ข้อกำหนดและขอบเขตงานงานด้านเทคนิค

โครงการจ้างตรวจสอบและประเมินความปลอดภัยระบบเทคโนโลยีสารสนเทศ ประจำปี 2563

1. หลักการและเหตุผล

บริษัทหลักทรัพย์จัดการกองทุน กรุงไทย จำกัด (มหาชน) มีความประสงค์ที่ตรวจสอบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศจากผู้เชี่ยวชาญภายนอก เพื่อประเมินสถานะความมั่นคงปลอดภัยด้านสารสนเทศ ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามด้านไซเบอร์ รวมถึงการเตรียมความพร้อมในการรับมือกับภัยคุกคามที่เกิดขึ้นได้ ดังนั้นบริษัทฯ จึงต้องการจ้างผู้รับจ้างจากภายนอกมาดำเนินการทดสอบเจาะระบบและหาจุดอ่อนของระบบพร้อมวิเคราะห์และให้คำแนะนำในการปิดช่องโหว่และตรวจสอบผลการปิดช่องโหว่เหล่านั้น เพื่อป้องกันไม่ให้เกิดความเสียหายต่อข้อมูลของลูกค้าหรือระบบเทคโนโลยีของบริษัทฯ

2. ขอบเขตงานงานด้านเทคนิค

2.1 ผู้รับจ้างจะต้องดำเนินการเจาะระบบจากเครือข่ายภายนอกด้วยวิธี External Black-Box Penetration testing เพื่อนำเอาข้อมูลสำคัญ เช่น บัญชีผู้ดูแลระบบพร้อมทั้งรหัสผ่าน หรือบัญชีผู้ใช้พร้อมรหัสผ่าน หรือข้อมูลอื่นๆ ที่มีความสำคัญ รวมถึงการกระทบใดๆ ที่อาจทำให้บริษัทฯ ได้ทราบถึงความเสี่ยงจากการถูกเจาะระบบ โดยในการทดสอบเจาะระบบจะดำเนินการเหมือนกับการเจาะระบบของไวรัสหรือแฮกเกอร์ที่ปฏิบัติการจริง ซึ่งจะดำเนินการหาช่องทางในการเข้าถึงระบบ (Exploit) ผ่านจุดอ่อนหรือช่องโหว่ต่างๆ ของเว็บไซต์หรือโมบายแอปพลิเคชัน (ช่องโหว่ที่พบอาจเป็น zero-day ที่ยังไม่พบการแจ้งเตือนจากผู้ให้บริการ (Vendor)) โดยครอบคลุมระบบงานเป้าหมายดังต่อไปนี้

- 2.1.1 หน้าเว็บไซต์ที่ให้บริการข้อมูลข่าวสาร www.ktam.co.th (https://www.ktam.co.th)
- 2.1.2 หน้าเว็บไซต์ที่ให้บริการข้อมูลข่าวสารการจัดซื้อจัดจ้าง (http://procurement.ktam.co.th/procurement/)
- 2.1.3 ช่องทางการเชื่องต่อที่ให้บริการข้อมูลข่าวสารบนไลน์แพลตฟอร์ม (API) (https://line.ktam.co.th/)
- 2.1.4 หน้าเว็บไซต์ที่ให้บริการเชื่อมต่อ VPN ของบริษัท (https://center.ktam.co.th/)
- 2.1.5 หน้าเว็บไซต์ที่ให้บริการ Virtual Application ของบริษัท (https://Mobile.ktam.co.th/)

2.2 การดำเนินการทดสอบการเจาะระบบจากเครือข่ายภายนอกบริษัทฯ External Penetration Testing ในรูปแบบ Black-Box จะต้องเลือกใช้วิธีการที่เป็นไปตามมาตรฐานอย่างน้อยได้แก่

- 2.2.1 Open Source Security Testing Methodology (OSSTM) หรือ
- 2.2.2 NIST SP800-115 Guideline on Network Security Testing หรือ
- 2.2.3 Open Web Application Security Project (OWASP) TOP 10 หรือ
- 2.2.4 Penetration Testing Framework (PTF).

