ขอบเขตของงาน (Terms of Reference : TOR)
การจัดจ้างที่ปรึกษางานระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ
(Information Security Management Systems)
ตามมาตรฐาน ISO/IEC 27001:2013
สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน)

---

1. ความเป็นมา

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

มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานการรักษาความมั่นคงปลอดภัยของสารสนเทศที่ได้รับการยอมรับในระดับนานาชาติ อีกทั้งยังเป็นมาตรฐานที่นำมาใช้อ้างอิงในกฎหมายด้านเทคโนโลยีสารสนเทศและการสื่อสาร แนวนโยบาย และแนวทางปฏิบัติที่บังคับใช้ของประเทศไทย อาทิ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 แนวนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553

ด้วยเหตุดังกล่าว ในปีงบประมาณ 2558 สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน) ซึ่งเป็นหน่วยงานภาครัฐที่นำระบบสารสนเทศมาใช้ในการเพิ่มประสิทธิภาพในงานบริหารจัดการองค์กร งานวิจัย และงานบริการต่างๆ จึงได้จัดทำระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 ซึ่งเป็นมาตรฐานด้านความมั่นคงปลอดภัยของสารสนเทศรุ่น (Version) ปัจจุบัน โดยมีวัตถุประสงค์เพื่อสร้างความปลอดภัยให้กับระบบสารสนเทศของสถาบันฯ ตลอดจนสามารถสร้างความเชื่อมั่นให้กับลูกค้าหรือผู้ใช้บริการระบบสารสนเทศได้ แต่เนื่องจาก สถาบันฯ ขาดบุคลากรที่มีความรู้และความเชี่ยวชาญในการดำเนินระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 จึงจำเป็นต้องจัดจ้างที่ปรึกษาเพื่อให้คำแนะนำและฝึกอบรมบุคลากรของสถาบันฯ ในการดำเนินระบบฯ และเตรียมความพร้อมเพื่อขอการรับรองมาตรฐาน ISO/IEC 27001:2013 ดังกล่าวต่อไป

2. วัตถุประสงค์

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

/3. คุณสมบัติ...

3. คุณสมบัติของผู้เสนอราคา

3.1 ผู้เสนอราคาจะต้องมีผลงานเกี่ยวกับการเป็นที่ปรึกษางานระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001 พร้อมสำเนาสัญญาผลงานที่กล่าวอ้างซึ่งเป็นวงเงินไม่น้อยกว่า 500,000 บาท (ห้าแสนบาทถ้วน) 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 ผู้เสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลการสั่งให้นิติบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของ ทางราชการ

3.4 ผู้เสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น

4. ขอบเขตการดำเนินงาน

ขอบเขตการดำเนินงานของที่ปรึกษางานระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน ISO/IEC 27001:2013 มีดังนี้

4.1 <u>การวางแผน (Planning)</u>

4.1.1 แนะนำและให้คำปรึกษาในการทบทวนแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันฯ รวมทั้งการปรับกิจกรรมให้สอดคล้องกับแผนฯ

4.2 <u>การปฏิบัติงาน (Doing)</u>

4.2.1 ฝึกอบรมให้กับบุคลากรซึ่งเป็นคณะทำงานหรือผู้ที่เกี่ยวข้อง ณ สำนักงานของสถาบันฯ หรือสถานที่ที่สถาบันฯ จัดให้ ในหลักสูตรดังต่อไปนี้เป็นอย่างน้อย

4.2.1.1 หลักสูตรเกี่ยวกับการสร้างความตระหนักและแนวปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของสารสนเทศ (ISMS Awareness Training Course)

4.2.1.2 หลักสูตรเกี่ยวกับการตรวจประเมินภายในระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (ISMS Internal Auditor Training Course)

4.2.2 แนะนำและให้คำปรึกษาในการจัดทำระเบียบปฏิบัติ (Procedure) รวมทั้งปรับปรุงและบูรณาการเอกสารด้านความมั่นคงปลอดภัยของสารสนเทศของสถาบันฯ

4.2.3 แนะนำและให้คำปรึกษาในปรับปรุงระบบสารสนเทศให้มีความมั่นคงปลอดภัย (Information System Hardening)

/4.3 การติดตาม...

