ขอบเขตงาน (Term of Reference: TOR)
การจัดจ้างการบำรุงรักษาระบบบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ
ของกรมการท่องเที่ยว (ISMS Maintenance Activities)

๑. หลักการและเหตุผล

อุตสาหกรรมท่องเที่ยวเป็นกิจกรรมที่มีการขยายตัวสูง และมีความสำคัญต่อระบบเศรษฐกิจและสังคมของประเทศไทย โดยเฉพาะอย่างยิ่งในการเป็นแหล่งสร้างรายได้ นำมาซึ่งเงินตราต่างประเทศ การสร้างงาน และการกระจายความเจริญไปสู่ภูมิภาค และมิใช่เพียงแต่ประเทศไทยเท่านั้นที่เห็นความสำคัญของอุตสาหกรรมท่องเที่ยว ประเทศต่าง ๆ ได้เล็งเห็นว่า การท่องเที่ยวก่อให้เกิดรายได้ และสามารถสร้างความเจริญให้แก่ประเทศในทุกภาคส่วน จึงส่งผลให้ทุกประเทศส่งเสริม สนับสนุน และให้ความสำคัญกับการพัฒนาด้านการท่องเที่ยว ซึ่งการพัฒนาอุตสาหกรรมการท่องเที่ยวให้ประสบความสำเร็จได้ด้วยดีนั้น ประเทศที่มีฐานข้อมูลด้านการท่องเที่ยวที่ดี และมีคุณภาพจะได้เปรียบในการนำข้อมูลดังกล่าว มาสร้างสรรค์มาตรการและนโยบายต่าง ๆ ที่มีผลกระทบต่อการท่องเที่ยวสูง ประกอบกับปัญหาความมั่นคงไซเบอร์ (Cyber Security) ที่มีความรุนแรงมากขึ้น โดยเฉพาะปัญหาการใช้ช่องทาง ไซเบอร์ในการจารกรรมข้อมูล การโจมตีระบบสาธารณูปโภค การทำลายเสถียรภาพของรัฐบาลและชื่อเสียงของประเทศ กลุ่มเทคโนโลยีสารสนเทศ กรมการท่องเที่ยว ได้รับมอบหมายนโยบายให้เข้าไปร่วมดำเนินการพัฒนาฐานข้อมูลของทุก สำนัก/กอง ภายในกรมการท่องเที่ยว เช่น การพัฒนาฐานข้อมูลแหล่งท่องเที่ยว การพัฒนาฐานข้อมูลทะเบียนธุรกิจนำเที่ยวและมัคคุเทศก์ และการพัฒนาฐานข้อมูลมาตรฐานการท่องเที่ยวไทย เป็นต้น กรมการท่องเที่ยว จึงได้จัดทำระบบบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศตามมาตรฐานสากล ISO/IEC 27001: 2013 (Information Security Management System : ISMS) และขอใบรับรองมาตรฐาน ISO/IEC 27001 : 2013 ในปี พ.ศ. ๒๕๖๔ แต่อย่างไรก็ตามใบรับรองต้องได้รับการดำเนินการ ติดตาม และตรวจต่ออายุทุกปี

ดังนั้น เพื่อคงไว้ซึ่งมาตรฐาน เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเป็นไปอย่างต่อเนื่อง มีประสิทธิภาพ และมีการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศจากมุมมองที่เป็นมาตรฐาน รวมถึงเป็นไปตามประเด็นยุทธศาสตร์ชาติด้านความมั่นคงในประกาศ เรื่อง ยุทธศาสตร์ชาติ (พ.ศ. ๒๕๖๑ - ๒๕๘๐) ในราชกิจจานุเบกษา ข้อที่ ๔ กลุ่มเทคโนโลยีสารสนเทศ กรมการท่องเที่ยว จึงมีความจำเป็นต่ออายุการรับรองมาตรฐานระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC 27001: 2013 ในปีพ.ศ. ๒๕๖๔ พร้อมทั้งพัฒนาบุคลากรซึ่งปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ให้มีความรู้สอดรับรับการเปลี่ยนแปลงที่จะเกิดขึ้นในอนาคต และพร้อมที่จะปฏิบัติงานได้อย่างมีประสิทธิภาพต่อไป

/๒. วัตถุประสงค์...

