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 ได้รับมอบหมายนโยบายให้เข้าไปร่วมดำเนินการพัฒนาฐานข้อมูลของทุกสำนัก/กอง ภายในกรมการท่องเที่ยว เช่น การพัฒนาฐานข้อมูลแหล่งท่องเที่ยว การพัฒนาฐานข้อมูลทะเบียนธุรกิจนำเที่ยวและมัคคุเทศก์ และการพัฒนาฐานข้อมูลมาตรฐานการท่องเที่ยวไทย เป็นต้น กรมการท่องเที่ยว จึงได้จัดทำระบบบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศตามมาตรฐานสากล ISO/IEC 27001 : 2013 (Information Security Management System : ISMS) และได้ดำเนินการตรวจรับรองมาตรฐานเพื่อขอและต่ออายุใบรับรองมาตรฐาน ISO/IEC 27001 : 2013 มาอย่างต่อเนื่อง อย่างไรก็ตาม มาตรฐานดังกล่าวได้มีรับการปรับปรุงเป็น ISO/IEC 27001 : 2022 และประกาศในเดือนตุลาคม 2565 เพื่อให้ครอบคลุมทั้งด้านความปลอดภัยของข้อมูล และความปลอดภัยไซเบอร์ โดยหน่วยงานที่เคยได้รับการรับรองระบบบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศตามมาตรฐานสากล ISO/IEC 27001 : 2013 สามารถปรับปรุงการดำเนินงานภายในให้สอดคล้องตามมาตรฐานฉบับใหม่ภายในปี ตุลาคม 2568

ดังนั้น เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศสอดคล้องตามมาตรฐานฉบับใหม่ รวมถึงเป็นไปตามประเด็นยุทธศาสตร์ชาติด้านความมั่นคงในประกาศ เรื่อง ยุทธศาสตร์ชาติ (พ.ศ. ๒๕๖๑ - ๒๕๘๐) ในราชกิจจานุเบกษา ข้อที่ ๔ กลุ่มเทคโนโลยีสารสนเทศ กรมการท่องเที่ยว จึงมีความจำเป็นในการเตรียมความพร้อมสำหรับการปรับเปลี่ยนของมาตรฐานฉบับใหม่ ในรอบปี2567 เนื่องจากครบรอบอายุใบรับรองมาตรฐาน พร้อมทั้งพัฒนาบุคลากรซึ่งปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ให้มีความรู้สอดรับกับการเปลี่ยนแปลงที่จะเกิดขึ้นในอนาคต และพร้อมที่จะปฏิบัติงานได้อย่างมีประสิทธิภาพต่อไป

/๒. วัตถุประสงค์ ...

๒. วัตถุประสงค์

๒.๑ เพื่อปรับปรุงกรอบแนวทางในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม กรมการท่องเที่ยว ให้สอดคล้องกับข้อกำหนดของมาตรฐานสากล ISO/IEC 27001 : 2022

๒.๒ เพื่อพัฒนาบุคลากรของกรมการท่องเที่ยว 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 ผู้ยื่นข้อเสนอที่ยื่นเสนอราคาในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในประกาศเชิญชวน

กิจการร่วมค้าที่ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน เว้นแต่ในกรณีกิจการร่วมค้าที่มีข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นสามารถใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานก่อสร้างของกิจการร่วมค้าที่ยื่นข้อเสนอ

/กรณีมีข้อตกลง ...

กรณีมีข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงดังกล่าวจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญา มากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

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

๓.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวกติดต่อกันเป็นระยะ

กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ

๓.๑๓ ผู้รับจ้างต้องมีประสบการณ์ในการดำเนินงานให้คำปรึกษาด้านระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC 27001 ให้กับหน่วยงานราชการ หรือรัฐวิสาหกิจ หรือบริษัทเอกชนที่เชื่อถือได้ในประเทศไทย โดยมีมูลค่าโครงการไม่น้อยกว่า ๕๐๐,๐๐๐ บาท จำนวน ๑ โครงการ ภายในระยะเวลา ๕ ปี ทั้งนี้ต้องแนบสำเนาหนังสือรับรองผลงานและหลักฐานสำเนาสัญญาเพื่อประกอบการพิจารณาดังกล่าว

