กองทุนบำเหน็จบำนาญข้าราชการ

ขอบเขตของงาน (Terms of Reference : TOR)
การจ้างผู้ให้บริการเฝ้าระวังภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Monitoring) ผ่านระบบเครือข่ายสื่อสารและอินเทอร์เน็ต

---

1. หลักการและเหตุผล

กองทุนบำเหน็จบำนาญข้าราชการ (กบข.) ได้ว่าจ้างผู้ให้บริการเฝ้าระวังภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Monitoring) ผ่านระบบเครือข่ายสื่อสารและอินเทอร์เน็ต อย่างต่อเนื่องเพื่อให้การบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ตของ กบข. มีความมั่นคงปลอดภัยที่ได้ตามมาตรฐานระดับสากลและพร้อมใช้งานอย่างมีประสิทธิภาพตลอดเวลา รวมทั้งสามารถรับมือภัยคุกคามเทคโนโลยีสารสนเทศรูปแบบใหม่ที่ทันสมัยได้อย่างทันท่วงที และสามารถแก้ไขเหตุการณ์ภัยคุกคามต่อความมั่นคงปลอดภัยด้านสารสนเทศแก่ กบข. ได้อย่างเหมาะสมหากมีการตรวจพบ กบข. จึงเห็นควรขอจ้างผู้ให้บริการเฝ้าระวังภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Monitoring) ผ่านระบบเครือข่ายสื่อสารและอินเทอร์เน็ต โดยติดตั้งระบบแล้วเสร็จพร้อมให้บริการไม่เกินวันที่ 15 กรกฎาคม 2563 ระยะเวลาสัญญา 1 ปี เริ่มตั้งแต่วันที่ 16 กรกฎาคม 2563 ถึงวันที่ 15 กรกฎาคม 2564

2. วัตถุประสงค์

เพื่อว่าจ้างผู้ให้บริการเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยด้านสารสนเทศผ่านระบบเครือข่ายสื่อสารและอินเทอร์เน็ต (IT Security Monitoring) เพื่อปฏิบัติงานดังต่อไปนี้

2.1 วิเคราะห์ เฝ้าระวัง และแจ้งเตือนภัยคุกคาม และ/หรือเหตุการณ์ผิดปกติอันอาจก่อให้เกิดความเสียหายอย่างรุนแรงกับข้อมูลและระบบสารสนเทศของ กบข. ผ่านระบบเครือข่ายสื่อสารและอินเทอร์เน็ต ให้เป็นไปอย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัยเป็นไปตามมาตรฐานสากลและสามารถรับมือภัยคุกคามเทคโนโลยีสารสนเทศรูปแบบใหม่ที่ทันสมัยได้อย่างทันท่วงที

2.2 ให้การสนับสนุนด้านเทคนิคแก่ กบข. เยี่ยงมืออาชีพในการเฝ้าระวังภัยคุกคามต่อความมั่นคงปลอดภัยด้านสารสนเทศและการแจ้งเตือนเหตุการณ์ผิดปกติทางด้านบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต ตลอดจนให้คำแนะนำด้านเทคนิคแก่ กบข. ในการแก้ไขเหตุการณ์ภัยคุกคามต่อความมั่นคงปลอดภัยด้านสารสนเทศแก่ กบข. หากมีการตรวจพบหรือตามที่ร้องขอด้วย

3. คุณสมบัติผู้ยื่นข้อเสนอ

ผู้ยื่นข้อเสนอต้องมีคุณสมบัติตามมาตรฐานที่ระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic GovernmentProcurement : e-GP) กำหนด

4. รายการรายละเอียดของงานจ้าง

4.1 รายการอุปกรณ์ระบบเครือข่ายสื่อสารและอินเทอร์เน็ต ภายใต้เงื่อนไขและข้อกำหนดการให้บริการ “วิเคราะห์ เฝ้าระวังภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Monitoring)” ประกอบด้วย 45 รายการ ดังต่อไปนี้

4.1.1 อุปกรณ์ Firewall (Active/Standby จำนวน 3 รายการ)

4.1.2 อุปกรณ์ Internet Proxy จำนวน 1 รายการ

4.1.3 เครื่องแม่ข่าย (Server) ทำหน้าที่ให้บริการ Web application จำนวน 23 รายการ โดยผู้ให้บริการต้องทำงานร่วมกับบริการ และ/หรือ ระบบ Web Application Firewall ที่ กบข. ใช้งานอยู่ในปัจจุบัน