๒. วัตถุประสงค์

๒.๑ เพื่อทบทวนกรอบแนวทางในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม กรมการท่องเที่ยว ให้สอดคล้องกับข้อกำหนดของมาตรฐานสากล ISO/IEC 27001: 2013

๒.๒ เพื่อต่ออายุมาตรฐานระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) ของกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม กรมการท่องเที่ยว ให้สอดคล้องกับข้อกำหนดของมาตรฐานสากล ISO/IEC 27001 : 2013

๒.๓ เพื่อพัฒนาบุคลากรของกลุ่มเทคโนโลยีสารสนเทศ กรมการท่องเที่ยว ให้มีความรู้ในการดำเนินการระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) และสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ

๓. คุณสมบัติของผู้เสนอราคา

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ เป็นบุคคลธรรมดาหรือนิติบุคคล ผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่กรมการท่องเที่ยว ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

/๓.๑๐ ผู้ยื่น...

๓.๑๐ ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e - GP) ของกรมบัญชีกลาง

๓.๑๑ ผู้รับจ้างต้องมีประสบการณ์ในการดำเนินงานให้คำปรึกษาด้านระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC 27001 ให้กับหน่วยงานราชการหรือรัฐวิสาหกิจ หรือบริษัทเอกชนที่เชื่อถือได้ในประเทศไทย อย่างน้อย ๒ แห่ง ทั้งนี้ต้องแนบสำเนาหนังสือรับรองผลงานเพื่อประกอบการพิจารณา

๓.๑๒ ผู้เสนอราคาต้องจัดหาบุคลากรที่มีความรู้ความสามารถให้เหมาะสมกับตำแหน่งหน้าที่ในจำนวนที่เพียงพอ เพื่อดำเนินโครงการได้อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดตามวัตถุประสงค์ของโครงการ โดยมีบุคลากรอย่างน้อย ดังนี้

ลำดับ	รายการ	จำนวน
๑	ผู้จัดการโครงการ (Project Manager) <u>หน้าที่ความรับผิดชอบ</u> ● ดูแลบริหารจัดการและควบคุมการดำเนินงานโครงการให้เป็นไปตามสัญญาและระยะเวลาที่กำหนดการส่งมอบโครงการ ● กำหนดขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้ถูกต้องและให้คำแนะนำระดับสูงในการดำเนินการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ <u>คุณสมบัติ</u> ● มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นระยะเวลาอย่างน้อย ๕ ปี ● จบการศึกษาอย่างน้อยในระดับปริญญาโทด้านเทคโนโลยีสารสนเทศ หรือเทียบเท่า ● มีประกาศนียบัตรสอบผ่านการอบรมหลักสูตร Information Security Management System Auditor/Lead Auditor Course (ISO/IEC 27001 : 2013 Standard) ซึ่งได้รับรองจากสถาบันInternational Register of Certificated Auditors (IRCA) และเป็น Certificate of Successful Completion	๑

/ลำดับ...

ลำดับ	รายการ	จำนวน
๒	ผู้เชี่ยวชาญ หน้าที่ความรับผิดชอบ • ดูแลการดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในองค์กร • ให้การสนับสนุนการดำเนินการโครงการ และการอบรมด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ • ดำเนินการตรวจสอบมาตรการที่มีอยู่และให้คำแนะนำแก่ทีมงาน คุณสมบัติ • มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นระยะเวลาอย่างน้อย ๑๐ ปี • จบการศึกษาอย่างน้อยในระดับปริญญาโท หรือเทียบเท่า • มีประกาศนียบัตรสอบผ่านการอบรมหลักสูตร Information Security Management System Auditor/Lead Auditor Course (ISO/IEC 27001 : 2013 Standard) ซึ่งได้รับรองจากสถาบัน International Register of Certificated Auditors (IRCA) และเป็น Certificate of Successful Completion • มีใบรับรองคุณวุฒิ CISSP (Certified Information System Security Professional) หรือ CISM (Certified Information Security Manager) หรือ CISA (Certified Information Security Auditor)	๑
๓	นักวิจัย หน้าที่ความรับผิดชอบ • ดำเนินงานตามขอบเขตของงานภายใต้คำแนะนำของผู้เชี่ยวชาญ • ดำเนินการตามรายละเอียดและขอบเขตของโครงการและฝึกอบรมที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ • รับผิดชอบการตรวจสอบช่องโหว่ทางเทคนิค (Technical Baseline: Security Vulnerability Assessment)	๑

