ขอบเขตงาน (Term of Reference)
จ้างที่ปรึกษาเพื่อตรวจสอบและติดตามการดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
(ISO/IEC ๒๗๐๐๑ Surveillance Audit)

๑. หลักการและเหตุผล

ด้วยสำนักเทคโนโลยีสารสนเทศ สำนักงาน กสทช. ได้มีการดำเนินโครงการจัดจ้างที่ปรึกษาเพื่อพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ ให้กับสำนักเทคโนโลยีสารสนเทศ ซึ่งจะได้รับการรับรองตามมาตรฐานดังกล่าว ในปลายปี ๒๕๖๒ อย่างไรก็ตาม ตามวงรอบของการรับรองจะต้องมีการตรวจติดตามจากรอบการรับรองแรก อีก ๒ ครั้ง เรียกว่ารอบ Surveillance Audit จึงจะครบหนึ่งวงรอบของการรับรองตามมาตรฐาน ด้วยเหตุดังกล่าว สำนักเทคโนโลยีสารสนเทศ จึงมีความจำเป็นต้องจัดจ้างที่ปรึกษาเพื่อเข้ามาดำเนินการติดตามการดำเนินงานของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และมีการจัดจ้างผู้ตรวจรับรองเข้ามาตรวจรับรองตามรอบการตรวจติดตามดังกล่าว และเพื่อเป็นการเพิ่มประสิทธิภาพและประสิทธิผลในการดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยอย่างต่อเนื่อง อีกทั้งสอดคล้องตามกฎหมาย ดังต่อไปนี้ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ภายใต้ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ สำนักเทคโนโลยีสารสนเทศจึงมีความประสงค์จัดจ้างที่ปรึกษาเพื่อตรวจสอบและติดตามการดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ Surveillance Audit รอบที่ ๑ ให้กับสำนักเทคโนโลยีสารสนเทศ โดยมีรายละเอียดการจ้างงานตามหัวข้อต่อไปนี้

๒. วัตถุประสงค์

จ้างที่ปรึกษาเพื่อดำเนินการทบทวน แก้ไข ปรับปรุง และตรวจติดตามระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของศูนย์คอมพิวเตอร์ (Data Center) ของสำนักเทคโนโลยีสารสนเทศ สำนักงาน กสทช. ให้เป็นไปตามข้อกำหนดมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๑๓ เพื่อให้การปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศมีความสอดคล้องเหมาะสมและเป็นไปตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง และเป็นการสร้างความเชื่อมั่นและภาพลักษณ์ที่ดีแก่สำนักงาน กสทช. จากการได้รับใบรับรองตามมาตรฐานสากลที่เป็นที่ยอมรับ

๓. คุณสมบัติที่ปรึกษา

๓.๑. ต้องเป็นบุคคล หรือนิติบุคคลที่ประกอบอาชีพเป็นที่ปรึกษาในสาขาที่จ้างและขึ้นทะเบียนเป็นที่ปรึกษากับศูนย์ข้อมูลที่ปรึกษาไทย กระทรวงการคลัง สาขามาตรฐานคุณภาพ (QS) : Quality Standard Sector ความเชี่ยวชาญ R๑๒๐: มาตรฐานระบบรักษาความปลอดภัยของข้อมูลองค์กร

๓.๒. มีความสามารถตามกฎหมาย

๓.๓. ไม่เป็นบุคคลล้มละลาย

๓.๔. ไม่อยู่ในระหว่างการเลิกกิจการ

๓.๕. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอ หรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๖. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๗. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับที่ปรึกษาอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน กสทช. ณ วันเสนอราคาหรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการเสนอราคาครั้งนี้

๓.๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของที่ปรึกษาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

๓.๑๐. ไม่เป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนด

๓.๑๑. ที่ปรึกษาต้องมีประสบการณ์หรือผลงานที่เกี่ยวข้องหรือคล้ายคลึงกับลักษณะของงานหรือภารกิจตามขอบเขตของงานจ้างที่ปรึกษาเกี่ยวกับการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศจนได้รับการรับรองมาตรฐานสากล ISO/IEC ๒๗๐๐๑: ๒๐๑๓ จาก Certification Body ให้กับหน่วยงานราชการ หรือองค์กรอิสระ หรือรัฐวิสาหกิจ หรือบริษัทเอกชน ในประเทศไทย อย่างน้อย ๓ แห่ง ทั้งนี้ ผู้เสนอราคาต้องนำสำเนาสัญญาจ้าง และ สำเนาหนังสือรับรองผลงาน พร้อมทั้งชื่อและหมายเลขโทรศัพท์ มอบให้กับสำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ ณ วันยื่นข้อเสนอราคา เพื่อให้สามารถดำเนินการตรวจสอบได้