4.1.4 เครื่องแม่ข่าย (Server) ทำหน้าที่ให้บริการ Advanced Endpoint Protection จำนวน 1 รายการ

4.1.5 เครื่องแม่ข่าย (Server) ทำหน้าที่ให้บริการ Active Directory จำนวน 5 รายการ

4.1.6 ระบบเครือข่ายไร้สาย (Wireless LAN) จำนวน 2 รายการ

4.1.7 เครื่องแม่ข่าย (Server) ทำหน้าที่ให้บริการ MS Office 365 จำนวน 6 รายการ

4.1.8 เครื่องแม่ข่าย (Server) ทำหน้าที่ให้บริการ DNS จำนวน 3 รายการ

4.1.9 อุปกรณ์ Load Balance จำนวน 1 รายการ

4.2 ผู้ให้บริการต้องตรวจสอบและตั้งค่า Configuration ตามรายการอุปกรณ์ระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ตที่กำหนดไว้ในข้อ 4.1 และติดตั้งใช้งานอุปกรณ์หรือโปรแกรมที่เกี่ยวข้องให้มีการส่งข้อมูลจราจรทางคอมพิวเตอร์ (Logs) จากเครื่องและอุปกรณ์ดังกล่าวไปยังระบบ Security Operation Center (SOC) ของผู้ให้บริการได้อย่างครบถ้วนสมบูรณ์ โดยติดตั้งระบบแล้วเสร็จพร้อมให้บริการไม่เกินวันที่ 15 กรกฎาคม 2563

4.3 ผู้ให้บริการต้องให้บริการเฝ้าระวังภัยคุกคาม วิเคราะห์ความเกี่ยวโยงของเหตุการณ์และภัยคุกคามด้านความปลอดภัยสารสนเทศ (IT Security Monitoring Services) จากข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของอุปกรณ์ต่าง ๆ ของ กบข. ที่เกี่ยวข้อง ทุกวันตลอด 24 ชั่วโมง และดำเนินการแจ้งเตือนเกิดเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตาม Service Level Agreement (SLA) ที่กำหนด รวมทั้งให้คำแนะนำด้านเทคนิคในการแก้ไขเหตุการณ์ภัยคุกคามดังกล่าวแก่ กบข. ตลอดระยะเวลาสัญญา ตามเงื่อนไขต่อไปนี้

ระดับความรุนแรง	การแจ้งเตือนผ่าน e-mail หรือโทรศัพท์	ให้คำแนะนำในการแก้ไข
Critical	ติดต่อกลับภายใน 30 นาที	ดำเนินการร่วมแก้ไขภายใน 4 ชั่วโมง
High	ติดต่อกลับภายใน 60 นาที	ดำเนินการร่วมแก้ไขภายใน 1 วันทำการ
Medium	ติดต่อกลับภายใน 3 ชั่วโมง หลังจากตรวจพบ	ดำเนินการร่วมแก้ไขภายใน 7 วันทำการ
Low	ติดต่อกลับภายใน 1 วัน หลังจากตรวจพบ	ดำเนินการร่วมแก้ไขภายใน 30 วันทำการ

ตามระดับความรุนแรงของปัญหา โดยแบ่งเป็น 4 ระดับดังต่อไปนี้

Critical ผลกระทบกับกลุ่มระบบสารสนเทศที่ให้บริการทางอินเทอร์เน็ต (Web Site) และระบบย่อยสำหรับสนับสนุนการดำเนินงานของระบบงานอื่น ๆ (Infrastructure System) เช่น Firewall,

Active Directory เป็นต้น ตามที่ กบข. กำหนด ซึ่งไม่สามารถใช้งานได้ทั้งหมด หรือหน้าที่หลักของระบบทำงานไม่ถูกต้อง และไม่สามารถหา Workaround เพื่อแก้ปัญหาเฉพาะหน้าได้

HIGH ผลกระทบกับระบบสารสนเทศ ทำให้ไม่สามารถใช้งานได้ หรือหน้าที่หลักของระบบทำงานไม่ถูกต้องและมีผลกระทบสูง แต่สามารถหา Workaround เพื่อแก้ปัญหาเฉพาะหน้าได้

