ขอบเขตงาน (Term of Reference)
การจ้างที่ปรึกษาเพื่อตรวจติดตามรอบที่ ๒ สำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001, 27701, 27035 และการรักษาความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑. หลักการและเหตุผล

ตามที่ได้มีการบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) ในฐานะหน่วยงานภาครัฐและหน่วยงานควบคุม กำกับหรือดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ซึ่งจัดเป็นหน่วยงานที่มีความสำคัญทั้งภาพลักษณ์และการสร้างมาตรฐานที่ดีของสำนักงาน กสทช. ในการดำเนินงานให้สอดคล้องกับพระราชบัญญัติข้างต้น ขณะเดียวกันในด้านของการคุ้มครองข้อมูลส่วนบุคคล สำนักงาน กสทช. ในฐานะที่เป็นหน่วยงานกำกับดูแลจำเป็นอย่างยิ่งที่จะต้องแสดงบทบาทสำคัญในการเป็นหน่วยงานต้นแบบในการกำกับดูแลและคุ้มครองข้อมูลส่วนบุคคล เพื่อทำหน้าที่เป็นเสาหลักในการกำกับดูแลกิจการภายใต้การกำกับดูแลให้ปฏิบัติสอดคล้องตามด้วย จึงเป็นที่มาที่สำนักงาน กสทช. จะต้องริเริ่มในการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลตามมาตรฐานสากลที่เกี่ยวข้อง มีการพัฒนาบุคลากร กระบวนการ และเครื่องมือให้เข้มแข็งทั้งในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และด้านการคุ้มครองข้อมูลส่วนบุคคล

เพื่อไปสู่จุดมุ่งหมายดังกล่าว สำนักงาน กสทช. โดยสำนักเทคโนโลยีสารสนเทศ (นบ.) ได้มีการดำเนินงานในเบื้องต้นโดยจัดทำกระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2022 กระบวนการบริหารจัดการความมั่นคงปลอดภัยข้อมูลส่วนบุคคลตามมาตรฐาน ISO/IEC 27701:2019 จนได้รับการรับรองตามมาตรฐานดังกล่าวตั้งแต่ปี พ.ศ. ๒๕๖๖ โดยดำเนินการจ้างที่ปรึกษาเพื่อปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2022 และจัดทำกระบวนการบริหารจัดการความมั่นคงปลอดภัยข้อมูลส่วนบุคคลตามมาตรฐาน ISO/IEC 27701:2019 ให้กับสำนักเทคโนโลยีสารสนเทศ สำนักงาน กสทช. สัญญาจ้างเลขที่ ๘๖๕๐๓๑๒ ลงวันที่ ๓๑ สิงหาคม ๒๕๖๕ แล้วนั้น นอกจากนี้ ยังมีการพัฒนากระบวนการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและภัยคุกคามทางไซเบอร์ ซึ่งเป็นหนึ่งในกระบวนการสำคัญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับมาตรฐาน ISO/IEC 27035:2023 (Information Security Incident Management) อย่างไรก็ตามยังมีความจำเป็นที่จะต้องมีการบำรุงรักษากระบวนการดังกล่าวให้สำนักงาน กสทช. มีมาตรฐานในการดำเนินงานและมีความพร้อมในการรองรับการตรวจประเมินจากผู้ตรวจประเมินภายนอก (Certification Body) ซึ่งจะเป็นส่วนหนึ่งที่จะช่วยตอบโจทย์ด้านการพัฒนาบุคลากรและการปรับปรุงกระบวนการและพัฒนาอย่างต่อเนื่อง อีกทั้งต้องเพิ่มเติมในด้านของการพัฒนาเครื่องมือเพื่อใช้ในการประเมินและตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และด้านการคุ้มครองข้อมูลส่วนบุคคล และต้องพัฒนาบุคลากรของสำนักงาน กสทช. ให้มีความรู้ความเข้าใจ และมีความสามารถในการนำกระบวนการของมาตรฐานไปประยุกต์ใช้กับงานของตน และสามารถใช้เครื่องมือในการตรวจประเมินทั้งในด้านของการรักษาความมั่นคงปลอดภัยและด้านของการคุ้มครองข้อมูลส่วนบุคคลในเบื้องต้นด้วยตนเองได้

นอกจากนี้ เพื่อให้สอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ข้อ ๒๒.๒.๒ - ๒๒.๒.๕ ซึ่งระบุให้หน่วยงานต้องมีการดำเนินการ ดังนี้ (๑) การกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration

Proof

Standards) ตามที่ระบุไว้ (๒) ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) (๓) ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) (๔) ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Managemrnt Process) ให้สอดคล้องกับบริการที่สำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง รวมถึง ข้อ ๒๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) และได้ดำเนินการเตรียมความพร้อมในการพัฒนาและบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management System ; BCMS) หรือมาตรฐาน ISO/IEC 22301 เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์ ตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) ทั้งนี้ ถือเป็นการยกระดับการดำเนินงานในภาพรวมของสำนักงาน กสทช. ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

กรณีการดำเนินงานตามพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ มาตรา ๔๑ (๑) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐต้องจัดให้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เพื่อปฏิบัติหน้าที่ดูแลและคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด ซึ่งสำนักงาน กสทช. เป็นผู้ควบคุมข้อมูลส่วนบุคคล และได้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามคำสั่งสำนักงาน กสทช. ที่ ๙๑๔/๒๕๖๖ ลงวันที่ ๑๑ ตุลาคม ๒๕๖๖ เพื่อปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของสำนักงาน กสทช. โดยในปี พ.ศ. ๒๕๖๖ ดำเนินการจ้างที่ปรึกษาเพื่อปฏิบัติหน้าที่ที่ปรึกษาด้านการคุ้มครองข้อมูลส่วนบุคคล ให้กับคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และดำเนินการตรวจสอบความสอดคล้องการปฏิบัติตามกฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคล ให้กับ สำนักงาน กสทช. (DPO Consultant) ตามสัญญาเลขที่ ๘๖๖๐๒๒๘ ลงวันที่ ๒๙ สิงหาคม ๒๕๖๖ มีการพัฒนารูปแบบ แนวทาง และวิธีปฏิบัติอ้างอิงตามมาตรฐานสากล ICO ของสหราชอาณาจักรเป็นอย่างน้อย ซึ่งจำเป็นต้องมีการตรวจประเมิน แจ้งข้อคิดเห็นและข้อเสนอแนะในการปรับปรุงแนวทางการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน กสทช. เพื่อให้เกิดการปรับปรุงแก้ไขนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล ประกาศความเป็นส่วนตัว การขอความยินยอม การตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การโอนข้อมูลส่วนบุคคล มาตรการการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และกระบวนการอื่น ๆ ที่เกี่ยวข้องให้สอดคล้องและเป็นไปตามบริบทที่เปลี่ยนแปลงไปทั้งในส่วนของโครงสร้างองค์กร ส่วนของข้อติดขัด และส่วนของกฎหมายลำดับรอง ระเบียบ และกรอบวิธีหรือแนวปฏิบัติ ที่กำหนดโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในขั้นตอนของการประกาศใช้

ดังนั้น เพื่อให้สำนักเทคโนโลยีสารสนเทศ สำนักงาน กสทช. ปฏิบัติตามเป้าหมายดังกล่าวได้ครบถ้วน จึงมีความจำเป็นต้องจัดจ้างที่ปรึกษาเพื่อเข้ามาดำเนินการ ๑) พัฒนา ปรับปรุง กระบวนการด้านมาตรฐานการรักษาความมั่นคงปลอดภัย (ISO/IEC 27001:2022) มาตรฐานข้อมูลส่วนบุคคล (ISO/IEC 27701:2019) และมาตรฐานการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ (ISO/IEC 27035:2023) รวมถึงการศึกษาแนวทางในการพัฒนาไปสู่มาตรฐาน Business Continuity Management System (BCMS) หรือ ISO/IEC 22301 ในภาพรวมของสำนักงาน กสทช. ๒) การตรวจประเมินและปรับปรุงแก้ไขตาม *ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔* ขยายผลระบบสารสนเทศทั้ง แอปพลิเคชันและเว็บแอปพลิเคชัน หรือระบบการบริหารจัดการข้อมูลดิจิทัลของสำนักงาน กสทช. โดยการพัฒนาบุคลากร กระบวนการ และเครื่องมือในการตรวจประเมินและปฏิบัติตามกระบวนการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัย

Proof

ไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งรวมถึงการให้คำปรึกษาในการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ๓) การจัดทำและตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของบริการที่สำคัญ ๔) การวิเคราะห์และออกแบบระบบสารสนเทศที่มีความมั่นคงปลอดภัย ตามภูมิทัศน์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Landscape) เพื่อให้สำนักงาน กสทช. สามารถเป็นหน่วยงานที่มีการรักษาความมั่นคงปลอดภัยสารสนเทศได้เทียบเท่าหน่วยงานกำกับดูแลในต่างประเทศ ๕) พัฒนาและปรับปรุงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนกระบวนการ วิธีปฏิบัติประกาศความเป็นส่วนตัว การขอความยินยอม การตอบสนองสิทธิของเจ้าของข้อมูลส่วนบุคคล การบริหารจัดการกรณีเกิดการรั่วไหลของข้อมูลส่วนบุคคล หรือกระบวนการอื่น ๆ ที่เกี่ยวข้อง ให้มีความทันสมัยและสอดคล้องกับกฎหมายลำดับรอง รวมถึง ระเบียบและข้อบังคับที่ได้มีการประกาศขึ้นมาในภายหลัง และเป็นไปตามมาตรฐานสากล ๖) มีการสร้างความตระหนักในการปฏิบัติตามนโยบายและแนวปฏิบัติดังกล่าวให้กับบุคลากรของสำนักงาน กสทช. เพื่อให้เกิดประสิทธิภาพและประสิทธิผลสูงสุดในการดำเนินการของสำนักงาน กสทช. ด้านความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย ตลอดจนขยายผลไปสู่ภาพรวมของสำนักงาน กสทช. รวมถึงเป็นการธำรงค์ไว้ซึ่งชื่อเสียง ภาพลักษณ์ และเป็นการปฏิบัติให้สอดคล้องกับกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง

๒. วัตถุประสงค์

เพื่อจ้างที่ปรึกษาเพื่อพัฒนาปรับปรุงแก้ไขการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001, 27701, 27035 การรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓. คุณสมบัติของที่ปรึกษา

ผู้ยื่นข้อเสนอต้องมีคุณสมบัติพื้นฐานที่กำหนด ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ ตลอดจนแนวปฏิบัติตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐ ตามภาคผนวก ๑

๔. ขอบเขตของงานจ้างที่ปรึกษา

ขอบเขตของการดำเนินงานของที่ปรึกษาต้องประกอบด้วยงาน ดังต่อไปนี้

๔.๑. ศึกษา วิเคราะห์ และจัดทำรายงานผลการศึกษาเบื้องต้น (Inception Report) โดยมีเนื้อหาประกอบอย่างน้อยดังนี้

๔.๑.๑. ดำเนินการวิเคราะห์ช่องว่าง (Gap Analysis) สำหรับการตรวจติดตามรอบที่ ๒ ของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27035 และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cyber Security Fremwork)

๔.๑.๒. ดำเนินการวิเคราะห์ช่องว่าง (Gap Analysis) ของการดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน กสทช. และบริบท (Context) ที่เกี่ยวข้องในปัจจุบัน เทียบกับข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตลอดจนกฎหมายลำดับรอง กฎ ระเบียบ ข้อบังคับ หรือประกาศที่เกี่ยวข้องเพิ่มเติม กรอบมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง อาทิ Information Commissioner's Office (ICO) สหราชอาณาจักร หรือมาตรฐานภายใต้ General Data Protection Regulation (GDPR)

Proof

๔.๑.๓. จัดทำแผนการตรวจสอบและให้ข้อเสนอแนะตามบทบาทหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Office: DPO)

๔.๑.๔. จัดทำแผนการดำเนินงานด้านประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๕

๔.๑.๕. จัดทำแผนการดำเนินโครงการที่เป็นภาพรวมของโครงการตลอดระยะเวลาการดำเนินโครงการที่สะท้อนถึงเนื้องานตามขอบเขตงานจ้างที่ปรึกษา

๔.๒. **การดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล** ที่ปรึกษาต้องดำเนินการให้คำปรึกษาและแนะนำแก่คณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) และพนักงานของสำนักงาน กสทช. ที่เกี่ยวข้อง และการเป็นที่ปรึกษาให้กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ให้สามารถปฏิบัติหน้าที่ได้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วยรายละเอียดอย่างน้อยต่อไปนี้