๓.๑๔ ผู้เสนอราคาต้องจัดหาบุคลากรที่มีความรู้ความสามารถให้เหมาะสมกับตำแหน่งหน้าที่ในจำนวนที่เพียงพอ เพื่อดำเนินโครงการได้อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดตามวัตถุประสงค์ของโครงการ โดยมีบุคลากรอย่างน้อย ดังนี้

ลำดับ	รายการ	จำนวน
๑	ผู้จัดการโครงการ (Project Manager) หน้าที่ความรับผิดชอบ - ดูแลบริหารจัดการและควบคุมการดำเนินงานโครงการให้เป็นไปตามสัญญาและระยะเวลาที่กำหนดการส่งมอบโครงการ - กำหนดขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้ถูกต้องและให้คำแนะนำระดับสูงในการดำเนินการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	๑

/คุณสมบัติ ...

ลำดับ	รายการ	จำนวน
	<u>คุณสมบัติ</u> - มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นระยะเวลาอย่างน้อย ๑๐ ปี - จบการศึกษาอย่างน้อยในระดับปริญญาโท หรือเทียบเท่า - มีประกาศนียบัตรสอบผ่านการอบรมหลักสูตร Information Security Management System Auditor/Lead Auditor Course (ISO/IEC 27001 : 2022 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)	
๒	ผู้เชี่ยวชาญ <u>หน้าที่ความรับผิดชอบ</u> - ดูแลการดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในองค์กร - ให้การสนับสนุนการดำเนินการโครงการ และการอบรมด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ - ดำเนินการตรวจสอบมาตรการที่มีอยู่และให้คำแนะนำแก่ทีมงาน <u>คุณสมบัติ</u> - มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นระยะเวลาอย่างน้อย ๑๐ ปี - จบการศึกษาอย่างน้อยในระดับปริญญาโท หรือเทียบเท่า - มีประกาศนียบัตรสอบผ่านการอบรมหลักสูตร Information Security Management System Auditor/Lead Auditor Course (ISO/IEC 27001 : 2022 Standard) ซึ่งได้รับรองจากสถาบัน International Register of Certificated Auditors (IRCA) และเป็น Certificate of Successful Completion	๑

/๓. นักวิจัย

ลำดับ	รายการ	จำนวน
๓	นักวิจัย <u>หน้าที่ความรับผิดชอบ</u> - ดำเนินงานตามขอบเขตของงานภายใต้คำแนะนำของผู้เชี่ยวชาญ - ดำเนินการตามรายละเอียดและขอบเขตของโครงการและฝึกอบรมที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ - รับผิดชอบการตรวจสอบช่องโหว่ทางเทคนิค (Technical Baseline: Security Vulnerability Assessment) <u>คุณสมบัติ</u> - มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นระยะเวลาอย่างน้อย ๕ ปี - จบการศึกษาอย่างน้อยในระดับปริญญาตรี หรือเทียบเท่า - มีประกาศนียบัตรสอบผ่านการอบรมหลักสูตร Information Security Management System Auditor/Lead Auditor Course (ISO/IEC 27001 : 2022 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. ขอบเขต...

๔. ขอบเขตการดำเนินงาน

ผู้รับจ้างต้องดำเนินโครงการร่วมกับเจ้าหน้าที่ของกรมการท่องเที่ยวในการปรับปรุงระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของกลุ่มเทคโนโลยีสารสนเทศ ให้เป็นไปตามมาตรฐานสากล ISO/IEC 27001 : 2022 โดยมีขอบเขตการดำเนินงาน ดังนี้

๔.๑ จัดทำแผนดำเนินงานและปฏิทินการปฏิบัติงานโครงการ ภายใน ๑๕ วัน นับถัดจากวันลงนามสัญญา

๔.๒ ดำเนินการทบทวนแนวทางและเกณฑ์การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์ ให้ตรงตามข้อกำหนดที่ระบุไว้ใน ISO/IEC 27001 : 2022 และพระราชบัญญัติความปลอดภัยไซเบอร์ พ.ศ. 2562

