เอกสารข้อกำหนดการจัดจ้าง
โครงการที่ปรึกษาในการจัดทำระบบบริหารความมั่นคงปลอดภัยสารสนเทศ
(Information Security Management System: ISMS)

บริษัท เฮงลิสซิ่ง แอนด์ แคปปิตอล จำกัด (มหาชน) มีความประสงค์ในการเชิญบริษัทที่ปรึกษาที่สนใจ จัดทำข้อเสนอโครงการ เพื่อการพิจารณาคัดเลือกบริษัทที่ปรึกษาที่มีคุณสมบัติเหมาะสมเป็นผู้ดำเนินการให้คำปรึกษาแก่ บริษัท เฮงลิสซิ่ง แอนด์ แคปปิตอล จำกัด (มหาชน) ในการจัดทำระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามข้อกำหนดของมาตรฐาน ISO 27001 โดยมีรายละเอียดดังต่อไปนี้

คำจำกัดความ

องค์กร	หมายถึง	บริษัท เฮงลิสซิ่ง แอนด์ แคปปิตอล จำกัด (มหาชน)
ผู้เสนอราคา	หมายถึง	นิติบุคคล หรือกลุ่มนิติบุคคล ที่มีสิทธิเข้าเสนอราคา เพื่อการรับจ้างดำเนินโครงการ
โครงการ	หมายถึง	โครงการที่ปรึกษาในการจัดทำระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS)
ผู้ว่าจ้าง	หมายถึง	บริษัท เฮงลิสซิ่ง แอนด์ แคปปิตอล จำกัด (มหาชน)
ผู้รับจ้าง	หมายถึง	ผู้เสนอราคาซึ่งได้รับการพิจารณาคัดเลือกและได้ลงนามในสัญญา
ผู้ตรวจสอบ	หมายถึง	องค์กรที่ได้รับอนุญาตให้ทำการตรวจสอบและออกประกาศนียบัตรรับรองมาตรฐาน ISO 27001 (Certification Body)

1 หลักการและเหตุผล

การดำเนินภารกิจขององค์กรในปัจจุบัน มีความเกี่ยวข้องกับข้อมูลลับและข้อมูลส่วนบุคคล โดยมีการนำระบบเทคโนโลยีสารสนเทศและการสื่อสาร มาใช้เป็นเครื่องมือในการจัดเก็บและประมวลผลข้อมูลดังกล่าว เพื่อสนับสนุนการดำเนินภารกิจขององค์กร ทั้งนี้ ข้อมูลและระบบเทคโนโลยีสารสนเทศ ถือเป็นทรัพย์สินที่มีค่าและสำคัญต่อองค์กรเป็นอย่างยิ่ง องค์กรจึงมีความต้องการจัดจ้างที่ปรึกษาที่มีความรู้ ความเชี่ยวชาญพิเศษเกี่ยวกับข้อกำหนดของมาตรฐาน ISO 27001 ซึ่งเป็นมาตรฐานสากลด้านการบริหารความมั่นคงปลอดภัยสารสนเทศ เพื่อให้คำปรึกษาแก่องค์กรในการจัดทำระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามข้อกำหนดของมาตรฐานดังกล่าว เพื่อปกป้องข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กรจากภัยคุกคามและความเสี่ยงในรูปแบบต่างๆ สามารถดำเนินภารกิจและปฏิบัติงานได้อย่างสอดคล้องกับข้อกำหนดของกฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง และเพื่อยกระดับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในองค์กร ให้ก้าวไปสู่ระดับสากล

2 วัตถุประสงค์ของโครงการ

เพื่อจัดจ้างบริษัทที่ปรึกษาผู้เชี่ยวชาญ เข้าให้คำปรึกษาในการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ในส่วนที่เกี่ยวข้องกับ Data Center และ Heng Application ให้สอดคล้องกับมาตรฐานการบริหารความมั่นคงปลอดภัยสารสนเทศ ISO 27001 และเตรียมความพร้อมเพื่อให้ได้การรับรอง (Certified) ภายใน 6 เดือน

3 ขอบเขตของงาน

ผู้รับจ้างต้องให้คำปรึกษาในการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ในส่วนที่เกี่ยวข้องกับระบบ Data Center และ Heng Application ดังนี้

3.1 ดำเนินการทำ Gap Analysis เพื่อวิเคราะห์การดำเนินงานในส่วนที่เกี่ยวข้องกับขอบข่ายของระบบ ISMS ขององค์กร เปรียบเทียบกับข้อกำหนดทั้ง 114 ข้อ ใน Annex A ของมาตรฐาน ISO 27001 พร้อมทั้งจัดทำรายงานสรุปผลการวิเคราะห์

3.2 จัดฝึกอบรมและให้ความรู้เกี่ยวกับมาตรฐาน ISO 27001 สำหรับเจ้าหน้าที่ขององค์กร เพื่อให้มีความรู้เพียงพอ ต่อการพัฒนาและปฏิบัติใช้ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) โดยครอบคลุมหัวข้อการอบรมอย่างน้อยดังนี้

