รายละเอียดคุณลักษณะเฉพาะของพัสดุที่จะจ้าง
โครงการเพิ่มประสิทธิภาพการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และการเฝ้าระวังภัยคุกคาม (CDDSOC)

๑. ความเป็นมา

ปัจจุบันเทคโนโลยีดิจิทัลมีบทบาทสำคัญในการขับเคลื่อนภารกิจของหน่วยงานภาครัฐ โดยเฉพาะด้านการให้บริการข้อมูล ระบบงาน และการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ต ซึ่งแม้จะอำนวยต่อการทำงานที่สะดวก รวดเร็ว และมีประสิทธิภาพมากขึ้น แต่ก็ส่งผลให้ความเสี่ยงด้านภัยคุกคามทางไซเบอร์เพิ่มสูงขึ้นด้วยเช่นกัน ทั้งในรูปแบบของ การโจมตีระบบเครือข่าย การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การแพร่กระจายมัลแวร์ การโจมตีแบบฟิชชิ่ง และ การโจมตีแบบ DDoS เป็นต้นเพื่อให้การดำเนินงานของหน่วยงานมีความปลอดภัยและสอดคล้องกับแนวนโยบายของรัฐบาลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หน่วยงานจึงมีความจำเป็นต้องพัฒนาและเพิ่มประสิทธิภาพการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ โดยการจัดตั้งและพัฒนาศูนย์เฝ้าระวังและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Community Development Department Security Operation Center : CDDSOC) เพื่อทำหน้าที่ในการเฝ้าระวัง วิเคราะห์ และตรวจจับภัยคุกคามที่อาจส่งผลกระทบต่อระบบสารสนเทศของกรมการพัฒนาชุมชน ตอบสนองต่อเหตุการณ์อย่างทันท่วงที บริหารจัดการข้อมูลและเหตุการณ์ด้านความปลอดภัยอย่างเป็นระบบ สนับสนุนให้การดำเนินงานและการให้บริการของกรมการพัฒนาชุมชนเป็นไปอย่างมั่นคงปลอดภัยและต่อเนื่อง

๒. วัตถุประสงค์

๒.๑ เพื่อให้บริการระบบศูนย์เฝ้าระวังและตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operation Center : SOC)

๒.๒ เพื่อเพิ่มประสิทธิภาพการให้บริการในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และการเฝ้าระวังภัยคุกคาม (CDDSOC)

๓. คุณสมบัติของผู้ยื่นข้อเสนอ

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนด ตามที่ประกาศและเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่กรมการพัฒนาชุมชน ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

/๓.๑๐ ผู้ยื่น...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๓.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้

(๑) การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

(๒) กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

(๓) การยื่นข้อเสนอของกิจการร่วมค้า

(๓.๑) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

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

๓.๑๒.๑ กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ ๑ ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้น ตามกฎหมายไทยหากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนอนั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม – เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก ๑ ปี ได้

๓.๑๒.๒ กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า หรือกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงิน ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ดังนี้

(๑) มูลค่าการจัดซื้อจัดจ้างไม่เกิน ๑ ล้านบาท ไม่ต้องกำหนดทุนจดทะเบียน

(๒) มูลค่าการจัดซื้อจัดจ้างเกิน ๑ ล้านบาท แต่ไม่เกิน ๕ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๑ ล้านบาท

(๓) มูลค่าการจัดซื้อจัดจ้างเกิน ๕ ล้านบาท แต่ไม่เกิน ๑๐ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๒ ล้านบาท

(๔) มูลค่าการจัดซื้อจัดจ้างเกิน ๑๐ ล้านบาท แต่ไม่เกิน ๒๐ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๓ ล้านบาท

/(๕) มูลค่า...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

(๕) มูลค่าการจัดซื้อจัดจ้างเกิน ๒๐ ล้านบาท แต่ไม่เกิน ๖๐ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๘ ล้านบาท

(๖) มูลค่าการจัดซื้อจัดจ้างเกิน ๖๐ ล้านบาท แต่ไม่เกิน ๑๕๐ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๒๐ ล้านบาท

(๗) มูลค่าการจัดซื้อจัดจ้างเกิน ๑๕๐ ล้านบาท แต่ไม่เกิน ๓๐๐ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๖๐ ล้านบาท

(๘) มูลค่าการจัดซื้อจัดจ้างเกิน ๓๐๐ ล้านบาท แต่ไม่เกิน ๕๐๐ ล้านบาท ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๑๐๐ ล้านบาท

(๙) มูลค่าการจัดซื้อจัดจ้างเกิน ๕๐๐ ล้านบาทขึ้นไป ต้องมีทุนจดทะเบียนไม่ต่ำกว่า ๒๐๐ ล้านบาท

๓.๑๒.๓ สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

๓.๑๒.๔ กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศหรือบริษัทหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทย แจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

๓.๑๒.๕ กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทยตามข้อ ๓.๑๒.๒, ๓.๑๒.๓ และข้อ ๓.๑๒.๔ (๒) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) จนถึงวันเสนอราคา

/ทั้งนี้...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องยื่นเอกสารที่แสดงให้เห็นถึงข้อมูลเกี่ยวกับมูลค่าสุทธิของกิจการแล้วแต่กรณี ประกอบกับเอกสารดังกล่าวจะต้องผ่านการรับรองตามระเบียบกระทรวงการต่างประเทศว่าด้วยการรับรองเอกสาร พ.ศ. ๒๕๓๙ และที่แก้ไขเพิ่มเติม กำหนด โดยจะต้องยื่นเอกสารดังกล่าวในวันยื่นข้อเสนอ หากผู้ยื่นข้อเสนอมิได้มีการยื่นเอกสารดังกล่าวมาพร้อมกับการยื่นข้อเสนอให้ถือว่าผู้ยื่นข้อเสนอรายนั้นยื่นเอกสารไม่ครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารประกวดราคา

๓.๑๒.๖ กรณีตามข้อ ๓.๑๒.๑ - ข้อ ๓.๑๒.๕ ไม่ใช้บังคับกับกรณีดังต่อไปนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

(๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการ ตามพระราชบัญญัติล้มละลาย พ.ศ. ๒๔๘๓ และที่แก้ไขเพิ่มเติม

(๓) งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

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

(๕) การซื้ออสังหาริมทรัพย์และการเช่าอสังหาริมทรัพย์

(๖) กรณีงานจ้างบริหารหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงานขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

