ร่างขอบเขตของงาน (Terms of Reference : TOR)
โครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อการให้บริการผู้เสียภาษีสรรพสามิต

.....

๑. หลักการและเหตุผล

ตามที่กรมสรรพสามิตได้ให้บริการงานต่าง ๆ ด้วยระบบอิเล็กทรอนิกส์แก่ผู้ประกอบการมามากกว่า ๒๐ ปี และหลายบริการเป็นการให้บริการด้วยตนเองของผู้ประกอบการ และในปี ๒๕๕๘ ประเทศไทยได้เข้าสู่ประชาคมเศรษฐกิจอาเซียนหรือ AEC อย่างเต็มรูปแบบ พร้อมทั้งได้มีการพัฒนาระบบอิเล็กทรอนิกส์เพื่อการรองรับการปรับเปลี่ยนโนบายของประเทศไทย เพื่อเข้าสู่ยุค Thailand ๔.๐ ทำให้กรมสรรพสามิตจำเป็นที่จะต้องสร้างความเชื่อมั่นในบริการอิเล็กทรอนิกส์แก่ผู้ประกอบอุตสาหกรรมทั้งภายในและภายนอกประเทศ โดยเตรียมความพร้อมในด้านความมั่นคงเชื่อถือได้ในบริการอิเล็กทรอนิกส์ต่าง ๆ ที่ใช้ในการแลกเปลี่ยนข้อมูล สามารถรักษาความลับทางการค้า และมีความมั่นคงปลอดภัยในระบบสารสนเทศที่มีมาตรฐานเป็นที่ยอมรับในระดับนานาชาติที่กลุ่มประเทศในภาคี AEC ให้การยอมรับ นอกจากนี้ ยังมีการประกาศบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อใช้ในการกำกับดูแลภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพ พร้อมทั้งสามารถคุ้มครองสิทธิ์ของประชาชนจากการละเมิดจากหน่วยงานหรือองค์กรต่าง ๆ ดังนั้น กรมสรรพสามิตจึงจำเป็นที่จะต้องมีผู้เชี่ยวชาญในการศึกษาวิเคราะห์ และพัฒนาแผนการปรับปรุงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อปฏิบัติตามข้อกำหนดพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ และเป็นการปฏิบัติตามข้อกำหนดพระราชบัญญัติทั้งสองฉบับ

กรมสรรพสามิตจึงมีความจำเป็นต้องพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล เพื่อเป็นการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมทั้งขยายขอบเขตการขอรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑ ซึ่งเป็นมาตรฐานสากล และเป็นมาตรฐานที่ได้รับการยอมรับในระดับนานาชาติ ให้ครอบคลุมห้องดาต้าเซ็นเตอร์อาคารศูนย์ข้อมูลสำรอง (DR Site) ของกรมสรรพสามิต

๒. วัตถุประสงค์

๒.๑ เพื่อดำเนินการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลของศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต เพื่อให้การดำเนินงานและมาตรการป้องกันที่มีประสิทธิภาพ

๒.๒ เพื่อให้กระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศของห้องดาต้าเซ็นเตอร์อาคารศูนย์ข้อมูลสำรอง (DR Site) กรมสรรพสามิต ได้รับการรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑

๒.๓ เพื่อดำเนินการให้กรมสรรพสามิตสามารถปฏิบัติตามข้อกำหนดของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

ON.U.64

๓. ขอบเขตการดำเนินโครงการกับหน้าที่ความรับผิดชอบ

ผู้เสนอราคาจะดำเนินการตามข้อกำหนดและรายละเอียด ขอบเขตการดำเนินงานตาม "โครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อการให้บริการผู้เสียภาษีสรรพสามิต" โดยมีขอบเขตงาน ดังนี้

๓.๑ ผู้เสนอราคาจะต้องศึกษา วิเคราะห์ วางแผน และพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลของศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต ให้มีประสิทธิภาพและประสิทธิผล สอดคล้องตามข้อกำหนดของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมทั้งการจัดหาซอฟต์แวร์ สนับสนุนการปฏิบัติงานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต เพื่อให้โครงสร้างพื้นฐานระบบเทคโนโลยีสารสนเทศของศูนย์คอมพิวเตอร์ (Data Center) หลักห้องปฏิบัติการระบบเครือข่าย (Network Operation Center: NOC) ห้องปฏิบัติการความมั่นคงปลอดภัยสารสนเทศ (Security Operation Center: SOC) และศูนย์คอมพิวเตอร์สำรอง (DR Site) ผ่านการรับรองมาตรฐานสากล ISO/IEC ๒๗๐๐๑ โดยมีรายละเอียดตามเอกสารประกวดราคาทางอิเล็กทรอนิกส์ **ตามเอกสารหมายเลข ๒**

๓.๒ ฝึกอบรมการใช้งานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อการให้บริการผู้เสียภาษีสรรพสามิต รวมจำนวน ๕ หลักสูตร โดยมีรายละเอียดตามเอกสารประกวดราคาทางอิเล็กทรอนิกส์ **ตามเอกสารหมายเลข ๓**

๔. คุณสมบัติของผู้ประสงค์เสนอราคา

๔.๑ มีความสามารถตามกฎหมาย

๔.๒ ไม่เป็นบุคคลล้มละลาย

๔.๓ ไม่อยู่ระหว่างเลิกกิจการ

๔.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลงานการปฏิบัติงานของผู้ประกอบการตามระเบียบรัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๔.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๔.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๔.๗ เป็นนิติบุคคล ผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๔.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่นที่เข้ายื่นเสนอราคาให้แก่กรมสรรพสามิต ณ วันที่ประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์นี้

๔.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

๔.๑๐ ผู้เสนอราคาต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

๔.๑๑ ผู้เสนอราคาต้องเป็นนิติบุคคลตามกฎหมายที่จดทะเบียนในประเทศไทย ที่มิใช่เป็นกิจการร่วมค้าหรือเทียบเท่า ซึ่งมีวัตถุประสงค์ในการประกอบธุรกิจเป็นผู้พัฒนา ปรับปรุง หรือออกแบบติดตั้ง หรือผู้ผลิต และ/หรือจำหน่าย และ/หรือเช่า/ให้เช่าซื้อ ด้านระบบคอมพิวเตอร์ หรือระบบเทคโนโลยีสารสนเทศ โดยมีหลักฐานการจดทะเบียนซึ่งกรมพัฒนาธุรกิจการค้ากระทรวงพาณิชย์ออกให้หรือรับรองให้ไม่เกิน ๖ เดือน นับจนถึงวันยื่นเอกสารประกวดราคา

๔.๑๒ ผู้เสนอราคาต้องเคยมีผลงานทางด้านการดำเนินโครงการที่เกี่ยวข้องกับการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑ หรือพัฒนาระบบงานเทคโนโลยีสารสนเทศ หรือติดตั้งระบบคอมพิวเตอร์ ซึ่งได้ส่งมอบและตรวจรับเป็นที่เรียบร้อยแล้ว โดยมีผลงานไม่ต่ำกว่า ๑๕,๐๐๐,๐๐๐ บาท (สิบห้าล้านบาทถ้วน) จำนวน ๑ สัญญา และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ โดยต้องเสนอสำเนาเอกสารสัญญาพร้อมเอกสารแนบท้ายสัญญา และหนังสือรับรองผลงานจากหน่วยงานเจ้าของงาน ซึ่งลงนามโดยหัวหน้าส่วนราชการ หรือรัฐวิสาหกิจ หรือหัวหน้าหน่วยงานของรัฐ เจ้าของงานนั้น ๆ

๔.๑๓ ผู้เสนอราคาต้องเสนอทีมงานที่ได้รับการรับรอง มาตรฐานความรู้ความสามารถจากหน่วยงานในระดับสากล พร้อมทั้งสำเนา Certification ที่ยังไม่หมดอายุตามข้อ ๕ **เอกสารหมายเลข ๑** ข้อกำหนดด้านบุคลากร มอบให้กรมสรรพสามิต ณ วันเสนอราคา เพื่อประกอบการพิจารณาและสามารถตรวจสอบได้ โดยทีมงานที่เสนอมีคุณสมบัติอย่างน้อยตามข้อ ๕ **เอกสารหมายเลข ๑** ข้อกำหนดด้านบุคลากร

๕. คุณลักษณะเฉพาะ

โดยมีรายละเอียดตามเอกสารแนบประกวดราคาจ้างด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) โครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อการให้บริการผู้เสียภาษีสรรพสามิต

๖. ระยะเวลาการดำเนินการ

๓๖๐ วัน นับถัดจากวันที่ลงนามในสัญญาจ้าง

๗. ระยะเวลาการส่งมอบงาน

งวดงานการส่งมอบมี ๔ งวด ดังนี้

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

งวดที่ ๑ ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา ส่งมอบเอกสาร ดังนี้

(๑) แผนการดำเนินงาน (Project Plan) ซึ่งต้องระบุกิจกรรม เวลา และผู้รับผิดชอบ

(๒) รายละเอียดซอฟต์แวร์ที่ต้องใช้ในโครงการฯ

จำนวน ๓ ชุด พร้อม Flash Drive บรรจุรายละเอียดตามเอกสาร จำนวน ๓ ชุด

งวดที่ ๒ ภายใน ๑๕๐ วัน นับถัดจากวันลงนามในสัญญา

(๑) จัดหาและติดตั้งซอฟต์แวร์ Risk Assessment พร้อมคู่มือการใช้งาน

(๒) จัดหาและติดตั้งซอฟต์แวร์ Vulnerability Assessment พร้อมคู่มือการใช้งาน

(๓) ส่งมอบเอกสารดำเนินการทดสอบการโจมตีระบบเทคโนโลยีสารสนเทศผ่านช่องทางระบบเครือข่ายอินเทอร์เน็ตในรูปแบบ Black-box

(๔) ส่งมอบเอกสารรายงานสรุปผลการวิเคราะห์ และข้อเสนอแนะเพื่อการเตรียมพร้อมในการตอบสนองคุกคามด้านไซเบอร์ ทั้งในด้านของบุคลากร (People) กระบวนการบริหารจัดการ (Process) และระบบเทคโนโลยีที่ใช้ในการป้องกันและตรวจจับภัยคุกคามด้านไซเบอร์ (Technology)

(๕) ส่งมอบเอกสารนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy)

(๖) ส่งมอบเอกสารขั้นตอนการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ (Risk Assessment Methodology)

(๗) ส่งมอบเอกสารรายงานผลการตรวจสอบช่องโหว่ (Vulnerability Assessment)

(๘) ส่งมอบเอกสารรายงานผลการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ (Risk Assessment Report)

(๙) ส่งมอบเอกสารนโยบาย (Policy) หรือขั้นตอนการปฏิบัติ (Procedure)

(๑๐) ส่งมอบเอกสารรายงานคำแนะนำทางกฎหมายสำหรับเป็นนโยบายหลักเกณฑ์ระเบียบและแนวทิธีปฏิบัติงานต่าง ๆ ที่ชัดเจน ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

จำนวน ๓ ชุด พร้อม Flash Drive บรรจุรายละเอียดตามเอกสาร จำนวน ๓ ชุด

งวดที่ ๓ ภายใน ๒๔๐ วัน นับถัดจากวันลงนามในสัญญา ส่งมอบเอกสาร ดังนี้

(๑) Statement Of Applicability (SOA)

(๒) การวัดประสิทธิผลมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ (Effectiveness Measurement)

(๓) ส่งมอบเอกสารประกอบการอบรม

(๔) รายงานผลการตรวจสอบภายใน

(๕) รายงานสรุปผลการดำเนินงานของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Review)

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

(๖) นโยบายหรือขั้นตอนการปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริหารจัดการระบบเทคโนโลยีสารสนเทศ

(๗) แผนงาน/โครงการ/กิจกรรมหลัก ในการพัฒนาความมั่นคงปลอดภัยสารสนเทศ (IT Security Master Plan)

จำนวน ๓ ชุด พร้อม Flash Drive บรรจุรายละเอียดตามเอกสาร จำนวน ๓ ชุด

งวดที่ ๔ ภายใน ๓๖๐ วัน นับถัดจากวันลงนามในสัญญา

(๑) ส่งมอบจดหมายยืนยัน (Attestation Letter) หรือใบประกาศนียบัตร (Certification) จาก Certification Body ที่แสดงหรือบ่งชี้ว่าสำนักงานศูนย์เทคโนโลยีสารสนเทศของกรมสรรพสามิต ผ่านการรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑

(๒) ส่งมอบการฝึกอบรม คู่มือผู้ใช้งาน พร้อมส่งมอบเอกสารการฝึกอบรม

จำนวน ๓ ชุด พร้อม Flash Drive บรรจุรายละเอียดตามเอกสาร จำนวน ๓ ชุด

๘. **การเบิกจ่ายเงิน** แบ่งการจ่ายเงินออกเป็น ๔ งวด ดังนี้

งวดที่ ๑ ชำระเงินในอัตราร้อยละ ๑๐ ของวงเงินที่จ้างตามสัญญา หลังจากกรมสรรพสามิตตรวจรับงานในงวดที่ ๑ เรียบร้อยแล้ว

งวดที่ ๒ ชำระเงินในอัตราร้อยละ ๔๐ ของวงเงินที่จ้างตามสัญญา หลังจากกรมสรรพสามิตตรวจรับงานในงวดที่ ๒ เรียบร้อยแล้ว

งวดที่ ๓ ชำระเงินในอัตราร้อยละ ๓๐ ของวงเงินที่จ้างตามสัญญา หลังจากกรมสรรพสามิตตรวจรับงานในงวดที่ ๓ เรียบร้อยแล้ว

งวดที่ ๔ ชำระเงินในอัตราร้อยละ ๒๐ ของวงเงินที่จ้างตามสัญญา หลังจากกรมสรรพสามิตตรวจรับงานในงวดที่ ๔ เรียบร้อยแล้ว

๙. **วงเงินและงบประมาณในการจัดจ้าง**

เงินฝากค่าใช้จ่ายเก็บภาษีท้องถิ่นปีงบประมาณ พ.ศ. ๒๕๖๕ รวมเป็นเงินจำนวนทั้งสิ้น ๓๒,๑๐๐,๐๐๐ บาท (สามสิบสองล้านหนึ่งแสนบาทถ้วน)

๑๐. **หน่วยงานผู้รับผิดชอบ**

ศูนย์เทคโนโลยีสารสนเทศ กรมสรรพสามิต
โทร ๐-๒๒๔๑-๕๖๐๐-๑๙ เบอร์ต่อ ๖๔๓๐๕
ติดต่อ นายไพโรจน์ สว่างภพ นักวิชาการสรรพสามิตชำนาญการ
e-mail : pok@excise.go.th