MEDIUM ผลกระทบกับระบบสารสนเทศ แม้ว่ายังสามารถใช้งานได้ แต่การทำงานในส่วนที่ไม่ใช่หน้าที่หลักของระบบไม่ถูกต้อง และมีผลกระทบต่ำ

LOW ผลกระทบกับระบบสารสนเทศ แม้ว่ายังสามารถใช้งานได้ แต่มีข้อผิดพลาดที่ไม่มีผลกระทบต่อการทำงานหลัก หรือก่อให้เกิดความไม่สะดวกในการปฏิบัติงาน

4.4 ผู้ให้บริการต้องให้บริการเฝ้าระวัง วิเคราะห์และแบ่งประเภทภัยคุกคามด้านเทคโนโลยีสารสนเทศและระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้น โดยแบ่งเป็น 6 ประเภทดังต่อไปนี้

ระดับความรุนแรง	ประเภทภัยคุกคาม	คำอธิบาย
MEDIUM	**1. ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)**	ภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ไม่ประสงค์ดี (Scanning)
HIGH	**2. ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)**	ภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ (CVE- Common Vulnerabilities and Exposures)
Critical	**3. การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)**	ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต
HIGH	**4. การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability)**	ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่างๆของระบบไม่สามารถให้บริการได้ตามปกติ
Critical	**5. การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security)**	ภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized

		Access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized modification) ได้
LOW	**6. โปรแกรมไม่พึงประสงค์ (Malicious Code)**	ภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบ (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบ

4.5 ผู้ให้บริการต้องจัดให้มีทีมงานที่มีความรู้ความสามารถในด้านการวิเคราะห์ เฝ้าระวัง และแจ้งเตือนภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Monitoring) และทีมผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศอื่น ๆ ที่เกี่ยวข้อง เพื่อให้คำปรึกษาด้านเทคนิคแก่ กบข. หากมีการตรวจพบหรือตามที่ร้องขอ ตลอดระยะเวลาสัญญา

4.6 ผู้ให้บริการต้องจัดให้มีทีมงานสนับสนุนด้านการค้นคว้าและติดตามข้อมูลข่าวสารเกี่ยวกับความปลอดภัยเทคโนโลยีสารสนเทศ (Security Research Team) เพื่ออัพเดทข้อมูลข่าวสาร หรือข่าวสารที่ทันสมัย และ/หรือภัยคุกคามร้ายแรงด้านความปลอดภัยสารสนเทศให้แก่ กบข. อย่างสม่ำเสมอ ตลอดระยะเวลาสัญญา

4.7 ผู้ให้บริการต้องเก็บรวบรวมข้อมูลจราจรและแจ้งเตือนภัยคุกคาม และ/หรือ เหตุการณ์ผิดปกติทางด้านบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต ตามรายการอุปกรณ์ระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต ที่กำหนดไว้ในข้อ 4.1 ของขอบเขตงานที่ว่าจ้าง

4.8 ผู้ให้บริการต้องให้บริการเฝ้าระวังภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร และ/หรือเหตุการณ์ผิดปกติทางด้านบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต วิเคราะห์ความเกี่ยวโยงของเหตุการณ์และภัยคุกคามด้านความปลอดภัยสารสนเทศ (IT Security Monitoring) และต้องมีการวิเคราะห์แบบรวมศูนย์และเงื่อนไขการโจมตี (Correlation and Use case) เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคามด้วยรูปแบบและมาตรฐานของผู้รับจ้างอ้างอิง มาตรฐาน NIST Incident Categories เป็นอย่างน้อยบริการเฝ้าระวังและแจ้งเตือนภัยคุกคามด้วยรูปแบบเงื่อนไขเฉพาะ หรือเงื่อนไขอื่น ๆ เพิ่มเติมพิเศษให้เหมาะสมกับ กบข. (Custom Use case) ตามที่ผู้ว่าจ้างกำหนด จากข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของอุปกรณ์ต่าง ๆ ของ กบข. ตามที่กำหนดไว้ ทุกวันตลอด 24 ชั่วโมง ตลอดจนแจ้งเตือน กบข. กรณีเกิดเหตุการณ์ผิดปกติหรือภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารตาม Service Level Agreement (SLA) ที่กำหนดในข้อ 4.3 และ 4.4 ของขอบเขตงานที่ว่าจ้าง รวมทั้งให้คำแนะนำด้านเทคนิคในการแก้ไขเหตุการณ์ภัยคุกคามดังกล่าวแก่ กบข. หากมีการตรวจพบหรือตามที่ร้องขอ ตลอดระยะเวลาสัญญา