2.3 ผู้รับจ้างจะต้องดำเนินการค้นหาจุดอ่อนหรือช่องโหว่ ประเมินความเสี่ยงและผลกระทบ (Vulnerability Assessment) จำนวนไม่เกิน 100 IP Address พร้อมทั้งจัดทำข้อเสนอแนะแนวทางแก้ไขระบบสารสนเทศและระบบที่เกี่ยวข้อง

2.4 ในการดำเนินการค้นหาจุดอ่อนหรือช่องโหว่ ประเมินความเสี่ยงและผลกระทบ (Vulnerability Assessment) ผู้รับจ้างต้องดำเนินการโดยยึดตามมาตรฐานไม่ต่ำกว่า SANS Top 20 Most Dangerous Software Errors โดยครอบคลุมในระดับต่างๆ ดังนี้

2.4.1 ระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย (Server Operating Systems)

2.4.2 อุปกรณ์เครือข่ายสื่อสาร (Network Equipment)

2.4.3 อุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Equipment)

2.5 ในการค้นหาจุดอ่อนหรือช่องโหว่ ประเมินความเสี่ยงและผลกระทบ (Vulnerability Assessment) ผู้รับจ้างจะต้องดำเนินการโดยใช้โปรแกรมหรือซอฟท์แวร์ที่เป็นแบบ Commercial ที่มีความน่าเชื่อถือและเป็นโปรแกรมที่ผู้รับจ้างมีลิขสิทธิ์ถูกต้อง

2.6 การดำเนินการทดสอบการเจาะระบบจากเครือข่ายภายนอกบริษัทฯ External Penetration Testing ผู้รับจ้างจะต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเองด้วย (Manual Test) มิให้ใช้เครื่องมืออัตโนมัติ (Automatic Test Tool) เพียงอย่างเดียว

2.7 การดำเนินการทดสอบการเจาะระบบจากเครือข่ายภายนอกบริษัทฯ External Penetration Testing ผู้รับจ้างต้องแต่งตั้งผู้แทนอย่างน้อยหนึ่งคนเพื่อรับผิดชอบและควบคุมการดำเนินงาน รวมทั้งเป็นผู้ติดต่อประสานงานระหว่างบริษัทฯ กับผู้รับจ้าง

2.8 บริษัทฯ มีสิทธิที่จะตรวจสอบประวัติของบุคคลที่ผู้รับจ้างแต่งตั้งเป็นผู้แทนได้

2.9 ผู้รับจ้างจะต้องจัดทำแผนประเมินความเสี่ยง พร้อมทั้งหาวิธีรับมือกับความเสี่ยงหรือผลกระทบนั้นๆ ก่อนการดำเนินการทดสอบเจาะระบบ หรือการค้นหาจุดอ่อนหรือช่องโหว่

2.10 ผู้รับจ้างจะต้องแจ้งพนักงานผู้มีหน้าที่รับผิดชอบของบริษัทฯ ให้ทราบทุกครั้งก่อนดำเนินงานทดสอบเจาะระบบ โดยผู้รับจ้างจะต้องแจ้งบริษัทฯ ทราบล่วงหน้าอย่างน้อย 1 วันทำการและจะดำเนินการได้หลังจากที่ได้รับความเห็นชอบทุกครั้ง

2.11 ผู้รับจ้างจะต้องจัดให้มีการประชุมเพื่อรายงานผลและความคืบหน้าของโครงการต่อบริษัทฯ เป็นระยะเวลาที่ชัดเจนอย่างต่อเนื่องจนกระทั่งสิ้นสุดงานจ้าง

2.12 ผู้รับจ้างต้องนำเสนอรายงานผลการดำเนินการ รายละเอียดช่องโหว่หรือจุดอ่อนที่พบ รวมถึงปริมาณช่องโหว่ของระบบ ความเสี่ยงที่พบ และผลกระทบที่อาจเกิดขึ้นอย่างละเอียดพร้อมแนวทางการแก้ไข รวมถึงเวลาโดยประมาณในการแก้ไขต่อบริษัทฯ