๔.๓ ทบทวนโครงสร้างการบริหารจัดการ และหน้าที่ความรับผิดชอบของคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) และคณะทำงานอื่นที่เกี่ยวข้อง

๔.๔ ดำเนินการทบทวนข้อมูลทะเบียนทรัพย์สิน (Asset) ในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๔.๕ จัดประชุมเชิงปฏิบัติการเพื่อดำเนินการประเมินความเสี่ยงและค้นหาแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์ จำนวนไม่น้อยกว่า 1 ครั้ง โดยมีจำนวนไม่น้อยกว่า 5 คน

๔.๖ ติดตามความคืบหน้าของการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์

๔.๗ จัดทำรายงานผลการบริหารจัดการความเสี่ยง และแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์

๔.๘ ดำเนินการทบทวน และปรับปรุงเอกสารสำคัญตามขอบเขตของระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ได้แก่ นโยบาย และขั้นตอนการปฏิบัติงาน เป็นต้น ให้สอดคล้องตามมาตรฐานสากล ISO/IEC 27001 : 2022 ถูกต้องครบถ้วน และเป็นปัจจุบัน และรองรับการขอรับรองมาตรฐาน ISO/IEC 27001 : 2022

๔.๙ ดำเนินการทบทวนรายการข้อกำหนดที่นำมาใช้ (Statement of Applicability - SOA) สำหรับการดำเนินการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) ของกรมการท่องเที่ยว ให้สอดคล้องตามมาตรฐานสากล ISO/IEC 27001 : 2022

๔.๑๐ ดำเนินการตรวจสอบช่องโหว่ทางเทคนิค (Technical Baseline : Security Vulnerability Assessment) สำหรับระบบสารสนเทศที่สำคัญ เพื่อทดสอบความปลอดภัยของสินทรัพย์และป้องกันช่องโหว่ที่สามารถเกิดขึ้น ไม่น้อยกว่า 20 IP Address

/๔.๑๑ ดำเนินการ ...

๔.๑๑ ดำเนินการทบทวนการบริหารจัดการความต่อเนื่องทางธุรกิจ (Information security aspect of business continuity management) ตามมาตรฐาน ISO/IEC 27001 : 2022 โดยการทบทวนเอกสาร จัดทำแผนความต่อเนื่องทางธุรกิจ และจัดทำการทดสอบแผนการกู้คืนระบบสารสนเทศ ตามขอบเขตที่กำหนด เป็นต้น

๔.๑๒ ดำเนินการตรวจประเมินภายใน (Internal Audit) ให้สอดคล้องกับข้อกำหนดในมาตรฐาน ISO/IEC 27001 : 2022 และพระราชบัญญัติความปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔.๑๓ ดำเนินการจัดเตรียม และทบทวนข้อมูลการดำเนินงานระบบการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) เพื่อนำเสนอต่อผู้บริหาร (Management Review)

๔.๑๔ ดำเนินการวางแผนแก้ไขเชิงป้องกันความไม่สอดคล้องที่พบในระหว่างการตรวจประเมินภายใน (Internal Audit)

๔.๑๕ ดำเนินการจัดฝึกอบรม สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์ โดยอบรมให้กับบุคลากรจำนวน ๓ ครั้ง ครั้งละไม่น้อยกว่า ๕๐ คน เพื่อให้เป็นไปตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 : 2022

๔.๑๖ ดำเนินการทบทวนแผนรับมือเหตุฉุกเฉินทางไซเบอร์ เพื่อให้เป็นไปตามพระราชบัญญัติความปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔.๑๗ ร่วมสำรวจและให้ข้อเสนอแนะ ในการออกแบบและจัดทำแผนผังห้อง Datacenter ของกรมการท่องเที่ยว ณ ศูนย์ราชการแจ้งวัฒนะ อาคาร C

๕. การรักษาข้อมูลที่เป็นความลับสำหรับหน่วยงานภายนอก

๕.๑ ขอบข่ายของข้อตกลง และคำจำกัดความข้อตกลงในสัญญาฉบับนี้จะใช้เป็นข้อกำหนด ในการเปิดเผยข้อมูลระหว่าง 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)” และมีป้ายระบุระดับชั้นความลับอย่างชัดเจนซึ่งได้แก่ข้อมูลหรือเอกสารกระบวนการดำเนินงาน ข้อมูลการดำเนินธุรกิจ เอกสารการออกแบบระบบ งานวิจัย องค์ความรู้ หรือทักษะขององค์กร Source Code สถาปัตยกรรมระบบ ข้อมูลภายในองค์กร เทคโนโลยี ที่ใช้ในองค์กร รายงานผลการดำเนินงาน แผนการตลาด แผนการเงิน รายงานการตรวจประเมินภายใน เป็นต้น

/๕.๓ การจัดการ ...

