

ขอบเขตของงาน (Terms of Reference : TOR)
โครงการจ้างบริการศูนย์เฝ้าระวังความปลอดภัยไซเบอร์ระบบ e-Service
ของกรมการกงสุล จำนวน ๑๒ เดือน

๑. หลักการและเหตุผล

กรมการกงสุล มีบทบาทสำคัญในการให้บริการด้านการกงสุลทั้งในและต่างประเทศ โดยเฉพาะอย่างยิ่งการให้บริการระบบ e-Service ของกรมการกงสุลมีการจัดเก็บข้อมูลที่มีความสำคัญ อาทิ ข้อมูลส่วนบุคคลของประชาชน ข้อมูลสถิติคนไทยในต่างประเทศ และข้อมูลที่เกี่ยวข้องกับการให้ความช่วยเหลือในสถานการณ์ฉุกเฉิน ข้อมูลเหล่านี้มีความอ่อนไหวและจำเป็นต้องได้รับการคุ้มครองอย่างเข้มงวด ซึ่งภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบันมีลักษณะซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว อาทิ การแพร่กระจายมัลแวร์ และการโจมตีผ่านระบบเครือข่าย การป้องกันภัยคุกคามเหล่านี้จำเป็นต้องอาศัยเทคโนโลยีที่ทันสมัยและการเฝ้าระวังระบบอย่างต่อเนื่อง

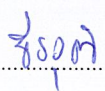
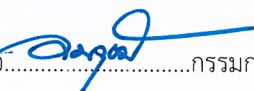
เพื่อเสริมสร้างความมั่นคงปลอดภัยในระบบ e-Service กรมการกงสุลจึงมีความจำเป็นต้องจ้างบริการดูแลรักษาความปลอดภัยทางไซเบอร์ โดยให้ผู้รับจ้างที่มีความเชี่ยวชาญเข้ามาดำเนินการดูแลระบบตลอด ๒๔ ชั่วโมง ๗ วัน เพื่อให้มั่นใจว่าระบบมีความปลอดภัยและสามารถตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ

๒. วัตถุประสงค์

- ๒.๑ เพื่อเฝ้าระวังและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับระบบ e-Services ของกรมการกงสุล
- ๒.๒ เพื่อเพิ่มประสิทธิภาพในการตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์
- ๒.๓ เพื่อปกป้องข้อมูลส่วนบุคคลของประชาชนและระบบการทำงานของกรมการกงสุลจากการโจมตีทางไซเบอร์
- ๒.๔ เพื่อเตรียมความพร้อมของกรมการกงสุลในการปฏิบัติตามกฎหมายและข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์

๓. คุณสมบัติของผู้ยื่นข้อเสนอ

- ๓.๑ มีความสามารถตามกฎหมาย
- ๓.๒ ไม่เป็นบุคคลล้มละลาย
- ๓.๓ ไม่อยู่ระหว่างเลิกกิจการ
- ๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง
- ๓.๕ ไม่เป็นบุคคลซึ่งถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วน ผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย
- ๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

ลงชื่อ..........ประธานกรรมการ ลงชื่อ..........กรรมการ ลงชื่อ..........กรรมการ

๓.๗ เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่กระทรวงการต่างประเทศ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

๓.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติ ดังนี้

(๑) การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

(๒) กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

(๓) การยื่นข้อเสนอของกิจการร่วมค้า

(๓.๑) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่ง เป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

(๓.๒) การยื่นข้อเสนอด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) ให้ผู้เข้าร่วมค้าที่ได้รับมอบหมายหรือมอบอำนาจตามข้อ (๓.๑) ดำเนินการซื้อเอกสารประกวดราคาอิเล็กทรอนิกส์ กรณีที่มีการจำหน่ายเอกสารซื้อหรือจ้าง

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

๓.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

๑. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศ ซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ ๑ ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนออยู่นั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก ๑ ปี ได้

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

๒. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มีรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๒ ล้านบาท

๓. สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมี เงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอ ในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

๔. กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดา ที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจ ค้าประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทย แจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือ บุคคลธรรมดาที่ไม่ได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารต่างประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้าประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

๕. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือ บุคคลธรรมดาที่ไม่ได้ถือสัญชาติไทยตามข้อ ๒ ข้อ ๓ และข้อ ๔ (๒) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตรา ตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e-GP) จนถึงวันเสนอราคา

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศว่าด้วย

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

การรับรองเอกสาร พ.ศ. ๒๕๓๙ และที่แก้ไขเพิ่มเติม กำหนด โดยจะต้องยื่นเอกสารดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอไม่ได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่าผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

๖. กรณีตามข้อ ๑ - และข้อ ๕ ไม่ใช่บังคับกับกรณีดังต่อไปนี้

(๖.๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

(๖.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตาม

พระราชบัญญัติล้มละลาย พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม

(๖.๓) งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติเบื้องต้นไว้แล้ว ก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

(๖.๔) การจัดซื้อจัดจ้างตามมาตรา ๕๖ วรรคหนึ่ง (๒) (ข) และ (ค) แห่งพระราชบัญญัติการจัดซื้อจัดจ้างฯ

(๖.๕) การซื้อสังหาริมทรัพย์และการเช่าสังหาริมทรัพย์

(๖.๖) กรณีงานจ้างบริการหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงานขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

๔. รายละเอียดขอบเขตของงาน

๔.๑ การให้บริการเฝ้าระวังความปลอดภัยไซเบอร์

ผู้รับจ้างต้องเสนอบริการเฝ้าระวังความปลอดภัยไซเบอร์ โดยมีคุณสมบัติ ดังนี้

๔.๑.๑ บริการระบบจัดเก็บรวบรวมและวิเคราะห์ข้อมูลความปลอดภัยทางเครือข่ายคอมพิวเตอร์ (SIEM) เพื่อจัดเก็บรวบรวมและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์จากอุปกรณ์เครือข่ายและรักษาความมั่นคงปลอดภัยของกรมการกงสุล โดยมีคุณสมบัติ ดังนี้

๔.๑.๑.๑ บริการที่ถูกรออกแบบมา เพื่อวิเคราะห์ข้อมูลทางด้านการรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ หรือ Security Information and Event Management (SIEM) โดยเฉพาะ

๔.๑.๑.๒ ผู้รับจ้างจะต้องใช้ผลิตภัณฑ์ระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ SIEM ที่อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for Security Information and Event Management (SIEM) ประจำปี ๒๐๒๔ และได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Forrester Wave Security Analytics Platforms ประจำปี ๒๐๒๒ สามารถรองรับปริมาณการใช้งาน ๕๐ GB/Day

๔.๑.๑.๓ สามารถจัดเก็บข้อมูล Log จากอุปกรณ์ในระบบเครือข่ายคอมพิวเตอร์ (Log Source) ของกรมการกงสุลได้น้อย ดังนี้

๑) ระบบ Cloudflare ของกรมการกงสุล

๒) ระบบ Zscaler ของกรมการกงสุล

๓) ระบบ EDR ของกรมการกงสุล

๔) ระบบสารสนเทศของกรมการกงสุลที่ใช้บริการระบบคลาวด์กลางภาครัฐ (Government Data Center and Cloud Service: GDCC)

๕) ระบบศูนย์บริหารข้อมูลกลางกรมการกงสุล (CCDC)

ลงชื่อ.....อธิบดี.....ประธานกรรมการ ลงชื่อ.....อธิบดี.....กรรมการ ลงชื่อ.....อธิบดี.....กรรมการ

๔.๑.๑.๔ สามารถจัดเก็บข้อมูล Log ตามระบบที่กรมการกงสุลกำหนด และสามารถจัดเก็บข้อมูลได้ไม่น้อยกว่า ๙๐ วัน

๔.๑.๑.๕ สามารถ Export ข้อมูล Log ในรูปแบบ XML หรือ CSV ได้

๔.๑.๑.๖ สามารถค้นหา (Search) ข้อมูล Log ด้วย Keyword หรือ Full Text ได้จากชื่อเครื่องคอมพิวเตอร์ ชื่อผู้ใช้ IP Address ช่วงวัน และช่วงเวลา เป็นอย่างน้อย

๔.๑.๑.๗ สามารถวิเคราะห์พฤติกรรมการเข้าใช้งานของผู้ใช้งาน โดยตรวจสอบและแจ้งเตือนภัยคุกคาม ได้อย่างน้อยดังนี้

- ๑) Web Attack
- ๒) Potentially unwanted program (PUP)
- ๓) Brute Force
- ๔) Data Transfer Volume
- ๕) Lateral Movement
- ๖) Suspicious Privileged Activity

๔.๑.๑.๘ สามารถปรับแต่ง (Customization) การแสดงผล (Dashboard) รายงาน (Report) การแจ้งเตือน (Alert) และ การสร้างความสัมพันธ์ของข้อมูล (Correlation) ของภัยคุกคามได้

๔.๑.๑.๙ สามารถแจ้งเตือน (Alert) เหตุการณ์ด้านความปลอดภัยและ ความผิดปกติในเครือข่ายให้ผู้ดูแลระบบ โดยมีรูปแบบเหตุการณ์อย่างน้อย ดังนี้

- ๑) Port Scanning
- ๒) Brute Force Attack
- ๓) DDoS Attack
- ๔) Botnet
- ๕) Malware Outbreak

๔.๑.๑.๑๐ สามารถ Export รายงานในรูปแบบ PDF และ CSV ได้

๔.๑.๑.๑๑ สามารถทำงานบนเครือข่าย IPv๔ และ IPv๖

๔.๑.๑.๑๒ สามารถทำงานร่วมกับระบบ Network Time Protocol ได้

๔.๑.๒ ผู้รับจ้างจะต้องเสนอบริการซอฟต์แวร์รักษาความปลอดภัยที่ช่วยตรวจจับและป้องกันภัยคุกคามที่มุ่งโจมตีอุปกรณ์ปลายทางในเครือข่าย (Endpoint Detection and Response : EDR) โดยสามารถกักกันเครื่อง เมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยมีคุณสมบัติ ดังต่อไปนี้

๔.๑.๒.๑ สามารถติดตั้งบนเครื่องคอมพิวเตอร์ แม้าข่ายและเครื่องคอมพิวเตอร์ของเจ้าหน้าที่ของกรมการกงสุลได้ไม่น้อยกว่า ๑๕๐ เครื่อง บนระบบปฏิบัติการ Windows Server ๒๐๑๙, Windows Server ๒๐๒๒, Windows ๑๐/๑๑, MacOS, Linux, Ubuntu และ CentOS ได้เป็นอย่างน้อย

๔.๑.๒.๒ ผู้รับจ้างต้องใช้ผลิตภัณฑ์รักษาความปลอดภัยที่ช่วยตรวจจับและป้องกันภัยคุกคามที่มุ่งโจมตีอุปกรณ์ปลายทางในเครือข่าย (Endpoint Detection and Response : EDR) และต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Endpoint Protection Platforms ประจำปี ๒๐๒๔ และ Forrester Wave Endpoint Security ประจำปี ๒๐๒๓ และ Forrester Wave for External Threat Intelligence Services Providers ประจำปี ๒๐๒๓

๔.๑.๒.๓ มีระบบบริหารจัดการแบบ Cloud management (SaaS) การเชื่อมต่อระหว่าง Agent กับ Cloud Management และเข้ารหัสแบบ TLS-Encrypted เพื่อความปลอดภัย สามารถบริหารจัดการแบบรวมศูนย์ (single console) โดยต้องบริหารจัดการ Policy ของ Endpoint ได้อย่างน้อยบนระบบปฏิบัติการ Windows Linux MacOS ใช้งานผ่านทาง Web Console และมีระบบยืนยันตัวตนด้วย MFA ได้