๔.๒.๑. จัดให้มีเจ้าหน้าที่อย่างน้อย ๒ คน เข้าปฏิบัติหน้าที่ ณ สำนักงาน กสทช. อย่างน้อยสัปดาห์ละ ๒ วัน ในการให้คำปรึกษาแนะนำในการจัดทำบันทึกรายการกิจกรรมการประมวลผล (ROPA) การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy Impact Assessment: DPIA) ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement: DSA) ให้กับสำนักต่าง ๆ ภายในสำนักงาน กสทช. โดยให้มีการจัดทำรายงานประจำเดือนเพื่อรายงานผลการดำเนินงาน

๔.๒.๒. ทบทวนและปรับปรุงหรือจัดทำเอกสารด้านการคุ้มครองข้อมูลส่วนบุคคล อาทิ นโยบาย ประกาศ แบบฟอร์ม ขั้นตอนการปฏิบัติ ระเบียบ เอกสารอื่นใดที่เกี่ยวข้องเพิ่มเติม เป็นต้น ให้สอดคล้องตามกฎหมายลำดับรอง กฎ ระเบียบ ข้อบังคับหรือประกาศต่าง ๆ ที่มีการประกาศเพิ่มเติมในภายหลัง และสอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และในกรณีที่มีความจำเป็นต้องมีการประมวลผลข้อมูลส่วนบุคคลของชาวต่างประเทศ ให้จัดทำหรือปรับปรุงเอกสารดังกล่าวเป็นฉบับแปลเป็นภาษาอังกฤษ

๔.๒.๒.๑. กรณีที่เอกสารหรือขั้นตอนการปฏิบัติตามข้อ ๔.๒.๒ จำเป็นต้องมีการรับฟังความคิดเห็นกลุ่มย่อย (Focus Group) ให้ดำเนินการจัดประชุมกลุ่มย่อยอย่างน้อย ๑ ครั้ง ผู้เข้ารับฟังไม่น้อยกว่า ๗๐ คน อย่างน้อยครั้งละ ๓ ชั่วโมง

๔.๒.๒.๒. จัดอบรมสร้างความตระหนักรู้ในนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อย ๓ ชั่วโมง สำหรับเจ้าหน้าที่ของสำนักงาน กสทช. ผู้เข้ารับฟังไม่น้อยกว่า ๖๐ คน

๔.๒.๒.๓. จัดการประเมินผลการรับรู้รับทราบและการปฏิบัติตามนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล (ทั้งสำนักงาน กสทช.) อย่างน้อย ๑ ครั้ง และจัดทำรายงานผลเชิงสถิติพร้อมบทสรุปผู้บริหาร (Executive Summary) อย่างน้อย ๑ ฉบับ

๔.๒.๓. จัดให้มีการซักซ้อมกระบวนการ หรือจำลองสถานการณ์จริงเกี่ยวกับการตอบสนองต่อคำร้องขอใช้สิทธิ และการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล อย่างน้อย ๑ ครั้ง ผู้เข้าร่วมไม่น้อยกว่า ๖๐ คน อย่างน้อยครั้งละ ๓ ชั่วโมง โดยต้องจัดทำแผนการซักซ้อม ดำเนินการซักซ้อม และจัดทำรายงานผลการซ้อมให้ครบถ้วน

๔.๒.๔. ดำเนินการจัดทำ infographic สำหรับการสื่อสารประชาสัมพันธ์เพื่อสร้างความตระหนักรู้ในสำนักงาน กสทช. ตามเอกสารหรือขั้นตอนการปฏิบัติ อย่างน้อย ๕ ชิ้นงาน

๔.๒.๕. ดำเนินการเป็นที่ปรึกษา ให้คำแนะนำหรือข้อคิดเห็นหรือแนวปฏิบัติที่ดี (Best Practice) ในการประชุมคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน กสทช. ตามรอบการประชุม

๔.๒.๖. ดำเนินการวิเคราะห์ ออกแบบ การกำหนดตัวชี้วัดด้านการคุ้มครองข้อมูลส่วนบุคคล (Privacy Metric) ให้กับสำนักงาน กสทช. เพื่อดำเนินการให้เกิดการวัดและปรับปรุงอย่างต่อเนื่อง ซึ่งมีรายละเอียดเนื้องาน ได้แก่

Proof

๔.๒.๖.๑. ศึกษาการกำหนดตัวชี้วัดจากแนวปฏิบัติที่ดีที่เป็นสากล และนำเสนอให้กับคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของสำนักงาน กสทช. ได้พิจารณาแนวทางเพื่อนำมาประยุกต์ใช้ เพื่อกำหนดเป็นตัวชี้วัดให้กับการดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคลของสำนักงาน กสทช.

๔.๒.๖.๒. จัดทำกระบวนการในการวัด และการประเมินผล ตัวชี้วัดตามรอบที่กำหนด

๔.๒.๖.๓. เก็บรวบรวมข้อมูลและจัดทำรายงานผลการวัด ตัวชี้วัดตามที่ได้กำหนดไว้รายงานต่อคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของสำนักงาน กสทช. พร้อมทั้งจัดทำแนวทางปรับปรุงในรอบถัดไป

๔.๒.๗. ดำเนินการตรวจประเมินด้านการคุ้มครองข้อมูลส่วนบุคคล ตามหน้าที่รับผิดชอบขอบเขตงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อประเมินความสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ตามแนวปฏิบัติที่ดี หรือตามข้อกำหนดของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีรายละเอียดอย่างน้อยต่อไปนี้

๔.๒.๗.๑. การตรวจประเมินด้านการคุ้มครองข้อมูลส่วนบุคคล ณ สำนักงาน กสทช. สำนักงานใหญ่ จำนวนไม่น้อยกว่า ๔๐ สำนัก ซึ่งการดำเนินการตรวจประเมินจะต้องมีกิจกรรมอย่างน้อยดังต่อไปนี้

(๑) การจัดทำแผนในการตรวจประเมิน

(๒) การจัดเกณฑ์การตรวจประเมิน

(๓) การดำเนินการตรวจประเมินตามแผน

(๔) การจัดทำรายงานสรุปผลการตรวจประเมินและนำเสนอคณะทำงาน DPO ให้ได้รับทราบ พร้อมทั้งแนวทางในการดำเนินการแก้ไขหรือปรับปรุงสิ่งที่ตรวจพบ

๔.๒.๗.๒. การตรวจประเมินด้านการคุ้มครองข้อมูลส่วนบุคคล ณ สำนักงานภาคหรือเขต จำนวนไม่น้อยกว่า ๔ ครั้ง ซึ่งการดำเนินการตรวจประเมินจะต้องมีกิจกรรมอย่างน้อยเป็นไปตามข้อ ๔.๒.๗.๑

๔.๒.๘. ดำเนินการจัดอบรมเพื่อสร้างเสริมทักษะบุคลากรของสำนักงาน กสทช. ให้ Data Protection Officer (DPO) และ PDPA Agent โดยมีรายละเอียดการดำเนินงาน อย่างน้อย ดังนี้

๔.๒.๘.๑. หลักสูตรฝึกอบรมเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อให้สามารถตรวจสอบได้ตามรายการคำถามการตรวจสอบ (Audit Checklist) ที่เป็นแนวปฏิบัติที่ดี อาทิ UK ICO หรือมาตรฐานที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด รวมทั้งมีการฝึกตรวจและฝึกจัดทำรายงานผลการตรวจประเมิน ระยะเวลาในการฝึกอบรมอย่างน้อย ๕ วันทำการ โดยมีผู้เข้าอบรม จำนวนไม่น้อยกว่า ๑๐ คน

๔.๒.๘.๒. จัดหลักสูตรฝึกอบรมเพื่อสร้างทักษะด้านการจัดทำบันทึกรายการกิจกรรมการประมวลผล (ROPA), การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล Breach Notification การจัดทำข้อตกลงการประมวลผล (DPA) การจัดทำข้อตกลงการแบ่งปันข้อมูล (DSA) การดำเนินการด้านการตอบสนองต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล (DSR) ให้กับบุคลากรของสำนักงาน กสทช. ที่ได้รับคัดเลือกเป็นตัวแทนเพื่อสร้างเป็น PDPA Agent ที่มีความเข้มแข็ง ระยะเวลาในการฝึกอบรมอย่างน้อย ๕ วันทำการ โดยมีผู้เข้าอบรมไม่น้อยกว่า ๖๐ คน

๔.๒.๘.๓. หลักสูตรฝึกอบรมด้านเทคโนโลยีสำหรับการบริหารจัดการด้านการคุ้มครองข้อมูลส่วนบุคคล (CIPT), Privacy by design by default ให้กับบุคลากรของสำนักงาน กสทช. ที่ได้รับคัดเลือกเป็นตัวแทนเพื่อสร้างเป็น PDPA Agent ที่มีความเข้มแข็ง ระยะเวลาในการฝึกอบรมอย่างน้อย ๕ วันทำการ โดยมีผู้เข้าอบรมที่เป็นเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ จำนวนไม่น้อยกว่า ๑๐ คน

Proof

๔.๒.๘.๔. จัดหลักสูตรฝึกอบรมธรรมภิบาลด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับปัญญาประดิษฐ์ อาทิ หลักสูตร AIGP ให้กับบุคลากรของสำนักงาน กสทช. ที่ได้รับคัดเลือกเป็นตัวแทนเพื่อสร้างเป็น PDPA Agent ที่มีความเข้มแข็ง ระยะเวลาในการฝึกอบรมอย่างน้อย ๕ วันทำการ โดยมีผู้เข้าอบรม จำนวนไม่น้อยกว่า ๑๐ คน

๔.๓. **การดำเนินการตามมาตรฐาน ISO/IEC จำนวน ๓ มาตรฐาน** ที่ปรึกษาต้องดำเนินการให้คำปรึกษาและแนะนำแก่พนักงานของสำนักงาน กสทช. เพื่อพัฒนาปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC 27001:2022 การบริหารจัดการข้อมูลส่วนบุคคลตามมาตรฐานสากล ISO/IEC 27701:2019 สำหรับรอบการตรวจติดตามรอบที่ ๒ และการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยตามมาตรฐานสากล ISO/IEC 27035:2023 ตามขอบเขตที่สำนักเทคโนโลยีสารสนเทศกำหนด ประกอบด้วยรายละเอียดอย่างน้อยต่อไปนี้

๔.๓.๑. จัดให้มีเจ้าหน้าที่อย่างน้อย ๒ คน เข้ามาปฏิบัติงานให้คำปรึกษา ณ สำนักงาน กสทช. อย่างน้อยสัปดาห์ละ ๒ วัน เพื่อดำเนินการติดตามการประเมินความเสี่ยง ขึ้นทะเบียนทรัพย์สินสารสนเทศ ติดตามตัวชี้วัด ปรับปรุงเอกสารและช่วยดำเนินการที่เกี่ยวข้องกับการบริหารจัดการตามมาตรฐานสากล ISO/IEC 27001:2022 มาตรฐานสากล ISO/IEC 27701:2019 และมาตรฐานสากล ISO/IEC 27035:2023 โดยให้มีการจัดทำรายงานประจำเดือนเพื่อรายงานผลการดำเนินงาน

๔.๓.๒. ทบทวนและปรับปรุงแก้ไข เอกสารบริบทองค์กรที่จะส่งผลกระทบต่อการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ การรักษาความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล โดยนำกรอบแนวคิด PESTEL Model มาใช้ในการดำเนินการ และให้สอดคล้องกับข้อกำหนดของมาตรฐานสากล ISO/IEC 27001:2022 มาตรฐานสากล ISO/IEC 27701:2019 และมาตรฐานสากล ISO/IEC 27035:2023 รวมถึงประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๓.๓. ดำเนินการทบทวนเกณฑ์การประเมินความเสี่ยงให้สอดคล้องกับบริบทที่เกี่ยวข้องและดำเนินการประเมินความเสี่ยงทรัพย์สินสารสนเทศ ข้อมูลส่วนบุคคล และการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยตามขอบเขต โดยต้องมีการระบุถึงเหตุการณ์ภัยคุกคาม (Threats) จุดอ่อน (Vulnerabilities) และโอกาสเกิด (Likelihood) ภัยคุกคามนั้น ๆ และจัดทำเป็นรายงานผลการประเมินความเสี่ยงที่สอดคล้องกับข้อกำหนดของมาตรฐาน รวมถึงประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๓.๔. ปรับปรุงแก้ไขเอกสารแสดงมาตรการที่เลือกใช้ (SoA) ของมาตรฐานสากล ISO/IEC 27001:2022 มาตรฐานสากล ISO/IEC 27701:2019 และมาตรฐานสากล ISO/IEC 27035:2023 และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) รวมถึงข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับผลการประเมินความเสี่ยง พร้อมทั้งจัดทำแผนการจัดการความเสี่ยง (Risk Treatment Plan) กรณีที่ต้องการลดความเสี่ยงหรือกำจัดความเสี่ยงตามเกณฑ์ที่กำหนด