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 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 หรือข้อมูลทั้งหมดที่ได้ร้องขอ กลับมายังกรมการท่องเที่ยว 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 ๒๑๐ วัน (นับถัดจากวันลงนามในสัญญาจ้าง)

/๗. การส่งมอบ ...

๗. การส่งมอบงานและเงื่อนไขการชำระเงิน

ผู้รับจ้างจะต้องส่งมอบเอกสารและรายงานต่าง ๆ โดยมีกำหนดการส่งมอบงาน จำนวน ๒ งวด โดยแต่ละงวดจะต้องประกอบด้วย เอกสารที่จัดพิมพ์เข้าเล่ม จำนวน ๒ ชุด พร้อมบันทึกลง Flash Drive จำนวน ๒ ชุด โดยมีรายละเอียดดังนี้

งวดที่ ๑ เป็นจำนวนเงินในอัตราร้อยละ ๕๐ ของค่าจ้างเมื่อปฏิบัติงานแล้วเสร็จและส่งมอบงาน ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญาซึ่งประกอบไปด้วยเอกสาร ดังนี้

๑) แผนดำเนินงานและปฏิทินการปฏิบัติงานโครงการ

๒) รายงานการศึกษาโครงสร้างการบริหารจัดการ และหน้าที่ความรับผิดชอบของคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) และคณะทำงานอื่นที่เกี่ยวข้อง

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

๔) รายงานการทบทวนข้อมูลทะเบียนทรัพย์สิน (Asset) ในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๕) รายงานการบริหารจัดการความเสี่ยง (การประเมินความเสี่ยง และการจัดการความเสี่ยง) ด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์

๖) รายงานการทบทวนเอกสารนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)

๗) รายงานสรุปผลการประเมินความสอดคล้องตามข้อกำหนดของมาตรฐาน

๘) รายงานการทบทวนเอกสารขั้นตอนการปฏิบัติงานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)

งวดที่ ๒ เป็นจำนวนเงินในอัตราร้อยละ ๕๐ ของค่าจ้างเมื่อปฏิบัติงานแล้วเสร็จและส่งมอบงาน ภายใน ๒๑๐ วันนับถัดจากวันลงนามในสัญญา ซึ่งประกอบไปด้วยเอกสาร ดังนี้

๑) รายงานการอบรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์

๒) รายงานการตรวจสอบช่องโหว่ทางเทคนิค (Technical Baseline : Security Vulnerability Assessment)

๓) รายงานผลการทบทวนแผนการบริหารความต่อเนื่องทางธุรกิจ

๔) รายงานผลการทดสอบแผนการกู้คืนระบบสารสนเทศ

๕) รายงานผลการตรวจประเมินภายใน

๖) แผนแก้ไขเชิงป้องกันความไม่สอดคล้องที่พบในระหว่างการตรวจประเมินภายใน (Internal Audit)

๗) แผนรับมือเหตุฉุกเฉินทางไซเบอร์

/๘. หลักเกณฑ์ ...