๔.๑.๒.๔ สามารถป้องกัน Malware และ การโจมตีที่ไม่เกิดจากมัลแวร์ (Malware-free attack) ด้วยเทคโนโลยี Machine learning และ Indicator of Attack (IOA) ได้เป็นอย่างดี

๔.๑.๒.๕ เป็นบริการที่มีความสามารถในการตรวจหาภัยคุกคามที่เกิดขึ้นในองค์กร (Threat Hunting) และสามารถหาข้อมูลความเกี่ยวข้องของภัยคุกคามที่เกิดขึ้น (Investigation) ของเครื่องคอมพิวเตอร์ที่ติดตั้ง Agent Software ได้

๔.๑.๒.๖ มีความสามารถในการป้องกันภัยคุกคามอย่างน้อย ดังนี้

- ๑) ป้องกันการโจมตีที่ช่องโหว่ของระบบ (Exploit Prevention)
- ๒) ป้องกันมัลแวร์ หรือไวรัส (Malware Prevention หรือ Antivirus)
- ๓) ป้องกันการโจมตีของมัลแวร์ระดับสูง ที่ใช้เทคนิคโจมตีแบบไม่ใช้ไฟล์

(Fileless Attacks)

๔) ป้องกันการโจมตีโดยใช้เทคนิคของ (AI-based local analysis engine)

หรือ Machine Learning

๕) ป้องกันการโจมตีโดยใช้การวิเคราะห์พฤติกรรม (Behavior)

๖) ป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware Protection)

๔.๑.๒.๗ มีความสามารถทำการตัดการเชื่อมต่อของระบบเครือข่าย (Network Containment) หรือแยกเครื่องคอมพิวเตอร์ที่มีความเสี่ยงจากภัยคุกคามออกจากระบบเครือข่าย (Isolate) บนเครื่องที่มีการติดตั้ง Agent Software

๔.๑.๒.๘ สามารถนำข้อมูลการแจ้งเตือนภัยคุกคามพร้อมแสดงข้อมูล MITRE ATT&CK Framework ของแต่ละรายการแจ้งเตือน

๔.๑.๒.๙ สามารถค้นหาข้อมูลการใช้งาน Source IP Address Domain และ Event ที่เกี่ยวข้องกับการใช้งาน (Activity) ได้

๔.๑.๒.๑๐ สามารถรองรับการตั้งค่าการส่ง Log จากระบบ EDR ไปยังระบบ SIEM ที่นำเสนอในโครงการได้

๔.๑.๒.๑๑ จัดให้มีผู้เชี่ยวชาญด้านการบริหารจัดการ EDR ที่ได้รับประกาศนียบัตรจากเจ้าของผลิตภัณฑ์อย่างน้อย ๑ คน เพื่อให้สามารถตรวจสอบการทำงานของระบบ EDR ได้อย่างถูกต้องและมีประสิทธิภาพ โดยแนบประวัติพร้อมใบประกาศนียบัตร (Certificate) ประกอบการยื่นข้อเสนอ

๔.๑.๓ ผู้รับจ้างต้องดำเนินการวิเคราะห์ เพื่อแจ้งภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศพร้อมเสนอแนวทางการแก้ไขหรือยับยั้งเหตุการณ์ให้ผู้ว่าจ้างทราบผ่านช่องทางอีเมล Line หรือช่องทางที่ทางกรมการกงสุลเห็นสมควร โดยสามารถใช้ระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ของผู้รับจ้างได้

๔.๑.๔ ผู้รับจ้างจะต้องดำเนินการแจ้งให้ผู้ว่าจ้างทราบทันทีทางโทรศัพท์เคลื่อนที่ของเจ้าหน้าที่ของกรมการกงสุลที่ได้รับมอบหมายและทางอีเมล หรือช่องทางที่ทางกรมการกงสุลเห็นสมควร พร้อมบันทึกในรายงานเฝ้าระวังภัยคุกคามทางไซเบอร์ (Incident Report) เมื่อพบว่ามีความรุนแรงตั้งแต่ระดับสูงขึ้นไป

๔.๑.๕ ผู้รับจ้างจะต้องดำเนินการแจ้งให้ผู้ว่าจ้างทราบทางอีเมล หรือช่องทางที่ทาง
กรมการกงสุลเห็นสมควร เมื่อพบว่ามีความรุนแรงตั้งแต่ระดับปานกลางจนถึงระดับต่ำ

๔.๑.๖ ผู้รับจ้างต้องดำเนินการหาสาเหตุและพิสูจน์หลักฐานของการโจมตีด้วยวิธีการ
Rootcause Analysis หรือ Digital forensic จำนวน ๑ ครั้ง ระยะเวลาที่ใช้ตรวจสอบแต่ละครั้งไม่เกิน
๑๐ วัน ก่อนดำเนินการตรวจสอบผู้ว่าจ้างจะแจ้งให้ทราบก่อนที่จะดำเนินการ

๔.๑.๗ ผู้รับจ้างต้องดำเนินการจัดทำรายงานเฝ้าระวังภัยคุกคามทางไซเบอร์ (Incident
Report) กรณีตรวจพบภัยคุกคามทางไซเบอร์ระดับความรุนแรงสูงมาก ภายในระยะเวลา ๒๔ ชั่วโมงโดยนับ
ถัดจากเวลาที่ตรวจพบหรือได้รับแจ้งจากเจ้าหน้าที่ของกรมการกงสุล โดยมีรายละเอียดของรายงานต้อง
ครอบคลุมเนื้อหาอย่างน้อยดังต่อไปนี้

๔.๑.๗.๑ ระบุประเภทของภัยคุกคาม

๔.๑.๗.๒ คำอธิบายอย่างละเอียด (Description)

๔.๑.๗.๓ วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

๔.๑.๗.๔ ระบุต้นทาง (Attacker) และปลายทาง (Target)

๔.๑.๗.๕ ภาพรวมการเชื่อมโยงเหตุการณ์ภัยคุกคามที่เกิดขึ้น

๔.๑.๗.๖ รายละเอียดเหตุการณ์และพฤติกรรมทั้งหมด โดยมีข้อมูลอย่างน้อย ได้แก่

๑) ผลกระทบ (Impact) (ถ้ามี)

๒) ระบบที่ได้รับผลกระทบ (System Affected) (ถ้ามี)

๓) แนวทางแก้ไข (Solution)

๔) อ้างอิง (Reference) (ถ้ามี)

๔.๑.๗.๗ ให้คำแนะนำพร้อมขั้นตอนการดำเนินการแก้ไขเชิงเทคนิคและแนวทางในการ
ป้องกันไม่ให้เกิดเหตุการณ์เดิมซ้ำอีก

๔.๑.๗.๘ ระบุระดับความรุนแรง (Severity) ตาม Service Level Agreement (SLA)
ตามข้อ ๕

๔.๑.๘ ผู้รับจ้างต้องดำเนินการจัดทำบทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผล
การเฝ้าระวังภัยคุกคามและความมั่นคงปลอดภัยไซเบอร์ประจำทุกเดือนตลอดระยะเวลาสัญญา โดยจัดส่งเอกสาร
รายงานที่เป็น soft file ทางระบบจดหมายอิเล็กทรอนิกส์ (Email) หรือ Shared File Cloud Service หรือ
ช่องทางอื่นใดตามที่กรมการกงสุลเห็นสมควรภายในวันที่ ๑๕ ของเดือนถัดไป

๔.๑.๙ ผู้รับจ้างต้องดำเนินการจัดทำรายงานประจำเดือน (Monthly Report) เป็นประจำ
ทุกเดือนตลอดระยะเวลาสัญญา โดยจัดส่งเอกสารรายงานที่เป็น soft file ทางระบบจดหมายอิเล็กทรอนิกส์
(Email) หรือ Shared File Cloud Service หรือช่องทางอื่นใดตามที่กรมการกงสุลเห็นสมควรภายในวันที่
๑๕ ของเดือนถัดไป โดยมีรายละเอียดของรายงานเป็นอย่างน้อย ดังนี้

๔.๑.๙.๑ ระบุประเภทของภัยคุกคาม

๔.๑.๙.๒ คำอธิบายอย่างละเอียด (Description)

๔.๑.๙.๓ วัน-เวลา ที่เกิดเหตุการณ์ของภัยคุกคาม

๔.๑.๙.๔ ระบุต้นทาง (Attacker) และปลายทาง (Target)

๔.๑.๙.๕ ภาพรวมการเชื่อมโยงเหตุการณ์ภัยคุกคามที่เกิดขึ้น

๔.๑.๙.๖ รายละเอียดเหตุการณ์และพฤติกรรมทั้งหมด โดยมีข้อมูลอย่างน้อย ได้แก่

- ๑) ผลกระทบ (Impact) (ถ้ามี)
- ๒) ระบบที่ได้รับผลกระทบ (System Affected) (ถ้ามี)
- ๓) แนวทางแก้ไข (Solution)
- ๔) อ้างอิง (Reference) (ถ้ามี)

๔.๑.๙.๗ สรุปข่าวสารหรือเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยด้านไซเบอร์ (Cyber Security News) โดยจัดส่งเอกสารรายงานที่เป็น soft file ทางระบบจดหมายอิเล็กทรอนิกส์ (Email) โดยมีรายละเอียดอย่างน้อย ดังนี้

- ๑) รายชื่อและคุณลักษณะภัยคุกคาม
- ๒) ช่องโหว่ใหม่ (Vulnerability) เช่น อุปกรณ์ในระบบเครือข่าย (Network Equipment) ระบบปฏิบัติการ (Operating System) ระบบฐานข้อมูลหลัก (Database) แอปพลิเคชัน (Applications) ซอฟต์แวร์ของบุคคลที่สาม (Third-Party Software) บริการคลาวด์ (Cloud Services) อุปกรณ์ Internet of Things (IoT) ระบบความมั่นคงปลอดภัย (Security Systems) ช่องโหว่จากผู้ใช้งานปลายทาง (Endpoint Vulnerabilities) หรือช่องโหว่ใหม่ของระบบและอุปกรณ์ต่าง ๆ ที่ผู้รับแจ้งเห็นว่า จะก่อให้เกิดผลเสียหายต่อการดำเนินงานของกรมการกงสุล โดยข่าวสารดังกล่าว ประกอบด้วยเนื้อหาที่สำคัญ อาทิ คำอธิบายโดยย่อ (Overview) คำอธิบายอย่างละเอียด (Description) ผลกระทบ (Impact) ระบบที่ได้รับผลกระทบ (System Affected) ทางแก้ไข (Solution) (ถ้ามี) อ้างอิง (Reference)

๔.๑.๙.๘ รายงานสถานะและประสิทธิภาพในภาพรวมบริการในโครงการในข้อ ๔.๑.๑ ๔.๑.๒ และ ๔.๒

๔.๑.๙.๙ รายงานการปฏิบัติงานตาม SLA ตามข้อ ๕

๔.๑.๑๐ ผู้รับแจ้งต้องสนับสนุนและตอบสนองต่อเหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคาม ระงับ ยับยั้ง หรือยุติกระบวนการที่เป็นอันตรายต่อระบบที่ติดตั้ง EDR ในโครงการ โดยต้องดำเนินการอย่างน้อย ดังนี้

