งานจ้างที่ปรึกษาจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร ของ ทอท. สำหรับระบบโครงสร้างพื้นฐานสำคัญและกระบวนการที่รองรับการทำงานระบบบริหารทรัพยากรองค์กร ตามมาตรฐาน ISO/IEC 27001

1. บทนำ ข้อมูลเกี่ยวกับโครงการ

บริษัท ท่าอากาศยานไทย จำกัด (มหาชน) (ทอท.) เป็นหน่วยงานที่รับผิดชอบการดำเนินธุรกิจด้านการให้บริการท่าอากาศยาน โดยให้บริการแก่ผู้โดยสาร สายการบิน ผู้ประกอบการ หน่วยงานภาครัฐ และหน่วยงานต่างๆ ที่เกี่ยวข้อง ซึ่งมีเป้าหมายในการให้บริการธุรกิจเพื่อตอบสนองต่อความต้องการของผู้ใช้บริการและดำเนินการธุรกิจได้อย่างต่อเนื่อง รวมทั้ง ทอท.เป็นหน่วยงานหนึ่งที่อยู่ภายใต้การกำกับดูแลของหน่วยงานภาครัฐที่ต้องปฏิบัติตามกฎหมายด้านเทคโนโลยีสารสนเทศของประเทศไทย เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. มีความมั่นคงปลอดภัย สามารถดำเนินงานได้ต่อเนื่องอย่างมีประสิทธิภาพ สามารถป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และการถูกคุกคามจากภัยต่างๆ ได้ รวมทั้งเพื่อให้ผู้ใช้บริการระบบทางเทคโนโลยีสารสนเทศและการสื่อสารทั้งภายในและภายนอก ทอท.เกิดความเชื่อมั่น ตลอดจนสร้างความตระหนักถึงความสำคัญต่อความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ปัจจุบัน ทอท. ได้จัดทำระบบบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร (Information Security Management System: ISMS) ที่เป็นไปตามมาตรฐานสากล ISO/IEC 27001 และได้รับประกาศนียบัตรรับรองระบบบริหารการจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. ตามมาตรฐาน ISO/IEC 27001: 2013 โดยมีขอบเขตครอบคลุมระบบสนับสนุนและสิ่งอำนวยความสะดวก (Facility) ของห้องศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง และอยู่ระหว่างการตรวจรับรองอย่างต่อเนื่องซึ่งจะสิ้นสุดในปี 2563 นั้น

ทอท. ได้เห็นถึงความสำคัญในการนำมาตรฐานมาประยุกต์ใช้ในการบริหารงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร โดยขยายขอบเขตระบบบริหารจัดการความมั่นคงฯจากเดิม ให้ครอบคลุมระบบโครงสร้างพื้นฐานที่สำคัญที่สนับสนุนระบบบริหารทรัพยากรองค์กร ดังนั้น ทอท. จึงมีความจำเป็นต้องจัดจ้างที่ปรึกษาที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทบทวนและจัดทำระบบบริหารจัดการความมั่นคงฯ ให้เป็นไปตามมาตรฐาน ISO/IEC 27001 ให้ครอบคลุมขอบเขตที่ ทอท. กำหนด

2. วัตถุประสงค์

ทอท. มีความประสงค์จัดจ้างที่ปรึกษาจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร ของ ทอท. สำหรับระบบโครงสร้างพื้นฐานสำคัญที่สนับสนุนระบบบริหารทรัพยากรองค์กรตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด จำนวน 1 งาน

3. เป้าหมาย

ทอท. สามารถรักษาระบบการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. ได้อย่างต่อเนื่อง เพื่อต่ออายุใบประกาศนียบัตรรับรองตามมาตรฐาน ISO/IEC 27001 โดยขยายขอบเขตครอบคลุมระบบโครงสร้างพื้นฐานสำคัญที่สนับสนุนระบบบริหารทรัพยากรองค์กร และได้รับการตรวจรับรองจากผู้ตรวจประเมินรับรองภายนอก (Certify Body : CB)

4. ขอบเขตการดำเนินงาน

ที่ปรึกษาฯ ต้องจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด โดยมีขอบเขตการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของห้องศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองของ ทอท.ในส่วนที่เกี่ยวข้องกับระบบสนับสนุนและสิ่งอำนวยความสะดวก (Facility) และระบบโครงสร้างพื้นฐานที่สำคัญที่สนับสนุนระบบบริหารทรัพยากรองค์กร จำนวน 2 ระบบ คือ ระบบจัดซื้อจัดจ้าง (Material Management: MM) และ ระบบงานซ่อมบำรุง (Plant Maintenance: PM) โดยต้องดำเนินการอย่างน้อย ดังนี้

4.1 เตรียมความพร้อม และดำเนินการเริ่มโครงการโดยประกอบด้วยแผนการดำเนินงานอย่างน้อย ดังนี้

4.1.1 จัดทำแผนการดำเนินงานโครงการ (Project Plan) เพื่อแสดงรายละเอียดของแผนการดำเนินงานที่เกี่ยวข้องกับโครงการทั้งหมด รวมทั้งโครงสร้างทีมงาน

4.1.2 จัดทำแผนการประชุม ฝึกอบรม สัมมนา หรือให้ความรู้ พร้อมหัวข้อในการให้ความรู้ รวมถึงรูปแบบการดำเนินการตามข้อ 4.10 เพื่อเตรียมความพร้อมและสร้างความรู้ความเข้าใจในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) ตามมาตรฐานสากล ISO/IEC 27001 เวอร์ชั่นล่าสุด ให้แก่ ทอท.

4.1.3 จัดทำแผนการดำเนินงานเพื่อนำระบบ ISMS ตามข้อ 4.5 ไปปฏิบัติงานจริง

4.1.4 จัดทำแผนการดำเนินงานระบบ ISMS เพื่อขอการรับรองตามมาตรฐาน ISO/IEC 27001

4.2 ศึกษา ...

4.2 ศึกษา ทบทวน วิเคราะห์การบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร ของ ทอท.ในปัจจุบันประกอบด้วยรายละเอียดที่เกี่ยวข้องอย่างน้อย ดังนี้

4.2.1 บริบทองค์กร สภาพแวดล้อมขององค์กร โครงสร้างองค์กร กฎระเบียบข้อบังคับของ ทอท.

4.2.2 นโยบายและแนวปฏิบัติ ข้อปฏิบัติ ขั้นตอนปฏิบัติ มาตรการ คู่มือการปฏิบัติงาน/ขั้นตอน (SOP หรือ Procedure) ตลอดจนกระบวนการปฏิบัติงานที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของ ทอท.

4.2.3 การบริหารจัดการความเสี่ยง ระบบบริหารความต่อเนื่องทางธุรกิจของ ทอท.(BCM) แผนความต่อเนื่องทางธุรกิจ (BCP) และแผนเตรียมความพร้อมกรณีฉุกเฉิน ในส่วนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสาร (หากมี)

4.2.4 กฎหมายเทคโนโลยีสารสนเทศของประเทศไทยที่เกี่ยวข้อง

4.3 ประเมินวิเคราะห์สถานภาพการดำเนินการมาตรฐานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.ในปัจจุบันตามผลการศึกษาในข้อ 4.2 เทียบกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC 27001 เวอร์ชั่นล่าสุด (Gap Analysis) (หากมี) พร้อมจัดทำรายงานผลการวิเคราะห์ช่องว่าง (Gap Analysis Report) และนำเสนอแก่ผู้ที่เกี่ยวข้อง

4.4 จัดทำระบบบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.ให้เป็นไปตามบริบทของ ทอท.และผลการวิเคราะห์ช่องว่าง (Gap Analysis) รวมทั้งให้สอดคล้องกับกฎระเบียบ และข้อบังคับของ ทอท. กฎหมายเทคโนโลยีสารสนเทศของประเทศไทย และเป็นไปตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด โดยดำเนินการอย่างน้อย ดังนี้

4.4.1 ทบทวน / จัดทำโครงสร้างและขอบเขตการบริหารจัดการระบบ ISMS ของ ทอท.

4.4.2 ทบทวน / กำหนดบทบาทหน้าที่ความรับผิดชอบและคุณสมบัติของคณะกรรมการ/คณะทำงาน/ส่วนงานที่เกี่ยวข้องตามโครงสร้างระบบ ISMS ของ ทอท.

4.4.3 จัดทำ / ทบทวนแนวทางการประเมินความเสี่ยง กระบวนการประเมินความเสี่ยง เกณฑ์การประเมินความเสี่ยง โอกาสและผลกระทบการประเมินความเสี่ยง และกระบวนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.ให้สอดคล้องหรือเชื่อมโยงกับรายละเอียดตามข้อ 4.2.3

4.4.4 ทบทวน / กำหนดวิธีปฏิบัติการดำเนินการของระบบบริหารจัดการ (Management System) ของระบบ ISMS อย่างน้อยดังนี้

(1) การนำองค์กรและความมุ่งมั่นของผู้บริหาร (Leadership and Commitment)

(2) การจัดการด้านทรัพยากร (Resources)

(3) การตรวจติดตามภายใน (Internal Audit)

(4) การทบทวนโดยฝ่ายบริหาร (Management Reviews)

(5) การปรับปรุง ...

(5) การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)

(6) การปฏิบัติการแก้ไข (Corrective Action)

(7) การจัดการเอกสารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Documented Information for ISMS)

4.5 ทอท. ต้องนำระบบ ISMS ไปปฏิบัติงานได้จริง โดยมีรายละเอียดอย่างน้อย ดังนี้

4.5.1 สร้างความเข้าใจให้กับผู้เกี่ยวข้องให้สามารถดำเนินงานได้ตามกระบวนการของระบบ ISMS ในการนำเอาระบบ ISMS ไปปฏิบัติงานจริง

4.5.2 ติดตาม ตรวจสอบ วิเคราะห์ และสรุปผลการนำเอาระบบ ISMS ไปปฏิบัติงานจริง

4.5.3 รายงานสรุปปัญหาที่พบจากการนำระบบ ISMS ไปปฏิบัติงานจริง พร้อมเสนอแนะการแก้ไขปัญหาที่พบให้เหมาะสมกับการปฏิบัติงานจริง

4.6 ทบทวนและจัดทำเอกสารต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นปัจจุบัน อย่างน้อย ดังนี้

4.6.1 นโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร (AOT ICT Security Policy) นโยบายสนับสนุนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Supporting Policy) แนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Guideline) ให้สอดคล้องตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และ ฉบับที่ 2 พ.ศ. 2556 และข้อกำหนดตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด

4.6.2 เอกสารต่างๆ และแบบประเมินประกอบการพิจารณา รวมทั้งให้การสนับสนุนการตรวจประเมินและปรับปรุงแก้ไข นโยบายฯ และนโยบายสนับสนุนฯ และแนวทางการปฏิบัติฯ ตามข้อ 4.6.1 ตามขั้นตอนที่ ทอท. กำหนด

4.6.3 ข้อปฏิบัติ/มาตรการ/คู่มือการปฏิบัติงานหรือขั้นตอนการปฏิบัติงาน (SOP หรือ Procedure) หรือกระบวนการปฏิบัติงานหรือเอกสารอื่นใดที่ต้องดำเนินการให้เป็นไปตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด และสอดคล้องตามที่กำหนดในนโยบายฯ และนโยบายและแนวปฏิบัติฯ ตามข้อ 4.6.1

4.7 ปรับปรุงกระบวนการและเอกสารที่เกี่ยวข้องกับระบบ ISMS ของ ทอท.ให้เป็นไปตามมาตรการด้านการรักษาความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด อย่างน้อยตามภาคผนวก ก

4.8 ดำเนินการ ...