3.2.1 ความรู้เกี่ยวกับข้อกำหนดของมาตรฐาน ISO 27001 และการพัฒนาและปฏิบัติใช้ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) สำหรับผู้บริหารและผู้ปฏิบัติงานขององค์กร

3.2.2 การประเมินความเสี่ยงและการบริหารความเสี่ยง (Risk Management)

3.2.3 การจัดทำนโยบายและขั้นตอนปฏิบัติงานด้านความมั่นคงปลอดภัย (Security Policy & Procedure) และเอกสารที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS)

3.2.4 การตรวจประเมินภายในสำหรับระบบ ISMS (Internal ISMS Audit)

3.2.5 หลักสูตรอื่นๆ ที่เป็นประโยชน์และเกี่ยวข้องกับการจัดทำระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) เพื่อนำไปสู่การได้รับการรับรองระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Certification) ตามมาตรฐาน ISO 27001

3.3 ให้คำปรึกษาและสนับสนุนในการจัดทำและตรวจสอบเอกสารที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) อย่างน้อยดังนี้

3.3.1 แผนการดำเนินโครงการ (Project Plan)

3.3.2 รายงานการประเมินความเสี่ยง (Risk Assessment Report)

3.3.3 แผนการจัดการกับความเสี่ยง (Risk Treatment Plan)

3.3.4 นโยบายและขั้นตอนปฏิบัติงานด้านความมั่นคงปลอดภัย (Security Policy & Procedure)

3.3.5 เอกสารอื่นๆ ที่เกี่ยวข้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) เพื่อนำไปสู่การได้รับการรับรองระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Certification) ตามมาตรฐาน ISO 27001

3.4 จัดหาแม่แบบ (Template) สำหรับการจัดทำเอกสาร อย่างน้อยดังนี้

3.4.1 นโยบายและขั้นตอนปฏิบัติงานด้านความมั่นคงปลอดภัย (Security Policy & Procedure)

3.4.2 เอกสาร Statement of Applicability

3.4.3 เอกสารอื่นๆ ที่จำเป็นสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) เพื่อนำไปสู่การได้รับการรับรองระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Certification) ตามมาตรฐาน ISO 27001

3.5 ให้คำปรึกษาและความสนับสนุนเกี่ยวกับการออกแบบ พัฒนา และปฏิบัติใช้กระบวนการและมาตรการควบคุมความมั่นคงปลอดภัยต่างๆ ที่มีความสำคัญต่อระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) อย่างน้อยดังนี้

3.5.1 การประเมินความเสี่ยง (Risk Assessment)

3.5.2 การแก้ไขความเสี่ยง (Risk Treatment)

3.5.3 การบังคับใช้นโยบายและขั้นตอนปฏิบัติงานด้านความมั่นคงปลอดภัย

3.5.4 การตรวจประเมินภายในสำหรับระบบ ISMS (Internal ISMS Audit)

3.5.5 กิจกรรมหรือกระบวนการอื่นๆ ที่จำเป็นสำหรับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) เพื่อนำไปสู่การได้รับการรับรองระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Certification) ตามมาตรฐาน ISO 27001

3.6 ให้คำแนะนำในการคัดเลือกหน่วยงานที่ให้การรับรองมาตรฐาน ISO 27001 (Certification Body: CB) และดำเนินการเพื่อเตรียมความพร้อมให้แก่องค์กร ก่อนการตรวจรับรองมาตรฐาน ISO 27001 (Certification Audit)

3.7 ให้ความสนับสนุนในระหว่างการตรวจรับรองมาตรฐาน ISO 27001 (Certification Audit)

3.8 ดำเนินการสรุปผล และข้อเสนอแนะภายหลังการตรวจรับรองมาตรฐาน ISO 27001 (Certification Audit) ก่อนปิดโครงการ

4 ระยะเวลาในการดำเนินโครงการ

ผู้รับจ้างต้องดำเนินการตามรายละเอียดของงานในข้อ 3.1 ถึง 3.8 ให้แล้วเสร็จภายใน 6 เดือนนับจากวันเริ่มต้นโครงการ (Kick-off Meeting)

5 คุณสมบัติของผู้เสนอราคา

5.1 ผู้เสนอราคาต้องเป็นบริษัทที่จดทะเบียนในประเทศไทยมาเป็นเวลาไม่ต่ำกว่า 5 ปี และมีวัตถุประสงค์ในการดำเนินธุรกิจที่เกี่ยวข้องกับการให้คำปรึกษาและตรวจสอบด้านความมั่นคงปลอดภัย

5.2 ผู้เสนอราคาต้องเป็นผู้มีความรู้ความสามารถเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security) และมาตรฐาน ISO 27001 โดยต้องมีประสบการณ์ตรงในการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) ให้กับหน่วยงานต่างๆ ในประเทศไทย จนได้รับการรับรองมาตรฐาน ISO 27001:2013

