

ขอบเขตงาน (Term of Reference)

จ้างที่ปรึกษาเพื่อพัฒนาปรับปรุงแก้ไขการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
ตามมาตรฐาน ISO/IEC 27001, 27701, 27035 และการรักษาความมั่นคงปลอดภัยไซเบอร์
ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑. หลักการและเหตุผล

ตามที่ได้มีการบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) ในฐานะหน่วยงานภาครัฐและหน่วยงานควบคุม กำกับหรือดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CI) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ซึ่งจัดเป็นหน่วยงานที่มีความสำคัญทั้งภาพลักษณ์และการสร้างมาตรฐานที่ดีของสำนักงาน กสทช. ในการดำเนินงานให้สอดคล้องกับพระราชบัญญัติข้างต้น ขณะเดียวกันด้านการคุ้มครองข้อมูลส่วนบุคคล สำนักงาน กสทช. ในฐานะที่เป็นหน่วยงานกำกับดูแลจำเป็นต้องต้องแสดงบทบาทสำคัญในการเป็นหน่วยงานต้นแบบในการกำกับดูแลและคุ้มครองข้อมูลส่วนบุคคล เพื่อทำหน้าที่เป็นเสาหลักในการกำกับดูแลกิจการภายใต้การกำกับดูแลให้ปฏิบัติสอดคล้องตามด้วย จึงเป็นที่มาที่สำนักงาน กสทช. จะต้องริเริ่มในการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล ตามมาตรฐานสากลที่เกี่ยวข้อง มีการพัฒนาบุคลากร กระบวนการ และเครื่องมือให้เข้มแข็งทั้งในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และด้านการคุ้มครองข้อมูลส่วนบุคคล

เพื่อไปสู่จุดมุ่งหมายดังกล่าว สำนักงาน กสทช. โดยสำนักเทคโนโลยีสารสนเทศ (นบ.) ได้มีการดำเนินงานในเบื้องต้นโดยจัดทำกระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2022 กระบวนการบริหารจัดการความมั่นคงปลอดภัยข้อมูลส่วนบุคคลตามมาตรฐาน ISO/IEC 27701:2019 จนได้รับการรับรองตามมาตรฐานทั้งสองดังกล่าวตั้งแต่ปี พ.ศ. ๒๕๖๖ โดยดำเนินการจ้างที่ปรึกษาเพื่อปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 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) อย่างไรก็ตามยังมีความจำเป็นที่จะต้องมีการบำรุงรักษากระบวนการดังกล่าวเหล่านี้ไว้เพื่อขยายผลให้สำนักงาน กสทช. มีมาตรฐานในการดำเนินงานและมีความพร้อมรองรับการตรวจประเมินจากผู้ตรวจประเมินภายนอก (Certification Body) ซึ่งเป็นส่วนหนึ่งที่จะช่วยตอบโจทย์ด้านการพัฒนาบุคลากร และกระบวนการในการปรับปรุงและพัฒนาในด้านเหล่านี้อย่างต่อเนื่องต่อไป อีกทั้ง ต้องเพิ่มเติมในด้านของการพัฒนาเครื่องมือเพื่อใช้ในการประเมินและตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และด้านการคุ้มครองข้อมูลส่วนบุคคล และต้องพัฒนาบุคลากรของสำนักงาน กสทช. ให้มีความรู้ความเข้าใจ และมีความสามารถในการนำกระบวนการของมาตรฐานไปประยุกต์ใช้กับงานของตน และสามารถใช้อุปกรณ์ในการตรวจประเมินทั้งในด้านของการรักษาความมั่นคงปลอดภัยและด้านการคุ้มครองข้อมูลส่วนบุคคลต่อไปด้วยตนเองได้

เพื่อให้สอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ข้อ ๒๒.๒.๓ - ๒๒.๒.๕ ซึ่งระบุให้หน่วยงานต้องมีการดำเนินการ ดังนี้ (๑) การกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ (๒) ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) (๓) ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) (๔) ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management 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 เพื่อให้สอดคล้องต่อข้อกำหนดดังกล่าว สำนักงาน กสทช. จะต้องมี การดำเนินการจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย และดำเนินการตรวจสอบค่าคอนฟิกูเรชันของอุปกรณ์ประมวลผลสารสนเทศ เพื่อป้องกันความเสี่ยงจากการถูกโจมตีด้วยภัยคุกคามทางไซเบอร์

รวมทั้ง เพื่อให้สอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. ๒๕๖๗ ข้อ ๕ (๓) ตรวจสอบการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน ให้เป็นไปตามมาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนด และจัดทำรายงานสรุปผลการตรวจสอบให้แก่สำนักงานภายใน ๓๐ วัน หลังกระบวนการตรวจสอบเสร็จสิ้น ทั้งนี้ ในการดำเนินการดังกล่าว ให้หน่วยงานควบคุมหรือกำกับดูแลแต่งตั้งกลุ่มบุคคลทำหน้าที่เป็นผู้ตรวจสอบอันประกอบไปด้วยหัวหน้าทีมผู้ตรวจสอบ (Lead Auditor) และผู้ตรวจสอบ (Auditor) ที่มีความรู้ความเชี่ยวชาญด้านการตรวจสอบเรื่องความมั่นคงปลอดภัยไซเบอร์ ในกรณีที่พบว่า การดำเนินการไม่เป็นไปตามมาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนด ให้หน่วยงานควบคุมหรือกำกับดูแล แจ้งหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแก้ไขให้ได้มาตรฐาน พร้อมทั้งกำหนดเวลา ให้ดำเนินการหากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ดำเนินการภายในระยะเวลาที่กำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้ง กกม. เพื่อดำเนินการตามมาตรา ๕๓ วรรคสอง ต่อไป ซึ่งสำนักงานจะต้องจัดเตรียมที่ปรึกษาเพื่อตรวจสอบการดำเนินงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับดูแลของสำนักงาน กสทช. และจัดทำรายงานสรุปผลการตรวจสอบให้แก่ สกมช. ตามระยะเวลาที่กำหนด

ดังนั้น เพื่อให้สำนักเทคโนโลยีสารสนเทศ สำนักงาน กสทช. ปฏิบัติตามเป้าหมายดังกล่าวได้ครบถ้วน จึงมีความจำเป็นต้องจัดจ้างที่ปรึกษาเพื่อเข้ามาดำเนินการ

๑) เพื่อพัฒนา ปรับปรุง แก้ไขการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2022 การบริหารจัดการข้อมูลส่วนบุคคล ตามมาตรฐาน ISO/IEC 27701:2019 และการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27035:2023 และการปฏิบัติตามมาตรฐาน NIST Cybersecurity Framework

๒) การตรวจประเมินและปรับปรุงแก้ไขตามประกาศ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ขยายผลระบบสารสนเทศทั้งแอปพลิเคชัน เว็บแอปพลิเคชัน เว็บไซต์ หรือระบบการบริหารจัดการข้อมูลดิจิทัลของสำนักงาน กสทช.

โดยการพัฒนาบุคลากร กระบวนการ และเครื่องมือในการตรวจประเมินและปฏิบัติตามกระบวนการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์

๓) การจัดทำและตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของบริการที่สำคัญ

๔) พัฒนาและปรับปรุงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ นโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนกระบวนการ วิธีปฏิบัติ ประกาศความเป็นส่วนตัว การขอความยินยอม การตอบสนองสิทธิของเจ้าของข้อมูลส่วนบุคคล การบริหารจัดการกรณีเกิดการรั่วไหลของข้อมูลส่วนบุคคล หรือกระบวนการอื่น ๆ ที่เกี่ยวข้อง ให้มีความทันสมัยและสอดคล้องกับกฎหมาย ลำดับรอง รวมถึง ระเบียบและข้อบังคับที่ได้มีการประกาศขึ้นมาในภายหลัง และเป็นไปตามมาตรฐานสากล

๕) มีการสร้างความตระหนักในการปฏิบัติตามนโยบายและแนวปฏิบัติดังกล่าวให้กับบุคลากรของสำนักงาน กสทช. เพื่อให้เกิดประสิทธิภาพและประสิทธิผลสูงสุดในการดำเนินการของสำนักงาน กสทช. ด้านความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย ตลอดจนขยายผลไปสู่ภาพรวมของสำนักงาน กสทช. รวมถึงเป็นการธำรงไว้ซึ่งชื่อเสียง ภาพลักษณ์ และเป็นการปฏิบัติให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง

๖) จัดเตรียมคณะผู้ตรวจสอบและผู้ตรวจสอบที่มีความรู้ความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ จัดทำแผนการตรวจสอบ ดำเนินการตรวจสอบ และจัดทำรายงานผลการตรวจสอบ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านรักษาความปลอดภัยไซเบอร์ ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับดูแลของสำนักงาน กสทช.

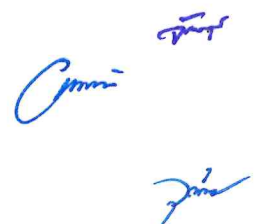
๒. วัตถุประสงค์

เพื่อพัฒนาปรับปรุงแก้ไขการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001, 27701, 27035 และการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓. คุณสมบัติของที่ปรึกษา

๓.๑. ผู้ยื่นข้อเสนอต้องมีคุณสมบัติพื้นฐานที่กำหนด ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ ตลอดจนแนวปฏิบัติตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐ ตามภาคผนวก ๑

๓.๒. มีผลงานที่ผ่านมาที่มีขอบเขตงานใกล้เคียงหรือเท่ากับเนื้อหาของโครงการนี้ เช่น เคยเป็นที่ปรึกษาให้กับหน่วยงานภาครัฐหรือเอกชนจนได้รับการรับรองตามมาตรฐาน ISO/IEC 27001:2022 หรือ ISO/IEC 27701:2019 หรือมีประวัติเคยเป็นที่ปรึกษาให้กับหน่วยงานที่ปฏิบัติหน้าที่กำกับดูแล หรือเคยดำเนินการพัฒนา ปรับปรุง กระบวนการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีมูลค่าโครงการไม่น้อยกว่า ๒,๐๐๐,๐๐ บาท (สองล้านบาทถ้วน) ภายใต้สัญญาเดียวที่ดำเนินการเสร็จสิ้นแล้ว และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐหรือหน่วยงานเอกชนที่สำนักงาน กสทช. เชื้อถือ โดยต้องส่งสำเนาหนังสือรับรองผลงานหรือสำเนาสัญญา มาพร้อมกับการยื่นข้อเสนอด้วย



๔. ขอบเขตของงานจ้างที่ปรึกษา

ขอบเขตของการดำเนินงานของที่ปรึกษาต้องประกอบด้วยงาน ดังต่อไปนี้

๔.๑. ในรอบการดำเนินงานนี้ ที่ปรึกษาจะต้องดำเนินการในบทบาทหน้าที่ของการให้คำปรึกษาและคำแนะนำแก่พนักงานของสำนักงาน กสทช. โดยการให้คำปรึกษาและแนะนำดังกล่าวเป็นไปเพื่อช่วยในการปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC 27001:2022 การบริหารจัดการข้อมูลส่วนบุคคลตามมาตรฐานสากล ISO/IEC 27701:2019 และการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27035:2023 ตามขอบเขตที่สำนักเทคโนโลยีสารสนเทศกำหนด ประกอบด้วยรายละเอียดอย่างน้อยต่อไปนี้