4.8 ดำเนินการตามขั้นตอน กระบวนการดำเนินงานและจัดทำเอกสารที่เกี่ยวข้องกับระบบ ISMS ให้เป็นไปตามมาตรฐาน ISO/IEC 27001 ตามขอบเขตการดำเนินงานที่ ทอท. กำหนด เพื่อให้ ทอท.ได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด โดยต้องดำเนินการอย่างน้อย ดังนี้

4.8.1 กำหนดกระบวนการดำเนินงานระบบ ISMS เพื่อขอการรับรองตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด ตามขอบเขตการดำเนินงานที่ ทอท. กำหนด และสร้างความเข้าใจให้กับผู้เกี่ยวข้องให้สามารถดำเนินงานได้ตามกระบวนการ

4.8.2 ตรวจประเมินสถานภาพด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามขอบเขตการดำเนินงานที่ ทอท.กำหนด เทียบกับมาตรการการรักษาความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด

4.8.3 ศึกษา วิเคราะห์ และดำเนินการกำหนดขอบเขตการรับรองตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด เป็นอย่างน้อยและได้รับความเห็นชอบจาก ทอท.

4.8.4 จัดทำขั้นตอนการบริหารจัดการทรัพย์สิน และบัญชีรายการทรัพย์สิน (Asset Inventory) ตามขอบเขตที่ ทอท. กำหนด

4.8.5 ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Assessment) ภายใต้ขอบเขตที่กำหนด ตามแนวทางการประเมินความเสี่ยงตามข้อ 4.4.3

4.8.6 ตรวจประเมินความเสี่ยงทางเทคนิค (Vulnerability Assessment) ในส่วนที่เกี่ยวข้องกับขอบเขตที่กำหนดพร้อมทั้งจัดทำรายงานสรุปผลการตรวจประเมินและให้ข้อเสนอแนะการแก้ไขปิดช่องโหว่ที่ตรวจพบ

4.8.7 คัดเลือกวิธีปฏิบัติและมาตรการควบคุมการรักษาความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด เพื่อจัดการความเสี่ยง

4.8.8 จัดทำแผนจัดการความเสี่ยง (Risk Treatments Plan) และเสนอแนะแนวทางในการปฏิบัติและวัดผลการดำเนินงานตามแผนจัดการลดความเสี่ยง

4.8.9 สรุปรายการหรือจัดทำหรือปรับปรุง เอกสารนโยบาย/มาตรการ/คู่มือการปฏิบัติงานหรือ ขั้นตอนปฏิบัติงาน (SOP หรือ Procedure) หรือเอกสารอื่นใด รวมทั้งกระบวนการปฏิบัติงาน ที่ต้องดำเนินการภายใต้ขอบเขตที่กำหนด

4.8.10 จัดทำเอกสารสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (Statement of Applicability : SOA) ที่เลือกใช้ในระบบ ISMS ตามขอบเขตที่กำหนด

4.8.11 กำหนดวิธีการวัดประสิทธิผล (Effectiveness Measurement) สำหรับกระบวนการและมาตรการควบคุมที่สำคัญในการดำเนินงานตามขอบเขตระบบ ISMS ที่กำหนด

4.8.12 กำหนดวิธีการจัดการเอกสารสำหรับระบบ ISMS ของ ทอท.ตามขอบเขตที่กำหนด

4.8.13 ทบทวน ...

4.8.13 ทบทวน / จัดทำแผนรองรับความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ตามขอบเขตที่กำหนด ให้สอดคล้องหรือเชื่อมโยงกับแผน BCP ของ ทอท.ที่มีส่วนเกี่ยวข้องกับขอบเขตที่กำหนด

4.8.14 ติดตามและรายงานการวัดประสิทธิผลด้านความมั่นคงปลอดภัยของกระบวนการและมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศตามเกณฑ์วิธีการวัดประสิทธิผลที่กำหนด

4.8.15 ให้คำปรึกษาและร่วมกับทีมงานตรวจสอบภายในของ ทอท.(Internal Audit) ในการดำเนินการตรวจสอบภายในระบบ ISMS ของ ทอท.ตามขอบเขตที่กำหนด ให้เป็นไปตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด และกรณีตรวจพบข้อบกพร่องหรือความไม่สอดคล้องกับข้อกำหนดตามมาตรฐาน ISO/IEC 27001 ที่ปรึกษาฯ ต้องให้คำแนะนำในการติดตามแก้ไขข้อบกพร่อง/ความไม่สอดคล้องนั้น

4.8.16 ติดตาม ตรวจสอบ วิเคราะห์และสรุปรายงานผลการดำเนินงานระบบ ISMS ของ ทอท.พร้อมทั้งให้คำปรึกษาและข้อเสนอแนะการปรับปรุงระบบ ISMS ของ ทอท.ให้เหมาะสมกับการปฏิบัติงานจริง

4.8.17 จัดเตรียมในส่วนความรับผิดชอบของผู้บริหารเพื่อพิจารณาทบทวนผลปฏิบัติในการพัฒนาและดำเนินงานระบบ ISMS ของ ทอท.(Management Review of the ISMS) โดยครอบคลุมหัวข้อการจัดเตรียมข้อมูลสำหรับการประชุม และจัดทำรายงานการประชุมสำหรับการปรับปรุงระบบ ISMS ของ ทอท.

4.8.18 ให้คำปรึกษา จัดเตรียมและรวบรวมเอกสารหลักฐานต่างๆ เพื่อยื่นตรวจสอบระบบ ISMS ของ ทอท. ให้ได้รับการรับรองตามมาตรฐานISO/IEC 27001 เวอร์ชั่นล่าสุด ตามขอบเขตที่กำหนด

4.8.19 เตรียมความพร้อมในการรับการตรวจประเมินระบบ ISMS ของ ทอท.ตามขอบเขตที่กำหนด (Pre-Assessment) รวมทั้งให้ข้อเสนอแนะ สนับสนุนการดำเนินการและปรับปรุงเอกสาร หรือกระบวนการดำเนินงาน เพื่อเตรียมความพร้อมให้กับ ทอท.ก่อนการยื่นตรวจสอบระบบ ISMS ของ ทอท.จากผู้ตรวจประเมินรับรองภายนอก (Certify Body: CB)

4.8.20 นำเสนอผู้ตรวจรับรองมาตรฐาน ISO/IEC 27001 ที่มีชื่อเสียงและเป็นที่ยอมรับในระดับสากล เพื่อให้ ทอท.พิจารณาคัดเลือกสำหรับดำเนินการตรวจสอบระบบ ISMS ของ ทอท.ทั้งนี้ ทอท.สามารถเลือกผู้ตรวจรับรองฯ รายอื่นนอกเหนือจากที่ ที่ปรึกษาฯ เสนอได้ โดยที่ปรึกษาฯ ต้องเป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมดในการตรวจประเมินระบบ ISMS จนกว่า ทอท.จะผ่านและได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด

4.8.21 ที่ปรึกษาฯ ต้องให้คำปรึกษา แนะนำ สนับสนุนการดำเนินงานหรือดำเนินการในส่วนที่เกี่ยวข้องเพื่อให้ ทอท.ผ่านการตรวจประเมินและได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด ตามขอบเขตที่กำหนด

4.8.22 ประชุมสรุปผลการตรวจสอบระบบ ISMS ของ ทอท.พร้อมทั้งให้ข้อเสนอแนะในการปรับปรุงระบบ ISMS ของ ทอท.ตามผลการตรวจสอบของผู้ตรวจรับรองมาตรฐาน ISO/IEC 27001

4.9 ให้คำปรึกษา ...

4.9 ให้คำปรึกษา แนะนำ และดำเนินการในส่วนที่เกี่ยวข้องสำหรับการตรวจรับรองการรักษามาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด (Surveillance Audit) อย่างต่อเนื่อง โดยที่ปรึกษาฯ ต้องรับผิดชอบค่าใช้จ่ายทั้งหมด จนกว่า ทอท.จะผ่านการตรวจรับรองการรักษามาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุดของทุกปี เป็นระยะเวลา 2 ปี นับจากวันที่ ทอท.ได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้

4.9.1 ทบทวนปรับปรุงเอกสารนโยบาย กระบวนการปฏิบัติงาน/มาตรการ/คู่มือการปฏิบัติงาน หรือขั้นตอนการปฏิบัติงาน (SOP หรือ Procedure) หรือเอกสารอื่นใด ภายใต้ขอบเขตการตรวจรับรองฯ ให้สอดคล้องและเหมาะสมกับการปฏิบัติงานจริง

4.9.2 ติดตาม ตรวจสอบและวิเคราะห์การดำเนินงานและการปฏิบัติตามระบบ ISMS ของ ทอท.พร้อมทั้งให้ข้อเสนอแนะและสนับสนุนการปรับปรุงการดำเนินงานระบบ ISMS ของ ทอท.ให้สามารถดำเนินการได้อย่างต่อเนื่องและเป็นไปตามข้อกำหนดมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด

4.9.3 ตรวจประเมินความเสี่ยงทางเทคนิค (Vulnerability Assessment) ในส่วนที่เกี่ยวข้องกับขอบเขตการตรวจรับรองฯ พร้อมทั้งจัดทำรายงานสรุปผลการตรวจประเมินและให้ข้อเสนอแนะการแก้ไขปิดช่องโหว่ที่ตรวจพบ

4.9.4 ประเมินความเสี่ยง ทบทวน และปรับปรุงแผนการจัดการความเสี่ยง

4.9.5 ร่วมดำเนินการตรวจสอบภายใน และให้ข้อเสนอแนะในการปรับปรุงตามผลการตรวจสอบ

4.9.6 เตรียมการและประชุมร่วมกับผู้บริหารตามระบบ ISMS ของ ทอท.

4.9.7 นำเสนอผู้ตรวจรับรองมาตรฐาน ISO/IEC 27001 ที่มีชื่อเสียงและเป็นที่ยอมรับในระดับสากลเพื่อให้ ทอท.พิจารณาคัดเลือกสำหรับดำเนินการตรวจรับรองการรักษามาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด ทั้งนี้ทอท.สามารถเลือกผู้ตรวจรับรองฯ รายอื่นนอกเหนือจากที่ ที่ปรึกษาฯ เสนอได้

4.9.8 ให้คำปรึกษา แนะนำ เตรียมการ จัดเตรียมเอกสารหลักฐาน และสนับสนุนการตรวจประเมิน Surveillance เพื่อให้ ทอท.ผ่านการตรวจรับรองการรักษามาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด (Surveillance Audit)

4.9.9 ประชุมสรุปผลการตรวจรับรองการรักษามาตรฐานระบบ ISMS ของ ทอท.พร้อมทั้งข้อเสนอแนะในการปรับปรุงระบบ ISMS ของ ทอท.ตามผลการตรวจสอบของผู้ตรวจรับรองมาตรฐาน ISO/IEC 27001

4.10 จัดประชุม ...

4.10 จัดประชุม ฝึกอบรม สัมมนา หรือให้ความรู้ พร้อมเอกสารประกอบการดำเนินการ เพื่อเตรียมความพร้อมและให้ความรู้ในการพัฒนาระบบ ISMS ของ ทอท. รวมถึงการสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยที่ปรึกษาฯ ต้องจัดทำรายละเอียดการประชุม หรือ ฝึกอบรมซึ่งประกอบด้วย หัวข้อการให้ความรู้ ระยะเวลา จำนวนผู้เข้าร่วม และส่วนงานที่เกี่ยวข้องให้ ทอท.พิจารณาให้ความเห็นชอบก่อนเริ่มดำเนินการ ทั้งนี้ ต้องดำเนินการให้ความรู้แต่ละหัวข้อ/หลักสูตรอย่างน้อยปีละ 1 ครั้ง ตลอดอายุสัญญา โดยที่ปรึกษาฯ ต้องเป็นผู้รับผิดชอบ ค่าใช้จ่ายทั้งหมดในการดำเนินการ โดยมีหัวข้อ/หลักสูตรอย่างน้อยดังนี้

4.10.1 การพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศและข้อกำหนดตามมาตรฐาน ISO/IEC 27001 เวอร์ชันล่าสุด สำหรับคณะกรรมการ ISMS คณะทำงาน ISMS

4.10.2 บทบาทของผู้เกี่ยวข้องในการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศและข้อกำหนดตามมาตรฐาน ISO/IEC 27001 เวอร์ชันล่าสุด สำหรับส่วนงาน ทอท.ที่เกี่ยวข้องตามขอบเขตการขอใบรับรอง

4.10.3 การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) สำหรับคณะทำงาน ISMS และส่วนงาน ทอท.ที่เกี่ยวข้องตามขอบเขต ISMS ของ ทอท.