๓.๑๓ ผู้ยื่นข้อเสนอต้องเป็นผู้มีอาชีพรับจ้างงานที่ประกวดราคาจ้าง และมีผลงานในการดำเนินการด้านระบบรักษาความปลอดภัยระบบสารสนเทศ หรืองานด้านการบริหารจัดการระบบสารสนเทศ หรืองานอื่น ๆ ที่เกี่ยวข้อง ที่เป็นคู่สัญญาโดยตรงกับหน่วยงานราชการ รัฐวิสาหกิจหรือบริษัทเอกชนในประเทศไทย อย่างน้อย ๑ สัญญา มูลค่าของแต่ละสัญญา ๆ ละไม่น้อยกว่า ๔,๙๒๕,๐๐๐ บาท (สี่ล้านเก้าแสนสองหมื่นห้าพันบาทถ้วน) ซึ่งสัญญาเป็นที่สิ้นสุดในระยะเวลาไม่เกิน ๕ ปีที่ผ่านมา นับจากวันยื่นเสนอราคา โดยต้องแนบสำเนาหนังสือรับรองผลงาน หรือสำเนาสัญญา หรือสำเนาใบสั่งซื้อ/จ้าง และเอกสารอันเป็นส่วนหนึ่งของสัญญาที่กำหนดรายละเอียดขอบเขตของงาน ทั้งนี้ กรมการพัฒนาชุมชนขอสงวนสิทธิที่จะตรวจสอบข้อเท็จจริงสำหรับผลงานที่เสนอ

๓.๑๔ ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความรู้ความเชี่ยวชาญด้านระบบรักษาความปลอดภัยระบบสารสนเทศ หรืองานด้านการบริหารจัดการระบบสารสนเทศ หรืองานอื่นๆ ที่เกี่ยวข้อง โดยต้องแนบเอกสารใบรับรองที่แสดงถึงขีดความสามารถในการทำงานเกี่ยวกับการให้บริการด้านระบบรักษาความปลอดภัยระบบสารสนเทศ หรืองานด้านการบริหารจัดการระบบสารสนเทศของบุคลากรที่มีความรู้ ความเชี่ยวชาญมาพร้อมวันยื่นเอกสารเสนอราคา

๔. ขอบเขตของงาน

ผู้ยื่นข้อเสนอต้องให้บริการศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC) สามารถใช้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ โดยผู้ยื่นข้อเสนอต้องดำเนินการดังต่อไปนี้

๔.๑ ผู้ยื่นข้อเสนอต้องศึกษา วิเคราะห์รายละเอียดความต้องการ ออกแบบจัดทำแผนการดำเนินงานโครงสร้างและรายละเอียดของระบบศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC) แผนปฏิบัติการโครงการฯแผนบริหารความเสี่ยง วิธีการ ขั้นตอน และรายละเอียดกิจกรรมอื่นๆ เสนอต่อกรมการพัฒนาชุมชนภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา เพื่อให้กรมการพัฒนาชุมชนพิจารณาเห็นชอบและจัดประชุมแผนการดำเนินงานและรายงานความก้าวหน้าเป็นประจำทุกเดือน

/พร้อมสำเนา...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

พร้อมสำเนาเอกสารในรูปแบบเอกสารอิเล็กทรอนิกส์ที่สามารถแก้ไขปรับปรุงได้ เช่น Word, Excel เป็นต้น หากมีค่าใช้จ่ายใด ๆ เกิดขึ้นเพิ่มเติมในภายหลัง เพื่อทำให้ระบบทำงานได้เหมือนเดิม ผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด

๔.๒ ผู้ยื่นข้อเสนอต้องศึกษา วิเคราะห์ข้อมูล ออกแบบ และจัดทำแผนโครงสร้างระบบศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC) ที่ครอบคลุมและเชื่อมโยงระบบต่างๆให้ถูกต้องเป็นปัจจุบัน และเสนอต่อกรมการพัฒนาชุมชนภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา เพื่อให้กรมการพัฒนาชุมชนพิจารณาเห็นชอบ

๔.๓ ผู้ยื่นข้อเสนอต้องจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC) สำหรับกรมการพัฒนาชุมชน จำนวน ๑ แห่ง ในการเฝ้าระวัง ตรวจสอบ ป้องกัน และรับมือภัยคุกคามทางด้านไซเบอร์ (Cyber Prevention , Detections & Responses) โดยมีรายละเอียด ดังนี้

๔.๓.๑ ให้บริการเฝ้าระวัง วิเคราะห์ ตรวจจับ และตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Security Monitoring) ตลอด ๒๔ ชั่วโมง ไม่เว้นวันหยุดราชการและวันหยุดนักขัตฤกษ์ ให้เป็นไปตามข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ตามที่กำหนด ตลอดระยะเวลาของสัญญา โดยมีเงื่อนไขดังต่อไปนี้

ระดับความรุนแรง	คำอธิบาย	เวลาในการตอบสนอง (Response time)
Critical	ผลกระทบกับระบบสารสนเทศหลักทำให้การดำเนินธุรกิจหยุดชะงัก และจะต้องแก้ไขอย่างเร่งด่วนที่สุด	ภายใน ๑๕ นาที
High	ผลกระทบกับระบบสารสนเทศที่ทำให้ธุรกิจไม่สามารถดำเนินการได้ อย่างมีประสิทธิภาพ และจำเป็นต้องแก้ไขอย่างเร่งด่วน	ภายใน ๓ ชั่วโมง
Medium	ผลกระทบกับระบบสารสนเทศทีมีผลต่อการดำเนินธุรกิจ และจำเป็นต้องแก้ไขอย่างทันท่วงที	ภายใน ๖ ชั่วโมง
Low	ผลกระทบกับระบบสารสนเทศที่มีผลต่อประสิทธิภาพการทำงานทั่วไป แต่ไม่มีผลกระทบต่อการดำเนินธุรกิจโดยรวม	ภายใน ๒๔ ชั่วโมง

๔.๓.๒ ผู้ยื่นข้อเสนอต้องจัดให้มีบริการส่งข้อมูลจราจรทางคอมพิวเตอร์ (Logs) จากอุปกรณ์และระบบเครือข่ายคอมพิวเตอร์ของกรมการพัฒนาชุมชน ไปยังศูนย์บริการปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ของผู้ยื่นข้อเสนอได้อย่างครบถ้วนสมบูรณ์ โดยมีข้อกำหนดและขั้นตอน ดังนี้