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

๔.๑.๒. ให้คำปรึกษาและคำแนะนำในการทบทวนและปรับปรุงแก้ไข เอกสารบริบทองค์กรที่จะส่งผลกระทบต่อการทำงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ การรักษาความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล โดยนำกรอบแนวคิด PESTEL Model มาใช้ในการดำเนินการ และให้สอดคล้องกับข้อกำหนดของมาตรฐาน ISO/IEC 27001:2022 มาตรฐานสากล 27001:2022 และมาตรฐาน ISO/IEC 27035:2023 รวมถึงประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๑.๓. ให้คำปรึกษาและคำแนะนำในการทบทวนเกณฑ์การประเมินความเสี่ยง และผลการประเมินความเสี่ยงให้สอดคล้องกับบริบทที่เกี่ยวข้อง รวมถึงทรัพย์สินสารสนเทศ ข้อมูลส่วนบุคคล และการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยตามขอบเขต โดยต้องมีการระบุถึงเหตุการณ์ภัยคุกคาม (Threats) จุดอ่อน (Vulnerabilities) และโอกาสเกิด (Likelihood) ภัยคุกคามนั้น ๆ ให้สอดคล้องกับข้อกำหนดของมาตรฐาน

๔.๑.๔. ให้คำปรึกษาและคำแนะนำในการปรับปรุงแก้ไขเอกสารแสดงมาตรการที่เลือกใช้ (SoA) ของมาตรฐาน ISO/IEC 27001:2022 มาตรฐานสากล ISO/IEC 27701:2019 และมาตรฐาน ISO/IEC 27035:2023 และ NIST Cybersecurity Framework รวมถึงข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับผลการประเมินความเสี่ยง

๔.๑.๕. ให้คำปรึกษาและคำแนะนำในการทบทวนและปรับปรุงแก้ไขนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ สอดคล้องตามกฎหมายและมาตรฐานที่เกี่ยวข้อง และบริบทขององค์กรทั้งภายในและภายนอก รวมถึงความคาดหวังและความต้องการจากผู้มีส่วนได้ส่วนเสียหรือบุคคลที่เกี่ยวข้อง (Interested parties) สำหรับขอบเขตที่กำหนดให้สอดคล้องตามมาตรฐาน ISO/IEC 27001:2022 มาตรฐานสากล ISO/IEC 27701:2019 และมาตรฐาน ISO/IEC 27035:2023 ตลอดจนมาตรฐานอื่นที่เกี่ยวข้อง รวมถึงประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๑.๖. 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 ครั้งภายหลังจากนำเสนอรายงานผลการตรวจสอบในครั้งแรก พร้อมทั้งจัดทำรายงานเปรียบเทียบผลการตรวจสอบช่องโหว่ของทั้งสองครั้ง และดำเนินการประชุมกับทีมงานผู้ดูแลระบบ เพื่อนำเสนอผลการดำเนินงาน

๔.๑.๗. ให้คำปรึกษาและสนับสนุนการนำเอกสารขึ้นประกาศในโปรแกรมบริหารจัดการเอกสาร และบริหารจัดการความเสี่ยง ที่มีลักษณะการใช้งานในรูปแบบของ Web-Based ที่สามารถนำมาประยุกต์ใช้ กับขั้นตอนปฏิบัติการบริหารจัดการความเสี่ยง ขั้นตอนปฏิบัติการควบคุมเอกสาร ที่มีการประกาศใช้งาน สำหรับรายการทรัพย์สินสารสนเทศตามขอบเขต และรายการเอกสารตามขอบเขต ตลอดจนสามารถค้นหา ข้อมูลและสร้างเงื่อนไขในการเรียกดูข้อมูลการประเมินความเสี่ยงได้ รวมถึงสามารถจัดทำเป็นรายงานเอกสารที่ ประกาศใช้งานและผลการประเมินความเสี่ยงได้

๔.๑.๘. ให้คำปรึกษาและคำแนะนำในการจัดทำเพิ่มเติม หรือปรับปรุงแก้ไข แผนและตัวชี้วัด เพื่อเป็นการวัดประสิทธิผลของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Effectiveness Measurement) ให้สอดคล้องตามมาตรฐานที่กำหนด

๔.๑.๙. ให้คำปรึกษาและคำแนะนำในการจัดทำ หรือปรับปรุง แผนบริหารความต่อเนื่องทาง ธุรกิจ (Business Continuity Plan) ให้กับระบบสารสนเทศตามขอบเขต และสอดคล้องตาม ข้อกำหนดของ มาตรฐาน ISO/IEC 27001:2022 มาตรฐานสากล ISO/IEC 27701:2019 และมาตรฐาน ISO/IEC 27035:2023 และ NIST Cybersecurity Framework รวมถึงประมวลแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ และ ให้คำปรึกษาและคำแนะนำในการดำเนินการซ้อมแผนบริหารความต่อเนื่องทางธุรกิจตามขอบเขตอย่างน้อย ๑ ครั้ง

๔.๑.๑๐. ให้คำปรึกษาและคำแนะนำในการตรวจสอบภายใน (Internal Auditor) รวมทั้งให้ คำปรึกษาและคำแนะนำแก่คณะตรวจสอบภายในที่ได้รับการแต่งตั้งจากคณะกรรมการบริหารจัดการความ มั่นคงปลอดภัยและบริการเทคโนโลยีสารสนเทศ (Security and Service Management Committee : SSMC)

๔.๑.๑๐.๑. ดำเนินการตรวจสอบภายในและจัดทำรายงานผลการตรวจสอบให้กับ ระบบบริหารจัดการตามมาตรฐาน ISO/IEC 27001:2022 มาตรฐานสากล ISO/IEC 27701:2019 และ มาตรฐาน ISO/IEC 27035:2023 จำนวน ๑ ครั้ง

๔.๑.๑๐.๒. ให้คำปรึกษา และคำแนะนำ ในการติดตามการแก้ไขข้อบกพร่องที่ตรวจ พบจากการตรวจสอบภายใน (Corrective and Preventive Actions) ของระบบบริหารจัดการตาม มาตรฐาน ISO/IEC 27001:2022 ISO/IEC 27701:2019 และ ISO/IEC 27035:2023

๔.๑.๑๑. ดำเนินการจัดให้มีการตรวจประเมินตาม NIST Cybersecurity Framework และให้ คำแนะนำในการปรับปรุงเพื่อลดช่องว่างจากผลตรวจประเมิน NIST Cybersecurity Framework รวมถึงให้ ข้อเสนอแนะเพื่อยกระดับการดำเนินการให้ดียิ่งขึ้น รวมถึงจัดเตรียมรายงานเพื่อส่ง สกมช. ตามมาตรา ๕๔ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

๔.๑.๑๒. ให้คำปรึกษา และคำแนะนำในการเตรียมการในส่วนความรับผิดชอบของผู้บริหาร (Management Review) เพื่อทบทวนการพัฒนาและการดำเนินงานระบบบริหารจัดการตามมาตรฐาน ISO/IEC 27001:2022 ISO/IEC 27701:2019 และ ISO/IEC 27035:2023 และดำเนินการเป็นที่ปรึกษา ให้คำแนะนำหรือข้อคิดเห็นหรือแนวปฏิบัติที่ดี (Best Practice) ในการประชุมคณะกรรมการบริหารจัดการ ความมั่นคงปลอดภัยและบริการเทคโนโลยีสารสนเทศ (Security and Service Management Committee : SSMC) ของสำนักงาน กสทช. ตามรอบการประชุม

๔.๑.๑๓. ให้คำปรึกษา และคำแนะนำ รวมทั้งให้การสนับสนุนการตรวจประเมินจาก Certification Body ในการตรวจรับรองระบบบริหารจัดการตามมาตรฐาน ISO/IEC 27001:2022 ISO/IEC 27701:2019 และ ISO/IEC 27035:2023 ตามขอบเขตที่กำหนด รวมทั้งให้คำปรึกษา และคำแนะนำใน การแก้ไข Non conformity (NC) (ถ้ามี) ที่ได้รับการตรวจประเมินของ Certification Body และจัดทำ แผนการดำเนินการเพื่อแก้ไขและตอบ NC ให้กับ Certification Body ภายในระยะเวลาที่กำหนด

๔.๒. ดำเนินการตรวจสอบ Security baseline configuration สำหรับ OS Platform ที่มีความสำคัญอย่างน้อย ๑ ระบบ เพื่อเป็นแนวทางตัวอย่างและให้คำแนะนำในการกำหนดค่าพารามิเตอร์ที่มีความมั่นคงปลอดภัยยิ่งขึ้น

๔.๓. ดำเนินการจัดทำ infographic สำหรับการสื่อสารประชาสัมพันธ์เพื่อสร้างความตระหนักรู้ในสำนักงาน กสทช. ที่เกี่ยวข้องกับนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ หรือองค์ความรู้ต่าง ๆ ด้านภัยคุกคามทางไซเบอร์ อย่างน้อย ๕ ชิ้นงาน

๔.๔. จัดเตรียมคณะผู้ตรวจสอบที่มีความรู้ความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ตามคุณสมบัติที่ สกมช. กำหนด และดำเนินการจัดทำแผนการตรวจสอบ ดำเนินการตรวจสอบ และจัดทำรายงานผลการตรวจสอบประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านรักษาความปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับดูแลของสำนักงาน กสทช. จำนวน ๘ แห่ง

๔.๕. ดำเนินการสร้างเสริมทักษะพนักงานของสำนักงาน กสทช. ตามขอบเขตการขอการรับรองและผู้ที่เกี่ยวข้อง โดยมีรายละเอียดหลักสูตรฝึกอบรม ดังนี้

๔.๕.๑. จัดหลักสูตรฝึกอบรมผู้ตรวจสอบ ตามมาตรฐาน ISO/IEC 27001:2022 ISO/IEC 27701:2019 ISO/IEC 27035:2023 และมาตรฐาน NIST Cybersecurity Framework โดยมีขั้นตอนดังนี้

๔.๕.๑.๑. จัดอบรมหลักสูตรทำความเข้าใจข้อกำหนดมาตรฐาน ISO/IEC 27001:2022 ISO/IEC 27701:2019 ISO/IEC 27035:2023 และมาตรฐาน NIST Cybersecurity Framework เรียนรู้วิธีการในการตรวจประเมินตามมาตรฐาน ISO 19011:2018 เพื่อใช้เป็นหลักการสำหรับการตรวจประเมินจำนวนไม่น้อยกว่า ๑๐ ท่าน ระยะเวลาในการฝึกอบรมอย่างน้อย ๒ วัน