- ๔.๑.๑๐.๑ ระบุขอบเขตของผลกระทบที่เกิดจากภัยคุกคามที่เกิดขึ้น
- ๔.๑.๑๐.๒ ทำการกักกันเครื่อง (Endpoint) ที่เป็นอันตรายออกจากระบบ เพื่อหลีกเลี่ยงการแพร่กระจายไปสู่เครื่องอื่น ๆ
- ๔.๑.๑๐.๓ ทำการระงับ ยับยั้ง หรือ ยุติกระบวนการที่เป็นอันตรายต่อระบบ
- ๔.๑.๑๐.๔ ทำการกำจัด ลบ หรือล้างไฟล์ที่เกี่ยวข้องกับภัยคุกคามดังกล่าว ในกรณีที่เครื่องได้รับผลกระทบจะต้องดำเนินการกู้คืนกลับสู่สภาพปกติ
- ๔.๑.๑๐.๕ ดำเนินการปรับปรุงการตั้งค่าของอุปกรณ์ที่เกี่ยวข้องในระบบ รวมถึงการกำหนด Blacklist หรือ Whitelist Asset ต่าง ๆ
- ๔.๑.๑๑ ผู้รับแจ้งต้องดำเนินงานภายใต้ SLA (Service Level Agreement) ที่กำหนด สำหรับ บริการเฝ้าระวังและแจ้งเตือนเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยอ้างอิงตามข้อ ๕

๔.๒ ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (Security Operation Center: SOC)

ผู้รับแจ้งต้องจัดให้มีศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (SOC) โดยมี คุณสมบัติอย่างน้อย ดังนี้

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

๔.๒.๑ ต้องมีห้องเฉพาะ (Dedicated Room) สำหรับเป็นศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (Cybersecurity Operations Center) ที่ผ่านการรับรองตามมาตรฐานสากล ISO๒๗๐๐๑

๔.๒.๒ ต้องมีระบบ Biometric Access Control สำหรับควบคุมการเข้า-ออก ของเจ้าหน้าที่ และมีการเก็บวันเวลาเข้า - ออก ไม่น้อยกว่า ๙๐ วัน

๔.๒.๓ ต้องมีระบบ CCTV สามารถบันทึกและดูภาพย้อนหลังได้ไม่น้อยกว่า ๙๐ วัน

๔.๓ ผู้เชี่ยวชาญด้าน Cyber Security จำนวน ๘ คน

ผู้รับจ้างต้องมีทีมผู้เชี่ยวชาญด้าน Cyber Security โดยมีคุณสมบัติอย่างน้อย ดังนี้

๔.๓.๑ ผู้จัดการโครงการ จำนวน ๑ คน มีคุณสมบัติอย่างน้อย ดังนี้

๔.๓.๑.๑ มีประสบการณ์ในตำแหน่งผู้จัดการโครงการที่เกี่ยวกับศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศ หรือตำแหน่งที่เกี่ยวข้อง ไม่น้อยกว่า ๕ ปี

๔.๓.๑.๒ คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีในสาขาเทคโนโลยีสารสนเทศ หรือวิศวกรรมคอมพิวเตอร์ หรือที่เกี่ยวข้อง

๔.๓.๑.๓ ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ Certified Information Systems Security Professional (CISSP) และ Certified Information Security Manager (CISM)

๔.๓.๒ ผู้บัญชาการหรือหัวหน้าหน่วยงานศูนย์เฝ้าระวังภัยคุกคาม (CSOC Lead) จำนวน ๑ คน มีคุณสมบัติอย่างน้อย ดังนี้

๔.๓.๒.๑ คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีในสาขาเทคโนโลยีสารสนเทศ หรือวิศวกรรมคอมพิวเตอร์ หรือที่เกี่ยวข้อง

๔.๓.๒.๒ มีประสบการณ์ทำงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศในตำแหน่ง Security Analyst หรือสูงกว่ามาแล้วไม่น้อยกว่า ๓ ปี

๔.๓.๒.๓ ได้รับประกาศนียบัตรรับรองคุณวุฒิมีประกาศนียบัตรด้านความปลอดภัยสารสนเทศ GIAC Certified Incident Handler Certification (GCIH) และ Assessing Information Security Risk using the OCTAVE Approach

๔.๓.๓ ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ ระดับ ๓ จำนวน ๑ คน มีคุณสมบัติอย่างน้อย ดังนี้

๔.๓.๓.๑ มีประสบการณ์ทำงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศในตำแหน่ง Security Analyst หรือ Digital forensic ปฏิบัติหน้าที่ทำการวิเคราะห์ Root cause analysis และ Digital forensic มาแล้วไม่น้อยกว่า ๓ ปี

๔.๓.๓.๒ คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีในสาขาเทคโนโลยีสารสนเทศ หรือวิศวกรรมคอมพิวเตอร์ หรือที่เกี่ยวข้อง

๔.๓.๓.๓ ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ GIAC Certified Forensic Analyst (GCFA)

๔.๓.๔ ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ ระดับ ๒ จำนวน ๑ คน มีคุณสมบัติอย่างน้อย ดังนี้

๔.๓.๔.๑ มีประสบการณ์ทำงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศในตำแหน่ง Security Analyst มาแล้วไม่น้อยกว่า ๓ ปี

๔.๓.๔.๒ คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีในสาขาเทคโนโลยีสารสนเทศหรือวิศวกรรมคอมพิวเตอร์ หรือที่เกี่ยวข้อง

๔.๓.๔.๓ ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ EC-Council Certified Security Analyst (ECSA) หรือ Certified CompTIA Cybersecurity Analyst

(CySA+) หรือ CompTIA Advanced Security Practitioner (CASP+) หรือ Certified Ethical Hacker (CEH) หรือเทียบเท่า

๔.๓.๕ ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ ระดับ ๑ จำนวน ๔ คน มีคุณสมบัติอย่างน้อย ดังนี้

๔.๓.๕.๑ คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีในสาขาเทคโนโลยีสารสนเทศหรือวิศวกรรมคอมพิวเตอร์ หรือที่เกี่ยวข้อง

๔.๓.๕.๒ มีประสบการณ์ทำงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศในตำแหน่ง Security Analyst มาแล้วไม่น้อยกว่า ๓ ปี

๔.๓.๕.๓ ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ Certified CompTIA Security + หรือเทียบเท่า

๔.๓.๕.๔ เจ้าหน้าที่ปฏิบัติงาน ณ ศูนย์เฝ้าระวังภัยคุกคาม (CSOC) ของผู้รับจ้างตลอด ๒๔ ชั่วโมง

ตารางสรุปรายละเอียดผู้เชี่ยวชาญด้าน Cyber Security

ลำดับ	หน้าที่รับผิดชอบ	จำนวนอย่างน้อย (คน)	ประสบการณ์ขั้นต่ำ (ปี)	ได้รับประกาศนียบัตรรับรองคุณวุฒิขั้นต่ำ
๑	ผู้จัดการโครงการ	๑	๕	Certified Information Systems Security Professional (CISSP) และ Certified Information Security Manager (CISM)
๒	ผู้บัญชาการหรือหัวหน้าหน่วยงานศูนย์เฝ้าระวังภัยคุกคาม (CSOC Lead)	๑	๓	GIAC Certified Incident Handler Certification (GCIH) และ Assessing Information Security Risk using the OCTAVE Approach
๓	ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ ระดับ ๓	๑	๓	GIAC Certified Forensic Analyst (GCFA)

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

๔	ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ ระดับ ๒	๑	๓	EC-Council Certified Security Analyst (ECSA) หรือ Certified CompTIA Cybersecurity Analyst (CySA+) หรือ CompTIA Advanced Security Practitioner (CASP+) หรือ Certified Ethical Hacker (CEH) หรือเทียบเท่า
๕	ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ ระดับ ๑	๔	๓	Certified CompTIA Security + หรือเทียบเท่า

ทั้งนี้ ใบประกาศนียบัตรหรือใบรับรองของบุคลากรที่ยื่นข้อเสนอทั้งหมดต้องมีอายุจนถึงวันที่ยื่นข้อเสนอ และต้องต่ออายุให้ครอบคลุมตลอดระยะเวลาตามสัญญา กรณีมีการเปลี่ยนแปลงบุคลากรในโครงการ ผู้รับจ้างต้องจัดหาบุคลากรที่มีใบประกาศนียบัตรหรือใบรับรองเทียบเท่าหรือดีกว่าบุคลากรเดิมมาทดแทน และต้องได้รับความเห็นชอบจากกรมการกงสุล กระทรวงการต่างประเทศ รวมถึงผู้รับจ้างจะต้องส่งรายชื่อทีมงานบุคลากรของผู้รับจ้างอย่างน้อย จำนวน ๘ คน โดยแนบประวัติบุคลากรที่มีความรู้ความชำนาญ พร้อมประสบการณ์การทำงาน เพื่อแสดงว่ามีความสามารถตรงกับงานที่รับจ้าง โดยแนบประวัติพร้อมประสบการณ์การทำงาน และใบประกาศนียบัตร (Certificate) ในขณะยื่นข้อเสนอ

๕. เงื่อนไขการให้บริการเผื่อสำรองและตอบสนองต่อเหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคามทางไซเบอร์และกรอบระดับการให้บริการ (Service Level Agreement)

๕.๑ ผู้รับจ้างต้องดำเนินการให้บริการ ดังนี้

ระดับความรุนแรง (Severity)	เวลาในการวิเคราะห์และแจ้งเตือน (Detection & Investigation)	เวลาในการตอบสนองยับยั้งภัยคุกคาม (Response/Contain)
สูงมาก (Very High)	๓๐ นาที	๔ ชั่วโมง
สูง (High)	๑ ชั่วโมง	๖ ชั่วโมง
ปานกลาง (Medium)	๒ ชั่วโมง	๑๒ ชั่วโมง
ต่ำ (Low)	๔ ชั่วโมง	๔๐ ชั่วโมง

๕.๒ เวลาในการวิเคราะห์และแจ้งเตือน (Detection & Investigation) นับเวลาตั้งแต่ได้รับการแจ้งเตือนจากระบบเผื่อสำรองภัยคุกคามทางไซเบอร์ของผู้รับจ้างแจ้งเตือนหรือได้รับการแจ้งเตือนจากกรมการกงสุล จนกระทั่งได้ทำการวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์พร้อมให้ข้อมูลประกอบเพิ่มเติมกับผู้ว่าจ้าง

๕.๓ เวลาในการตอบสนองยับยั้งภัยคุกคาม (Response/Contain) นับเวลาตั้งแต่ได้รับผลวิเคราะห์และแจ้งเตือน (Detection & Investigation) เสร็จสิ้น จนกระทั่งได้ดำเนินการแก้ไขหรือยับยั้งภัยคุกคามทางไซเบอร์ เฉพาะเหตุการณ์ที่สามารถยับยั้งภัยคุกคามทางไซเบอร์ด้วย Endpoint Detection and Response ที่นำเสนอและเป็นเครื่องมือที่อยู่ภายใต้การให้บริการ EDR ตามขอบเขตการให้บริการ

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

๖. การให้บริการ

๖.๑ ผู้รับจ้างจะต้องจัดเตรียมระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ SIEM ของผู้รับจ้าง ให้รองรับการตรวจสอบข้อมูลของกรมการกงสุล ที่จะใช้ในการตรวจสอบด้านความปลอดภัยทางไซเบอร์ ในวันที่เริ่มการให้บริการ

๖.๒ ผู้รับจ้างจะต้องติดตั้งซอฟต์แวร์รักษาความปลอดภัยที่ช่วยตรวจจับและป้องกันภัยคุกคามที่มุ่งโจมตีอุปกรณ์ปลายทางในเครือข่าย (Endpoint Detection and Response : EDR) ให้กับเครื่องคอมพิวเตอร์

แม่ข่ายและเครื่องของเจ้าหน้าที่ของกรมการกงสุล พร้อมทั้งค่าการตรวจจับและแจ้งเตือนไปยังระบบ SIEM ให้สามารถทำงานได้อย่างมีประสิทธิภาพ ตามที่กรมการกงสุลกำหนด ในวันที่เริ่มการให้บริการ

๖.๓ ผู้รับจ้างจะต้องตรวจสอบการส่งข้อมูลการจราจรทางคอมพิวเตอร์จากระบบของผู้ว่าจ้างไปยังระบบ SIEM ของผู้รับจ้างให้ถูกต้องครบถ้วนตามจำนวนที่ได้ติดตั้งไว้