๑) ตรวจสอบอุปกรณ์และระบบทั้งหมดที่มีอยู่ในระบบเครือข่ายคอมพิวเตอร์ของกรมการพัฒนาชุมชน

๒) วิเคราะห์อุปกรณ์และระบบที่มีความจำเป็นในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs)

๓) ตั้งค่าอุปกรณ์และระบบเครือข่ายคอมพิวเตอร์ของกรมการพัฒนาชุมชน เพื่อให้อุปกรณ์สามารถส่งข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ออกมาได้อย่างครบถ้วนสมบูรณ์

๔) จัดให้มีบริการเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์จัดเก็บข้อมูล ให้เพียงพอกับการใช้งานระบบส่งข้อมูลจราจรทางคอมพิวเตอร์ (Log Collector) และดำเนินการติดตั้ง ณ ศูนย์ควบคุมระบบคอมพิวเตอร์ของกรมการพัฒนาชุมชน จำนวนไม่น้อยกว่า ๑ เครื่อง โดยมีรายละเอียดดังนี้

/๔.๑) มีหน่วย...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๔.๑) มีหน่วยประมวลผลกลาง (CPU) แบบ ๑๐ แกนหลัก (๑๐ core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า ๒.๒ GHz จำนวนไม่น้อยกว่า ๑ หน่วย

๔.๒) หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ ๖๔ bit มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันไม่น้อยกว่า ๑๓ MB

๔.๓) มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR๔ หรือดีกว่า มีขนาดไม่น้อยกว่า ๑๖ GB

๔.๔) สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID ๐, ๑, ๕

๔.๕) มีหน่วยจัดเก็บข้อมูลชนิด SAS หรือ SATA ที่มีความเร็วรอบไม่น้อยกว่า ๑๐,๐๐๐ รอบต่อนาที ขนาดความจุไม่น้อยกว่า ๑ TB หรือ ชนิด Solid State Drive หรือดีกว่า ขนาดความจุไม่น้อยกว่า ๔๘๐ GB จำนวนไม่น้อยกว่า ๒ หน่วย

๔.๖) มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๒ ช่อง

๔.๗) มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย

๕) จัดให้มีบริการระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายที่รองรับการใช้งานที่เหมาะสม และดำเนินการติดตั้ง ให้สามารถทำงานได้อย่างมีประสิทธิภาพ

๖) ติดตั้งระบบส่งข้อมูลจราจรทางคอมพิวเตอร์ (Log Collector) เพื่อใช้ในการรวมรวบข้อมูลจราจรทางคอมพิวเตอร์ (Logs) และส่งไปยังศูนย์บริการปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์

๗) ระบบส่งข้อมูลจราจรทางคอมพิวเตอร์ (Log Collector) ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยมีปริมาณไม่น้อยกว่า ๑๐ กิกะไบต์ต่อวัน (Gigabyte Per Day) เป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน

๘) ดำเนินการให้บริการส่งข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ภายใน ๖๐ วัน นับถัดจากวันที่ลงนามในสัญญา

๔.๓.๓ ผู้ยื่นข้อเสนอต้องจัดให้มีบริการระบบ Security Information & Event Management : SIEM สำหรับให้บริการภายในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์และเป็นผลิตภัณฑ์ที่ได้รับมาตรฐานการประเมินของ Gartner Magic Quadrant for Security Information and Event Management ตั้งแต่ปี ๒๐๒๔ เป็นต้นไป โดยมีคุณสมบัติเป็นอย่างน้อย ดังนี้

๑) สามารถรวบรวมและจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Data Aggregation & Log Management) จากแหล่งต่างๆที่กรมการพัฒนาชุมชนใช้งานอยู่ในระบบเครือข่ายคอมพิวเตอร์ เช่น Firewall, Server, Endpoint, Network Device, Cloud มาไว้ที่ตัวระบบได้

๒) สามารถสร้างความสัมพันธ์ระหว่างชุดข้อมูลจราจรทางคอมพิวเตอร์ (Logs) และทำการวิเคราะห์เพื่อตรวจจับภัยคุกคามทางด้านไซเบอร์ได้ (Correlation & Analysis) ได้อย่างน้อย ดังนี้

๒.๑) การเข้าถึงระบบโดยไม่ได้รับอนุญาต (Unauthorized Access)

๒.๒) โปรแกรมอันตรายที่ส่งผลต่อระบบคอมพิวเตอร์ (Malicious Code)

๒.๓) การจราจรของข้อมูลต้องสงสัยที่เกิดขึ้นต่อระบบเครือข่าย (Suspect Traffic)

๒.๔) กิจกรรมต้องสงสัยที่เกิดขึ้นบนระบบคอมพิวเตอร์ (Suspect Activity)

๒.๕) การหลอกลวงเชิงจิตวิทยาประเภทฟิชชิ่ง (Phishing Attack)

๒.๖) การค้นหา เคลื่อนย้าย และขยายการโจมตีภายในระบบเครือข่าย (Lateral Movement)

๒.๗) มัลแวร์เรียกค่าไถ่ (Ransomware)

๒.๘) การลักลอบขโมยข้อมูล (Data Exfiltration)

/๒.๙) การโจมตี...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๒.๙) การโจมตีเพื่อทำให้ระบบหยุดให้บริการ (DoS/DDoS Attack)

๓) สามารถวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์แบบ Real-Time Analytics

๔) สามารถตรวจจับภัยคุกคามทางไซเบอร์ด้วย Threat Detection Engine ที่มีการใช้เทคโนโลยี Artificial Intelligence (AI) และ Machine Learning (ML) เพื่อเพิ่มประสิทธิภาพความรวดเร็วและความแม่นยำในการตรวจจับภัยคุกคาม เช่น การวิเคราะห์พฤติกรรม (UEBA & Anomaly Detection) การเรียนรู้และตรวจจับพฤติกรรมที่ผิดปกติของผู้ใช้งานและอุปกรณ์ (User and Entity Behavior Analytics) ได้โดยอัตโนมัติ เป็นต้น