๔.๓.๕. ทบทวนและปรับปรุงแก้ไขนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ สอดคล้องตามกฎหมายและมาตรฐานที่เกี่ยวข้อง และบริบทขององค์กรทั้งภายในและภายนอก ตามข้อ ๔.๓.๒ รวมถึงความคาดหวังและความต้องการจากผู้มีส่วนได้ส่วนเสียหรือบุคคลที่เกี่ยวข้อง (Interested parties) สำหรับขอบเขตที่กำหนด ให้สอดคล้องตามมาตรฐานสากล ISO/IEC 27001:2022 มาตรฐานสากล ISO/IEC 27701:2019 และมาตรฐานสากล ISO/IEC 27035:2023 ตลอดจนมาตรฐานอื่นที่เกี่ยวข้อง รวมถึงประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

Proof

๔.๓.๕.๑. จัดการสื่อสารและชี้แจงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ กับผู้ที่เกี่ยวข้อง อย่างน้อยครั้งละ ๓ ชั่วโมง (สำหรับเจ้าหน้าที่ของสำนักงาน กสทช.) ผู้เข้ารับฟังไม่น้อยกว่า ๗๐ คน

๔.๓.๕.๒. จัดการประเมินผลการรับรู้รับทราบและการปฏิบัติตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ (ทั้งสำนักงาน กสทช. และผู้ให้บริการภายนอก (Third parties) และจัดทำรายงานผลเชิงสถิติ พร้อมบทสรุปผู้บริหาร (Executive Summary) อย่างน้อย ๑ ฉบับ

๔.๓.๖. ดำเนินการจัดทำ infographic สำหรับการสื่อสารประชาสัมพันธ์เพื่อสร้างความตระหนักรู้ในสำนักงาน กสทช. ที่เกี่ยวข้องกับนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ หรือองค์ความรู้ต่างๆ ด้านภัยคุกคามทางไซเบอร์ อย่างน้อย ๕ ชิ้นงาน

๔.๓.๗. ดำเนินการตรวจสอบ วิเคราะห์และประเมินช่องโหว่ด้านความมั่นคงปลอดภัย (Vulnerability Assessment Scan) ของระบบสารสนเทศตามขอบเขต จำนวนไม่น้อยกว่า ๑๐ ระบบ ให้สอดคล้องกับข้อกำหนด Management of technical vulnerabilities โดยการตรวจสอบต้องดำเนินการทั้งในระดับ ระบบปฏิบัติการ (Operation System: OS) ของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์เครือข่าย (Network Device) ของสำนักงาน กสทช. รวมทั้งจัดทำรายงานผลการตรวจสอบช่องโหว่ แนวทางการป้องกัน แก้ไขช่องโหว่ที่ตรวจพบ และดำเนินการประชุมกับทีมงานผู้ดูแลระบบเพื่อนำเสนอผลการดำเนินงานทั้งหมด และดำเนินการตรวจสอบซ้ำอีก ๑ ครั้ง ภายหลังการนำเสนอรายงานผลการตรวจสอบในครั้งแรก พร้อมทั้งจัดทำรายงานเปรียบเทียบผลการตรวจสอบช่องโหว่ของทั้งสองครั้ง และดำเนินการประชุมกับทีมงานผู้ดูแลระบบ เพื่อนำเสนอผลการดำเนินงาน

๔.๓.๘. นำข้อมูลเข้าระบบบริหารจัดการเอกสารและบริหารจัดการความเสี่ยง ที่มีลักษณะการใช้งานในรูปแบบของ Web-Based ที่สามารถนำมาประยุกต์ใช้กับขั้นตอนปฏิบัติการบริหารจัดการความเสี่ยง ขั้นตอนปฏิบัติการควบคุมเอกสาร ที่สำนักงาน กสทช. ใช้งานอยู่ในปัจจุบัน สำหรับรายการทรัพย์สินสารสนเทศ และรายการเอกสารตามขอบเขต ตลอดจนสามารถค้นหาข้อมูลและสร้างเงื่อนไขในการเรียกดูข้อมูลการประเมินความเสี่ยงได้ รวมถึงสามารถจัดทำเป็นรายงานเอกสารที่ประกาศใช้งานและผลการประเมินความเสี่ยงได้

๔.๓.๙. จัดทำเพิ่มเติม หรือปรับปรุงแก้ไข แผนและตัวชี้วัดเพื่อเป็นการวัดประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Effectiveness Measurement) ให้สอดคล้องตามมาตรฐานที่กำหนด

๔.๓.๑๐. จัดทำ หรือปรับปรุง แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan) ให้กับระบบสารสนเทศตามขอบเขต และสอดคล้องตาม ข้อกำหนดของมาตรฐานสากล ISO/IEC 27001:2022 มาตรฐานสากล ISO/IEC 27035:2023 และมาตรฐานสากล ISO/IEC 27035:2023 ISO/IEC 22301 และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) รวมถึงประมวลแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ และดำเนินการซ้อมแผนบริหารความต่อเนื่องทางธุรกิจตามขอบเขตอย่างน้อย ๑ ครั้ง

๔.๓.๑๑. ให้คำแนะนำในการดำเนินการบริหารจัดการเอกสารสารสนเทศ (Documented Information) นำเอกสารขึ้นระบบเพื่อใช้ในการอ้างอิงและดำเนินการให้สอดคล้องตาม ข้อกำหนดของมาตรฐาน

๔.๓.๑๒. ดำเนินการตรวจสอบภายใน (Internal Auditor) รวมทั้งให้คำปรึกษาและคำแนะนำแก่คณะตรวจสอบภายในที่ได้รับการแต่งตั้งจากคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยและบริการเทคโนโลยีสารสนเทศ (Security and Service Management Committee : SSMC)

Proof

๔.๓.๑๒.๑. ดำเนินการตรวจสอบภายในและจัดทำรายงานผลการตรวจสอบให้กับระบบบริหารจัดการตามมาตรฐานสากล ISO/IEC 27001:2022 มาตรฐานสากล ISO/IEC 27701:2019 และมาตรฐานสากล ISO/IEC 27035:2023 อย่างน้อย ๑ ครั้งต่อปี

๔.๓.๑๒.๒. ให้คำปรึกษา และคำแนะนำ ในการติดตามการแก้ไขข้อบกพร่องที่ตรวจพบจากการตรวจสอบภายใน (Corrective and Preventive Actions) ของระบบบริหารจัดการตามมาตรฐานสากล ISO/IEC 27001:2022 ISO/IEC 27701:2019 และ ISO/IEC 27035:2023

๔.๓.๑๒.๓. ให้คำปรึกษา และดำเนินการเตรียมการในส่วนความรับผิดชอบของผู้บริหาร (Management Review) เพื่อทบทวนการพัฒนาและการดำเนินงานระบบบริหารจัดการตามมาตรฐานสากล ISO/IEC 27001:2022 ISO/IEC 27701:2019 และ ISO/IEC 27035:2023

๔.๓.๑๓. ดำเนินการจัดให้มีการตรวจประเมินตาม กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) และให้คำแนะนำในการปรับปรุงเพื่อลดช่องว่างจากผลตรวจประเมิน รวมถึงให้ข้อเสนอแนะเพื่อยกระดับการดำเนินการให้ดียิ่งขึ้น

๔.๓.๑๔. จัดทำหรือปรับปรุงภูมิทัศน์ด้านความมั่นคงปลอดภัยไซเบอร์ ของสำนักงาน กสทช. (NBTC Cybersecurity Landscape)

๔.๓.๑๕. ดำเนินการเป็นที่ปรึกษา ให้คำแนะนำหรือข้อคิดเห็นหรือแนวปฏิบัติที่ดี (Best Practice) ในการประชุมคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยและบริการเทคโนโลยีสารสนเทศ (Security and Service Management Committee : SSMC) ของสำนักงาน กสทช. ตามรอบการประชุม

๔.๓.๑๖. ให้คำปรึกษา และคำแนะนำ รวมทั้งให้การสนับสนุนการตรวจประเมินจากผู้ตรวจประเมินภายนอก (Certification Body) ในการตรวจรับรองระบบบริหารจัดการตามมาตรฐานสากล ISO/IEC 27001:2022 ISO/IEC 27701:2019 และ ISO/IEC 27035:2023 รอบการตรวจติดตามที่ ๒ ตามขอบเขตที่กำหนด รวมทั้งให้คำปรึกษา และคำแนะนำในการแก้ไข Non conformity (NC) (ถ้ามี) ที่ได้รับจากการตรวจประเมินของผู้ตรวจประเมินภายนอก และจัดทำแผนการดำเนินการเพื่อแก้ไขและตอบ NC ให้กับผู้ตรวจประเมินภายนอก ภายในระยะเวลาที่กำหนด

๔.๓.๑๗. จัดทำ Security baseline สำหรับ OS Platform ที่มีความสำคัญเพื่อใช้กำหนดค่าพารามิเตอร์ได้อย่างมั่นคงปลอดภัยให้สอดคล้องกับมาตรฐานสากล อาทิ ระบบปฏิบัติการ Windows เวอร์ชั่นที่สำนักงาน กสทช. มีการใช้งาน เป็นต้น

๔.๓.๑๘. ดำเนินการศึกษา Gap Analysis เทียบกับมาตรฐาน ISO/IEC 22301 และจัดทำรายงานเพื่อให้ข้อแนะนำในการเตรียมความพร้อมในการดำเนินงานตามมาตรฐานการบริหารความต่อเนื่องทางธุรกิจหรือมาตรฐาน ISO/IEC 22301

๔.๓.๑๙. ดำเนินการสร้างเสริมทักษะพนักงานของสำนักงาน กสทช. ตามขอบเขตการขอการรับรองโดยมีรายละเอียดหลักสูตรฝึกอบรม ดังนี้

๔.๓.๑๙.๑. จัดหลักสูตรฝึกอบรมความมั่นคงปลอดภัยและการบริหารจัดการปัญญาประดิษฐ์ ISO/IEC 42001:2023 (Artificial intelligence - Management system) ให้กับบุคลากรในขอบเขต จำนวนไม่น้อยกว่า ๒๐ คน ระยะเวลาในการฝึกอบรมอย่างน้อย ๑ วัน

๔.๓.๑๙.๒. จัดหลักสูตรฝึกอบรมนโยบาย และขั้นตอนการปฏิบัติงานตามมาตรฐานสากล ISO/IEC 27001:2022 ISO/IEC 27701:2019 และ ISO/IEC 27035:2023 ให้กับบุคลากรในขอบเขตการขอการรับรองจำนวนไม่น้อยกว่า ๒๐ คน ระยะเวลาในการฝึกอบรมอย่างน้อย ๑ วัน

Proof

๔.๓.๑๙.๓. จัดหลักสูตรฝึกอบรมเชิงปฏิบัติการให้ความรู้เกี่ยวกับข้อกำหนดมาตรฐานสากล ISO/IEC 27001:2022 ISO/IEC 27701:2019 และ ISO/IEC 27035:2023 และแนวทางการตรวจประเมินภายใน สำหรับทีมตรวจสอบภายใน จำนวนไม่เกิน ๑๐ ท่าน ระยะเวลาในการฝึกอบรมอย่างน้อย ๑ วัน

๔.๓.๑๙.๔. หลักสูตรฝึกอบรมมาตรฐานสากล ISO/IEC 27001:2022 IRCA Lead Auditor เพื่อพัฒนาการเป็นผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ จำนวนผู้เข้าอบรมไม่น้อยกว่า ๑๐ คน ระยะเวลาในการฝึกอบรมอย่างน้อย ๕ วัน

๔.๓.๑๙.๕. หลักสูตรฝึกอบรมมาตรฐานสากล ISO/IEC 27035:2023 จำนวนผู้เข้าอบรมไม่เกิน ๑๐ คน ระยะเวลาในการฝึกอบรมอย่างน้อย ๒ วัน

๔.๓.๑๙.๖. หลักสูตรฝึกอบรมกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) และประมวลแนวทางปฏิบัติและกรอบมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวนผู้เข้าอบรมไม่เกิน ๑๐ คน ระยะเวลาในการฝึกอบรมอย่างน้อย ๓ วัน