4.10.4 การจัดทำระบบความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 (Information Security Lead Implementer) สำหรับคณะทำงาน ISMS และส่วนงาน ทอท.ที่เกี่ยวข้องตามขอบเขต ISMS ของ ทอท.

4.10.5 การดำเนินการตรวจสอบตามมาตรฐาน ISO/IEC 27001 (Information Security Management System Auditor/Lead Auditor) สำหรับคณะผู้ตรวจสอบ ISMS

4.10.6 การสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศสำหรับผู้บริหาร และพนักงาน ทอท. ทั้ง 7 แห่ง ได้แก่ สำนักงานใหญ่ ท่าอากาศยานดอนเมือง ท่าอากาศยานเชียงใหม่ ท่าอากาศยานภูเก็ต ท่าอากาศยานหาดใหญ่ ท่าอากาศยานแม่ฟ้าหลวงเชียงราย และท่าอากาศยานสุวรรณภูมิ

4.11 จัดทำสื่อประชาสัมพันธ์โครงการ เพื่อสื่อสารและเผยแพร่ข้อมูลข่าวสารหรือความรู้เกี่ยวกับโครงการให้พนักงาน ทอท. ได้รับทราบในรูปแบบสื่ออิเล็กทรอสิกส์อย่างน้อยปีละ 4 ชิ้น

5. บุคลากร ...

5. บุคลากรที่ต้องการ

ที่ปรึกษาฯ ต้องมีบุคลากรที่มีความรู้ ความชำนาญ และประสบการณ์ในลักษณะงานที่เกี่ยวข้องในแต่ละตำแหน่งอย่างน้อย ดังนี้

บุคลากร	วุฒิการศึกษา	ประสบการณ์ / คุณสมบัติ	ประสบการณ์การทำงานอย่างน้อย (ปี)[1]
5.1 ผู้จัดการโครงการ จำนวนอย่างน้อย 1 คน	ไม่ต่ำกว่าระดับปริญญาตรีทุกสาขา	(1) เป็นผู้จัดการโครงการ [2] ด้านความมั่นคงปลอดภัยสารสนเทศ หรือเทียบเท่า	11
		(2) ประกาศนียบัตรสากลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ อย่างน้อย 1 ใบ	-
5.2 ผู้เชี่ยวชาญด้านการจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศจำนวนอย่างน้อย 1 คน	ไม่ต่ำกว่าระดับปริญญาตรีสาขาเทคโนโลยีสารสนเทศและการสื่อสารหรือสาขาที่เกี่ยวข้อง	(1) ด้านการจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ <u>หรือ</u> เทียบเท่า	11
		(2) ประกาศนียบัตรสากลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ อย่างน้อย 1 ใบ เช่น CISA (Certified Information System Auditor), CISSP (Certified Information System Security Professional), CISM (Certified Information Security Management) , (IRCA) ISO/IEC 27001 Information security management System Audit/Lead Auditor เป็นต้น	-

5.3 ผู้เชี่ยวชาญ...

บุคลากร	วุฒิการศึกษา	ประสบการณ์ / คุณสมบัติ	ประสบการณ์การทำงานอย่างน้อย (ปี)[1]
5.3 ผู้เชี่ยวชาญด้านการตรวจประเมินรับรองระบบการจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ จำนวนอย่างน้อย 1 คน	ไม่ต่ำกว่าระดับปริญญาตรีสาขาเทคโนโลยีารสนเทศและการสื่อสารหรือสาขาที่เกี่ยวข้อง	(1) เป็นผู้ตรวจประเมินภายใน (Internal Audit) หรือเป็นผู้ตรวจประเมินรับรองระบบการจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ(Certify Body : CB) หรือสนับสนุนการตรวจประเมินรับรองตามมาตรฐาน ISO/IEC 27001 จำนวนไม่น้อยกว่า 2 โครงการ	11
		(2) ประกาศนียบัตรสากลที่เกี่ยวข้องกับการตรวจประเมินรับรองมาตรฐานด้านจัดการ การรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System Auditor ตามมาตรฐาน ISO27001) อย่างน้อย 1 ใบ เช่น CISA (Certified Information System Auditor, IRCA ISO/IEC 27001:2013 Lead Auditor หรือสอบผ่านการอบรมหลักสูตร ด้านการตรวจสอบระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System) ซึ่งได้รับการรับรองจากสถาบัน IRCA (International Register of Certificated Auditors) ในระดับ Provisional เป็นต้น	-

5.4 ที่ปรึกษา ...

บุคลากร	วุฒิการศึกษา	ประสบการณ์ / คุณสมบัติ	ประสบการณ์การทำงานอย่างน้อย (ปี)[1]
5.4 ที่ปรึกษาด้านวิศวกรรมระบบศูนย์คอมพิวเตอร์ จำนวนอย่างน้อย 1 คน	ไม่ต่ำกว่าระดับปริญญาตรีสาขาเทคโนโลยีสารสนเทศและการสื่อสารหรือสาขาที่เกี่ยวข้อง	(1) ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของระบบภายในห้องศูนย์คอมพิวเตอร์ จำนวนไม่น้อยกว่า 2 โครงการ	5
		(2) ประกาศนียบัตรสากลที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ อย่างน้อย 1 ใบ เช่น CompTIA Security+, CompTIA CySA+, CompTIA CASP, CompTIA Pentest+, PECB Lead Implementer 27001,PECB Lead Auditor 27001,IRCA Lead Auditor 27001 เป็นต้น	
5.5 ที่ปรึกษาด้านระบบสื่อสารอิเล็กทรอนิกส์, ระบบคอมพิวเตอร์และระบบเครือข่ายจำนวนอย่างน้อย 1 คน	ไม่ต่ำกว่าระดับปริญญาตรีสาขาเทคโนโลยีสารสนเทศและการสื่อสารหรือสาขาที่เกี่ยวข้อง	ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับระบบสื่อสารอิเล็กทรอนิกส์ ระบบคอมพิวเตอร์ และระบบเครือข่าย จำนวน อย่างน้อย 2 โครงการ	5

5.6 ที่ปรึกษา...

บุคลากร	วุฒิการศึกษา	ประสบการณ์ / คุณสมบัติ	ประสบการณ์การทำงานอย่างน้อย (ปี)[1]
5.6 ที่ปรึกษาด้านระบบสารสนเทศ จำนวนอย่างน้อย 1 คน	ไม่ต่ำกว่าระดับปริญญาตรีสาขาเทคโนโลยีสารสนเทศและการสื่อสารหรือสาขาที่เกี่ยวข้อง	(1) ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับระบบสารสนเทศจำนวนไม่น้อยกว่า 2 โครงการ	5
		(2) ประกาศนียบัตรสากลที่เกี่ยวข้องกับการตรวจสอบความความมั่นคงปลอดภัยสารสนเทศอย่างน้อย 1 ใบ เช่น GIAC Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), CompTIA Pentest+, Certified Ethical Hacker(CEH), EC-Council Certified Security Analyst (ECSA), PECB Lead Implementer 27001,PECB Lead Auditor 27001,IRCA Lead Auditor 27001 เป็นต้น	

หมายเหตุ

(1) ประสบการณ์การทำงาน (ปี) หมายถึง ประสบการณ์ในการทำงานด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) โดยจะนับจำนวนเวลาตามระยะเวลาที่ทำงานตามปฏิทิน

(2) เป็นผู้จัดการโครงการ หรือเทียบเท่า หมายถึง ตำแหน่งต่างๆ ที่ใกล้เคียง ได้แก่ ผู้จัดการโครงการร่วม หัวหน้าคณะที่ปรึกษาด้านเทคโนโลยีสารสนเทศและการสื่อสาร ผู้บริหารโครงการ ผู้อำนวยการโครงการ หัวหน้าทีมงาน เป็นต้น

(3) การพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ หรือเทียบเท่า หมายถึง การดำเนินงานที่มีลักษณะใกล้เคียงได้แก่ การเป็นที่ปรึกษาในการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ หรือดำเนินงานพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ หรือเป็นที่ปรึกษาการตรวจประเมินรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ หรือสนับสนุนการตรวจประเมินรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

6. ระยะเวลาการดำเนินงาน

ระยะเวลาดำเนินงานให้แล้วเสร็จตามเป้าหมายภายใน 1,230 วัน นับถัดจากวันลงนามในสัญญา รวมระยะเวลาการตรวจรับของคณะกรรมการตรวจรับพัสดุของ ทอท. โดยแบ่งการดำเนินการเป็น 3 ระยะ ดังนี้

6.1 ระยะที่ 1 ภายใน 420 วันนับจากวันที่ลงนามในสัญญา

6.2 ระยะที่ 2 ภายใน 825 วันนับจากวันที่ลงนามในสัญญา

6.3 ระยะที่ 3 ภายใน 1,230 วันนับจากวันที่ลงนามในสัญญา

7. ระยะเวลาการส่งมอบผลงาน

ที่ปรึกษาฯ ต้องส่งมอบเอกสารอย่างเป็นลายลักษณ์อักษร โดยเอกสารที่ส่งมอบต้องเป็นภาษาไทย จำนวน 4 ชุด และในรูปแบบอิเล็กทรอนิกส์ บันทึกลง Thumb Drive จำนวน 4 ชุด โดยแบ่งเป็น 3 ระยะ ดังนี้

7.1 ระยะ 1 ภายใน 420 วัน นับจากวันที่ลงนามในสัญญา ดังนี้

7.1.1 *งวดงานที่ 1* ภายใน 30 วัน นับจากวันที่ลงนามในสัญญา เมื่อที่ปรึกษาฯ ดำเนินการและส่งเอกสารตามข้อ 4.1

7.1.2 *งวดงานที่ 2* ภายใน 60 วัน นับจากวันที่ลงนามในสัญญา เมื่อที่ปรึกษาฯ ดำเนินการ ตามข้อ 4.2, 4.3 และส่งเอกสารผลการดำเนินงานที่เกี่ยวข้อง

7.1.3 *งวดงานที่ 3* ภายใน 135 วัน นับจากวันที่ลงนามในสัญญา เมื่อที่ปรึกษาฯ ดำเนินการตามข้อ 4.4, 4.5.1, จัดฝึกอบรม/สัมมนาหรือให้ความรู้หลักสูตรตามข้อ 4.10.1 (ครั้งที่ 1) และ ส่งเอกสารผลการดำเนินงานที่เกี่ยวข้อง

7.1.4 *งวดงานที่ 4* ภายใน 210 วัน นับจากวันที่ลงนามในสัญญา เมื่อที่ปรึกษาฯ ดำเนินการตามข้อ 4.5.2, 4.5.3, 4.7, จัดฝึกอบรม/สัมมนาหรือให้ความรู้หลักสูตรตามข้อ 4.10.2 - 4.10.4 (ครั้งที่ 1), สื่อประชาสัมพันธ์โครงการฯ จำนวนอย่างน้อย 2 ชิ้น และ ส่งเอกสารผลการดำเนินงานที่เกี่ยวข้อง

7.1.5 *งวดงานที่ 5* ภายใน 315 วัน นับจากวันที่ลงนามในสัญญา เมื่อที่ปรึกษาฯ ดำเนินการตามข้อ 4.8.1-4.8.17 , จัดฝึกอบรม/สัมมนาหรือให้ความรู้หลักสูตรตามข้อ 4.10.5 (ครั้งที่ 1) และส่งเอกสารผลการดำเนินงานที่เกี่ยวข้อง

7.1.6 งวดงาน ...