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

เอกสารหมายเลข ๑
รายละเอียดหลักเกณฑ์และข้อกำหนด

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

รายละเอียดหลักเกณฑ์และข้อกำหนด

"โครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อการให้บริการผู้เสียภาษีสรรพสามิต" ต่อไปนี้เรียกว่า "ระบบงาน" ซึ่งประกอบด้วย

ลำดับ	รายการ	จำนวน	หน่วย
๑. งานจัดหาเครื่องมือ (Software)			
๑.๑	จัดหาซอฟต์แวร์ Risk Assessment	๑	ระบบ
๑.๒	จัดหาซอฟต์แวร์ Vulnerability Assessment	๑	ระบบ
๑.๓	งานการติดตั้งซอฟต์แวร์ ปรับแต่ง และทดสอบการใช้งาน	๑	งาน
๒. งานจัดทำแผน ระบบงาน และเอกสารขั้นตอนกระบวนงาน			
๒.๑	จัดทำแผนการดำเนินงาน (Project Plan) และรายละเอียดในการดำเนินงาน ซึ่งต้องระบุกิจกรรม ระยะเวลา และผู้รับผิดชอบ	๑	งาน
๒.๒	จัดทำแผนการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อปฏิบัติตามข้อกำหนดพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒	๑	งาน
๒.๓	จัดทำแผนพัฒนาหรือปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑ โดยครอบคลุมขอบเขตของโครงสร้างพื้นฐานระบบเทคโนโลยีสารสนเทศของศูนย์คอมพิวเตอร์ (Data Center) หลัก ห้องปฏิบัติการระบบเครือข่าย (Network Operation Center: NOC) ห้องปฏิบัติการความมั่นคงปลอดภัยสารสนเทศ (Security Operation Center: SOC) และศูนย์คอมพิวเตอร์สำรอง (DR Site) พร้อมกับตรวจสอบเพื่อให้ได้รับการรับรองมาตราฐาน ISO/IEC ๒๗๐๐๑	๑	งาน
๒.๔	จัดทำแผนพัฒนาและการปรับปรุงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อปฏิบัติตามข้อกำหนดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	๑	งาน
๒.๕	ดำเนินการนำผลการศึกษา และวิเคราะห์ที่ได้มาพัฒนาแผนงาน/โครงการ/กิจกรรมหลัก ในการพัฒนาความมั่นคงปลอดภัยสารสนเทศ (IT Security Master Plan) ระยะ ๓ ปี	๑	งาน
๓. งานฝึกอบรม			
๓.๑	หลักสูตรมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ สำหรับคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) ของกรมสรรพสามิต จำนวนผู้เข้าอบรมอย่างน้อย ๑๐ คน จำนวน ๑ รุ่น	๑	หลักสูตร
๓.๒	หลักสูตรมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ สำหรับคณะทำงานในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Operation Team) ของกรมสรรพสามิตจำนวนผู้เข้าอบรมอย่างน้อย ๑๐ คน จำนวน ๑ รุ่น	๑	หลักสูตร

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

ลำดับ	รายการ	จำนวน	หน่วย
๓.๓	หลักสูตรการสร้าง Awareness ในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จำนวนผู้เข้าอบรมอย่างน้อย ๕๐ คน จำนวน ๑ รุ่น	๑	หลักสูตร
๓.๔	หลักสูตรการตรวจสอบภายใน ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Internal Audit) สำหรับคณะผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศจำนวนผู้เข้าอบรมอย่างน้อย ๑๐ คน จำนวน ๑ รุ่น	๑	หลักสูตร
๓.๕	หลักสูตรการเตรียมความพร้อมในการปฏิบัติตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จำนวนผู้เข้าอบรมอย่างน้อย ๕๐ คน จำนวน ๑ รุ่น	๑	หลักสูตร

โดยมีรายละเอียดหลักเกณฑ์ และข้อกำหนด ซึ่งผู้เสนอราคาต้องดำเนินการให้เป็นไปตามเงื่อนไขต่างๆ ดังต่อไปนี้

๑. <u>ข้อกำหนดด้านเอกสารการเสนอราคา</u>

๑.๑ ผู้ยื่นข้อเสนอราคาต้องนำเสนอเอกสารหลักฐานยื่นมาพร้อมใบเสนอราคาทางระบบจัดซื้อจัดจ้างภาครัฐด้วยวิธีอิเล็กทรอนิกส์ ตามข้อกำหนดในเอกสารประกวดราคาอิเล็กทรอนิกส์ โดยให้มีเลขที่กำกับเอกสารทุกหน้า

๑.๒ ให้ผู้เสนอราคาจัดทำข้อเสนอด้านคุณลักษณะเฉพาะของงานตามเอกสารการประกวดราคาจ้างด้วยวิธีการทางอิเล็กทรอนิกส์ โดยให้จัดทำในรูปแบบ ดังนี้

หัวข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อเสนอของบริษัท	เอกสารอ้างอิง (หน้า,ข้อ)
ระบุหัวข้อให้ตรงกับหัวข้อที่ระบุในเอกสารประกวดราคา	ให้คัดลอกคุณลักษณะเฉพาะที่กรมสรรพสามิตกำหนด	ให้ระบุคุณลักษณะเฉพาะที่บริษัทฯ เสนอ	ให้ระบุหรืออ้างถึงเอกสารในข้อเสนอที่เกี่ยวข้องและขีดเส้นใต้คุณลักษณะที่เสนอในแคตตาล็อก หรือเอกสารที่เกี่ยวข้อง

๑.๓ ผู้เสนอราคาต้องจัดทำสารบัญเอกสารอ้างอิง และแนบเอกสารอ้างอิงให้มีความครบถ้วนสมบูรณ์ตามสารบัญเอกสารอ้างอิงด้วย

๑.๔ ผู้เสนอราคาจะต้องเสนอรายละเอียดการฝึกอบรม โดยให้มีรายละเอียด **ตามเอกสารหมายเลข ๓** เป็นอย่างน้อย

๑.๕ ผู้เสนอราคาจะต้องเสนอแผนและทีมงานในการดำเนินงานและประสบการณ์ **ตามเอกสารหมายเลข ๕** ดังนี้

๑.๕.๑ คุณสมบัติทั่วไป และประสบการณ์ของผู้เสนอราคา

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๑.๕.๒ ตารางสรุปคุณสมบัติ ประสบการณ์ และประวัติของบุคลากรที่เสนอรายชื่อ ให้เสนอเฉพาะตำแหน่งตามรายละเอียดในข้อ ๕ ข้อกำหนดด้านบุคลากร

๑.๕.๓ ตารางแผนงาน วิธีดำเนินการ และเครื่องมือในการบริหารจัดการและเทคนิคที่ใช้โดยละเอียด

๑.๖ การนำเสนอ (Presentation) กรมสรรพสามิตอาจจะเรียกผู้เสนอราคามาบรรยายสรุปต่อคณะกรรมการฯ ในวัน/เวลา และสถานที่ที่กรรมการจะแจ้งให้ทราบในภายหลัง ทั้งนี้กรมสรรพสามิตขอสงวนสิทธิ์เฉพาะผู้ที่ผ่านการพิจารณาข้อเสนอด้านเอกสารเท่านั้น จึงจะมีสิทธิในการนำเสนอ

๑.๗ ผู้ยื่นข้อเสนอราคาต้องส่งแคตตาล็อก และ/หรือรูปแบบรายละเอียดคุณลักษณะเฉพาะของ “ระบบงาน” ไปพร้อมเอกสารหลักฐาน เพื่อประกอบการพิจารณา โดยผู้ยื่นข้อเสนอราคาต้องทำเครื่องหมายคุณลักษณะที่เสนอในแคตตาล็อกให้ตรงกับข้อกำหนดคุณลักษณะเฉพาะที่กรมสรรพสามิตกำหนด หลักฐานดังกล่าวนี้กรมสรรพสามิตจะยึดไว้เป็นเอกสารของทางราชการ สำหรับแคตตาล็อกที่แนบให้พิจารณา หากเป็นสำเนารูปถ่ายจะต้องรับรองสำเนาถูกต้องโดยผู้มีอำนาจทำนิติกรรมแทนนิติบุคคล หากคณะกรรมการประกวดราคามีความประสงค์จะขอดูเอกสารแคตตาล็อกต้นฉบับ ผู้ยื่นข้อเสนอราคาต้องนำเอกสารแคตตาล็อกต้นฉบับมาให้คณะกรรมการประกวดราคาตรวจสอบภายใน ๓ วัน นับแต่วันที่ได้รับแจ้ง

๑.๘ เงื่อนไขและรายละเอียดของเอกสารการประกวดราคาพร้อมข้อเสนอขอบเขตงาน และเอกสารประกอบผู้ยื่นข้อเสนอราคา ให้ถือเป็นส่วนหนึ่งของสัญญาด้วย

๑.๙ ผู้ยื่นข้อเสนอราคาต้องทำความเข้าใจในเอกสารทุกฉบับให้เป็นที่เข้าใจโดยชัดแจ้ง และไม่ว่าในกรณีใด ๆ ผู้เสนอราคาจะยกขึ้นมาเป็นข้ออ้างโดยอาศัยเหตุผลจากการที่ละเลยไม่ทำความเข้าใจในข้อความดังกล่าว หรือละเลยไม่ปฏิบัติตามข้อความนั้น หรือโดยอ้างความสำคัญผิดในความหมายของข้อความในเอกสารการประกวดราคานั้นไม่ได้

๑.๑๐ รายละเอียดต่าง ๆ ที่ผู้ยื่นข้อเสนอราคา เสนอมานั้น หากมีปัญหาเกี่ยวกับการตีความของข้อความใดในระหว่างพิจารณาตัดสิน ให้ถือคำวินิจฉัยของคณะกรรมการฯ เป็นเด็ดขาด

๑.๑๑ ข้อกำหนดด้านการทดสอบระบบ

กรมสรรพสามิตจะมีการทดสอบความสามารถของผู้ยื่นข้อเสนอราคาด้านเทคนิค POC : Proof of Concept ผู้ยื่นข้อเสนอราคาต้องมีความพร้อมในการดำเนินการทำ POC ทั้งนี้กรมสรรพสามิตขอสงวนสิทธิ์เฉพาะผู้ที่ผ่านการพิจารณาข้อเสนอด้านเอกสารเท่านั้น จึงจะมีสิทธิในการทดสอบด้านเทคนิค POC ผู้ยื่นข้อเสนอราคาจะต้องเข้าร่วมในการทดสอบ ภายในระยะเวลา ๑ ชั่วโมง โดยมีรายละเอียด ดังนี้

๑.๑๑.๑ ข้อกำหนดการทดสอบทางด้านเทคนิคของซอฟต์แวร์การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Assessment) ประกอบไปด้วย

๑.๑๑.๑.๑ นำเสนอโปรแกรมสาธิตการใช้งานซอฟต์แวร์การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Assessment) ตามข้อกำหนดใน**ตามเอกสารหมายเลข ๒**

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๑.๑๑.๑.๒ สาธิตการเชื่อมต่อกับระบบ Single Sign On (SSO) ของกรมสรรพสามิต

๑.๑๑.๑.๓ สาธิตวิธีการปรับเปลี่ยนกระบวนการประเมินความเสี่ยง (Risk Assessment Methodology) โดยจะต้องแสดงการปรับเปลี่ยน Heat Map ของการประเมินความเสี่ยงในรูปแบบ Matrix ๓x๓ และ ๕x๕

๑.๑๑.๑.๔ สาธิตการจัดทำรายงานผลการประเมินความเสี่ยง และการ Export รายงานออกจากระบบ

๑.๑๑.๒ ข้อกำหนดการทดสอบทางด้านเทคนิคของซอฟต์แวร์ตรวจสอบช่องโหว่ (Vulnerability Assessment) ประกอบไปด้วย

๑.๑๑.๒.๑ นำเสนอโปรแกรมสาธิตการใช้งานซอฟต์แวร์ในการตรวจสอบช่องโหว่ (Vulnerability Assessment) ตามข้อกำหนดใน**ตามเอกสารหมายเลข ๒**

๑.๑๑.๒.๒ สาธิตการตรวจสอบช่องโหว่บนอุปกรณ์ที่รองรับทั้ง IPv๔ และ IPv๖

๑.๑๑.๒.๓ สาธิตการตรวจสอบช่องโหว่ของระบบปลายทางได้แบบ Credentialed Scanning เพื่อตรวจหาการตั้งค่าความปลอดภัยของระบบ (system hardening) และ Patches ที่ไม่ได้ติดตั้ง

๑.๑๑.๒.๔ สาธิตวิธีการตั้งเวลาในการตรวจสอบช่องโหว่

ทั้งนี้ หากมีรายละเอียดเพิ่มเติม กรมสรรพสามิตจะชี้แจงรายละเอียดในการทดสอบด้านเทคนิคภายใน ๓ วันทำการ นับถัดจากวันเสนอราคาสิ้นสุดในการประกวดราคาจ้างด้วยวิธีอิเล็กทรอนิกส์ในครั้งนี้

๑.๑๑.๓ การทดสอบทางด้านเทคนิคจะทดสอบภายใน ๕ วันทำการ นับถัดจากวันเสนอราคาสิ้นสุดในการประกวดราคาจ้างด้วยวิธีอิเล็กทรอนิกส์ในครั้งนี้

๑.๑๑.๔ ผู้ยื่นข้อเสนอราคาจะต้องนำอุปกรณ์เข้าร่วมในการทดสอบและค่าใช้จ่ายที่เกิดขึ้น ผู้ยื่นข้อเสนอราคาเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมด โดยกรมสรรพสามิตจะรับผิดชอบในส่วนกระแสไฟฟ้าที่จ่ายให้ระบบเท่านั้น

๑.๑๑.๕ ในการพิจารณาผล ถ้ามีเหตุโต้แย้ง คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ขอสงวนสิทธิ์ในการพิจารณาในเฉพาะประเด็นที่ส่วนราชการได้ประโยชน์เท่านั้น และถือว่าความเห็นของคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์นั้นถือเป็นที่สิ้นสุด โดยผู้เสนอราคาจะฟ้องร้องหรือเรียกร้องสิ่งใดในภายหลังมิได้

๑.๑๑.๖ ในการทดสอบด้านเทคนิคนั้น คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์จะชี้แจงรายละเอียดให้ผู้ผ่านการพิจารณาด้านเอกสารอีกครั้ง ในเวลา ๐๘.๓๐ ถึง ๑๖.๓๐ น. ณ ห้องประชุม กรมสรรพสามิต