๔. ขอบเขตการดำเนินงาน

ขอบเขตของการดำเนินงานของที่ปรึกษาต้องประกอบด้วยงาน ดังต่อไปนี้

๔.๑. ดำเนินการร่วมกับคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยและบริการเทคโนโลยีสารสนเทศในการทบทวนและบำรุงรักษาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของสำนักเทคโนโลยีสารสนเทศ ในลักษณะการทำงานร่วมกับที่ปรึกษา (Co-Sourcing) เพื่อทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ โดยมีขอบเขตการดำเนินงานดังนี้

๔.๑.๑. ศึกษา และทบทวนบริบทขององค์กรทั้งภายในและภายนอก รวมถึงความคาดหวังและความต้องการจากผู้มีส่วนได้ส่วนเสีย เพื่อนำมาทบทวนขอบเขตในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System; ISMS) และนำเสนอคณะกรรมการเพื่อพิจารณาอนุมัติ

๔.๑.๒. ทบทวนระเบียบวิธีในการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ ทบทวนเกณฑ์ที่ใช้ในการประเมินความเสี่ยง และกลยุทธ์ในการจัดการกับความเสี่ยงในระดับต่าง ๆ ให้สอดคล้องกับข้อกำหนดของมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๑๓ และสอดคล้องกับบริบทขององค์กรที่มีการเปลี่ยนแปลงไป

๔.๑.๓. ทบทวนการประเมินความเสี่ยงทรัพย์สินสารสนเทศตามขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยพิจารณาถึงการเปลี่ยนแปลงต่าง ๆ ตามบริบทขององค์กรโดยมีการระบุเหตุการณ์ภัยคุกคาม (Threats) จุดอ่อน (Vulnerabilities) และโอกาสเกิด (Likelihood) ภัยคุกคามนั้น ๆ และทบทวน ปรับปรุงรายงานผลการ

ประเมินความเสี่ยงที่และการระบุมาตรการที่ใช้งานอยู่ ให้สอดคล้องกับข้อกำหนดของมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๑๓

๔.๑.๔. ดำเนินการตรวจสอบ วิเคราะห์และประเมินช่องโหว่ด้านความมั่นคงปลอดภัย (Vulnerability Assessment Scan) ของระบบสารสนเทศตามขอบเขตหรือตามที่สำนักฯ กำหนด ไม่เกิน ๕๐ ไอพี ให้สอดคล้องกับข้อกำหนดที่ A.๑๒.๖.๑ Management of technical vulnerabilities โดยการตรวจสอบต้องดำเนินการทั้งในระดับ ระบบปฏิบัติการ (Operation System: OS) ของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์เครือข่าย (Network Device) ของสำนักงาน กสทช. รวมทั้งจัดทำรายงานผลการตรวจสอบช่องโหว่ แนวทางการป้องกัน แก้ไขช่องโหว่ที่ตรวจพบ และดำเนินการประชุมกับทีมงานผู้ดูแลระบบเพื่อนำเสนอผลการดำเนินงานทั้งหมด และดำเนินการตรวจสอบซ้ำอีก ๑ ครั้งภายหลังการนำเสนอรายงานผลการตรวจสอบในครั้งแรก พร้อมทั้งจัดทำรายงานเปรียบเทียบผลการตรวจสอบช่องโหว่ของทั้งสองครั้ง และดำเนินการประชุมกับทีมงานผู้ดูแลระบบ เพื่อนำเสนอผลการดำเนินงานทั้งหมด

๔.๑.๕. ทบทวนและปรับปรุงเอกสารแสดงมาตรการที่เลือกใช้มาตรการรักษาความมั่นคงปลอดภัยในระบบบริหารจัดการรักษาความมั่นคงปลอดภัยสารสนเทศ (Statement of Application: SoA) โดยอ้างอิงตามภาคผนวกของมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๑๓ (Annex A: Control Objectives and Controls) เช่น การทบทวนการระบุเหตุผลของการเลือกใช้มาตรการ

๔.๑.๖. ทบทวน ปรับปรุง หรือจัดทำเพิ่มเติม นโยบายและขั้นตอนปฏิบัติต่าง ๆ (Policies & Procedures) ให้สอดคล้องตามข้อกำหนดมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓

๔.๑.๗. ทบทวน ปรับปรุง แผนตัวชี้วัดเพื่อเป็นการวัดประสิทธิผลของระบบบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (Effectiveness Measurement) ให้สอดคล้องตามบริบทที่มีการเปลี่ยนแปลงไป

๔.๑.๘. ทบทวน ปรับปรุง และทดสอบ แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) ให้กับระบบสารสนเทศตามขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยพิจารณาตามบริบทขององค์กรที่มีการเปลี่ยนแปลงไป