7.1.6 *งวดงานที่ 6* ภายใน 420 วัน นับจากวันที่ลงนามในสัญญา เมื่อที่ปรึกษาฯ ดำเนินการ ดังนี้

(1) ดำเนินการตามข้อ 4.6, 4.8.18 - 4.8.22

(2) เอกสารยืนยันการผ่านการตรวจรับรองระบบ ISMS ของ ทอท.ตามมาตรฐาน ISO/IEC 27001 ตามขอบเขตที่ทอท.กำหนด ซึ่งออกโดยผู้ตรวจประเมินภายนอก รับรองมาตรฐาน ISO/IEC 27001 (Certification Body) ได้แก่ ใบประกาศนียบัตรรับรองมาตรฐาน ISO/IEC 27001 เวอร์ชั่นล่าสุด (Certification) หรือจดหมายรับรองการผ่านการตรวจรับรองฯ พร้อมรายงานผลการตรวจประเมินเพื่อการรับรองฯ (Certification Audit Report)

(3) จัดประชุม ฝึกอบรม สัมมนา หรือให้ความรู้หลักสูตรตามข้อ 4.10.6 (ครั้งที่ 1)

(4) สื่อประชาสัมพันธ์โครงการฯ จำนวนอย่างน้อย 2 ชิ้น

7.2 <u>ระยะที่ 2</u> การตรวจรับรองการรักษามาตรฐานระบบ ISMS ของ ทอท.ปีที่ 1 (Surveillance Audit) ภายใน 825 วัน นับจากวันที่ลงนามในสัญญา

7.2.1 *งวดงานที่ 7* ภายใน 525 วัน นับจากวันที่ลงนามในสัญญา ประกอบด้วย การดำเนินงานตามข้อ 4.9.1 (ครั้งที่ 1), 4.9.2 (ครั้งที่ 1), จัดฝึกอบรม/สัมมนาหรือให้ความรู้หลักสูตรตามข้อ 4.10.1 (ครั้งที่ 2) และส่งเอกสารผลการดำเนินงานที่เกี่ยวข้อง

7.2.2 *งวดงานที่ 8* ภายใน 625 วัน นับจากวันที่ลงนามในสัญญา ประกอบด้วย การดำเนินงานตามข้อ 4.9.2 (ครั้งที่ 2), 4.9.3, 4.9.4, จัดฝึกอบรม/สัมมนาหรือให้ความรู้หลักสูตรตามข้อ 4.10.2-4.10.4 (ครั้งที่ 2) สื่อประชาสัมพันธ์โครงการฯ จำนวนอย่างน้อย 2 ชิ้น และส่งเอกสารผลการดำเนินงานที่เกี่ยวข้อง

7.2.3 *งวดงานที่ 9* ภายใน 720 วัน นับจากวันที่ลงนามในสัญญา ประกอบด้วย การดำเนินงานตามข้อ 4.9.2 (ครั้งที่ 3), 4.9.5-4.9.7, จัดฝึกอบรม/สัมมนาหรือให้ความรู้หลักสูตรตามข้อ 4.10.5 (ครั้งที่ 2) และส่งเอกสารผลการดำเนินงานที่เกี่ยวข้อง

7.2.4 งวดงานที่ *10* ภายใน 825 วัน นับจากวันที่ลงนามในสัญญา ประกอบด้วย การดำเนินงานตามข้อ 4.9.2 (ครั้งที่ 4), 4.9.8, 4.9.9, จัดฝึกอบรม/สัมมนาหรือให้ความรู้หลักสูตรตามข้อ 4.10.6 (ครั้งที่ 2), สื่อประชาสัมพันธ์โครงการฯ จำนวนอย่างน้อย 2 ชิ้น และส่งเอกสารผลการดำเนินงานที่เกี่ยวข้อง

7.3 ระยะที่ ...

7.3 ระยะที่ 3 การตรวจรับรองการรักษามาตรฐานระบบ ISMS ของ ทอท. ปีที่ 2 (Surveillance Audit) ภายใน 1,230 นับจากวันที่ลงนามในสัญญา

7.3.1 *งวดงานที่ 11* ภายใน 930 วัน นับจากวันที่ลงนามในสัญญา ประกอบด้วย การดำเนินงานตามข้อ 4.9.1(ครั้งที่ 2), 4.9.2(ครั้งที่ 5), จัดฝึกอบรม/สัมมนาหรือให้ความรู้หลักสูตรตามข้อ 4.10.1 (ครั้งที่ 3) และส่งเอกสารผลการดำเนินงานที่เกี่ยวข้อง

7.3.2 *งวดงานที่ 12* ภายใน 1,020 วัน นับจากวันที่ลงนามในสัญญา ประกอบด้วย การดำเนินงานตามข้อ 4.9.2 (ครั้งที่ 6), 4.9.3, 4.9.4, จัดฝึกอบรม/สัมมนาหรือให้ความรู้หลักสูตรตามข้อ 4.10.2-4.10.4 (ครั้งที่ 3), สื่อประชาสัมพันธ์โครงการฯ จำนวนอย่างน้อย 2 ชิ้น และส่งเอกสารผลการดำเนินงานที่เกี่ยวข้อง

7.3.3 *งวดงานที่ 13* ภายใน 1,125 วัน นับจากวันที่ลงนามในสัญญา ประกอบด้วย การดำเนินงานตามข้อ 4.9.2 (ครั้งที่ 7), 4.9.5-4.9.7 และ จัดฝึกอบรม/สัมมนาหรือให้ความรู้หลักสูตรตามข้อ 4.10.5 (ครั้งที่ 3) และส่งเอกสารผลการดำเนินงานที่เกี่ยวข้อง

7.3.4 *งวดงานที่ 14* ภายใน 1,230 วัน นับจากวันที่ลงนามในสัญญา ประกอบด้วย การดำเนินงานตามข้อ 4.9.2 (ครั้งที่ 8), 4.9.8, 4.9.9, จัดฝึกอบรม/สัมมนาหรือให้ความรู้หลักสูตรตามข้อ 4.10.6 (ครั้งที่ 3), สื่อประชาสัมพันธ์โครงการฯ จำนวนอย่างน้อย 2 ชิ้น และส่งเอกสารผลการดำเนินงานที่เกี่ยวข้อง

8. การจ่ายเงินค่าจ้าง

ทอท.จะจ่ายเงินค่าจ้างให้ผู้รับจ้าง จำนวน 14 งวด เมื่อผู้รับจ้างดำเนินการส่งมอบงานในแต่ละงวดและคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว ดังนี้

8.1 งวดที่ 1 จ่ายให้เป็นจำนวนร้อยละ 5 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.1.1 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.2 งวดที่ 2 จ่ายให้เป็นจำนวนร้อยละ 5 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.1.2 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.3 งวดที่ 3 จ่ายให้เป็นจำนวนร้อยละ 8 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.1.3 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.4 งวดที่ 4 จ่ายให้เป็นจำนวนร้อยละ 6 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.1.4 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.5 งวดที่ 5 จ่ายให้เป็นจำนวนร้อยละ 13 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.1.5 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.6 งวดที่ 6 ...

8.6 งวดที่ 6 จ่ายให้เป็นจำนวนร้อยละ 12 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.1.6 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.7 งวดที่ 7 จ่ายให้เป็นจำนวนร้อยละ 6 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.2.1 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.8 งวดที่ 8 จ่ายให้เป็นจำนวนร้อยละ 7 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.2.2 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.9 งวดที่ 9 จ่ายให้เป็นจำนวนร้อยละ 6 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.2.3 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.10 งวดที่ 10 จ่ายให้เป็นจำนวนร้อยละ 6 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.2.4 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.11 งวดที่ 11 จ่ายให้เป็นจำนวนร้อยละ 6 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.3.1 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.12 งวดที่ 12 จ่ายให้เป็นจำนวนร้อยละ 7 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.3.2 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.13 งวดที่ 13 จ่ายให้เป็นจำนวนร้อยละ 6 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.3.3 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

8.14 งวดที่ 14 จ่ายให้เป็นจำนวนร้อยละ 7 ของเงินค่าจ้างทั้งหมดตามที่ระบุในสัญญา เมื่อผู้รับจ้างดำเนินการตามข้อ 7.3.4 และคณะกรรมการตรวจรับพัสดุของ ทอท.ได้ตรวจรับงานไว้เรียบร้อยแล้ว

9. การกำกับหน้าที่ของบริษัทที่ปรึกษาฯ

ทอท. จะแต่งตั้งคณะกรรมการตรวจรับพัสดุและผู้ควบคุมงาน เพื่อประสานและกำกับการทำงานของที่ปรึกษา เพื่อให้เป็นไปตามข้อกำหนดและรายละเอียดในการจัดจ้างบริษัทที่ปรึกษาฯ

10. หน้าที่ความรับผิดชอบของ ทอท.

ทอท.จะรับผิดชอบจัดหาพื้นที่สำหรับการดำเนินงานเมื่อเข้ามาปฏิบัติงาน ณ ทอท.ให้แก่ที่ปรึกษาฯ ตามความเหมาะสม ซึ่งไม่ใช่สำนักงานประจำ โดยที่ปรึกษาฯ จะต้องรับผิดชอบค่าใช้จ่ายด้านสาธารณูปโภค การใช้งานระบบอินเตอร์เน็ต เครื่องใช้สำนักงาน และวัสดุสิ้นเปลืองต่าง ๆ ที่ใช้ในการดำเนินการ (ถ้ามี) ตลอดระยะเวลาของสัญญา

11. อัตรา ...

11. อัตราค่าปรับ

หากที่ปรึกษาฯ ไม่สามารถทำงานให้แล้วเสร็จตามเวลาที่กำหนดในสัญญา ที่ปรึกษาฯ จะต้องชำระค่าปรับให้แก่ ทอท.เป็นรายวันในอัตราร้อยละ 0.1 (ศูนย์จุดหนึ่ง) ของราคาค่าจ้างตามสัญญาในแต่ละงวด แต่ต้องไม่ต่ำกว่าวันละ 100.- บาท (หนึ่งร้อยบาท)

12. การยกเลิกสัญญา

ในกรณีที่บริษัทที่ปรึกษาผิดเงื่อนไขตามสัญญา ทอท. จะมีหนังสือบอกกล่าวเตือนไปยังบริษัทที่ปรึกษา เพื่อให้แก้ไขหรือปฏิบัติให้ถูกต้องแล้วเสร็จภายใน 15 วัน นับแต่วันที่ได้รับการแจ้งจาก ทอท. หากบริษัทที่ปรึกษามิได้แก้ไขหรือปฏิบัติให้ถูกต้องแล้วเสร็จภายในกำหนดเวลาดังกล่าว ทอท. มีสิทธิ์บอกเลิกสัญญาได้ทันที และบริษัทที่ปรึกษายินยอมให้ ทอท. เรียกร้องค่าเสียหายใดๆ ที่เกิดขึ้นจากการปฏิบัติผิดสัญญา

13. ข้อมูลที่เป็นความลับและการรักษาความลับ

ทอท.ขอสงวนสิทธิ์ห้ามเผยแพร่ข้อมูลของ ทอท.โดยมีรายละเอียดดังนี้

13.1 ที่ปรึกษาฯ จะต้องรักษาข้อมูลทางธุรกิจของ ทอท.หรือข้อมูลความรู้อื่นๆ ของ ทอท.โดยต้องไม่นำข้อมูล เอกสาร และผลการศึกษา ออกแบบ และงานต่างๆ ตลอดจนข้อกำหนดและรายละเอียดหรืออื่นๆ ภายใต้การจัดจ้างทั้งหมดของ ทอท.ที่ ทอท.ได้เปิดเผย ส่งต่อ หรือส่งมอบให้แก่ที่ปรึกษาฯ เพื่อใช้ในการปฏิบัติงานไปทำซ้ำ ดัดแปลง เผยแพร่หรือกระทำการใดๆ อันเป็นทางที่จะก่อให้เกิดความเสียหายแก่ ทอท.