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๒. ข้อกำหนดด้านการเสนอราคา

๒.๑ ราคาของ “โครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อการให้บริการผู้เสียภาษีสรรพสามิต” ผู้ยื่นข้อเสนอราคาต้องระบุราคาต่อหน่วยต่อรายการ และราคารวมทั้งโครงการ โดยแสดงรายการตามรายละเอียดใบเสนอราคา ภายหลังผู้ยื่นข้อเสนอราคาเป็นผู้ชนะการประกวดราคาแล้ว ประกอบด้วย

ลำดับ	รายการ	จำนวน	หน่วย
๑. งานจัดหาเครื่องมือ (Software)			
๑.๑	จัดหาซอฟต์แวร์ Risk Assessment	๑	ระบบ
๑.๒	จัดหาซอฟต์แวร์ Vulnerability Assessment	๑	ระบบ
๑.๓	งานการติดตั้งซอฟต์แวร์ ปรับแต่ง และทดสอบการใช้งาน	๑	งาน
๒. งานจัดทำแผน ระบบงาน และเอกสารขั้นตอนกระบวนงาน			
๒.๑	จัดทำแผนการดำเนินงาน (Project Plan) และรายละเอียดในการดำเนินงาน ซึ่งต้องระบุกิจกรรม ระยะเวลา และผู้รับผิดชอบ	๑	งาน
๒.๒	จัดทำแผนการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อปฏิบัติตามข้อกำหนดพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒	๑	งาน
๒.๓	จัดทำแผนพัฒนาหรือปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑ โดยครอบคลุมขอบเขตของโครงสร้างพื้นฐานระบบเทคโนโลยีสารสนเทศของศูนย์คอมพิวเตอร์ (Data Center) หลัก ห้องปฏิบัติการระบบเครือข่าย (Network Operation Center: NOC) ห้องปฏิบัติการความมั่นคงปลอดภัยสารสนเทศ (Security Operation Center: SOC) และศูนย์คอมพิวเตอร์สำรอง (DR Site) พร้อมกับตรวจสอบเพื่อให้ได้รับการรับรองมาตราฐาน ISO/IEC ๒๗๐๐๑	๑	งาน
๒.๔	จัดทำแผนพัฒนาและการปรับปรุงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อปฏิบัติตามข้อกำหนดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	๑	งาน
๒.๕	ดำเนินการนำผลการศึกษา และวิเคราะห์ที่ได้มาพัฒนาแผนงาน/โครงการ/กิจกรรมหลัก ในการพัฒนาความมั่นคงปลอดภัยสารสนเทศ (IT Security Master Plan) ระยะ ๓ ปี	๑	งาน
๓. งานฝึกอบรม			
๓.๑	หลักสูตรมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ สำหรับคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) ของกรมสรรพสามิต จำนวนผู้เข้าอบรมอย่างน้อย ๑๐ คน จำนวน ๑ รุ่น	๑	หลักสูตร
๓.๒	หลักสูตรมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ สำหรับคณะทำงานในการพัฒนาระบบบริหารจัดการความมั่นคง	๑	หลักสูตร

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

ลำดับ	รายการ	จำนวน	หน่วย
	ปลอดภัยสารสนเทศ (ISMS Operation Team) ของกรมสรรพสามิตจำนวนผู้เข้าอบรมอย่างน้อย ๑๐ คน จำนวน ๑ รุ่น		
๓.๓	หลักสูตรการสร้าง Awareness ในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จำนวนผู้เข้าอบรมอย่างน้อย ๕๐ คน จำนวน ๑ รุ่น	๑	หลักสูตร
๓.๔	หลักสูตรการตรวจสอบภายใน ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Internal Audit) สำหรับคณะผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศจำนวนผู้เข้าอบรมอย่างน้อย ๑๐ คน จำนวน ๑ รุ่น	๑	หลักสูตร
๓.๕	หลักสูตรการเตรียมความพร้อมในการปฏิบัติตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จำนวนผู้เข้าอบรมอย่างน้อย ๕๐ คน จำนวน ๑ รุ่น	๑	หลักสูตร

๒.๒ ราคาของระบบงานรวมอุปกรณ์ และค่าใช้จ่ายต่าง ๆ ที่ต้องมีเพื่อให้โครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อการให้บริการผู้เสียภาษีสรรพสามิตทำงานได้อย่างสมบูรณ์ และมีประสิทธิภาพ ให้รวมไปถึงค่า Hardware, Software ค่าติดตั้ง และค่าอุปกรณ์เชื่อมต่อเข้ากับระบบเครือข่ายของกรมสรรพสามิต โดยกรมสรรพสามิตไม่ต้องเสียค่าใช้จ่ายใด ๆ เพิ่มเติมจากที่ปรากฏในใบเสนอราคา

๒.๓ ราคาที่เสนอจะต้องเสนอกำหนดยืนราคาไม่น้อยกว่า ๑๒๐ วัน นับแต่วันเสนอราคา โดยภายในกำหนดยืนราคาผู้ยื่นข้อเสนอราคาต้องรับผิดชอบราคาที่ตนเสนอไว้ และจะถอนการเสนอราคามิได้

๓. ข้อกำหนดทั่วไปของระบบงานที่เสนอ

๓.๑ คุณสมบัติของระบบงาน และขอบเขตการดำเนินงานที่กำหนดไว้ **ตามเอกสารหมายเลข ๒** เป็นข้อมูลเบื้องต้นซึ่งอาจมีการปรับเปลี่ยน โดยคู่สัญญาต้องจัดส่งทีมงานตามที่เสนอมาดำเนินการรวบรวม และวิเคราะห์ความต้องการของระบบในรายละเอียดอีกครั้ง

๓.๒ อุปกรณ์ ฮาร์ดแวร์ และซอฟต์แวร์ที่เสนอใช้ในโครงการต้องเป็นรุ่น Version ล่าสุด ในวันยื่นประกวดราคาจ้างด้วยวิธีอิเล็กทรอนิกส์ในครั้งนี้ และระบบคอมพิวเตอร์ที่จะนำมาติดตั้งให้กรมสรรพสามิตจะต้องเป็นเครื่องใหม่ (New) ไม่ใช่เครื่องเก่าใช้แล้ว (Used) หรือเครื่องล้าสมัย (Obsolete) หรือเครื่องที่ใช้งานแล้วและนำมาปรับปรุงใหม่ (Reconditioned)

๓.๓ อุปกรณ์ ฮาร์ดแวร์ และซอฟต์แวร์ ที่เสนอต้องไม่เป็นผลิตภัณฑ์ของบริษัทผู้ผลิตที่อยู่ในระหว่างการคุ้มครอง การเป็นบุคคลหรือนิติบุคคลผู้ล้มละลายตามคำสั่งของศาลที่ได้สั่งการตามกฎหมายของประเทศที่บริษัทของผู้ผลิตนั้นตั้งอยู่

๓.๔ อุปกรณ์ ฮาร์ดแวร์ และซอฟต์แวร์ ที่เสนอให้รวมค่าติดตั้งและค่าอุปกรณ์อื่นเชื่อมต่อเข้ากับระบบเครือข่ายของกรมสรรพสามิต รวมถึงค่าใช้จ่ายในการดำเนินการต่าง ๆ ที่ต้องมีเพื่อให้ระบบงาน

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ โดยกรมสรรพสามิตไม่ต้องเสียค่าใช้จ่ายใด ๆ เพิ่มเติมจากที่ปรากฏในใบเสนอราคา

๓.๕ ผู้ชนะการประกวดราคาต้องเป็นผู้รับผิดชอบในการติดตั้ง “ระบบงาน” และอุปกรณ์อื่นที่กรมสรรพสามิตจัดเตรียมไว้ ให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ และใช้งานได้จริง

๓.๖ ต้องสามารถใช้รหัสภาษาไทยตามมาตรฐานที่กำหนดโดยสำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม กระทรวงอุตสาหกรรม (สมอ.)

๓.๗ หากผู้ยื่นข้อเสนอราคาพิจารณาเห็นว่าข้อกำหนดหรือคุณลักษณะข้อใดมีไม่เพียงพอ ผู้ยื่นข้อเสนอราคาสามารถเสนอสิ่งที่ดีกว่าข้อเสนอที่นำเสนอไว้ได้ เพื่อให้ระบบงานใช้งานได้อย่างมีประสิทธิภาพ โดยต้องได้รับความเห็นชอบจากกรมสรรพสามิตก่อนจึงจะดำเนินการ

๔. ข้อกำหนดด้านการให้บริการและบำรุงรักษาระบบ

๔.๑ ผู้ชนะการประกวดราคาจะต้องรับประกันความชำรุดบกพร่อง หรือความขัดข้องของ“ระบบงาน” เป็นระยะเวลาไม่น้อยกว่า ๑ ปี นับจากวันที่กรมสรรพสามิตได้ตรวจรับมอบงานครบถ้วนตามสัญญาเป็นที่เรียบร้อยแล้ว และภายในกำหนดเวลาดังกล่าวหาก “ระบบงาน” เกิดความชำรุดบกพร่องหรือขัดข้องอันเนื่องมาจากการใช้งานตามปกติ ผู้ชนะการประกวดราคาจะต้องเริ่มทำการปรับปรุงแก้ไขภายใน ๑ วันนับแต่ได้รับแจ้งจากกรมสรรพสามิต และให้สามารถทำงานได้อย่างถูกต้องภายใน ๒ วันทำการ โดยไม่ทำให้ระบบหยุดชะงักหรือเกิดความเสียหายแก่ทางราชการ หากผู้ชนะการประกวดราคาไม่เริ่มดำเนินการแก้ไขข้อขัดข้องได้ภายในเวลาดังกล่าว ผู้ชนะการประกวดราคาจ้างด้วยวิธีการทางอิเล็กทรอนิกส์ต้องชำระค่าปรับตามค่าปรับ **ตามเอกสารหมายเลข ๔**

๔.๒ การบริการในช่วงรับประกัน ผู้ชนะการประกวดราคาจะต้องมีการสนับสนุนโดยมีรายละเอียด **ตามเอกสารหมายเลข ๔**

๕. ข้อกำหนดด้านบุคลากร

ผู้เสนอราคาจะต้องเสนอรายชื่อทีมงานเพื่อดำเนินโครงการฯ พร้อมสำเนาเอกสารใบแสดงผลการศึกษาหรือเอกสารหลักฐานการจบการศึกษา ซึ่งบุคลากรตามข้อ ๕.๑ - ๕.๘ ไม่ใช่บุคลากรทั้งหมดที่ใช้ในโครงการแต่เป็นบุคลากรหลักที่จะต้องทำงานตลอดระยะเวลาสัญญา โดยเมื่อเริ่มดำเนินโครงการ ผู้ชนะการประกวดราคาต้องเสนอบุคลากรตามตำแหน่งที่ปรากฏ **ตามเอกสารหมายเลข ๕** ข้อ ๕. (ตารางบุคลากรที่ต้องใช้ในโครงการ) เป็นอย่างน้อย ทั้งนี้ เพื่อให้เพียงพอต่อการดำเนินงานตามระยะเวลาส่งมอบงาน ดังนี้

๕.๑ ผู้จัดการโครงการ (Project Manager) จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาโท ที่เกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ด้านเทคโนโลยีสารสนเทศ เป็นระยะเวลาอย่างน้อย ๑๕ ปี
- มีประสบการณ์ด้านการบริหารโครงการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นระยะเวลาอย่างน้อย ๕ ปี
- ได้รับประกาศนียบัตรรวมกันอย่างน้อย ดังนี้
  - ประกาศนียบัตร CISSP
  - ประกาศนียบัตร CISM

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

- ประกาศนียบัตร COBIT Foundation
- ประกาศนียบัตร PMP หรือ CompTIA Project+
- ประกาศนียบัตรรับรองผ่านการอบรม DPO เช่น CEPAS หรือ PECB เป็นต้น

๕.๒ ที่ปรึกษาด้านการวางแผนการรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวน ๒ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาโทที่เกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ด้านเทคโนโลยีสารสนเทศ เป็นระยะเวลาอย่างน้อย ๑๐ ปี
- มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑ หรือการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นระยะเวลาอย่างน้อย ๕ ปี
- ได้รับประกาศนียบัตรสากลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ อย่างน้อย ๒ ประกาศนียบัตร เช่น CISSP หรือ CISA หรือ ISO/IEC ๒๗๐๐๑ Lead Implementor หรือ ISMS Lead Auditor หรือ ISMS Transition to ISO/IEC ๒๗๐๐๑ เป็นต้น

๕.๓ ที่ปรึกษาด้านการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอาวุโส จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาตรีเกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นระยะเวลาอย่างน้อย ๕ ปี
- มีประสบการณ์ด้านการทดสอบเจาะระบบ
- ได้รับประกาศนียบัตรสากลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ อย่างน้อย ๒ ประกาศนียบัตร เช่น CISSP หรือ OSCP หรือ GPEN หรือ CEH เป็นต้น

๕.๔ ที่ปรึกษาด้านการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาตรีเกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ด้านการทดสอบเจาะระบบ เป็นระยะเวลาอย่างน้อย ๒ ปี
- ได้รับประกาศนียบัตรด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ อย่างน้อย ๑ ประกาศนียบัตร เช่น OSCP หรือ GPEN หรือ CEH เป็นต้น

๕.๕ ที่ปรึกษาด้านการวางแผนการคุ้มครองข้อมูลส่วนบุคคล จำนวน ๒ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาตรีเกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือการคุ้มครองข้อมูลส่วนบุคคล เป็นระยะเวลาอย่างน้อย ๘ ปี
- มีประกาศนียบัตรที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (Personal Data Protection) เช่น CDPSE หรือ PECB ISO/IEC ๒๗๗๐๑ Lead Implementor หรือ IRCA ISMS Lead Auditor เป็นต้น

๕.๖ ที่ปรึกษาด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาโท ที่เกี่ยวข้องกับด้านนิติศาสตร์ หรือกฎหมาย
- มีประสบการณ์ทำงานด้านกฎหมายอย่างน้อย ๘ ปี และมีประสบการณ์การคุ้มครองข้อมูลส่วนบุคคลอย่างน้อย ๑ ปี

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

- มีประกาศนียบัตรที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) ของสถาบัน IAPP เช่น CIPP/E เป็นต้น
- มีประกาศนียบัตรรับรองการผ่านการอบรมหลักสูตร Data Protection Officer ของหน่วยงานในต่างประเทศ เช่น CEPAS หรือ PECB เป็นต้น
- มีประกาศนียบัตรรับรองความรู้ความสามารถเกี่ยวกับมาตรฐาน ISO/IEC ๒๗๐๐๑ หรือ ISO/IEC ๒๗๗๐๑ ที่ออกโดย Certification Body (CB)

๕.๗ ที่ปรึกษาด้านการคุ้มครองข้อมูลส่วนบุคคล จำนวน ๒ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาตรี ที่เกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หรือนิติศาสตร์ หรือกฎหมาย
- มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือการคุ้มครองข้อมูลส่วนบุคคล เป็นระยะเวลาอย่างน้อย ๑ ปี