2.13 ผู้รับจ้างจะต้องรับผิดชอบในการให้คำแนะนำแนวทางการปิดช่องโหว่ ที่อาจส่งผลกระทบต่อระดับความปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ ให้กับผู้ดูแลและผู้พัฒนาระบบของบริษัท ฯ ภายหลังจากการทดสอบการเจาะระบบ และการประเมินความเสี่ยง รวมถึงให้คำแนะนำแนวทางการปรับปรุงความมั่นคงปลอดภัยของระบบให้เป็นไปอย่างเหมาะสม

2.14 บริษัทฯ จะเป็นผู้ดำเนินการแก้ไขและปิดช่องโหว่ที่พบ ตามคำแนะนำและวิธีการที่ผู้รับจ้างได้นำเสนอ

2.15 หลังจากที่บริษัทฯ ดำเนินการปิดช่องโหว่ตามข้อ 2.14 แล้ว ผู้รับจ้างจะต้องดำเนินการตรวจสอบผลการแก้ไข การปิดช่องโหว่หรือจุดอ่อนอีกครั้ง เพื่อยืนยันช่องโหว่ที่พบว่าได้รับการแก้ไขแล้ว

2.16 หากในข้อ 2.15 ผู้รับจ้างตรวจสอบและยังพบช่องโหว่หรือจุดอ่อนเดิมที่ได้รายงานและแก้ไขไปแล้ว ให้ถือเป็นความรับผิดชอบของบริษัทฯ ที่ต้องดำเนินการหาทางแก้ไขให้แล้วเสร็จ หรือวางแผนเพื่อลดความเสี่ยง

2.17 ในกรณีที่มีระบบใดๆ ที่บริษัทฯ ไม่สามารถดำเนินการปิดช่องโหว่ตามคำแนะนำการปิดช่องโหว่ของผู้รับจ้างที่ได้แจ้ง ไว้ในข้อ 2.14, 2.15 และ 2.16 ได้ ให้ถือเป็นความรับผิดชอบของผู้รับจ้างในการที่จะต้องช่วยวิเคราะห์ และแนะนำหาแนวทางการแก้ไขอื่นๆ ที่จะสามารถลดผลกระทบหรือลดความเสี่ยงของช่องโหว่นั้นๆ ให้แก่บริษัทฯ เพื่อดำเนินการต่อไป

2.18 ผู้รับจ้างจะต้องรวบรวมและจัดทำรายงานการทดสอบเจาะระบบทั้งก่อนและหลังการแก้ไข รวมถึงบทวิเคราะห์คำแนะนำการแก้ไขและบทสรุปผู้บริหาร โดยจัดทำเป็นเอกสารพร้อมส่งทั้งแบบ Hardcopy และ Softcopy เพื่อนำเสนอผู้บริหารของบริษัทฯ

2.19 ในการดำเนินการใดๆ ผู้รับจ้างจะต้องปฏิบัติตามนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทฯ

2.20 ในการดำเนินงานของผู้รับจ้างจะต้องไม่ส่งผลกระทบหรือสร้างความเสียหายต่อระบบงานของบริษัทฯ หากมีความเสียหายใดๆ อันเกิดจากการดำเนินการของผู้รับจ้าง ผู้รับจ้างจะต้องรายงานให้บริษัทฯ ได้ทราบในทันทีและจะต้องเป็นผู้รับผิดชอบต่อความเสียหายนั้น โดยความเสียหายที่เกิดขึ้นจริงนั้น ต้องมีการตรวจสอบว่าความเสียหายนั้นเกิดจากการกระทำของผู้รับจ้างจริง รวมถึงผู้รับจ้างจะต้องทำให้ระบบงานที่เสียหายหรือได้รับผลกระทบนั้นกลับใช้งานได้เป็นปกติดังเดิมภายในระยะอันรวดเร็ว โดยไม่มีค่าใช้จ่ายใดๆ ทั้งสิ้น