13.2 ข้อมูล เอกสารหรือสิ่งที่สื่อความหมายให้รู้ข้อความ เรื่องราว ข้อเท็จจริง หรือสิ่งใด ไม่ว่าการสื่อความหมายนั้นจะผ่านวิธีการใดๆ และไม่ว่าจะจัดทำไว้ในรูปใดๆ รวมถึงรูปแบบ รูปภาพ วิธีการ หรืองานที่ได้รวบรวมหรือประกอบขึ้นทั้งหมด ที่ ทอท.เปิดเผยแก่พนักงานของที่ปรึกษาฯ รวมถึงผลการศึกษา แนวทางการดำเนินงาน และแผนต่างๆ ตลอดจนข้อกำหนดและรายละเอียดหรืออื่นๆ ภายใต้การจัดจ้างที่ปรึกษาจะต้องใช้เพื่อการปฏิบัติงานตามสัญญานี้เท่านั้น

13.3 ห้ามมิให้ที่ปรึกษาฯ ใช้หรือพยายามที่จะใช้ข้อมูลหรือสิ่งที่ได้มาจากข้อมูลตามข้อ 13.2 เพื่อวัตถุประสงค์ในเชิงพาณิชย์ หรือทำการพัฒนาเป็นผลิตภัณฑ์หรือเทคโนโลยี หรือใช้อ้างถึงหรือรวมเข้าไปเป็นส่วนหนึ่งของการประดิษฐ์ใดๆ หรือการขอรับความคุ้มครองทรัพย์สินทางปัญญาใดๆ เว้นแต่ ทอท.จะอนุญาตหรือให้ความยินยอมเป็นลายลักษณ์อักษร

13.4 ห้ามมิให้ที่ปรึกษาฯ ใช้หรือพยายามที่จะใช้ข้อมูลหรือสิ่งที่ได้มาจากข้อมูลตามข้อ 13.2 เพื่อการอื่นใดโดยไม่ได้รับอนุญาตจาก ทอท.ซึ่งพนักงานของที่ปรึกษาฯ จะต้องรักษาข้อมูลเป็นความลับ และไม่นำข้อมูลทั้งหมดหรือส่วนหนึ่งส่วนใดของข้อมูลไปเผยแพร่ต่อสาธารณชน บุคคลที่สาม หรือไปแสวงหาผลประโยชน์ไม่ว่าทางหนึ่งทางใดในเชิงพาณิชย์

13.5 หากเป็น ...

13.5 หากเป็นกรณีที่จำเป็นต้องเปิดเผยข้อมูลทางธุรกิจของ ทอท. หรือข้อมูลความรู้อื่นๆ ของ ทอท. ตามข้อ 13.1 ไม่ว่ากรณีใดๆ ต้องได้รับความยินยอมเป็นลายลักษณ์อักษรจาก ทอท. ก่อนทุกครั้ง และการส่งมอบข้อมูลดังกล่าวข้างต้น ทอท.ขอสงวนสิทธิ์เป็นผู้ส่งมอบข้อมูลดังกล่าวให้แก่ผู้รับมอบด้วยตนเอง หากข้อมูลส่วนหนึ่งส่วนใดที่เกี่ยวเนื่องกับงานนี้ ถูกนำไปใช้เป็นบรรทัดฐานเพื่อการศึกษา วิเคราะห์หรือพิจารณาเรื่องหนึ่งเรื่องใด ที่ปรึกษาฯ ต้องจัดการข้อมูลที่จะส่งมอบให้ผู้รับมอบ โดยไม่มีการอ้างอิง ทอท. ด้วยประการใดๆ ทั้งสิ้น

13.6 ที่ปรึกษาฯ ต้องรับผิดชอบต่อการละเมิดบทบัญญัติแห่งกฎหมายหรือสิทธิใดๆ ในสิทธิบัตร หรือลิขสิทธิ์ของบุคคลที่สาม ซึ่งที่ปรึกษาฯ นำมาใช้ในการปฏิบัติงานตามสัญญานี้

13.7 หากพบว่าที่ปรึกษาฯ มิได้ปฏิบัติตามเงื่อนไขตามข้อ 13.1-13.6 หรือบางส่วน ที่ปรึกษาฯ ต้องยินยอมชดใช้ค่าเสียหายต่างๆ ที่เกิดขึ้นในภายหลังให้แก่ ทอท.ตามความเสียหายที่เกิดขึ้นจริง และ ทอท.มีสิทธิดำเนินการตามกฎหมาย

14. เงื่อนไขที่ที่ปรึกษาฯ ต้องปฏิบัติและความรับผิดชอบ

14.1 บุคลากรที่ระบุตามข้อ 5 ต้องเป็นผู้ดำเนินการจริง และจะต้องเป็นบุคลากรเดียวกันกับที่ที่ปรึกษาฯ เสนอตามเงื่อนไขการเสนอราคา หากมีความจำเป็นต้องเปลี่ยนบุคลากรตามที่ได้เสนอไว้ บุคลาการที่มาดำเนินการแทนจะต้องมีประสบการณ์และคุณสมบัติอย่างน้อยเท่ากับบุคลากรที่นำเสนอ โดยต้องมีเอกสารหลักฐานยืนยันการส่งมอบงานของบุคลากรที่มีการเปลี่ยนแปลงเป็นลายลักษณ์อักษรให้ ทอท.พิจารณา ยกเว้นกรณีเกิดเหตุสุดวิสัยให้ขึ้นอยู่กับดุลยพินิจของ ทอท.โดยต้องทำหนังสือแจ้ง ทอท.เป็นลายลักษณ์อักษรและต้องได้รับการอนุมัติจาก ทอท. เป็นลายลักษณ์อักษรก่อนเริ่มปฏิบัติงานอย่างน้อย 3 วันทำการ หาก ทอท.พิจารณาแล้วคุณสมบัติไม่เหมาะสม ที่ปรึกษาฯ ต้องจัดหาบุคลากรใหม่มาเปลี่ยน หรือในระหว่างการทำงาน ทอท.พบว่าบุคลากรใดไม่สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ ทอท.สามารถแจ้งที่ปรึกษาฯ ให้เปลี่ยนแปลงได้ทันที

14.2 ในกรณีการเปลี่ยนแปลงบุคลากร ที่ปรึกษาฯ จะเปลี่ยนได้เฉพาะบุคลากรที่ดำเนินงานในโครงการนี้มาแล้วไม่ต่ำกว่า 12 เดือนและต้องดำเนินการตามที่ ทอท.ได้ระบุไว้ข้างต้น

14.3 ที่ปรึกษาฯ ต้องใช้ความชำนาญ ความระมัดระวัง และความขยันหมั่นเพียรในการปฏิบัติงาน และจะต้องปฏิบัติหน้าที่ความรับผิดชอบให้สำเร็จลุล่วง เป็นไปตามมาตรฐานของวิชาชีพที่ยอมรับนับถือโดยทั่วไป

14.4 ที่ปรึกษาฯ ต้องประชุมร่วมกับ ทอท.เพื่อรายงานความก้าวหน้าและผลดำเนินการตามที่ ทอท. ร้องขอ พร้อมทั้งจัดทำรายงานการประชุมเสนอ ทอท.โดย ทอท.จะแจ้งให้ทราบล่วงหน้า รวมทั้งจัดทำรายงานการประชุมทุกครั้งเมื่อมีการประชุมร่วมกับ ทอท.

14.5 ที่ปรึกษาฯ ...

14.5 ที่ปรึกษาฯ จะต้องชดใช้ค่าเสียหายให้แก่ ทอท.และป้องกันมิให้ ทอท.ต้องรับผิดชอบในบรรดาสิทธิเรียกร้องค่าเสียหาย ค่าใช้จ่าย หรือราคา รวมตลอดถึงการเรียกร้องโดยบุคคลที่สาม อันเกิดจากความผิดพลาดหรือการละเว้นไม่กระทำการของที่ปรึกษาฯ หรือพนักงานของที่ปรึกษาฯ

14.6 ที่ปรึกษาฯ ต้องทำงานให้สอดคล้องกับกฎระเบียบและข้อบังคับในการปฏิบัติงานของ ทอท. รวมถึงนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีและการสื่อสารของ ทอท. (AOT ICT Security Policy) นโยบายสนับสนุนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Supporting Policy) และ แนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Guideline) โดยเคร่งครัด

14.7 ที่ปรึกษาฯ ต้องนำเสนอผลการดำเนินงานของการศึกษาและช่วยสนับสนุนในการชี้แจงผลการดำเนินงานของการศึกษาโดยส่งผู้แทนเข้าร่วมชี้แจง ทั้งกับส่วนงานภายใน และหน่วยงานภายนอกเมื่อได้รับการร้องขอจาก ทอท. โดยไม่คิดค่าใช้จ่ายเพิ่มเติมใดๆ

14.8 ในกรณีที่ ทอท.ตรวจพบว่าเอกสารตามที่ที่ปรึกษาฯ เสนอในโครงการเป็นเท็จ ทอท.มีสิทธิบอกเลิกสัญญาหรือดำเนินการตามความเหมาะสม ทั้งนี้ขึ้นอยู่กับผลการพิจารณาของ ทอท.ถือเป็นที่สิ้นสุด

14.9 ที่ปรึกษาฯ ต้องลงนามในบันทึกข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA) ของ ทอท. ตามเอกสารที่ ทอท. กำหนด ภายใน 30 วัน นับถัดจากวันที่ลงนามในสัญญา

14.10 ในกรณีที่มีการปรับปรุงมาตรฐาน ISO/IEC 27001 เป็นเวอร์ชันใหม่(Third Edition) ในระยะเวลาของสัญญา ที่ปรึกษาฯ ต้องรับผิดชอบดำเนินการตามกรอบมาตรฐาน ISO/IEC 27001 เวอร์ชันใหม่(Third Edition) โดยไม่คิดค่าใช้จ่ายใดๆ เพิ่มจาก ทอท.

15. นโยบายต่อต้านคอรัปชั่นของ ทอท.

15.1 คู่ค้าต้องสนับสนุนนโยบายต่อต้านการคอรัปชั่นของ ทอท. ที่กำหนดให้บุคลากรทุกคนของ ทอท. ต้องไม่เข้าไปเกี่ยวข้องกับการคอรัปชั่นในทุกรูปแบบไม่ว่าโดยทางตรงหรือทางอ้อมและต้องปฏิบัติตามนโยบายต่อต้านคอรัปชั่นของ ทอท. อย่างเคร่งครัด

15.2 ห้ามมิให้ผู้เสนอราคาหรือคู่ค้าให้ของขวัญ ทรัพย์สินหรือประโยชน์อื่นใด รวมถึงจ่ายค่าบริการต้อนรับและค่าใช้จ่ายอื่นๆ ที่อาจส่งผลกระทบต่อการตัดสินใจในการปฏิบัติหน้าที่หรือส่งผลกระทบต่อการดำเนินงานของบริษัทให้แก่บุคลากรของ ทอท.

16. การดำเนินการ ...

16. การดำเนินการตามแนวทางการปฏิบัติอย่างยั่งยืนของคู่ค้า ทอท.