๔.๑.๙. ให้คำปรึกษา คำแนะนำ หรือร่วมตรวจสอบกับคณะตรวจสอบภายในของสำนักเทคโนโลยีสารสนเทศ (ISMS Internal Auditor) ในการดำเนินการตรวจสอบภายในและจัดทำรายงานผลการตรวจสอบให้กับระบบบริหารจัดการความมั่นคงปลอดภัยอย่างสอดคล้องกับข้อกำหนดมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๑๓

๔.๑.๑๐. ให้คำปรึกษาและคำแนะนำในการติดตามการแก้ไขข้อบกพร่องที่ตรวจพบจากการตรวจสอบภายใน (Corrective and Preventive Actions) และจัดทำรายงานการติดตาม CAR ให้กับคณะตรวจสอบภายในของสำนักเทคโนโลยีสารสนเทศ

๔.๑.๑๑. ให้คำปรึกษาและดำเนินการเตรียมการในส่วนความรับผิดชอบของผู้บริหารเพื่อทบทวนการดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Review of ISMS) และรวบรวมรายงานการประชุมนำเสนอคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยและบริการสารสนเทศ

๔.๑.๑๒. ให้คำปรึกษา และคำแนะนำ รับผิดชอบค่าใช้จ่าย รวมทั้งให้การสนับสนุนการตรวจประเมินจาก Certification Body ในรอบการตรวจติดตามรอบที่หนึ่ง (Surveillance

Audit) ตามแผนการตรวจประเมินที่ Certification Body ออกมาให้ และติดตามรายงานผลการตรวจประเมินเบื้องต้นจาก Certification Body

๔.๑.๑๓. ให้คำปรึกษา และคำแนะนำในการแก้ไข Non conformity (NC) ที่ได้รับจากการตรวจประเมินของ Certification Body และจัดทำแผนการดำเนินการเพื่อแก้ไขและตอบ NC ให้กับ Certification Body ภายในระยะเวลาที่กำหนด รวมทั้งจัดทำรายงานแผนการดำเนินการเพื่อแก้ไขและตอบ NC

๔.๒. การดำเนินการจัดการฝึกอบรม อย่างน้อยตามหลักสูตรต่อไปนี้

๔.๒.๑. หลักสูตรข้อกำหนดมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ เพื่อทบทวนข้อกำหนด ระยะเวลาอย่างน้อย ๓ ช.ม. จำนวน ๑ ครั้ง ผู้เข้ารับการอบรมไม่ต่ำกว่า ๑๕ คน

๔.๒.๒. หลักสูตรสร้างความเข้าใจในนโยบายและขั้นตอนปฏิบัติ ตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ ระยะเวลาอย่างน้อย ๖ ช.ม. ผู้เข้ารับการอบรมไม่ต่ำกว่า ๑๐ คน

๔.๒.๓. หลักสูตรเพื่อสร้างความตระหนักเกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และเนื้อหาเกี่ยวกับ Security Awareness ให้กับบุคลากรของสำนักงาน กสทช. ระยะเวลาอย่างน้อย ๓ ชั่วโมง ผู้เข้ารับการอบรมไม่ต่ำกว่า ๗๐ คน โดยใช้สถานที่ของสำนักงาน กสทช. ในการจัดอบรม

๔.๓. ดำเนินการ บำรุงรักษา และปรับปรุงฐานข้อมูลของโปรแกรมประยุกต์ในรูปแบบของ Web-Based ที่จัดไว้ให้สำหรับสำนักเทคโนโลยีสารสนเทศใช้งาน เพื่อดำเนินการประเมินความเสี่ยงตามระเบียบวิธีการประเมินความเสี่ยงของสำนักเทคโนโลยีสารสนเทศ ขึ้นทะเบียนทรัพย์สินสารสนเทศและบริหารจัดการเอกสารในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ รวมทั้งจัดทำรายงานผลการบำรุงรักษาและการดำเนินการที่เกี่ยวข้องกับโปรแกรมประยุกต์ดังกล่าว

๕. บุคลากรของที่ปรึกษา

ที่ปรึกษาจะต้องจัดให้มีบุคลากรที่มีความรู้ความชำนาญเพื่อดำเนินงานตามขอบเขตงาน โดยมีคุณวุฒิ ประสบการณ์ และจำนวนอย่างน้อย ดังนี้

๕.๑ หัวหน้าโครงการ จำนวน ๑ คน

๕.๑.๑ จบการศึกษาอย่างน้อยในระดับปริญญาเอกในสาขาที่เกี่ยวข้องกับคอมพิวเตอร์หรือการจัดการเทคโนโลยีสารสนเทศ และมีประสบการณ์ด้านการบริหารโครงการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เป็นระยะเวลาอย่างน้อย ๑๐ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๐.๕ man-month

๕.๑.๒ ได้รับประกาศนียบัตรอย่างน้อย ดังนี้ Information Security Management System, ISO/IEC ๒๗๐๐๑:๒๐๑๓ Lead Auditor