4.9 ต้องมี Use Case ที่ใช้สำหรับเฝ้าระวังภัยคุกคาม โดยต้องสามารถตรวจจับเหตุการณ์ต่าง ๆ ที่เกิดขึ้นกับอุปกรณ์ที่กำหนดไว้ในข้อ 4.1

4.10 ผู้ให้บริการต้องเตรียมข้อมูลสำหรับให้กบข. เพื่อนำไปออกแบบแสดงภาพรวมของสถานะการณ์ความปลอดภัย โดยข้อมูลจะต้องปรับรูปแบบให้เหมาะสมกับหน้าที่และบทบาทที่ต่างกันของผู้ใช้งาน เช่น ผู้บริหาร, เจ้าหน้าที่ปฏิบัติการ เป็นต้น หรือมีเครื่องมือที่สามารถจัดการในส่วนของ Dashboard ที่สามารถแสดงภาพรวมของสถานะการณ์ความปลอดภัย ซึ่งสามารถปรับแต่งรูปแบบการแสดงผลให้เหมาะสมกับหน้าที่และบทบาทที่ต่างกันของผู้ใช้งาน เช่น ผู้บริหาร, เจ้าหน้าที่ปฏิบัติการ เป็นต้น

4.11 ผู้ให้บริการจัดทำแผนการจัดการและแจ้งเตือนภัยคุกคาม (Incident Handling) พร้อมทั้งระบบบันทึกรายงานและแสดงสถานะการแก้ไขและรายงานผลการแก้ไขปัญหา

4.12 ผู้ให้บริการต้องจัดทำรายงานประจำวัน (Daily Report), รายงานประจำเดือน (Monthly Report), รายงานสรุปรายไตรมาสหรือทุกรอบระยะเวลา 3 เดือน (Quarterly Report) และรายงานสรุปประจำปี (Yearly Report) และนำส่งรายงานให้แก่ กบข. ภายในระยะเวลาที่กำหนด โดยมีรายงานอย่างน้อยดังต่อไปนี้

4.12.1 รายงานประจำวัน (Daily Report)

ผู้ให้บริการต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ กบข. ผ่านช่องทาง E-mail หรือ Shared File Cloud Services หรือช่องทางอื่นใดที่ กบข. กำหนด โดยจัดส่งให้แก่ กบข. ภายในเวลา 7.30 น. ของทุกวัน โดยมีรายละเอียดของรายงานเป็นอย่างน้อย ครอบคลุมถึง

(ก) สรุปเหตุการณ์ที่ตรวจพบพฤติกรรมภาพรวมภัยคุกคามที่เกิดขึ้นและระดับความรุนแรง
- ระบุประเภทของภัยคุกคาม
- วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม
- ระบุต้นทาง (Attacker) และปลายทาง (Target)
- ระบุระดับความรุนแรง (Severity)

(ข) ภาพการเชื่อมโยงเหตุการณ์ภัยคุกคามที่เกิดขึ้น

(ค) รายละเอียดเหตุการณ์และพฤติกรรมทั้งหมด

(ง) คำแนะนำและขั้นตอนการดำเนินการแก้ไขด้านเทคนิค Action & Recommendation

4.12.2 รายงานประจำเดือน (Monthly Report)

ผู้ให้บริการต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ กบข. ผ่านช่องทาง e-mail หรือช่องทางอื่นใดที่ กบข. กำหนด ภายในวันที่ 5 ของเดือนถัดไป โดยมีรายละเอียดของรายงานเป็นอย่างน้อย ครอบคลุมถึง

(ก) บทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security Monitoring) ในแต่ละเดือน

(ข) สรุปเหตุการณ์ภัยคุกคามคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่เกิดขึ้นในแต่ละเดือน โดยมีการจัดระดับความรุนแรง และวิเคราะห์ผลกระทบต่อการดำเนินธุรกิจของ กบข.