๕) สามารถทำการค้นหา (Search) ข้อมูล Logs ด้วย Keyword หรือ Full Text ได้

๖) สามารถทำงานบนระบบเครือข่าย IPv๔ หรือ IPv๖ ได้

๗) มีเทคโนโลยีหน่วยข่าวกรองภัยคุกคามทางไซเบอร์ (Threat Intelligence) ซึ่งเก็บรวบรวมข้อมูลภัยคุกคามทางไซเบอร์จากทั่วโลก เพื่อเพิ่มประสิทธิภาพในการเฝ้าระวังและตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์

๘) มีหน้าจอแสดงผล (Dashboard & Visualization) ซึ่งสามารถแสดงผลข้อมูลได้อย่างน้อยดังนี้

๘.๑) แสดงผลข้อมูลในรูปแบบของแผนภูมิหรือตารางได้

๘.๒) แสดงภาพรวมสถานะความปลอดภัย

๘.๓) จัดลำดับความสำคัญของเหตุการณ์

๘.๔) แสดงรายละเอียด (Drill Down) เพื่อตรวจสอบเชิงลึกได้

๘.๕) แสดงสถานะการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ของอุปกรณ์และระบบ

๙) สามารถปรับแต่ง (Customization) หน้าจอแสดงผล (Dashboard & Virtualization) เพื่อให้สอดคล้องกับความต้องการได้อย่างน้อย ดังนี้

๙.๑) รูปแบบการแสดงผลข้อมูล เช่น กราฟแผนภูมิ, กราฟตาราง, กราฟแท่ง, กราฟเส้น, กราฟวงกลม เป็นต้น

๙.๒) การแสดงภาพรวมสถานะความปลอดภัย

๙.๓) การจัดลำดับความสำคัญของเหตุการณ์

๙.๔) การแสดงรายละเอียด (Drill Down) เพื่อตรวจสอบเชิงลึกได้

๙.๕) การแสดงสถานะการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ของอุปกรณ์และระบบ

๑๐) สามารถแจ้งเตือน (Notification) เหตุการณ์ภัยคุกคามทางไซเบอร์ ได้อย่างน้อย ดังนี้

๑๐.๑) Email

๑๐.๒) HTTP/JSON

๑๐.๓) ServiceNow

๑๐.๔) Slack

๑๐.๕) Jira

๑๐.๖) Line

๑๑) สามารถ Export ข้อมูลจราจรทางคอมพิวเตอร์ (Logs) แบบ XLSX หรือ JSON หรือ CSV ได้เป็นอย่างน้อย

๑๒) สามารถ Export รายงาน ในรูปแบบ PDF หรือ CSV หรือ JSON ได้เป็นอย่างน้อย

๑๓) สามารถสร้างรายงานตามมาตรฐานด้านความปลอดภัยหรือการปฏิบัติตามข้อกำหนด (Compliance) ได้อย่างน้อย ดังนี้

๑๓.๑) ISO ๒๗๐๐๑

๑๓.๒) NIST Cybersecurity Framework

/๑๔) สามารถ...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๑๔) สามารถกำหนดสิทธิ์ผู้ใช้งานระบบได้ (Role Based Access Control)

๔.๓.๔ ผู้ยื่นข้อเสนอต้องจัดให้มีบริการประสานงาน การทำงานอัตโนมัติ และการตอบสนองด้านความปลอดภัยโดยเฉพาะ (Security Orchestration, Automation and Response : SOAR) และต้องเป็นบริการที่อยู่ใน SPARK Matrix ™: Security Orchestration, Automation and Response : (SOAR) ตั้งแต่ปี ๒๐๒๔ เป็นต้นไป โดยมีความสามารถอย่างน้อย ดังนี้

๑) สามารถเชื่อมต่อกับระบบรักษาความปลอดภัยที่กรมการพัฒนาชุมชนใช้งานอยู่ได้ ยกตัวอย่างเช่น Anti-Malware และ Next Generation Firewall เป็นต้น

๒) สามารถสร้างคู่มือหรือแผนการปฏิบัติงานเพื่อรับมือภัยคุกคามทางไซเบอร์ (Playbook) สำหรับการตอบสนองต่อภัยคุกคามด้านไซเบอร์แบบอัตโนมัติได้ตามที่กรมการพัฒนาชุมชนกำหนดอย่างน้อย ๕ คู่มือ (Playbook)

๓) สามารถกำหนดนโยบาย (Policy) คู่มือหรือแผนการปฏิบัติงานเพื่อรับมือภัยคุกคามทางไซเบอร์ (Playbook) เพื่อบรรเทาเหตุการณ์ภัยคุกคามทางไซเบอร์ (Mitigation) ได้อย่างน้อย ดังนี้

๓.๑) บล็อก IP Address ผ่านอุปกรณ์ Next Generation Firewall

๓.๒) การแยกอุปกรณ์ที่ตรวจพบความเสี่ยงออกจากระบบเครือข่าย (Isolation/Quarantine Computer) ผ่านระบบ Anti-Malware

๔) สามารถบริหารจัดการคู่มือหรือแผนการ (Playbook) โดยรองรับการสร้าง, การปรับปรุงแก้ไขหรือการลบผ่านหน้าจอ GUI หรือ Web Browser ได้เป็นอย่างน้อย

๕) มีความสามารถทางด้าน Artificial Intelligence Technology เพื่อให้คำแนะนำในการสร้างคู่มือหรือแผนการ (Playbook) การตอบสนองต่อภัยคุกคามทางด้านไซเบอร์แบบอัตโนมัติ (Automatic) เพื่อเพิ่มประสิทธิภาพ ความรวดเร็วและความแม่นยำของนโยบาย (Policy)

๔.๓.๕ ผู้ยื่นข้อเสนอต้องจัดให้มีระบบบริหารจัดการการให้บริการด้านเทคโนโลยีสารสนเทศ (IT Service Management: ITSM) และได้รับการรับรองมาตรฐานสากล Gartner Magic Quadrant for IT Service Management Platforms: ITSM ตั้งแต่ปี ๒๐๒๒ เป็นต้นไป โดยมีความสามารถอย่างน้อย ดังนี้

๑) การจัดการคำขอบริการ (Request Management) เพื่อให้ผู้ใช้ส่งคำขอและติดตามสถานะของเหตุการณ์ภัยคุกคามทางด้านไซเบอร์ได้

๒) การจัดการเหตุการณ์ (Incident Management) เพื่อใช้ในการตอบสนองต่อเหตุการณ์ภัยคุกคามทางด้านไซเบอร์ตามลำดับความสำคัญก่อนหลัง

