



ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่ายในการจ้างที่ปรึกษา

1. ชื่อโครงการจ้าง การจัดทำที่ปรึกษางานยกระดับระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 /หน่วยงานเจ้าของโครงการ ฝ่ายเทคโนโลยีสารสนเทศ
2. วงเงินงบประมาณที่ได้รับจัดสรร 300,000 บาท
3. วันที่กำหนดราคากลาง (ราคาอ้างอิง)1.9.๒๕๖๐.....
เป็นเงิน 256,800 บาท
4. ค่าตอบแทนบุคลากร 300,000 บาท
 - 4.1 ประเภทที่ปรึกษา
ที่ปรึกษาด้านมาตรฐานความมั่นคงปลอดภัยของสารสนเทศ ISO/IEC 27001
 - 4.2 คุณสมบัติที่ปรึกษา
 - 4.2.1 มีผลงานเกี่ยวกับการเป็นที่ปรึกษางานจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001 พร้อมสำเนาสัญญาผลงานที่กล่าวอ้าง ซึ่งเป็นวงเงินไม่น้อยกว่า 300,000 บาท (ห้าแสนบาทถ้วน) ต่อหนึ่งสัญญา ภายในระยะเวลา 5 ปี นับจากวันทำงานแล้วเสร็จจนถึงวันที่ยื่นข้อเสนอด้านราคา และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานราชการ รัฐวิสาหกิจ หรือ หน่วยงาน... เอกชนที่เชื่อถือได้
 - 4.2.2 เป็นนิติบุคคลไทยที่ได้รับจดทะเบียนประกอบธุรกิจในประเทศไทย
 - 4.2.3 ไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลกรรมสั่งให้นิติบุคคลอื่นเป็นผู้ทำงานตามระเบียบของทางราชการ
 - 4.2.4 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่... รัฐบาลของที่ปรึกษาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นนั้น
 - 4.3 จำนวนที่ปรึกษา
1 คน
5. ค่าวัสดุอุปกรณ์ :-
6. การเดินทางไปต่างประเทศ (ถ้ามี) :-
7. ค่าใช้จ่ายอื่นๆ :-
8. รายชื่อผู้รับผิดชอบในการกำหนดค่าใช้จ่าย/ดำเนินการ/ขอบเขตดำเนินการ (TOR)
นายคมสัน วรกุล หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
9. ที่มาของการกำหนดราคากลาง (ราคาอ้างอิง)
การจัดทำที่ปรึกษางานระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ปีงบประมาณ 2559

Amn ๑๗๓



ขอบเขตของงาน (Terms of Reference : TOR)
การจัดจ้างที่ปรึกษางานยกระดับระบบบริหารจัดการ
ความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013
สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน)

1. ความเป็นมา

ปัจจุบันข้อมูล (Data) และสารสนเทศ (Information) เปรียบเสมือนสินทรัพย์ที่มีมูลค่าและมีบทบาทสำคัญต่อการบริหารจัดการองค์กร ดังนั้น องค์กรต่างๆ จึงเริ่มตระหนักถึงการปกป้องรักษาข้อมูลและสารสนเทศที่สำคัญอันนำมาซึ่งความท้าทายในการบริหารความมั่นคงปลอดภัยของสารสนเทศอย่างเป็นมาตรฐานและมีประสิทธิภาพคู่มากับการลงทุนเพื่อให้ผู้ใช้ข้อมูลและสารสนเทศมีความเชื่อมั่นว่าข้อมูลและสารสนเทศดังกล่าวมีความปลอดภัย

มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานการรักษาความมั่นคงปลอดภัยของสารสนเทศที่ได้รับการยอมรับในระดับนานาชาติ อีกทั้งยังเป็นมาตรฐานที่นำมาใช้อ้างอิงในกฎหมายด้านเทคโนโลยีสารสนเทศและการสื่อสาร แผนนโยบาย และแนวทางปฏิบัติที่บังคับใช้ของประเทศไทย อาทิ พระราชบัญญัติว่าด้วยการประกอบธุรกิจกรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 แผนนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 แผนนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