๕.๘ เจ้าหน้าที่ตอบคำถามให้ความช่วยเหลือ และประสานงานโครงการ (Help Desk) จำนวน ๑ คน

- มีวุฒิการศึกษาขั้นต่ำปริญญาตรี ที่เกี่ยวข้องกับให้ด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ
- โดยมีประสบการณ์ด้านสารสนเทศ หรือการคุ้มครองข้อมูลส่วนบุคคล เป็นระยะเวลาอย่างน้อย ๑ ปี

หมายเหตุ : ตำแหน่งที่เกี่ยวข้องกับด้านคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศ หมายถึง สาขาหนึ่งสาขาใดหรือเทียบเท่าวิศวกรรมคอมพิวเตอร์ วิศวกรรมไฟฟ้า วิศวกรรมอิเล็กทรอนิกส์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติ สถิติประยุกต์ คณิตศาสตร์ คณิตศาสตร์ประยุกต์ คอมพิวเตอร์ธุรกิจ บริหารธุรกิจ และครุศาสตร์อุตสาหกรรม

๖. <u>เงื่อนไขการติดตั้ง ส่งมอบ และการตรวจรับงาน</u>

๖.๑ ผู้ชนะการประกวดราคาต้องติดตั้งและส่งมอบ “ระบบงานและเอกสารขั้นตอนกระบวนงาน” ณ สถานที่ที่กรมสรรพสามิตกำหนด ทั้งนี้อาจมีการเปลี่ยนแปลงได้ตามที่กรมสรรพสามิตเห็นสมควร

๖.๒ กำหนดส่งมอบ “ระบบงานและเอกสารขั้นตอนกระบวนงาน” ตามขอบเขตในสัญญานี้ทั้งหมด ภายใน ๓๖๐ วัน นับถัดจากวันลงนามในสัญญา ณ หน่วยงานตามที่กรมสรรพสามิตกำหนด

๖.๓ ผู้ชนะการประกวดราคาต้องส่งมอบคู่มือการใช้งาน (User Manual) และคู่มือปฏิบัติงาน (Operation Manual) “ระบบงานและเอกสารขั้นตอนกระบวนงาน” โดยเป็นเอกสาร อย่างละ ๓ ชุด พร้อมไฟล์ข้อมูลเอกสารดังกล่าวบรรจุใน Flash Drive บรรจุรายละเอียดตามเอกสาร จำนวน ๓ ชุด

๖.๔ ผู้ชนะการประกวดราคาต้องส่งมอบ “ระบบงานและเอกสารขั้นตอนกระบวนงาน” ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

๖.๕ กรณีที่มีการเปลี่ยนแปลง แก้ไขขอบเขตการดำเนินงาน ผู้ชนะการประกวดราคาต้องดำเนินการปรับปรุงเอกสารที่ส่งมอบในโครงการ ให้สอดคล้องกับขอบเขตการดำเนินงาน โดยให้ส่งมอบก่อนสิ้นระยะเวลารับประกัน โดยเป็นเอกสาร อย่างละ ๓ ชุด พร้อมไฟล์ข้อมูลเอกสารดังกล่าวบรรจุใน Flash Drive จำนวน ๓ ชุด

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

หมายเหตุ : กรมสรรพสามิตสงวนสิทธิ์ที่จะให้ผู้ชนะการประกวดราคาจัดทำเอกสารเพิ่มเติม ในกรณีที่กรมสรรพสามิตเห็นว่าเอกสารที่มีไม่เพียงพอต่อการใช้งานภายในระยะเวลารับประกัน

๗. <u>หลักเกณฑ์และสิทธิในการพิจารณา</u>

๗.๑ ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ กรมสรรพสามิตจะพิจารณาตัดสินจากผู้ที่ผ่านการพิจารณาข้อเสนอด้านเอกสาร

๗.๒ ในขั้นตอนถัดไป กรมสรรพสามิตทำการทดสอบด้านเทคนิค POC โดยให้เฉพาะผู้ที่ผ่านการพิจารณาข้อเสนอด้านเอกสารยื่นข้อเสนอราคา เข้าร่วมในการทดสอบ POC

๗.๓ ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์หลังจากผ่านการพิจารณาข้อเสนอด้านเอกสารยื่นข้อเสนอราคา และผ่านการทดสอบ POC กรมสรรพสามิตจะพิจารณาตัดสินโดยใช้หลักเกณฑ์การเสนอราคาต่ำสุด เป็นผู้ชนะการเสนอราคา

๗.๔ หากผู้ยื่นข้อเสนอรายใดมีคุณสมบัติไม่ถูกต้องหรือยื่นหลักฐานการยื่นข้อเสนอไม่ถูกต้อง หรือไม่ครบถ้วน หรือยื่นข้อเสนอไม่ถูกต้อง คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์จะไม่รับพิจารณาข้อเสนอของผู้ยื่นเสนอรายนั้น เว้นแต่ ผู้ยื่นข้อเสนอรายใดเสนอเอกสารทางเทคนิคหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะจ้างไม่ครบถ้วน หรือเสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่กรมสรรพสามิตกำหนดไว้ในประกาศและเอกสารประกวดราคาอิเล็กทรอนิกส์ในส่วนที่มิใช่สาระสำคัญและความแตกต่างนั้นไม่มีผลทำให้เกิดการได้เปรียบเสียเปรียบต่อผู้ยื่นข้อเสนอรายอื่น หรือเป็นการผิดพลาดเล็กน้อย คณะกรรมการฯ อาจพิจารณาผ่อนปรนการตัดสิทธิผู้ยื่นข้อเสนอรายนั้น ทั้งนี้ เฉพาะในกรณีที่คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ พิจารณาเห็นว่าจะเป็นประโยชน์ต่อราชการเป็นสำคัญเท่านั้น

๗.๕ กรมสรรพสามิตสงวนสิทธิ์ไม่พิจารณาข้อเสนอของผู้ยื่นข้อเสนอโดยไม่มีการผ่อนผัน ในกรณีดังต่อไปนี้

๗.๕.๑ ไม่ปรากฏชื่อผู้ยื่นข้อเสนอรายนั้นในบัญชีรายชื่อผู้รับเอกสารประกวดราคาอิเล็กทรอนิกส์ทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์ หรือบัญชีรายชื่อผู้ซื้อเอกสารประราคาอิเล็กทรอนิกส์ทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์ของกรมสรรพสามิต

๗.๕.๒ ไม่กรอกชื่อผู้ยื่นข้อเสนอในการเสนอราคาทางระบบจัดซื้อจัดจ้างด้วยอิเล็กทรอนิกส์

๗.๕.๓ เสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่กำหนดในเอกสารประกวดราคาอิเล็กทรอนิกส์ที่เป็นสาระสำคัญ หรือมีผลทำให้เกิดความได้เปรียบเสียเปรียบแก่ผู้ยื่นข้อเสนอรายอื่น

๗.๕.๔ ไม่ยื่นบัญชีรายการที่เสนอทั้งหมดทุกรายการ **ตามเอกสารหมายเลข ๒** โดยต้องระบุยี่ห้อ แบบ รุ่น แหล่งผลิต รวมถึงคุณลักษณะต่าง ๆ ของแต่ละรายการที่เสนอให้ชัดเจนและครบถ้วน

๗.๖ ในการตัดสินการประกวดราคาอิเล็กทรอนิกส์หรือในการทำสัญญา คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์หรือกรมสรรพสามิตมีสิทธิให้ผู้ยื่นข้อเสนอชี้แจงข้อเท็จจริงเพิ่มเติมได้

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

กรมสรรพสามิตมีสิทธิที่จะไม่รับข้อเสนอ ไม่รับราคา หรือไม่ทำสัญญา หากข้อเท็จจริงดังกล่าวไม่เหมาะสมหรือไม่ถูกต้อง

๗.๗ กรมสรรพสามิตทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดเลยก็ได้ และอาจพิจารณาเลือกจ้างในจำนวน หรือขนาด หรือเฉพาะรายการหนึ่งรายการใดหรืออาจจะยกเลิกการประกวดราคาอิเล็กทรอนิกส์โดยไม่พิจารณาจัดจ้างเลยก็ได้ สุดแต่จะพิจารณา ทั้งนี้เพื่อประโยชน์ของทางราชการเป็นสำคัญ และให้ถือว่าการตัดสินของกรมสรรพสามิตเป็นเด็ดขาด ผู้ยื่นข้อเสนอจะเรียกร้องค่าใช้จ่าย หรือค่าเสียหายใด ๆ มิได้ รวมทั้งกรมสรรพสามิตจะพิจารณายกเลิกการประกวดราคาอิเล็กทรอนิกส์และลงโทษผู้ยื่นข้อเสนอเป็นผู้ทิ้งงาน ไม่ว่าจะเป็นผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่เชื่อถือได้ว่าการยื่นข้อเสนอกระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ชื่อบุคคลธรรมดา หรือนิติบุคคลอื่นมายื่นข้อเสนอแทน เป็นต้น ในกรณีที่ผู้ยื่นข้อเสนอรายที่เสนอราคาต่ำสุด เสนอราคาต่ำมากจนคาดหมายได้ว่าไม่อาจดำเนินงานตามเอกสารประกวดราคาอิเล็กทรอนิกส์ได้ คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ หรือกรมสรรพสามิตจะให้ผู้ยื่นข้อเสนอนั้นชี้แจงและแสดงหลักฐานที่ทำให้เชื่อได้ว่าผู้ยื่นข้อเสนอสามารถดำเนินงานตามเอกสารประกวดราคาอิเล็กทรอนิกส์ให้เสร็จสมบูรณ์ หากคำชี้แจงไม่เป็นที่รับฟังได้กรมสรรพสามิตมีสิทธิที่จะไม่รับข้อเสนอหรือไม่รับราคาของผู้ยื่นข้อเสนอรายนั้น ทั้งนี้ผู้ยื่นข้อเสนอดังกล่าวไม่มีสิทธิเรียกร้องค่าใช้จ่ายหรือค่าเสียหายใด ๆ จากกรมสรรพสามิต

๗.๘ ก่อนลงนามในสัญญา กรมสรรพสามิตอาจประกาศยกเลิกการประกวดราคาอิเล็กทรอนิกส์ หากปรากฏว่ามีการกระทำที่เข้าลักษณะผู้ยื่นข้อเสนอที่ชนะการประกวดราคาหรือที่ได้รับการคัดเลือกมีผลประโยชน์ร่วมกัน หรือมีส่วนได้เสียกับผู้ยื่นข้อเสนอรายอื่น หรือขัดขวางการแข่งขันอย่างเป็นธรรม หรือสมยอมกันกับผู้ยื่นข้อเสนอรายอื่นหรือเจ้าหน้าที่ในการเสนอราคา หรือส่อว่ากระทำการทุจริตอื่นใดในการเสนอราคา

๘. <u>ข้อกำหนดด้านการจัดทำระบบงานและเอกสารขั้นตอนกระบวนงาน</u>

๘.๑ ผู้ชนะการเสนอราคาต้องทำการศึกษาและวิเคราะห์ระบบงานจากการสัมภาษณ์ สังเกตการณ์ เข้าร่วมประชุม และศึกษาจากกฎหมายและระเบียบต่าง ๆ ที่กำหนดไว้ และที่เกี่ยวข้องกับโครงการนี้ รวมไปถึงเอกสารอื่นที่คณะทำงานของกรมสรรพสามิตจะมอบให้เมื่อเริ่มดำเนินการโครงการ ซึ่งอาจเปลี่ยนแปลงได้ตามสถานการณ์ที่เป็นปัจจุบันในระหว่างการพัฒนาระบบตามความเหมาะสม

๘.๒ ผู้ชนะการเสนอราคาต้องจัดทำรายงานการประชุมการสำรวจความต้องการของผู้ใช้งาน

๘.๓ ผู้ชนะการเสนอราคาต้องใช้วิธีการจัดทำระบบงานและเอกสารขั้นตอนกระบวนงานตามมาตรฐานสากล ในการพัฒนาระบบงาน

๘.๔ ผู้ชนะการเสนอราคาต้องออกแบบวิธีการจัดทำระบบงานและเอกสารขั้นตอนกระบวนงาน โดยคำนึงถึงมาตรฐานการรักษาความปลอดภัยของระบบและข้อมูลเป็นสำคัญ เพื่อให้ระบบงานและเอกสารขั้นตอนกระบวนงานมีความมั่นคงปลอดภัยและสามารถป้องกันการโจมตีจากผู้ไม่ประสงค์ดีได้

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๑๑.๒ ผู้ชนะการประกวดราคาต้องจัดหาและให้บริการ Help Desk ในการให้บริการถาม-ตอบทางโทรศัพท์และผ่านทางช่องทางอื่น ๆ ที่มีบริการ จำนวน ๑ คน ณ กรมสรรพสามิต กรณีที่กรมสรรพสามิตไม่มีสถานที่เพียงพอ ผู้ชนะการประกวดราคามีหน้าที่รับผิดชอบในการจัดหาสถานที่ตลอดระยะเวลาการบำรุงรักษาระบบเป็นระยะเวลา ๑ ปี โดยกรมสรรพสามิตเป็นผู้จัดหาสถานที่ดำเนินการ และสายสัญญาณโทรศัพท์เพื่อใช้ในการให้บริการ กรณีที่กรมสรรพสามิตไม่มีสถานที่เพียงพอ ผู้ชนะการประกวดราคามีหน้าที่รับผิดชอบในการจัดหาสถานที่

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

เอกสารหมายเลข ๒
คุณลักษณะเฉพาะของโครงการ

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

คุณลักษณะเฉพาะของโครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อการให้บริการผู้เสียภาษีสรรพสามิต

การวางแผนการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศฯของกรมสรรพสามิต ผู้เสนอราคาต้องวางแผนจัดทำระบบงานและขั้นตอนกระบวนงานเพื่อให้กรมสรรพสามิต ได้รับประโยชน์สูงสุด และสามารถนำไปใช้ในการสนับสนุนภารกิจของกรมสรรพสามิตในด้านต่างๆ กับระบบงานทุกระบบของกรมสรรพสามิต และการเพิ่มประสิทธิภาพในการจัดเก็บภาษี เพื่อการสนับสนุน นโยบายการเพิ่มผลการจัดเก็บภาษีอย่างถูกต้องและเป็นธรรม รวมทั้งการใช้ข้อมูลประกอบการ วางแผน และการตัดสินใจของผู้บริหารได้อย่างมีประสิทธิภาพ ซึ่งในโครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อการให้บริการผู้เสียภาษีสรรพสามิต มีปัจจัยต่าง ๆ ที่ต้องคำนึงถึง ดังนี้