๕.๒ ที่ปรึกษาโครงการ จำนวน ๑ คน

๕.๒.๑ จบการศึกษาอย่างน้อยในระดับปริญญาเอก และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศหรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือ การตรวจสอบด้านสารสนเทศ เป็นระยะเวลาไม่น้อยกว่า ๑๐ ปี โดยต้องมีระยะเวลาดำเนินงานอย่างน้อย ๐.๕ man-month

๕.๒.๒ ต้องได้รับประกาศนียบัตรที่เกี่ยวข้อง ได้แก่ ISO/IEC ๒๗๐๐๑:๒๐๑๓ Lead Auditor หรือ COBIT Foundation (Control Objectives for Information and Related Technology)

๕.๓ หัวหน้าทีมที่ปรึกษา ISMS จำนวน ๑ คน

๕.๓.๑ จบการศึกษาอย่างน้อยในระดับปริญญาเอก และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศหรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือ การตรวจสอบด้านสารสนเทศ เป็นระยะเวลาอย่างน้อย ๑๐ ปี โดยต้องมีระยะเวลาดำเนินงานอย่างน้อย ๒ man-month

๕.๓.๒ ได้รับประกาศนียบัตร Certified ISMS Auditor รับรองโดยสถาบัน International Register of Certificated Auditors (IRCA) ในระดับหลักสูตรไม่ต่ำกว่า ISO/IEC ๒๗๐๐๑:๒๐๑๓ Lead Auditor

๕.๔ ทีมที่ปรึกษา ISMS จำนวนอย่างน้อย ๓ คน

๕.๔.๑ จบการศึกษาอย่างน้อยในระดับปริญญาตรี และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศหรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือ การตรวจสอบด้านสารสนเทศ เป็นระยะเวลาอย่างน้อย ๕ ปี โดยต้องมีระยะเวลาดำเนินงานอย่างน้อย ๓ man-month

๕.๔.๒ ต้องเป็นพนักงานเต็มเวลาของบริษัท และทำงานกับบริษัทมาแล้วอย่างน้อยเป็นระยะเวลา ๒ ปี

๕.๔.๓ ได้รับประกาศนียบัตรที่เกี่ยวข้อง ได้แก่ ISO/IEC ๒๗๐๐๑:๒๐๑๓ Implementation หรือ ISO/IEC ๒๗๐๐๑:๒๐๑๓ Lead Auditor

๕.๕ ที่ปรึกษาการตรวจสอบภายใน ISMS จำนวน ๑ คน

๕.๕.๑ จบการศึกษาอย่างน้อยในระดับปริญญาโท และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศหรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือ การตรวจสอบด้านเทคโนโลยีสารสนเทศ เป็นระยะเวลาอย่างน้อย ๕ ปี โดยต้องมีระยะเวลาดำเนินงานอย่างน้อย ๐.๕ man-month

๕.๕.๒ ได้รับประกาศนียบัตรที่เกี่ยวข้อง ได้แก่ ISO/IEC ๒๗๐๐๑:๒๐๑๓ Internal Audit หรือ ISO/IEC ๒๗๐๐๑:๒๐๑๓ Lead Auditor

๕.๖ ทีมที่ปรึกษาด้านเทคนิค จำนวนอย่างน้อย ๑ คน

๕.๖.๑ จบการศึกษาอย่างน้อยในระดับปริญญาตรี และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศหรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือ การตรวจสอบด้านสารสนเทศ เป็นระยะเวลาอย่างน้อย ๕ ปี โดยต้องมีระยะเวลาดำเนินงานอย่างน้อย ๒ man-month

๕.๖.๒ ต้องเป็นพนักงานเต็มเวลาของบริษัท และทำงานกับบริษัทมาแล้วอย่างน้อยเป็นระยะเวลา ๒ ปี

๕.๖.๓ ได้รับประกาศนียบัตรที่เกี่ยวข้อง ได้แก่ ISO/IEC ๒๗๐๐๑:๒๐๑๓ Implementation หรือดีกว่า หรือ CompTIA Security+ หรือ CEH (Certified Ethical Hacker)

๕.๗ เจ้าหน้าที่ทดสอบระบบ จำนวนอย่างน้อย ๑ คน

๕.๗.๑ จบการศึกษาอย่างน้อยในระดับปริญญาตรี และมีประสบการณ์ในการทดสอบระบบเทคโนโลยีสารสนเทศ เป็นระยะเวลาไม่น้อยกว่า ๕ ปี โดยต้องมีระยะเวลาดำเนินงานอย่างน้อย ๑.๒๕ man-month

๖. ระยะเวลาดำเนินการ

ภายใน ๒๔๐ วัน นับถัดจากวันลงนามในสัญญา

๗. ระยะเวลาการส่งมอบงาน

ที่ปรึกษาต้องส่งมอบงานพร้อม Data Files ที่จัดเก็บในสื่อบันทึกข้อมูลชนิด Flash Drive และในรูปแบบเอกสารจำนวน ๕ ชุด โดยแบ่งออกเป็นงวดงานดังนี้