๖.๔ ผู้รับจ้างจะต้องปรับปรุงอัปเดตซอฟต์แวร์ EDR ให้ทันสมัยอยู่เสมออย่างเหมาะสมตลอดระยะเวลาการให้บริการดูแลบริหารจัดการระบบ

๖.๕ ในกรณีที่เกิดเหตุหรือประสบปัญหาด้าน Cyber Security กับระบบที่ให้บริการเฝ้าระวังอยู่ ผู้รับจ้างจะต้องให้คำปรึกษา แนะนำโดยการดำเนินการวิเคราะห์ ตรวจสอบ incidents หรือปัญหาภัยคุกคาม Cyber ที่เกิดขึ้น และแก้ไขปัญหาหรือร่วมแก้ไขปัญหาดังกล่าวกับเจ้าหน้าที่ของกรมการกงสุล จนกว่าจะแก้ไขปัญหาเสร็จสิ้น

๖.๖ ในระหว่างอายุสัญญา หากกระทรวงฯ เห็นว่าผู้รับจ้างไม่อาจปฏิบัติตามสัญญาได้ และ/หรือ ผู้รับจ้างผิดสัญญาข้อใดข้อหนึ่ง ที่ส่งผลกระทบสร้างความเสียหายต่อกระทรวงฯ ดังนั้น กระทรวงฯ มีสิทธิให้บุคคลอื่นมาดำเนินการแทน โดยค่าใช้จ่ายจากการดำเนินการดังกล่าว ผู้รับจ้างต้องเป็นผู้รับผิดชอบทั้งหมด หรือกระทรวงฯ มีสิทธิบอกเลิกสัญญาได้ ในกรณีเช่นนี้ ผู้รับจ้างยินยอมให้กระทรวงฯ ดำเนินการโดยไม่มี การร้องเรียน เรียกร้อง ฟ้องร้องใด ๆ ทั้งสิ้น

๖.๗ การตั้งค่าระบบ (Configuration) ข้อมูลภายในระบบ และรายละเอียดต่าง ๆ ภายใต้ระบบที่ผู้รับจ้างให้บริการ ถือเป็นความลับ หากสูญหายหรือถูกเผยแพร่จากผู้รับจ้าง เป็นเหตุให้เกิดความเสียหาย ซึ่งเกิดการดำเนินการของผู้รับจ้างทั้งที่ตั้งใจหรือไม่ก็ตามผู้รับจ้างต้องรับผิดชอบต่อความเสียหายและความบกพร่องนั้น ๆ

๖.๘ กรณีที่มีการปรับเปลี่ยนซอฟต์แวร์ หรือระบบที่ให้บริการ จะต้องมีความสมบัติน้อยกว่าของเดิมที่มีอยู่หรือดีกว่า

๖.๙ ผู้รับจ้างจะต้องจัดซ้อมการรับมือภัยคุกคามทางไซเบอร์ (Cyber Drill) ให้กับเจ้าหน้าที่ของกรมการกงสุล อย่างน้อย ๑ ครั้ง โดยมีขอบเขตงานสำหรับการซ้อมแผนการจัดการเหตุคุกคามทางไซเบอร์ประกอบไปด้วย ๕ ขั้นตอน ดังนี้

- ๑) การวางแผนงานโครงการ (Planning)
- ๒) การสอบทานเอกสารและเตรียมการซ้อม (Review Document & Prepare Exercise)
- ๓) การเตรียมความพร้อมการซ้อม (Pre-exercise Briefing Session)
- ๔) การซ้อมแผนการจัดการเหตุคุกคามทางด้านไซเบอร์ (Exercise)
- ๕) การจัดทำรายงานและนำเสนอผลการซ้อม (Report and Presentation)

๗. ระยะเวลาการดำเนินงาน

ภายใน ๑๒ เดือน นับถัดจากวันลงนามในสัญญา

๘. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

๘.๑ ในการพิจารณาผลการยื่นข้อเสนอราคาครั้งนี้ จะพิจารณาโดยใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่นในการพิจารณา (Price Performance)

๘.๒ การพิจารณาผู้ชนะการยื่นข้อเสนอ จะใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่น โดยพิจารณา ให้คะแนนตามปัจจัย และน้ำหนักตามที่กำหนด ดังนี้

๘.๒.๑ ราคาที่เสนอ กำหนดน้ำหนักเท่ากับ ร้อยละ ๓๐

๘.๒.๒ ข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ๆ กำหนดน้ำหนักเท่ากับร้อยละ ๗๐ โดยคุณภาพของข้อเสนอจะต้องสอดคล้อง กับการดำเนินโครงการอย่างมีประสิทธิภาพและละเอียดรอบคอบ มีคุณภาพเป็นประโยชน์สูงสุดแก่ทางราชการ โดยขอสงวนสิทธิ์ในการงดให้คะแนนรายที่ยื่นข้อเสนอที่ไม่มีความเหมาะสมหรือไม่อยู่ในเกณฑ์คุณภาพที่ไม่ได้มาตรฐาน ทั้งนี้ มีเกณฑ์การให้คะแนน ดังนี้

ตารางเกณฑ์การให้คะแนนข้อเสนอด้านเทคนิค คะแนนเต็ม ๑๐๐ คะแนน คิดเป็นร้อยละ ๗๐ ตามที่ระบุในข้อ ๘.๒.๒

ลำดับ	ข้อพิจารณา	คะแนน
๑.	ความน่าเชื่อถือ ผลงาน และประสบการณ์	๗๐
	๑.๑ ผู้ยื่นข้อเสนอต้องเคยมีผลงานประเภทเดียวกัน (งานให้บริการศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์) กับงานที่จ้างในวงเงินไม่น้อยกว่า ๓,๐๐๐,๐๐๐ บาท ในสัญญาเดียวและเป็นผลงานที่เสร็จสิ้นแล้วไม่เกิน ๒ ปี นับถึงวันยื่นเอกสารเสนอราคาพร้อมเอกสารขอบเขตของงานที่ได้ปฏิบัติพร้อมรับรองสำเนาถูกต้อง โดยผลงานดังกล่าวจะต้องเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับส่วนราชการ หน่วยงานตามกฎหมายว่าด้วยระเบียบบริหารราชการส่วนท้องถิ่น หน่วยงานอื่นซึ่งมีกฎหมายบัญญัติให้มีฐานะเป็นราชการบริหารส่วนท้องถิ่น รัฐวิสาหกิจ หรือหน่วยงานเอกชนที่เชื่อถือได้ โดยมีรายละเอียดการให้คะแนน ดังนี้ มี ๑ ผลงาน ได้ ๕ คะแนน มี ๒ ผลงาน ได้ ๑๐ คะแนน มี ๓ ผลงาน ได้ ๑๕ คะแนน มี ๔ ผลงานขึ้นไป ได้ ๒๐ คะแนน	๒๐
	๑.๒ ผู้ยื่นข้อเสนอหรือบุคลากรในโครงการมีผลงานได้รับรางวัลจากการแข่งขัน Cyber Security ในรูปแบบ Blue Team และหรือ Red Team ระดับประเทศย้อนหลังไม่เกิน ๒ ปี นับถึงวันยื่นเอกสารเสนอราคา โดยมีรายละเอียดการให้คะแนน ดังนี้ รางวัลรองชนะเลิศอันดับที่ ๒ ได้ ๓ คะแนน รางวัลรองชนะเลิศอันดับที่ ๑ ได้ ๖ คะแนน	๑๐

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

	รางวัลชนะเลิศ ได้ ๑๐ คะแนน	
	๑.๓ ผู้ยื่นข้อเสนอหรือบุคลากรในโครงการเคยได้รับรางวัลด้าน Cyber Security Award ระดับเอเชียหรือสูงกว่า ย้อนหลังไม่เกิน ๒ ปี นับถึงวันยื่นเอกสารเสนอราคา	๑๐
	๑.๔ ผู้ยื่นข้อเสนอหรือบุคลากรในโครงการเคยมีผลงานหรือได้รับรางวัล Top bounty rewards จากการนำเสนอผลงาน Threat Bounty Program ย้อนหลังไม่เกิน ๓ ปี นับถึงวันยื่นเอกสารเสนอราคา	๑๐
	๑.๕ ผู้ยื่นข้อเสนอหรือบุคลากรในโครงการเคยมีผลงานในการตรวจพบช่องโหว่ใหม่ที่มีประกาศ CVE ในเว็บไซต์เผยแพร่ CVE อย่างเป็นทางการ https://cve.mitre.org/ ย้อนหลังไม่เกิน ๓ ปี นับถึงวันยื่นเอกสารเสนอราคา	๑๐
	๑.๖ ผู้ยื่นข้อเสนอหรือบุคลากรในโครงการเคยมีผลงานวิเคราะห์เทคนิคการโจมตีที่มีประกาศ MITRE ในเว็บไซต์เผยแพร่ MITRE อย่างเป็นทางการ https://attack.mitre.org/techniques/ ย้อนหลังไม่เกิน ๓ ปี นับถึงวันยื่นเอกสารเสนอราคา	๑๐
๒	ใบประกาศนียบัตรหรือการรับรองคุณสมบัติผู้รับจ้างและบุคลากร	๓๐
	๒.๑ ผู้ยื่นข้อเสนอได้รับการรับรองตามมาตรฐานการบริหารความต่อเนื่องทางธุรกิจ ISO ๒๒๓๐๑ Business Continuity Management Systems สำหรับ SOC Service	๑๐
	๒.๒ ผู้ยื่นข้อเสนอได้รับการรับรองตามมาตรฐานระบบการจัดการงานบริการด้านเทคโนโลยีสารสนเทศ ISO ๒๐๐๐๐-๑ Service Management System สำหรับ SOC Service	๑๐
	๒.๓ บุคลากรในโครงการมีใบประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ Advanced Topics in Incident Handling	๕
	๒.๔ บุคลากรในโครงการมีใบประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ ISA/IEC ๖๒๔๔๓ Cybersecurity Fundamentals Specialist	๕

๘.๓ กรรมการจะพิจารณาไม่ให้คะแนนผู้รับจ้างในการประกวดราคา หากผู้รับจ้างไม่ยื่นหรือยื่นเอกสารคุณสมบัติไม่ตรงตามข้อ ๘.๒.๒

๘.๔ ผู้ที่ได้คะแนนรวมสูงสุดถือเป็นผู้ชนะการคัดเลือก

๘.๕ กระทรวงการต่างประเทศทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใด หรือราคาที่ยื่นขอทั้งหมดก็ได้ และอาจพิจารณาเลือกจ้างในจำนวนหรือขนาดหรือเฉพาะรายการหนึ่งรายการใด หรืออาจจะยกเลิกการประกวดราคาจ้าง โดยไม่พิจารณาจัดจ้างเลยก็ได้ แต่พิจารณา ทั้งนี้ เพื่อประโยชน์ ของทางราชการเป็นสำคัญ และให้ถือการตัดสินใจของกระทรวงการต่างประเทศเป็นเด็ดขาด ผู้ยื่นข้อเสนอจะเรียกร้องค่าเสียหายใด ๆ มิได้

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

๙. วงเงินงบประมาณ

จำนวนทั้งสิ้น ๖,๕๐๐,๐๐๐.- บาท (หกล้านห้าแสนบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงไว้แล้วด้วย โดยเบิกจ่ายจากเงินค่าใช้จ่ายในการดำเนินงานการกงสุล ประจำปีงบประมาณ ๒๕๖๘

๑๐. งานและการจ่ายเงิน

โดยแบ่งงวดงานและงวดเงินเป็น ๔ งวด ดังนี้

๑๐.๑ งวดที่ ๑ จ่ายเป็นเงินร้อยละ ๒๕ ของราคาค่าจ้าง เมื่อผู้รับจ้างส่งมอบแผนการปฏิบัติงาน และรายงานการปฏิบัติงาน ตามข้อ ๔ และข้อ ๕ นับถัดจากวันลงนามในสัญญา ๓ เดือน และคณะกรรมการตรวจรับพัสดุ ได้ตรวจรับงานเรียบร้อยแล้ว

