องรับประกันความชำรุดบกพร่องของงานที่เกิดขึ้นเป็นระยะเวลาไม่น้อยกว่า 1 ปี

11. วงเงินในการจัดจ้าง

วงเงินในการจัดจ้างครั้งนี้เป็นเงิน 799,000 บาท (เจ็ดแสนเก้าหมื่นเก้าพันบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น และค่าใช้จ่ายทั้งปวงด้วยแล้ว

12. ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่น ๆ

ผู้รับจ้างและบุคลากรของผู้รับจ้างที่มาปฏิบัติงานตาม TOR นี้ จะต้องรักษาข้อมูลที่เป็นความลับของ กบข. รายละเอียดดังนี้

1. ข้อมูลที่เป็นความลับ

“**ข้อมูลที่เป็นความลับ**” หมายความถึง ข้อมูลใด ๆ ที่สามารถสื่อความหมายได้ที่ กบข. หรือพนักงานของ กบข. ซึ่งต่อไปจะเรียกว่า “ผู้ให้ข้อมูล” ได้เปิดเผยให้แก่ผู้รับจ้าง ลูกจ้าง หรือผู้แทนของผู้รับจ้าง ซึ่งต่อไปจะเรียกว่า “ผู้รับข้อมูล” ทราบ และมีความประสงค์ให้ผู้รับข้อมูลเก็บรักษาข้อมูลดังกล่าวไว้เป็นความลับ

2. **การเปิดเผยและการรักษาข้อมูลที่เป็นความลับ**

ผู้รับข้อมูลตกลงจะเก็บรักษาข้อมูลที่เป็นความลับเป็นระยะเวลาหนึ่งปีนับแต่วันที่สัญญาสิ้นสุดลงโดยผู้รับข้อมูลตกลงที่จะดำเนินการดังต่อไปนี้

(1) เก็บรักษาข้อมูลที่เป็นความลับไว้ในสถานที่ปลอดภัยและไม่เปิดเผยข้อมูลที่เป็นความลับไม่ว่าทั้งหมดหรือแต่บางส่วนให้แก่บุคคลใดทราบ เว้นแต่จะเป็นการเปิดเผยข้อมูลที่เป็นความลับให้แก่บุคคลที่ต้องเกี่ยวข้องโดยตรงกับข้อมูลที่เป็นความลับนั้นและผู้รับข้อมูลจะต้องจัดให้บุคคลนั้นได้ผูกพันและปฏิบัติตามเงื่อนไขในการรักษาข้อมูลที่เป็นความลับด้วย หรือเป็นกรณีที่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ให้ข้อมูล

(2) ใช้ข้อมูลที่เป็นความลับเพียงเพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนดไว้ในสัญญาเท่านั้น

(3) ในกรณีที่ผู้รับข้อมูลมีเหตุผลความจำเป็นต้องเปิดเผยข้อมูลที่เป็นความลับโดยกฎหมายหรือตามคำสั่งศาล ผู้รับข้อมูลจะต้องแจ้งเป็นหนังสือให้ผู้ให้ข้อมูลทราบถึงข้อกำหนดหรือคำสั่งดังกล่าวก่อนที่จะดำเนินการเปิดเผยข้อมูลที่เป็นความลับ และในการเปิดเผยข้อมูลที่เป็นความลับ ผู้รับข้อมูลจะต้องดำเนินการตามขั้นตอนทางกฎหมายเพื่อขอให้คุ้มครองข้อมูลดังกล่าวไม่ให้ถูกเปิดเผยต่อสาธารณะด้วย

3. วิธีปฏิบัติเมื่อสัญญาสิ้นสุดลง

เมื่อสัญญาสิ้นสุดลง ผู้รับข้อมูลจะต้องส่งมอบข้อมูลที่เป็นความลับและสำเนาของข้อมูลที่เป็นความลับ (ถ้ามี) คืนให้แก่ผู้ให้ข้อมูล หรือทำลายข้อมูลที่เป็นความลับที่ได้รับจากผู้ให้ข้อมูลทั้งหมดและแจ้งยืนยันเป็นลายลักษณ์อักษรถึงการทำลายดังกล่าวให้ผู้ให้ข้อมูลทราบ ตลอดจนยุติการใช้ข้อมูลที่เป็นความลับ

13. มาตรการป้องกันการทุจริตและประพฤติมิชอบ

ด้วย กบข. มีนโยบายต่อต้านการทุจริตและประพฤติมิชอบที่บั่นทอนเศรษฐกิจและสังคมของประเทศ กบข. ไม่ยอมรับการทุจริตและประพฤติมิชอบทุกรูปแบบ (Zero Tolerance) ไม่ว่าจะเป็นการกระทำโดยบุคลากรของ กบข. หรือบริษัทในเครือของ กบข. หรือบุคคลที่เกี่ยวข้องกับกิจการของ กบข. ซึ่งรวมถึงคู่ค้าของ กบข. ทุกราย นอกจากนี้ กบข. ยังยึดมั่นในการดำเนินธุรกิจอย่างมีจริยธรรม จรรยาบรรณ และรับผิดชอบต่อสังคมและผู้มีส่วนได้เสียทุกกลุ่มด้วย

กบข. จึงขอความร่วมมือจากผู้ยื่นข้อเสนอ หากพบเห็นการกระทำของบุคลากรของ กบข. หรือบริษัทในเครือของ กบข. หรือบุคคลที่เกี่ยวข้องกับกิจการของ กบข. หรือคู่ค้าของ กบข. รายใดที่มีการกระทำเข้าข่ายทุจริต ติดสินบน หรือเรียกรับเงิน ทรัพย์สินหรือประโยชน์อื่นใดที่ไม่เหมาะสม ไม่ว่าในรูปแบบใด ขอให้แจ้งโดยตรงไปยังบุคคลและที่อยู่ดังต่อไปนี้

“ประธานอนุกรรมการตรวจสอบ
ฝ่ายตรวจสอบภายใน กองทุนบำเหน็จบำนาญข้าราชการ
เลขที่ 990 อาคารอับดุลราฮิม เพลส ถนนพระราม 4
แขวงสีลม เขตบางรัก กรุงเทพมหานคร 10500”

14. ผู้จัดทำขอบเขตของงาน (Terms of Reference : TOR)

1. นายพีรทัศน์ นามสกุล กวินธนานันท์