คู่ค้าต้องลงนามรับทราบในเอกสารแนวทางการปฏิบัติอย่างยั่งยืนของคู่ค้า ทอท. (AOT Supplier Sustainable Code of Conduct) ตามภาคผนวก ข. พร้อมทั้งปฏิบัติให้เป็นไปตามแนวทางดังกล่าว เพื่อส่งเสริมให้คู่ค้าของทอท. มีการดำเนินงานอย่างโปร่งใส มีจริยธรรม เคารพสิทธิมนุษยชน ดูแลอาชีวอนามัย และคำนึงถึงความปลอดภัยของลูกจ้าง รวมถึงการดำเนินงานที่อันซึ่งจะส่งผลกระทบถึงชุมชน และสิ่งแวดล้อมต่างๆ ที่เกี่ยวข้องผ่านการกำกับดูแลกิจการ ทั้งด้านเศรษฐกิจ สังคมและสิ่งแวดล้อม

17. การหักเงินประกันผลงาน (กรณีที่ผู้รับจ้างเป็นหน่วยงานของรัฐ)

ในการจ่ายเงินค่าจ้างให้แก่ที่ปรึกษาแต่ละงวด ทอท. จะหักเงินที่จ่ายในแต่ละครั้งในอัตราร้อยละ 5 (ห้า) ของเงินที่ต้องจ่ายในงวดนั้น เพื่อเป็นการประกันผลงาน และจ่ายคืนให้แก่ที่ปรึกษาโดยไม่มีดอกเบี้ยพร้อมกับการจ่ายเงินค่าจ้างงวดสุดท้าย

ที่ปรึกษาอาจจะขอให้ ทอท. จ่ายเงินประกันผลงานคืนให้แก่ที่ปรึกษาได้ แต่ที่ปรึกษาจะต้องนำหนังสือค้ำประกันของธนาคารเท่ากับจำนวนเงินประกันผลงานที่ขอรับคืนมามอบให้แก่ ทอท. ไว้แทน ที่มีสาขาในประเทศไทย และจะต้องมีอายุการค้ำประกันตลอดไปจนกว่าภาระหน้าที่ของที่ปรึกษาตามสัญญานี้สิ้นสุดลง

18. คุณสมบัติของผู้ยื่นข้อเสนอ

ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลที่ได้ขึ้นทะเบียนไว้กับศูนย์ข้อมูลที่ปรึกษาด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)

19. เงื่อนไขที่ผู้เสนอราคาต้องปฏิบัติในการเสนอราคา

19.1 <u>คุณสมบัติของผู้ยื่นข้อเสนอ</u>

ผู้ยื่นข้อเสนอต้องยื่นเอกสารการขึ้นทะเบียนไว้กับศูนย์ข้อมูลที่ปรึกษาด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)

19.2 <u>ข้อเสนอด้านคุณภาพ</u> ผู้เสนอราคาต้องจัดส่งรายละเอียดของการยื่นข้อเสนอโดยมีรายละเอียดอย่างน้อย ดังนี้

19.2.1 ผลงานและประสบการณ์ของที่ปรึกษา

หนังสือรับรองผลงานที่เกี่ยวข้องกับการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Information Security Management System) ตามมาตรฐาน ISO/IEC 27001 ที่เป็นสัญญาฉบับเดียวกัน นับย้อนหลังจากวันที่ยื่นข้อเสนอราคาไม่เกิน 5 ปี อย่างน้อย 1 โครงการ และเป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงานเอกชนที่ ทอท.เชื่อถือ กรณีที่ผลงานที่ผู้เสนอราคานำมาแสดงเป็นผลงานที่ออกโดยหน่วยงานเอกชน ผู้รับรองต้องเป็นผู้มีอำนาจของหน่วยงานเอกชนนั้น พร้อมทั้งประทับตราของหน่วยงาน(ถ้ามี) โดยต้องแนบสำเนาสัญญาและสำเนาหนังสือรับรองการหักภาษี ณ ที่จ่ายของสัญญาที่เสนอมาเพื่อประกอบการพิจารณาด้วย

ในกรณีที่ ...

ในกรณีที่ชื่อผลงานไม่ตรงกับผลงานด้านการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Information Security Management System) ตามมาตรฐาน ISO/IEC 27001 แต่มีลักษณะการทำงานที่เกี่ยวกับงานด้านการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้ผู้เสนอราคาแสดงหนังสือชี้แจงผลงานที่เกี่ยวข้อง พร้อมแนบรายละเอียดของสัญญาจ้างที่ระบุขอบเขตงานหรือลักษณะการทำงานที่เกี่ยวข้องมาด้วย

19.1.2 ประวัติ ประสบการณ์ และผลงานของบุคลากร

(1) โครงสร้างทีมงานสำหรับการดำเนินโครงการ

(2) รายละเอียดและคุณสมบัติของบุคลากรตามข้อ 5 โดยกรอกข้อมูลลงในแบบฟอร์มตามภาคผนวก ค. พร้อมแนบรายละเอียดที่เกี่ยวข้อง ทั้งนี้บุคลากรที่นำเสนอต้องเป็นที่ปรึกษาประจำกับบริษัท โดยผู้เสนอราคาต้องแสดงหนังสือยืนยันการเข้าร่วมงานโครงการของบุคลากรตามข้อ 5 พร้อมทั้งแสดงหลักฐานการเป็นพนักงานประจำเต็มเวลากับบริษัทที่ปรึกษา โดยมีระยะเวลาไม่น้อยกว่า 6 เดือน และหนังสือแสดงอัตราเงินเดือนที่นำไปใช้เป็นเงินเดือนพื้นฐานในการคิดค่าตอบแทน ซึ่งจะต้องเป็นหลักฐานแสดงการยื่นชำระภาษีเงินได้ต่อกรมสรรพากร ที่สามารถแสดงความเป็นพนักงานประจำของบริษัท (แบบ ภ.ง.ด.90 หรือ ภ.ง.ด.91 เฉพาะบุคคลที่เสนอเท่านั้น พร้อมใบปะหน้าและใบเสร็จรับเงินจากกรมสรรพากร)

(3) ประสบการณ์/ผลงานของบุคลากรตามข้อ 5

19.1.3 วิธีการดำเนินงานโครงการ ประกอบด้วย

(1) กรอบแนวคิด หลักการ กรรมวิธีและการบริหารการดำเนินโครงการ

(2) ความเข้าใจในโครงการและงานตามข้อกำหนด

(3) การออกแบบหลักสูตรการให้ความรู้ในการพัฒนาระบบ ISMS รวมถึงการสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัย

19.2 ข้อเสนอด้านราคา ประกอบด้วย

19.2.1 ใบเสนอราคา

19.2.2 ใบประมาณการราคา

(1) เอกสารแสดงรายละเอียดการเสนอราคาค่างานจ้างที่ปรึกษาฯ โดยผู้เสนอราคาต้องเสนอราคาเป็นราคาเหมารวม (Lump Sum) เป็นเงินบาท โดยเขียนเป็นตัวเลขและกำกับตัวอักษรให้ตรงกัน ถ้าไม่ตรงกันให้ถือตัวอักษรเป็นสำคัญ และจะต้องไม่มีการขูดลบหรือแก้ไข หากมีการขูด ลบ ตก เติม แก้ไขเปลี่ยนแปลง จะต้องลงลายมือชื่อผู้เสนอราคาพร้อมประทับตรา (ถ้ามี) กำกับไว้ด้วยทุกแห่ง

(2) ตารางสรุปค่าจ้างบุคลากร ซึ่งแสดงรายละเอียดจำนวน Man-Month ของแต่ละบุคคลและอัตราค่าจ้างเป็นรายบุคคล

(3) รายละเอียด ...

(3) รายละเอียดค่าใช้จ่ายอื่นๆ ในการดำเนินงาน เช่น ค่าที่พัก ค่าเดินทาง อุปกรณ์เครื่องใช้สำนักงาน ค่าใช้จ่ายทางด้านเอกสาร ฯลฯ

(หมายเหตุ การคำนวณค่าตอบแทนที่ปรึกษาอ้างอิงจาก หลักเกณฑ์ราคากลางการจ้างที่ปรึกษา สำนักเลขาธิการคณะรัฐมนตรี (นร 0506/ว128 ลง 8 ส.ค.56)

20. หลักเกณฑ์การพิจารณาคัดเลือกผู้เสนอราคา

ทอท.พิจารณาคัดเลือกผู้เสนอราคา โดยใช้เกณฑ์ราคา ดังนี้

20.1 ทอท.จะตรวจสอบคุณสมบัติของผู้เสนอราคาแต่ละราย จากเอกสารแสดงคุณสมบัติเป็นอันดับแรก หากผู้เสนอราคารายใดมีคุณสมบัติไม่ครบถ้วนตามที่ ทอท.กำหนด ทอท.สงวนสิทธิ์ที่จะไม่พิจารณาข้อเสนอด้านคุณภาพและซองข้อเสนอด้านราคา ของผู้เสนอราคาที่ไม่ผ่านการพิจารณาคุณสมบัติ

20.2 ทอท.จะพิจารณาข้อเสนอด้านคุณภาพของผู้เสนอราคาทุกรายที่ผ่านการพิจารณาคุณสมบัติตามข้อ 20.1 โดยผู้เสนอราคาจะต้องมีคะแนนรวมด้านคุณภาพไม่น้อยกว่า 80 คะแนน

20.3 ทอท. จะพิจารณาข้อเสนอด้านราคาของผู้เสนอราคาทุกรายที่ผ่านการพิจารณาข้อเสนอด้านคุณภาพตามข้อ 20.2 โดยคัดเลือกผู้ยื่นข้อเสนอราคาที่เสนอราคาต่ำสุด

20.4 ในกรณีที่ผู้ยื่นข้อเสนอรายที่เสนอราคาต่ำสุด เสนอราคาสูงกว่าวงเงินที่จะจ้าง ทอท. จะต่อรองราคา หากราคายังสูงกว่าวงเงินที่จะจ้าง ทอท. จะดำเนินการตามที่เห็นสมควรต่อไป

20.5 ทอท. มีหลักเกณฑ์การให้คะแนนข้อเสนอด้านคุณภาพ โดยมีคะแนนเต็ม 100 คะแนน ดังนี้

20.5.1 ผลงานและประสบการณ์ของที่ปรึกษาตามรายละเอียดข้อ 19.1.1	25
(1) จำนวนโครงการ	10
(1.1) จำนวนโครงการตั้งแต่ 2 โครงการขึ้นไป	10
(1.2) จำนวนโครงการ 1 โครงการ	8
(1.3) ไม่มีโครงการเสนอ	0
(2) มูลค่าของผลงานสูงสุดที่นำเสนอ	15
(2.1) มูลค่ามากกว่า 3,000,000 บาท ขึ้นไป	15
(2.2) มูลค่า 2,000,000 - 3,000,000 บาท	12
(2.3) มูลค่าต่ำกว่า 2,000,000 บาท	0
20.5.2 ประวัติ ประสบการณ์ และผลงานของบุคลากร ตามข้อ 19.1.2	40
(1) โครงสร้างทีมงานสำหรับการดำเนินโครงการ	10
(1.1) จำนวนบุคลากรมากกว่าที่ระบุในข้อกำหนดฯ ฉบับนี้	10
(1.2) จำนวนบุคลากรครบทั้ง 6 ตำแหน่ง	8
(1.3) จำนวนบุคลากรไม่ครบตามข้อกำหนด (6 ตำแหน่ง จำนวน 6 คน)	0

(2) รายละเอียด ...

(2) รายละเอียด วุฒิการศึกษา ประสบการณ์ และคุณสมบัติของบุคลากร 30

(2.1) วุฒิการศึกษา ประสบการณ์ และคุณสมบัติบุคลากร ตำแหน่งใดตำแหน่งหนึ่งสูงกว่าที่ระบุในข้อกำหนดฯ 30

(2.2) วุฒิการศึกษา ประสบการณ์ และคุณสมบัติบุคลากร ทั้ง 6 ตำแหน่งตามที่ระบุในข้อกำหนดฯ 24

(2.3) วุฒิการศึกษา ประสบการณ์ และคุณสมบัติบุคลากรตำแหน่งใดตำแหน่งหนึ่งต่ำกว่าที่ระบุในข้อกำหนดฯ 0

20.5.3 วิธีการดำเนินงานโครงการ 35

(1) กรอบแนวคิด หลักการ กรรมวิธีและการบริหารการดำเนินโครงการซึ่งมีวิธีการดำเนินงานและขั้นตอนการดำเนินงานครบถ้วนตามขอบเขตการดำเนินงานในข้อ 4 10

(2) ความเข้าใจในโครงการและขอบเขตงานตามข้อกำหนด 10

(2.1) แผนการดำเนินงานครบถ้วนตามขอบเขตการดำเนินงานในข้อ 4 และมีแนวทางการดำเนินงานที่ปฏิบัติได้จริง กำหนดแผนการดำเนินงานที่ชัดเจน และครบถ้วนอย่างน้อยตามที่ระบุในข้อกำหนด ในรูปแบบ Gantt Chart หรือรูปแบบที่เข้าใจได้ง่าย 5

(2.2) แนวทางการดำเนินงานที่สนับสนุนกิจกรรมต่างๆ ในแผนการดำเนินงานที่สามารถปฏิบัติได้จริง 5

(3) การออกแบบหลักสูตรการให้ความรู้ในการพัฒนาระบบ ISMS รวมถึงการสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัย 15