ด้วยเหตุดังกล่าว สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน) ซึ่งเป็นหน่วยงานภาครัฐที่นำระบบสารสนเทศมาใช้ในการเพิ่มประสิทธิภาพในงานบริหารจัดการองค์กร งานวิจัย และงานบริการต่างๆ จึงได้จัดทำระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ซึ่งเป็นมาตรฐานด้านความมั่นคงปลอดภัยของสารสนเทศรุ่น (Version) ปัจจุบัน โดยมีวัตถุประสงค์เพื่อสร้างความปลอดภัยให้กับระบบสารสนเทศของสถาบันฯ ตลอดจนสามารถสร้างความเชื่อมั่นให้กับลูกค้าหรือผู้ใช้บริการระบบสารสนเทศได้ และเมื่อวันที่ 9 สิงหาคม 2560 สถาบันฯ ได้รับการรับรองมาตรฐานดังกล่าวจากสำนักงานคณะกรรมการว่าด้วยการรับรองระบบประจำสหราชอาณาจักร (United Kingdom Accreditation Service: UKAS) ซึ่งเป็นองค์กรในระดับนานาชาติที่ได้รับการยอมรับจากนานาชาติประเทศ แต่เนื่องจาก ในปีงบประมาณ 2561 สถาบันฯ ต้องการยกระดับระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศให้มีความแข็งแกร่งและเหมาะสมต่อการนำมาประยุกต์ใช้กับงานตามภารกิจใหม่ของสถาบันฯ จึงมีความจำเป็นต้องจัดจ้างที่ปรึกษาที่มีความเชี่ยวชาญในการดำเนินระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 เพื่อให้คำแนะนำและฝึกอบรมบุคลากรของสถาบันฯ ในการธำรงและพัฒนาระบบฯ ตลอดจนเตรียมความพร้อมสำหรับการตรวจประเมินจากหน่วยรับรอง (Certification Body: CB) ในรอบการตรวจประเมินครั้งต่อไป

อนุทิน อานนท์

/2. วัตถุประสงค์...

2. วัตถุประสงค์

เพื่อจัดจ้างที่ปรึกษางานยกระดับระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ซึ่งเป็นมาตรฐานรุ่น (Version) ปัจจุบัน

3. คุณสมบัติของผู้เสนอราคา

3.1 ผู้เสนอราคาจะต้องมีผลงานเกี่ยวกับการเป็นที่ปรึกษางานจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001 พร้อมสำเนาสัญญาผลงานที่กล่าวอ้างซึ่งเป็นวงเงินไม่น้อยกว่า 300,000 บาท (สามแสนบาทถ้วน) ต่อหนึ่งสัญญา ภายในระยะเวลา 5 ปี นับจากวันที่งานแล้วเสร็จจนถึงวันที่ยื่นข้อเสนอด้านราคา และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานราชการ รัฐวิสาหกิจ หรือ หน่วยงานเอกชนที่เชื่อถือได้

3.2 ผู้เสนอราคาต้องเป็นนิติบุคคลไทยที่ได้รับจดทะเบียนประกอบธุรกิจในประเทศไทย ทั้งนี้ ผู้เสนอราคาจะต้องแนบหนังสือรับรองการจดทะเบียนจัดตั้งห้างหุ้นส่วนบริษัทรับรองสำเนาโดยกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ไม่เกิน 3 เดือน/หนังสือบริคณห์สนธิ/ใบทะเบียนภาษีมูลค่าเพิ่ม (ภ.พ. 20)/บัญชีรายชื่อผู้ถือหุ้น (บอจ.5)/บัญชีรายชื่อหุ้นส่วนผู้จัดการ ผู้มีอำนาจควบคุม พร้อมรับรองสำเนาถูกต้อง และหนังสือมอบอำนาจติดอากรแสตมป์ตามกฎหมายให้ครบถ้วน ในกรณีที่ผู้เสนอราคามอบอำนาจให้บุคคลอื่นลงนามในใบเสนอราคาแทน (ถ้ามี) มาเพื่อประกอบการพิจารณา

3.3 ผู้เสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลการสั่งให้นิติบุคคลอื่นเป็นผู้ทำงานตามระเบียบของทางราชการ

3.4 ผู้เสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นนั้น

4. ขอบเขตการดำเนินงาน

ขอบเขตการดำเนินงานของที่ปรึกษางานยกระดับระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 มีดังนี้