๔.๓.๖ ผู้ยื่นข้อเสนอต้องจัดให้มีชุดกฎการวิเคราะห์ความสัมพันธ์ของเหตุการณ์ภัยคุกคามทางไซเบอร์ (Set of Correlation Rules) ภายใต้เงื่อนไขดังต่อไปนี้

๑) จัดให้มีการออกแบบชุดกฎการวิเคราะห์ความสัมพันธ์ของเหตุการณ์ภัยคุกคามทางไซเบอร์ (Set of Correlation Rules) จากข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ที่ได้รับจากอุปกรณ์และระบบเครือข่ายคอมพิวเตอร์ของกรมการพัฒนาชุมชน โดยใช้แนวทางปฏิบัติของ MITRE ATT&CK Framework ในการจำแนกประเภท หรือเทคนิคของภัยคุกคามทางด้านไซเบอร์ที่ตรวจพบ

๒) การเพิ่มและการปรับปรุงชุดกฎการวิเคราะห์ความสัมพันธ์ของเหตุการณ์ภัยคุกคามทางไซเบอร์ (Set of Correlation Rules) ในอนาคตจะอยู่ภายใต้การกับกำดูแล ตัดสินใจและดุลพินิจของผู้ยื่นข้อเสนอ

๔.๓.๗ ผู้ยื่นข้อเสนอต้องจัดให้มีบริการการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นพร้อมทั้งแจ้งเตือนกรมการพัฒนาชุมชนตามข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) ที่กำหนด โดยผู้ยื่นข้อเสนอต้องมีการจำแนกประเภทภัยของคุกคามทางไซเบอร์ไว้เบื้องต้นเป็นอย่างน้อย ดังนี้

/๑) การเข้าถึง...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๑) การเข้าถึงระบบโดยไม่ได้รับอนุญาต (Unauthorized Access)

๒) โปรแกรมอันตรายที่ส่งผลกระทบต่อระบบคอมพิวเตอร์ (Malicious Code)

๓) การจราจรของข้อมูลต้องสงสัยที่เกิดขึ้นต่อระบบเครือข่าย (Suspect Traffic)

๔) กิจกรรมต้องสงสัยที่เกิดขึ้นบนระบบคอมพิวเตอร์ (Suspect Activity)

๕) การหลอกลวงเชิงจิตวิทยาประเภทฟิชชิ่ง (Phishing Attack)

๖) การค้นหา เคลื่อนย้าย และขยายการโจมตีภายในระบบเครือข่าย (Lateral Movement)

๗) มัลแวร์เรียกค่าไถ่ (Ransomware)

๘) การลักลอบขโมยข้อมูล (Data Exfiltration)

๙) การโจมตีเพื่อทำให้ระบบหยุดให้บริการ (DoS/DDoS Attack)

๔.๓.๘ ผู้ยื่นข้อเสนอต้องจัดให้มีระบบบริหารจัดการและติดตามสถานะการดำเนินงานเหตุการณ์ภัยคุกคามทางไซเบอร์ (Incident Management System) ให้กับกรมการพัฒนาชุมชน โดยจัดให้มีประเภทบัญชีรายชื่อไม่น้อยกว่า ๒ ประเภท เช่น บัญชีรายชื่อประเภทเจ้าหน้าที่ (Admin), บัญชีรายชื่อประเภทผู้ใช้งานทั่วไป (User) เป็นต้น โดยจำนวนแต่ละประเภทต้องเป็นไปตามที่กรมการพัฒนาชุมชนกำหนด

๔.๓.๙ ผู้ยื่นข้อเสนอต้องจัดให้มีบริการประเมินความมั่นคงปลอดภัยทางไซเบอร์จากมุมมองภายนอกผ่านระบบโดเมนตามที่กรมการพัฒนาชุมชนกำหนด โดยมีรายละเอียดเป็นอย่างน้อย ดังนี้

๑) จัดให้มีบริการประเมินความมั่นคงปลอดภัยทางไซเบอร์จากมุมมองภายนอกผ่านระบบโดเมน (External Attack Surface Management) โดยเฉพาะ สำหรับการเฝ้าระวังและติดตามความเสี่ยงทรัพย์สินดิจิทัลของกรมการพัฒนาชุมชนที่มีการเปิดเผยต่อสาธารณะผ่านโดเมนของกรมการพัฒนาชุมชน (cdd.go.th)

๒) จัดให้มีบริการการให้คะแนนความมั่นคงปลอดภัย (Security Rating) และแสดงผลรายงานในรูปแบบที่เข้าใจง่าย ตามปัจจัยความเสี่ยง (Risk Factors) ที่กรมการพัฒนาชุมชนกำหนดได้อย่างน้อย ดังนี้

๒.๑) ด้านความปลอดภัยบนระบบเครือข่าย (Network Security)

๒.๒) ด้านการตั้งค่าใช้งานของระบบโดเมนเนม (DNS Health)

๒.๓) ด้านช่องโหว่ที่ยังไม่ได้การอัปเดตและติดตั้งแพตช์ (Patching Cadence)

๒.๔) ด้านความปลอดภัยของเครื่องคอมพิวเตอร์ (Endpoint Security)

๒.๕) ด้านประวัติและความน่าเชื่อถือของไอพีแอดเดรส (IP Reputation)

๒.๖) ด้านความปลอดภัยของแอปพลิเคชั่น (Application Security)

๒.๗) ด้านการตกเป็นเป้าหมายของกลุ่มแฮกเกอร์ (Hacker Chatter)

๒.๘) ด้านการหลอกลวงเชิงจิตวิทยา (Social Engineering)

๒.๙) ด้านการรั่วไหลของข้อมูล (Information Leak)

๓) จัดให้มีบริการเฝ้าระวังและติดตามความเสี่ยงทรัพย์สินดิจิทัลของกรมการพัฒนาชุมชนที่มีการเปิดเผยต่อสาธารณะผ่านโดเมนของกรมการพัฒนาชุมชน (cdd.go.th) ตลอด ๒๔ ชั่วโมง

๔) หากตรวจพบความเสี่ยงซึ่งเกี่ยวข้องกับทรัพย์สินดิจิทัลของกรมการพัฒนาชุมชน ผู้ยื่นข้อเสนอต้องดำเนินการตอบสนองต่อความเสี่ยงที่ตรวจพบให้เป็นไปตามที่กรมการพัฒนาชุมชนกำหนดเป็นอย่างน้อย ดังนี้