๔.๔. **การตรวจสอบระบบสารสนเทศนอกขอบเขต ISO และการพัฒนาทีมผู้ตรวจประเมิน** ที่ปรึกษาดำเนินการเตรียมการโดยจัดทำแผนตรวจประเมินความสอดคล้องตามประมวลแนวทางและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ ๒๕๖๔ โดยพัฒนาพนักงานของสำนักงาน กสทช. ที่เป็นทีมตรวจประเมิน กระบวนการและเครื่องมือในการตรวจประเมิน สร้างทักษะการจัดการด้านความมั่นคงปลอดภัยไซเบอร์ให้กับสำนักที่เป็นเจ้าของระบบสารสนเทศ ประกอบด้วยรายละเอียดอย่างน้อยต่อไปนี้

๔.๔.๑. จัดทำคู่มือและแนวทางในการตรวจประเมินด้านความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ

๔.๔.๑.๑. จัดหลักสูตรฝึกอบรมผู้นำการตรวจสอบตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ระยะเวลาในการฝึกอบรมอย่างน้อย ๕ วัน จำนวนผู้เข้าอบรมไม่น้อยกว่า ๑๐ คน

๔.๔.๑.๒. จัดทำรายงานผลการฝึกอบรมและการประเมินผลการฝึกอบรมเป็นรายบุคคลเพื่อบ่งชี้สมรรถนะการเป็นผู้ตรวจประเมินความมั่นคงปลอดภัยไซเบอร์

๔.๔.๒. ประเมิน Gap Analysis ของระบบสารสนเทศที่ได้รับการกำหนดเป็นระบบงานสารสนเทศที่สนับสนุนงานบริการสำคัญ กับประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พร้อมกำหนดบทบาทหน้าที่การดูแลรักษาระบบสารสนเทศสำคัญตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พร้อมประชุมชี้แจง ฝึกทักษะ และให้คำแนะนำในการจัดทำทะเบียนทรัพย์สินสารสนเทศ และการดำเนินงานอื่นๆ ที่เกี่ยวข้องตามกรอบของประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ

๔.๔.๒.๑. ดำเนินการประเมินความเสี่ยงระบบงานสารสนเทศที่สนับสนุนงานบริการสำคัญเพื่อให้สอดคล้องตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ รวมถึงให้คำแนะนำในการจัดการความเสี่ยง (Risk Treatment Plan)

๔.๔.๒.๒. ให้ข้อแนะนำในการจัดทำหรือปรับปรุงแผนรับมือกับภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่สอดคล้องตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ ระบบงานสารสนเทศที่สนับสนุนงานบริการสำคัญ รวมถึงดำเนินการซ้อมแผนการรับมือกับภัยคุกคามทางไซเบอร์อย่างน้อย ๑ ครั้ง

๔.๔.๒.๓. ดำเนินการปรับปรุงแก้ไข และจัดให้มีมาตรการใน ๔ หัวข้อหลัก ตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cyber Security Fremwork) ให้กับระบบงานสารสนเทศที่สนับสนุนงานบริการสำคัญ ได้แก่

Proof

(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์

(๒) ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

(๓) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

(๔) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

(๕) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

(๖) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๔.๔.๓. จัดให้มีการตรวจประเมินระบบงานสารสนเทศที่สนับสนุนงานบริการสำคัญของสำนักงาน กสทช. ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cyber Security Fremwork) พร้อมทั้งจัดทำรายงานผลการตรวจประเมิน

๕. บุคลากรของที่ปรึกษา

ที่ปรึกษาจะต้องจัดให้มีบุคลากรที่มีความรู้ความชำนาญเพื่อดำเนินงานตามขอบเขตงาน โดยมีคุณวุฒิ ประสบการณ์ และจำนวนอย่างน้อย ดังนี้

๕.๑ ผู้จัดการโครงการ จำนวน ๑ คน

จบการศึกษาอย่างน้อยในระดับปริญญาโท ในสาขาที่เกี่ยวข้องกับคอมพิวเตอร์ สาขาวิศวกรรมศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือโทรคมนาคมและการสื่อสาร หรือด้านอื่น ๆ ที่เกี่ยวข้อง และมีประสบการณ์ด้านการบริหารโครงการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ หรือวิศวกรรมคอมพิวเตอร์ หรือโทรคมนาคมและการสื่อสาร หรือการบริหารจัดการโครงการเป็นระยะเวลาไม่น้อยกว่า ๑๐ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๘ man-month

๕.๒ ที่ปรึกษาโครงการ จำนวน ๑ คน

ที่ปรึกษาด้าน ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27035 และ ISO/IEC 22301 จบการศึกษาอย่างน้อยในระดับปริญญาโทหรือสูงกว่า สาขาวิศวกรรมศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือโทรคมนาคมและการสื่อสาร หรือด้านอื่น ๆ ที่เกี่ยวข้องและมีประสบการณ์ด้านเทคโนโลยีสารสนเทศหรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือการตรวจสอบด้านสารสนเทศ เป็นระยะเวลาไม่น้อยกว่า ๑๐ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๗ man-month และได้รับประกาศนียบัตรที่เกี่ยวข้องอย่างใดอย่างหนึ่ง ดังต่อไปนี้

- ISO/IEC 27001 Lead Auditor หรือ
- ISO/IEC 27701 Lead Auditor หรือ
- ISO/IEC 27035 Implementation หรือ
- CISSP หรือ
- CompTIA Security+ หรือ
- CompTIA Cybersecurity Analysis+ หรือ
- ComTIA Advanced Security practitioner+

Proof

๕.๓ หัวหน้าทีมที่ปรึกษา PDPA จำนวน ๑ คน

จบการศึกษาอย่างน้อยในระดับปริญญาโท ด้านนิติศาสตร์ ด้านบริหารธุรกิจ หรือด้านอื่นๆ ที่เกี่ยวข้อง มีประสบการณ์การทำงานเป็นระยะเวลาไม่น้อยกว่า ๑๐ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๘ man-month มีความเชี่ยวชาญด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล และได้รับประกาศนียบัตรอย่างใดอย่างหนึ่ง ดังต่อไปนี้

- IAPP CIPP/E (Certified Information Privacy Professional/Europe) หรือ CIPP/US หรือ
- IAPP CIPM (Certified Information Privacy Manager) หรือ
- Certified Data Protection Officer จากสถาบันชั้นนำในต่างประเทศ อาทิ PECB, CEPAS, TUV SUD หรือ EXIN หรือ
- DPO-GDPR หรือ
- Certified Data Privacy Solutions Engineer (CDPSE) หรือ
- หลักสูตรเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภาครัฐ (GDPO) หรือ
- หลักสูตรเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลรับรอง หรือ
- ประกาศนียบัตรอื่นที่เกี่ยวข้องด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐานเทียบเท่ากับประกาศนียบัตรข้างต้น

๕.๔ ทีมที่ปรึกษา PDPA จำนวน ๓ คน

จบการศึกษาอย่างน้อยในระดับปริญญาตรี ด้านนิติศาสตร์ ด้านบริหารธุรกิจ หรือด้านอื่นๆ ที่เกี่ยวข้อง และมีประสบการณ์ด้านการคุ้มครองข้อมูลส่วนบุคคล เป็นระยะเวลาไม่น้อยกว่า ๕ ปี โดยต้องมีระยะเวลาดำเนินงานคนละไม่น้อยกว่า ๘ man-month และได้รับประกาศนียบัตรอย่างใดอย่างหนึ่ง ดังต่อไปนี้

- IAPP CIPP/E (Certified Information Privacy Professional/Europe) หรือ CIPP/US หรือ
- IAPP CIPM (Certified Information Privacy Manager) หรือ
- Certified Data Protection Officer จากสถาบันชั้นนำในต่างประเทศ อาทิ PECB, CEPAS, TUV SUD หรือ EXIN หรือ
- DPO-GDPR หรือ
- Certified Data Privacy Solutions Engineer (CDPSE) หรือ
- หลักสูตรเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภาครัฐ (GDPO) หรือ
- หลักสูตรเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลรับรอง หรือ
- ประกาศนียบัตรอื่นที่เกี่ยวข้องด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐานเทียบเท่ากับประกาศนียบัตรข้างต้น

๕.๕ หัวหน้าทีมที่ปรึกษาด้านเทคนิค จำนวนอย่างน้อย ๑ คน

จบการศึกษาอย่างน้อยในระดับปริญญาโท สาขาวิศวกรรมคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือโทรคมนาคมและการสื่อสาร และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศหรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือความมั่นคงปลอดภัยไซเบอร์ เป็นระยะเวลาอย่างน้อย ๑๐ ปี โดยต้องมีระยะเวลาดำเนินงานอย่างน้อย ๘ man-month และได้รับประกาศนียบัตร อย่างใดอย่างหนึ่ง ดังต่อไปนี้

Proof

- Certified ISMS Auditor รับรองโดยสถาบัน International Register of Certificated Auditors (IRCA) หรือ PECB หรือ
- ISO/IEC 27001 Lead Auditor หรือ
- ISO/IEC 27701 Implementation หรือ
- ISO/IEC 27035 Implementation หรือ
- CompTIA Security+ หรือ
- CompTIA Cybersecurity Analysis+ หรือ
- ComTIA Advanced Security practitioner+

๕.๖ ผู้เชี่ยวชาญระดับอาวุโสด้านความปลอดภัยคอมพิวเตอร์ จำนวนอย่างน้อย ๑ คน

จบการศึกษาในระดับปริญญาโท สาขาวิศวกรรมคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือโทรคมนาคมและการสื่อสาร และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศ หรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือการตรวจสอบด้านสารสนเทศ หรือวิศวกรรมความปลอดภัยคอมพิวเตอร์ เป็นระยะเวลาอย่างน้อย ๑๐ ปี โดยต้องมีระยะเวลาดำเนินงานคนละไม่น้อยกว่า ๘ man-month และได้รับประกาศนียบัตร อย่างใดอย่างหนึ่ง ดังนี้

- IRCA Lead auditor ISO/IEC ๒๗๐๐๑ หรือ
- ISO ๓๑๐๐๐ Application of Risk Management system หรือ
- CompTIA Security+ หรือ
- CompTIA Cybersecurity Analyst (CySA+) หรือ
- ประกาศนียบัตรด้านความมั่นคงสารสนเทศหรือคอมพิวเตอร์ หรือ
- ประกาศนียบัตรด้าน Information security risk management

๕.๗ ทีมที่ปรึกษาด้านเทคนิค จำนวนอย่างน้อย ๒ คน

จบการศึกษาอย่างน้อยในระดับปริญญาตรี สาขาวิศวกรรมคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือโทรคมนาคมและการสื่อสาร และมีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือ การตรวจสอบด้านสารสนเทศ เป็นระยะเวลาอย่างน้อย ๕ ปี โดยต้องมีระยะเวลาดำเนินงานคนละไม่น้อยกว่า ๘ man-month และได้รับประกาศนียบัตรที่เกี่ยวข้องอย่างใดอย่างหนึ่ง ดังต่อไปนี้

- ISO/IEC 27701 Implementation หรือ
- ISO/IEC 27001 Lead Auditor หรือ
- ISO/IEC 27035 Implementation หรือ
- CompTIA Security+ หรือ
- CEH (Certified Ethical Hacker) หรือ
- ประกาศนียบัตรด้านความมั่นคงสารสนเทศหรือคอมพิวเตอร์

Proof

๕.๘ ผู้เชี่ยวชาญระดับอาวุโสด้าน Internal Audit ISO/IEC 27001 จำนวน ๑ คน

สำเร็จการศึกษาอย่างน้อยในระดับปริญญาโทหรือสูงกว่า มีประสบการณ์ในการทำงานด้านระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศหรืองานอื่นที่เกี่ยวข้อง เป็นระยะเวลาไม่น้อยกว่า ๕ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๒ man-month และได้รับประกาศนียบัตรอย่างใดอย่างหนึ่ง ดังนี้

- IRCA Lead auditor ISO/IEC 27001 หรือ
- ISO ๓๑๐๐๐ Application of Risk Management system หรือ
- CompTIA Security+ หรือ
- CompTIA Cybersecurity Analyst (CySA+) หรือ
- ประกาศนียบัตรด้าน Lead Auditor อื่นๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ หรือข้อมูลส่วนบุคคล

๕.๙ ผู้เชี่ยวชาญด้าน Business Continuity Management จำนวน ๑ คน

สำเร็จการศึกษาอย่างน้อยในระดับปริญญาตรีหรือสูงกว่า สาขาวิศวกรรมคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือโทรคมนาคมและการสื่อสาร มีประสบการณ์ในการทำงานด้านการบริหารความต่อเนื่องทางธุรกิจหรืองานอื่นที่เกี่ยวข้อง เป็นระยะเวลาไม่น้อยกว่า ๕ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๘ man-month และได้รับประกาศนียบัตร อย่างน้อยดังนี้