4.1 การวางแผน (Planning)

แนะนำและให้คำปรึกษาในเรื่องดังต่อไปนี้

4.1.1 การทบทวนความเสี่ยง อันได้แก่ เกณฑ์ประเมินความเสี่ยง การประเมินความเสี่ยง และแผนบริหารจัดการความเสี่ยง (RTP)

4.1.2 การทบทวน Statement of Applicability (SOA)

4.1.3 การควบคุมการปฏิบัติงาน (Operational Control)

4.2 การปฏิบัติงาน (Doing)

4.2.1 แนะนำและให้คำปรึกษาในเรื่องดังต่อไปนี้

4.2.1.1 การทบทวนและปรับปรุงการปฏิบัติตามระเบียบปฏิบัติที่เกี่ยวข้องกับกฎหมายด้านความมั่นคงปลอดภัยของสารสนเทศ รวมถึงข้อบังคับที่เกี่ยวข้อง

Amr 16 อมร

4.2.1.2 การทบทวนและปรับปรุงมาตรการด้านความมั่นคงปลอดภัยที่สำคัญ เช่น การจัดการช่องโหว่ด้านความมั่นคงปลอดภัยของสารสนเทศ (Vulnerability Management) การควบคุมการเปลี่ยนแปลง (Change Control) การรักษาความปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) การสำรองและกู้คืนข้อมูล (Backup and Restore) ฯลฯ

4.2.1.3 การวิเคราะห์หลักฐานการใช้งานสารสนเทศ (Log Analysis)

4.2.1.4 การวัดผลความมั่นคงปลอดภัยของสารสนเทศ (Information Security Performance Measurement)

4.2.1.5 การฝึกซ้อมแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCP)

4.2.2 ฝึกอบรมหลักสูตรเกี่ยวกับการตรวจประเมินภายในด้านระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Internal Auditor Training Course) ให้กับบุคลากรซึ่งเป็นคณะทำงานหรือผู้ที่เกี่ยวข้อง ณ สำนักงานของสถาบันฯ หรือสถานที่ที่สถาบันฯ จัดให้

4.3 การติดตามและประเมินผล (Checking and Acting)

4.3.1 แนะนำและให้คำปรึกษาแก่คณะทำงานในการตรวจสอบช่องโหว่ด้านความมั่นคงปลอดภัยของสารสนเทศ (Vulnerabilities) รวมถึงแนะนำแนวทางแก้ไขช่องโหว่ที่ตรวจพบ

4.3.2 ตรวจประเมินภายในร่วมกับคณะทำงานซึ่งได้รับมอบหมายให้เป็นคณะผู้ตรวจสอบภายในตามมาตรฐาน ISO/IEC 27001:2013

4.3.3 แนะนำและให้คำปรึกษาในการแก้ไขข้อบกพร่องหรือจุดอ่อนที่พบจากการตรวจประเมินภายใน

4.3.4 ร่วมประชุมทบทวนการบริหาร (Management Review)

5. สถานที่ดำเนินงาน

สถานที่ที่ผู้เสนอราคาจะดำเนินงานอยู่ที่ สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน) 140, 140/1-3, 140/5 อาคารไอทีเอฟ ทาวเวอร์ ชั้น 1 - 4 และชั้น 6 ถนนสีลม แขวงสุริยวงศ์ เขตบางรัก กรุงเทพฯ 10500

6. ระยะเวลาดำเนินงาน

ผู้เสนอราคาต้องส่งมอบงานทั้งหมดตามข้อ 4. ภายในระยะเวลา 9 เดือน นับแต่วันที่ลงนามในสัญญา โดยผู้เสนอราคาจะต้องจัดทำแผนดำเนินงานและแจ้งเป็นหนังสือให้สถาบันฯ ทราบก่อนดำเนินงานภายใน 15 วัน นับแต่วันที่ลงนามในสัญญา

7. การชำระเงิน

7.1 เงินงวดที่ 1 ในอัตราร้อยละ 20 ของราคาที่ได้ตกลงจัดจ้าง โดยจะชำระภายใน 15 วัน นับแต่วันที่ลงนามในสัญญา

7.2 เงินงวดที่ 2 ในอัตราร้อยละ 30 ของราคาที่ได้ตกลงจัดจ้าง โดยจะชำระภายใน 30 วัน นับแต่วันที่ผู้เสนอราคาได้อบรมบุคลากรซึ่งเป็นคณะทำงานหรือผู้ที่เกี่ยวข้องตามที่ระบุในข้อ 4.2.2 เป็นที่เรียบร้อยแล้ว

Amn 10/27/25

/7.3 เงินงวดที่ 3...