(3.1) การกำหนดรูปแบบการให้ความรู้ตามกลุ่มของผู้เรียน 10

1) Classroom Format, การประชุมสัมมนา 10

2) กำหนดรูปแบบอื่น เช่น e-Learning, Online เป็นต้น 7

(3.2) จำนวนหลักสูตรและเนื้อหา (Content / Outline) ที่นำเสนอ 5

1) จำนวนหลักสูตร มากกว่ารายละเอียดตามข้อกำหนด ข้อ 4.10 5

2) จำนวนหลักสูตร ครบตามข้อกำหนด ข้อ 4.10 (6 หลักสูตร ต่อปี) 4

3) จำนวนหลักสูตร ไม่ครบถ้วนตามที่ระบุในข้อกำหนด ข้อ 4.10 0

ในกรณีที่ผู้เสนอราคาไม่ส่งเอกสารในหัวข้อใดหัวข้อหนึ่ง ทอท.จะถือว่าคะแนนในหัวข้อนั้นเท่ากับศูนย์ (0 คะแนน)

<u>หมายเหตุ</u> ในการพิจารณาตัดสิน ผู้เสนอราคาที่ผ่านเกณฑ์การพิจารณาจากคณะกรรมการจัดหาพัสดุ ถือเป็นที่สิ้นสุดและจะไม่มีข้อโต้แย้งใดๆ ทั้งสิ้น

21. ข้อมูลสำหรับระบบศูนย์ข้อมูลบุคลากรที่ปรึกษากลางกระทรวงคมนาคม

ผู้เสนอราคาที่ได้รับการคัดเลือก ต้องจัดทำรายละเอียดของบุคลากรที่เสนอในงานจ้างนี้ ตามรูปแบบเอกสารในภาคผนวก ง. ลงใน Thumb Drive ในรูปแบบ Microsoft Excel จำนวน 1 ชุด และนำมายื่นให้ ทอท.ในวันลงนามในสัญญาจ้าง และข้อมูลที่ผู้เสนอราคายื่นต่อ ทอท.ผู้เสนอราคายินดีให้จัดเก็บไว้ในระบบศูนย์ข้อมูลบุคลากรที่ปรึกษากลางของกระทรวงคมนาคม เพื่อใช้เป็นประโยชน์ในราชการของคมนาคม

ลงชื่อ .....ผู้ออกข้อกำหนดและรายละเอียด

(น.ส.พิชญา หมายเจริญ)

จทช.วรค.7 สมส.ฝกท.

ลงชื่อ..... ผู้รับรอง

(นางสาวฉัตรวดี ศิริโภค)

ผอก.สมส.ฝกท.

๒๐ พ.ย.63

บัญชีรายการเอกสาร

ภาคผนวก ก. : รายการเอกสารที่เกี่ยวข้องกับระบบ ISMS ของ ทอท.

ภาคผนวก ข. : แนวทางการปฏิบัติอย่างยั่งยืนของคู่ค้า ทอท.
(AOT Supplier Sustainable Code of Conduct)

ภาคผนวก ค. : แบบฟอร์มรายละเอียดของบุคลากร

ภาคผนวก ง. : รายละเอียดของบุคลากรที่เสนอ

ภาคผนวก ก.

ภาคผนวก ก. **: รายการเอกสารที่เกี่ยวข้องกับระบบ ISMS ของ ทอท.**

1. นโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร (AOT ICT Security Policy)
2. นโยบายในการคุ้มครองข้อมูลส่วนบุคคลของ ทอท. (AOT Data Privacy Policy)
3. นโยบายสนับสนุนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Supporting Policy)
4. นโยบายสนับสนุนในการคุ้มครองข้อมูลส่วนบุคคล(Data Privacy Supporting Policy)
5. แนวทางการปฏิบัติงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท. (AOT ICT Security Guideline)
6. แนวทางการปฏิบัติงานในการคุ้มครองข้อมูลส่วนบุคคล(Data Privacy Guideline)
7. การลงนามรับทราบและถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของ ทอท.
8. กรอบการดำเนินงาน ISMS (ISMS Framework)
9. รายงานผลการศึกษาบริบทองค์กรด้าน ICT (The Study of ICT Organizational Context)
10. วิธีการบริหารความเสี่ยง ISMS (ISMS Risk Management Methodology)
11. รายการมาตรการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร ISMS (Statement of Applicability: SOA)
12. การวัดประสิทธิผล ISMS (ISMS Effectiveness)
13. รายงานการบริหารความเสี่ยง ISMS (ISMS Risk Management Report)
14. ขั้นตอนการปฏิบัติงานการจัดการและการควบคุมเอกสาร ISMS (ISMS Document Control Procedure)
15. แบบฟอร์มคำขอดำเนินการเอกสาร ISMS (Document Action Request: DAR Form)
16. แบบบันทึกแผนบริหารความเสี่ยง ISMS (ISMS Risk Management Plan - Template)
17. แบบบันทึกรายการเอกสาร ISMS (ISMS Master List Template)
18. แบบประเมินความเสี่ยง ISMS (ISMS Information Security Risk Assessment Template)
19. ขั้นตอนการปฏิบัติงานการตรวจสอบภายใน ISMS (Internal ISMS Audits Procedure)
20. ขั้นตอนการปฏิบัติงานการปรับปรุงแก้ไขความไม่สอดคล้อง (ISMS Corrective Action Procedure)
21. แบบฟอร์มดำเนินการปรับปรุงแก้ไขความไม่สอดคล้อง (ISMS Corrective Action Request: CAR Form)
22. แผนการตรวจสอบภายใน ISMS ประจำปี (Internal ISMS Audits Program)
23. แผนกำหนดการตรวจสอบภายใน ISMS (Internal ISMS Audit Plan)
24. รายการตรวจสอบภายใน ISMS (Internal ISMS Audit Checklist)

25. รายงานผลการตรวจสอบภายใน ISMS (Internal ISMS Audit Report)
26. เอกสารข้อตกลงการไม่เปิดเผยข้อมูลของ ทอท. (Non-disclosure Agreement: NDA)
27. ขั้นตอนการปฏิบัติงานการทำลายข้อมูลสารสนเทศ (Data Disposal Procedure)
28. แบบฟอร์มการขอทำลายข้อมูลสารสนเทศ (Data Disposal Request Form)
29. ขั้นตอนการปฏิบัติงานการควบคุมการเปลี่ยนแปลง (Change Management Procedure)
30. แบบฟอร์มการขอเปลี่ยนแปลง (Request for Change Form)
31. ข้อตกลงการใช้งานสินทรัพย์สารสนเทศของ ทอท. (Acceptable Use Agreement: AUA)
32. แนวทางการปฏิบัติงานการจัดชั้นความลับข้อมูลสารสนเทศและการจัดการตามชั้นความลับ (Information Classification, Labelling and Handling Guideline)
33. แนวทางการใช้งานวิทยาการเข้ารหัสลับและการจัดการกุญแจรหัสลับ (Cryptography and Key Management Guideline)
34. แนวทางการปฏิบัติงานการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกกิจกรรมการใช้งานของระบบสารสนเทศ (Log Protection Guideline)
35. แนวทางการปฏิบัติงานการบำรุงรักษาระบบสนับสนุนของศูนย์คอมพิวเตอร์ (Supporting Facilities Maintenance Guideline)
36. ขั้นตอนการปฏิบัติงานการกำหนดสิทธิ์การใช้งานระบบสารสนเทศ (Information System Access Right Management)
37. ขั้นตอนการปฏิบัติงานการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Incident Management Procedure)
38. ขั้นตอนการปฏิบัติงานการแลกเปลี่ยนข้อมูลสารสนเทศ (Information Exchange Procedure)
39. รายชื่อส่วนงาน หน่วยงาน และผู้ติดต่อ (Contact list)
40. ขั้นตอนการปฏิบัติงานการเข้าถึงศูนย์คอมพิวเตอร์ (Data Center Access Management Procedure)
41. แบบฟอร์มขออนุญาตเข้าศูนย์คอมพิวเตอร์ (Data Center Access Request Form)
42. แบบฟอร์มบันทึกการเข้า - ออกศูนย์คอมพิวเตอร์ (Data Center Access Record Form)
43. ขั้นตอนการปฏิบัติงานการสำรองข้อมูลและการกู้คืนข้อมูล (Backup and Restore Procedure)
44. แบบฟอร์มขอกู้คืนข้อมูล (Restore Request Form)
45. ขั้นตอนการปฏิบัติงานการขนย้ายสื่อบันทึกที่สำรองข้อมูล (Physical Backup Media Transfer Procedure)
46. แบบฟอร์มขอขนย้ายสื่อบันทึกที่สำรองข้อมูล (Physical Backup Media Transfer Request Form)
47. แบบฟอร์มใบนำส่งสื่อบันทึกข้อมูล (Cover Media Transfer Request Form)

48. ขั้นตอนการปฏิบัติงานการควบคุมการนำสินทรัพย์เข้า-ออกศูนย์คอมพิวเตอร์ (Removal of Assets in Data Center Procedure)
49. แบบฟอร์มการนำสินทรัพย์เข้า – ออกศูนย์คอมพิวเตอร์ (Removal of Asset in Data Center Form)
50. แบบรับทราบข้อตกลงการปฏิบัติงานของผู้รับจ้างในพื้นที่ศูนย์คอมพิวเตอร์ (Data Center Work Rule Acknowledgement)
51. แบบฟอร์มการขอใช้/โยกย้าย/ส่งคืนสินทรัพย์สารสนเทศ (Information Asset Usage/Move/Return Request Form)
52. แบบฟอร์มลงทะเบียนการใช้งานเครื่องคอมพิวเตอร์และสื่อสารส่วนตัว (Personal Computer and Device Register Form)

ภาคผนวก ข

สัญญาเลขที่.....

แนวทางการปฏิบัติอย่างยั่งยืนของคู่ค้า บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)
(AOT Supplier Sustainable Code of Conduct)

ข้าพเจ้า .....โดย.....
มีสำนักงาน/ภูมิลำเนาตั้งอยู่ ณ .....
.....
ซึ่งเป็นคู่สัญญากับบริษัท ท่าอากาศยานไทย จำกัด (มหาชน) (ทอท.) ตามสัญญาเลขที่.....
ซึ่งต่อไปนี้จะเรียกว่า "คู่ค้าของ ทอท." ได้รับทราบแนวทางการปฏิบัติอย่างยั่งยืนของคู่ค้า ทอท.รายละเอียดดังนี้

บทนำ

ทอท.มีความมุ่งมั่นต่อการดำเนินธุรกิจให้เติบโตอย่างยั่งยืนในทุกกระบวนการ ดังนั้น "แนวทางการปฏิบัติอย่าง ยั่งยืนของคู่ค้า ทอท." จึงได้ถูกกำหนดขึ้น โดยพิจารณาเนื้อหาและขอบเขตให้อยู่ภายใต้ข้อกำหนดและกฎหมายที่เกี่ยวข้อง ครอบคลุมทั้ง 3 มิติ ได้แก่ เศรษฐกิจ สังคม และสิ่งแวดล้อม เพื่อส่งเสริมให้คู่ค้าของ ทอท. ดำเนินงานอย่างโปร่งใส มีจริยธรรม เคารพสิทธิมนุษยชน ดูแลอาชีวอนามัยและความปลอดภัยของลูกจ้าง คำนึงถึงผลกระทบต่อชุมชนและสิ่งแวดล้อมจากการดำเนินงาน ผ่านการกำกับดูแลกิจการและแนวปฏิบัติที่ดี ดังนี้