2.21 ผู้รับจ้างต้องทำหนังสือรับรองเพื่อยืนยันต่อบริษัทฯ ว่า ซอฟต์แวร์ทุกประเภทที่นำมาใช้กับงานของบริษัทฯ ในครั้งนี้ ไม่มีโปรแกรมแอบแฝงหรือโปรแกรมมุ่งประสงค์ร้ายที่ไม่ได้เกี่ยวข้องกับการทำทดสอบเจาะระบบ และผู้รับจ้างจะต้องเป็นผู้รับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นจากการนำเอาโปรแกรมเหล่านั้นมาใช้ในงานดังกล่าว

2.22ผู้รับจ้างจะต้องใช้เอกสารข้อมูล เครื่องมือ ฮาร์ดแวร์และซอฟท์แวร์ต่างๆ ในการดำเนินการอย่างถูกต้องตามกฎหมาย ไม่ละเมิดลิขสิทธิ์หรือสิทธิบัตรของผู้อื่น ในกรณีเอกสาร ข้อมูล เครื่องมือฮาร์ดแวร์ และซอฟท์แวร์ต่างๆ ที่ผู้รับจ้างนำมาใช้ในการดำเนินการเป็นการละเมิดลิขสิทธิ์หรือสิทธิบัตรของผู้อื่น ผู้รับจ้างต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายที่เกี่ยวกับหรือเกี่ยวเนื่องกับกรณีดังกล่าวทั้งสิ้นให้แก่บริษัทฯ และ/หรือบุคคลภายนอกผู้ถูกละเมิดนั้น

2.23 ผู้รับจ้างจะต้องจัดทำสัญญาไม่เปิดเผยข้อมูลพร้อมลงนามให้แก่บริษัทฯ และบริษัทฯ ขอสงวนสิทธิ์ในข้อมูลทั้งหมดของโครงการนี้ ทั้งระบบงานและเอกสารทั้งหมดที่จัดทำขึ้นจะถือเป็นลิขสิทธิ์ของบริษัทฯ

2.24ผู้รับจ้างจะไม่นำเอกสารและข้อมูลใดๆ ที่ได้รับหรือจัดทำขึ้นเกี่ยวกับระบบนี้ไปทำการเปิดเผยโดยไม่ได้รับความเห็นชอบอย่างเป็นทางการจากบริษัทฯ

2.25ผู้รับจ้างมีหน้าที่ในการเก็บรักษาข้อมูลที่ได้รับจากบริษัทฯ และข้อมูลที่เกี่ยวข้องกับบริษัทฯ ตลอดจนรายงานผลการทดสอบเจาะรบบไว้เป็นความลับ ทั้งในระหว่างระยะเวลาสัญญารับจ้างและสิ้นสุดการรับจ้าง

2.26ผู้รับจ้างจะต้องเป็นผู้จัดหาสื่อเก็บข้อมูลที่เหมาะสมและปลอดภัย หากจำเป็นที่จะต้องนำข้อมูลออกจากบริษัทฯ

2.27 ผู้รับจ้างห้ามนำอุปกรณ์ประมวลผลที่ไม่ใช่ของบริษัทฯ มาต่อเข้าระบบเครือข่ายภายในของบริษัทฯ เว้นแต่ได้รับอนุญาตจากหน่วยงานของบริษัทฯ ที่ควบคุมดูแลการทำงาน

2.28 ผู้รับจ้างต้องยินยอมให้บริษัทฯ มีสิทธิในการเข้าตรวจสอบการทำงานจนกระทั่งสิ้นสุดงานจ้าง

2.29 หากส่วนหนึ่งส่วนใดที่มิได้ระบุไว้ในเอกสารนี้ แต่มีความจำเป็นต้องจัดทำ หรือจัดหาเพื่อให้งานแล้วเสร็จ ผู้รับจ้างต้องจัดทำ หรือจัดหามาให้เพียงพอต่อการใช้งานของบริษัทฯ