๔.๕.๑.๒. ดำเนินการฝึกฝนการตรวจประเมินในสถานการณ์จริง (on the job training) โดยเริ่มจากการ จัดทำแผนการตรวจ คำถามที่ใช้ในการตรวจ ฝึกการสัมภาษณ์เพื่อใช้ในการเก็บรวบรวมข้อมูล การประเมินหลักฐานที่เทียบกับเกณฑ์การตรวจประเมิน และการจัดทำรายงานผลการตรวจสอบด้วยตนเอง จำนวนไม่น้อยกว่า ๑๐ ท่าน โดยเข้าร่วมดำเนินการตรวจสอบ Internal Audit ตามแผนการดำเนินโครงการตามขอบเขตงานข้อ ๔.๑.๑๐ โดยมีการมอบหมายหน้าที่ความรับผิดชอบให้กับผู้ฝึกฝนแต่ละท่านและให้มีการรายงานผลการตรวจสอบในการประชุมคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยและบริการเทคโนโลยีสารสนเทศ (Security and Service Management Committee : SSMC)

๔.๕.๒. จัดหลักสูตรฝึกอบรมนโยบาย และขั้นตอนการปฏิบัติงานตามมาตรฐาน ISO/IEC 27001:2022 ISO/IEC 27701:2019 และ ISO/IEC 27035:2023 ให้กับบุคลากรในขอบเขตการขอการรับรองจำนวนไม่น้อยกว่า ๒๐ คน ระยะเวลาในการฝึกอบรมอย่างน้อย ๑.๕ วัน (Online)

๔.๕.๓. จัดประชุมชี้แจงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ กับผู้ที่เกี่ยวข้อง อย่างน้อย ๓ ชั่วโมง (Onsite ๔๐ คน Online ไม่จำกัดจำนวน)

๔.๕.๔. จัดประชุมชี้แจงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และข้อกำหนดด้านการว่าจ้างผู้ให้บริการภายนอกเพื่อจัดทำระบบสารสนเทศให้กับสำนักงาน กสทช. อย่างมั่นคงปลอดภัย อย่างน้อย ๓ ชั่วโมง (Onsite ๔๐ คน Online ไม่จำกัดจำนวน)



๕. บุคลากรของที่ปรึกษา

ที่ปรึกษาจะต้องจัดให้มีบุคลากรที่มีความรู้ความชำนาญเพื่อดำเนินงานตามขอบเขตงาน โดยมีคุณสมบัติ ประสบการณ์ และจำนวนอย่างน้อย ดังนี้

๕.๑ ผู้จัดการโครงการ จำนวน ๑ คน

๕.๑.๑ จบการศึกษอย่างน้อยในระดับปริญญาโท ในสาขาที่เกี่ยวข้องกับคอมพิวเตอร์ สาขา วิศวกรรมศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือโทรคมนาคมและการสื่อสาร หรือด้านอื่น ๆ ที่เกี่ยวข้อง และมีประสบการณ์ด้านการบริหารโครงการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ หรือวิศวกรรมคอมพิวเตอร์ หรือโทรคมนาคมและการสื่อสาร หรือการบริหารจัดการโครงการ เป็นระยะเวลาไม่น้อยกว่า ๑๐ ปี โดยต้องมีระยะเวลาดำเนินงาน ไม่น้อยกว่า ๖ man-month

๕.๒ ที่ปรึกษาโครงการ จำนวน ๑ คน

๕.๒.๑ ที่ปรึกษาด้าน ISO/IEC 27001 และ ISO/IEC 27701 จบการศึกษอย่างน้อยในระดับปริญญาโทหรือสูงกว่า สาขาวิศวกรรมศาสตร์ หรือเทคโนโลยีสารสนเทศ หรือโทรคมนาคมและการสื่อสาร หรือด้านอื่น ๆ ที่เกี่ยวข้องและมีประสบการณ์ด้านเทคโนโลยีสารสนเทศหรือการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือการตรวจสอบด้านสารสนเทศ เป็นระยะเวลาไม่น้อยกว่า ๑๐ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๖ man-month

๕.๒.๒ ต้องได้รับประกาศนียบัตรที่เกี่ยวข้องอย่างใดอย่างหนึ่ง ดังต่อไปนี้

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

๕.๓ หัวหน้าทีมที่ปรึกษาด้านเทคนิค จำนวนอย่างน้อย ๑ คน

๕.๓.๑ จบการศึกษอย่างน้อยในระดับปริญญาโท สาขาวิศวกรรมคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือโทรคมนาคมและการสื่อสาร หรือด้านอื่น ๆ ที่เกี่ยวข้อง และมีประสบการณ์ด้านการกำกับดูแลด้านเทคโนโลยีสารสนเทศหรือ การรักษาความมั่นคงปลอดภัยสารสนเทศ หรือความมั่นคงปลอดภัยไซเบอร์ เป็นระยะเวลาอย่างน้อย ๕ ปี โดยต้องมีระยะเวลาดำเนินงานอย่างน้อย ๖ man-month

๕.๓.๒ ได้รับประกาศนียบัตร อย่างใดอย่างหนึ่ง ดังต่อไปนี้

- 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
- CompTIA Advanced Security practitioner+

๕.๔ ทีมที่ปรึกษาด้านเทคนิค จำนวนอย่างน้อย ๒ คน

๕.๔.๑ จบการศึกษาอย่างน้อยในระดับปริญญาตรี สาขาวิศวกรรมคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือโทรคมนาคมและการสื่อสาร หรือด้านอื่น ๆ ที่เกี่ยวข้อง และมีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือ การตรวจสอบด้านสารสนเทศ เป็นระยะเวลาอย่างน้อย ๕ ปี โดยต้องมีระยะเวลาดำเนินงานคนละไม่น้อยกว่า ๖ man-month

๕.๔.๒ ได้รับประกาศนียบัตรที่เกี่ยวข้อง อย่างใดอย่างหนึ่ง ดังต่อไปนี้

- ISO/IEC 27001 Lead Auditor หรือ
- ISO/IEC 27001 Implementation หรือ
- ISO/IEC 27701 Implementation หรือ
- ISO/IEC 27035 Implementation หรือ
- CompTIA Security+ หรือ
- CEH (Certified Ethical Hacker) หรือ
- Cyber Security Foundation Professional Certificate (CSFPC) หรือ
- ประกาศนียบัตรด้านความมั่นคงสารสนเทศหรือคอมพิวเตอร์ที่เกี่ยวข้อง

๕.๕ ผู้ประสานงานโครงการ จำนวน ๑ คน

๕.๕.๑ สำเร็จการศึกษาอย่างน้อยในระดับปริญญาตรีหรือสูงกว่า สาขาวิศวกรรมคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือโทรคมนาคมและการสื่อสาร หรือสาขาบริหารจัดการธุรกิจ หรือด้านอื่น ๆ ที่เกี่ยวข้อง มีประสบการณ์ในการทำงานด้านประสานงานโครงการ หรืองานอื่นที่เกี่ยวข้อง เป็นระยะเวลาไม่น้อยกว่า ๕ ปี โดยต้องมีระยะเวลาดำเนินงานไม่น้อยกว่า ๖ man-month

๖. กำหนดเวลาส่งมอบงาน

ภายใน ๓๖๐ วัน นับถัดจากวันลงนามในสัญญา

๗. ระยะเวลาการส่งมอบงาน

ที่ปรึกษาต้องส่งมอบงานพร้อม Data Files ที่จัดเก็บในสื่อบันทึกข้อมูลชนิด Flash Drive รวมทั้งส่งอีเมล และในรูปแบบเอกสารจำนวน ๕ ชุด โดยแบ่งออกเป็นงวดงานดังนี้

งวดที่ ๑ ส่งมอบงาน รายละเอียดตามที่ระบุด้านล่างนี้ ภายใน ๖๐ วัน นับถัดจากวันลงนามในสัญญา
ข้อ ๔.๑.๑, ๔.๑.๒

งวดที่ ๒ ส่งมอบงาน รายละเอียดตามที่ระบุด้านล่างนี้ ภายใน ๙๐ วัน นับถัดจากวันลงนามในสัญญา
ข้อ ๔.๑.๑, ๔.๑.๓, ๔.๑.๔, ๔.๕.๓

งวดที่ ๓ ส่งมอบงาน รายละเอียดตามที่ระบุด้านล่างนี้ ภายใน ๒๑๐ วัน นับถัดจากวันลงนามในสัญญา ข้อ ๔.๑.๑, ๔.๑.๕, ๔.๑.๖, ๔.๑.๗, ๔.๑.๘, ๔.๑.๙, ๔.๒, ๔.๕.๑.๑, ๔.๕.๑.๒

งวดที่ ๔ ส่งมอบงาน รายละเอียดตามที่ระบุด้านล่างนี้ ภายใน ๓๖๐ วัน นับถัดจากวันลงนามในสัญญา
ข้อ ๔.๑.๑, ๔.๑.๑๐.๑, ๔.๑.๑๐.๒, ๔.๑.๑๑, ๔.๑.๑๓, ๔.๓, ๔.๔, ๔.๕.๒, ๔.๕.๔

๘. วงเงินที่ใช้ในการจัดหา

วงเงินรวมทั้งสิ้น ๔,๕๙๐,๐๐๐.- บาท (สี่ล้านห้าแสนเก้าหมื่นบาทถ้วน) ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่ม และค่าใช้จ่ายที่ส่งไปเรียบร้อยแล้ว โดยเบิกจ่ายจากงบประมาณ ปี ๒๕๖๘ จำนวนเงิน ๔๕๙,๐๐๐.- บาท (สี่แสนห้าหมื่นเก้าพันบาทถ้วน) และงบประมาณปี ๒๕๖๙ จำนวนเงิน ๔,๑๓๑,๐๐๐.-บาท (สี่ล้านหนึ่งแสนสามหมื่นหนึ่งพันบาทถ้วน) รายจ่ายอื่น ค่าจ้างที่ปรึกษาเพื่อศึกษา วิจัย ประเมินผล หรือพัฒนาระบบต่าง ๆ

๙. เงื่อนไขการชำระเงิน

สำนักงาน กสทช. จะชำระเงินตามจำนวนในสัญญาจ้างหลังจากที่ได้ตรวจรับถูกต้องเรียบร้อยแล้ว และที่ปรึกษาปฏิบัติถูกต้องครบถ้วนตามที่สำนักงาน กสทช. กำหนด โดยจะชำระเงินตามเงื่อนไขและกำหนดเวลาการชำระเงินดังนี้

- งวดที่ ๑ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๑๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ได้รับส่งมอบงานในงวดงานที่ ๑ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว
- งวดที่ ๒ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๓๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ได้รับส่งมอบงานในงวดงานที่ ๒ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว
- งวดที่ ๓ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๒๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ได้รับส่งมอบงานในงวดงานที่ ๓ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว
- งวดที่ ๔ เบิกจ่ายเงินเป็นจำนวน ร้อยละ ๔๐ ของวงเงินตามสัญญาของการดำเนินงานโครงการ หลังจากที่ได้รับส่งมอบงานในงวดงานที่ ๔ แล้วเสร็จและผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุในงานจ้างที่ปรึกษา เรียบร้อยแล้ว

๑๐. การจัดทำข้อเสนอของที่ปรึกษา

ที่ปรึกษาจะต้องทำข้อเสนอโครงการเป็นภาษาไทย ประกอบด้วย เอกสารและหลักฐาน ข้อเสนอทางเทคนิค และข้อเสนอทางการเงิน โดยมีรายละเอียดข้อเสนอ ดังนี้