(ค) สรุปการแจ้งเตือนเหตุการณ์ผิดปกติหรือภัยคุกคามคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตาม Service Level Agreement (SLA) และสรุปสถานะการดำเนินการบริหารจัดการภัยคุกคามที่พบหรือความผิดปกติที่กระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Incident Management) ที่เกิดขึ้นในแต่ละเดือน

(ง) อัพเดทข้อมูลข่าวสารเกี่ยวกับภัยคุกคามร้ายแรงด้านความปลอดภัยสารสนเทศ (Security News) ที่เกิดขึ้นในแต่ละเดือน (ถ้ามี)

4.12.3 รายงานสรุปรายไตรมาส หรือทุกรอบระยะ 3 เดือน (Quarterly Report)

ผู้ให้บริการต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ กบข. ผ่านช่องทาง e-mail หรือช่องทางอื่นใดที่ กบข. กำหนด ภายใน 15 วัน นับจากวันที่สิ้นสุดไตรมาส หรือรอบระยะเวลาทุก 3 เดือน โดยมีรายละเอียดของรายงานเป็นอย่างน้อย ครอบคลุมถึง

(ก) บทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security Monitoring) ในแต่ละไตรมาส หรือทุกรอบระยะเวลา 3 เดือน

(ข) สรุปเหตุการณ์ภัยคุกคามคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่เกิดขึ้นในแต่ละไตรมาส หรือทุกรอบระยะเวลา 3 เดือน โดยมีการจัดระดับความรุนแรง และวิเคราะห์ผลกระทบต่อการดำเนินธุรกิจของ กบข.

(ค) อัพเดทข้อมูลข่าวสารเกี่ยวกับภัยคุกคามร้ายแรงด้านความปลอดภัยสารสนเทศ (Security News) ที่เกิดขึ้นในแต่ละไตรมาส หรือทุกรอบระยะวเลา 3 เดือน (ถ้ามี)

4.12.4 รายงานสรุปประจำปี (Yearly Report)

ผู้ให้บริการต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ กบข. ผ่านช่องทาง e-mail หรือช่องทางอื่นใดที่ กบข. กำหนด ภายใน 20 วัน นับจากวันสิ้นปี โดยมีรายละเอียดของรายงานเป็นอย่างน้อย ครอบคลุมถึง

(ก) บทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security Monitoring) โดยสรุปเป็นภาพรวมทั้งปี

(ข) สรุปเหตุการณ์ภัยคุกคามคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่เกิดขึ้นทั้งหมดภายในปี โดยมีการจัดระดับความรุนแรง และวิเคราะห์ผลกระทบต่อการดำเนินธุรกิจของ กบข.

(ค) สรุปการดำเนินการแจ้งเตือนเกิดเหตุการณ์ภัยคุกคามคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตาม Service Level Agreement และรายงานสถานะการดำเนินการบริหารจัดการภัยคุกคามที่พบหรือความผิดปกติที่กระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Incident Management) ที่เกิดขึ้นเป็นภาพรวมทั้งปี

(ง) อัพเดทข้อมูลข่าวสารเกี่ยวกับภัยคุกคามร้ายแรงด้านความปลอดภัยสารสนเทศ (Security News) และสรุปแนวโน้ม หรือ Trend ของภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร และ ข้อแนะนำที่ กบข. ควรดำเนินการเพื่อรับมือกับภัยคุกคามเหล่านั้น

4.13 ผู้ให้บริการต้องวิเคราะห์ปัญหาที่เกิดจากภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร หากถูกตรวจพบ โดยให้คำปรึกษาและวิเคราะห์เชิงลึก (Incident Report) แก่ กบข. ในการจัดการหรือแก้ไขเหตุการณ์ภัยคุกคามดังกล่าว พร้อมทั้งแนวทางในการป้องกันปัญหาทางด้านความปลอดภัยที่อาจเกิดขึ้นได้อีกในอนาคต

4.14 ผู้ให้บริการต้องดำเนินการเข้ารหัสข้อมูลระหว่างการจัดส่งข้อมูลจาก กบข. ไปยังศูนย์จัดเก็บข้อมูล (Security Operation Center) ของผู้ให้บริการ ให้เป็นไปตามมาตรฐานด้านความปลอดภัยที่ กบข. กำหนด