- ISO 22301 Lead Auditor Certified หรือ
- ISO 22301 Lead Implementer Certified

๕.๑๐ ผู้ประสานงานโครงการ จำนวน ๑ คน

สำเร็จการศึกษาอย่างน้อยในระดับปริญญาตรีหรือสูงกว่า สาขาวิศวกรรมคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือโทรคมนาคมและการสื่อสาร หรือสาขาบริหารจัดการธุรกิจ มีประสบการณ์ในการทำงานด้านประสานงานโครงการหรืองานอื่นที่เกี่ยวข้อง เป็นระยะเวลาไม่น้อยกว่า ๕ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๑๐ man-month

๖. ระยะเวลาดำเนินการ

ภายใน ๓๖๐ วัน นับถัดจากวันลงนามในสัญญา

๗. ระยะเวลาการส่งมอบงาน

ที่ปรึกษาต้องส่งมอบงานพร้อม Data Files ที่จัดเก็บในสื่อบันทึกข้อมูลชนิด Flash Drive และในรูปแบบเอกสารจำนวน ๕ ชุด โดยแบ่งออกเป็นงวดงานดังนี้

งวดที่ ๑ ส่งมอบงาน รายละเอียดตามที่ระบุด้านล่างนี้ ภายใน ๖๐ วัน นับถัดจากวันลงนามในสัญญา

ข้อ ๔.๑ :๔.๑.๑, ๔.๑.๒

งวดที่ ๒ ส่งมอบงาน รายละเอียดตามที่ระบุด้านล่างนี้ ภายใน ๙๐ วัน นับถัดจากวันลงนามในสัญญา

ข้อ ๔.๑ : ๔.๑.๓, ๔.๑.๔ และ ๔.๑.๕

ข้อ ๔.๒ : ๔.๒.๑ รายงานประจำเดือน และ ๔.๒.๘.๑

ข้อ ๔.๓ : ๔.๓.๑ รายงานประจำเดือน และ ๔.๓.๒

Proof

งวดที่ ๓ ส่งมอบงาน รายละเอียดตามที่ระบุด้านล่างนี้ ภายใน ๒๑๐ วัน นับถัดจากวันลงนามในสัญญา

ข้อ ๔.๒ : ๔.๒.๑ รายงานประจำเดือน ๔.๒.๓, ๔.๒.๖, และ ๔.๒.๘.๒

ข้อ ๔.๓ : ๔.๓.๑ รายงานประจำเดือน ๔.๓.๓, ๔.๓.๔, ๔.๓.๕.๑ และ ๔.๓.๕.๒

ข้อ ๔.๔ : ๔.๔.๑.๑

งวดที่ ๔ ส่งมอบงาน รายละเอียดตามที่ระบุด้านล่างนี้ ภายใน ๓๖๐ วัน นับถัดจากวันลงนามในสัญญา

ข้อ ๔.๒ : ๔.๒.๑ รายงานประจำเดือน ๔.๒.๒, ๔.๒.๒.๑, ๔.๒.๒.๒, ๔.๒.๔, ๔.๒.๗, ๔.๒.๘.๓ และ ๔.๒.๘.๔

ข้อ ๔.๓ : ๔.๓.๑ รายงานประจำเดือน ๔.๓.๖, ๔.๓.๗, ๔.๓.๘, ๔.๓.๙, ๔.๓.๑๐, ๔.๓.๑๒, ๔.๓.๑๓, ๔.๓.๑๔, ๔.๓.๑๖, ๔.๓.๑๗, ๔.๓.๑๘ และ ๔.๓.๑๙

ข้อ ๔.๔ : ๔.๔.๑.๒, ๔.๔.๒ และ ๔.๔.๓

๘. วงเงินที่ใช้ในการจัดหา

วงเงินรวมทั้งสิ้น ๑๑,๒๓๑,๘๐๐.- บาท (สิบเอ็ดล้านสองแสนสามหมื่นหนึ่งพันแปดร้อยบาทถ้วน) ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่มและค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว โดยเบิกจ่ายจากงบประมาณ ปี ๒๕๖๗ จำนวนเงิน ๓,๓๖๙,๖๐๐.-บาท (สามล้านสามแสนหกหมื่นเก้าพันหกร้อยบาทถ้วน) และผูกพันงบประมาณปี ๒๕๖๘ จำนวนเงิน ๗,๘๖๒,๒๐๐.-บาท (เจ็ดล้านแปดแสนหกหมื่นสองพันสองร้อยบาทถ้วน) รายจ่ายอื่น ค่าจ้างที่ปรึกษาเพื่อศึกษา วิจัย ประเมินผล หรือพัฒนาระบบต่าง ๆ

๙. เงื่อนไขการชำระเงิน

สำนักงาน กสทช. จะชำระเงินตามจำนวนในสัญญาจ้างหลังจากที่ได้ตรวจรับถูกต้องเรียบร้อยแล้ว และที่ปรึกษาปฏิบัติถูกต้องครบถ้วนตามที่สำนักงาน กสทช. กำหนด โดยจะชำระเงินตามเงื่อนไขและกำหนดเวลาการชำระเงินดังนี้

งวดที่ ๑ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๑๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ปรึกษาส่งมอบงานในงวดงานที่ ๑ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว

งวดที่ ๒ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๒๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ปรึกษาส่งมอบงานในงวดงานที่ ๒ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว

งวดที่ ๓ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๓๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ปรึกษาส่งมอบงานในงวดงานที่ ๓ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว

งวดที่ ๔ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๔๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ปรึกษาส่งมอบงานในงวดงานที่ ๔ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว

Proof

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 รวมทั้งอำนาจหน้าที่ของหน่วยงานซึ่งรับรองสำเนาถูกต้องโดยผู้มีอำนาจลงนามของหน่วยงาน

๑๐.๑.๔ หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมายในกรณีที่ปรึกษามอบอำนาจให้บุคคลอื่นลงนามในเอกสารข้อเสนอแทน

๑๐.๒. ข้อเสนอทางเทคนิค

ที่ปรึกษาจะต้องจัดทำข้อเสนอด้านเทคนิคที่ประกอบด้วย

๑๐.๒.๑ ผลงานและประสบการณ์ของที่ปรึกษา ประกอบด้วย ผลงานที่ทางหน่วยงานเคยทำมาก่อน โดยเฉพาะส่วนที่เกี่ยวข้องกับการศึกษาในด้านที่เกี่ยวข้องหรือการศึกษาที่คล้ายคลึงกับลักษณะของงานหรือภารกิจตามขอบเขตของงานนี้ ทั้งนี้ ในส่วนผลงานให้แนบหนังสือรับรองผลงาน และ/หรือ สำเนาเอกสารสัญญาที่ได้ดำเนินการแล้วเสร็จ และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับส่วนราชการ หน่วยงานของรัฐ หน่วยงานตามกฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น หน่วยงานอื่นซึ่งมีกฎหมายบัญญัติให้มีฐานะเป็นราชการบริหารส่วนท้องถิ่น รัฐวิสาหกิจ หรือหน่วยงานเอกชนที่สำนักงาน กสทช. เชื่อถือ ตลอดจนหลักฐานอื่น ๆ เพื่อเพิ่มความเชื่อมั่น เช่น รางวัลและเอกสารอื่น ๆ ที่สามารถอ้างอิงได้ (ถ้ามี)

๑๐.๒.๒ วิธีการบริหารและวิธีการดำเนินงาน ตามที่กำหนดในขอบเขตของงานข้อ ๔ โดยผู้ยื่นข้อเสนอจะต้องนำเสนอแผนงาน แนวทางการบริหารและวิธีการดำเนินงานอย่างละเอียด ระยะเวลาการดำเนินงาน บุคลากรที่ดำเนินงาน นอกจากนี้ จะต้องนำเสนอเพื่อแสดงให้เห็นถึงความเข้าใจในโครงการและทักษะความสามารถในการดำเนินการโครงการได้ตามวัตถุประสงค์โครงการและขอบเขตของงาน หรือข้อเสนออื่น ๆ ที่เป็นประโยชน์ต่อการดำเนินงานและสอดคล้องกับขอบเขตของงาน

Proof

๑๐.๒.๓ คุณสมบัติ ประสบการณ์ และจำนวนของบุคลากรที่เข้าร่วมงาน โดยต้องประกอบด้วยรายละเอียดประวัติ คุณวุฒิ และประสบการณ์การทำงานของที่ปรึกษาที่ผ่านมาของบุคลากรที่ได้เสนอมาในโครงการ ซึ่งสอดคล้องตาม ข้อ ๕ บุคลากรของที่ปรึกษา

๑๐.๓. ข้อเสนอทางด้านราคา

๑๐.๓.๑ ราคาที่จะเสนอจะต้องรวมถึงค่าใช้จ่ายต่าง ๆ ซึ่งรวมถึงภาษีมูลค่าเพิ่มภาษีเงินได้ ค่าอากรแสตมป์ ฯลฯ โดยจะต้องแสดงรายละเอียดค่าใช้จ่ายต่าง ๆ ที่จะต้องใช้ในการดำเนินการตามขอบเขตของงานแต่ละรายการตามแผนปฏิบัติการ และเสนอสรุปเป็นราคาค่าบริการทั้งหมด

๑๐.๓.๒ รายละเอียดค่าจ้างบุคลากร โดยแสดงรายละเอียดจำนวนคน-เดือน และอัตราค่าจ้างเป็นรายบุคคล **<u>และแนบหลักฐานด้านการเงิน เช่น สลิปเงินเดือน หนังสือรับรองเงินเดือน หรือสำเนาหลักฐานการชำระภาษี (ภ.ง.ด. ๙๑)</u>**

๑๐.๓.๓ รายละเอียดค่าใช้จ่ายเพิ่มเติมต่าง ๆ เช่น ค่าใช้จ่ายในการจัดการประชุม การจัดฝึกอบรมเพื่อถ่ายทอดความรู้ การประชุมหารือกลุ่มย่อย ค่าพาหนะเดินทาง ค่าวัสดุอุปกรณ์ ค่าจัดทำรายงาน ค่าถ่ายเอกสาร และค่าใช้จ่ายที่เกี่ยวเนื่อง เป็นต้น

๑๐.๔. วิธีการยื่นข้อเสนอ ผู้ยื่นข้อเสนอต้องแยกซองในการยื่นข้อเสนอเป็น ๓ ซอง และให้ยื่นพร้อมกัน โดยถือปฏิบัติ ดังนี้

๑๐.๔.๑. ซองที่ ๑ ให้บรรจุเอกสารและหลักฐานเกี่ยวกับผู้ยื่นข้อเสนอ จำนวน ๕ ชุด (ตัวจริง ๑ ชุด สำเนา ๔ ชุด)

๑๐.๔.๒. ซองที่ ๒ ให้บรรจุข้อเสนอด้านเทคนิค จำนวน ๕ ชุด (ตัวจริง ๑ ชุด สำเนา ๔ ชุด)

๑๐.๔.๓. ซองที่ ๓ ให้บรรจุข้อเสนอด้านราคา จำนวน ๑ ชุด

โดยเอกสารทั้ง ๓ ซอง จะต้องปิดผนึกให้เรียบร้อย และรับรองสำเนาถูกต้องโดยผู้มีอำนาจทำนิติกรรมแทนนิติบุคคล/ผู้มีอำนาจลงนามของหน่วยงาน/ผู้ได้รับมอบอำนาจถูกต้องตามกฎหมาย พร้อมทั้งประทับตรา

จ่าหน้าซองถึงประธานกรรมการดำเนินงานจ้างที่ปรึกษา สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เลขที่ ๘๗ ซอยพหลโยธิน ๘ แขวงสามเสนใน เขตพญาไท กรุงเทพฯ ๑๐๔๐๐ ภายในกำหนดตามหนังสือเชิญชวน

๑๑. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

โดยที่งานจ้างที่ปรึกษาครั้งนี้ เพื่อให้ดำเนินการตรวจสอบและติดตามการดำเนินงานของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Surveillance Audit) รอบที่ ๒ และมีการจัดจ้างผู้ตรวจรับรอง (Certificate Body) เข้ามาตรวจรับรองตามรอบการตรวจติดตามดังกล่าว ซึ่งเป็นงานต่อเนื่องที่ต้องดำเนินการต่อจากเดิมให้ครบวงรอบ เพื่อคงสถานะใบรับรองที่สำนักงาน กสทช. ได้รับไว้ให้ถูกต้อง นอกจากนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) ได้มีประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ข้อ ๑๙.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ข้อ ๒๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise) จึงจำเป็นต้องมีการขอการรับรองมาตรฐานในส่วนที่เกี่ยวข้องกับ ISO/IEC 27035 (Information Security Incident Management) นอกจากนี้ ประมวลแนวทางปฏิบัติฯ ยังกำหนดข้อ ๒๒.๒.๒-๒๒.๒.๕ ซึ่งระบุให้หน่วยงานต้องมีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ และต้อง