๑๐.๑. เอกสารและหลักฐานเกี่ยวกับผู้ยื่นข้อเสนอ ประกอบด้วย

- ๑๐.๑.๑ หลักฐานการจดทะเบียนเป็นนิติบุคคลที่จัดตั้งตามกฎหมายไทย ต้องมีสำเนาหรือภาพถ่ายหนังสือการรับรองการจดทะเบียนเป็นนิติบุคคลของสำนักงานทะเบียนหุ้นส่วนบริษัทกลาง หรือสำนักงานทะเบียนหุ้นส่วนบริษัทจังหวัด กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ที่แสดงว่าได้จดทะเบียนเป็นผู้มีอำนาจทำนิติกรรมแทนนิติบุคคล ทะเบียนจดทะเบียน และวัตถุประสงค์ของนิติบุคคลฉบับที่จดทะเบียนล่าสุด ซึ่งรับรองสำเนาถูกต้องโดยผู้มีอำนาจทำนิติกรรมแทนนิติบุคคลพร้อมทั้งประทับตราสำคัญของนิติบุคคลโดยหนังสือรับรองการจดทะเบียนดังกล่าวต้องออกให้ไม่เกิน ๓ เดือน นับจากวันที่ยื่นเสนอ
- ๑๐.๑.๒ หลักฐานของกรรมการผู้จัดการ หรือหุ้นส่วนผู้จัดการ ต้องมีสำเนาหรือภาพถ่ายทะเบียนบ้านระบุสัญชาติของกรรมการผู้จัดการหรือหุ้นส่วนผู้จัดการซึ่งรับรองสำเนาถูกต้องโดยผู้มีอำนาจทำนิติกรรมแทนนิติบุคคล
- ๑๐.๑.๓ ในกรณีที่ปรึกษาเป็นส่วนงานราชการ/ สถาบันการศึกษา ให้ยื่นหนังสือมอบอำนาจของหัวหน้าส่วนราชการ/ สถาบันการศึกษา ที่ให้ผู้ใดเป็นผู้ดำเนินการ รวมทั้งหลักฐานสำเนาบัตรประชาชน บัตรราชการ พร้อมรับรองสำเนาถูกต้อง พร้อมทั้งต้องมีสำเนา

ภาพถ่ายหนังสือจัดตั้งหน่วยงาน รวมทั้งอำนาจหน้าที่ของหน่วยงาน ซึ่งรับรองสำเนาถูกต้องโดยผู้มีอำนาจลงนามของหน่วยงาน

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

๑๐.๒.๓ คุณสมบัติ ประสบการณ์ และจำนวนของบุคลากรที่เข้าร่วมงาน โดยต้องประกอบด้วยรายละเอียดประวัติ คุณวุฒิ และประสบการณ์การทำงานของที่ปรึกษาที่ผ่านมาของบุคลากรที่ได้เสนอมานในโครงการ 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 และแนบหลักฐานด้านการเงิน เช่น สลิปเงินเดือน หนังสือรับรองเงินเดือน หรือสำเนาหลักฐานการชำระภาษี (ภ.ง.ด. ๙๑)

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

๑๐.๔. วิธีการยื่นข้อเสนอ ผู้ยื่นข้อเสนอต้องแยกซองในการยื่นข้อเสนอเป็น ๓ ซอง และให้ยื่นพร้อมกันโดยถือปฏิบัติ 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 ของ จะต้องปิดผนึกให้เรียบร้อย และรับรองสำเนาถูกต้องโดยผู้มีอำนาจทำ
นิติกรรมแทนนิติบุคคล/ผู้มีอำนาจลงนามของหน่วยงาน/ผู้ได้รับมอบอำนาจถูกต้องตามกฎหมาย พร้อมทั้ง
ประทับตรา

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

๑๑. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

โดยที่งานจ้างที่ปรึกษาครั้งนี้ เพื่อให้ดำเนินการตรวจสอบและติดตามการดำเนินงานของระบบบริหาร
จัดการความมั่นคงปลอดภัยสารสนเทศ (Surveillance Audit) รอบที่ ๒ และมีการจัดจ้างผู้ตรวจรับรอง
(Certificate Body) เข้ามาตรวจรับรองตามรอบการตรวจติดตามดังกล่าว ซึ่งเป็นงานต่อเนื่องที่ต้องดำเนินการ
ต่อจากเดิมให้ครบวงจร เพื่อคงสถานะใบรับรองที่สำนักงาน กสทช. ได้รับไว้ให้ถูกต้อง นอกจากนี้ สำนักงาน
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) ได้มีประกาศคณะกรรมการกำกับดูแลด้านความ
มั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซ
เบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ข้อ ๑๙.๑
ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ข้อ ๒๔.๓ การ
ฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise) จึงจำเป็นต้องมีการขอการรับรองมาตรฐานใน
ส่วนที่เกี่ยวข้องกับ ISO/IEC 27035:2023 (Information Security Incident Management) นอกจากนี้
ประมวลแนวทางปฏิบัติฯ ยังกำหนดข้อ ๒๒.๒.๒ - ๒๒.๒.๕ ซึ่งระบุให้หน่วยงานต้องมีการใช้มาตรฐานการ
กำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้
และต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงของบริการที่สำคัญของหน่วยงานของรัฐ และ
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้
ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์ และการยกระดับการดำเนินงานตาม NIST Cybersecurity
Framework เพื่อให้สำนักเทคโนโลยีสารสนเทศ มีกระบวนการบริหารจัดการเพื่อตอบสนองต่อเหตุการณ์ด้าน
ความมั่นคงปลอดภัยและภัยคุกคามทางไซเบอร์ ได้อย่างเป็นมาตรฐานสากลเพิ่มเติมไปจากเดิม สำนักงาน
กสทช. จะดำเนินการจัดจ้างโดยวิธีคัดเลือก ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ
พ.ศ. ๒๕๖๐ มาตรา ๗๕ และมาตรา ๗๖ (๒) ประกอบกับระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้าง
และการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ ข้อ ๑๒๖ (๒) ในสัดส่วนด้านคุณภาพ ๗๐ และด้านราคา ๓๐
โดยคณะกรรมการจ้างที่ปรึกษาตามวิธีที่กำหนด จะพิจารณาคัดเลือกข้อเสนอตามลำดับ ดังนี้

๑๑.๑. สำนักงาน กสทช. จะพิจารณาข้อเสนอของที่ปรึกษาทุกราย เว้นแต่ที่ปรึกษาที่ยื่นเอกสาร
หลักฐานไม่ครบถ้วนตามข้อ ๑๐.๑ ในส่วนที่เป็นสาระสำคัญ หรือครบถ้วนแต่ไม่ถูกต้อง จะไม่รับพิจารณา
ข้อเสนอของที่ปรึกษารายนั้น และในการพิจารณาคัดเลือกข้อเสนอจะคำนึงถึงความคุ้มค่าและวัตถุประสงค์
ของงานจ้างที่ปรึกษาเป็นสำคัญ โดยพิจารณาเกณฑ์ด้านคุณภาพเป็นลำดับแรกก่อน คุณภาพด้านต่าง ๆ รวม
๓ หัวข้อ มีคะแนนน้ำหนักรวม ๗๐ และจำแนกสัดส่วนน้ำหนักแต่ละหัวข้อ ประกอบด้วย ดังนี้

- | | |
|--|------------------|
| (๑) ผลงานที่ผ่านมาของผู้ยื่นข้อเสนอ | น้ำหนักร้อยละ ๒๐ |
| (๑.๑) ผลงานของที่ปรึกษา | (ร้อยละ ๑๐) |
| (๑.๒) ประสบการณ์เฉพาะ | (ร้อยละ ๑๐) |
| (๒) วิธีบริหารและวิธีปฏิบัติงาน | น้ำหนักร้อยละ ๔๐ |
| (๒.๑) กรอบแนวคิดและแผนการดำเนินงานตาม ข้อ ๔ | (ร้อยละ ๕) |
| (๒.๒) ความเข้าใจในแนวทางการประเมินความเสี่ยงทั้งด้านการบริหารจัดการความ
มั่นคงปลอดภัยสารสนเทศ การบริหารจัดการด้านข้อมูลส่วนบุคคล และการ | |

๑๓. อัตราค่าปรับ

หากที่ปรึกษาไม่สามารถทำงานให้แล้วเสร็จตามเวลาที่กำหนดไว้ในสัญญา และผู้ว่าจ้างยังมิได้บอกเลิกสัญญา ที่ปรึกษาจะต้องชำระค่าปรับให้แก่ผู้ว่าจ้างในอัตรา ร้อยละ ๐.๑ ของวงเงินค่าจ้างฯ นับถัดจากวันที่กำหนดแล้วเสร็จตามสัญญา หรือวันที่ผู้ว่าจ้างได้ขยายระยะเวลาตามสัญญาจนถึงวันที่ทำงานแล้วเสร็จจริง นอกจากนี้ที่ปรึกษายอมให้ผู้ว่าจ้างเรียกค่าเสียหายอันเกิดจากการที่ปรึกษาทำงานล่าช้า เฉพาะส่วนที่เกินกว่าจำนวนค่าปรับ และค่าใช้จ่ายดังกล่าวได้อีกด้วย

๑๔. เงื่อนไขอื่น ๆ

๑๔.๑ ที่ปรึกษาต้องเก็บรักษาข้อมูลของสำนักงาน กสทช. และข้อมูลที่ได้รับจากการดำเนินโครงการไว้เป็นความลับ จะเปิดเผยให้ผู้ใดทราบมิได้ และไม่นำไปใช้ในวัตถุประสงค์อื่นนอกเหนือจากการดำเนินการในโครงการนี้

๑๔.๒ ลิขสิทธิ์ในผลงานและเอกสาร รวมถึงไฟล์ดิจิทัลที่ได้รับจากผลการศึกษา ให้ตกเป็นของสำนักงาน กสทช. แต่เพียงผู้เดียว การเผยแพร่เอกสารหรือจัดทำสำเนาเพิ่มเติมจากที่จ้างเป็นสิทธิชอบธรรมของสำนักงาน กสทช.