มาแล้วไม่น้อยกว่า 5 หน่วยงาน โดยต้องมีอย่างน้อย 2 หน่วยงานที่เป็นธนาคารหรือสถาบันการเงิน โดยต้องมีหนังสือรับรองผลงานหรือสำเนาสัญญามาเสนอเป็นหลักฐานหรือหลักฐานอื่นๆ ที่สามรถระบุได้

5.3 ต้องมีบุคลากรที่มีความรู้และประสบการณ์ ในการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS) และมาตรฐาน ISO 27001 โดยอย่างน้อยต้องมีมีผู้จัดการโครงการ (Project Manager) และหัวหน้าทีมที่ปรึกษา (Lead Consultant) ที่ได้รับประกาศนียบัตรรับรองคุณวุฒิในระดับ ISO 27001 Lead Implementor จาก PECB

5.4 การดำเนินโครงการต้องได้รับการควบคุมคุณภาพโดยผู้ควบคุมคุณภาพ (QA) ที่ได้รับประกาศนียบัตรรับรองคุณวุฒิในระดับ ISO 27001 Lead Implementor จาก PECB

5.5 บุคลากรที่เสนอชื่อตามข้อ 5.3 – 5.4 ต้องถือสัญชาติไทยและพำนักอยู่ในประเทศไทยตลอดระยะเวลาในการดำเนินโครงการ

5.6 ต้องเป็นบริษัทที่ปรึกษาที่ได้รับอนุมัติขึ้นทะเบียนจากศูนย์ข้อมูลที่ปรึกษาไทย กระทรวงการคลัง สาขา ISO 27001 ระดับ 1

5.7 ต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการ และได้รับหนังสือแจ้งเวียนชื่อแล้วหรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ

6 การส่งมอบงาน

ผู้รับจ้างต้องส่งมอบผลงานดังนี้

6.1 รายงาน Gap Analysis Report

6.2 หลักสูตรฝึกอบรมตามที่ระบุไว้ในหัวข้อ 3.2.1-3.2.5

6.3 เอกสารสรุปการให้คำปรึกษาตามที่ระบุไว้ในหัวข้อ 3.3.1-3.3.5

6.4 เอกสารแม่แบบ (Template) ตามที่ระบุไว้ในหัวข้อ 3.4.1-3.4.3

6.5 เอกสารสรุปการให้คำปรึกษาตามที่ระบุไว้ในหัวข้อ 3.5.1-3.5.5

7 เงื่อนไขการชำระเงิน

องค์กรจะชำระเงินให้แก่ผู้รับจ้างโดยแบ่งเป็นงวดๆ ตามความคืบหน้าของการดำเนินโครงการ ทั้งนี้การส่งมอบงาน ต้องผ่านการตรวจรับงานโดยองค์กรหรือตัวแทนที่ได้รับมอบหมาย ดังนี้

7.1 งวดที่ 1 องค์กร จะชำระเงินให้ผู้รับจ้าง 20% ของวงเงินตามสัญญา เมื่อผู้รับจ้างดำเนินการและส่งมอบงานตามข้อ 3.1 แล้วเสร็จ

7.2 งวดที่ 2 องค์กร จะชำระเงินให้ผู้รับจ้าง 25% ของวงเงินตามสัญญา เมื่อผู้รับจ้างดำเนินการและส่งมอบงานตามข้อ 3.2.1-3.2.2, 3.3.1-3.3.3 และ 3.5.1-3.5.2 แล้วเสร็จ

7.3 งวดที่ 3 องค์กร จะชำระเงินให้ผู้รับจ้าง 25% ของวงเงินตามสัญญา เมื่อผู้รับจ้างดำเนินการและส่งมอบงานตามข้อ 3.2, 3.3, 3.4 และ 3.5 ในส่วนที่เหลือทั้งหมด แล้วเสร็จ

7.4 งวดที่ 4 (งวดสุดท้าย) องค์กร จะชำระเงินให้ผู้รับจ้าง 30% ของวงเงินตามสัญญา เมื่อผู้รับจ้างดำเนินการและส่งมอบงานตามข้อ 3.6-3.8 แล้วเสร็จ

8 การสนับสนุนจากผู้ว่าจ้าง

8.1 องค์กร จะจัดเตรียมสถานที่ และสิ่งอำนวยความสะดวกสำหรับการปฏิบัติงานของผู้รับจ้าง

8.2 องค์กร จะจัดตั้งคณะทำงานเพื่อรับผิดชอบในการทำงานตามคำแนะนำของผู้รับจ้าง ตลอดจนประสานงานกับส่วนงานต่างๆ ที่เกี่ยวข้องภายในองค์กร

8.3 องค์กร จะเป็นผู้รับผิดชอบค่าใช้จ่ายในการจ้างหน่วยงานที่ให้การรับรองมาตรฐาน ISO 27001 (Certification Body: CB)

8.4 องค์กร จะเป็นผู้รับผิดชอบค่าใช้จ่ายในการเดินทาง ตลอดจนค่าที่พักและสิ่งอำนวยความสะดวกอื่นๆ ที่เกี่ยวข้อง สำหรับการให้คำปรึกษา ตามที่เกิดขึ้นจริง