/คุณสมบัติ...

ลำดับ	รายการ	จำนวน
	<u>คุณสมบัติ</u> ● มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นระยะเวลาอย่างน้อย ๓ ปี ● จบการศึกษาอย่างน้อยในระดับปริญญาตรี หรือเทียบเท่า ● มีประกาศนียบัตรสอบผ่านการอบรมหลักสูตร Information Security Management System Auditor/Lead Auditor Course (ISO/IEC 27001 : 2013 Standard) ซึ่งได้รับรองจากสถาบัน International Register of Certificated Auditors (IRCA) และเป็น Certificate of Successful Completion	๑
๔	ผู้ประสานงาน <u>หน้าที่ความรับผิดชอบ</u> ● รับผิดชอบประสานงานระหว่างผู้เชี่ยวชาญ และกรมการท่องเที่ยว เพื่อให้โครงการดำเนินได้อย่างราบรื่น ● รับผิดชอบในการจัดเตรียมเอกสารต่าง ๆ ที่เกี่ยวข้องภายใต้โครงการการพัฒนาการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ ● รับผิดชอบในการจัดเตรียมเอกสารส่งมอบ <u>คุณสมบัติ</u> ● จบการศึกษาอย่างน้อยในระดับปริญญาตรี หรือเทียบเท่า	๑

๔. ขอบเขตการดำเนินงาน

ผู้รับจ้างต้องดำเนินโครงการร่วมกับเจ้าหน้าที่ของกรมการท่องเที่ยวในการต่ออายุมาตรฐานระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของกลุ่มเทคโนโลยีสารสนเทศ ให้เป็นไปตามมาตรฐานสากล ISO/IEC 27001: 2013 โดยมีขอบเขตการดำเนินงาน ดังนี้

๔.๑ จัดทำแผนดำเนินงานและปฏิทินการปฏิบัติงานโครงการ

๔.๒ ดำเนินการทบทวนข้อมูลทะเบียนทรัพย์สิน (Asset) ในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

/๔.๓ ดำเนินการ...

๔.๓ ทบทวนโครงสร้างการบริหารจัดการ และหน้าที่ความรับผิดชอบของคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) และคณะทำงานอื่นที่เกี่ยวข้อง

๔.๔ ดำเนินการทบทวนแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Risk Management) ให้ตรงตามข้อกำหนดที่ระบุไว้ใน ISO/IEC 27001:2013 และ ISO/IEC 27005 โดยอย่างน้อยต้อง ประกอบด้วย

๔.๔.๑ ทบทวนแนวทางในการประเมินความเสี่ยง

๔.๔.๒ ดำเนินการประเมินความเสี่ยง

๔.๔.๓ ทบทวนการบริหารจัดการความเสี่ยง

๔.๔.๔ จัดทำแผนจัดการความเสี่ยง และติดตามผลความคืบหน้าของแผน

๔.๕ ดำเนินการทบทวน และปรับปรุงเอกสารสำคัญตามขอบเขตของระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ได้แก่ นโยบาย และขั้นตอนการปฏิบัติงาน เป็นต้น ให้สอดคล้องตามมาตรฐานสากล (ISO/IEC 27001:2013) ถูกต้องครบถ้วน และเป็นปัจจุบัน