3. คุณสมบัติด้านการบริหารจัดการและประสบการณ์ของผู้เสนอราคา

3.1 ผู้รับจ้างจะต้องเป็นนิติบุคคลที่จดทะเบียนในประเทศไทย ซึ่งประกอบธุรกิจเกี่ยวกับการเป็นที่ปรึกษาหรือผู้ตรวจประเมินความมั่นคงปลอดภัยด้านสารสนเทศ หรือดำเนินการทดสอบความแข็งแกร่งของระบบสารสนเทศมาแล้วเป็นเวลาไม่น้อยกว่า 3 ปี รวมถึงเป็นคู่สัญญาโดยตรงแก่หน่วยงานที่เป็นส่วนราชการ องค์การ เทศบาล รัฐวิสาหกิจ หรือ เอกชนในประเทศไทยที่น่าเชื่อถือ โดยผลงานนั้นต้องเป็นผลงานในระยะเวลาไม่เกิน 3 ปี นับจากวันที่เสนอราคา โดย จะต้องมีราคางานในสัญญาเดียวไม่ต่ำกว่า 475,000.00 บาท (สี่แสนเจ็ดหมื่นห้าพันบาทถ้วน) รวมภาษีมูลค่าเพิ่ม

3.2 กรณีผู้รับจ้างผ่านการรับรอง (Certified) จากหน่วยงานที่เป็นมาตรฐานสากลอย่างน้อยดังนี้ จะได้รับการพิจารณาเป็นพิเศษ

3.2.1 ISO/IEC 27001:2013 Information security management systems โดยขอบเขตของ ISO จำเป็นต้องครอบคลุมในการทดสอบเจาะระบบและการเก็บข้อมูลลูกค้า หรือ

3.2.2 ISO 9001:2015 Quality management systems โดยขอบเขตของ ISO จำเป็นต้องครอบคลุมในการทดสอบเจาะระบบและการเก็บข้อมูลลูกค้า หรือ

3.2.3 Certificate อื่นๆที่เกี่ยวข้องกับการดำเนินงาน

4. คุณสมบัติด้านบุคลากรของผู้เสนอราคา

ผู้รับจ้างจะต้องมีบุคลากรที่ความรู้และความสามารถด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ อย่างน้อย ดังนี้

4.1 มีประสบการณ์ไม่น้อยกว่า 3 ปี ในงานด้านการหาช่องโหว่หรือทดสอบเจาะระบบ

4.2 มีใบประกาศนียบัตรหรือหนังสือรับรอง (Certificate) ที่เป็นมาตรฐานและเป็นของเฉพาะบุคคล โดยหน่วยงานในระดับสากล ตรงตามหน้าที่ที่ได้รับของบุคลากรนั้น และยังมีผลบังคับใช้ต่อบุคลากรดังกล่าว อย่างน้อยดังนี้

4.2.1 Certified Information Systems Security Professional (CISSP) จาก (ISC)2 และ

4.2.2 Offensive Security Certified Professional (OSCP) หรือ

4.2.3 GCCC: GIAC Critical Controls หรือ Certification GIAC: GPEN (Penetration Testing Certification) หรือ GWAPT (Web application penetration tester certification) หรือ GXPN (GIAC Exploit Researcher and Advanced Penetration Tester) หรือ

4.2.4 Certified Ethical Hacker (C|EH) จาก EC-council หรือ

4.2.5 Certificate อื่นๆที่เทียบเท่าในด้านการ Pentest

4.3 ผู้รับจ้างจะต้องมีบุคลากรที่เคยได้รับรางวัล จากการเข้าร่วมแข่งขันหาช่องโหว่หรือทดสอบเจาะระบบ ในรายการระดับสากลหรือระดับประเทศ เข้าร่วมการทดสอบเจาะระบบในโครงการ

4.4 การเปลี่ยนแปลงตัวบุคลากรที่รับผิดชอบดังกล่าวข้างต้นในภายหลัง จะทำได้ก็ต่อเมื่อได้แจ้งให้บริษัทฯ ทราบเป็นหนังสือ และได้รับความเห็นชอบจากบริษัทฯ แล้ว โดยผู้เข้ามาแทนที่จะต้องมีคุณสมบัติไม่น้อยกว่าผู้ที่ตนจะเข้ามาแทนที่ด้วย