4.15 ผู้ให้บริการต้องจัดเก็บข้อมูลจราจรไว้ในที่ปลอดภัย เป็นระยะเวลาไม่น้อยกว่า 90 วัน หรือตามระยะเวลาขั้นต่ำที่กฎหมายกำหนด เป็นอย่างน้อย

4.16 ผู้ให้บริการต้องสำรองข้อมูลสำคัญ (Backup Log) ที่เกี่ยวข้องกับการให้บริการตามขอบเขตงานที่ว่าจ้าง อย่างน้อย 1 สำเนา โดยจัดเก็บไว้ที่ศูนย์สำรองข้อมูลของผู้ให้บริการ ซึ่งผ่านการรับรองมาตรฐานสากลด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

4.17 ผู้ให้บริการต้องตรวจสอบสถานะการส่งข้อมูลจราจรทางคอมพิวเตอร์จาก กบข. พร้อมทั้งแจ้งเตือนมายังเจ้าหน้าที่ผู้รับผิดชอบของ กบข. ผ่านทางอีเมล์ ในกรณีที่อุปกรณ์ตามที่ระบุในข้อ 4.1 ดังกล่าวไม่อาจส่งข้อมูลมายังสถานที่จัดเก็บข้อมูลของผู้ให้บริการได้ ภายในระยะเวลา 4 ชั่วโมงนับแต่เกิดเหตุการณ์ขึ้น

4.18 ผู้ให้บริการต้องให้คำปรึกษาด้านเทคนิคแก่ กบข. หรือเจ้าหน้าที่ผู้รับผิดชอบของ กบข. ผ่านทางอีเมล์และโทรศัพท์ได้ทุกวัน ตลอด 24 ชั่วโมง ตลอดระยะเวลาสัญญา

4.19 ผู้ให้บริการต้องให้บริการเฝ้าระวังความพร้อมใช้งานและแจ้งเตือนหากเกิดเหตุการณ์ผิดปกติทางด้านบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายและอินเทอร์เน็ต ที่กำหนดไว้ในข้อ 4.1 เช่น แจ้งเตือนสถานะ Up/Down ของ Firewall หรือ Server เป็นต้น

4.20 รองรับกับการเชื่อมต่อและจัดทำกลไกหรือขั้นตอนการเฝ้าระวังและรับมือกับภัยคุกคามไซเบอร์ทั้งระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤต โดยมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานกลาง และใช้ในการประสานงานกับ ThaiCERT, TB-CERT, หน่วยงานควบคุมและกำกับดูแลที่เกี่ยวข้องตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

5. หลักฐานการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องเสนอเอกสารหลักฐานยื่นมาพร้อมการเสนอราคาโดยแยกเป็น 2 ส่วน ดังต่อไปนี้

5.1 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

5.2 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

6. การเสนอราคา

6.1ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอและเสนอราคาโดยไม่มีเงื่อนไขใด ๆ ทั้งสิ้น

6.2 ราคาที่เสนอจะต้องเป็นราคาที่รวมภาษีมูลค่าเพิ่ม ภาษีอื่น (ถ้ามี) รวมค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว

6.3 ผู้ยื่นข้อเสนอต้องยืนราคาเป็นเวลาไม่น้อยกว่า 90 วัน นับตั้งแต่วันที่เสนอราคา โดยภายในกำหนดยืนราคา ผู้ยื่นข้อเสนอจะต้องรับผิดชอบราคาที่ตนเสนอไว้และถอนการเสนอราคามิได้

6.4 ผู้ยื่นข้อเสนอจะต้องติดตั้งระบบแล้วเสร็จพร้อมให้บริการไม่เกินวันที่ 15 กรกฎาคม 2563 ระยะเวลาสัญญา 1 ปี เริ่มตั้งแต่วันที่ 16 กรกฎาคม 2563 ถึงวันที่ 15 กรกฎาคม 2564

6.5 กรณีงานจัดจ้างที่ประกอบด้วยพัสดุหลายประเภทในโครงการเดียวกัน ผู้เสนอราคาต้องแยกราคาต่อหน่วยของพัสดุแต่ละประเภท (**cost breakdown)** ให้ชัดเจน (ถ้ามี)