๔.๖ ดำเนินการทบทวนรายการข้อกำหนดที่นำมาใช้ (Statement of Applicability - SOA) สำหรับการดำเนินการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) ของกรมการท่องเที่ยว

๔.๗ ดำเนินการตรวจสอบช่องโหว่ทางเทคนิค (Technical Baseline : Security Vulnerability Assessment) สำหรับระบบสารสนเทศที่สำคัญ เพื่อทดสอบความปลอดภัยของสินทรัพย์และป้องกันช่องโหว่ที่สามารถเกิดขึ้น

๔.๘ ดำเนินการทบทวนการบริหารจัดการความต่อเนื่องทางธุรกิจ (Information security aspect of business continuity management) ตามมาตรฐาน ISO/IEC 27001 : 2013 โดยการทบทวนเอกสาร จัดทำแผนความต่อเนื่องทางธุรกิจ และจัดทำการทดสอบแผนการกู้คืนระบบสารสนเทศ ตามขอบเขตที่กำหนด เป็นต้น

๔.๙ ดำเนินการตรวจประเมินภายใน (Internal Audit) ให้สอดคล้องกับข้อกำหนดในมาตรฐาน ISO/IEC 27001 : 2013

๔.๑๐ ดำเนินการร่วมกับเจ้าหน้าที่กรมการท่องเที่ยว ในการจัดเตรียม และทบทวนข้อมูลการดำเนินงานระบบการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) เพื่อนำเสนอต่อผู้บริหาร (Management Review)

๔.๑๑ ดำเนินการสนับสนุนให้สามารถรับการตรวจรับรองมาตรฐาน ISO/IEC 27001 : 2013 (Certification Body) จากหน่วยงานภายนอกที่เป็นที่ยอมรับในระดับสากลและสนับสนุนในขณะมีการตรวจประเมินการรับรองตามมาตรฐาน ISO/IEC 27001 : 2013

/ ๔.๑๒ ดำเนินการร่วมกับ...

๔.๑๒ ดำเนินการร่วมกับเจ้าหน้าที่กรมการท่องเที่ยว ในการวางแผนแก้ไขเชิงป้องกันความไม่สอดคล้องที่พบในระหว่างการตรวจประเมินภายใน (Internal Audit) และการตรวจรับรองมาตรฐาน ISO/IEC 27001 : 2013 (Certification Body)

๔.๑๓ ดำเนินการจัดฝึกอบรม สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ โดยอบรมให้กับบุคลากรไม่น้อยกว่า ๘ คน เป็นระยะเวลา อย่างน้อย ๓ ชั่วโมง

๔.๑๔ ดำเนินการจัดประชุมเพื่อเตรียมความพร้อมสำหรับการตรวจบำรุงรักษามาตรฐาน ISO/IEC 27001: 2013

๕. การรักษาข้อมูลที่เป็นความลับสำหรับหน่วยงานภายนอก

๕.๑ ขอบข่ายของข้อตกลง และคำจำกัดความข้อตกลงในสัญญาฉบับนี้จะใช้เป็นข้อกำหนดในการเปิดเผยข้อมูลระหว่าง กรมการท่องเที่ยว (ผู้เปิดเผยข้อมูล) และผู้รับจ้างข้อมูลต่าง ๆ จะต้องเป็นไปซึ่งการเปิดเผย (ผู้รับข้อมูล) เพื่อให้บรรลุวัตถุประสงค์ในการดำเนินงานตามขอบเขตของโครงการเท่านั้น โดยลักษณะการเผยแพร่ หรือการให้ข้อมูลอาจทำได้โดยวิธีการต่าง ๆ เช่น การอธิบายด้วยวาจา รูปภาพ เอกสาร การเรียกดูข้อมูล การบรรยายสรุป หรือวิธีการใด ๆ ที่จะทำให้ได้มาซึ่งข้อมูลที่เกี่ยวข้อง