๔.๑) ทำการแจ้งเตือนความเสี่ยงที่ตรวจพบพร้อมรายละเอียด

๔.๒) ให้คำปรึกษาแนะนำรวมถึงวิธีการจัดการความเสี่ยงที่ตรวจพบ

๔.๓) ดำเนินการจัดส่งข้อมูลให้กับทางกรมการพัฒนาชุมชนผ่านช่องทาง Email หรือ Line เป็นอย่างน้อย

/๕) จัดให้มี...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๕) จัดให้มีบริการสรุปผลการประเมินความมั่นคงปลอดภัยทางไซเบอร์จากมุมมองภายนอกผ่านระบบโดเมนให้กับทางกรมการพัฒนาชุมชน อย่างน้อย ๓ เดือน ๑ ครั้ง โดยแต่ละครั้งมีรายละเอียด ดังนี้

๕.๑) จัดทำรายงานสรุปผลการประเมินและสถานะความปลอดภัยทางไซเบอร์ในรูปแบบของเอกสาร PDF หรือตามที่กรมการพัฒนาชุมชนกำหนด

๕.๒) จัดทำแผนการปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่จำเป็นตามลำดับความสำคัญก่อนหลัง ในรูปแบบของเอกสาร PDF หรือตามที่กรมการพัฒนาชุมชนกำหนด

๕.๓) ดำเนินการจัดส่งให้กับทางกรมการพัฒนาชุมชนผ่านช่องทาง Email หรือ Line เป็นอย่างน้อย

๕.๔) จัดการประชุมเพื่อสรุปผลการดำเนินงาน

๔.๓.๑๐ ผู้ยื่นข้อเสนอต้องจัดให้มีบริการประเมินความมั่นคงปลอดภัยทางไซเบอร์จากมุมมองภายในด้วยการทดสอบเจาะระบบ (Penetration Testing) โดยมีรายละเอียดอย่างน้อย ดังนี้

๑) ตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญจากภายในระบบเครือข่ายคอมพิวเตอร์ของกรมการพัฒนาชุมชน ด้วยการทดสอบเจาะระบบแบบ Grey-Box เป็นจำนวนไม่น้อยกว่า ๑๐ ระบบ

๒) จัดให้มีบริการการทดสอบเจาะระบบและตรวจสอบช่องโหว่โดยอ้างอิงมาตรฐานการกำหนดความเสี่ยง และพิจารณาช่องโหว่ที่พบในรอบ ๑๒ เดือนล่าสุด รวมทั้งใช้โปรแกรมคอมพิวเตอร์ที่มีลิขสิทธิ์ซึ่งเป็นที่ยอมรับได้ในระดับสากลตั้งแต่ปี ๒๐๒๔ ขึ้นไปเป็นอย่างน้อย ดังนี้

๒.๑) Open-Source Security Testing Methodology Manual (“OSSTMM”)

๒.๒) NIST Special Publication ๘๐๐-๑๑๕

๒.๓) NIST Special Publication ๘๐๐-๓๐

๒.๔) OWASP Top Ten

๒.๕) Penetration Testing Execution Standard

๒.๖) Penetration Testing Framework

๒.๗) CVSS Score เวอร์ชั่นล่าสุด

๓) จัดให้มีบริการสรุปผลการประเมินความมั่นคงปลอดภัยทางไซเบอร์จากมุมมองภายในด้วยการทดสอบเจาะระบบ เป็นจำนวน ๒ ครั้ง โดยแต่ละครั้งมีรายละเอียด ดังนี้

๓.๑) จัดทำรายงานครั้งที่ ๑ (Recommendation Report) หลังจากตรวจสอบช่องโหว่ของระบบ (Penetration Testing) ตามขอบเขตของงาน ซึ่งประกอบด้วยรายละเอียดช่องโหว่ที่พบและคำแนะนำในการแก้ไขปัญหาช่องโหว่ดังกล่าว เพื่อให้กรมการพัฒนาชุมชนสามารถนำข้อมูลที่ได้รับไปใช้แก้ไขปัญหาช่องโหว่ของระบบได้

๓.๒) จัดทำรายงานครั้งที่ ๒ (Final Report) หลังจากการตรวจสอบช่องโหว่ที่กรมการพัฒนาชุมชนแก้ไขช่องโหว่ตามรายงานครั้งที่ ๑ เรียบร้อยแล้ว (Re-Test) โดยมีหัวข้อรายงานสรุปผลการตรวจสอบ สำหรับผู้บริหาร (Executive Summary) และ หัวข้อรายงานผลการทดสอบอย่างละเอียดโดยมีเนื้อหา ครอบคลุมถึง วิธีการทดสอบ ผลการทดสอบ คำแนะนำในการแก้ไขปัญหาที่ค้นพบเพื่อปรับปรุงความมั่นคงปลอดภัย

๔) จัดให้มีการประชุมเพื่อสรุปผลการดำเนินงานบริการประเมินความมั่นคงปลอดภัยทางไซเบอร์จากมุมมองภายในด้วยการทดสอบเจาะระบบทั้ง ๒ ครั้ง

/๔.๓.๑๑ ผู้ยื่น...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๔.๓.๑๑ ผู้ยื่นข้อเสนอต้องจัดให้มีบริการระบบแสดงผล (Dashboard & Visualization) ที่สามารถเข้าถึงได้ผ่านระบบเครือข่าย (Web-based) อย่างปลอดภัย โดยมีคุณสมบัติเป็นอย่างน้อย ดังนี้

๑) แสดงผลข้อมูลในรูปแบบของแผนภูมิและตารางได้เป็นอย่างน้อย

๒) แสดงภาพรวมสถานะความปลอดภัยได้

๓) จัดลำดับความสำคัญของเหตุการณ์ได้

๔) แสดงรายละเอียด (Drill Down) เพื่อตรวจสอบเชิงลึกได้

๕) แสดงสถานะการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ของอุปกรณ์และระบบได้

๖) สามารถปรับแต่ง (Customization) หน้าจอ เพื่อให้สอดคล้องกับความต้องการของกรมการพัฒนาชุมชนได้อย่างน้อย ดังนี้

๖.๑) รูปแบบการแสดงผลข้อมูล เช่น กราฟแผนภูมิ, กราฟวงกลม, กราฟตาราง, กราฟเส้น เป็นต้น