งวดที่ ๑ ส่งมอบรายงานตามข้อ ๔.๑.๑, ๔.๑.๒, ๔.๑.๓, ๔.๒.๑ ภายใน ๖๐ วัน ถัดจากวัน ลงนามในสัญญา

งวดที่ ๒ ส่งมอบรายงานตามข้อ ๔.๑.๔, ๔.๑.๕, ๔.๑.๖, ๔.๑.๗, ๔.๒.๒ ภายใน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญา

งวดที่ ๓ ส่งมอบรายงานตามข้อ ๔.๑.๘, ๔.๑.๙, ๔.๑.๑๐, ๔.๑.๑๑, ๔.๑.๑๒, ๔.๑.๑๓, ๔.๒.๓, ๔.๓ ภายใน ๒๔๐ วัน ถัดจากวันลงนามในสัญญา

๘. วงเงินที่ใช้ในการจัดหา

วงเงินรวมทั้งสิ้น ๑,๘๕๐,๐๐๐ บาท (หนึ่งล้านแปดแสนห้าหมื่นบาทถ้วน) โดยเบิกจ่ายจากงบประมาณปี ๒๕๖๓ สำนักเทคโนโลยีสารสนเทศ หมวดรายจ่ายอื่น การจ้างที่ปรึกษาเพื่อศึกษา วิจัย และประเมินผลหรือพัฒนาระบบต่างๆ การจัดจ้างที่ปรึกษาเพื่อตรวจสอบและติดตามการดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC ๒๗๐๐๑ Surveillance Audit)

๙. เงื่อนไขการจ่ายชำระเงิน

สำนักงาน กสทช. จะชำระเงินตามจำนวนในสัญญาจ้างหลังจากที่ได้ตรวจรับถูกต้องเรียบร้อยแล้ว และที่ปรึกษาปฏิบัติถูกต้องครบถ้วนตามที่สำนักงาน กสทช. กำหนด โดยจะชำระเงินตามเงื่อนไขและกำหนดเวลาการชำระเงินดังนี้

งวดที่ ๑ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๓๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ปรึกษาส่งมอบงานในงวดงานที่ ๑ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว

งวดที่ ๒ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๓๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ปรึกษาส่งมอบงานในงวดงานที่ ๒ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว

งวดที่ ๓ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๔๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ปรึกษาส่งมอบงานในงวดงานที่ ๓ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว

๑๐. การจัดทำข้อเสนอของที่ปรึกษา

ที่ปรึกษาจะต้องทำข้อเสนอโครงการเป็นภาษาไทย ประกอบด้วย เอกสารและหลักฐาน ข้อเสนอทางเทคนิค และข้อเสนอทางการเงิน โดยมีรายละเอียดข้อเสนอ ดังนี้

๑๐.๑ เอกสารและหลักฐานเกี่ยวกับผู้ยื่นข้อเสนอ ประกอบด้วย

๑๐.๑.๑ หลักฐานการจดทะเบียนเป็นนิติบุคคลที่จัดตั้งตามกฎหมายไทย ต้องมีสำเนาหรือภาพถ่ายหนังสือการรับรองการจดทะเบียนเป็นนิติบุคคลของสำนักงานทะเบียนหุ้นส่วนบริษัทกลาง หรือสำนักงานทะเบียนหุ้นส่วนบริษัทจังหวัด กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ที่แสดงว่าได้จดทะเบียนเป็นผู้มีอำนาจทำนิติกรรมแทนนิติบุคคล ทุนจดทะเบียน และวัตถุประสงค์ของนิติบุคคลฉบับที่จดทะเบียนหลังสุด ซึ่งรับรองสำเนาถูกต้องโดยผู้มีอำนาจทำนิติกรรมแทนนิติบุคคลพร้อมทั้งประทับตราสำคัญของนิติบุคคลโดยหนังสือรับรองการจดทะเบียนดังกล่าวต้องออกให้ไม่เกิน ๓ เดือน นับจากวันที่ยื่นเสนอ

๑๐.๑.๒ หลักฐานของกรรมการผู้จัดการ หรือหุ้นส่วนผู้จัดการ ต้องมีสำเนาหรือภาพถ่ายทะเบียนบ้านระบุสัญชาติของกรรมการผู้จัดการหรือหุ้นส่วนผู้จัดการซึ่งรับรองสำเนาถูกต้องโดยผู้มีอำนาจทำนิติกรรมแทนนิติบุคคล