๑๐.๒ งวดที่ ๒ เบิกจ่ายร้อยละ ๒๕ ของราคาค่าจ้าง เมื่อผู้รับจ้างส่งมอบรายงานการปฏิบัติงาน ตามข้อ ๔ และข้อ ๕ นับถัดจากวันลงนามในสัญญา ๖ เดือน และคณะกรรมการตรวจรับพัสดุ ได้ตรวจรับงานเรียบร้อยแล้ว

๑๐.๓ งวดที่ ๓ เบิกจ่ายร้อยละ ๒๕ ของราคาค่าจ้าง เมื่อผู้รับจ้างส่งมอบรายงานการปฏิบัติงาน ตามข้อ ๔ และข้อ ๕ นับถัดจากวันลงนามในสัญญา ๙ เดือน และคณะกรรมการตรวจรับพัสดุ ได้ตรวจรับงานเรียบร้อยแล้ว

๑๐.๔ งวดที่ ๔ เบิกจ่ายร้อยละ ๒๕ ของราคาค่าจ้าง เมื่อผู้รับจ้างส่งมอบรายงานการปฏิบัติงาน ตามข้อ ๔ และข้อ ๕ นับถัดจากวันลงนามในสัญญา ๑๒ เดือน และคณะกรรมการตรวจรับพัสดุ ได้ตรวจรับงานเรียบร้อยแล้ว

๑๑. การรับประกัน

ในกรณีที่ผู้รับจ้างไม่สามารถปฏิบัติตามข้อกำหนดในข้อที่ ๕ และข้อ ๖ จะต้องชำระค่าปรับเป็นราย ชั่วโมง ตามเกณฑ์การคำนวณดังนี้

เกณฑ์การคำนวณค่าปรับ

ค่าปรับรายชั่วโมง = (จำนวนชั่วโมงที่เกินเวลาที่กำหนด โดยเศษของชั่วโมงให้คิดเป็น

๑ ชั่วโมง) × (ร้อยละ ๐.๐๓๕ × วงเงินในสัญญารายงวด) × ค่าตัวถ่วง (ตามตารางกำหนดตัวถ่วงด้านล่าง)

ตารางกำหนดตัวถ่วงและกรอบระยะเวลาในการวิเคราะห์และแจ้งเตือนพร้อมตอบสนองยับยั้งภัยคุกคาม

ลำดับ	รายการ	ค่าตัวถ่วง	ระยะเวลาในการแก้ไข	ขอบเขตงานอ้างอิงจาก TOR
๑	การวิเคราะห์และแจ้งเตือน ระดับความรุนแรง - สูงมาก (Very High)	๑.๐	๓๐ นาที	ข้อ ๕
๒	การวิเคราะห์และแจ้งเตือน ระดับความรุนแรง - สูง (High)	๑.๐	๑ ชั่วโมง	ข้อ ๕

ลงชื่อ..........ประธานกรรมการ ลงชื่อ..........กรรมการ ลงชื่อ..........กรรมการ

๓	การวิเคราะห์และแจ้งเตือน ระดับความรุนแรง - ปานกลาง (Medium)	๑.๐	๒ ชั่วโมง	ข้อ ๕
๔	การวิเคราะห์และแจ้งเตือน ระดับความรุนแรง - ต่ำ (Low)	๐.๕	๔ ชั่วโมง	ข้อ ๕
๕	การตอบสนองยับยั้งภัยคุกคาม ระดับความรุนแรง - สูงมาก (Very High)	๑.๐	๔ ชั่วโมง	ข้อ ๕
๖	การตอบสนองยับยั้งภัยคุกคาม ระดับความรุนแรง - สูง (High)	๑.๐	๖ ชั่วโมง	ข้อ ๕
๗	การตอบสนองยับยั้งภัยคุกคาม ระดับความรุนแรง - ปานกลาง (Medium)	๑.๐	๑๒ ชั่วโมง	ข้อ ๕
๘	การตอบสนองยับยั้งภัยคุกคาม ระดับความรุนแรง - ต่ำ (Low)	๐.๕	๔๐ ชั่วโมง	ข้อ ๕
๙	ความพร้อมของการให้บริการศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์	๑.๐	๑ ชั่วโมง	ข้อ ๖

๑๒. อัตราค่าปรับ

๑๒.๑ กรณีผู้รับจ้างปฏิบัติงานผิดจากสัญญา จะต้องชำระค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๑๐ ของราคางานจ้างในงวดงานนั้น ๆ (แต่ต้องไม่ต่ำกว่าวันละ ๑๐๐.- บาท)

๑๒.๒ ห้ามมิให้เอางานทั้งหมดหรือแค่บางส่วนแห่งสัญญานี้ไปจ้างช่วงอีกทอดหนึ่ง เว้นแต่การจ้างช่วง แต่บางส่วนจะได้รับความยินยอมเป็นหนังสือจากผู้ว่าจ้างก่อน หากฝ่าฝืนผู้รับจ้างต้องชำระค่าปรับในอัตราร้อยละ ๑๐ ของวงเงินของงานที่จ้างช่วงตามสัญญา

๑๓. กำหนดยื่นราคาข้อเสนอ

ผู้เสนอราคาจะต้องกำหนดยื่นราคาที่เสนอไม่น้อยกว่า ๙๐ วัน นับถัดจากวันที่ยื่นข้อเสนอราคา

๑๔. การลงนามในสัญญา

ภายใน ๑๕ วัน นับถัดจากวันที่ได้รับหนังสือแจ้งให้มาทำสัญญา

๑๕. แผนการทำงาน

ภายใน ๗ วัน นับถัดจากวันลงนามในสัญญา

๑๖. ข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.

๒๕๖๒

๑๖.๑ ผู้รับจ้างต้องดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ว่าจ้างเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

ลงชื่อ.....ประธานกรรมการ ลงชื่อ.....กรรมการ ลงชื่อ.....กรรมการ

๑๖.๒ จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ว่าจ้าง ทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

๑๖.๓ ผู้รับจ้างต้องจัดทำ และเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activity: RoPA) ไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด โดยมีรายละเอียดที่บันทึกใน RoPA อย่างน้อยตามมาตรา ๓๙ แห่งพระราชบัญญัติ ดังกล่าว เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบได้ ซึ่งจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

๑๖.๔ ผู้รับจ้างต้องลงนามในแบบสัญญาการรักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement) และสัญญาประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ร่วมกับผู้ว่าจ้าง ตามข้อ ๑๗ เพื่อควบคุมการดำเนินงานตามที่ของผู้รับจ้างให้เป็นไปตามพระราชบัญญัตินี้ โดยจัดทำ ข้อตกลงดังกล่าวในวันลงนามในสัญญา

๑๗. เอกสารแนบท้าย

๑๗.๑ ตัวอย่างแบบสัญญาการรักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement)

๑๗.๒ ตัวอย่างแบบสัญญาประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

๑๘. สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติม และส่งข้อเสนอแนะ วิจัยารณ์ หรือแสดงความคิดเห็น

ศูนย์บริหารข้อมูลการกงสุลและสารสนเทศ กรมการกงสุล กระทรวงการต่างประเทศ

เลขที่ ๑๒๓ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

หมายเลขโทรศัพท์ : ๐ ๒๒๐๓ ๕๐๐๐ ต่อ ๓๓๕๐๕

Email Address : kosin.s@mfa.go.th , teerawut.m@mfa.go.th

หมายเหตุ สาธารณชนที่ต้องการเสนอแนะ วิจัยารณ์ หรือมีความเห็น ต้องเปิดเผยชื่อ ที่อยู่ และ หมายเลขโทรศัพท์ ของผู้ให้ข้อเสนอแนะ วิจัยารณ์ หรือมีความเห็นด้วย

ลงชื่อ..........ประธานกรรมการ ลงชื่อ..........กรรมการ ลงชื่อ..........กรรมการ



- ร่าง -

สัญญาการรักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement)

และการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

สัญญาฉบับนี้ ทำขึ้น ณ กระทรวงการต่างประเทศ แขวงทุ่งพญาไท เขตราชเทวี จังหวัด
กรุงเทพมหานคร 10400 เมื่อวันที่ ระหว่าง กระทรวงการต่างประเทศ โดย
..... ซึ่งต่อไปเรียกว่า "ผู้ให้ข้อมูล"
ฝ่ายหนึ่ง กับ โดย
..... ซึ่งมีนิติสัมพันธ์กับ กระทรวงการต่างประเทศ
ตาม

ซึ่งต่อไปเรียกว่า "ผู้รับข้อมูล" อีกฝ่ายหนึ่ง

ทั้งคู่สัญญาได้ตกลงกัน โดยมีข้อความดังต่อไปนี้

ข้อ 1. คำนิยาม

"ข้อมูลที่เป็นความลับ" หมายความว่า บรรดาข้อความ เอกสาร ข้อมูล ตลอดจน
รายละเอียดทั้งปวงที่เป็นของผู้ให้ข้อมูล รวมถึงที่อยู่ในความครอบครองหรือควบคุมดูแลของผู้ให้ข้อมูล
และไม่เป็นที่รับรู้ของสาธารณชนโดยทั่วไป ไม่ว่าจะในรูปแบบที่จับต้องได้หรือไม่ หรือสื่อแบบใด ไม่ว่าจะถูก
ดัดแปลงแก้ไขโดยผู้รับข้อมูลหรือไม่ และไม่ว่าจะเปิดเผยเมื่อใดและอย่างไร ให้ถือว่าเป็นความลับ

ข้อ 2. การรักษาข้อมูลที่เป็นความลับ

2.1 ผู้รับข้อมูลต้องรับผิดชอบรักษาข้อมูลที่เป็นความลับ และเก็บข้อมูลความลับไว้โดย
ครบถ้วน และอย่างเคร่งครัดเป็นเวลา 10 ปี โดยที่ผู้รับข้อมูลจะต้องไม่เปิดเผย ทำสำเนา หรือทำการอื่นใด
ทำนองเดียวกันแก่บุคคลอื่นไม่ว่าทั้งหมดหรือบางส่วน เว้นแต่ได้รับอนุญาตเป็นหนังสือจากผู้ให้ข้อมูล

/2.2 ผู้รับข้อ...

889ค

.....

.....