๑. มีประสิทธิภาพสามารถใช้ปฏิบัติงานได้จริง
๒. มีลักษณะการทำงานที่ไม่ซ้ำซ้อน
๓. อำนวยความสะดวกให้แก่เจ้าหน้าที่และผู้มารับบริการได้
๔. จะต้องมีระบบการรักษาความมั่นคงปลอดภัยของข้อมูล

๑. เงื่อนไขทั่วไป

การประกวดราคาครั้งนี้ เป็นการประกวดราคาจ้าง “โครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อการให้บริการผู้เสียภาษีสรรพสามิต”

๑.๑ คุณลักษณะเฉพาะของ “โครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อการให้บริการผู้เสียภาษีสรรพสามิต” จะต้องเหมาะสมกับลักษณะงานของกรมสรรพสามิตที่จะดำเนินการตามโครงการนี้ และมีการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศที่มีประสิทธิภาพ มีหลักธรรมาภิบาล และเป็นตามข้อกำหนดของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และมาตรฐานสากล ISO/IEC ๒๗๐๐๑

๑.๒ คุณสมบัติของการจัดทำมาตรฐานตามข้อกำหนดของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และมาตรฐานสากล ISO/IEC ๒๗๐๐๑ และรายละเอียดข้อมูลขั้นตอนการดำเนินงานที่กำหนดไว้ตาม**เอกสารหมายเลข ๒** เป็นข้อมูลเบื้องต้น โดยคู่สัญญาต้องมีการจัดเก็บความต้องการของระบบในรายละเอียดอีกครั้ง

๑.๓ ระบบงาน และโปรแกรมที่เสนอต้องไม่เป็นผลิตภัณฑ์ของบริษัทผู้ผลิต ที่อยู่ในระหว่างการคุ้มครองการเป็นบุคคลหรือนิติบุคคลผู้ล้มละลายตามคำสั่งของศาล ที่ได้สั่งการตามกฎหมายของประเทศที่บริษัทของผู้ผลิตนั้นตั้งอยู่ และอยู่ในสายการผลิต และมีคุณลักษณะเฉพาะตรงตามที่กำหนดไว้

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๑.๔ ข้อกำหนดทั่วไปของการจัดทำมาตรฐานตามข้อกำหนดของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และมาตรฐานสากล ISO/IEC ๒๗๐๐๑ ต้องเป็นการจัดทำมาตรฐานตามข้อกำหนดของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และมาตรฐานสากล ISO/IEC ๒๗๐๐๑ ที่ครบถ้วนสมบูรณ์แบบในตัว เพื่อให้กรมสรรพสามิตมีการดำเนินการตามข้อกำหนดของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และผ่านการรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑

๑.๕ “โครงการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลด้านเทคโนโลยีสารสนเทศ เพื่อการให้บริการผู้เสียภาษีสรรพสามิต” โดยกรมสรรพสามิตจะมีการทดสอบความสามารถของผู้ยื่นข้อเสนอราคาด้านเทคนิค POC: Proof of Concept ผู้ยื่นข้อเสนอราคาต้องมีความพร้อมในการดำเนินการทำ POC

๒. รูปแบบรายการ หรือคุณสมบัติเฉพาะของโครงการ

๒.๑ จัดทำแผนการดำเนินงาน (Project Plan) และรายละเอียดในการดำเนินงานซึ่งต้องระบุกิจกรรม ระยะเวลา และผู้รับผิดชอบจำนวน ๑ งาน โดยมีรายละเอียดคุณลักษณะอย่างน้อย ดังนี้

จัดทำแผนการดำเนินงาน (Project Plan) ให้กรมสรรพสามิตพิจารณาเห็นชอบ ซึ่งประกอบด้วย

๒.๑.๑ ขอบเขตการดำเนินงานโครงการ

๒.๑.๒ วิธีการดำเนินงานโครงการ

๒.๑.๓ การบริหารจัดการโครงการ

๒.๑.๔ แผนการดำเนินงานโครงการ และรายละเอียดในการดำเนินงานพร้อมระยะเวลาดำเนินงานในแต่ละกิจกรรม

๒.๑.๕ โครงสร้างการบริหารงานโครงการ รายชื่อผู้รับผิดชอบ สถานที่ติดต่อ หมายเลขโทรศัพท์

๒.๑.๖ รายละเอียดอื่น ๆ ตามที่กรมสรรพสามิตกำหนด

๒.๒ จัดทำแผนการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อปฏิบัติตามข้อกำหนดพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จำนวน ๑ งาน โดยมีรายละเอียดคุณลักษณะอย่างน้อย ดังนี้

๒.๒.๑ ดำเนินการพัฒนาระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อปฏิบัติตามข้อกำหนดพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ดังนี้

๒.๒.๒ ดำเนินการศึกษา และวิเคราะห์ช่องว่าง (GAP Analysis) สถานะในปัจจุบัน (As-IS) ด้านความมั่นคงปลอดภัยสารสนเทศ และเปรียบเทียบกับกรอบการปฏิบัติ (Framework) ในระดับสากลที่ได้รับความน่าเชื่อถือ เช่น NIST Cybersecurity Framework เป็นต้น หรือประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

ประกาศตามข้อกำหนดของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยจะมีขอบเขตการดำเนินงาน ดังนี้

๒.๒.๒.๑ ดำเนินการศึกษาการในภาพรวมของการดำเนินธุรกิจของหน่วยงาน หรือการให้บริการระบบเทคโนโลยีสารสนเทศ เพื่อระบุระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง

๒.๒.๒.๒ ดำเนินการรวบรวมข้อมูลที่เกี่ยวข้องเพื่อดำเนินการทำ GAP & Risk Assessment โดยมีขอบเขตการรวบรวมอย่างน้อย ดังนี้

๑) ดำเนินการสัมภาษณ์บุคลากรที่เกี่ยวข้อง

๒) ดำเนินการตรวจสอบจากเอกสารรายงานที่เกี่ยวข้อง

๓) ดำเนินการตรวจสอบขั้นตอนการปฏิบัติในด้านการตอบสนองต่ออุบัติการณ์ และเอกสารประกอบอื่น ๆ

๒.๒.๒.๓ ดำเนินการทดสอบการโจมตีระบบเทคโนโลยีสารสนเทศผ่านช่องทางระบบเครือข่ายอินเทอร์เน็ตในรูปแบบ Black-box จำนวน ๑ ครั้ง จำนวน ๕ URLs หรือ IP Addresses เพื่อตรวจสอบหาช่องโหว่ที่อาจจะส่งผลกระทบต่อให้บริการแบบ online ของกรมสรรพสามิต

๒.๒.๒.๔ ดำเนินการศึกษา และวิเคราะห์สถานะภาพของการตรวจสอบความพร้อมในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร (GAP Assessment) เปรียบเทียบกับข้อกำหนดของกรอบปฏิบัติที่ได้รับการยอมรับในระดับสากล NIST Cybersecurity Framework โดยครอบคลุมหัวข้อ ดังนี้

๑) การระบุความเสี่ยง (Identify)

๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๒.๒.๒.๕ ดำเนินการประเมินความเสี่ยง (Risk Assessment) ที่จะส่งผลกระทบต่อการดำเนินงานของระบบเทคโนโลยีสารสนเทศ ซึ่งการประเมินความเสี่ยงจะประเมินในรูปแบบของ Scenario base approach ตามวิธีการประเมินความเสี่ยง ที่ออกแบบตามหลักของมาตรฐานสากล

๒.๒.๒.๖ ดำเนินการสรุปผลการวิเคราะห์ และข้อเสนอแนะเพื่อการเตรียมพร้อมในการตอบสนองภัยคุกคามด้านไซเบอร์ ทั้งในด้านของบุคลากร (People) กระบวนการบริหารจัดการ (Process) และระบบเทคโนโลยีที่ใช้ในการป้องกันและตรวจจับภัยคุกคามด้านไซเบอร์ (Technology)

๒.๓ จัดทำแผนพัฒนาหรือปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑ โดยครอบคลุมขอบเขตของโครงสร้างพื้นฐานระบบเทคโนโลยีสารสนเทศของศูนย์คอมพิวเตอร์ (Data Center) หลัก ห้องปฏิบัติการระบบเครือข่าย (Network Operation Center: NOC) ห้องปฏิบัติการความมั่นคงปลอดภัยสารสนเทศ

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

(Security Operation Center: SOC) และศูนย์คอมพิวเตอร์สำรอง (DR Site) พร้อมกับตรวจสอบเพื่อให้ได้รับการรับรองมาตราฐาน ISO/IEC ๒๗๐๐๑ จำนวน ๑ งาน โดยมีรายละเอียดคุณลักษณะอย่างน้อย ดังนี้

๒.๓.๑ ดำเนินการร่วมกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศของกรมสรรพสามิต กำหนดขอบเขต (Scope of Work) และวางแผนการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑ และสำหรับโครงสร้างพื้นฐานระบบเทคโนโลยีสารสนเทศของศูนย์คอมพิวเตอร์ (Data Center) หลักห้องปฏิบัติการระบบเครือข่าย (Network Operation Center: NOC) ห้องปฏิบัติการความมั่นคงปลอดภัยสารสนเทศ (Security Operation Center: SOC) และศูนย์คอมพิวเตอร์สำรอง (DR Site)

๒.๓.๒ ดำเนินการร่วมกับคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ในการปรับปรุงนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy)

๒.๓.๓ ดำเนินการร่วมกับคณะทำงานในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ในการปรับปรุงขั้นตอนการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ (Risk Assessment Methodology) ให้สอดคล้องตามมาตรฐาน ISO/IEC ๒๗๐๐๑ โดยเนื้อหาต้องครอบคลุม

๒.๓.๓.๑ เกณฑ์การยอมรับความเสี่ยง

๒.๓.๓.๒ การสร้างผลลัพธ์ที่สามารถเปรียบเทียบได้ และดำเนินการซ้ำได้

๒.๓.๓.๓ การระบุความเสี่ยงที่เกี่ยวข้องกับการสูญเสียความลับ ความถูกต้องสมบูรณ์และความพร้อมใช้

๒.๓.๓.๔ การระบุเจ้าของความเสี่ยง

๒.๓.๓.๕ การวิเคราะห์ผลกระทบ และประเมินโอกาสเกิด

๒.๓.๓.๖ การประมาณระดับความเสี่ยง

๒.๓.๔ จัดหาซอฟต์แวร์ Risk Assessment สำหรับสนับสนุนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่มีความสอดคล้องกับขั้นตอนการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ (Risk Assessment Methodology) โดยสามารถรองรับการทำงานได้อย่างน้อยดังนี้

๒.๓.๔.๑ มีความสามารถในจัดเก็บทรัพย์สินในขอบเขตการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศได้

๒.๓.๔.๒ มีความสามารถในการระบุรายละเอียดของทรัพย์สินและเจ้าของทรัพย์สินในระบบได้

๒.๓.๔.๓ มีความสามารถกำหนดรอบการประเมินความเสี่ยง และนำข้อมูลรายละเอียดของรอบการประเมินความเสี่ยงออกจากระบบในรูปแบบไฟล์ Excel หรือ CSV

๒.๓.๔.๔ มีความสามารถกำหนดเกณฑ์การประเมินผลกระทบ และรายละเอียดระดับของเกณฑ์ดังกล่าวในแต่ละรอบการประเมินความเสี่ยงได้ เช่น ด้านการเงิน ด้านการปฏิบัติการ ด้านชื่อเสียง ด้านกฎหมาย

๒.๓.๔.๕ มีความสามารถกำหนดระดับผลกระทบและ

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๒.๓.๔.๖ โอกาสเกิดขึ้นได้ในแต่ละรอบประเมินความเสี่ยงได้ เช่น ระดับสูง ระดับปานกลาง ระดับต่ำ

๒.๓.๔.๗ มีความสามารถในการระบุความเสี่ยงที่เกี่ยวข้องกับการสูญเสียความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้

๒.๓.๔.๘ มีความสามารถในการประเมินความเสี่ยง โดยระบุรายละเอียด เช่น ความเสี่ยงสืบเนื่อง (Inherit Risk) ความเสี่ยงคงเหลือ (Residual) ผลกระทบ โอกาสเกิด และเจ้าของความเสี่ยง

๒.๓.๔.๙ มีความสามารถกำหนดแผนการจัดการความเสี่ยง โดยระบุรายละเอียด เช่น มาตรการควบคุมตามมาตรฐาน ISO/IEC ๒๗๐๐๑, แผนการปฏิบัติ, ความคืบหน้าเป็นเปอร์เซ็นต์ความสำเร็จของแผนการปฏิบัติ เป็นอย่างน้อย และนำข้อมูลดังกล่าวออกจากระบบในรูปแบบไฟล์ Excel หรือ CSV ได้

๒.๓.๔.๑๐ มีความสามารถรายงานสรุปการประเมินความเสี่ยง และสถานะการตอบสนองความเสี่ยงในลักษณะแผนภาพ (Dashboard) เช่น Heatmap, Pie graph เป็นอย่างน้อย

๒.๓.๔.๑๑ ดำเนินการดูแลปรับปรุงและแก้ไขปัญหาของเครื่องมือตลอดระยะเวลาของสัญญา

๒.๓.๕ จัดหาซอฟต์แวร์การตรวจสอบช่องโหว่ระบบเทคโนโลยีสารสนเทศ (Vulnerability Assessment) โดยมีคุณสมบัติอย่างน้อย ดังนี้

๒.๓.๕.๑ เป็นซอฟต์แวร์ที่ออกแบบมาเพื่อทำหน้าที่ตรวจสอบช่องโหว่ (Vulnerability Assessment) และการตั้งค่าความปลอดภัยตามมาตรฐาน Compliance โดยเฉพาะ

๒.๓.๕.๒ สามารถตรวจสอบช่องโหว่ของอุปกรณ์ปลายทาง ได้แก่

๒.๓.๕.๒.๑ อุปกรณ์ Network เช่น Firewall, Router, Switch, Printer, Storage เป็นอย่างน้อย

๒.๓.๕.๒.๒ ระบบ Virtualization เช่น VMware ESX, ESXi, vSphere, vCenter เป็นอย่างน้อย

๒.๓.๕.๒.๓ ระบบปฏิบัติการ (Operating System) เช่น Windows, OS X, Linux, Solaris เป็นอย่างน้อย

๒.๓.๕.๒.๔ ระบบฐานข้อมูล (Database) เช่น Oracle, SQL Server, MySQL, DB๒, Informix, PostgreSQL, MongoDB เป็นอย่างน้อย

๒.๓.๕.๓ ฐานข้อมูลในการตรวจสอบช่องโหว่ตามมาตรฐาน CVE (Common Vulnerabilities and Exposures)