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

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

๑๔.๕ ที่ปรึกษาที่ได้รับการคัดเลือกจะต้องทำสัญญากับสำนักงาน กสทช. ตามแบบสัญญาจ้างที่ที่ปรึกษาคณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดตามที่ประกาศในราชกิจจานุเบกษา และวางหลักประกันสัญญาเป็นอย่างใดอย่างหนึ่งที่กำหนด มูลค่าร้อยละ ๕ ของค่าจ้างที่ปรึกษา เว้นแต่กรณีที่ปรึกษาที่ได้รับการคัดเลือกเป็นหน่วยงานของรัฐ ไม่ต้องวางหลักประกันสัญญา

๑๔.๖ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ชนะการเสนอราคา หรือชนะการประกวดราคา จะต้องทำแผนการทำงานที่แสดงถึงขั้นตอนต่าง ๆ ตามขอบเขตของงานฯ ให้สอดคล้องกับระยะเวลาดำเนินงานหรือระยะเวลาการส่งมอบที่เสนอไว้ เพื่อให้คณะกรรมการตรวจรับพัสดุ ติดตามเร่งรัด และประเมินผลการทำงานให้เป็นไปตามที่กำหนด โดยต้องจัดทำแผนการทำงานเสนอภายใน ๑๕ วัน นับถัดจากวันลงนามในสัญญา ทั้งนี้ แผนการทำงานดังกล่าว ให้ถือเป็นเอกสารส่วนหนึ่งของสัญญา

คุณสมบัติของผู้ยื่นข้อเสนอ

๑. มีความสามารถตามกฎหมาย
๒. ไม่เป็นบุคคลล้มละลาย
๓. ไม่อยู่ระหว่างเลิกกิจการ
๔. ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง
๕. ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย
๖. มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุ ภาครัฐกำหนดในราชกิจจานุเบกษา
๗. เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่จ้างครั้งนี้
๘. ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน กสทช. ณ วันที่ได้รับหนังสือเชิญชวนให้เข้ายื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการยื่นข้อเสนอครั้งนี้
๙. ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอ ได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น
๑๐. ที่ปรึกษาที่จะเข้าร่วมการเสนองานกับหน่วยงานของรัฐ ต้องเป็นที่ปรึกษาที่ได้ขึ้นทะเบียนไว้กับ ศูนย์ข้อมูลที่ปรึกษา กระทรวงการคลัง สาขาสาขา ICT: เทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology Sector) มาตรฐานคุณภาพ (QS) : Quality Standard Sector ความเชี่ยวชาญ R๑๒๐: มาตรฐานระบบรักษาความปลอดภัยของข้อมูลองค์กร
๑๑. ที่ปรึกษาผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้
 - (๑) กรณีเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย/กฎหมายต่างประเทศ ซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ
 - (๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย/กฎหมายต่างประเทศ ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่น้อยกว่า ๑,๐๐๐,๐๐๐ บาท
 - (๓) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอ ผู้ยื่นข้อเสนอสามารถขอหนังสือรับรองวงเงินสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหรือบริษัทหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารกลางของประเทศนั้น ตามรายชื่อบริษัทเงินทุนที่ธนาคารกลางของประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงิน

สินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน โดยต้องมียอดเงินรวมของวงเงินสินเชื่อไม่น้อยกว่า ๑,๑๔๗,๕๐๐ บาท คิดเป็น ๑ ใน ๔ ของมูลค่าโครงการหรือรายการที่ยื่นเสนอในแต่ละครั้ง ทั้งนี้ สำหรับธนาคารภายในประเทศหนังสือรับรองวงเงินสินเชื่อให้เป็นไปตามแบบที่กำหนด

(๔) กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาถือสัญชาติไทย/บุคคลธรรมดาที่มีได้ถือสัญชาติไทย จะต้องแสดงหนังสือรับรองบัญชีเงินฝาก โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่าไม่น้อยกว่า ๑,๑๔๗,๕๐๐ บาท คิดเป็น ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือก จะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา ทั้งนี้ หนังสือรับรองบัญชีเงินฝากซึ่งธนาคารออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอหรือวันลงนามในสัญญา ไม่เกิน ๙๐ วัน

(๕) กรณีเป็นนิติบุคคลที่จัดตั้งตามกฎหมายต่างประเทศและบุคคลธรรมดาที่มีได้ถือสัญชาติไทยตามข้อ (๒) (๓) (๔) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนดในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารเชิญชวนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e-GP) หรือมีหนังสือเชิญชวน จนถึงวันยื่นข้อเสนอ

คุณสมบัติในข้อ (๑) - (๔) นี้ ยกเว้นกรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ หรือนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม

๑๒. ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กิจการร่วมค้าที่ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน เว้นแต่ในกรณีกิจการร่วมค้าที่มีข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค่านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียว เป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงดังกล่าวจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญา มากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

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

แบบหนังสือรับรองวงเงินสินเชื่อ

เลขที่.....

วันที่.....

เรื่อง รับรองวงเงินสินเชื่อ

ตามที่.....(ชื่อผู้ประกอบการ นิติบุคคล/บุคคลธรรมดา).....เลขประจำตัว
 ผู้เสียภาษีอากร /เลขประจำตัวประชาชนเลขที่.....จะยื่นข้อเสนอในงาน จ้างที่ปรึกษาเพื่อ
 พัฒนาปรับปรุงแก้ไขการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001,
 27701, 27035 และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคง
 ปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งตามหลักเกณฑ์และวิธีการคัดเลือกเป็นผู้ประกอบการงาน จ้างที่ปรึกษาเพื่อ
 พัฒนาปรับปรุงแก้ไขการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001,
 27701, 27035 และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคง
 ปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้ผู้ยื่นคำขอต้องเสนอหนังสือรับรองวงเงินสินเชื่อ/จะเข้ายื่นข้อเสนอ
 กับหน่วยงานของรัฐซึ่งเงื่อนไขการยื่นข้อเสนอกรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสิทธิของกิจการหรือทุนจดทะเบียน
 หรือมีแต่ไม่เพียงพอ ที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอต้องขอวงเงินสินเชื่อจากธนาคาร โดยต้องมีวงเงิน
 สินเชื่อ ๑ ใน ๔ ของมูลค่า งบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอใน แต่ละครั้ง.....
 ชื่อผู้ประกอบการ นิติบุคคล/บุคคลธรรมดา.....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/เลขประจำตัวประชาชน เลขที่.....จะยื่นข้อเสนอในงานจ้างที่ปรึกษาเพื่อพัฒนาปรับปรุงแก้ไขการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001, 27701, 27035 และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งตามหลักเกณฑ์และวิธีการคัดเลือกเป็นผู้ประกอบการงานจ้างที่ปรึกษาเพื่อพัฒนาปรับปรุงแก้ไขการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001, 27701, 27035 และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้ผู้ยื่นคำขอต้องเสนอหนังสือรับรองวงเงินสินเชื่อ/จะเข้ายื่นขอเสนอกับหน่วยงานของรัฐซึ่งเงื่อนไขการยื่นข้อเสนอกรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสิทธิของกิจการหรือทุนจดทะเบียนหรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอต้องขอวงเงินสินเชื่อจากธนาคาร โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอใน แต่ละครั้ง.....ชื่อผู้ประกอบการ นิติบุคคล/บุคคลธรรมดา.....จึงมีความประสงค์ให้ธนาคาร..... (ชื่อธนาคาร).....รับรองวงเงินสินเชื่อ เพื่อประกอบการพิจารณาด้วย นั้น

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

ขอแสดงความนับถือ

..... (ชื่อธนาคาร).....

** เอกสารฉบับนี้จัดพิมพ์โดยระบบอิเล็กทรอนิกส์ **

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

การกำหนดเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

- ๑. ผลงานที่ผ่านมาของผู้ยื่นข้อเสนอ (น้ำหนักร้อยละ ๒๐)
 ในหัวข้อนี้ จะพิจารณาการให้คะแนนในเชิงคุณภาพและเชิงปริมาณ ดังนี้
 - (๑) ผลงานของที่ปรึกษา : โดยพิจารณาจากลักษณะของผลงานที่มีขอบเขตและวิธีการนำเสนอที่สอดคล้องหรือใกล้เคียงกับลักษณะงานตามขอบเขตของงานและวัตถุประสงค์มากที่สุด
 - (๒) ประสิทธิภาพเฉพาะ : โดยพิจารณาจากผลงาน จำนวนผลงาน และมูลค่าของผลงานที่มีลักษณะสอดคล้องหรือใกล้เคียงกับงานตามขอบเขตของงาน โดยเทียบสัดส่วนกับจำนวนผลงานของผู้ยื่นข้อเสนอด้วยกัน

เกณฑ์การพิจารณาที่ให้คะแนน	ระดับคะแนน
๑. ผลงานที่ผ่านมาของผู้ยื่นข้อเสนอ (๑๐๐ คะแนน) (น้ำหนักร้อยละ ๒๐) มีผลงานที่ผ่านมาจำนวนอย่างน้อย ๑ โครงการ/ชิ้นงาน ที่มีขอบเขตงานใกล้เคียงหรือเท่ากับเนื้อหาของโครงการนี้ เช่น เคยเป็นที่ปรึกษาให้กับหน่วยงานภาครัฐหรือเอกชนจนได้รับการรับรองตามมาตรฐาน ISO/IEC 27001:2022 หรือ ISO/IEC 27701:2019 และมีประวัติเคยเป็นที่ปรึกษาให้กับหน่วยงานที่ปฏิบัติหน้าที่กำกับดูแล หรือเคยดำเนินการพัฒนา ปรับปรุง กระบวนการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	
๑.๑ ผลงานของที่ปรึกษา : ผลงานที่ผ่านมาตามข้อ ๑๐.๒.๑ (๑๐๐ คะแนน) (น้ำหนักร้อยละ ๑๐)	
มีการนำเสนอผลงานที่ผ่านมา โดยในขอบเขตงานที่นำเสนอมีการให้คำปรึกษาหน่วยงานจนผ่านการรับรองตามมาตรฐาน ISO/IEC 27001:2022 และ ISO/IEC 27701:2019 และ มาตรฐานอื่น ๆ เช่น ISO/IEC 27035 หรือ ISO/IEC 22301 เป็นต้น	๑๐๐ คะแนน
มีการนำเสนอผลงานที่ผ่านมา โดยในขอบเขตงานที่นำเสนอมีการให้คำปรึกษาหน่วยงานจนผ่านการรับรองตามมาตรฐาน 27001:2022 และ ISO/IEC 27701:2019	๙๐ คะแนน
มีการนำเสนอผลงานที่ผ่านมา โดยในขอบเขตงานที่นำเสนอมีการให้คำปรึกษาหน่วยงานจนผ่านการรับรองตามมาตรฐาน ISO/IEC 27001:2022 เพียงมาตรฐานเดียว	๘๐ คะแนน
๑.๒ ประสิทธิภาพเฉพาะ : จำนวนผลงานที่ผ่านมา (๑๐๐ คะแนน) (น้ำหนักร้อยละ ๑๐)	
มีผลงานที่มีขอบเขตและวิธีการนำเสนอใกล้เคียงกับลักษณะงานตามขอบเขตของงาน จำนวน ๓ ผลงานขึ้นไป	๑๐๐ คะแนน
มีผลงานที่มีขอบเขตและวิธีการนำเสนอใกล้เคียงกับลักษณะงานตามขอบเขตของงาน จำนวน ๒ ผลงาน	๙๐ คะแนน
มีผลงานที่มีขอบเขตและวิธีการนำเสนอใกล้เคียงกับลักษณะงานตามขอบเขตของงาน จำนวน ๑ ผลงาน	๘๐ คะแนน

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

๒. วิธีการบริหารและวิธีปฏิบัติงาน (น้ำหนักร้อยละ ๔๐)

ในหัวข้อนี้ จะพิจารณาการให้คะแนนจากข้อเสนอที่สามารถนำขอบเขตของงานที่กำหนดไว้มาจัดทำเป็นแผนและวิธีการดำเนินงาน การตรวจสอบ ที่สอดคล้องกับระยะเวลาดำเนินงานของสำนักงาน กสทช. ได้ชัดเจนและเป็นรูปธรรมมากที่สุด