2.2 ผู้รับข้อมูลต้องใช้ข้อมูลที่เป็นความลับเพื่อการอันเกี่ยวกับหรือสัมพันธ์กับการดำเนินการที่มีอยู่ระหว่างผู้ให้ข้อมูลกับผู้รับข้อมูล โดยผู้รับข้อมูลต้องแจ้งให้ผู้ให้ข้อมูลทราบโดยทันทีที่พบการใช้หรือการเปิดเผยข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต หรือการละเมิดหรือฝ่าฝืนข้อกำหนดตามสัญญานี้ อีกทั้งผู้รับข้อมูลจะต้องให้ความร่วมมือกับผู้ให้ข้อมูลอย่างเต็มที่ในการเรียกคืนซึ่งการครอบครองข้อมูลที่เป็นความลับ การป้องกันการใช้อข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต และการระงับยับยั้งการเผยแพร่ข้อมูลที่เป็นความลับออกสู่สาธารณะ

2.3 ผู้รับข้อมูลต้องใช้มาตรการที่เหมาะสมในการเก็บรักษาข้อมูลที่เป็นความลับ เพื่อป้องกันมิให้ข้อมูลที่เป็นความลับถูกนำไปใช้โดยมิได้รับอนุญาตหรือถูกเปิดเผยแก่บุคคลอื่น โดยผู้รับข้อมูลต้องใช้มาตรการการเก็บรักษาข้อมูลที่เป็นความลับในระดับเดียวกันกับที่ผู้รับข้อมูลใช้กับข้อมูลที่เป็นความลับของตนเองซึ่งต้องไม่น้อยกว่าการดูแลที่สมควร

2.4 ผู้รับข้อมูลต้องแจ้งให้บุคลากร พนักงาน ลูกจ้าง ที่ปรึกษาของผู้รับข้อมูล และ/หรือ บุคคลภายนอกที่ต้องเกี่ยวข้องกับข้อมูลที่เป็นความลับนั้นทราบถึงความเป็นความลับและข้อจำกัดสิทธิในการใช้และการเปิดเผยข้อมูลที่เป็นความลับ และผู้รับข้อมูลต้องดำเนินการให้บุคคลดังกล่าวต้องผูกพันด้วยสัญญาหรือข้อตกลงเป็นหนังสือในการรักษาข้อมูลที่เป็นความลับโดยมีข้อกำหนดเช่นเดียวกับหรือไม่น้อยกว่าข้อกำหนดและเงื่อนไขในสัญญานี้ด้วย

2.5 ข้อมูลที่เป็นความลับตามข้อตกลงฉบับนี้ ไม่รวมไปถึงข้อมูลดังต่อไปนี้

- (1) ข้อมูลที่ ผู้ให้ข้อมูล เปิดเผยแก่สาธารณะ
- (2) ข้อมูลที่ผู้รับข้อมูลทราบอยู่ก่อนที่ ผู้ให้ข้อมูล จะเปิดเผยข้อมูลนั้น
- (3) ข้อมูลที่มาจากการพัฒนาโดยอิสระของผู้รับข้อมูลเอง
- (4) ข้อมูลที่ต้องเปิดเผยโดยกฎหมายหรือตามคำสั่งศาล ทั้งนี้ผู้รับข้อมูลต้องมีหนังสือแจ้งให้ ผู้ให้ข้อมูล ได้รับทราบถึงข้อกำหนดหรือคำสั่งดังกล่าวพร้อมทั้งหมายศาลและ/หรือ หมายค้นอย่างเป็นทางการยื่นต่อผู้ให้ข้อมูล ก่อนที่จะดำเนินการเปิดเผยข้อมูลดังกล่าว และในการเปิดเผยข้อมูลดังกล่าวผู้รับข้อมูลจะต้องดำเนินการตามขั้นตอนทางกฎหมายเพื่อขอให้คุ้มครองข้อมูลดังกล่าวไม่ให้ถูกเปิดเผยต่อสาธารณะด้วย

- (5) เป็นการเปิดเผยข้อมูลโดยได้รับความเห็นชอบจากผู้ให้ข้อมูล เป็นลายลักษณ์อักษร ก่อนที่ผู้รับข้อมูลจะเปิดเผยข้อมูลนั้น

ชวต



ข้อ 3. ทรัพย์สินทางปัญญา

สัญญาฉบับนี้ไม่มีผลบังคับใช้เป็นการโอนสิทธิหรือการอนุญาตให้ใช้สิทธิ (ไม่ว่าโดยตรง หรือโดยอ้อม) ให้แก่ผู้รับข้อมูลที่ได้รับความลับซึ่ง สิทธิบัตร ลิขสิทธิ์ การออกแบบ เครื่องหมายการค้า ตราสัญลักษณ์รูปประดิษฐ์อื่นใด ชื่อทางการค้า ความลับทางการค้า ไม่ว่าจดทะเบียนไว้ตามกฎหมายหรือไม่ก็ตาม หรือสิทธิอื่น ๆ ของผู้ให้ข้อมูล ซึ่งอาจมีอยู่ใน ปรากฏอยู่ หรือนำมาทำซ้ำไว้ในเอกสารข้อมูลที่เป็นความลับ ทั้งนี้ ผู้รับข้อมูลหรือบุคคลอื่นใดที่เกี่ยวข้องกับผู้รับข้อมูล และเกี่ยวข้องกับข้อมูลที่เป็นความลับดังกล่าว จะไม่ยื่นขอรับสิทธิและหรือขอจดทะเบียนเกี่ยวกับทรัพย์สินทางปัญญาใด ๆ ตลอดจนไม่นำไปใช้โดยไม่ได้รับการอนุญาตเป็นหนังสือจากผู้ให้ข้อมูล เกี่ยวกับรายละเอียดข้อมูลที่เป็นความลับหรือส่วนหนึ่งส่วนใดของรายละเอียดดังกล่าว

ข้อ 4. หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

ผู้รับข้อมูลต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งใช้บังคับอยู่ในปัจจุบัน รวมถึงที่จะได้แก้ไขในอนาคต รวมทั้งต้องปฏิบัติตามแนวปฏิบัติ หลักเกณฑ์ ประกาศ ระเบียบ กฎหมาย ที่จะมีการประกาศใช้ในอนาคตด้วย

ข้อ 5. การส่งคืน ลบ หรือการทำลายข้อมูลที่เป็นความลับ

เมื่อการดำเนินการที่มีอยู่ระหว่างผู้ให้ข้อมูลกับผู้รับข้อมูลเสร็จสิ้นลง ผู้รับข้อมูลจะต้องส่งมอบข้อมูลที่เป็นความลับและสำเนาของข้อมูลที่เป็นความลับที่ผู้รับข้อมูลได้รับไว้คืนให้แก่ผู้ให้ข้อมูล ตลอดจนลบหรือทำลายข้อมูลที่เป็นความลับที่ถูกจัดเก็บไว้ในคอมพิวเตอร์ หรืออุปกรณ์อื่นใดที่ใช้จัดเก็บข้อมูล (ถ้ามี) หรือดำเนินการอื่นตามที่ได้รับการแจ้งเป็นหนังสือจากผู้ให้ข้อมูล ตลอดจนยุติการใช้ข้อมูลที่เป็นความลับที่ได้จากผู้ให้ข้อมูลทันที และผู้รับข้อมูลจะต้องรักษาความลับของข้อมูลที่ได้รับจากผู้ให้ข้อมูลตลอดไป แม้ว่าการดำเนินการเสร็จสิ้นลงแล้วก็ตาม

ข้อ 6. การชดเชยค่าเสียหาย

ในกรณีที่ผู้รับข้อมูล และ/หรือบุคคลที่ได้รับข้อมูลที่เป็นความลับตามสัญญานี้ซึ่งอยู่ในความรับผิดชอบดูแลของผู้รับข้อมูล ผ่าฝืนข้อกำหนดตามข้อตกลงนี้ และก่อให้เกิดความเสียหายแก่ผู้ให้ข้อมูลผู้รับข้อมูลจะต้องชดเชยค่าเสียหายที่เกิดขึ้นทั้งหมดให้แก่ผู้ให้ข้อมูลภายใน 30 (สามสิบ) วัน นับแต่ได้รับหนังสือแจ้งค่าเสียหาย

/ข้อ 7. การ...

8/10/2564




ข้อ 7. การบังคับใช้

7.1 ในกรณีที่ปรากฏในภายหลังว่าส่วนใดส่วนหนึ่งในสัญญาฉบับนี้เป็นโมฆะ ให้ถือว่าข้อกำหนดส่วนที่เป็นโมฆะไม่มีผลบังคับในสัญญานี้ และข้อกำหนดที่เหลืออยู่ในสัญญาฉบับนี้ ยังคงใช้บังคับและมีผลอยู่อย่างสมบูรณ์

7.2 สัญญาฉบับนี้อยู่ภายใต้การบังคับใช้และตีความตามกฎหมายไทย

7.3 สัญญานี้ทำขึ้นสองฉบับมีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความโดยละเอียดตลอดแล้ว จึงได้ลงลายมือชื่อพร้อมทั้งประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยาน และคู่สัญญาต่างยึดถือไว้ฝ่ายละหนึ่งฉบับ

ลงชื่อ ผู้ให้ข้อมูล
(.....)

ลงชื่อ ผู้รับข้อมูล
(.....)

ลงชื่อ พยาน
(.....)

ลงชื่อ พยาน
(.....)

ชื่อ
.....
.....

- ร่าง -

สัญญาประมวลผลข้อมูลส่วนบุคคล
(Data Processing Agreement)

แนบท้ายสัญญา.....

สัญญานี้ทำที่ กรมการกงสุล กระทรวงการต่างประเทศ เมื่อวันที่.....
ระหว่างกรมการกงสุล กระทรวงการต่างประเทศ โดย..... อธิบดีกรมการกงสุล
สำนักงานตั้งอยู่เลขที่ 123 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210 ซึ่งต่อไปนี้
เรียกว่า “กรมการกงสุล” หรือ “ผู้ควบคุมข้อมูลส่วนบุคคล” ฝ่ายหนึ่งกับ บริษัท.....
โดย..... กรมการผู้มิอำนาจ สำนักงานตั้งอยู่ที่
อีเมลติดต่อทางธุรกิจ หมายเลขโทรศัพท์ติดต่อ.....

ซึ่งต่อไปในสัญญานี้ เรียกว่า “ผู้รับจ้าง” หรือ “ผู้ประมวลผลข้อมูลส่วนบุคคล” อีกฝ่ายหนึ่ง
โดยที่กรมการกงสุลและผู้รับจ้างได้ทำสัญญาจ้างเลขที่..... ลงวันที่
ซึ่งต่อไปในสัญญานี้ เรียกว่า “สัญญาจ้าง” เพื่อจ้างโครงการจ้างบริการศูนย์เฝ้าระวังความปลอดภัย
ไซเบอร์ระบบ e-Service ของกรมการกงสุล จำนวน 12 เดือน ซึ่งในการดำเนินงานตามสัญญาดังกล่าว
กรมการกงสุลจำเป็นต้องเปิดเผยข้อมูลจราจรคอมพิวเตอร์ (Log file) ซึ่งอาจมีข้อมูลส่วนบุคคลรวมอยู่ด้วย
ให้แก่ผู้รับจ้าง และผู้รับจ้างสามารถเข้าถึง จัดเก็บ และใช้งาน (“ประมวลผล”) ข้อมูลส่วนบุคคลดังกล่าว
ตามคำสั่งหรือในนามของกรมการกงสุลเพื่อให้บริการตามสัญญาที่มีอยู่

คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันให้สัญญานี้เป็นส่วนที่เพิ่มเติม และถือเป็นส่วนหนึ่งของสัญญาที่มีอยู่
โดยหากสัญญานี้มีเนื้อหาหรือข้อความใดที่ขัดแย้งกับสัญญาที่มีอยู่ ให้ถือตามคำวินิจฉัยของกรมการกงสุล
ซึ่งการปฏิบัติตามสัญญาจ้างและสัญญานี้ได้ละเมิดสิทธิและหน้าที่ของคู่สัญญาทั้งสองฝ่าย รวมถึงพนักงาน
ลูกจ้าง ผู้รับจ้างช่วง และบุคคลภายนอกซึ่งกระทำการแทนในนามผู้รับจ้าง

คู่สัญญาทั้งสองฝ่ายจึงตกลงกัน ดังนี้

ข้อ 1. คำรับรองของคู่สัญญา

1.1 คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า กรมการกงสุลในฐานะผู้ควบคุมข้อมูลส่วนบุคคล
อนุญาตให้ผู้รับจ้างเข้าถึงข้อมูลส่วนบุคคลเพื่อประมวลผลข้อมูลส่วนบุคคลในการดำเนินการตามคำสั่งหรือในนามของ
กรมการกงสุลเท่านั้น โดยที่ผู้รับจ้างในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลตกลงที่จะดำเนินการภายใต้คำสั่ง
หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลตามที่กำหนดในสัญญาที่มีอยู่ รวมถึงในสัญญานี้เท่านั้น

1.2 คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า การประมวลผลข้อมูลส่วนบุคคลภายใต้สัญญานี้มีวัตถุประสงค์
ดังต่อไปนี้

(1) ...