7. **หลักเกณฑ์และสิทธิในการพิจารณา**

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

(1) ราคาที่ยื่นข้อเสนอ (Price) กำหนดน้ำหนักเท่ากับร้อยละ 40

(2) ข้อเสนอด้านเทคนิค กำหนดน้ำหนักเท่ากับร้อยละ 60

โดยแบ่งหัวข้อการพิจารณาออกเป็น 4 หัวข้อย่อย ดังนี้

1) ความน่าเชื่อถือ ผลงาน และความมั่นคงของผู้ยื่นข้อเสนอ (10 คะแนน)

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

2) แผนดำเนินการบริหารจัดการเฝ้าระวังตามมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (10 คะแนน)

- เอกสารการบริหารโครงการติดตั้งระบบฯ
- เอกสารแสดงแผนผัง Network Diagram หรืออุปกรณ์ที่จะออกแบบให้ กบข.
- รายละเอียดการจัดเตรียมเจ้าหน้าที่ตามตำแหน่งหน้าที่ของผู้ติดตั้งระบบฯเพื่อดำเนินการตามแผนงาน
- รายละเอียดเจ้าหน้าที่ประจำผู้มีความชำนาญ ประวัติการศึกษาและประกาศนียบัตรของผู้ติดตั้งระบบฯบอกถึงระดับของความรู้และประสบการณ์ที่เกี่ยวข้อง

3) คุณลักษณะของบริการวิเคราะห์ เฝ้าระวัง และแจ้งเตือนภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Monitoring ตามที่กำหนดไว้ใน TOR นี้ รวมทั้งรายละเอียดของเทคนิคที่ใช้ในการให้บริการ (20 คะแนน)

- รายละเอียดแสดงกระบวนการหรือเทคนิคการจัดการข้อมูลการจราจรคอมพิวเตอร์และการเฝ้าระวังตามมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ กบข.

- ตัวอย่างเอกสารรายงานบทสรุปผู้บริหาร รายงานประจำวัน (Daily Report), รายงานประจำเดือน (Monthly Report), รายงานสรุปรายไตรมาส หรือทุกรอบระยะเวลา 3 เดือน (Quarterly Report) และรายงานสรุปประจำปี (Yearly Report)

4) รายละเอียดการบริการและความพร้อมให้บริการ (Service Availability) (20 คะแนน)

- เอกสารรายละเอียดบริการแจ้งเหตุขัดข้องระบบฯ
- เอกสารที่แสดงถึงการกำหนดข้อตกลงความพร้อมให้บริการ (Service Availability)
- รายละเอียดการจัดเตรียมเจ้าหน้าที่ตามตำแหน่งหน้าที่ของผู้ให้บริการบำรุงรักษาเพื่อดำเนินการตามแผนงาน
- รายละเอียดเจ้าหน้าที่ผู้ให้บริการบำรุงรักษาประจำ ผู้มีความชำนาญ ประวัติการศึกษาและประกาศนียบัตร บอกถึงระดับของความรู้และประสบการณ์ที่เกี่ยวข้อง

การทำสัญญาจ้าง

ผู้ชนะการคัดเลือกจะต้องทำสัญญาจ้างตามแบบที่ กบข. กำหนดภายใน 15 วัน นัดถัดจากวันที่ได้รับแจ้งจาก กบข. และจะต้องวางหลักประกันสัญญาเป็นเงินเท่ากับร้อยละ 5 ของราคาค่าจ้าง

8. ค่าจ้างและการจ่ายเงิน

<u>สำหรับการจ้างที่จ่ายค่าจ้างให้ผู้รับจ้างแบ่งเป็นงวด</u>

กบข. จะจ่ายค่าจ้างซึ่งได้รวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น และค่าใช้จ่ายทั้งปวงด้วยแล้ว ให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้รับจ้างภายใน 30 วัน เมื่อผู้รับจ้างได้ปฏิบัติงานถูกต้องและครบถ้วนตามสัญญาจ้างหรือข้อตกลง และ กบข. ได้ตรวจรับมอบงานจ้างเรียบร้อยแล้วพร้อมทั้ง กบข. ได้รับหนังสือเรียกเก็บเงินจากผู้รับจ้าง โดยแบ่งการจ่ายเงินออกเป็น 4 งวด ดังต่อไปนี้

งวดที่ 1 เป็นจำนวนเงินร้อยละ 25 ของค่าจ้าง เมื่อผู้รับจ้างได้ปฏิบัติงาน บริการเฝ้าระวังภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Monitoring) ผ่านระบบเครือข่ายสื่อสารและอินเทอร์เน็ต ตามเงื่อนไขและข้อกำหนดของ TOR นี้แก่ กบข. เป็นระยะเวลา 3 เดือน (ประจำเดือนกรกฎาคม - กันยายน 2563)