๑๐.๑.๓ ในกรณีที่ปรึกษาเป็นส่วนงานราชการ/ สถาบันการศึกษา ให้ยื่นหนังสือมอบอำนาจของหัวหน้าส่วนราชการ/ สถาบันการศึกษา ที่ให้ผู้ใดเป็นผู้ดำเนินการ รวมทั้งหลักฐานสำเนาบัตรประชาชน บัตรราชการ พร้อมรับรองสำเนาถูกต้อง พร้อมทั้งต้องมีสำเนาภาพถ่ายหนังสือจัดตั้งหน่วยงาน รวมทั้งอำนาจหน้าที่ของหน่วยงาน ซึ่งรับรองสำเนาถูกต้องโดยผู้มีอำนาจลงนามของหน่วยงาน

๑๐.๑.๔ หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมายในกรณีที่ปรึกษามอบอำนาจให้บุคคลอื่นลงนามในเอกสารข้อเสนอแทน

๑๐.๒ ข้อเสนอทางเทคนิค

ที่ปรึกษาจะต้องจัดทำข้อเสนอด้านเทคนิคที่ประกอบด้วย

๑๐.๒.๑ ผลงานและประสบการณ์ของที่ปรึกษา

๑๐.๒.๒ คุณสมบัติ ประสบการณ์ และจำนวนของบุคลากรเข้าร่วมงาน

๑๐.๒.๓ วิธีการบริหารและวิธีการปฏิบัติงาน

๑๐.๓ ข้อเสนอทางด้านราคา

๑๐.๓.๑ ราคาที่จะเสนอจะต้องรวมถึงค่าใช้จ่ายต่าง ๆ ซึ่งรวมถึงภาษีมูลค่าเพิ่ม ภาษีเงินได้ ค่าอากรแสตมป์ ฯลฯ โดยจะต้องแสดงรายละเอียดค่าใช้จ่ายต่าง ๆ ที่จะต้องใช้ในการดำเนินการตามขอบเขตของงานแต่ละรายการตามแผนปฏิบัติการ และเสนอสรุปเป็นราคาค่าบริการทั้งหมด

๑๐.๓.๒ รายละเอียดค่าจ้างบุคลากร โดยแสดงรายละเอียดจำนวนคน-เดือน และอัตราค่าจ้างเป็นรายบุคคล และแนบหลักฐานด้านการเงิน เช่น สลิปเงินเดือน หนังสือรับรองเงินเดือน หรือสำเนาหลักฐานการชำระภาษี (ภ.ง.ด. ๙๑)

๑๐.๓.๓ รายละเอียดค่าใช้จ่ายเพิ่มเติมต่าง ๆ เช่น ค่าใช้จ่ายในการจัดประชุมกลุ่มย่อย/ประชุมเชิงปฏิบัติการ และค่าใช้จ่ายที่เกี่ยวเนื่อง เป็นต้น

๑๑. หลักเกณฑ์การพิจารณาข้อเสนอ

๑๑.๑ สำนักงาน กสทช. จะพิจารณาข้อเสนอที่ปรึกษาทุกราย เว้นแต่ที่ปรึกษาที่ยื่นเอกสารหลักฐานไม่ครบถ้วนตามข้อ ๑๐.๑ ในส่วนที่เป็นสาระสำคัญ หรือครบถ้วนแต่ไม่ถูกต้อง จะไม่รับพิจารณาข้อเสนอของที่ปรึกษารายนั้น และในการพิจารณาคัดเลือกข้อเสนอที่จะคำนึงถึง ความคุ้มค่าและวัตถุประสงค์ของงานจ้างที่ปรึกษาเป็นสำคัญ โดยพิจารณาเกณฑ์ด้านคุณภาพ เป็นลำดับแรกก่อน ดังนี้

(๑) ผลงานและประสบการณ์ของที่ปรึกษา ๑๐๐ คะแนน

ในหัวข้อนี้ จะพิจารณาการให้คะแนนในเชิงคุณภาพและเชิงปริมาณ ดังนี้

(๑) ผลงานเชิงคุณภาพ : โดยพิจารณาจากลักษณะของผลงานที่มีขอบเขตและวิธีการนำเสนอที่สอดคล้องหรือใกล้เคียงกับลักษณะงานตามขอบเขตของงานและวัตถุประสงค์มากที่สุด จำนวน ๔๐ คะแนน

(๒) ผลงานเชิงปริมาณ : โดยพิจารณาจากผลงานจำนวนผลงานและมูลค่าของผลงานที่มีลักษณะงานสอดคล้องหรือใกล้เคียงกับงานตามขอบเขตของงานโดยเทียบสัดส่วนกับจำนวนผลงานของผู้ยื่นข้อเสนอด้วยกัน จำนวน ๖๐ คะแนน