๖.๒) การแสดงภาพรวมสถานะความปลอดภัย

๖.๓) การจัดลำดับความสำคัญของเหตุการณ์

๖.๔) การแสดงรายละเอียด (Drill Down) เพื่อตรวจสอบเชิงลึกได้

๖.๕) แสดงสถานะการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ของอุปกรณ์และระบบได้

๔.๓.๑๒ ผู้ยื่นข้อเสนอต้องจัดให้มีบริการให้คำปรึกษา แนะนำ และดำเนินการแก้ไขปัญหาของระบบฯ หรือระบบที่เกี่ยวข้อง รวมถึงการสรุปสาเหตุ วิธีการแก้ไขปัญหา และแนวทางป้องกันในอนาคต ให้สอดคล้องกับการทำงานของเจ้าหน้าที่กรมการพัฒนาชุมชนตลอด ๒๔ ชั่วโมง

๔.๓.๑๓ ผู้ยื่นข้อเสนอต้องจัดทำรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ (Incident Report) ในกรณีมีเหตุการณ์ภัยคุกคามทางไซเบอร์เกิดขึ้น

๑) องค์ประกอบของรายงาน จะต้องมีหัวข้อและรายละเอียดของข้อมูลอย่างน้อย ดังนี้

๑.๑) ข้อมูลเหตุการณ์ภัยคุกคาม (Even Information)

๑.๒) ตัวบ่งชี้สำคัญที่เกี่ยวข้องในเหตุการณ์ (Incident Identification)

๑.๓) บทวิเคราะห์สรุปเรื่องราวภัยคุกคาม (Threat Analysis)

๑.๔) ข้อมูลรายละเอียดการตรวจสอบภัยคุกคาม (Incident Information)

๑.๕) คำแนะนำหรือแนวทางในการป้องกันหรือรับมือ (Recommendation)

๑.๖) หลักฐานที่ตรวจพบจากเหตุการณ์ภัยคุกคาม (Artifact)

๒) จัดทำรายงานให้อยู่ในรูปแบบของเอกสาร PDF

๓) ดำเนินการจัดส่งให้กับทางกรมการพัฒนาชุมชนผ่านช่องทาง Email ตาม SLA ที่ถูกกำหนดไว้ระหว่างผู้ยื่นข้อเสนอและกรมการพัฒนาชุมชน

๔.๓.๑๔ จัดให้มีบริการสรุปการบริหารการจัดการศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์แบบรายวัน โดยมีรายละเอียดอย่างน้อย ดังนี้

๑) รายงานบทสรุป มีรายละเอียดอย่างน้อย ดังนี้

๑.๑) จำนวนและภาพรวมการแจ้งเตือน (Alert Summary)

๑.๒) สรุปเหตุการณ์ภัยคุกคามทางไซเบอร์ (Incident Summary)

๑.๓) สรุปสถานะของงานที่ได้รับ (Service Request)

๒) รายงานสรุปสถานะอุปกรณ์หรือระบบต้นทาง มีรายละเอียด ดังนี้

๒.๑) สถานการณ์เชื่อมต่อ (Online / Offline)

๒.๒) IP Address / Hostname / Device Type

๒.๓) ปริมาณข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ที่มีการส่งออก

/๔.๓.๑๕ จัดให้มี...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๔.๓.๑๕ จัดให้มีบริการสรุปการบริหารการจัดการศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์แบบรายเดือน โดยมีรายละเอียดอย่างน้อย ดังนี้

๑) รายงานบทสรุป มีรายละเอียดอย่างน้อย ดังนี้

๑.๑) ระดับความรุนแรงและระดับความสำคัญ (Severity and Priority)

๑.๒) จำนวนและภาพรวมการแจ้งเตือน (Alert Summary)

๑.๓) สรุปเหตุการณ์ภัยคุกคามทางไซเบอร์ (Incident Summary)

๑.๔) สรุปสถานะของงานที่ได้รับ (Service Request)

๑.๕) สรุปทรัพยากรของอุปกรณ์เครือข่ายที่เกี่ยวข้อง (Infra Structure)

๒) รายงานสรุปภาพรวมการเฝ้าระวังภัยคุกคาม มีรายละเอียดอย่างน้อย ดังนี้

๒.๑) ปริมาณและลักษณะการใช้งานเครือข่าย (Traffic Statistic)

๒.๒) ภัยคุกคามทางไซเบอร์ที่อุปกรณ์หรือระบบรักษาความปลอดภัยตรวจจับและป้องกันได้

๒.๓) การใช้งานหรือบริการต่างๆ ภายในองค์กร (Usage)

๓) จัดทำรายงานให้อยู่ในรูปแบบของเอกสาร PDF หรือในรูปแบบที่กรมการพัฒนาชุมชนกำหนด

๔) ดำเนินการจัดส่งให้กับทางกรมการพัฒนาชุมชนผ่านช่องทาง Email

๕) รายงานข่าวสารภัยคุกคามทางด้านไซเบอร์ที่สำคัญหรือที่เกี่ยวข้องกับกรมการพัฒนาชุมชนทั้งทางตรงหรือทางอ้อม

๖) จัดการประชุมเพื่อสรุปผลการดำเนินงาน

๔.๓.๑๖ รูปแบบรายการข้อมูลในรายงาน (Data Fields) ตามข้อ ๔.๓.๑๔ และ ๔.๓.๑๕ ต้องสอดคล้องและครอบคลุมหัวข้อตามแบบฟอร์มมาตรฐานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หรือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) เพื่อให้หน่วยงานสามารถนำข้อมูลไปดำเนินการรายงานต่อหน่วยงานกำกับดูแลได้ทันทีตามระยะเวลาที่กฎหมายกำหนด

๔.๓.๑๗ ผู้ยื่นข้อเสนอต้องจัดให้มีทีมงานที่มีความเชี่ยวชาญในการบริหารจัดการศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์โดยแบ่งระดับความรับผิดชอบ ดังนี้

๑) ผู้จัดการโครงการ จำนวน ๑ คน มีวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีด้านคอมพิวเตอร์ หรือด้านที่เกี่ยวข้อง พร้อมแนบใบรับรองคุณวุฒิ มีประสบการณ์ทางด้านไซเบอร์ซีเคียวริตี้ไม่น้อยกว่า ๑๐ ปี และต้องได้รับประกาศนียบัตร CISSP หรือ CISM หรือ CSIE เป็นอย่างน้อย เพื่อทำหน้าที่วางแผน บริหาร ติดตาม ประเมินผลการดำเนินงานและปรับปรุงแก้ไขงานและปัญหาเฉพาะหน้าต่าง ๆ ให้เป็นไปตามแผนเพื่อให้โครงการนี้เสร็จตามเป้าหมายและระยะเวลาที่กำหนด โดยสามารถใช้งานได้อย่างมีประสิทธิภาพ