๒.๓.๕.๔ สามารถตรวจสอบการตั้งค่าความปลอดภัยตามมาตรฐานสากลต่าง ๆ เช่น CIS เป็นต้น

๒.๓.๕.๕ สามารถตรวจสอบช่องโหว่ภายในระบบเครือข่ายผ่าน IPV๔ และ IPV๖

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๒.๓.๕.๖ สามารถตรวจสอบช่องโหว่ของระบบปลายทางได้แบบ Credentialed Scanning เพื่อตรวจหาการตั้งค่าความปลอดภัยของระบบ (system hardening) และ Patches ที่ไม่ได้ติดตั้ง

๒.๓.๕.๗ สามารถตั้งเวลาในการตรวจสอบช่องโหว่ (Schedule scan) ได้ตามระยะเวลาที่กำหนด

๒.๓.๕.๘ สามารถสร้างรายงานในรูปแบบของ PDF และ CSV ได้เป็นอย่างน้อย

๒.๓.๖ ดำเนินการตรวจสอบช่องโหว่ (Vulnerability Assessment) ในระดับระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์เครือข่าย (Network Equipment) อุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Device) จำนวน ๕๐ หมายเลขไอพี (IP Address) จำนวน ๑ ครั้ง พร้อมจัดทำรายงานการการตรวจสอบและวิเคราะห์ความเสี่ยงของช่องโหว่

๒.๓.๗ ดำเนินการให้คำปรึกษาและร่วมกับคณะทำงานในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ในการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ ตามขั้นตอนการประเมินความเสี่ยงฯ ที่กำหนด โดยการประเมินความเสี่ยงฯ ต้องมีบริบทครอบคลุมขอบเขตที่ขอรับรองมาตรฐานตามที่กำหนด

๒.๓.๘ ดำเนินการร่วมกับคณะทำงานในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ในการทบทวน หรือปรับปรุงเอกสาร เช่น นโยบาย (Policy) ขั้นตอนการปฏิบัติ (Procedure) เป็นต้น ที่ต้องถูกพัฒนาตามแผนการลดความเสี่ยง โดยจะต้องครอบคลุมรายละเอียดอย่างน้อย ดังนี้

๒.๓.๘.๑ นโยบายการใช้งานอุปกรณ์พกพา

๒.๓.๘.๒ นโยบายการปฏิบัติงานจากภายนอกหน่วยงาน

๒.๓.๘.๓ นโยบายการควบคุมการเข้าถึงข้อมูล

๒.๓.๘.๔ นโยบายการเข้ารหัสข้อมูล

๒.๓.๘.๕ นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และนโยบายการป้องกันหน้าจอคอมพิวเตอร์

๒.๓.๘.๖ นโยบายการสำรองข้อมูล

๒.๓.๘.๗ นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย

๒.๓.๘.๘ นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก

๒.๓.๘.๙ ขั้นตอนการปฏิบัติการระบุป้ายชื่อสารสนเทศ (Labeling of information)

๒.๓.๘.๑๐ ขั้นตอนการปฏิบัติการจัดการกับทรัพย์สิน (Handling of assets)

๒.๓.๘.๑๑ ขั้นตอนการปฏิบัติการจัดการกับสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ (Management of removable media)

๒.๓.๘.๑๒ ขั้นตอนการปฏิบัติการทำลายสื่อบันทึกข้อมูล (Disposal of media)

๒.๓.๘.๑๓ ขั้นตอนการปฏิบัติการควบคุมการเข้าสู่ระบบอย่างปลอดภัย (Secure log-on procedure)

๒.๓.๘.๑๔ ขั้นตอนการปฏิบัติการปฏิบัติงานในพื้นที่ที่ต้องการความปลอดภัย (Working in secure areas)

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๒.๓.๘.๑๕ ขั้นตอนการปฏิบัติงานรายวันที่เกี่ยวข้องกับระบบ (Documented operating procedures)

๒.๓.๘.๑๖ ขั้นตอนการปฏิบัติการควบคุมการติดตั้งซอฟต์แวร์ (Installation of software on operational systems)

๒.๓.๘.๑๗ ขั้นตอนการปฏิบัติการแลกเปลี่ยนข้อมูล (Information transfer policies and procedures)

๒.๓.๘.๑๘ ขั้นตอนการปฏิบัติการควบคุมการเปลี่ยนแปลงระบบ (System change control procedures)

๒.๓.๘.๑๙ ขั้นตอนการปฏิบัติการจัดการกับอุบัติการณ์ (Incident management)

๒.๓.๘.๒๐ ขั้นตอนการปฏิบัติการควบคุมทรัพย์สินทางปัญญา (Intellectual property rights)

๒.๓.๙ ดำเนินการการระบุรายการมาตรการควบคุมที่เลือกใช้งาน และจัดเตรียมเอกสาร Statement Of Applicability (SOA) ตาม Annex A ของมาตรฐานสากล ISO/IEC ๒๗๐๐๑

๒.๓.๑๐ ดำเนินการให้คำปรึกษาในการจัดทำการวัดประสิทธิผลมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ (Effectiveness Measurement) โดยให้ดัชนีชี้วัดมีประสิทธิผลสอดคล้องกับข้อกำหนดของมาตรฐาน

๒.๓.๑๑ ดำเนินการให้คำปรึกษาและร่วมกับคณะผู้ตรวจสอบภายใน ดำเนินการตรวจสอบภายในเพื่อแนะนำและถ่ายถอดหลักการตรวจสอบภายใน โดยการดำเนินการต้องสอดคล้องตามมาตรฐาน ISO/IEC ๒๗๐๐๑

๒.๓.๑๒ ดำเนินการร่วมกับคณะทำงานในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อติดตามการแก้ไขข้อบกพร่องที่ตรวจพบในการดำเนินการตรวจสอบภายในโดยอ้างอิงจากรายงานตรวจสอบภายในเป็นหลัก

๒.๓.๑๓ ดำเนินการประชุมร่วมกับคณะทำงานในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อสรุปผลการดำเนินงานของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ให้แก่คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Review)

๒.๓.๑๔ ดำเนินการให้คำปรึกษาการคัดเลือกผู้ตรวจรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑ (Certification Body) ที่มีชื่อเสียงและเป็นที่ยอมรับในระดับสากล เพื่อดำเนินการตรวจรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑ ตามขอบเขตที่กำหนด พร้อมรับผิดชอบค่าใช้จ่ายในการตรวจสอบขอใบรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑ ของผู้ตรวจสอบที่ศูนย์เทคโนโลยีสารสนเทศของกรมสรรพสามิตเป็นผู้คัดเลือก และรับผิดชอบค่าจ้างผู้ตรวจสอบตรวจสอบใบรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑ เป็นจำนวน ๓ ครั้ง

๒.๓.๑๕ ดำเนินการให้คำปรึกษาและร่วมกับคณะทำงานในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ในการจัดเตรียมความพร้อมด้านเอกสาร สำหรับให้ผู้ตรวจรับรองมาตรฐานมาดำเนินการตรวจสอบ และต้องเข้าร่วมสนับสนุนการตรวจสอบเพื่อขอรับรองมาตรฐาน เพื่อให้การสนับสนุนการหาหลักฐาน เอกสาร และแนะนำจนกว่าศูนย์เทคโนโลยีสารสนเทศของกรมสรรพสามิตจะผ่านการตรวจสอบขอใบรับรองมาตรฐาน

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

ISO/IEC ๒๗๐๐๑ หรือได้รับเอกสารยืนยันใด ๆ ที่แสดงหรือบ่งชี้ว่าสำนักงานศูนย์เทคโนโลยีสารสนเทศของกรมสรรพสามิตผ่านการรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑

๒.๔ จัดทำแผนพัฒนาและแผนการปรับปรุงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อปฏิบัติตามข้อกำหนดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ จำนวน ๑ งาน โดยมีรายละเอียดคุณลักษณะอย่างน้อย ดังนี้

๒.๔.๑ ดำเนินการศึกษาและรวบรวมกิจกรรมการประมวลผลข้อมูล (Processing Activities) ซึ่งรวมถึง ประเภทข้อมูล ขั้นตอนในการเก็บ รวบรวม ใช้ หรือเปิดเผย และการเคลื่อนที่ของข้อมูลส่วนบุคคล (Data Flow) โดยการจัดส่งแบบสอบถาม (Questionnaire) หรือดำเนินการนัดหมายเข้าสัมภาษณ์เพื่อเก็บรวบรวมข้อมูล กับเจ้าหน้าที่ที่เกี่ยวข้อง ซึ่งเป็นผู้มีส่วนได้ส่วนเสียเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Privacy Stakeholder) เพื่อได้มาซึ่งข้อมูลที่ถูกต้องและครบถ้วน และสามารถกำหนดขอบเขตการจัดเก็บข้อมูล Data Inventory และการไหลของข้อมูล Data Flow ทั้งหมด ที่เกี่ยวข้องกับกระบวนการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้อง และให้เป็นไปตามที่พระราชบัญญัติทั้งสองฉบับกำหนด และกฎเกณฑ์อื่น ๆ ที่เกี่ยวข้อง

๒.๔.๒ ดำเนินการวิเคราะห์ช่องว่าง (GAP) ในการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยการวิเคราะห์สถานะภาพการปฏิบัติงานตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยสารสนเทศ (As Is) โดยเปรียบเทียบกับข้อกำหนดในกฎหมาย มาตรฐานสากล หรือแนวปฏิบัติรักษาความมั่นคงปลอดภัยสากล เพื่อนำผลการศึกษาเปรียบเทียบ และจัดทำสรุปผลการวิเคราะห์และเปรียบเทียบความแตกต่าง (Gap Assessment) และเสนอแนะแนวทางในการปรับปรุงทั้งด้านบุคลากร กระบวนการปฏิบัติงาน และเทคโนโลยี

๒.๔.๓ ดำเนินการจัดทำคำแนะนำทางกฎหมายสำหรับเป็นนโยบายหลักเกณฑ์ระเบียบและแนววิธีปฏิบัติงานต่าง ๆ ที่ชัดเจน ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล โดยอย่างน้อยประกอบด้วย

๒.๔.๓.๑ แนวปฏิบัติและข้อแนะนำเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล

๒.๔.๓.๒ แนวปฏิบัติเกี่ยวกับการจำแนกประเภทของข้อมูลส่วนบุคคล (Data Classification) ซึ่งรวมถึง ข้อมูลส่วนบุคคล (Personal Data) และข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Personal Data)

๒.๔.๓.๓ แนวปฏิบัติและข้อแนะนำเกี่ยวกับงานการจัดการคำร้องของเจ้าของข้อมูลส่วนบุคคล ซึ่งจะครอบคลุมตั้งแต่วิธีการหรือช่องทางในการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เงื่อนไขการอนุมัติหรือปฏิเสธการใช้สิทธินั้น โดยอย่างน้อยประกอบด้วย

๑) สิทธิในการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลของตนเอง

๒) สิทธิการขอให้เปิดเผยการได้มา

๓) สิทธิในการคัดค้านการเก็บรวบรวม ใช้ เปิดเผยข้อมูล ส่วนบุคคล

๔) สิทธิในการขอถอนการให้ความยินยอม

๕) สิทธิในการขอให้แก้ไข ลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๖) สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้

๗) สิทธิในการร้องเรียนต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๒.๔.๓.๔ ข้อแนะนำเกี่ยวกับระยะเวลาการจัดเก็บ วิธีทำลายและ/หรือลบทิ้งข้อมูลส่วนบุคคลที่เหมาะสม และแนวทางในการแจ้งผลการทำลาย และ/หรือ ลบทิ้งข้อมูลส่วนบุคคล

๒.๔.๔ ดำเนินการจัดทำเอกสารนโยบาย หรือขั้นตอนการปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริหารจัดการระบบเทคโนโลยีสารสนเทศ โดยอย่างน้อยจะต้องประกอบด้วย

๒.๔.๔.๑ นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

๒.๔.๔.๒ นโยบายในการจัดเก็บข้อมูลส่วนบุคคล (Data Retention Policy) และนโยบายในการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด (Personal Data Disposal Policy)

๒.๔.๔.๓ นโยบายหรือแนวปฏิบัติในการเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก หรือการส่ง หรือโอนข้อมูลส่วนบุคคลไปหน่วยงานในต่างประเทศ (Third Parties / Cross Border Data Transfer Policy)

๒.๔.๔.๔ นโยบายหรือแนวทางในการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Outsourcing Policy for Personal Data Processing)

๒.๔.๔.๕ ตัวอย่างแบบฟอร์ม หรือหนังสือการขอความยินยอม (Consent) จากเจ้าของข้อมูลส่วนบุคคล สำหรับการใช้งานบนเว็บไซต์หรือเว็บแอพพลิเคชั่น

๒.๔.๔.๖ ตัวอย่างเอกสาร หรือข้อกำหนด หรือข้อตกลง ของการเป็นผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

๒.๔.๔.๗ ขั้นตอนปฏิบัติในการบริหารจัดการ การละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Management)

๒.๔.๔.๘ บทบาทหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

๒.๕ ดำเนินการนำผลการศึกษา และวิเคราะห์ที่ได้มาพัฒนาแผนงาน/โครงการ/กิจกรรมหลัก ในการพัฒนาความมั่นคงปลอดภัยสารสนเทศ (IT Security Master Plan) ระยะ ๓ ปี จำนวน ๑ งาน โดยมีรายละเอียดคุณลักษณะอย่างน้อย ดังนี้

โดยนำผลที่ได้จากข้อที่ ๒.๑ – ๒.๔ มาพัฒนาแผนงาน/โครงการ/กิจกรรมหลัก ในการพัฒนาความมั่นคงปลอดภัยสารสนเทศ (IT Security Master Plan) ระยะ ๓ ปี โดยจะต้องมีเนื้อหาครอบคลุมดังนี้

๒.๕.๑ โครงการด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมรายละเอียดเบื้องต้น

๒.๕.๒ แผนงาน/โครงการ/กิจกรรมหลัก ในการพัฒนาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่ระบุถึง

๑) Impact – หมายถึง ระดับผลกระทบที่อาจเกิดขึ้น หากหน่วยงานไม่เร่งดำเนินการ เช่น ผลกระทบต่อภาพลักษณ์ การดำเนินงาน การเงิน และกฎหมายข้อบังคับ

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๒) Urgency – หมายถึง ระดับความเร่งด่วน เมื่อพิจารณาจากปัญหาและปัจจัยอื่น ๆ เช่น กฎหมายข้อบังคับ แนวโน้มของภัยคุกคาม