๕.๒ คำจำกัดความ “ข้อมูลที่เป็นความลับ” หมายถึง ข้อมูลอยู่ในระดับชั้น “ปกปิด (Restricted)” และระดับชั้น “ลับ (Confidential)” และมีป้ายระบุระดับชั้นความลับอย่างชัดเจนซึ่งได้แก่ ข้อมูลหรือเอกสารกระบวนการดำเนินงาน ข้อมูลการดำเนินธุรกิจ เอกสารการออกแบบระบบ งานวิจัย องค์ความรู้ หรือทักษะขององค์กร Source Code สถาปัตยกรรมระบบ ข้อมูลภายในองค์กร เทคโนโลยีที่ใช้ในองค์กร รายงานผลการดำเนินงาน แผนการตลาด แผนการเงิน รายงานการตรวจประเมินภายใน เป็นต้น

๕.๓ การจัดการกับข้อมูลที่เป็นความลับ “ผู้รับข้อมูล” จะต้องจัดการข้อมูลที่เป็นความลับให้สอดคล้องกับข้อกำหนดในการจัดการข้อมูลในแต่ละระดับชั้น ตามที่องค์กรของ “ผู้เปิดเผยข้อมูล” กำหนดอย่างเคร่งครัด ทั้งนี้ หากข้อมูลถูกเผยแพร่ออกไปภายนอก ไม่ว่าด้วยสาเหตุใด ๆ “ผู้รับข้อมูล” จะต้องรับผิดชอบต่อ ความเสียหายที่เกิดขึ้นทั้งทางแพ่ง และทางอาญา

๕.๔ การรับรองการเปิดเผยข้อมูล การเปิดเผย “ข้อมูลที่เป็นความลับ” นั้น จะดำเนินการได้ต่อเมื่อ “ ผู้รับข้อมูล” ได้ลงนามในสัญญาฉบับนี้เสียก่อน โดย “ ผู้รับข้อมูล” จะต้องปฏิบัติตามเงื่อนไขในสัญญาฉบับนี้โดยเคร่งครัด ทั้งนี้ “ผู้เปิดเผยข้อมูล” จะจัดส่งหรือให้ข้อมูลตามที่ร้องขอได้ ภายใน ๓๐ วัน นับตั้งแต่วันที่ลงนามในสัญญาฉบับนี้

/๕.๕ ความรับผิดชอบ...

๕.๕ ความรับผิดชอบของผู้รับข้อมูล “ผู้รับข้อมูล” เห็นชอบที่จะ (๑) จัดการข้อมูลตามระดับชั้นความลับของข้อมูลดังกล่าวอย่างเคร่งครัด (๒) ไม่ใช้ข้อมูลความลับที่ได้รับเพื่อจุดประสงค์ใด ๆ ที่นอกเหนือจากจุดประสงค์ที่กล่าวมาแล้วข้างต้น และ (๓) ไม่เปิดเผยข้อมูลความลับดังกล่าวแก่บุคคลภายนอก เว้นแต่ในกรณีที่ “ผู้รับข้อมูล” มีความจำเป็นที่จะต้องเปิดเผยข้อมูลที่เป็นความลับให้กับบุคคลอื่นรับทราบ ในที่นี้เรียกว่า“ผู้กระทำการแทน” เพื่อให้สามารถดำเนินงานให้บรรลุวัตถุประสงค์ได้ “ผู้รับข้อมูล” จะต้องประสานงานให้ “ผู้กระทำการแทน” ทุกฝ่ายลงนามในสัญญาดังกล่าวนี้ ก่อนให้ข้อมูลต่อไป

๕.๖ การร้องขอข้อมูล การร้องขอข้อมูลใด ๆ ภายใต้ข้อตกลงในเอกสารฉบับนี้ “ผู้รับข้อมูล” จะต้องจัดทำเป็นลายลักษณ์อักษร โดยจะต้องจัดส่งให้ “ผู้เปิดเผยข้อมูล” ล่วงหน้าอย่างน้อยห้า (๕) วัน