(2) ...

(3) ...

ช.ก.อ.

.....

.....

นอกเหนือจากวัตถุประสงค์ที่กล่าวมาในวรรคก่อน ถือว่าเป็นการกระทำหรือการประมวลผลข้อมูลส่วนบุคคลของผู้รับจ้างโดยลำพัง ไม่เกี่ยวข้องกับกรรมการกงสุลในทางใด ๆ และผู้รับจ้างจะรับผิดชอบเกี่ยวกับการดำเนินการดังกล่าวแต่เพียงผู้เดียวเสมือนหนึ่งว่าผู้รับจ้างเป็นผู้ควบคุมข้อมูลส่วนบุคคลในส่วนของการงานดังกล่าวเป็นการส่วนตัว

1.3 คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า ในการปฏิบัติตามสัญญาฉบับนี้ ต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอ โดยผู้รับจ้างรับรองว่าผู้รับจ้างมีมาตรการรักษาความปลอดภัย และดูแลรักษามาตรการดังกล่าวเป็นประจำ ซึ่งรวมไปถึงการพัฒนา และแก้ไขเปลี่ยนแปลงให้ดีขึ้น โดยผู้รับจ้างจะบอกกล่าวล่วงหน้า

1.4 ผู้รับจ้างให้คำรับรองต่อกรรมการกงสุลว่าจะจัดให้มี (1) ธรรมาภิบาลที่ดี (Good Corporate Governance) ในการประมวลผลข้อมูลส่วนบุคคล (2) การรักษาความลับอย่างเคร่งครัด ตามสัญญาจ้าง และ (3) เมื่อสัญญาที่มีอยู่ใด ๆ สิ้นสุดลงหรือถูกบอกเลิกหรือเมื่อได้รับแจ้งจากกรรมการกงสุล ผู้รับจ้างจะดำเนินการลบ และทำลายข้อมูลส่วนบุคคลทั้งหมดด้วยวิธีการที่มีความมั่นคงปลอดภัยตามที่ตกลงกับกรรมการกงสุล และตามกฎหมายที่เกี่ยวข้อง รวมถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งนี้ ผู้รับจ้างจะคำนึงถึงความปลอดภัยของข้อมูลส่วนบุคคลอย่างถึงที่สุด

1.5 คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า สัญญาฉบับนี้จะต้องอ่านร่วมกับสัญญาจ้าง และประกอบเป็นส่วนหนึ่งของสัญญาจ้างดังกล่าว

ข้อ 2. ข้อตกลงและเงื่อนไข

ในกรณีที่มีข้อขัดแย้งกันระหว่างข้อ 2 นี้กับข้อ 5 ของสัญญาฉบับนี้เกี่ยวกับขอบเขตหน้าที่ในการรักษาความลับของคู่สัญญาฝ่ายหนึ่ง และ/หรือ ข้อยกเว้นการรักษาความลับที่ใช้บังคับใด ๆ ที่เกี่ยวกับข้อมูลส่วนบุคคล ให้ข้อกำหนดและเงื่อนไขในข้อ 2 นี้ใช้บังคับ

คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันให้ข้อกำหนดและเงื่อนไขต่อไปนี้ใช้บังคับเกี่ยวกับข้อมูลส่วนบุคคล

2.1 ข้อกำหนดทั่วไป

คู่สัญญาทั้งสองฝ่ายรับทราบและเข้าใจว่า ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กรรมการกงสุลในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ควบคุมให้ผู้รับจ้างในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังนั้น ผู้รับจ้างจึงตกลงที่จะปฏิบัติตามคำสั่งเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของกรรมการกงสุลอย่างเคร่งครัด และจะไม่กระทำการใด ๆ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในนามของกรรมการกงสุลโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษร และผู้รับจ้างจะปฏิบัติตามใด ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดหรือภายใต้ขอบเขตของกฎหมายคุ้มครองข้อมูลส่วนบุคคลเท่านั้น

2.2 ข้อมูลส่วนบุคคลที่เปิดเผย

ผู้ควบคุมข้อมูลส่วนบุคคลตกลงแบ่งปันข้อมูลส่วนบุคคลดังรายการต่อไปนี้แก่ผู้ประมวลผลข้อมูลส่วนบุคคล ดังนี้

สรุป

นางสาว

ก

ข้อมูลส่วนบุคคลที่แบ่งปัน โดยผู้ควบคุมข้อมูลส่วนบุคคล	วัตถุประสงค์ในการแบ่งปันข้อมูลส่วนบุคคล
1. ข้อมูล...	
2. ข้อมูล...	
3. ข้อมูล...	
4. ข้อมูล...	

2.3 การประมวลผลข้อมูลส่วนบุคคล

ผู้รับจ้างมีหน้าที่ ดังนี้

- (1) ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมไปถึงแต่ไม่จำกัดเพียง นโยบาย คุ้มครองข้อมูลส่วนบุคคล ประกาศความเป็นส่วนตัว ข้อตกลงหรือแนวทางปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหรือการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ในการให้บริการและการปฏิบัติตามหน้าที่อื่น ๆ ของตนภายใต้สัญญาที่มีอยู่ทั้งหมด
- (2) แจ้งให้พนักงาน ตัวแทน บุคลากรของตนทราบและดำเนินการให้แน่ใจว่า บุคคลเหล่านั้น ปฏิบัติตามคำสั่งของกรรมการกงสุล และกฎหมายคุ้มครองข้อมูลส่วนบุคคลเท่านั้น
- (3) การประมวลผลข้อมูลส่วนบุคคลต้องทำภายใต้คำสั่งที่เป็นลายลักษณ์อักษรหรือมีบันทึก จากกรรมการกงสุล เว้นแต่กรณีที่ผู้รับจ้างจะต้องปฏิบัติตามกฎหมาย โดยต้องแจ้งให้ กรรมการกงสุลทราบเป็นลายลักษณ์อักษรก่อนดำเนินการ
- (4) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยทั้งปวงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล อย่างเคร่งครัด
- (5) แจ้งให้กรรมการกงสุลทราบเป็นลายลักษณ์อักษรทันทีโดยไม่ชักช้า เมื่อผู้รับจ้างทราบถึง กรณี ดังต่อไปนี้
 - การฝ่าฝืนอย่างร้ายแรงในการรักษาความปลอดภัยหรือมีเหตุที่น่าจะเชื่อได้ว่า ข้อมูลส่วนบุคคลอาจถูกเปิดเผย เข้าถึง หรือใช้โดยไม่ได้รับอนุญาต รวมถึงมี เหตุการณ์ละเมิดข้อมูลส่วนบุคคล
 - เมื่อมีคำร้องขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
 - เมื่อมีหมายเรียก หรือคำสั่งจากศาล หรือเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐ ที่มีอำนาจ หรือหน่วยงานกำกับดูแลที่เกี่ยวข้องกับการประมวลผลข้อมูล ส่วนบุคคล

สรุป

 /-

- (6) ดำเนินการตามที่เหมาะสมและสมควร โดยค่าใช้จ่ายของผู้รับจ้าง รวมไปถึงการแจ้งบุคคลที่ได้รับผลกระทบ การเยียวยาผลกระทบ จากการที่ผู้รับจ้างไม่สามารถดำเนินการรักษาความปลอดภัยหรือป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตต่อข้อมูลส่วนบุคคลได้
- (7) ไม่โอนข้อมูลส่วนบุคคลออก หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลจากบุคคลอื่น ที่อยู่นอกประเทศไทยโดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากกรรมการกฤษฎีกาก่อน

2.4 การป้องกันและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ผู้รับจ้างรับรองและรับประกันว่า ณ วันที่ตกลงให้มีผลใช้บังคับและตลอดระยะเวลาของสัญญาที่มีอยู่ ผู้รับจ้างได้จัดให้มีการควบคุมเมื่อมีการลงข้อมูล ควบคุมการเข้าถึง ป้องกันการแทรกแซง ควบคุมการเปิดเผย มีการใส่รหัสและมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ได้มาตรฐานสากลและเพียงพอเพื่อให้แน่ใจว่า ข้อมูลส่วนบุคคลจะปลอดภัยและคงไว้ซึ่งความลับ ซึ่งรวมถึงการได้รับการป้องกันจากการคุกคามหรืออันตรายที่อาจมีขึ้นจากการเข้าถึงหรือใช้ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

2.5 การละเมิดข้อมูลส่วนบุคคล

ในกรณีที่เกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ไม่ว่าจะเกิดกับกรรมการกฤษฎีกา และ/หรือผู้รับจ้าง และ/หรือผู้รับจ้างช่วง คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันว่าจะดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด แจ้งให้คู่สัญญาอีกฝ่ายรับทราบในทันที ภายในกำหนด 24 (ยี่สิบสี่) ชั่วโมงนับแต่ทราบเหตุ บรรเทาความเสียหาย รวมไปถึงแต่ไม่จำกัดเพียงให้ความช่วยเหลือ อำนาจความสะดวกซึ่งกันและกัน

ข้อ 3. หน้าที่ของกรรมการกฤษฎีกา

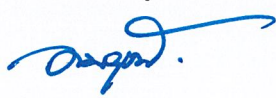
3.1 เป็นผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามสัญญาฉบับนี้

3.2 พิจารณาถึงลักษณะ บริบท ขอบเขต และวัตถุประสงค์ในการประมวลข้อมูลส่วนบุคคล รวมถึงประเมินความเสี่ยงและโอกาสที่อาจเกิดขึ้น และความร้ายแรงที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยกำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ซึ่งครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) เพื่อให้มั่นใจว่ามีระดับความมั่นคงปลอดภัยที่เหมาะสมกับความเสี่ยง และมาตรการดังกล่าวสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3.3 กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามข้อ 3.2 ข้างต้น ในนโยบายคุ้มครองข้อมูลของกรรมการกฤษฎีกาตามสัดส่วนเท่าที่จำเป็นสำหรับกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

3.4 จัดให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลมีการประมวลผลเท่าที่จำเป็น รวมถึงจำนวนข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ขอบเขตระยะเวลาการเก็บรักษา และการเข้าถึงข้อมูล โดยมาตรการดังกล่าวจะต้องทำให้มั่นใจได้ว่าข้อมูลส่วนบุคคลจะถูกจำกัดไม่ให้มีการถูกแทรกแซงโดยบุคคลอื่น

8/2/2562




ข้อ 4. หน้าที่ของผู้รับจ้าง

ผู้รับจ้างตกลงจะดำเนินการ ดังต่อไปนี้

4.1 ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของ กรรมการกงสุล ตลอดจนปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

4.2 ประมวลผลข้อมูลส่วนบุคคลตามที่กรรมการกงสุลกำหนดไว้เป็นลายลักษณ์อักษรเท่านั้น

4.3 ทำให้มั่นใจว่าบุคคลที่ได้รับอนุญาตในการประมวลผลข้อมูลส่วนบุคคลจะเก็บรักษาข้อมูลส่วนบุคคลไว้เป็นความลับและดำเนินการตามกฎหมายอย่างเหมาะสม

4.4 จัดให้มีการปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามกฎหมาย คุ้มครองข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) เพื่อให้มั่นใจว่าระดับความมั่นคงปลอดภัยเป็นไปอย่างเหมาะสมตามความเสี่ยงที่อาจเกิดต่อสิทธิและเสรีภาพของบุคคล และมาตรการดังกล่าวสอดคล้องกับมาตรา 40 (2) ของพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4.5 เก็บรักษาและไม่เปิดเผยข้อมูลส่วนบุคคลของกรรมการกงสุลต่อบุคคลภายนอก เว้นแต่จะได้รับ ความยินยอมเป็นลายลักษณ์อักษรล่วงหน้าจากกรรมการกงสุล