7.3 เงินงวดที่ 3 ในอัตราร้อยละ 50 ของราคาที่ตกลงจัดจ้าง โดยจะชำระภายใน 30 วัน นับแต่วันที่สถาบันฯ ได้รับรายงานการดำเนินงานทั้งหมดตามข้อ 4. เป็นที่เรียบร้อยแล้ว

8. ค่าปรับกรณีผู้เสนอราคามีได้ปฏิบัติตามสัญญา

เมื่อครบกำหนดการส่งมอบงานตามระยะเวลาการส่งมอบที่กำหนดไว้ในสัญญา แต่ผู้เสนอราคายังไม่ได้ส่งมอบ หรือส่งมอบไม่ถูกต้องครบถ้วนตามที่กำหนดไว้ในสัญญา ผู้เสนอราคาจะต้องชำระค่าปรับให้กับสถาบันฯ เป็นรายวันในอัตราร้อยละ 0.10 ของราคาที่ตกลงจัดจ้าง

9. เงื่อนไขการจ้าง

9.1 ผู้เสนอราคาที่ได้รับคัดเลือกจะต้องทำสัญญาจัดจ้างตามแบบสัญญาที่สถาบันฯ กำหนด และจะต้องวางหลักประกันการปฏิบัติตามสัญญาเป็นจำนวนเงินเท่ากับร้อยละ 5 ของราคาที่ตกลง จัดจ้าง ให้สถาบันฯ ยึดถือไว้ในขณะทำสัญญาโดยใช้หลักประกันอย่างหนึ่งอย่างใด ดังต่อไปนี้

(1) เงินสด

(2) แคนเชียร์เช็คที่ธนาคารส่งจ่ายให้แก่ สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน) โดยเป็นเช็คลงวันที่ทำสัญญาหรือก่อนหน้านั้นไม่เกิน 3 วันทำการ

(3) หนังสือค้ำประกันของธนาคารภายในประเทศ

9.2 ผู้เสนอราคาซึ่งสถาบันฯ ได้คัดเลือกแล้วไม่ไปทำสัญญา หรือข้อตกลงภายในเวลาที่สถาบันฯ กำหนด สถาบันฯ อาจพิจารณาเรียกร้องให้ชดใช้ความเสียหายอื่นๆ (ถ้ามี) รวมทั้งจะพิจารณาให้เป็นผู้ทำงาน

9.3 สถาบันฯ สงวนสิทธิ์ที่จะแก้ไขเพิ่มเติมเงื่อนไขหรือข้อกำหนดในแบบสัญญาให้เหมาะสมได้

9.4 สถาบันฯ สงวนสิทธิ์ในการลงนามสัญญาจ้างกับผู้เสนอราคาซึ่งได้รับการพิจารณาแล้ว เห็นว่ามีความเหมาะสมและเป็นประโยชน์สูงสุดกับสถาบันฯ โดยไม่จำเป็นต้องเป็นผู้เสนอราคาต่ำสุด แต่ทั้งนี้ต้องอยู่ในวงเงินงบประมาณที่ได้รับจัดสรร

10. หน่วยงานรับผิดชอบดำเนินการ

สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติม สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน) 140, 140/1-3, 140/5 อาคารไอทีเอฟ ทาวเวอร์ ชั้น 1 - 4 และชั้น 6 ถนนสีลม แขวงสุริยวงศ์ เขตบางรัก กรุงเทพฯ 10500

(1) ส่วนงานพัสดุฯ โทรศัพท์ 0 2634 4999 ต่อ 617 โทรสาร 0 2634 4970

(2) ฝ่ายเทคโนโลยีสารสนเทศ โทรศัพท์ 0 2634 4999 ต่อ 434 โทรสาร 0 2634 4970

ฝ่ายเทคโนโลยีสารสนเทศ
สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน)

สมคิด อรรถ