๕.๗ การส่งคืนข้อมูล “ผู้รับข้อมูล” จะต้องจัดส่งเอกสาร หรือข้อมูลทั้งหมดที่ได้ร้องขอกลับมายัง กรมการท่องเที่ยว สามสิบ (๓๐) วัน หลังจากที่ได้รับเอกสารหรือข้อมูลดังกล่าว และจะต้องจัดส่งตามแนวปฏิบัติในการจัดการข้อมูล ของกรมการท่องเที่ยวอย่างเคร่งครัด

๕.๘ ระยะเวลาการคุ้มครอง ข้อตกลงฉบับนี้จะได้รับการคุ้มครอง ข้อตกลงฉบับนี้ยังคงมีผลบังคับใช้ต่อเนื่องอีกสาม (๓) ปี นับจากวันสุดท้ายที่จบสิ้นโครงการ หรือสัญญาที่เกี่ยวข้องกับการเปิดเผยข้อมูล

๕.๙ อื่น ๆ (๑) การจัดการข้อมูลใด ๆ ที่ร้องขอให้ปฏิบัติตามข้อกำหนดในการจัดการข้อมูลของหน่วยงาน (๒) ข้อตกลงฉบับนี้ร่างขึ้นโดยคู่สัญญาเพื่อให้เกิดความเข้าใจร่วมกัน (๓) การเพิ่ม ลบ หรือแก้ไข ส่วนใด ๆ ของข้อตกลงฉบับนี้ต้องกระทำเป็นลายลักษณ์อักษร และลงนามโดยผู้แทนที่มีอำนาจของแต่ละฝ่าย (๔) เกณฑ์ และเงื่อนไขในข้อตกลงว่าด้วยการไม่เปิดเผยข้อมูลนี้จะนำเข้ามาเป็นส่วนหนึ่งของข้อตกลงอื่น ๆ ที่คู่สัญญาจะลงนามร่วมกันในอนาคต (๕) หัวข้อของหมวดต่าง ๆ ในข้อตกลงฉบับนี้มีไว้เพื่อการอ้างอิงเท่านั้น ทั้งนี้ไม่สามารถจำกัด หรือขยายความหมายของบทบัญญัติใด ๆ ของข้อตกลงฉบับนี้ได้

๖. กำหนดส่งมอบงาน

ระยะเวลาดำเนินการ ภายใน ๒๔๐ วัน (นับถัดจากวันลงนามในสัญญาจ้าง)

๗. การส่งมอบงานและเงื่อนไขการชำระเงิน

ผู้รับจ้างจะต้องส่งมอบเอกสารและรายงานต่าง ๆ โดยมีกำหนดการส่งมอบงานจำนวน ๓ งวด โดยแต่ละงวดจะต้องประกอบด้วย เอกสารที่จัดพิมพ์เข้าเล่ม จำนวน ๕ ชุด พร้อมบันทึกลงแผ่นซีดีจำนวน ๒ ชุด โดยมีรายละเอียดดังนี้

<u>งวดที่ ๑</u> เป็นจำนวนเงินในอัตราร้อยละ ๔๐ ของค่าจ้างเมื่อปฏิบัติงานแล้วเสร็จและส่งมอบงาน ภายใน ๑๕๐ วัน นับถัดจากวันลงนามในสัญญาซึ่งประกอบไปด้วยเอกสารดังนี้

๑) แผนดำเนินงานและปฏิทินการปฏิบัติงานโครงการ

/๒) รายงานการศึกษา...

๒) รายงานการศึกษาโครงสร้างการบริหารจัดการ และหน้าที่ความรับผิดชอบของคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) และคณะทำงานอื่นที่เกี่ยวข้อง

๓) รายงานการทบทวนขอบเขตการดำเนินงานตามระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System Scope) ของกลุ่มเทคโนโลยีสารสนเทศ กรมการท่องเที่ยว

๔) รายงานการทบทวนข้อมูลทะเบียนทรัพย์สิน (Asset) ในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๕) รายงานการบริหารจัดการความเสี่ยง (การประเมินความเสี่ยง และการจัดการความเสี่ยง)