Proof

ตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงของบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์ และข้อ ๒๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) และการยกระดับการดำเนินงานตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) เพื่อให้สำนักเทคโนโลยีสารสนเทศ มีกระบวนการบริหารจัดการเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยและภัยคุกคามทางไซเบอร์ ได้อย่างเป็นมาตรฐานสากลเพิ่มเติมไปจากเดิม สำนักงาน กสทช. จะดำเนินการจัดจ้างโดยวิธีคัดเลือก ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ มาตรา ๗๕ และมาตรา ๗๖ (๒) ประกอบกับระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ ข้อ ๑๒๖ (๒) ในสัดส่วนด้านคุณภาพ ๗๐ และด้านราคา ๓๐ โดยคณะกรรมการจ้างที่ปรึกษาตามวิธีที่กำหนด จะพิจารณาคัดเลือกข้อเสนอตามลำดับ ดังนี้

๑๑.๑. สำนักงาน กสทช. จะพิจารณาข้อเสนอของที่ปรึกษาทุกราย เว้นแต่ที่ปรึกษาที่ยื่นเอกสารหลักฐานไม่ครบถ้วนตามข้อ ๑๐.๑ ในส่วนที่เป็นสาระสำคัญ หรือครบถ้วนแต่ไม่ถูกต้อง จะไม่รับพิจารณาข้อเสนอของที่ปรึกษารายนั้น และในการพิจารณาคัดเลือกข้อเสนอจะคำนึงถึงความคุ้มค่าและวัตถุประสงค์ของงานจ้างที่ปรึกษาเป็นสำคัญ โดยพิจารณาเกณฑ์ด้านคุณภาพเป็นลำดับแรกก่อน คุณภาพด้านต่าง ๆ รวม ๓ หัวข้อ มีคะแนนน้ำหนักรวม ๗๐ และจำแนกสัดส่วนน้ำหนักแต่ละหัวข้อ ประกอบด้วย ดังนี้

(๑)	ผลงานที่ผ่านมาของผู้ยื่นข้อเสนอ	น้ำหนักร้อยละ ๓๐
	(๑.๑) ผลงานของที่ปรึกษา	(ร้อยละ ๑๕)
	(๑.๒) ประสบการณ์เฉพาะ	(ร้อยละ ๑๕)
(๒)	วิธีบริหารและวิธีปฏิบัติงาน	น้ำหนักร้อยละ ๓๐
(๓)	จำนวนและคุณลักษณะเฉพาะของบุคลากรที่ร่วมงาน	น้ำหนักร้อยละ ๑๐

ทั้งนี้ การประเมินคะแนนตามเกณฑ์ด้านคุณภาพแต่ละหัวข้อ มีรายละเอียดคะแนนหัวข้อย่อยและการให้คะแนนตามเอกสารแนบท้ายของงานใน**ภาคผนวก ๒** และพิจารณาเปรียบเทียบคุณภาพระหว่างผู้ยื่นข้อเสนอด้วยกัน ซึ่งคะแนนที่ได้รับการประเมินแต่ละหัวข้อจะแปลงเป็นคะแนนน้ำหนักตามสัดส่วนของแต่ละหัวข้อที่กำหนด รวมคะแนนน้ำหนักเต็ม ๗๐ ข้อเสนอที่ผ่านเกณฑ์คุณภาพจะต้องได้คะแนนน้ำหนักไม่น้อยกว่าร้อยละ ๘๐ (๕๖)

๑๑.๒. ข้อเสนอของที่ปรึกษาด้านคุณภาพที่ได้รับการประเมินคะแนนและถ่วงน้ำหนักตามข้อ ๑๑.๑ แล้ว เพื่อนำไปรวมกับคะแนนตามสัดส่วนน้ำหนักของราคา (คะแนนเต็มร้อยละ ๓๐) โดยข้อเสนอด้านราคาที่ดีที่สุด (ต่ำสุด) จะได้คะแนนน้ำหนักเต็มตามสัดส่วนที่กำหนด และข้อกำหนดด้านราคาของรายลำดับถัดไปจะได้คะแนนลดลงตามสัดส่วนความแตกต่างของระหว่างข้อเสนอราคาของรายนั้นกับข้อเสนอด้านราคาของรายต่ำสุด

๑๑.๓. ข้อเสนอของที่ปรึกษาที่ได้รับคะแนนน้ำหนักรวมตามสัดส่วนด้านคุณภาพและด้านราคาตามข้อ ๑๑.๒ มากที่สุดจะได้รับการคัดเลือกให้เป็นที่ปรึกษาในงานจ้างครั้งนี้ ทั้งนี้ คณะกรรมการจ้างที่ปรึกษาตามวิธีที่กำหนด จะพิจารณาความเหมาะสมของข้อเสนอด้านราคาของที่ปรึกษาที่ได้รับการคัดเลือก รวมทั้งเจรจาต่อรองอัตราค่าจ้างที่ปรึกษาและอื่น ๆ ตามความเหมาะสมและเป็นไปตามหลักเกณฑ์การคำนวณอัตราค่าจ้างที่ปรึกษาตามระเบียบและกฎหมายที่เกี่ยวข้องต่อไป

๑๒. เงื่อนไขอื่น ๆ

๑๒.๑ ที่ปรึกษาต้องเก็บรักษาข้อมูลของสำนักงาน กสทช. และข้อมูลที่ได้รับจากการดำเนินโครงการไว้เป็นความลับ จะเปิดเผยให้ผู้ใดทราบมิได้ และไม่นำไปใช้ในวัตถุประสงค์อื่นนอกเหนือจากการดำเนินการในโครงการนี้

๑๒.๒ ลิขสิทธิ์ในผลงานและเอกสาร รวมถึงไฟล์ดิจิทัลที่ได้รับจากผลการศึกษา ให้ตกเป็นของสำนักงาน กสทช. แต่เพียงผู้เดียว การเผยแพร่เอกสารหรือจัดทำสำเนาเพิ่มเติมจากที่จ้างเป็นสิทธิชอบธรรมของสำนักงาน กสทช.

๑๒.๓ ที่ปรึกษามีหน้าที่จะต้องตรวจสอบบุคลากรที่เสนอเข้ามาในโครงการว่ามีบุคลากรที่ยังคงดำเนินการเป็นที่ปรึกษาให้กับสำนักงาน กสทช. อยู่ในโครงการใดหรือไม่ กรณีอยู่ในโครงการจะต้องตรวจสอบรับรองระยะเวลาดำเนินงาน เพื่อมิให้เป็นการใช้ทรัพยากรซ้ำซ้อน ซึ่งจะส่งผลต่อความคุ้มค่าของการใช้เงินงบประมาณ ทั้งนี้บุคลากรหลักของที่ปรึกษา ต้องมีระยะเวลาปฏิบัติงานตามสัญญาไม่ซ้ำซ้อนกับงานในโครงการอื่น ๆ ของที่ปรึกษาที่ดำเนินการในช่วงเวลาเดียวกัน หากผู้ว่าจ้างพบว่าบุคลากรหลักไม่ว่าคนหนึ่งคนใดหรือหลายคนปฏิบัติงานซ้ำซ้อนกับงานในโครงการอื่น ๆ ไม่ว่าจะพบในระหว่างปฏิบัติงานตามสัญญาหรือในภายหลัง ผู้ว่าจ้างมีสิทธิบอกเลิกสัญญา และ/หรือเรียกค่าเสียหายจากที่ปรึกษาหรือปรับค่าจ้างได้

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

๑๒.๕ หากที่ปรึกษาไม่สามารถทำงานให้แล้วเสร็จตามเวลาที่กำหนดไว้ในสัญญา และผู้ว่าจ้างยังมิได้บอกเลิกสัญญา ที่ปรึกษาจะต้องชำระค่าปรับให้แก่ผู้ว่าจ้างในอัตรา ร้อยละ ๐.๑ ของวงเงินค่าจ้างฯ นับถัดจากวันที่กำหนดแล้วเสร็จตามสัญญา หรือวันที่ผู้ว่าจ้างได้ขยายระยะเวลาตามสัญญาจนถึงวันที่ทำงานแล้วเสร็จจริงนอกจากนี้ที่ปรึกษายอมให้ผู้ว่าจ้างเรียกค่าเสียหายอันเกิดจากการที่ปรึกษาทำงานล่าช้า เฉพาะส่วนที่เกินกว่าจำนวนค่าปรับ และค่าใช้จ่ายดังกล่าวได้อีกด้วย

๑๒.๖ ที่ปรึกษาที่ได้รับการคัดเลือกจะต้องทำสัญญากับสำนักงาน กสทช. ตามแบบสัญญาจ้างที่ที่ปรึกษาคณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดตามที่ประกาศในราชกิจจานุเบกษา และวางหลักประกันสัญญาเป็นอย่างใดอย่างหนึ่งที่กำหนด มูลค่าร้อยละ ๕ ของค่าจ้างที่ปรึกษา เว้นแต่กรณีที่ปรึกษาที่ได้รับการคัดเลือกเป็นหน่วยงานของรัฐไม่ต้องวางหลักประกันสัญญา

Proof

คุณสมบัติของผู้ยื่นข้อเสนอ

๑. มีความสามารถตามกฎหมาย

๒. ไม่เป็นบุคคลล้มละลาย

๓. ไม่อยู่ระหว่างเลิกกิจการ

๔. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๕. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๖. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุ ภาครัฐกำหนดในราชกิจจานุเบกษา

๗. เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่จ้างครั้งนี้

๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน กสทช. ณ วันที่ได้รับหนังสือเชิญชวนให้เข้ายื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการยื่นข้อเสนอครั้งนี้

๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๑๐. ที่ปรึกษาที่จะเข้าร่วมการเสนองานกับหน่วยงานของรัฐ ต้องเป็นที่ปรึกษาที่ได้ขึ้นทะเบียนไว้กับศูนย์ข้อมูลที่ปรึกษา กระทรวงการคลัง สาขา ICT: เทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Sector) มาตรฐานคุณภาพ (QS) : Quality Standard Sector ความเชี่ยวชาญ R๑๒๐: มาตรฐานระบบรักษาความปลอดภัยของข้อมูลองค์กร

๑๑. ที่ปรึกษาผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(๑) กรณีเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันที่ยื่นข้อเสนอ

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่ตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่น้อยกว่า ๓,๐๐๐,๐๐๐ บาท

(๓) กรณีที่ปรึกษาผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอ ผู้ยื่นข้อเสนอต้องมีวงเงินสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยมียอดเงินรวมของวงเงินสินเชื่อไม่น้อยกว่า ๒,๘๐๗,๙๕๐ บาทคิดเป็น ๑ ใน ๔ ของมูลค่าโครงการหรือรายการที่ยื่นเสนอในแต่ละครั้ง ซึ่งสำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

Proof

(๔) กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาจะต้องแสดงหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่าไม่น้อยกว่ากว่า ๒,๘๐๗,๙๕๐ บาท คิดเป็น ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

คุณสมบัติในข้อนี้ ยกเว้นกรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ หรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑

๑๒. ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

กิจการร่วมค้าที่ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน เว้นแต่ในกรณีกิจการร่วมค้าที่มีข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียว เป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงดังกล่าวจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญา มากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

ทั้งนี้ กิจการร่วมค้า หมายถึง “กิจการที่มีข้อตกลงระหว่างผู้เข้าร่วมค้าเป็นลายลักษณ์อักษรว่าจะดำเนินการร่วมกันเป็นทางการค้าหรือหากำไรระหว่างบริษัทกับบริษัท บริษัทกับห้างหุ้นส่วนนิติบุคคล ห้างหุ้นส่วนนิติบุคคลกับห้างหุ้นส่วนนิติบุคคล หรือระหว่างบริษัทและ/หรือห้างหุ้นส่วนนิติบุคคลกับบุคคลธรรมดาคณะบุคคลที่มิใช่นิติบุคคล ห้างหุ้นส่วนสามัญ นิติบุคคลอื่น หรือนิติบุคคลที่ตั้งขึ้นตามกฎหมายของต่างประเทศ โดยข้อตกลงนั้นอาจกำหนดให้มีผู้เข้าร่วมค้าหลักก็ได้”

Proof

แบบหนังสือรับรองวงเงินสินเชื่อ

เลขที่..... วันที่.....