งวดที่ 2 เป็นจำนวนเงินร้อยละ 25 ของค่าจ้าง เมื่อผู้รับจ้างได้ปฏิบัติงาน บริการเฝ้าระวังภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Monitoring) ผ่านระบบเครือข่ายสื่อสารและอินเทอร์เน็ต ตามเงื่อนไขและข้อกำหนดของ TOR นี้แก่ กบข. เป็นระยะเวลา 3 เดือน (ประจำเดือนตุลาคม - ธันวาคม 2563)

งวดที่ 3 เป็นจำนวนเงินร้อยละ 25 ของค่าจ้าง เมื่อผู้รับจ้างได้ปฏิบัติงาน บริการเฝ้าระวังภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Monitoring) ผ่านระบบเครือข่ายสื่อสารและอินเทอร์เน็ต ตามเงื่อนไขและข้อกำหนดของ TOR นี้แก่ กบข. เป็นระยะเวลา 3 เดือน (ประจำเดือนมกราคม - มีนาคม 2564)

งวดที่ 4 (งวดสุดท้าย) เป็นจำนวนเงินร้อยละ 25 ของค่าจ้าง เมื่อผู้รับจ้างได้ปฏิบัติงานทั้งหมดให้แล้วเสร็จเรียบร้อยตามสัญญาหรือข้อตกลงเป็นหนังสือ และ กบข. ได้ตรวจรับมอบงานจ้างเรียบร้อยแล้ว

ผู้รับจ้างจะต้องทำข้อมูลเปรียบเทียบงานที่ส่งมอบแต่ละงวดงานกับงานตามที่สัญญากำหนดว่าส่งมอบได้ครบถ้วนหรือไม่ โดยให้จัดทำในรูปแบบ ดังต่อไปนี้

ลำดับ	ข้อกำหนดตาม TOR	ความสอดคล้อง	รายละเอียดของงานที่ส่งมอบ	เอกสารอ้างอิง
	▪ คัดลอกข้อกำหนดรายละเอียดคุณลักษณะเฉพาะของงานตามที่กำหนดใน TOR ▪ คัดลอกการรับประกัน	▪ ตรงหรือดีกว่าข้อกำหนดตาม TOR	▪ ระบุรายการและรายละเอียดคุณลักษณะเฉพาะของงานที่ส่งมอบ ▪ ระบุรายละเอียดการรับประกันงานที่ส่งมอบ	▪ ระบุเลขหน้าของเอกสารอ้างอิงหรือแคตตาล็อก

10. อัตราค่าปรับ

ค่าปรับตามสัญญาจ้างหรือข้อตกลงจ้างเป็นหนังสือจะกำหนดไว้ดังต่อไปนี้

10.1 กรณีที่ผู้รับจ้างนำงานที่รับจ้างไปจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจาก กบข. จะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนร้อยละ 10 ของวงเงินของงานจ้างช่วงนั้น

10.2 กรณีที่ผู้รับจ้างปฏิบัติผิดสัญญาจ้างนอกเหนือจากข้อ 10.1 จะกำหนดค่าปรับเป็นรายวันในอัตราร้อยละ 0.1 ของราคาค่าจ้าง แต่จะต้องไม่ต่ำกว่าวันละ 100 บาท

11. การรับประกันความชำรุดบกพร่อง

ผู้ชนะการคัดเลือกจะต้องรับประกันความชำรุดบกพร่องของงานที่เกิดขึ้นเป็นระยะเวลาไม่น้อยกว่า 1 ปี และตั้งแต่วันที่ 16 กรกฎาคม 2563 จนถึงวันที่ 15 กรกฎาคม 2564

12. วงเงินในการจัดจ้าง

วงเงินในการจัดจ้างครั้งนี้เป็นเงิน 2,800,000 บาท (สองล้านแปดแสนบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น และค่าใช้จ่ายทั้งปวงด้วยแล้ว

13. 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

14. 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”

15. ผู้จัดทำขอบเขตของงาน (Terms of Reference : TOR)

1. นายวัชรพงศ์ นามสกุล ชัยกิจ