(๒) วิธีการบริหารและวิธีปฏิบัติงาน ๑๐๐ คะแนน

ในหัวข้อนี้ จะพิจารณาการให้คะแนนจากจ้อเสนอที่สามารถนำขอบเขตของงานที่กำหนดไว้มาจัดทำเป็นแผนและวิธีการดำเนินงานการตรวจสอบที่สอดคล้องกับระยะเวลาดำเนินงานของสำนักงาน กสทช. ได้ชัดเจนและเป็นรูปธรรมมากที่สุด

(๓) คุณสมบัติและจำนวนบุคลากรที่ร่วมงาน ๑๐๐ คะแนน

ในหัวข้อนี้ จะพิจารณาการให้คะแนน ดังนี้

(๑) ภาพรวมของความครบถ้วนถูกต้องของบุคลากรของที่ปรึกษาที่เสนอ โดยพิจารณาจากคุณวุฒิ ประสบการณ์ และจำนวนบุคลากรที่เสนอทั้งหมด จำนวน ๓๐ คะแนน

(๒) คุณวุฒิ และประสบการณ์ของบุคลากรแต่ละคนแต่ละระดับ โดยพิจารณาจากคุณวุฒิซึ่งไม่ต่ำกว่าที่กำหนด และมีประสบการณ์ตรงหรือใกล้เคียงกับขอบเขตของงาน มากที่สุด รวมทั้งระยะเวลาของประสบการณ์หรือจำนวนชิ้นงานที่เป็นประสบการณ์ในเรื่องนั้น ๆ จำนวน ๔๐ คะแนน โดยคุณวุฒิและประสบการณ์ที่ตรงกับที่กำหนดมากที่สุดจะได้คะแนนเต็ม สำหรับคุณวุฒิและประสบการณ์ที่มีความใกล้เคียงจะได้คะแนนลดหลั่นลงไป

(๓) จำนวนบุคลากรทั้งหมดที่เข้าดำเนินงาน โดยพิจารณาจากจำนวนขั้นต่ำ ซึ่งต้องไม่น้อยกว่าที่กำหนด หรือจำนวน man-month สอดคล้องกับระยะเวลาการทำงานของบุคลากรแต่ละคนแต่ละระดับ จำนวน ๓๐ คะแนน

ทั้งนี้ ในการพิจารณาให้คะแนนตามหัวข้อต่าง ๆ ข้างต้น สำนักงาน กสทช. จะพิจารณาเปรียบเทียบระหว่างข้อเสนอของที่ปรึกษาที่ยื่นข้อเสนอด้วยกัน ข้อเสนอของที่ปรึกษาที่ผ่านเกณฑ์การพิจารณาด้านคุณภาพจะต้องได้คะแนนประเมินในแต่ละหัวข้อหลักไม่น้อยกว่าร้อยละ ๘๐ และจัดลำดับเรียงตามคะแนน

๑๑.๒ การจ้างที่ปรึกษาครั้งนี้ ลักษณะงานมีความซับซ้อนและหลากหลายทั้งด้านวิชาการและด้านเทคนิค เป็นงานจ้างที่จำเป็นต้องใช้ที่ปรึกษาที่มีความรู้ ความสามารถเฉพาะด้านมาตรฐานความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑:๒๐๑๓ และได้รับใบประกาศนียบัตรตามที่กำหนด อีกทั้งต้องมีประสบการณ์ในการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ให้กับองค์กรอื่นมาแล้ว และต้องอาศัยทีมงานที่มี

ความหลากหลาย เช่น ทีมงานด้านมาตรฐาน ทีมงานด้านเทคนิคเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศและผู้ตรวจสอบที่มีความเชี่ยวชาญตามข้อกำหนดของมาตรฐาน สำนักงาน กสทช. จะพิจารณาคัดเลือกข้อเสนอของที่ปรึกษาที่ผ่านการพิจารณาคัดเลือกด้วยเกณฑ์คุณภาพตามข้อ ๑๑.๑ แล้ว ด้วยเกณฑ์ด้านราคาและเกณฑ์ด้านคุณภาพ โดยมีสัดส่วนน้ำหนักระหว่างเกณฑ์ด้านราคา เท่ากับ ๓๐ และเกณฑ์คุณภาพ เท่ากับ ๗๐ โดยเกณฑ์ด้านคุณภาพจะแบ่งน้ำหนักเกณฑ์ย่อย ประกอบด้วย

(๑) ผลงานและประสบการณ์ของที่ปรึกษา น้ำหนัก ๒๐
(๒) วิธีการบริหารและวิธีปฏิบัติงาน น้ำหนัก ๓๐
(๓) จำนวนบุคลากรที่ร่วมงาน น้ำหนัก ๒๐

สำนักงาน กสทช. จะปรับคะแนนที่ได้รับจากการประเมินด้านคุณภาพตามข้อ ๑๑.๑ ตามสัดส่วนน้ำหนักแต่ละเกณฑ์ เพื่อรวมกับเกณฑ์ด้านราคา เป็นลำดับต่อไป