เรื่อง รับรองวงเงินสินเชื่อ

ตามที่.....(ชื่อผู้ประกอบการ นิติบุคคล/บุคคลธรรมดา).....เลขประจำตัวผู้เสียภาษีอากร /เลขประจำตัวประชาชนเลขที่.....จะยื่นข้อเสนอในงาน จ้างที่ปรึกษาเพื่อตรวจติดตามรอบที่ ๒ สำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001, 27701, 27035 และการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งตามหลักเกณฑ์และวิธีการคัดเลือกเป็นผู้ประกอบการงาน จ้างที่ปรึกษาเพื่อตรวจติดตามรอบที่ ๒ สำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001, 27701, 27035 และการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ยื่นคำขอต้องเสนอหนังสือรับรองวงเงินสินเชื่อ/จะเข้ายื่นข้อเสนอกับหน่วยงานของรัฐซึ่งเงื่อนไขการยื่นข้อเสนอกรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอ ที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอต้องขอวงเงินสินเชื่อจากธนาคาร โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่า งบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จึงมีความประสงค์ให้ธนาคาร ..... (ชื่อธนาคาร).....รับรองวงเงินสินเชื่อเพื่อประกอบการพิจารณาด้วย นั้น

.....(ชื่อธนาคาร).....ขอรับรองว่า.....(ชื่อผู้ประกอบการ นิติบุคคล/บุคคลธรรมดา).....มีวงเงินทุนหมุนเวียนในวงเงินไม่ต่ำกว่า.....บาท (.....จำนวนเงินเป็นอักษร.....) และยินดีให้วงเงินสินเชื่อภายในวงเงิน ..... บาท (.....จำนวนเงินเป็นอักษร.....)

ขอแสดงความนับถือ

.....

.....(ชื่อผู้ลงนาม).....

.....(ชื่อธนาคาร).....

แบบหนังสือรับรองวงเงินสินเชื่ออิเล็กทรอนิกส์

เลขที่..... วันที่.....

เรื่อง รับรองวงเงินสินเชื่อ

ตามที่.....(ชื่อผู้ประกอบการ นิติบุคคล/บุคคลธรรมดา).....เลขประจำตัวผู้เสียภาษีอากร /เลขประจำตัวประชาชนเลขที่.....จะยื่นข้อเสนอในงาน จ้างที่ปรึกษาเพื่อตรวจติดตามรอบที่ ๒ สำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001, 27701, 27035 และการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งตามหลักเกณฑ์และวิธีการคัดเลือกเป็นผู้ประกอบการงาน จ้างที่ปรึกษาเพื่อตรวจติดตามรอบที่ ๒ สำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001, 27701, 27035 และการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ยื่นคำขอต้องเสนอหนังสือรับรองวงเงินสินเชื่อ/จะเข้ายื่นข้อเสนอกับหน่วยงานของรัฐซึ่งเงื่อนไขการยื่นข้อเสนอกรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอ ที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอต้องขอวงเงินสินเชื่อจากธนาคาร โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่า งบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จึงมีความประสงค์ให้ธนาคาร..... (ชื่อธนาคาร).....รับรองวงเงินสินเชื่อเพื่อประกอบการพิจารณาด้วย นั้น

.....(ชื่อธนาคาร).....ขอรับรองว่า.....(ชื่อผู้ประกอบการนิติบุคคล/บุคคลธรรมดา).....มีวงเงินทุนหมุนเวียนในวงเงินไม่ต่ำกว่า.....
บาท(.....จำนวนเงินเป็นอักษร.....) และยินดีให้วงเงินสินเชื่อภายในวงเงิน .....
บาท (.....จำนวนเงินเป็นอักษร.....)

ขอแสดงความนับถือ

..... (ชื่อธนาคาร).....

** เอกสารฉบับนี้จัดพิมพ์โดยระบบอิเล็กทรอนิกส์ **

Proof

การกำหนดเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

๑. ผลงานที่ผ่านมาของผู้ยื่นข้อเสนอ (น้ำหนักร้อยละ ๓๐)

ในหัวข้อนี้ จะพิจารณาการให้คะแนนในเชิงคุณภาพและเชิงปริมาณ ดังนี้

(๑) ผลงานของที่ปรึกษา : โดยพิจารณาจากลักษณะของผลงานที่มีขอบเขตและวิธีการนำเสนอที่สอดคล้องหรือใกล้เคียงกับลักษณะงานตามขอบเขตของงานและวัตถุประสงค์มากที่สุด

(๒) ประสบการณ์เฉพาะ : โดยพิจารณาจากผลงาน จำนวนผลงาน และมูลค่าของผลงานที่มีลักษณะสอดคล้องหรือใกล้เคียงกับงานตามขอบเขตของงาน โดยเทียบสัดส่วนกับจำนวนผลงานของผู้ยื่นข้อเสนอด้วยกัน

เกณฑ์การพิจารณาที่ให้คะแนน	ระดับคะแนน
๑. ผลงานที่ผ่านมาของผู้ยื่นข้อเสนอ (๑๐๐ คะแนน) (น้ำหนักร้อยละ ๓๐) มีผลงานที่ผ่านมาจำนวนอย่างน้อย ๑ โครงการ/ชิ้นงาน ที่มีขอบเขตงานตรงหรือใกล้เคียงกับเนื้องานของโครงการนี้ เช่น เคยเป็นที่ปรึกษาให้กับหน่วยงานภาครัฐหรือเอกชนจนได้รับการรับรองตามมาตรฐาน ISO/IEC 27001:2013 หรือ ISO/IEC 27701:2019 หรือ ISO/IEC 27035 และมีประวัติเคยเป็นที่ปรึกษาให้กับหน่วยงานที่ปฏิบัติหน้าที่กำกับดูแล หรือเคยดำเนินการพัฒนา ปรับปรุง กระบวนการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	
๑.๑ ผลงานของที่ปรึกษา : ผลงานที่ผ่านมาตามข้อ ๑๐.๒.๑ (๑๐๐ คะแนน) (น้ำหนักร้อยละ ๑๕)	
มีการนำเสนอผลงานที่ผ่านมา โดยในขอบเขตงานที่นำเสนอมีการให้คำปรึกษาหน่วยงานจนผ่านการรับรองตามมาตรฐาน ISO/IEC 27001:2013 และ ISO/IEC 27701:2019 และ ISO/IEC 27035 และ มาตรฐานอื่น ๆ เช่น ISO/IEC 22301 เป็นต้น	๑๐๐ คะแนน
มีการนำเสนอผลงานที่ผ่านมา โดยในขอบเขตงานที่นำเสนอมีการให้คำปรึกษาหน่วยงานจนผ่านการรับรองตามมาตรฐาน ISO/IEC 27001:2013 และ ISO/IEC 27701:2019	๙๐ คะแนน
มีการนำเสนอผลงานที่ผ่านมา โดยในขอบเขตงานที่นำเสนอมีการให้คำปรึกษาหน่วยงานจนผ่านการรับรองตามมาตรฐาน ISO/IEC 27001:2013 เพียงมาตรฐานเดียว	๘๐ คะแนน
๑.๒ ประสบการณ์เฉพาะ : จำนวนผลงานที่ผ่านมา (๑๐๐ คะแนน) (น้ำหนักร้อยละ ๑๕)	
มีผลงานการตรวจติดตาม การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001, ISO/IEC 27701 และ ISO/IEC 27035 รวมกันจำนวน ๓ มาตรฐาน	๑๐๐ คะแนน
มีผลงานการตรวจติดตาม การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ที่เป็นมาตรฐาน ISO/IEC 27001 หรือ ISO/IEC 27701 หรือ ISO/IEC 27035 จำนวน ๒ ใน ๓ รวมกันจำนวน ๒ มาตรฐาน	๙๐ คะแนน
มีผลงานการตรวจติดตาม การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ที่เป็นมาตรฐาน ISO/IEC 27001 หรือ ISO/IEC 27701 หรือ ISO/IEC 27035 อันใดอันหนึ่ง	๘๐ คะแนน

Proof

๒. วิธีการบริหารและวิธีปฏิบัติงาน (น้ำหนักร้อยละ ๓๐)

ในหัวข้อนี้ จะพิจารณาการให้คะแนนจากข้อเสนอที่สามารถนำขอบเขตของงานที่กำหนดไว้มาจัดทำเป็นแผนและวิธีการการดำเนินงาน การตรวจสอบ ที่สอดคล้องกับระยะเวลาดำเนินงานของสำนักงาน กสทช. ได้ชัดเจนและเป็นรูปธรรมมากที่สุด

รายละเอียดการให้คะแนน	ระดับคะแนน
๒. วิธีการบริหารและวิธีการดำเนินงาน (๑๐๐ คะแนน) (น้ำหนักร้อยละ ๓๐)	
เกณฑ์การพิจารณาที่ให้คะแนน	คะแนน
อธิบายแต่ละหัวข้อตามขอบเขตของงาน พร้อมทั้งมีการอธิบายวิธีการอย่างชัดเจน มีกรอบแนวคิดและแผนการดำเนินงานตามวัตถุประสงค์และขอบเขตของงานมีรายละเอียดอย่างชัดเจน มีกรอบระยะเวลาการดำเนินการและแจกแจงบุคคลากรที่รับผิดชอบตามแผนการดำเนินงาน และมีการนำเอากรอบมาตรฐานสากลหรือกรอบแนวคิดที่เป็นประโยชน์เข้ามาประยุกต์ใช้กับการดำเนินงานและสามารถตอบวัตถุประสงค์และขอบเขตของงาน และมีแผนงานที่สามารถนำไปปฏิบัติได้จริง	
๑. ศึกษา วิเคราะห์ และจัดทำรายงานผลการศึกษาเบื้องต้น (Inception Report) - แนวทางการจัดทำแผนการดำเนินโครงการที่เป็นภาพรวมของโครงการตลอดระยะเวลาการดำเนินโครงการที่สะท้อนถึงเนื้องานตามขอบเขตงานจ้างที่ปรึกษา	๒๐
๒. การดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล ที่ปรึกษาต้องดำเนินการให้คำปรึกษาและแนะนำแก่คณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อปฏิบัติให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และการเป็นที่ปรึกษาให้กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) - แนวทางการตรวจประเมินด้านการคุ้มครองข้อมูลส่วนบุคคล ตามหน้าที่รับผิดชอบขอบเขตงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อประเมินความสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ตามแนวปฏิบัติที่ดี หรือตามข้อกำหนดของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	๒๕
๓. การดำเนินการตามมาตรฐาน ISO/IEC จำนวน ๓ มาตรฐาน ที่ปรึกษาต้องดำเนินการให้คำปรึกษาและแนะนำแก่พนักงานของสำนักงาน กสทช. เพื่อพัฒนาปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC 27001:2022 การบริหารจัดการข้อมูลส่วนบุคคลตามมาตรฐานสากล ISO/IEC 27701:2019 สำหรับรอบการตรวจติดตามรอบที่ ๒ และการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27035:2023 ตามขอบเขตที่สำนักเทคโนโลยีสารสนเทศกำหนด - แนวทางการทบทวนและปรับปรุงแก้ไขนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ สอดคล้องตามกฎหมายและมาตรฐานที่เกี่ยวข้อง และบริบทขององค์กรทั้งภายในและภายนอก	๒๕
๔. การตรวจสอบระบบสารสนเทศนอกขอบเขต ISO และการพัฒนาทีมผู้ตรวจประเมินที่ปรึกษาดำเนินการเตรียมการโดยจัดทำแผนตรวจประเมินความสอดคล้องตามประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๕ โดยพัฒนาพนักงานของสำนักงาน กสทช. ที่เป็นทีมตรวจประเมิน กระบวนการ และเครื่องมือในการตรวจประเมิน สร้างทักษะการจัดการด้านความมั่นคงปลอดภัยไซเบอร์ให้กับสำนักที่เป็นเจ้าของระบบสารสนเทศ	๓๐

Proof

- แนวทางการดำเนินการสอนทีมตรวจประเมินเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
วิธีการให้คะแนน : พิจารณาให้คะแนนแต่ละหัวข้อย่อย ดังนี้ - อธิบายแต่ละส่วนหรือขั้นตอนในข้อนั้นได้ครบถ้วน ชัดเจน ได้คะแนน ๑๐๐% - อธิบายแต่ละส่วนหรือขั้นตอนในข้อนั้นครบแต่ขาดความชัดเจน หรือขาดความสมบูรณ์ในส่วนใดส่วนหนึ่ง หรือขั้นตอนใดขั้นตอนหนึ่ง ได้คะแนน ๘๒% - อธิบายแต่ละส่วนหรือขั้นตอนในข้อนั้นครบแต่ขาดความชัดเจน หรือขาดความสมบูรณ์ในหลายส่วนหรือหลายขั้นตอน ได้คะแนน ๗๒% - อธิบายไม่ครบส่วนหรือขั้นตอน ได้คะแนน ๕๐% - ไม่อธิบายในหัวข้อนั้น ไม่ได้คะแนน	