มิติเศรษฐกิจ - การกำกับดูแลกิจการที่ดี

1. ***การปฏิบัติตนตามกฎหมาย ระเบียบข้อบังคับ และความซื่อสัตย์สุจริต***: คู่ค้าของ ทอท.ต้องดำเนินธุรกิจอย่างเคารพกฎหมายของประเทศและระเบียบข้อบังคับของ ทอท.อย่างเคร่งครัด และดำเนินธุรกิจตามหลักจริยธรรม โดยปราศจากการติดสินบน หรือทุจริตในทุกรูปแบบ หรือประกอบธุรกิจผิดกฎหมาย
2. ***การรักษาความลับ***: คู่ค้าของ ทอท.ต้องเก็บรักษาข้อมูลและป้องกันการรั่วไหลของข้อมูลที่เป็นความลับของ ทอท. และไม่นำข้อมูลของ ทอท.ไปใช้เพื่อวัตถุประสงค์ที่ผิดกฎหมาย เพื่อประโยชน์ส่วนบุคคล หรือเพื่อประโยชน์ทางการค้า
3. ***ความขัดแย้งทางผลประโยชน์หรือผลประโยชน์ทับซ้อน***: คู่ค้าของ ทอท.ต้องแจ้งให้ ทอท.ทราบเป็นลายลักษณ์อักษร หากพบการดำเนินการใด ๆ ที่เป็นผลประโยชน์ทับซ้อนระหว่าง ทอท.และคู่ค้า
4. ***การแข่งขันเสรีและกฎหมายการแข่งขันทางการค้า***: คู่ค้าของ ทอท.จะต้องปฏิบัติตนภายใต้การแข่งขันที่เสรีเป็นธรรมและดำเนินการตามกฎหมายการแข่งขันทางการค้าอย่างเคร่งครัด และไม่กระทำการอื่นใดซึ่งจะส่งผลกระทบเชิงลบต่อคู่แข่งทางการค้า

มิติสังคม - การจ้างงานและการเคารพสิทธิมนุษยชน

1. ***อาชีวอนามัยและความปลอดภัยของแรงงาน***: คู่ค้าของ ทอท.ต้องดูแลแรงงานด้านอาชีวอนามัยและความปลอดภัยให้เหมาะสม อาทิ สถานที่และสภาพแวดล้อมในการทำงาน และการดูแลสุขภาพของลูกจ้างและผู้รับเหมาช่วงให้สอดคล้องตามกฎหมายหรือมาตรฐานสากล
2. ***อิสรภาพของการจ้างงาน***: คู่ค้าของ ทอท.ต้องดำเนินธุรกิจโดยปราศจากการใช้แรงงานบังคับ ต้องไม่มีการใช้แรงงานไม่สมัครใจ และเปิดโอกาสให้แรงงานสามารถรวมกลุ่มเพื่อเจรจาและต่อรองได้ตามกฎหมายของประเทศ
3. ***ค่าจ้างและสิทธิประโยชน์***: คู่ค้าของ ทอท.จะต้องจ่ายค่าจ้างและให้สิทธิประโยชน์อื่นใดที่ลูกจ้างพึงได้รับอย่างถูกต้อง เป็นธรรม และตรงตามกำหนดเวลา
4. ***การใช้แรงงานเด็ก***: คู่ค้าของ ทอท.ต้องไม่จ้างแรงงานเด็กที่มีอายุไม่ถึงเกณฑ์ตามที่กฎหมายกำหนด และไม่อนุญาตให้เด็กหรือบุคคลที่มีอายุต่ำกว่า 18 ปี ทำงานในเวลากลางคืน หรือในสถานที่ที่มีลักษณะเป็นอันตราย
5. ***ระยะเวลาในการทำงาน***: คู่ค้าของ ทอท. จะต้องดูแลไม่ให้แรงงานทำงานนานเกินกว่าที่กฎหมายกำหนด ทั้งนี้จะรวมถึงการทำงานล่วงเวลาและการทำงานในวันหยุด
6. ***การปฏิบัติอย่างเท่าเทียม***: คู่ค้าของ ทอท.ต้องปฏิบัติอย่างเท่าเทียมต่อลูกจ้าง โดยไม่เลือกปฏิบัติในการจ้างงาน การจ่ายค่าตอบแทน การเข้ารับการฝึกอบรม การเลื่อนตำแหน่ง การเลิกจ้างหรือการให้ออกจากงาน อันเนื่องมาจากการแบ่งแยกเพศ เชื้อชาติ ถิ่นกำเนิด สีผิว ศาสนา อายุ ความนิยมทางการเมือง สถานภาพการสมรส สภาพการตั้งครรภ์ หรือความพิการ
7. ***การเลิกจ้าง***: คู่ค้าของ ทอท.ต้องปฏิบัติและการดำเนินการเลิกจ้างในแต่ละขั้นตอนตามกฎหมายกำหนด และไม่ยกเลิกสัญญาจ้างด้วยความไม่เป็นธรรม
8. ***การเคารพสิทธิมนุษยชน***: คู่ค้าของ ทอท.ต้องเคารพสิทธิมนุษยชนและมีการปฏิบัติต่อลูกจ้างของตนอย่างเป็นธรรม ตามกฎหมายและมาตรฐานสากล และห้ามมิให้มีการกระทำอันเป็นการล่วงละเมิดทางร่างกายและวาจา รวมถึงการคุกคามและการข่มขู่ใด ๆ แก่ลูกจ้าง
9. ***แรงงานต่างด้าวหรือแรงงานอพยพ***: คู่ค้าของ ทอท.ต้องปฏิบัติตามกฎหมายแรงงานหากมีการจ้างแรงงานต่างด้าวหรือแรงงานอพยพ โดยต้องจัดเตรียมเอกสารสัญญาจ้างในภาษาแม่ของแรงงานหรือภาษาที่แรงงานอ่านแล้วเข้าใจก่อนการจ้างงาน รวมทั้ง หนังสือเดินทางและเอกสารประจำตัวของแรงงานต้องเก็บโดยเจ้าของเอกสารตลอดเวลา นายจ้างหรือบุคคลที่สามไม่สามารถถือครองเอกสารดังกล่าวของแรงงานได้
10. ***ความรับผิดชอบต่อสังคม***: คู่ค้าของ ทอท.ควรแสดงออกถึงการมีส่วนร่วมในการพัฒนาและรับผิดชอบต่อสังคม

มิติสิ่งแวดล้อม - การบริหารจัดการสิ่งแวดล้อมและมลพิษ

1. ***การบริหารจัดการสิ่งแวดล้อม***: คู่ค้าของ ทอท.ต้องบริหารจัดการสิ่งแวดล้อมตามมาตรฐาน ข้อกำหนด และแนวปฏิบัติที่ดีที่เกี่ยวข้อง ในทุกกระบวนการผลิตและการให้บริการ เพื่อการใช้ทรัพยากรอย่างรู้คุณค่า ลดผลกระทบด้านสิ่งแวดล้อม และไม่สร้างความเดือดร้อนรำคาญให้กับชุมชนรอบข้าง
2. ***มาตรการป้องกันและลดผลกระทบทางสิ่งแวดล้อม***: คู่ค้าของ ทอท.จะต้องดำเนินมาตรการป้องกันและควบคุมมลพิษ อาทิ ของเสีย น้ำเสีย เสียงรบกวน มลพิษทางอากาศ และก๊าซเรือนกระจก โดยต้องควบคุมหรือบำบัดก่อนปล่อยออกสู่ภายนอกตามกฎหมายและมาตรฐานสากล

ทอท.คาดหวังให้คู่ค้าพิจารณานำแนวทางการปฏิบัติเหล่านี้ ทั้งการกำกับดูแลกิจการที่ดี การจ้างงานและการเคารพสิทธิมนุษยชน และการบริหารจัดการสิ่งแวดล้อมและมลพิษ มาปรับใช้ในการดำเนินงานของคู่ค้า พร้อมส่งเสริมให้คู่ค้ามีแนวทางปฏิบัติอย่างยั่งยืนในห่วงโซ่อุปทานของตนเองตามความเหมาะสม

ข้าพเจ้าได้อ่าน เข้าใจ และรับทราบ แนวทางการปฏิบัติอย่างยั่งยืนของคู่ค้าของ ทอท. และตกลงที่จะปฏิบัติตามแนวทางดังกล่าวนี้ในทุกประเด็นที่การดำเนินธุรกิจของบริษัทข้าพเจ้าเกี่ยวข้อง โดยจะแจ้งให้ลูกจ้างของบริษัทที่เกี่ยวข้องทุกคนรับทราบรวมถึงเก็บข้อมูลซึ่งเป็นหลักฐานการปฏิบัติตามแนวทางนี้ไว้ และส่งมอบให้ตามที่ ทอท. ร้องขอ

(ลงชื่อ).....(คู่ค้าของ ทอท.)

(.....)

.....

(ประทับตราบริษัท)

ภาคผนวก ค.

ภาคผนวก ค. : แบบฟอร์มรายละเอียดบุคลากร

ตำแหน่ง	5.1 ผู้จัดการโครงการ	อ้างอิงเอกสารประกอบ (เอกสารแนบ.., หน้า..)
ชื่อ-สกุล		
วุฒิการศึกษา		
ประสบการณ์-(ระยะเวลา)		
ประกาศนียบัตร		
อื่นๆ		
ตำแหน่ง	5.2 ผู้เชี่ยวชาญด้านการจัดการ การรักษาความมั่นคงปลอดภัยสารสนเทศ	อ้างอิงเอกสารประกอบ (เอกสารแนบ.., หน้า..)
ชื่อ-สกุล		
วุฒิการศึกษา		
ประสบการณ์		
ประกาศนียบัตร		
อื่นๆ		
ตำแหน่ง	5.3 ผู้เชี่ยวชาญด้านการตรวจประเมินรับรอง ระบบการจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ	อ้างอิงเอกสารประกอบ (เอกสารแนบ.., หน้า..)
ชื่อ-สกุล		
วุฒิการศึกษา		
ประสบการณ์		
ประกาศนียบัตร		
อื่นๆ		

ตำแหน่ง	5.4 ที่ปรึกษาด้านวิศวกรรมระบบศูนย์คอมพิวเตอร์	อ้างอิงเอกสารประกอบ (เอกสารแนบ.., หน้า..)
ชื่อ-สกุล		
วุฒิการศึกษา		
ประสบการณ์		
ประกาศนียบัตร		
อื่นๆ		
ตำแหน่ง	5.5 ที่ปรึกษาด้านระบบสื่อสารอิเล็กทรอนิกส์, ระบบคอมพิวเตอร์และระบบเครือข่าย	อ้างอิงเอกสารประกอบ (เอกสารแนบ.., หน้า..)
ชื่อ-สกุล		
วุฒิการศึกษา		
ประสบการณ์		
ประกาศนียบัตร		
อื่นๆ		
ตำแหน่ง	5.6 ที่ปรึกษาด้านระบบสารสนเทศ	อ้างอิงเอกสารประกอบ (เอกสารแนบ.., หน้า..)
ชื่อ-สกุล		
วุฒิการศึกษา		
ประสบการณ์		
ประกาศนียบัตร		
อื่นๆ		

ภาคผนวก ง.

งานจ้างที่ปรึกษาผู้เสนอราคาทุกรายต้องเสนอรายละเอียดของบุคลากรดังนี้

- เลขบัตรประจำตัวประชาชน/หนังสือเดินทาง *
- เลขที่ประจำตัวผู้เสียภาษี *
- คำนำหน้าชื่อ *
- เพศ *
- ชื่อ *
- สัญชาติ *
- ที่อยู่ปัจจุบัน *
- เขต/อำเภอ *
- แขวง/ตำบล *
- รหัสไปรษณีย์ *
- เบอร์โทรศัพท์ที่ติดต่อสะดวก
- เบอร์ต่อ
- เบอร์มือถือ *
- โทรสาร
- อีเมล์ *
- อาชีพหลัก *
- จำนวนชั่วโมงที่ทำอาชีพหลัก/สัปดาห์ *
- ปีที่เริ่มทำงานเป็นที่ปรึกษา *
- ประสบการณ์ *
- ความเชี่ยวชาญ
- หมายเลข License
- เลขที่ใบอนุญาตประกอบวิชาชีพ *
- สาขาวิชาชีพ *
- วันหมดอายุของใบอนุญาตประกอบวิชาชีพ *
- ตำแหน่งในโครงการ *
- Man-month *
- ระยะเวลาที่ทำงานโครงการตั้งแต่ * ถึง *
- ประเภทเวลาทำงาน *
- ระดับวุฒิการศึกษา
- ปีที่สำเร็จการศึกษา
- วุฒิการศึกษา
- สถาบันการศึกษา