5. ระยะเวลาดำเนินการและส่งมอบงาน

5.1 ผู้รับจ้างจะต้องดำเนินงานตามขอบเขตงานที่ว่าจ้างให้แล้วเสร็จและส่งมอบงานภายในระยะเวลา 120 วัน นับแต่วันที่ลงนามสัญญาจ้าง

6. การยื่นเอกสาร

ในการยื่นข้อเสนอผู้เสนอราคาจะต้องยื่นข้อเสนอโดยไม่มีเงื่อนไขใด ๆ ทั้งสิ้น พร้อมด้วยเอกสารหลักฐานโดยผู้มีอำนาจของบริษัทลงลายมือชื่อรับรองสำเนาถูกต้องทุกฉบับ ปิดผนึกซองแยกดังนี้

ซองที่ 1 เอกสารประกอบคุณสมบัติผู้เสนอราคา ประกอบด้วย

(1) สำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล ที่คัดถ่ายจากกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ไม่เกิน 6 เดือน นับถึงวันที่ยื่นเอกสารเสนอราคา สำเนาบริคณห์สนธิ บัญชีรายชื่อกรรมการผู้จัดการ/หุ้นส่วนผู้จัดการ รายชื่อผู้มีอำนาจควบคุม (ถ้ามี) บัญชีรายชื่อผู้ถือหุ้นรายใหญ่ สำเนาหนังสือจดทะเบียนพาณิชย์ สำเนาใบทะเบียนภาษีมูลค่าเพิ่ม

(2) ในกรณีผู้ประสงค์จะเสนอราคาร่วมกันในฐานะเป็นกลุ่มนิติบุคคลซึ่งรวมกันเป็นผู้ร่วมค้า (Consortium) ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้าด้วย

(3) หนังสือมอบอำนาจ (ในกรณีที่ผู้เสนอราคามอบอำนาจให้บุคคลอื่นดำเนินการแทน)

(4) สำเนาบัตรประชาชนผู้มีอำนาจลงนาม

(5) สำเนาสัญญาหรือหนังสือรับรองผลงาน รายละเอียดตามข้อ 3.1

ซองที่ 2 เงื่อนไขทางเทคนิค

(1) เอกสาร Proposal แสดงรายละเอียดนำเสนอโครงการ

(2) หลักฐานใบประกาศนียบัตรหรือหนังสือรับรอง (Certificate) รายละเอียดตามข้อ 3.1 (ถ้ามีจะได้รับพิจารณาเป็นพิเศษ)

(3) รายชื่อบุคคลากรและใบประกาศนียบัตรหรือหนังสือรับรอง (Certificate) รายละเอียดตามข้อ 4.1 และ 4.2

(4) หลักฐานการได้รับรางวัล จากการเข้าร่วมแข่งขันหาช่องโหว่หรือทดสอบเจาะระบบ รายละเอียดตามข้อ 4.3

ซองที่ 3 เอกสารด้านราคา ประกอบด้วย

(1) ใบเสนอราคา แยกรายการค่าวัสดุอุปกรณ์ ค่าแรง และค่าดำเนินการออกจากกันอย่างชัดเจน

ทั้งนี้ ผู้เสนอราคาจะต้องกำหนดยืนราคาไม่น้อยกว่า 90 วัน นับแต่ยื่นเอกสารเสนอราคา โดยภายในกำหนดยืนราคา ผู้เสนอราคารับผิดชอบราคาที่ได้เสนอไว้และจะถอนการเสนอราคามิได้

7. เงื่อนไขการจ่ายเงิน

บริษัทฯ จะจ่ายเงินทั้งหมด หลังจากบริษัทตรวจรับงานที่ผู้ให้บริการส่งมอบตามที่กำหนดเรียบร้อยแล้ว ภายใน 30 วัน (สามสิบ) นับแต่วันที่ได้รับเอกสารเรียกเก็บเงินจากผู้รับจ้าง