Proof

<table>
<tr><th>รายละเอียดการให้คะแนน</th><th colspan="8">ระดับคะแนน</th></tr>
<tr><td colspan="9">๓. จำนวนและคุณลักษณะเฉพาะของบุคลากรที่ร่วมงาน (น้ำหนักร้อยละ ๑๐)</td></tr>
<tr><td colspan="9">โดยที่ปรึกษาจะต้องแสดงรายละเอียดคุณวุฒิการศึกษา ความเชี่ยวชาญหรือประสบการณ์ของบุคลากรหลัก และประกาศนียบัตรตามขอบเขตงานข้อ ๕ (ถ้ามี) พร้อมเอกสารหลักฐานอ้างอิง
โดยมีคะแนนรวมทั้งสิ้น ๑๐๐ คะแนน ซึ่งผู้ประเมินจะให้คะแนนแก่บุคลากรของผู้ยื่นข้อเสนอทั้ง ๑๓ คน ดังนี้</td></tr>
<tr><td rowspan="3">๑. ผู้จัดการโครงการ
จะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๑)</td><td colspan="8">คะแนนเต็ม ๘ คะแนน</td></tr>
<tr><td colspan="3">ด้านประสบการณ์
(๔ คะแนน)</td><td colspan="5">ด้านวุฒิการศึกษา
(๔ คะแนน)</td></tr>
<tr><td>มากกว่า ๑๕ ปี</td><td>มากกว่า ๑๐ ปี</td><td>๑๐ ปี</td><td colspan="3">ปริญญาเอก</td><td colspan="2">ปริญญาโท</td></tr>
<tr><td>๔ คะแนน</td><td>๓.๖ คะแนน</td><td>๓.๒ คะแนน</td><td colspan="3">๔ คะแนน</td><td colspan="2">๓.๒ คะแนน</td></tr>
<tr><td rowspan="3">๒. ที่ปรึกษาโครงการ
จะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๒)</td><td colspan="8">คะแนนเต็ม ๑๐ คะแนน</td></tr>
<tr><td colspan="3">ด้านประสบการณ์
(๔ คะแนน)</td><td colspan="2">ด้านวุฒิการศึกษา
(๓ คะแนน)</td><td colspan="3">ด้านประกาศนียบัตร
(๓ คะแนน)</td></tr>
<tr><td>มากกว่า ๑๕ ปี</td><td>มากกว่า ๑๐ ปี</td><td>๑๐ ปี</td><td>ปริญญาเอก</td><td>ปริญญาโท</td><td>มากกว่า ๒ ใบ</td><td>๒ ใบ</td><td>๑ ใบ</td></tr>
<tr><td>๔ คะแนน</td><td>๓.๖ คะแนน</td><td>๓.๒ คะแนน</td><td>๓ คะแนน</td><td>๒.๔ คะแนน</td><td>๓ คะแนน</td><td>๒.๗ คะแนน</td><td>๒.๔ คะแนน</td></tr>
<tr><td rowspan="3">๓. หัวหน้าทีมที่ปรึกษา PDPA
จะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๓)</td><td colspan="8">คะแนนเต็ม ๑๐ คะแนน</td></tr>
<tr><td colspan="3">ด้านประสบการณ์
(๔ คะแนน)</td><td colspan="2">ด้านวุฒิการศึกษา
(๓ คะแนน)</td><td colspan="3">ด้านประกาศนียบัตร
(๓ คะแนน)</td></tr>
<tr><td>มากกว่า ๑๕ ปี</td><td>มากกว่า ๑๐ ปี</td><td>๑๐ ปี</td><td>ปริญญาเอก</td><td>ปริญญาโท</td><td>มากกว่า ๒ ใบ</td><td>๒ ใบ</td><td>๑ ใบ</td></tr>
<tr><td>๔ คะแนน</td><td>๓.๖ คะแนน</td><td>๓.๒ คะแนน</td><td>๓ คะแนน</td><td>๒.๔ คะแนน</td><td>๓ คะแนน</td><td>๒.๗ คะแนน</td><td>๒.๔ คะแนน</td></tr>
<tr><td rowspan="3">๔. ทีมที่ปรึกษา PDPA (คนที่ ๑)
จะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๔)</td><td colspan="8">คะแนนเต็ม ๘ คะแนน</td></tr>
<tr><td colspan="3">ด้านประสบการณ์
(๓ คะแนน)</td><td colspan="2">ด้านวุฒิการศึกษา
(๒ คะแนน)</td><td colspan="3">ด้านประกาศนียบัตร
(๓ คะแนน)</td></tr>
<tr><td>มากกว่า ๑๐ ปี</td><td>มากกว่า ๕ ปี</td><td>๕ ปี</td><td>ปริญญาโท</td><td>ปริญญาตรี</td><td>มากกว่า ๒ ใบ</td><td>๒ ใบ</td><td>๑ ใบ</td></tr>
<tr><td>๓ คะแนน</td><td>๒.๗ คะแนน</td><td>๒.๔ คะแนน</td><td>๒ คะแนน</td><td>๑.๖ คะแนน</td><td>๓ คะแนน</td><td>๒.๗ คะแนน</td><td>๒.๔ คะแนน</td></tr>
</table>

Proof

๕. ทีมที่ปรึกษา PDPA (คนที่ ๒) จะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๔)	**คะแนนเต็ม ๘ คะแนน**							
	ด้านประสบการณ์ (๓ คะแนน)			ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๓ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี	มากกว่า ๒ ใบ	๒ ใบ	๑ ใบ
	๓ คะแนน	๒.๗ คะแนน	๒.๔ คะแนน	๒ คะแนน	๑.๖ คะแนน	๓ คะแนน	๒.๗ คะแนน	๒.๔ คะแนน
๖. ทีมที่ปรึกษา PDPA (คนที่ ๓) จะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๔)	**คะแนนเต็ม ๘ คะแนน**							
	ด้านประสบการณ์ (๓ คะแนน)			ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๓ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี	มากกว่า ๒ ใบ	๒ ใบ	๑ ใบ
	๓ คะแนน	๒.๗ คะแนน	๒.๔ คะแนน	๒ คะแนน	๑.๖ คะแนน	๓ คะแนน	๒.๗ คะแนน	๒.๔ คะแนน
๗. หัวหน้าทีมที่ปรึกษาด้านเทคนิค จะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๕)	**คะแนนเต็ม ๑๐ คะแนน**							
	ด้านประสบการณ์ (๔ คะแนน)			ด้านวุฒิการศึกษา (๓ คะแนน)		ด้านประกาศนียบัตร (๓ คะแนน)		
	มากกว่า ๑๕ ปี	มากกว่า ๑๐ ปี	๑๐ ปี	ปริญญาเอก	ปริญญาโท	มากกว่า ๒ ใบ	๒ ใบ	๑ ใบ
	๔ คะแนน	๓.๖ คะแนน	๓.๒ คะแนน	๓ คะแนน	๒.๔ คะแนน	๓ คะแนน	๒.๗ คะแนน	๒.๔ คะแนน
๘. ผู้เชี่ยวชาญอาวุโสด้านความปลอดภัยความปลอดภัยคอมพิวเตอร์ จะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๖)	**คะแนนเต็ม ๘ คะแนน**							
	ด้านประสบการณ์ (๓ คะแนน)			ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านวุฒิการศึกษา (๓ คะแนน)		
	มากกว่า ๑๕ ปี	มากกว่า ๑๐ ปี	๑๐ ปี	ปริญญาเอก	ปริญญาโท	มากกว่า ๒ ใบ	๒ ใบ	๑ ใบ
	๓ คะแนน	๒.๗ คะแนน	๒.๔ คะแนน	๒ คะแนน	๑.๖ คะแนน	๓ คะแนน	๒.๗ คะแนน	๒.๔ คะแนน
๙. ทีมที่ปรึกษาด้านเทคนิค คนที่ ๑ จะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๗)	**คะแนนเต็ม ๘ คะแนน**							
	ด้านประสบการณ์ (๓ คะแนน)			ด้านวุฒิการศึกษา (๒ คะแนน)		ด้านประกาศนียบัตร (๓ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี	มากกว่า ๒ ใบ	๒ ใบ	๑ ใบ
	๓ คะแนน	๒.๗ คะแนน	๒.๔ คะแนน	๒ คะแนน	๑.๖ คะแนน	๓ คะแนน	๒.๗ คะแนน	๒.๔ คะแนน

Proof

<table>
<tr><td rowspan="3">๑๐. ทีมที่ปรึกษาด้านเทคนิค คนที่ ๒
จะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๗)</td><td colspan="8">คะแนนเต็ม ๘ คะแนน</td></tr>
<tr><td colspan="3">ด้านประสบการณ์
(๓ คะแนน)</td><td colspan="2">ด้านวุฒิการศึกษา
(๒ คะแนน)</td><td colspan="3">ด้านประกาศนียบัตร
(๓ คะแนน)</td></tr>
<tr><td>มากกว่า ๑๐ ปี</td><td>มากกว่า ๕ ปี</td><td>๕ ปี</td><td>ปริญญาโท</td><td>ปริญญาตรี</td><td>มากกว่า ๒ ใบ</td><td>๒ ใบ</td><td>๑ ใบ</td></tr>
<tr><td>๓ คะแนน</td><td>๒.๗ คะแนน</td><td>๒.๔ คะแนน</td><td>๒ คะแนน</td><td>๑.๖ คะแนน</td><td>๓ คะแนน</td><td>๒.๗ คะแนน</td><td>๒.๔ คะแนน</td></tr>
<tr><td rowspan="3">๑๑. ผู้เชี่ยวชาญระดับอาวุโสด้าน Internal Audit
จะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๘)</td><td colspan="8">คะแนนเต็ม ๘ คะแนน</td></tr>
<tr><td colspan="3">ด้านประสบการณ์
(๓ คะแนน)</td><td colspan="2">ด้านวุฒิการศึกษา
(๒ คะแนน)</td><td colspan="3">ด้านประกาศนียบัตร
(๓ คะแนน)</td></tr>
<tr><td>มากกว่า ๑๐ ปี</td><td>มากกว่า ๕ ปี</td><td>๕ ปี</td><td>ปริญญาเอก</td><td>ปริญญาโท</td><td>มากกว่า ๒ ใบ</td><td>๒ ใบ</td><td>๑ ใบ</td></tr>
<tr><td>๓ คะแนน</td><td>๒.๗ คะแนน</td><td>๒.๔ คะแนน</td><td>๒ คะแนน</td><td>๑.๖ คะแนน</td><td>๓ คะแนน</td><td>๒.๗ คะแนน</td><td>๒.๔ คะแนน</td></tr>
<tr><td rowspan="3">๑๒. ผู้เชี่ยวชาญด้าน Business Continuity Management
จะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๙)</td><td colspan="8">คะแนนเต็ม ๖ คะแนน</td></tr>
<tr><td colspan="3">ด้านประสบการณ์
(๒ คะแนน)</td><td colspan="2">ด้านวุฒิการศึกษา
(๒ คะแนน)</td><td colspan="3">ด้านประกาศนียบัตร
(๒ คะแนน)</td></tr>
<tr><td>มากกว่า ๑๐ ปี</td><td>มากกว่า ๕ ปี</td><td>๕ ปี</td><td>ปริญญาโท</td><td>ปริญญาตรี</td><td>มากกว่า ๒ ใบ</td><td>๒ ใบ</td><td>๑ ใบ</td></tr>
<tr><td>๒ คะแนน</td><td>๑.๘ คะแนน</td><td>๑.๖ คะแนน</td><td>๒ คะแนน</td><td>๑.๖ คะแนน</td><td>๒ คะแนน</td><td>๑.๘ คะแนน</td><td>๑.๖ คะแนน</td></tr>
<tr><td colspan="9">การให้คะแนนในหัวข้อนี้ จะขึ้นอยู่กับประสบการณ์ คุณวุฒิ และประกาศนียบัตรที่เกี่ยวข้องของบุคลากรหลักและบุคลากรสนับสนุนที่เสนอ เป็นไปตามที่กำหนดตามข้อ ๕ นอกจากนี้ จะพิจารณารายละเอียดและความครอบคลุมครบถ้วนดังกล่าวแล้ว จะพิจารณาเปรียบเทียบระหว่างข้อเสนอของผู้ยื่นข้อเสนอแต่ละราย ข้อเสนอที่ดีที่สุดจะได้คะแนนเต็มหรือได้มากที่สุด ข้อเสนอที่ดีรองลงไปจะได้คะแนนลดหลั่นตามความเหมาะสมในช่วงคะแนนของหัวข้อนั้น</td></tr>
</table>

Proof