๘. หลักเกณฑ์และสิทธิ์ในการพิจารณา

๘.๑ ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ กรมการท่องเที่ยวจะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่น

๘.๒ ในการพิจารณาผู้ชนะการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ ส่วนราชการจะใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่น (Price Performance) โดยพิจารณาให้คะแนนตามปัจจัยและน้ำหนักที่กำหนด ดังนี้

(๑) พิจารณาตามราคาที่ยื่นข้อเสนอ (Price) เป็นตัวแปรหลักบังคับ ร้อยละ ๓๐

(๒) พิจารณาตามข้อเสนอทางเทคนิค ร้อยละ ๗๐

ทั้งนี้ กรมการท่องเที่ยวจะพิจารณาคุณภาพและคุณสมบัติเพื่อเป็นประโยชน์ของหน่วยงานเป็นสำคัญ โดยพิจารณาจากเกณฑ์การให้คะแนน ๑๐๐ คะแนน ดังนี้

เกณฑ์การพิจารณา	รายละเอียด	คะแนนเต็ม
๑. ภาพรวมโครงการ	๑. ภาพรวมของโครงการ ๒. มีแผนการปฏิบัติงาน แผนงานตลอดโครงการตามขอบเขตงาน ๓. มีขั้นตอนการปฏิบัติงาน ๔. ขอบเขตของงาน <u>เกณฑ์การให้คะแนน</u> - มีเอกสารภาพรวมของโครงการ แผนการปฏิบัติงาน ของเขตของงานที่มีความละเอียด ครบถ้วน เข้าใจง่าย และมีความสอดคล้องกับการปฏิบัติงานจริง คะแนน ๑๑ – ๑๕ - มีเอกสารนำเสนอครบทุกหัวข้อตามข้อกำหนด และสอดคล้องกับการปฏิบัติงานจริง คะแนน ๖ - ๑๐ - มีการนำเสนอครบทุกหัวข้อตามข้อกำหนด คะแนน ๑ – ๕ - เอกสารที่ไม่เป็นไปตามข้อกำหนด คะแนน ๐	๑๕ คะแนน

/๒. การดำเนินงาน ...

เกณฑ์การพิจารณา	รายละเอียด	คะแนนเต็ม
๒. การดำเนินงานบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ	การดำเนินงานบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ มีวิธีการดำเนินงาน ที่ครอบคลุมการดำเนินงานดังต่อไปนี้ ๑) ทบทวนโครงสร้างการบริหารจัดการ และหน้าที่ความรับผิดชอบของคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) และคณะทำงานอื่นที่เกี่ยวข้อง ๒) จัดทำรายงานสรุปผลการประเมินความสอดคล้องตามข้อกำหนดของมาตรฐาน ๓) ทบทวนข้อมูลทะเบียนทรัพย์สิน (Asset) ๔) การทบทวน และปรับปรุงเอกสารสำคัญตามขอบเขตของระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ๕) ตรวจสอบช่องโหว่ทางเทคนิค ๖) ทบทวนการบริหารจัดการความต่อเนื่องทางธุรกิจ ๗) ตรวจประเมินภายใน ๘) จัดเตรียมข้อมูลเพื่อนำเสนอต่อผู้บริหาร ๙) จัดเตรียมเนื้อหา เพื่ออบรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์ ๑๐) คัดเลือกและจัดทำแผนรับมือเหตุฉุกเฉินทางไซเบอร์ <u>เกณฑ์การให้คะแนน</u> - วิธีการดำเนินงานที่ครอบคลุมขอบเขตการดำเนินงาน และเสนอวิธีการดำเนินงานในแต่ละขั้นตอนครบถ้วน คะแนน ๒๙ – ๓๕ - วิธีการดำเนินงานที่ครอบคลุมขอบเขตการดำเนินงาน และเสนอวิธีการดำเนินงานครอบคลุมบางหัวข้อ คะแนน ๒๒ – ๒๘ - วิธีการดำเนินงานที่ครอบคลุมขอบเขตการดำเนินงาน และเสนอวิธีการดำเนินงานบางหัวข้อและน้อยกว่าที่กำหนด คะแนน ๑๕ – ๒๑ - วิธีการดำเนินงานที่ครอบคลุมขอบเขตการดำเนินงาน และเสนอวิธีการดำเนินงานมีไม่ครบถ้วน และไม่เป็นไปตามข้อกำหนด คะแนน ๑ – ๗	๓๕ คะแนน

/ -วิธีการดำเนินงาน ...