<u>งวดที่ ๒</u> เป็นจำนวนเงินในอัตราร้อยละ ๓๐ ของค่าจ้างเมื่อปฏิบัติงานแล้วเสร็จและส่งมอบงาน ภายใน ๒๑๐ วันนับถัดจากวันลงนามในสัญญา ซึ่งประกอบไปด้วยเอกสาร ดังนี้

๑) รายงานการทบทวนเอกสารนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)

๒) รายงานการทบทวนเอกสารขั้นตอนการปฏิบัติงานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)

๓) รายงานการอบรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ

๔) รายงานการตรวจสอบช่องโหว่ทางเทคนิค (Technical Baseline : Security Vulnerability Assessment)

๕) รายงานผลการทบทวนแผนการบริหารความต่อเนื่องทางธุรกิจ

๖) รายงานผลการทดสอบแผนการกู้คืนระบบสารสนเทศ

๗) รายงานผลการตรวจประเมินภายใน

<u>งวดที่ ๓ (งวดสุดท้าย)</u> เป็นจำนวนเงินในอัตราร้อยละ ๓๐ ของค่าจ้างเมื่อปฏิบัติงานแล้วเสร็จและส่งมอบงาน ภายใน ๒๔๐ วัน นับถัดจากวันลงนามในสัญญา ซึ่งประกอบไปด้วยเอกสาร ดังนี้

๑) รายงานผลการตรวจบำรุงรักษามาตรฐาน ISO/IEC 27001 : 2013 (Certified Body Audit Report)

๒) จดหมายรับรองการตรวจบำรุงรักษารองมาตรฐาน ISO/IEC 27001 : 2013

/๘. หลักเกณฑ์...

๘. หลักเกณฑ์และสิทธิ์ในการพิจารณา

๘.๑ ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ กรมการท่องเที่ยว จะพิจารณาตัดสินโดยใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance) และจะพิจารณาจากราคารวม

๘.๒ ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ กรมการท่องเที่ยว จะพิจารณาตัดสินให้คะแนนส่วนของผลงานและประสบการณ์ของผู้เสนอราคา ดังนี้

๘.๒.๑ ที่เสนอราคา (Price) เป็นตัวแปรหลักบังคับ ร้อยละ ๓๐

๘.๒.๒ คุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อทางราชการ ร้อยละ ๗๐

โดยคณะกรรมการฯ จะพิจารณาคุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อทางราชการ ร้อยละ ๗๐ โดยพิจารณาการจ้างคะแนนเต็ม ๑๐๐ คะแนน ดังนี้

๑. ข้อเสนอทางเทคนิค และรูปแบบการดำเนินงาน ร้อยละ ๔๐

๒. ขีดความสามารถหรือข้อเสนออื่น ๆ ร้อยละ ๓๐

- บุคลากร/ทีมงาน/ผู้เชี่ยวชาญประจำโครงการ
- ผลงานและประสบการณ์ของผู้เสนอราคา

ลำดับ	ข้อพิจารณา	๗๐ คะแนน
๑	ข้อเสนอทางเทคนิค และรูปแบบการดำเนินงาน - ความถูกต้องครบถ้วนของรายละเอียดตามข้อกำหนด TOR (๑๐ คะแนน) - เครื่องมือในการดำเนินงาน (๒๐ คะแนน) - แผนการดำเนินงาน (๑๐ คะแนน)	๔๐ คะแนน
๒	ขีดความสามารถหรือความพร้อมของผู้เสนอราคา - บุคลากร/ทีมงาน/ผู้เชี่ยวชาญประจำโครงการ (๑๐ คะแนน) - ผลงานและประสบการณ์ของผู้เสนอราคา (๒๐)	๓๐ คะแนน

๙. วงเงินงบประมาณ

๑,๐๐๐,๐๐๐ บาท (หนึ่งล้านบาทถ้วน)

๑๐. อัตราค่าปรับ

อัตราค่าปรับตามแบบสัญญาจ้าง จะกำหนดในอัตราร้อยละ ๐.๑ ของราคางานที่ยังไม่ได้รับมอบต่อวัน