๒.๕.๓ แนวทางในการบริหารจัดการและติดตามประเมินผลแผนแม่บทความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๓. ข้อกำหนดทางเทคนิคของโครงการ

๓.๑ ข้อกำหนดทั่วไป

๓.๑.๑ ผู้รับจ้างต้องพัฒนาแผนการดำเนินงาน (Project Plan) ซึ่งต้องระบุกิจกรรม เวลา และผู้รับผิดชอบ ให้กรมสรรพสามิตพิจารณาเห็นชอบ ภายใน ๓๐ วันนับจากวันลงนามในสัญญา ซึ่งประกอบด้วย

(๑) ขอบเขตการดำเนินงานโครงการ

(๒) วิธีการดำเนินงานโครงการ

(๓) การบริหารจัดการโครงการ

(๔) แผนการดำเนินงานโครงการ และรายละเอียดในการดำเนินงานพร้อมระยะเวลาดำเนินงานในแต่ละกิจกรรม

(๕) โครงสร้างการบริหารงานโครงการ รายชื่อผู้รับผิดชอบ สถานที่ติดต่อ หมายเลขโทรศัพท์

(๖) รายละเอียดอื่น ๆ ตามที่กรมสรรพสามิตกำหนด

(๗) เอกสารรายละเอียดซอฟต์แวร์ที่ต้องใช้ในโครงการ

๓.๑.๒ ผู้รับจ้างต้องเสนอเอกสารประกอบแผนการดำเนินงานตามขอบเขตการดำเนินงานให้กรมสรรพสามิตพิจารณาเห็นชอบ ภายใน ๑๕๐ วันนับจากวันลงนามในสัญญา ซึ่งประกอบด้วย

(๑) ส่งมอบซอฟต์แวร์ Risk Assessment พร้อมติดตั้งระบบ Risk Assessment

(๒) ส่งมอบซอฟต์แวร์ Vulnerability Assessment พร้อมติดตั้งระบบ Vulnerability Assessment

(๓) ส่งมอบเอกสารดำเนินการทดสอบการโจมตีระบบเทคโนโลยีสารสนเทศผ่านช่องทางระบบเครือข่ายอินเทอร์เน็ตในรูปแบบ Black-box

(๔) ส่งมอบเอกสารรายงานสรุปผลการวิเคราะห์ และข้อเสนอแนะเพื่อการเตรียมพร้อมในการตอบสนองคุกคามด้านไซเบอร์ ทั้งในด้านของบุคลากร (People) กระบวนการบริหารจัดการ (Process) และระบบเทคโนโลยีที่ใช้ในการป้องกันและตรวจจับภัยคุกคามด้านไซเบอร์ (Technology)

(๕) ส่งมอบเอกสารนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy)

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

(๖) ส่งมอบเอกสารขั้นตอนการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ (Risk Assessment Methodology)

(๗) ส่งมอบเอกสารรายงานผลการตรวจสอบช่องโหว่ (Vulnerability Assessment)

(๘) ส่งมอบเอกสารรายงานผลการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ (Risk Assessment Report)

(๙) ส่งมอบเอกสารนโยบาย (Policy) หรือขั้นตอนการปฏิบัติ (Procedure) ของระบบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑

(๑๐) ส่งมอบเอกสารรายงานคำแนะนำทางกฎหมายสำหรับเป็นนโยบายหลักเกณฑ์ระเบียบและแนววิธีปฏิบัติงานต่าง ๆ ที่ชัดเจน ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

๓.๑.๓ ผู้รับจ้างต้องเสนอเอกสารประกอบแผนการดำเนินงานตามขอบเขตการดำเนินงานให้กรมสรรพสามิตพิจารณาเห็นชอบ ภายใน ๒๔๐ วันนับจากวันลงนามในสัญญา ซึ่งประกอบด้วย

(๑) ส่งมอบเอกสาร Statement Of Applicability (SOA)

(๒) ส่งมอบเอกสารการวัดประสิทธิผลมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ (Effectiveness Measurement)

(๓) ส่งมอบเอกสารประกอบการอบรม

(๔) ส่งมอบเอกสารรายงานผลการตรวจสอบภายใน

(๕) ส่งมอบเอกสารรายงานสรุปผลการดำเนินงานของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Review)

(๖) ส่งมอบเอกสารนโยบายหรือขั้นตอนการปฏิบัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการบริหารจัดการระบบเทคโนโลยีสารสนเทศ

(๗) ส่งมอบเอกสารแผนงาน/โครงการ/กิจกรรมหลัก ในการพัฒนาความมั่นคงปลอดภัยสารสนเทศ (IT Security Master Plan)

๓.๑.๔ ผู้รับจ้างต้องเสนอเอกสารประกอบแผนการดำเนินงานตามขอบเขตการดำเนินงานให้กรมสรรพสามิตพิจารณาเห็นชอบ ภายใน ๓๖๐ วันนับจากวันลงนามในสัญญา ซึ่งประกอบด้วย

(๑) ส่งมอบจดหมายยืนยัน (Attestation Letter) หรือใบประกาศนียบัตร (Certification) จาก Certification Body ที่แสดงหรือบ่งชี้ว่าสำนักงานศูนย์เทคโนโลยีสารสนเทศของกรมสรรพสามิต ผ่านการรับรองมาตรฐาน ISO/IEC ๒๗๐๐๑

(๒) ส่งมอบการฝึกอบรม คู่มือผู้ใช้งาน พร้อมส่งมอบเอกสารการฝึกอบรม

๓.๒ งานการติดตั้งซอฟต์แวร์ ปรับแต่ง และทดสอบการใช้งาน

๓.๒.๑ ผู้รับจ้างจะต้องมีบุคลากรที่มีคุณภาพ และมีความเชี่ยวชาญในการติดตั้งซอฟต์แวร์ โดยต้องเสนอรายชื่อบุคลากรพร้อมหลักฐานการศึกษาในกรมสรรพสามิตพิจารณาก่อนเข้าดำเนินการปฏิบัติงาน

๓.๒.๒ ก่อนที่ผู้รับจ้างจะเข้าดำเนินการติดตั้งซอฟต์แวร์ใดๆ ที่กรมสรรพสามิต ผู้รับจ้างจะต้องทำหนังสือแจ้งให้กรมสรรพสามิตรับทราบก่อนเข้าดำเนินการอย่างน้อย ๕ วันทำการ และจะต้องรอให้ได้รับการอนุมัติจึงจะสามารถดำเนินการติดตั้งซอฟต์แวร์ใด ๆ ได้ ซึ่งหากผู้รับจ้างเข้าทำการติดตั้งซอฟต์แวร์ใด ๆ โดยไม่ได้รับการอนุมัติ กรมสรรพสามิตมีสิทธิที่จะให้ผู้รับจ้างดำเนินการรื้อถอนซอฟต์แวร์ต่าง ๆ ที่ได้ติดตั้งไปแล้ว โดยถือเป็นความผิดและความรับผิดชอบของผู้รับจ้าง

๓.๒.๓ ผู้รับจ้างจะต้องทำแผนงานการติดตั้งซอฟต์แวร์ให้กรมสรรพสามิต เพื่อพิจารณาเห็นชอบก่อนการติดตั้ง

๓.๒.๔ ผู้รับจ้างจะต้องเป็นผู้ติดตั้งซอฟต์แวร์ตามที่เสนอ ตลอดจนจัดหาและติดตั้งวัสดุ สายไฟ อุปกรณ์ต่าง ๆ จนทำให้ระบบงานที่เสนอ สามารถใช้งานได้อย่างมีประสิทธิภาพ

๓.๒.๕ ผู้รับจ้างต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น เนื่องจากการติดตั้งซอฟต์แวร์ หรือความเสียหายใดที่เกิดขึ้นเนื่องจากการปฏิบัติงานของผู้รับจ้าง ผู้รับจ้างจะต้องดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพเดิมโดยเร็ว และยินยอมชดใช้ค่าเสียหายที่เกิดขึ้นให้กับกรมสรรพสามิต

๓.๓ ข้อกำหนดการติดตั้งและทดสอบซอฟต์แวร์

ผู้รับจ้างจะต้องเป็นผู้ติดตั้งและทดสอบซอฟต์แวร์ที่จัดหาในโครงการให้เป็นไปตามแผนงาน และข้อเสนอแนะจากกรมสรรพสามิต หากพบข้อผิดพลาดให้ทำการแก้ไข และทดสอบซ้ำจนแล้วเสร็จ โดยดำเนินการอย่างน้อย ดังนี้

(๑) จัดทำแผนการทดสอบระบบ

(๒) จัดทำเอกสารที่เกี่ยวกับขั้นตอนการทดสอบระบบงาน (Test Case)

(๓) จัดทำรายงานผลการทดสอบระบบ (Test Document)

(๔) ดำเนินการทดสอบการทำงานร่วมกัน (Integration Testing)

(๕) ดำเนินการทดสอบระบบโดยรวม (System Testing)

(๖) ดำเนินการทดสอบการยอมรับของผู้ใช้งาน (User Acceptance Test : UAT)

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

เอกสารหมายเลข ๓
การฝึกอบรมและการสนับสนุน

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

การฝึกอบรมและการสนับสนุน

๑. <u>การฝึกอบรม</u> มีรายละเอียดดังนี้

ลำดับ	หลักสูตร	จำนวนวัน/รุ่น (อย่างน้อย)	จำนวนคน/รุ่น (อย่างน้อย)	จำนวนรุ่น	จำนวนคนรวม
๑.	หลักสูตรมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ สำหรับคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) ของกรมสรรพสามิต	๑	๑๐	๑	๑๐
๒.	หลักสูตรมาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ สำหรับคณะทำงานในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Operation Team) ของกรมสรรพสามิต	๑	๑๐	๑	๑๐
๓.	หลักสูตรการสร้าง Awareness ในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	๑	๕๐	๑	๕๐
๔.	หลักสูตรการตรวจสอบภายใน ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Internal Audit) สำหรับคณะผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	๑	๑๐	๑	๑๐
๕.	หลักสูตรการเตรียมความพร้อมในการปฏิบัติตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	๑	๕๐	๑	๕๐

หมายเหตุ : จำนวนวันและจำนวนคนในการอบรมในแต่ละรุ่นอาจมีการเปลี่ยนแปลงตามที่กรมสรรพสามิตพิจารณาเห็นชอบ

๑.๑ ผู้ชนะการประกวดราคาต้องเสนอรายละเอียดการฝึกอบรมโดยระบุ ชื่อหลักสูตรวิชาและเนื้อหา จำนวน วัน เวลา ที่จะฝึกอบรม

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๑.๒ ก่อนการฝึกอบรม ผู้ชนะการประกวดราคาต้องเสนอรายละเอียดหลักสูตรการอบรมพร้อมประวัติผู้สอนให้กรมสรรพสามิตพิจารณาก่อนดำเนินการฝึกอบรม

๑.๓ การฝึกอบรมต้องประกอบไปด้วยการบรรยายในห้องเรียนและการปฏิบัติเพื่อให้ผู้เข้ารับการฝึกอบรมสามารถทดสอบความรู้และทำงานได้จริง

๑.๔ คู่มือและเอกสารทั้งหมดที่จัดทำให้กรมสรรพสามิต ต้องได้รับความเห็นชอบจากกรมสรรพสามิตในเรื่องเนื้อหาสาระ และรูปแบบการนำเสนอก่อนการฝึกอบรม

๑.๕ คู่มือการปฏิบัติงาน ขั้นตอนการดูแลรักษา และวิธีการตั้งค่าอุปกรณ์ จัดทำเป็นเอกสารรูปเล่มภาษาไทยที่อ่านเข้าใจง่าย และ File ในรูปแบบ PDF และ Microsoft Word (ถ้ามี) บรรจุในสื่อบันทึกข้อมูลแบบ USB Flash Drive จำนวนไม่น้อยกว่า ๑ ชุด

๑.๖ กรมสรรพสามิตมีสิทธิที่จะสำเนาและ/หรือคัดลอกข้อความบางส่วนของเอกสารและคู่มือใด ๆ ที่ผู้ชนะการประกวดราคาส่งมอบให้ภายใต้สัญญานี้ เพื่อใช้งานภายในกรมสรรพสามิต

๑.๗ เมื่อสิ้นสุดการอบรมจะมีการประเมินการอบรม โดยจะประเมินจากการตอบแบบสอบถาม

๑.๘ ผู้ชนะการประกวดราคาเป็นผู้รับผิดชอบจัดหาสถานที่ อุปกรณ์สื่อการเรียนการสอน ค่าสถานที่ ค่าเดินทาง ค่าที่พัก ค่าเบี้ยเลี้ยง ค่าวิทยากร ค่าอาหาร ค่าอาหารว่าง ค่าเอกสารต่าง ๆ และค่าใช้จ่ายอื่น ๆ ที่อาจเกิดขึ้นตลอดหลักสูตรการฝึกอบรม

๑.๙ สถานที่การฝึกอบรมจะต้องได้รับความเห็นชอบจากกรมสรรพสามิต ทั้งนี้สามารถอบรมแบบออนไลน์ได้ ขึ้นอยู่กับการพิจารณาเห็นชอบของกรมสรรพสามิต

๒. <u>การสนับสนุน</u>

หลังจากลงนามในสัญญาแล้ว ผู้ชนะการประกวดราคาจ้างต้องจัดให้มีการสนับสนุนอย่างต่อเนื่องตลอดระยะเวลาการดำเนินงาน และการรับประกัน "ระบบงาน" โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้นจากกรมสรรพสามิตนอกเหนือจากราคาที่เสนอในใบเสนอราคา ในเรื่องต่าง ๆ ดังนี้

๒.๑ จัดเตรียมอุปกรณ์ประกอบไปด้วย เครื่องคอมพิวเตอร์แบบพกพา และ LCD Projector อย่างน้อย ๑ ชุด ทุกการประชุมพร้อมบุคลากรในการจดรายงานการประชุมและทำรายงานการประชุม

๒.๒ หลังจากตรวจรับงานงวดสุดท้าย และติดตั้งใช้งานระบบจริง ผู้เสนอราคาต้องจัดให้มีเจ้าหน้าที่ให้บริการถาม-ตอบทางโทรศัพท์ (Help Desk) อย่างน้อย ๑ คน ระยะเวลา ๑ ปี ประจำที่กรมสรรพสามิต กรณีที่กรมสรรพสามิตไม่มีสถานที่เพียงพอ ผู้เสนอราคามีหน้าที่รับผิดชอบในการจัดหาสถานที่ ตลอดระยะเวลาการรับประกัน โดยมีหน้าที่ ดังนี้