๑๑.๓ สำนักงาน กสทช. จะพิจารณาข้อเสนอด้านราคาของรายที่ผ่านเกณฑ์ด้านคุณภาพตามข้อ ๑๑.๑ โดยข้อเสนอด้านราคาที่ดีที่สุด (ต่ำสุด) จะได้คะแนนน้ำหนักเต็มตามสัดส่วนที่กำหนด และข้อเสนอด้านราคาของรายลำดับถัดไปจะได้คะแนนน้ำหนักลดลงตามสัดส่วนความแตกต่างของระหว่างข้อเสนอราคาของรายนั้นกับราคาข้อเสนอด้านราคาของรายต่ำสุด

๑๑.๔ สำนักงาน กสทช. จะรวมคะแนนข้อเสนอด้านคุณภาพและด้านราคาตามเกณฑ์สัดส่วนน้ำหนักที่กำหนดในข้อ ๑๑.๒ และผู้ยื่นข้อเสนอที่ได้รับคะแนนรวมด้านคุณภาพและด้านราคามากที่สุด จะได้รับการคัดเลือกให้เป็นที่ปรึกษาครั้งนี้ ทั้งนี้ สำนักงาน กสทช. จะพิจารณาความเหมาะสมของข้อเสนอด้านราคาของที่ปรึกษาที่ได้รับการคัดเลือก รวมทั้งเจรจาต่อรองอัตราค่าจ้างที่ปรึกษาและอื่นๆ ตามความเหมาะสมและเป็นไปตามหลักเกณฑ์การคำนวณอัตราค่าจ้างที่ปรึกษาตามระเบียบและกฎหมายที่เกี่ยวข้องต่อไป

๑๒. เงื่อนไขอื่นๆ

๑๒.๑ ที่ปรึกษาต้องเก็บรักษาข้อมูลของสำนักงาน กสทช. และข้อมูลที่ได้รับจากการดำเนินโครงการไว้เป็นความลับ จะเปิดเผยให้ผู้ใดทราบมิได้ และไม่นำไปใช้ในวัตถุประสงค์อื่นนอกเหนือจากการดำเนินการในโครงการนี้

๑๒.๒ ลิขสิทธิ์ในผลงานและเอกสาร รวมถึงไฟล์ดิจิทัลที่ได้รับจากผลการศึกษา ให้ตกเป็นของสำนักงาน กสทช. แต่เพียงผู้เดียว การเผยแพร่เอกสารหรือจัดทำสำเนาเพิ่มเติมจากที่จ้างเป็นสิทธิชอบธรรมของสำนักงาน กสทช.

๑๒.๓ ที่ปรึกษามีหน้าที่จะต้องตรวจสอบบุคลากรที่เสนอเข้ามาในโครงการว่ามีบุคลากรที่ยังคงดำเนินการเป็นที่ปรึกษาให้กับสำนักงาน กสทช. อยู่ในโครงการใดหรือไม่ กรณีอยู่ในโครงการจะต้องตรวจสอบรับรองระยะเวลาดำเนินงาน เพื่อมิให้เป็นการใช้ทรัพยากรซ้ำซ้อน ซึ่งส่งผลต่อความคุ้มค่าของการใช้เงินงบประมาณ

๑๒.๔ ในกรณีที่ที่ปรึกษาฯ มีเหตุจำเป็นต้องเปลี่ยนตัวบุคลากรดำเนินงานในโครงการนี้ ที่ปรึกษาฯ ต้องเสนอขอความเห็นชอบจากสำนักงาน กสทช. ก่อน โดยบุคลากรใหม่ต้องมีคุณสมบัติเทียบเท่าหรือดีกว่าบุคลากรเดิม ทั้งนี้สำนักงาน กสทช. สงวนสิทธิ์ในการพิจารณาปรับลดอัตราค่าจ้างบุคลากรที่ปรึกษาได้ตามความเหมาะสม

๑๒.๕ หากที่ปรึกษาไม่สามารถทำงานให้แล้วเสร็จตามเวลาที่กำหนดไว้ในสัญญา และผู้ว่าจ้างยังมิได้บอกเลิกสัญญา ที่ปรึกษาจะต้องชำระค่าปรับให้แก่ผู้ว่าจ้างในอัตรา ร้อยละ ๐.๑ ของวงเงินค่าจ้างฯ นับถัดจากวันที่กำหนดแล้วเสร็จตามสัญญา หรือวันที่ผู้ว่าจ้างได้ขยายระยะเวลาตามสัญญาจนถึงวันที่ทำงานแล้วเสร็จจริง นอกจากนี้ที่ปรึกษายอมให้ผู้ว่าจ้างเรียกค่าเสียหายอันเกิดจากการที่ปรึกษาทำงานล่าช้า เฉพาะส่วนที่เกินกว่าจำนวนค่าปรับ และค่าใช้จ่ายดังกล่าวได้อีกด้วย