รายละเอียดการให้คะแนน	ระดับคะแนน	วิธีการประเมิน
๒. วิธีการบริหารและวิธีการดำเนินงาน (๑๐๐ คะแนน) (น้ำหนักร้อยละ ๔๐)		
๒.๑ กรอบแนวคิดและแผนการดำเนินงานตาม ข้อ ๔ (น้ำหนักร้อยละ ๕)		
เกณฑ์การพิจารณาที่ให้คะแนน	คะแนน	วิธีการประเมิน
มีกรอบแนวคิดและแผนการดำเนินงานตามวัตถุประสงค์และขอบเขตของงาน มีรายละเอียดอย่างชัดเจน มีกรอบระยะเวลาการดำเนินการและแจกแจงบุคคลากรที่รับผิดชอบตามแผนการดำเนินงาน และมีการนำเอากรอบมาตรฐานสากลหรือกรอบแนวคิดที่เป็นประโยชน์เข้ามาประยุกต์ใช้กับการดำเนินงานและสามารถตอบวัตถุประสงค์และขอบเขตของงาน และมีแผนงานที่สามารถนำไปปฏิบัติได้จริง	๑๐๐	ผู้ประเมินจะพิจารณาจากเอกสารที่ผู้ยื่นข้อเสนอยื่นมา โดยจัดทำเป็นรูปแบบเอกสาร ขนาดกระดาษ A๔ และผู้ประเมินจะให้ คะแนนตามรายการที่ผู้ยื่นข้อเสนอ นำเอกสารยื่นมา
มีกรอบแนวคิดและแผนการดำเนินงานตามวัตถุประสงค์และขอบเขตของงาน มีรายละเอียดอย่างชัดเจน มีกรอบระยะเวลาการดำเนินการแต่ไม่แจกแจงบุคคลากรที่รับผิดชอบตามแผนการดำเนินงาน	๘๐	
๒.๒ ความเข้าใจในแนวทางการประเมินความเสี่ยงทั้งด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ การบริหารจัดการด้านข้อมูลส่วนบุคคล และการบริหารจัดการด้านการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (น้ำหนักร้อยละ ๑๕)		
เกณฑ์การพิจารณาที่ให้คะแนน	คะแนน	วิธีการประเมิน
มีการนำเสนอแนวทางการประเมินความเสี่ยงและวิธีการบริหารจัดการเอกสารที่สอดคล้องกับมาตรฐาน ISO/IEC 27001 ISO/IEC 27701 และ ISO/IEC 27035 และ NIST Cybersecurity Framework รวมถึงข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยนำมาประยุกต์ใช้กับระบบจัดการเอกสารที่สำนักเทคโนโลยีสารสนเทศมีการใช้งานในปัจจุบันได้	๑๐๐	ผู้ประเมินจะพิจารณาจากเอกสารที่ผู้ยื่นข้อเสนอยื่นมา โดยจัดทำเป็นรูปแบบเอกสาร ขนาดกระดาษ A๔ และผู้ประเมินจะให้ คะแนนตามรายการที่ผู้ยื่นข้อเสนอ นำเอกสารยื่นมา
มีการนำเสนอแนวทางการประเมินความเสี่ยงที่สอดคล้องกับมาตรฐาน ISO/IEC 27001 ISO/IEC 27701 และ ISO/IEC 27035 และนำไปใช้กับแนวทางที่สำนักเทคโนโลยีสารสนเทศมีการใช้งานในปัจจุบันได้	๘๐	

[Handwritten signatures and initials in blue ink]

๒.๓ ทักษะในการประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบของเครือข่ายและระบบเทคโนโลยีสารสนเทศ (น้ำหนักร้อยละ ๑๕)		
เกณฑ์การพิจารณาที่ให้คะแนน	คะแนน	วิธีการประเมิน
มีทักษะในการประเมิน วิเคราะห์ พัฒนา และจัดทำ ภูมิทัศน์ด้านความมั่นคงปลอดภัยไซเบอร์ ของ สำนักงาน กสทช. (NBTC Cybersecurity Landscape) รวมถึง Threat categories เพื่อให้สำนักงาน กสทช. สามารถดำเนินการได้ตามมาตรฐานสอดคล้องกับ มาตรฐาน ISO/IEC 27001, ISO/IEC 27701 และ ISO/IEC 27035 และ NIST Cybersecurity Framework รวมถึงข้อกำหนดด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์	๑๐๐	ผู้ประเมินจะพิจารณาจากเอกสารที่ผู้ยื่น ข้อเสนอขึ้นมา โดยจัดทำเป็นรูปแบบ เอกสาร ขนาดกระดาษ A๔ และผู้ ประเมินจะให้ คะแนนตามรายการที่ผู้ยื่น ข้อเสนอ นำเอกสารขึ้นมา
มีทักษะในการประเมิน วิเคราะห์ พัฒนา และจัดทำ ภูมิทัศน์ด้านความมั่นคงปลอดภัยไซเบอร์ ของ สำนักงาน กสทช. (NBTC Cybersecurity Landscape) รวมถึง Threat categories เพื่อให้สำนักงาน กสทช. สามารถดำเนินการได้ตามมาตรฐานสอดคล้องกับ มาตรฐาน ISO/IEC 27001 และ ISO/IEC 27701	๙๐	
มีทักษะในการประเมินหา วิเคราะห์ และออกแบบ ระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่าย สารสนเทศอย่างมั่นคงปลอดภัย	๘๐	
๒.๔ ข้อเสนออื่น ๆ ที่เป็นประโยชน์ต่อการดำเนินงาน และสอดคล้องกับขอบเขตของงาน (น้ำหนักร้อยละ ๕)		
เกณฑ์การพิจารณาที่ให้คะแนน	คะแนน	วิธีการประเมิน
มีข้อเสนออื่น ๆ ที่เป็นประโยชน์ต่อการดำเนินงาน และสอดคล้องกับขอบเขตของงาน	๑๐๐	ผู้ประเมินจะพิจารณาจากเอกสารที่ผู้ยื่น ข้อเสนอขึ้นมา โดยจัดทำเป็นรูปแบบ เอกสาร ขนาดกระดาษ A๔ และผู้ ประเมินจะให้ คะแนนตามรายการที่ผู้ยื่น ข้อเสนอ นำเอกสารขึ้นมา
ไม่มีข้อเสนออื่น ๆ ที่เป็นประโยชน์ต่อการดำเนินงาน และสอดคล้องกับขอบเขตของงาน	๐	

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

รายละเอียดการให้คะแนน	ระดับคะแนน												
<p>๓. จำนวนและคุณลักษณะของบุคลากรที่ร่วมงาน (น้ำหนักร้อยละ ๑๐)</p> <p>โดยที่ปรึกษาจะต้องแสดงรายละเอียดคุณวุฒิการศึกษา ความเชี่ยวชาญหรือประสบการณ์ของบุคลากรหลัก และประกาศนียบัตรตามขอบเขตงานข้อ ๕ (ถ้ามี) พร้อมเอกสารหลักฐานอ้างอิง โดยมีคะแนนรวมทั้งสิ้น ๑๐๐ คะแนน ซึ่งผู้ประเมินจะให้คะแนนแก่บุคลากรของผู้ยื่นข้อเสนอทั้ง ๕ คน ดังนี้</p>													
<p>๑. ผู้จัดการโครงการ</p> <p>ผู้จัดการโครงการจะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาซึ่งเป็นสาขาวิชาเดียวกันกับที่กำหนดตามข้อ ๕ (๕.๑)</p>	<p style="text-align: center;">คะแนนเต็ม ๓๐ คะแนน</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 25%;">ด้านประสบการณ์ (๑๕ คะแนน)</th> <th style="width: 25%;">ด้านวุฒิการศึกษา (๑๐ คะแนน)</th> <th style="width: 25%;">ด้านประกาศนียบัตร (๕ คะแนน)</th> </tr> <tr> <td>มากกว่า ๑๐ ปี</td> <td>ปริญญาเอก</td> <td>มากกว่า ๓ ใบ</td> </tr> <tr> <td>๑๕ คะแนน</td> <td>๑๐ คะแนน</td> <td>๕ คะแนน</td> </tr> <tr> <td>๑๓ คะแนน</td> <td>๘ คะแนน</td> <td>๔ คะแนน</td> </tr> </table>	ด้านประสบการณ์ (๑๕ คะแนน)	ด้านวุฒิการศึกษา (๑๐ คะแนน)	ด้านประกาศนียบัตร (๕ คะแนน)	มากกว่า ๑๐ ปี	ปริญญาเอก	มากกว่า ๓ ใบ	๑๕ คะแนน	๑๐ คะแนน	๕ คะแนน	๑๓ คะแนน	๘ คะแนน	๔ คะแนน
ด้านประสบการณ์ (๑๕ คะแนน)	ด้านวุฒิการศึกษา (๑๐ คะแนน)	ด้านประกาศนียบัตร (๕ คะแนน)											
มากกว่า ๑๐ ปี	ปริญญาเอก	มากกว่า ๓ ใบ											
๑๕ คะแนน	๑๐ คะแนน	๕ คะแนน											
๑๓ คะแนน	๘ คะแนน	๔ คะแนน											
<p>๒. ที่ปรึกษาโครงการ</p> <p>ที่ปรึกษาโครงการจะต้องมีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๒)</p>	<p style="text-align: center;">คะแนนเต็ม ๓๐ คะแนน</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 25%;">ด้านประสบการณ์ (๑๕ คะแนน)</th> <th style="width: 25%;">ด้านวุฒิการศึกษา (๑๐ คะแนน)</th> <th style="width: 25%;">ด้านประกาศนียบัตร (๕ คะแนน)</th> </tr> <tr> <td>มากกว่า ๑๐ ปี</td> <td>ปริญญาเอก</td> <td>มากกว่า ๓ ใบ</td> </tr> <tr> <td>๑๕ คะแนน</td> <td>๑๐ คะแนน</td> <td>๕ คะแนน</td> </tr> <tr> <td>๑๓ คะแนน</td> <td>๘ คะแนน</td> <td>๔ คะแนน</td> </tr> </table>	ด้านประสบการณ์ (๑๕ คะแนน)	ด้านวุฒิการศึกษา (๑๐ คะแนน)	ด้านประกาศนียบัตร (๕ คะแนน)	มากกว่า ๑๐ ปี	ปริญญาเอก	มากกว่า ๓ ใบ	๑๕ คะแนน	๑๐ คะแนน	๕ คะแนน	๑๓ คะแนน	๘ คะแนน	๔ คะแนน
ด้านประสบการณ์ (๑๕ คะแนน)	ด้านวุฒิการศึกษา (๑๐ คะแนน)	ด้านประกาศนียบัตร (๕ คะแนน)											
มากกว่า ๑๐ ปี	ปริญญาเอก	มากกว่า ๓ ใบ											
๑๕ คะแนน	๑๐ คะแนน	๕ คะแนน											
๑๓ คะแนน	๘ คะแนน	๔ คะแนน											
<p>๓. หัวหน้าทีมที่ปรึกษาด้านเทคนิค</p> <p>หัวหน้าทีมที่ปรึกษาด้านเทคนิค จะต้อง มีประสบการณ์ทำงานและวุฒิการศึกษาซึ่งเป็นสาขาวิชาเดียวกันกับที่กำหนดตามข้อ ๕ (๕.๓)</p>	<p style="text-align: center;">คะแนนเต็ม ๒๐ คะแนน</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 25%;">ด้านประสบการณ์ (๑๐ คะแนน)</th> <th style="width: 25%;">ด้านวุฒิการศึกษา (๕ คะแนน)</th> <th style="width: 25%;">ด้านประกาศนียบัตร (๕ คะแนน)</th> </tr> <tr> <td>มากกว่า ๑๐ ปี</td> <td>ปริญญาเอก</td> <td>มากกว่า ๓ ใบ</td> </tr> <tr> <td>๑๐ คะแนน</td> <td>๕ คะแนน</td> <td>๕ คะแนน</td> </tr> <tr> <td>๘ คะแนน</td> <td>๔ คะแนน</td> <td>๔ คะแนน</td> </tr> </table>	ด้านประสบการณ์ (๑๐ คะแนน)	ด้านวุฒิการศึกษา (๕ คะแนน)	ด้านประกาศนียบัตร (๕ คะแนน)	มากกว่า ๑๐ ปี	ปริญญาเอก	มากกว่า ๓ ใบ	๑๐ คะแนน	๕ คะแนน	๕ คะแนน	๘ คะแนน	๔ คะแนน	๔ คะแนน
ด้านประสบการณ์ (๑๐ คะแนน)	ด้านวุฒิการศึกษา (๕ คะแนน)	ด้านประกาศนียบัตร (๕ คะแนน)											
มากกว่า ๑๐ ปี	ปริญญาเอก	มากกว่า ๓ ใบ											
๑๐ คะแนน	๕ คะแนน	๕ คะแนน											
๘ คะแนน	๔ คะแนน	๔ คะแนน											
<p>๔. ทีมที่ปรึกษาด้านเทคนิค (คนที่ ๑)</p> <p>ทีมที่ปรึกษาด้านเทคนิค (คนที่ ๑) จะต้อง มีประสบการณ์ทำงานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๔)</p>	<p style="text-align: center;">คะแนนเต็ม ๑๐ คะแนน</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 25%;">ด้านประสบการณ์ (๕ คะแนน)</th> <th style="width: 25%;">ด้านวุฒิการศึกษา (๒.๕ คะแนน)</th> <th style="width: 25%;">ด้านประกาศนียบัตร (๒.๕ คะแนน)</th> </tr> <tr> <td>มากกว่า ๑๐ ปี</td> <td>ปริญญาโท</td> <td>มากกว่า ๓ ใบ</td> </tr> <tr> <td>๕ คะแนน</td> <td>๒.๕ คะแนน</td> <td>๒.๕ คะแนน</td> </tr> <tr> <td>๓ คะแนน</td> <td>๒ คะแนน</td> <td>๒ คะแนน</td> </tr> </table>	ด้านประสบการณ์ (๕ คะแนน)	ด้านวุฒิการศึกษา (๒.๕ คะแนน)	ด้านประกาศนียบัตร (๒.๕ คะแนน)	มากกว่า ๑๐ ปี	ปริญญาโท	มากกว่า ๓ ใบ	๕ คะแนน	๒.๕ คะแนน	๒.๕ คะแนน	๓ คะแนน	๒ คะแนน	๒ คะแนน
ด้านประสบการณ์ (๕ คะแนน)	ด้านวุฒิการศึกษา (๒.๕ คะแนน)	ด้านประกาศนียบัตร (๒.๕ คะแนน)											
มากกว่า ๑๐ ปี	ปริญญาโท	มากกว่า ๓ ใบ											
๕ คะแนน	๒.๕ คะแนน	๒.๕ คะแนน											
๓ คะแนน	๒ คะแนน	๒ คะแนน											