4.6 สนับสนุนกรรมการกงสุลอย่างเต็มความสามารถโดยการใช้มาตรการทางเทคนิคและองค์กร ที่เหมาะสมเพื่อให้กรรมการกงสุลสามารถปฏิบัติหน้าที่ในการตอบสนองต่อคำร้องขอใช้สิทธิของเจ้าของข้อมูล ส่วนบุคคลตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

4.7 แจ้งให้กรรมการกงสุลทราบทันทีเมื่อเกิดเหตุการณ์รั่วไหล การละเมิด การเข้าถึง ใช้ หรือ เปลี่ยนแปลงข้อมูลส่วนบุคคลที่ได้รับจากกรรมการกงสุลโดยไม่ได้รับอนุญาต

4.8 เมื่อกรรมการกงสุลเห็นสมควร ผู้รับจ้างจะต้องดำเนินการลบหรือส่งคืนข้อมูลส่วนบุคคลให้แก่ กรรมการกงสุลทั้งหมดภายหลังจากการประมวลผลข้อมูลส่วนบุคคลสิ้นสุด รวมถึงการลบสำเนาข้อมูลที่มีอยู่ ทั้งหมด เว้นแต่จะมีกฎหมายกำหนดให้เก็บข้อมูลส่วนบุคคลนั้นต่อไปได้ โดยต้องแจ้งให้กรรมการกงสุลทราบ เป็นลายลักษณ์อักษร

4.9 เมื่อกรรมการกงสุลร้องขอ ผู้รับจ้างจะต้องจัดเตรียมข้อมูลที่จำเป็นเพื่อให้กรรมการกงสุลตรวจสอบ การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และเพื่อให้กรรมการกงสุลหรือผู้มีอำนาจของกรรมการกงสุล สามารถดำเนินการตรวจสอบการปฏิบัติงานได้

4.10 ปกป้องและชดใช้ความสูญเสีย ความเสียหาย และค่าใช้จ่ายต่าง ๆ ที่เกิดขึ้นต่อกรรมการกงสุล อันเป็นผลมาจากการที่ผู้รับจ้างละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือการกระทำผิดข้อใดข้อหนึ่งใน สัญญานี้

80/ด  

4.11 ให้การสนับสนุนตามสมควรแก่กรรมการกงสุลเกี่ยวกับการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล และการปรึกษาหารือล่วงหน้ากับคณะกรรมการหรือหน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล

ข้อ 5. การรักษาความลับ

5.1 ข้อจำกัดการใช้และการเปิดเผย

(1) ผู้รับจ้างตกลงจะรักษาข้อมูลที่เป็นความลับทั้งหมดของกรรมการกงสุลไว้เป็นความลับอย่างเคร่งครัด และจะใช้มาตรการที่จำเป็นตามสมควรเพื่อรักษาข้อมูลที่เป็นความลับ รวมทั้ง

(1.1) ปฏิบัติตามมาตรการรักษาความปลอดภัยทั้งหมดที่กำหนดขึ้นเพื่อป้องกันการเข้าถึงหรือการใช้ข้อมูลที่เป็นความลับจากโดยไม่ได้รับอนุญาต

(1.2) เก็บรักษาข้อมูลที่เป็นความลับทั้งหมดภายในการควบคุมของคู่สัญญาฝ่ายนั้น ทั้งนี้ ผู้รับจ้างจะต้องไม่ดำเนินการต่อไปนี้ โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากกรรมการกงสุล

(ก)เปิดเผยข้อมูลที่เป็นความลับดังกล่าวแก่บุคคลภายนอก (ที่ไม่ใช่หน่วยงานกำกับดูแลที่มีอำนาจเหนือผู้รับข้อมูล) เว้นแต่จะได้รับอนุญาตโดยประการอื่นใดภายใต้สัญญาที่มีอยู่

(ข) ใช้ข้อมูลความลับดังกล่าวเพื่อวัตถุประสงค์ใด ๆ ที่นอกเหนือไปจากการใช้สิทธิหรือการปฏิบัติตามหน้าที่ผูกพันของตนภายใต้สัญญาที่มีอยู่

(2) ผู้รับจ้างจะเปิดเผยข้อมูลที่เป็นความลับของกรรมการกงสุลไม่ได้ เว้นแต่เฉพาะบุคคลหรือกรณี ดังนี้

(2.1) ให้แก่บุคลากรของตนที่เป็นพนักงาน ตัวแทน ที่จำเป็นต้องรู้ข้อมูลที่เป็นความลับดังกล่าวเพื่อใช้สิทธิของผู้รับข้อมูลดังกล่าวหรือเพื่อปฏิบัติตามหน้าที่ผูกพันของผู้รับข้อมูลดังกล่าว ตามสัญญาที่มีอยู่

(2.2) ให้แก่หน่วยงานกำกับดูแลที่มีอำนาจเหนือตามกฎหมายของผู้รับจ้าง โดยต้องแจ้งให้กรรมการกงสุลทราบเป็นลายลักษณ์อักษร

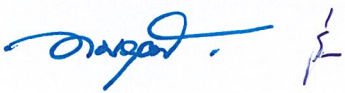
(2.3) ตามที่ได้รับอนุญาตโดยเหตุผลประการอื่นภายใต้สัญญาที่ตกลงร่วมกัน

(3) ในการใช้ข้อมูลที่เป็นความลับข้างต้น ผู้รับจ้างต้องใช้ความสามารถและความเชี่ยวชาญตามสมควรในการค้นหาหรือป้องกันการใช้หรือการเปิดเผยข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต

(4) ในกรณีที่ผู้รับจ้างทราบว่าหรือมีเหตุผลที่จะเชื่อได้ว่ามีบุคคลใด ๆ ที่ได้เข้าถึงข้อมูลที่เป็นความลับ โดยฝ่าฝืนหรือมีเจตนาที่จะฝ่าฝืนข้อกำหนดของสัญญาที่มีอยู่ ผู้รับจ้างจะต้องแจ้งให้กรรมการกงสุลทราบทันที และให้ความร่วมมือกับหน่วยงานที่มีอำนาจในการยับยั้งการกระทำที่ฝ่าฝืนนั้น

(5) ผู้รับจ้างอาจใช้หรือเปิดเผยข้อมูลที่เป็นความลับ (เว้นแต่ข้อมูลส่วนบุคคล) ตามกระบวนการทางกฎหมายที่กำหนดให้ต้องเปิดเผยข้อมูลที่เป็นความลับดังกล่าว โดยมีเงื่อนไขว่า ผู้รับจ้างจะต้องบอกกล่าวล่วงหน้าเป็นลายลักษณ์อักษรเกี่ยวกับการถูกบังคับให้เปิดเผยดังกล่าวแก่กรรมการกงสุล และ

8000



- ความเสียหายที่สามารถคำนวณเป็นตัวเงินได้ในเบื้องต้น
- ข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการละเมิด

ข้อ 8. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เมื่อเจ้าของข้อมูลส่วนบุคคลติดต่อผู้รับจ้างหรือผู้รับจ้างช่วง แล้วแต่กรณี เพื่อขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้รับจ้างตกลงที่จะแจ้งกรรมการกงสุลทันที หรือผู้รับจ้างอาจดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลได้ ก็ต่อเมื่อผู้รับจ้างไม่สามารถติดต่อกรรมการกงสุล และต้องดำเนินการข้างต้นโดยไม่อาจหลีกเลี่ยงได้ ทั้งนี้ ผู้รับจ้างต้องพิจารณาถึงปัจจัยต่าง ๆ โอกาสที่จะเกิดความเสียหายแก่กรรมการกงสุล และแนวทางปฏิบัติระหว่างคู่สัญญาทั้งสองฝ่าย โดยมีบันทึกการพิจารณาดังกล่าวเป็นหลักฐานในการดำเนินการข้างต้น ทั้งนี้ บันทึกดังกล่าวไม่ตัดสิทธิกรรมการกงสุลที่จะเรียกร้องค่าเสียหายกับผู้รับจ้าง (ถ้ามี)

ข้อ 9. ความสมบูรณ์ของสัญญา

ในกรณีที่ข้อตกลงใดข้อตกลงหนึ่งภายใต้สัญญานี้เป็นโมฆะ คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันว่าข้อตกลงอื่นภายใต้สัญญานี้ที่ไม่เป็นโมฆะ ยังมีผลบังคับใช้ระหว่างคู่สัญญาทั้งสองฝ่ายต่อไป และคู่สัญญาทั้งสองฝ่ายจะร่วมกันแก้ไขข้อตกลงที่มีผลเป็นโมฆะให้มีผลบังคับใช้ได้ตามกฎหมาย โดยให้มีผลในทางการค้าที่ใกล้เคียงกับข้อตกลงที่มีผลเป็นโมฆะนั้นมากที่สุดเท่าที่จะทำได้

ข้อ 10. การแก้ไขเปลี่ยนแปลง

คู่สัญญาทั้งสองฝ่ายตกลงร่วมกันที่จะไม่ดำเนินการแก้ไขหรือเปลี่ยนแปลงข้อตกลง เว้นแต่จะทำการเป็นลายลักษณ์อักษรและลงนามโดยคู่สัญญาทั้งสองฝ่ายหรือโดยการบอกกล่าวล่วงหน้าจากกรรมการกงสุล โดยให้การเปลี่ยนแปลงดังกล่าวมีผลบังคับใช้ไม่เกิน 60 วัน นับแต่วันที่กรรมการกงสุล ได้ส่งคำบอกกล่าวข้างต้น

ข้อ 11. ความรับผิดชอบตามสัญญา

ผู้รับจ้างจะรับผิดชอบค่าใช้จ่ายให้กับกรรมการกงสุลสำหรับค่าปรับ ความสูญเสีย หรือความเสียหายทั้งหมด อันเนื่องมาจากการที่ผู้รับจ้างฝ่าฝืนข้อกำหนดหรือเงื่อนไขใด ๆ ภายใต้สัญญานี้ ตลอดจนการกระทำใด ๆ อันเกิดจากความประมาทเลินเล่อของผู้รับจ้างและผู้รับจ้างช่วง

ข้อ 12. การสิ้นสุดของสัญญา

12.1 สัญญานี้จะสิ้นสุดได้โดยการตกลงร่วมกันระหว่างคู่สัญญาทั้งสองฝ่ายหรือการสิ้นสุดของสัญญาหลักที่ได้อ้างถึงในสัญญานี้

12.2 สัญญานี้ เป็นสัญญาอุปกรณ์ของสัญญา..... หากสัญญา..... สิ้นผลผูกพันลงไม่ว่ากรณีใด ให้ถือว่าสัญญานี้สิ้นสุดตามกฎหมายด้วยโดยปริยาย

เพื่อเป็นหลักฐานแห่งการนี้คู่สัญญาทั้งสองฝ่ายภายใต้สัญญานี้ ได้รับทราบและเข้าใจ คำรับรองข้อตกลงและเงื่อนไข ตลอดจนเอกสารแนบท้ายที่ได้ตกลงกันไว้ทั้งหมดแล้ว และได้ลงลายมือชื่อพร้อม

8/8/20

ประทับตราสำคัญ (หากมี) ด้านล่างในต้นฉบับสัญญาฉบับนี้จำนวนสองฉบับไว้เป็นสำคัญต่อหน้าพยานทั้งสองแล้ว
โดยต่างฝ่ายต่างถือต้นฉบับไว้ฝ่ายละฉบับเพื่อเก็บไว้เป็นหลักฐาน

ลงชื่อ.....กรรมการกงสุล

(.....)

ลงชื่อ.....ผู้รับจ้าง

กรรมการผู้มีอำนาจ

บริษัท จำกัด

ลงชื่อ.....พยาน

(.....)

ลงชื่อ.....พยาน

(.....)

8090

นางสาว.....