๒.๒.๑ เจ้าหน้าที่ Help Desk มีหน้าที่วิเคราะห์ปัญหาและประสานงานในการแก้ไขปัญหาติดตาม และสรุปผลการดำเนินการในแต่ละครั้งพร้อมทั้งแจ้งข้อสรุปของปัญหาและวิธีการดำเนินการแก้ไขปัญหา และจัดทำรายการคำถามคำตอบที่พบบ่อย (Frequently Asked Questions : FAQ)

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๒.๒.๒ ฝึกอบรมเจ้าหน้าที่ Help Desk ของกรมสรรพสามิตเพื่อให้มีความรู้ความสามารถในการดำเนินงานและมีความรู้พื้นฐานเกี่ยวกับระบบงาน

๒.๒.๓ ทั้งนี้ กรมสรรพสามิตเป็นผู้จัดหาสถานที่ดำเนินการ และสายสัญญาณโทรศัพท์เพื่อใช้ในการให้บริการ กรณีที่กรมสรรพสามิตไม่มีสถานที่เพียงพอ ผู้ชนะการประกวดราคามีหน้าที่รับผิดชอบในการจัดหาสถานที่

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

เอกสารหมายเลข ๔
การบำรุงรักษาและแก้ไขระบบงาน

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

การบำรุงรักษาและแก้ไขระบบงาน

ผู้ชนะการประกวดราคาต้องรับประกันความบกพร่อง บำรุงรักษา แก้ไขระบบงานที่เกิดขึ้นทั้งหมด หรือเปลี่ยนทดแทนในทุกรายการที่เสนอ อันเนื่องจากข้อผิดพลาดของการปฏิบัติงาน ตลอดระยะเวลารับประกันเป็นเวลา ๑ ปีนับถัดจากวันที่กรมสรรพสามิตตรวจรับงานเสร็จสมบูรณ์ทั้งหมด โดยไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น จากกรมสรรพสามิต และในระยะเวลารับประกัน โดยต้องปฏิบัติตามเงื่อนไข ต่อไปนี้

๑. ผู้ชนะการประกวดราคาต้องทำการบำรุงรักษาระบบงาน **ตามเอกสารหมายเลข ๒** โดยผู้ชนะการประกวดราคาต้องเริ่มจัดการปรับปรุงแก้ไขให้อยู่ในสภาพดีได้ดังเดิม โดยต้องเริ่มจัดการแก้ไขภายใน ๑ วันทำการถัดไป นับแต่ได้รับแจ้งจากกรมสรรพสามิต และให้สามารถทำงานได้อย่างถูกต้องภายใน ๒ วันทำการ โดยไม่ทำให้ระบบงานหยุดชะงัก หรือเกิดความเสียหายแก่ทางราชการ โดยกรมสรรพสามิตจะทำการจดบันทึกวันเวลา และชื่อผู้รับแจ้งของผู้ชนะการประกวดราคาไว้เป็นหลักฐาน

ถ้าหากผู้ชนะการประกวดราคาไม่เริ่มดำเนินการแก้ไขข้อขัดข้องได้ภายในเวลาดังกล่าวผู้ชนะการประกวดราคาต้องถูกปรับในอัตราวันละ ๓,๐๐๐ บาท

ถ้าผู้ชนะการประกวดราคาไม่สามารถแก้ไขปัญหาดังกล่าวได้ภายในระยะเวลาที่กำหนด กรมสรรพสามิตสามารถจัดจ้างผู้อื่นมาแก้ปัญหาได้ โดยคู่สัญญาจะต้องเป็นผู้ออกค่าใช้จ่ายในการจัดจ้างดังกล่าวทั้งหมด

๒. ผู้ชนะการประกวดราคาต้องทำการบำรุงรักษาและแก้ไขระบบงานให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตลอดระยะเวลาการรับประกัน หากไม่ทำการบำรุงรักษาในระยะเวลาการรับประกันดังกล่าว ผู้ชนะการประกวดราคาต้องยินยอมให้กรมสรรพสามิตคิดค่าปรับครั้งละ ๕,๐๐๐ บาท (ห้าพันบาทถ้วน)

๓. ผู้ชนะการประกวดราคาต้องทำการบำรุงรักษาระบบงานหรือโปรแกรม (Software Application) ตามที่กำหนด **ตามเอกสารหมายเลข ๒** โดยผู้ชนะการประกวดราคาต้องทำการบำรุงรักษา แก้ไข และปรับปรุงระบบงาน หรือโปรแกรม (Software Application) ในกรณีที่มีข้อผิดพลาดอันเนื่องมาจากการทำงานของระบบงาน หรือโปรแกรม (Software Application) และ/หรือการปรับปรุงตามวัตถุประสงค์ของกรมสรรพสามิตให้ถูกต้องแล้วเสร็จโดยเร็ว โดยไม่ทำให้ระบบงานหยุดชะงักหรือเกิดความเสียหายแก่ทางราชการ

๔. เมื่อมีการเปลี่ยนแปลง แก้ไข ปรับปรุงเพิ่มเติมซอฟต์แวร์ระบบ (System Software) หรือ Software Tool ต่าง ๆ ที่เกี่ยวข้องกับระบบงาน ในลักษณะการ Upgrade Release หรือ Upgrade Version ใหม่ให้ทันสมัยขึ้น ผู้ชนะการประกวดราคาต้องเสนอรายละเอียดพร้อมค่าใช้จ่ายต่อกรมสรรพสามิต เพื่อพิจารณาให้ความเห็นชอบที่จะดำเนินการต่อไป

๕. การเรียกเงินค่าปรับ หากผู้ชนะการประกวดราคาไม่ชำระเงินค่าปรับภายใน ๗ วัน นับแต่วันที่กรมสรรพสามิตแจ้งให้ทราบเป็นลายลักษณ์อักษร กรมสรรพสามิตมีสิทธิหักเงินค่าปรับจากเงินประกันสัญญาหรือเรียกจากธนาคารผู้ค้ำประกันได้ทันที

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๖. ให้ผู้เสนอราคา เสนอรายละเอียดการบำรุงรักษา รายละเอียดข้อเสนอ วิธีการบำรุงรักษา เพื่อประกอบการพิจารณาทางด้านเทคนิค

๗. ผู้เสนอราคา เสนอราคาค่าบำรุงรักษาราคาค่าบำรุงรักษาซอฟต์แวร์ระบบ (System Software) หรือ Software Tool ต่าง ๆ ที่ใช้ในโครงการ ทั้งนี้ ให้เสนอราคาค่าบำรุงรักษาเป็นรายปี ในระยะเวลา ๓ ปี

๘. ข้อเสนอตามข้อ ๖, ๗ ผู้เสนอราคาให้เสนอรายละเอียดมาในเอกสารทางเทคนิค ทั้งนี้ กรมสรรพสามิตอาจจ้างบำรุงรักษาหรือไม่จ้างบำรุงรักษาหลังจากพ้นระยะเวลารับประกัน ๑ ปีแล้วก็ได้

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

เอกสารหมายเลข ๕

รายละเอียดข้อเสนอด้านคุณสมบัติของผู้เสนอราคา

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๑. คุณสมบัติทั่วไป และประสบการณ์ของผู้เสนอราคา

(๑) บทสรุปสำหรับผู้บริหาร .....

(๒) รายละเอียดบริษัท (Company Profile).....

(๓) ประสบการณ์ของผู้เสนอราคา

ข้อมูลรายละเอียดลูกค้าที่อ้างอิง				ข้อมูลรายละเอียดโครงการที่อ้างอิง						
ชื่อลูกค้า	ที่อยู่/ประเทศ	ประเภทธุรกิจ	บุคคลที่สามารถติดต่อได้ (ชื่อ/ตำแหน่ง/โทรศัพท์/e-mail)	ชื่อโครงการ	ปีที่ดำเนินการ (ย้อนหลังไม่เกิน ๕ ปี)	ระยะเวลา		มูลค่าโครงการ	อธิบายรายละเอียดของโครงการที่ทำ	หมายเหตุ
						ตามสัญญา	ทำงานจริง			

ประทับตรา
(ถ้ามี)

ลงชื่อ.....
(.....)
ตำแหน่ง.....
บริษัท/.....
ผู้เสนอราคา
วันที่...../...../.....

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๒. ตารางสรุปคุณสมบัติ ประสบการณ์ และประวัติของบุคลากรที่เสนอรายชื่อ

ลำดับที่	ชื่อ/ชื่อสกุล	ตำแหน่งในโครงการที่จัดจ้าง	วุฒิการศึกษา/สาขา	ประสบการณ์ (ปี)

ข้าพเจ้าขอรับรองว่ารายละเอียดตามรายการข้างต้นเป็นความจริงทุกประการ และยินยอมให้กรมสรรพสามิตตรวจสอบข้อมูล ตลอดจนให้ข้อมูลดังกล่าวในการใด ๆ อันเกี่ยวกับการจ้างพัฒนาระบบงานของกรมสรรพสามิต

ลงชื่อ.....

ประทับตรา (.....)

(ถ้ามี) ตำแหน่ง.....

บริษัท.....

ผู้เสนอราคา

วันที่...../...../.....

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

ประวัติ คุณสมบัติ และประสบการณ์ ของบุคลากร (ต่อ)

ชื่อ/ชื่อสกุล.....

หมายเลขประจำตัวประชาชน/หมายเลขหนังสือเดินทาง.....

อาชีพ ..... ที่อยู่.....

สัญชาติ ..... จำนวนปีที่ทำงานอยู่ในบริษัท.....

ตำแหน่งและหน้าที่ความรับผิดชอบที่ได้รับในโครงการ

ตำแหน่ง	หน้าที่ความรับผิดชอบ	ระยะเวลา

ประวัติการศึกษา

ตั้งแต่ - ถึง	ชื่อสถานศึกษา/ประเทศ	ปริญญา/ประกาศนียบัตรที่ได้รับ	คณะและภาควิชา

ประวัติการฝึกอบรม ดูงาน ฝึกงาน

ตั้งแต่ เดือน/ปี ถึง เดือน/ปี	ชื่อฝึกอบรม ดูงาน ฝึกงาน/ประเทศ	ชื่อหลักสูตร	ขอบเขต/รายละเอียด	ประโยชน์และการนำไปใช้งาน

ประวัติการทำงาน

ตั้งแต่ เดือน/ปี ถึง เดือน/ปี	ชื่อสถานที่ทำงาน/ประเทศ	ตำแหน่งและชื่อโครงการ	ขอบเขตและหน้าที่ความรับผิดชอบ	บุคคลอ้างอิง

ข้าพเจ้าขอรับรองว่ารายละเอียดตามรายการข้างต้นเป็นความจริงทุกประการ และยินยอมให้กรมสรรพสามิต ตรวจสอบข้อมูลตลอดจนใช้ข้อมูลดังกล่าวในการใด ๆ อันเกี่ยวกับการจ้างพัฒนาระบบงานของกรมสรรพสามิตได้

ลงชื่อเจ้าของประวัติ .....

(.....)

ประทับตรา (ถ้ามี)

ลงชื่อ.....

(.....)

ตำแหน่ง.....

บริษัท .....

ผู้เสนอราคา

วันที่...../...../.....

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๓. ตารางแผนงาน วิธีดำเนินการ และเครื่องมือในการพัฒนา

(๑) ตารางแผนงาน

ลำดับ	กิจกรรม	Man-Day	ระยะเวลา	เดือน													รายละเอียดทีมงาน	
				๑				๒				๓				๔	ชื่อ/ชื่อสกุล	Man-Day
				๑	๒	๓	๔	๕	๖	๗	๘	๙	...	...	...	...		

(๒) วิธีดำเนินการ และเครื่องมือในการพัฒนาและเทคนิคที่ใช้.....

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๔. ตารางแรงงานของบุคลากร (Man-Day) ที่เสนอในการดำเนินงานโครงการ

ชื่อ/ชื่อสกุล	ตำแหน่งในโครงการ	รายละเอียดกิจกรรมที่ทำ	Man-Day	หมายเหตุ

ลงชื่อ.....

ประทับตรา (ถ้ามี)

(.....)

ตำแหน่ง.....

บริษัท.....

ผู้เสนอราคา

วันที่...../...../.....

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

๕. ตารางบุคลากรที่ต้องใช้ในโครงการ

เมื่อเริ่มดำเนินโครงการ ผู้ชนะการประกวดราคาต้องเสนอบุคลากรตามตำแหน่งดังต่อไปนี้ เพื่อให้เพียงพอต่อการดำเนินงานตามระยะเวลาส่งมอบงาน

ลำดับที่	ตำแหน่ง	วุฒิการศึกษา	ประสบการณ์ (ปี)	จำนวน คน
๑.	ผู้จัดการโครงการ (Project Manager)	ปริญญาโท	๑. ด้านเทคโนโลยีสารสนเทศ อย่างน้อย ๑๕ ปี ๒. ด้านบริหารโครงการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ เป็นระยะเวลาอย่างน้อย ๕ ปี	๑
๒.	ที่ปรึกษาด้านการวางแผนการรักษาความมั่นคงปลอดภัยสารสนเทศ	ปริญญาโท	๑. ด้านเทคโนโลยีสารสนเทศ อย่างน้อย ๑๐ ปี ๒. ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑ หรือ การรักษาความมั่นคงปลอดภัยสารสนเทศเป็นระยะเวลาอย่างน้อย ๕ ปี	๒
๓.	ที่ปรึกษาด้านการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอาวุโส	ปริญญาตรี	ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ อย่างน้อย ๕ ปี	๑
๔.	ที่ปรึกษาด้านการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	ปริญญาตรี	ด้านการทดสอบเจาะระบบอย่างน้อย ๒ ปี	๑
๕.	ที่ปรึกษาด้านการวางแผนการคุ้มครองข้อมูลส่วนบุคคล	ปริญญาตรี	ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือการคุ้มครองข้อมูลส่วนบุคคล อย่างน้อย ๘ ปี	๒
๖.	ที่ปรึกษาด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล	ปริญญาโท	ด้านกฎหมายไม่น้อยกว่า ๘ ปี และมีประสบการณ์การคุ้มครองข้อมูลส่วนบุคคล อย่างน้อย ๑ ปี	๑

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ

ลำดับที่	ตำแหน่ง	วุฒิการศึกษา	ประสบการณ์ (ปี)	จำนวน คน
๗.	ที่ปรึกษาด้านการคุ้มครองข้อมูลส่วนบุคคล	ปริญญาตรี	ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือการคุ้มครองข้อมูลส่วนบุคคล อย่างน้อย ๑ ปี	๒
๘.	เจ้าหน้าที่ตอบคำถามให้ความช่วยเหลือ และประสานงานโครงการ (Help Desk)	ปริญญาตรี	ด้านสารสนเทศ หรือการคุ้มครองข้อมูลส่วนบุคคล อย่างน้อย ๑ ปี	๑

.....ประธานกรรมการ.....กรรมการ.....กรรมการ.....กรรมการ.....กรรมการ