4.3 การติดตามและประเมินผล (Checking and Acting)

4.3.1 แนะนำและให้คำปรึกษาแก่คณะทำงานในการตรวจสอบช่องโหว่ด้านความมั่นคงปลอดภัยของสารสนเทศ (Vulnerabilities) รวมถึงแนะนำแนวทางแก้ไขช่องโหว่ที่ตรวจพบ

4.3.2 แนะนำและให้คำปรึกษาในการตรวจประเมินภายในโดยคณะทำงานหรือบุคลากรซึ่งได้รับมอบหมายให้เป็นคณะผู้ตรวจสอบภายในตามมาตรฐาน ISO/IEC 27001:2013

4.3.3 แนะนำและให้คำปรึกษาในการแก้ไขข้อบกพร่องหรือจุดอ่อนที่พบจากการตรวจประเมินภายใน

4.3.4 ตรวจประเมินความพร้อมทั้งระบบก่อนขอการรับรองมาตรฐาน ISO/IEC 27001:2013

4.3.5 ให้คำแนะนำในการแก้ไขข้อบกพร่องภายหลังการตรวจประเมินเพื่อขอการรับรองจากผู้ตรวจประเมินภายนอก (Certified Body)

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 10 เดือน นับแต่วันที่ลงนามในสัญญา โดยผู้เสนอราคาจะต้องจัดทำแผนดำเนินงานและแจ้งเป็นหนังสือให้สถาบันฯ ทราบก่อนดำเนินงานภายใน 15 วัน นับแต่วันที่ลงนามในสัญญา

7. การชำระเงิน

7.1 เงินงวดที่ 1 ในอัตราร้อยละ 20 ของราคาที่ตกลงจัดจ้าง โดยจะชำระภายใน 15 วัน นับแต่วันที่ลงนามในสัญญา

7.2 เงินงวดที่ 2 ในอัตราร้อยละ 30 ของราคาที่ตกลงจัดจ้าง โดยจะชำระภายใน 30 วัน นับแต่วันที่ผู้เสนอราคาได้อบรมบุคลากรซึ่งเป็นคณะทำงานหรือผู้ที่เกี่ยวข้องตามที่ระบุในข้อ 4.2.1 เป็นที่เรียบร้อยแล้ว

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

8. ค่าปรับกรณีผู้เสนอราคามิได้ปฏิบัติตามสัญญา

เมื่อครบกำหนดการส่งมอบงานตามระยะเวลาการส่งมอบที่กำหนดไว้ในสัญญา แต่ผู้เสนอราคายังไม่ได้ส่งมอบ หรือส่งมอบไม่ถูกต้องครบถ้วนตามที่กำหนดไว้ในสัญญา ผู้เสนอราคาจะต้องชำระค่าปรับให้กับสถาบันฯ เป็นรายวันในอัตราร้อยละ 0.10 ของราคาที่ตกลงจัดจ้าง

/9. เงื่อนไข...

9. เงื่อนไขการจ้าง

9.1 ผู้เสนอราคาที่ได้รับคัดเลือกจะต้องทำสัญญาจัดจ้างตามแบบสัญญาที่สถาบันฯ กำหนด และจะต้องวางหลักประกันการปฏิบัติตามสัญญาเป็นจำนวนเงินเท่ากับร้อยละ 5 ของราคาที่ตกลง จัดจ้าง ให้สถาบันฯ ยึดถือไว้ในขณะทำสัญญาโดยใช้หลักประกันอย่างหนึ่งอย่างใด ดังต่อไปนี้

(1) เงินสด

(2) แคชเชียร์เช็คที่ธนาคารสั่งจ่ายให้แก่ สถาบันวิจัยและพัฒนาอัญมณีและเครื่องประดับแห่งชาติ (องค์การมหาชน) โดยเป็นเช็คลงวันที่ที่ทำสัญญาหรือก่อนหน้านั้นไม่เกิน 3 วันทำการ

(3) หนังสือค้ำประกันของธนาคารภายในประเทศ

9.2 ผู้เสนอราคาซึ่งสถาบันฯ ได้คัดเลือกแล้วไม่ไปทำสัญญา หรือข้อตกลงภายในเวลาที่สถาบันฯ กำหนด สถาบันฯ อาจพิจารณาเรียกร้องให้ชดใช้ความเสียหายอื่นๆ (ถ้ามี) รวมทั้งจะพิจารณาให้เป็นผู้ทิ้งงาน

9.3 สถาบันฯ สงวนสิทธิที่จะแก้ไขเพิ่มเติมเงื่อนไขหรือข้อกำหนดในแบบสัญญาให้เหมาะสมได้

9.4 สถาบันฯ สงวนสิทธิในการลงนามสัญญาจ้างกับผู้เสนอราคาซึ่งได้รับการพิจารณาแล้วเห็นว่ามีความเหมาะสมและเป็นประโยชน์สูงสุดกับสถาบันฯ 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) ส่วนงานจัดซื้อและพัสดุฯ 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)