เกณฑ์การพิจารณา	รายละเอียด	คะแนนเต็ม
	- วิธีการดำเนินงานที่ครอบคลุมขอบเขตการดำเนินงาน และเสนอวิธีการดำเนินงานไม่ครบถ้วนตามข้อที่กำหนด คะแนน ๘ – ๑๔ - เอกสารที่ไม่เป็นไปตามข้อกำหนด คะแนน ๐	
๓. การบริหารจัดการความเสี่ยง	การบริหารจัดการความเสี่ยง มีวิธีการบริหารจัดการความเสี่ยง ที่ครอบคลุมการดำเนินงานดังต่อไปนี้ ๑) ทบทวนแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์ ๒) ระบุความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์ ๓) ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์ ๔) จัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์ ๕) จัดทำรายงานผลการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์ ๖) จัดทำแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยไซเบอร์ <u>เกณฑ์การให้คะแนน</u> - วิธีการดำเนินงานที่ครอบคลุมขอบเขตการดำเนินงาน และเสนอวิธีการดำเนินงานในแต่ละขั้นตอนครบถ้วน คะแนน ๒๙ – ๓๕ - วิธีการดำเนินงานที่ครอบคลุมขอบเขตการดำเนินงาน และเสนอวิธีการดำเนินงานครอบคลุมบางหัวข้อ คะแนน ๒๒ – ๒๘ - วิธีการดำเนินงานที่ครอบคลุมขอบเขตการดำเนินงาน และเสนอวิธีการดำเนินงานบางหัวข้อและน้อยกว่าที่กำหนด คะแนน ๑๕ – ๒๑ - วิธีการดำเนินงานที่ครอบคลุมขอบเขตการดำเนินงาน และเสนอวิธีการดำเนินงานมีไม่ครบถ้วน และไม่เป็นไปตามข้อกำหนด คะแนน ๑ – ๗	๓๐ คะแนน

/ -วิธีการดำเนินงาน ...

เกณฑ์การพิจารณา	รายละเอียด	คะแนนเต็ม
	- วิธีการดำเนินงานที่ครอบคลุมขอบเขตการดำเนินงาน และเสนอวิธีการดำเนินงานไม่ครบถ้วนตามข้อที่กำหนด คะแนน ๘ – ๑๔ - เอกสารที่ไม่เป็นไปตามข้อกำหนด คะแนน ๐	
๔. การบริหารจัดการความด้านความมั่นคงปลอดภัยทางไซเบอร์	การบริหารจัดการความด้านความมั่นคงปลอดภัยทางไซเบอร์ <u>เกณฑ์การให้คะแนน</u> - วิธีการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) เช่น กระบวนการ วิธีการปฏิบัติเพื่อป้องกันและรับมือ คะแนน ๕ – ๑๕ - วิธีการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) เช่น กระบวนการ วิธีการปฏิบัติเพื่อป้องกันและรับมือ เสนอไม่ครบถ้วน คะแนน ๑ – ๕ - ไม่มีวิธีการ คะแนน ๐	๑๕ คะแนน
๕. ข้อเสนอพิเศษ	ข้อเสนอพิเศษที่ทำให้โครงการดำเนินการได้ดียิ่งขึ้นหรือเพิ่มประสิทธิภาพในการทำงานของระบบ	๕ คะแนน

๙. อัตราค่าปรับ

อัตราค่าปรับตามแบบสัญญาจ้าง จะกำหนดในอัตราร้อยละ ๐.๑ ของราคางานที่ยังไม่ได้รับมอบต่อวัน

๑๐. การรับประกันความชำรุดบกพร่องของงานที่เกิดขึ้น

ภายในระยะเวลาไม่น้อยกว่า....๑....เดือน นับถัดจากวันที่กรมการท่องเที่ยวได้รับมอบงาน โดยผู้รับจ้างต้องรีบจัดการซ่อมแซมแก้ไขให้ใช้การได้ดีดังเดิมภายใน...๓...วัน นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง

๑๑. ราคากลาง

ราคากลาง (ราคาอ้างอิงฯ) เป็นเงินทั้งสิ้น ๙๙๕,๑๐๐ บาท (เก้าแสนเก้าหมื่นห้าพันหนึ่งร้อยบาทถ้วน)

๑๒. วงเงินในการจัดหา

ค่าใช้จ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๖ เป็นเงิน ๑,๐๐๐,๐๐๐ บาท (หนึ่งล้านบาทถ้วน)