 [Signature]

คะแนนเต็ม ๑๐ คะแนน							
๕. ทีมที่ปรึกษาด้านเทคนิค (คนที่ ๒) ทีมที่ปรึกษาด้านเทคนิค (คนที่ ๒) จะต้องมีการปฏิบัติงานที่งานและวุฒิการศึกษาตรงกับที่กำหนดตามข้อ ๕ (๕.๔)	ด้านประสบการณ์ (๕ คะแนน)		ด้านวุฒิการศึกษา (๒.๕ คะแนน)		ด้านประกาศนียบัตร (๒.๕ คะแนน)		
	มากกว่า ๑๐ ปี	มากกว่า ๕ ปี	๕ ปี	ปริญญาโท	ปริญญาตรี	มากกว่า ๓ ปี	๒ ปี
	๕ คะแนน	๔ คะแนน	๓ คะแนน	๒.๕ คะแนน	๒ คะแนน	๒.๕ คะแนน	๑ คะแนน

การให้คะแนนในหัวข้อนี้ จะขึ้นอยู่กับประสบการณ์ คุณวุฒิ และประกาศนียบัตรที่เกี่ยวข้องของบุคลากรหลักและบุคลากรสนับสนุนที่เสนอ เป็นไปตามที่กำหนดตามข้อ ๕ นอกจากนี้ จะพิจารณารายละเอียดและความครบถ้วนครบครันดังกล่าวแล้ว จะพิจารณาเปรียบเทียบระหว่างข้อเสนอของผู้ยื่นข้อเสนอแต่ละราย ข้อเสนอที่ดีที่สุดจะได้คะแนนเต็มหรือได้มากที่สุด ข้อเสนอที่รองลงไปจะได้คะแนนลดหลั่นตามความเหมาะสมในช่วงคะแนนของหัวข้อนั้น

Handwritten signature and initials in blue ink.

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล
(Data Processing Agreement : DPA) กับสำนักงาน กสทช.

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (“ข้อตกลง”) นี้ จัดทำขึ้นเพื่อให้สอดคล้องกับหน้าที่ของสำนักงาน กสทช. และ ผู้ประมวลผลข้อมูลส่วนบุคคลตามมาตรา ๔๐ วรรคสามและมาตรา ๓๗ (๒) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และข้อ ๖ ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และถือเป็นส่วนหนึ่งของการจ้างที่ปรึกษาเพื่อพัฒนาปรับปรุงแก้ไขการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001, 27701, 27035 และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งสำนักงาน กสทช. มีฐานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” และ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก มีฐานะเป็น “ผู้ประมวลผลข้อมูลส่วนบุคคล” ซึ่งเป็นผู้ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผย (“ประมวลผล”) ข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของสำนักงาน กสทช. โดย ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการเพื่อวัตถุประสงค์ ดังนี้

๑. เพื่อจ้างที่ปรึกษาเป็นที่ปรึกษาพัฒนาปรับปรุงแก้ไขการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2022 การบริหารจัดการข้อมูลส่วนบุคคล ตามมาตรฐาน ISO/IEC 27701:2019 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย ตามมาตรฐาน ISO/IEC 27035:2023 และการปฏิบัติตามมาตรฐาน NIST Cybersecurity Framework

๒. เพื่อดำเนินการตามวัตถุประสงค์ที่กำหนดไว้ในสัญญาหลัก

โดยข้อมูลส่วนบุคคลที่มีการประมวลผลตามวัตถุประสงค์ข้างต้น ประกอบด้วย

๑. ข้อมูลชื่อ - นามสกุล, อีเมล, เบอร์โทรศัพท์, ภาพถ่าย, วิดีโอ, เสียง

๒. ข้อมูลส่วนบุคคลอื่นใดที่อาจมีความจำเป็นเพื่อให้บรรลุวัตถุประสงค์ตามสัญญาหลัก

๓. ข้อมูลจะถูกจัดเก็บเอกสารในรูปแบบ Digital File (Softcopy, PDF) และรูปแบบของเอกสาร (Hardcopy)

การควบคุมดูแลการประมวลผลข้อมูลส่วนบุคคลที่สำนักงาน กสทช. มอบหมายหรือแต่งตั้งให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการ ซึ่งจะต้องดำเนินการตามหน้าที่และความรับผิดชอบตามขอบเขตงานในสัญญาหลัก และดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชกฤษฎีกา ระเบียบ และประกาศ ที่ออกตามความในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงนี้ รวมเรียกว่า “กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล” ทั้งที่มีผลใช้บังคับอยู่บนแต่วันที่มีการทำ สัญญาหลัก และที่จะมีการแก้ไขเพิ่มเติมในภายหลัง โดยผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งต่อไปนี้เรียกว่า “ผู้ประมวลผลข้อมูลส่วนบุคคล” ต้องดำเนินงานตามสัญญาหลัก ในส่วนของข้อมูลตามที่กำหนดในวัตถุประสงค์ข้างต้น ให้เป็นไปตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล มีรายละเอียดดังนี้

๑. ผู้ประมวลผลข้อมูลส่วนบุคคลรับทราบ ว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดยจะดำเนินการตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย

๒. ผู้ประมวลผลข้อมูลส่วนบุคคลจะกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้ จำกัดเฉพาะบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงนี้เท่านั้น และจะดำเนินการเพื่อให้บุคคลดังกล่าวทำการประมวลผลและรักษาความลับของข้อมูลส่วนบุคคลตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้

๓. ผู้ประมวลผลข้อมูลส่วนบุคคลจะควบคุมดูแลให้บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และดำเนินการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ของการดำเนินการตามขอบเขตงานในสัญญาหลัก หรือที่แก้ไขเพิ่มเติมในภายหลัง โดยจะไม่ทำซ้ำ คัดลอก ทำสำเนา บันทึกภาพข้อมูลส่วนบุคคลไม่ว่าทั้งหมด หรือแต่บางส่วนเป็นอันขาด เว้นแต่เป็นไปตามเงื่อนไขของขอบเขตงานในสัญญาหลัก หรือที่แก้ไขเพิ่มเติมในภายหลัง หรือกฎหมายที่เกี่ยวข้องที่กำหนดไว้เป็นประการอื่น

๔. ผู้ประมวลผลข้อมูลส่วนบุคคลจะดำเนินการเพื่อช่วยเหลือหรือสนับสนุนสำนักงาน กสทช. ในการตอบสนองต่อคำร้องที่เจ้าของข้อมูลส่วนบุคคลแจ้งต่อสำนักงาน กสทช. ในการตอบสนองต่อคำร้องที่เจ้าของข้อมูลส่วนบุคคลแจ้งต่อสำนักงาน กสทช. อันเป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในขอบเขตงานในสัญญาหลัก

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิดังกล่าวต่อผู้ประมวลผลข้อมูลส่วนบุคคลโดยตรง ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องดำเนินการแจ้งและส่งคำร้องดังกล่าวให้แก่สำนักงาน กสทช. ทันที โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่ใช่ผู้ตอบสนองต่อคำร้องดังกล่าว เว้นแต่สำนักงาน กสทช. จะได้มอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเฉพาะเรื่องที่เกี่ยวข้องกับคำร้องดังกล่าว

๕. ผู้ประมวลผลข้อมูลส่วนบุคคลจะจัดทำและเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing) ทั้งหมดที่ผู้ประมวลผลข้อมูลส่วนบุคคลประมวลผลในขอบเขตงานในสัญญาหลัก และจะดำเนินการส่งมอบบันทึกการดังกล่าวให้แก่สำนักงาน กสทช. ภายใน ๓๐ วันนับถัดจากวันลงนามในสัญญา หรือเมื่อสำนักงาน กสทช. ร้องขอเป็นลายลักษณ์อักษร

๖. ผู้ประมวลผลข้อมูลส่วนบุคคลจะจัดให้มีและคงไว้ซึ่งมาตรการรักษาความมั่นคงปลอดภัยสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเหมาะสมทั้งมาตรการเชิงองค์กรและเชิงเทคนิค รวมถึงมาตรการทางกายภาพที่จำเป็นตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และตามประกาศสำนักงาน กสทช. เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงาน กสทช. รวมถึงที่ได้มีการแก้ไขเพิ่มเติมในอนาคต โดยคำนึงถึงระดับความเสี่ยงตามลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดในขอบเขตงานในสัญญาหลักเป็นสำคัญ เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสียหายอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิด อุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือไม่ชอบด้วยกฎหมาย เป็นต้น โดยต้องจัดให้มีมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสมซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกัน หรือใกล้เคียงกัน ลักษณะหรือประเภทของข้อมูลส่วนบุคคล ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

๗. เว้นแต่กฎหมายที่เกี่ยวข้องจะบัญญัติไว้เป็นประการอื่น ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องส่งคืนข้อมูลส่วนบุคคลให้กับสำนักงาน กสทช. หรือดำเนินการลบ ทำลาย ยกเลิกการเข้าถึง หรือทำให้เป็นข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ ทั้งนี้ ตามที่สำนักงาน กสทช. กำหนด

โดยทันทีเมื่อการดำเนินการประมวลผลตามวัตถุประสงค์ของขอบเขตงานในสัญญาหลักเสร็จสิ้นลง โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องควบคุมดูแล ตรวจสอบ และรับรองว่าข้อมูลส่วนบุคคลดังกล่าว จะไม่อยู่ในความครอบครองของตนเองและของบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคลอีกต่อไป

๘. เหตุแห่งการละเมิดข้อมูลส่วนบุคคล

๘.๑ ในกรณีที่ ผู้ประมวลผลข้อมูลส่วนบุคคลได้ทราบหรือมีเหตุอันควรทราบว่ามีเหตุแห่งการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น ภายใน ๒๔ ชั่วโมงนับแต่ทราบหรือมีเหตุอันควรทราบถึงเหตุแห่งการละเมิดข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการดังต่อไปนี้

(ก) ให้ข้อมูลที่จำเป็นแก่สำนักงาน กสทช. เพื่อให้สำนักงาน กสทช. สามารถปฏิบัติหน้าที่ภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและทันภายในระยะเวลาที่กฎหมายกำหนด เช่น ลักษณะของเหตุแห่งการละเมิดข้อมูลส่วนบุคคล ประเภทและจำนวนโดยประมาณของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุแห่งการละเมิด และรายละเอียดของเจ้าของข้อมูลส่วนบุคคลดังกล่าว ผลกระทบที่อาจเกิดขึ้นได้จากเหตุแห่งการละเมิด มาตรการที่ได้ดำเนินการแล้วหรือที่จะเสนอให้ดำเนินการ และมาตรการที่จะเยียวยาผลกระทบที่อาจเกิดขึ้นจากเหตุแห่งการละเมิดข้อมูลส่วนบุคคลนั้น

(ข) ให้ความร่วมมืออย่างเต็มที่กับสำนักงาน กสทช. และดำเนินการใด ๆ ตามที่สำนักงาน กสทช. กำหนดเพื่อช่วยในการดำเนินการตรวจสอบ บรรเทา และเยียวยาความเสียหายอันเกิดจากเหตุแห่งการละเมิดข้อมูลส่วนบุคคลนั้น

๘.๒ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่เปิดเผยเหตุแห่งการละเมิดข้อมูลส่วนบุคคลให้แก่บุคคลอื่นใดทราบโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช. ก่อน เว้นแต่กรณีที่เป็น การปฏิบัติตามกฎหมาย

๘.๓ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องชดใช้บรรดาค่าใช้จ่ายที่เกิดขึ้นจริงในการดำเนินการใด ๆ เพื่อจัดการเหตุแห่งการละเมิดข้อมูลส่วนบุคคลให้แก่สำนักงาน กสทช. หากปรากฏว่า ผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลของ ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในความรับผิดชอบของตน เป็นผู้ก่อให้เกิดเหตุแห่งการละเมิดข้อมูลส่วนบุคคลดังกล่าว

๙. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

๙.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลรับรองและยืนยันว่าจะไม่ส่งหรือโอน หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลภายใต้ขอบเขตงานในสัญญาหลัก ไปยังต่างประเทศโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช.

๙.๒ ในกรณีที่ ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช. แล้ว ผู้ประมวลผลข้อมูลส่วนบุคคลสามารถส่งหรือโอน หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลภายใต้ขอบเขตงานในสัญญาหลัก ไปยังต่างประเทศได้ ทั้งนี้ การส่งหรือโอน หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลดังกล่าว จะต้องกระทำภายใต้บทบัญญัติของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งเป็นลายลักษณ์อักษรของสำนักงาน กสทช. เท่านั้น โดย ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องเข้าทำข้อตกลงเพิ่มเติมหรือจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลบังคับใช้

๑๐. การให้บริการช่วง

๑๐.๑ ภายใต้หน้าที่และขอบเขตงานที่กำหนดในสัญญาหลัก ผู้ประมวลผลข้อมูลส่วนบุคคล ไม่สามารถว่าจ้างหรือแต่งตั้งบุคคลภายนอกเป็นผู้ประมวลผลข้อมูลส่วนบุคคลช่วงเพื่อทำการประมวลผลข้อมูลส่วนบุคคลตามขอบเขตงานในสัญญาหลัก ในนามของสำนักงาน กสทช. ได้ เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช. ก่อน

๑๐.๒ ในกรณีที่ ผู้ประมวลผลข้อมูลส่วนบุคคลได้รับอนุญาตให้สามารถว่าจ้าง ผู้ประมวลผลข้อมูลส่วนบุคคลช่วงได้ตามข้อ ๑๐.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดทำข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคลช่วงเป็นลายลักษณ์อักษร โดยกำหนดขอบเขตเนื้อหาและหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลช่วงให้สอดคล้องกับหน้าที่และความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงนี้

ในกรณีที่สำนักงาน กสทช. ร้องขอเป็นลายลักษณ์อักษร ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการตรวจสอบการปฏิบัติหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลช่วงในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ได้รับจากสำนักงาน กสทช. และจัดทำผลการตรวจสอบ รวมทั้งส่งมอบผลการตรวจสอบให้แก่สำนักงาน กสทช. ในกรณีที่ปรากฏว่าผู้ประมวลผลข้อมูลส่วนบุคคลช่วงไม่ปฏิบัติตามหรือมีเหตุอันควรเชื่อว่าผู้ประมวลผลข้อมูลส่วนบุคคลช่วงอาจไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรืออาจก่อให้เกิดความเสียหายต่อสำนักงาน กสทช. ไม่ว่าในกรณีใด ๆ สำนักงาน กสทช. อาจขอให้ผู้ประมวลผลข้อมูลส่วนบุคคลเปลี่ยนผู้ประมวลผลข้อมูลส่วนบุคคลช่วงได้ทันที โดยสำนักงาน กสทช. ไม่ต้องรับผิดชอบในความเสียหายหรือค่าใช้จ่ายใด ๆ อันเกิดจากการเปลี่ยนผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

๑๑. การตรวจสอบ

๑๑.๑ ในกรณีที่สำนักงาน กสทช. มีการร้องขอเป็นลายลักษณ์อักษร ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องดำเนินการส่งมอบข้อมูลที่จำเป็นทั้งหมดให้แก่สำนักงาน กสทช. เพื่อเป็นการปฏิบัติหน้าที่ตามข้อตกลงนี้

๑๑.๒ ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงอนุญาตให้สำนักงาน กสทช. และบุคคลที่ได้รับมอบหมายจากสำนักงาน กสทช. เข้าตรวจสอบการปฏิบัติหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้ โดยสำนักงาน กสทช. จะแจ้งให้ ผู้ประมวลผลข้อมูลส่วนบุคคลทราบล่วงหน้าเป็นลายลักษณ์อักษรไม่น้อยกว่า ๗ วัน และ ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงให้ความร่วมมือแก่สำนักงาน กสทช. และบุคคลที่ได้รับมอบหมายจากสำนักงาน กสทช. ในการเข้าตรวจสอบดังกล่าวข้างต้น

๑๒. การชดเชยและการเยียวยา

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องชดเชยค่าเสียหายหรือค่าใช้จ่ายใด ๆ ให้แก่สำนักงาน กสทช. ในกรณีที่เกิดความเสียหาย การสูญหาย การเรียกร้อง ค่าเสียหาย ความรับผิดชอบทางแพ่ง โทษปรับทางปกครอง หรือค่าใช้จ่ายใด ๆ ที่เกิดขึ้นต่อบุคคลภายนอก หรือในกรณีที่สำนักงาน กสทช. จะต้องรับผิดชอบเนื่องมาจากการไม่ปฏิบัติตามข้อใดข้อหนึ่งภายใต้ข้อตกลงนี้หรือตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือการละเมิดคำรับรองและรับประกันของ ผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลที่ได้รับมอบหมายจากผู้ประมวลผลข้อมูลส่วนบุคคลให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคล ผู้รับจ้างช่วง ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง หรือตัวแทนของ ผู้ประมวลผลข้อมูลส่วนบุคคล

๑๓. การบอกกล่าว

บรรดาคำบอกกล่าวหรือการติดต่อสื่อสารใด ๆ ตามข้อตกลงนี้ ให้ทำเป็นลายลักษณ์อักษรโดยให้ส่งโดยบุคคล หรือไปรษณีย์ หรือโทรสาร ไปยังสถานที่ของผู้รับตามที่ระบุไว้ในข้อตกลงนี้ หรือตามที่ได้รับแจ้งเปลี่ยนแปลงจากผู้รับ (ถ้ามี) คำบอกกล่าวหรือการติดต่อสื่อสารทั้งหลายจะถือว่าผู้รับได้รับแล้วเมื่อคำบอกกล่าวหรือการติดต่อสื่อสารนั้นไปถึงสถานที่นั้นแล้ว

๑๔. หน้าที่และความรับผิดชอบ ผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตามข้อตกลงนี้จะสิ้นสุดลงนับแต่วันที่การปฏิบัติงานตามขอบเขตงานในสัญญาหลักเสร็จสิ้น หรือวันที่ ผู้ประมวลผลข้อมูลส่วนบุคคลและสำนักงาน กสทช. ได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิกการดำเนินการตามขอบเขตงานนี้แล้วแต่กรณีใดจะเกิดขึ้นก่อน โดยคู่สัญญาตกลงจะไม่โอนสิทธิเรียกร้องตามข้อตกลงนี้ให้แก่บุคคลอื่น