๒) ผู้จัดการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ จำนวน ๑ คน มีวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีด้านคอมพิวเตอร์ หรือด้านที่เกี่ยวข้อง พร้อมแนบใบรับรองคุณวุฒิ มีประสบการณ์ทางด้านไซเบอร์ซีเคียวริตี้ไม่น้อยกว่า ๕ ปี และต้องได้รับประกาศนียบัตร CISSP หรือ CISM หรือ CSAE และ ITIL เป็นอย่างน้อย เพื่อทำหน้าที่บริหารจัดการภาพรวมศูนย์ปฏิบัติการเฝ้าระวังภัยคุมคามทางไซเบอร์ (SOC) วางแผนกลยุทธ์ บริหารกำลังคน และควบคุมคุณภาพการปฏิบัติงานให้เป็นไปตามข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) เป็นผู้บัญชาการเหตุการณ์ (Incident Commander) ตัดสินใจสั่งการและบริหารจัดการสถานการณ์เมื่อเกิดภัยคุกคามระดับวิกฤต พิจารณาอนุมัติและทบทวนกฎการตรวจจับ (Detection Rules) และกระบวนการตอบสนองอัตโนมัติ (Playbooks) ให้มีประสิทธิภาพ เป็นจุดศูนย์กลางในการสื่อสาร ประสานงานกับเจ้าหน้าที่กรมการพัฒนาชุมชนที่เกี่ยวข้อง และรายงานสถานะความมั่นคงปลอดภัยพร้อมข้อเสนอแนะต่อผู้บริหารระดับสูง

/๓) ผู้เชี่ยวชาญ...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๓) ผู้เชี่ยวชาญด้านการตอบสนองต่อภัยคุกคามทางไซเบอร์ จำนวน ๑ คน มีวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีด้านคอมพิวเตอร์ หรือด้านที่เกี่ยวข้องพร้อมแนบใบรับรองคุณวุฒิ มีประสบการณ์ทางด้านไซเบอร์ซีเคียวริตี้ไม่น้อยกว่า ๓ ปี และต้องได้รับประกาศนียบัตร ECIH หรือ CySA+ เป็นอย่างน้อย เพื่อทำหน้าที่วิเคราะห์ตรวจสอบเหตุการณ์ภัยคุกคามเชิงลึก (Deep Analysis) และดำเนินการระงับเหตุ (Containment) เพื่อจำกัดความเสียหายทันทีที่ตรวจพบ สืบสวนหาสาเหตุที่แท้จริง (Root Cause Analysis) เก็บกู้พยานหลักฐานทางดิจิทัล (Forensics) และกำจัดภัยคุกคามออกจากระบบ ประสานงานกู้คืนระบบให้กลับสู่สภาพปกติ และจัดทำรายงานสรุปผลการตอบสนองต่อเหตุการณ์ (Incident Report) อย่างละเอียด ให้คำแนะนำและช่วยเหลือเชิงเทคนิคแก่เจ้าหน้าที่กรมการพัฒนาชุมชนเพื่อปิดช่องโหว่และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำเดิม (Remediation & Prevention)

๔) นักวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์ จำนวน ๔ คน มีวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีด้านคอมพิวเตอร์ หรือด้านที่เกี่ยวข้องพร้อมแนบใบรับรองคุณวุฒิ มีประสบการณ์ทางด้านไซเบอร์ซีเคียวริตี้ไม่น้อยกว่า ๒ ปี และต้องได้รับประกาศนียบัตร SAL1 หรือ ECSA หรือ SEC+ เป็นอย่างน้อยเพื่อทำหน้าที่เฝ้าระวังและตรวจสอบการแจ้งเตือนจากระบบ SIEM ตลอด ๒๔ ชั่วโมง เพื่อตรวจจับความผิดปกติแบบ Real-time วิเคราะห์และคัดกรองเหตุการณ์เบื้องต้น (Triage) เพื่อยืนยันว่าเป็นภัยคุกคามจริง และแยกแยะเหตุการณ์หลอก (False Positive) บันทึกข้อมูลรับแจ้งเหตุ (Ticketing) และดำเนินการแก้ไขปัญหาเบื้องต้นตามคู่มือปฏิบัติงานมาตรฐาน (SOP) ประสานงานและส่งต่อเหตุการณ์ (Escalation) ไปยังผู้เชี่ยวชาญระดับสูงเมื่อพบภัยคุกคามที่มีความซับซ้อนเกินขอบเขต

๕) นักทดสอบเจาะระบบ ระดับเชี่ยวชาญ จำนวน ๑ คน มีวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีด้านคอมพิวเตอร์ หรือด้านที่เกี่ยวข้องพร้อมแนบใบรับรองคุณวุฒิ มีประสบการณ์ทางด้านไซเบอร์ซีเคียวริตี้ไม่น้อยกว่า ๕ ปี และต้องได้รับประกาศนียบัตร CISSP, GXPN และ CRTM เป็นอย่างน้อยเพื่อทำหน้าที่วางแผนและดำเนินการทดสอบเจาะระบบเชิงลึก (Penetration Testing) ทั้งระดับ Network และ Application เพื่อค้นหาช่องโหว่ก่อนถูกโจมตีจริง จำลองเทคนิคการโจมตีขั้นสูง (Advanced Exploitation) ทั้งแบบ Manual และ Automated เพื่อประเมินความเสี่ยงและผลกระทบทางธุรกิจ จัดทำรายงานสรุปผลการเจาะระบบ วิเคราะห์สาเหตุ และประเมินระดับความรุนแรงของช่องโหว่ตามมาตรฐานสากล (เช่น CVSS) ให้คำปรึกษาเชิงลึกแก่เจ้าหน้าที่กรมการพัฒนาชุมชนในการแก้ไขช่องโหว่ (Remediation) และดำเนินการตรวจสอบซ้ำ (Retest) เพื่อยืนยันความปลอดภัย

๖) นักทดสอบเจาะระบบ ระดับชำนาญการ จำนวน ๓ คน มีวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรีด้านคอมพิวเตอร์ หรือด้านที่เกี่ยวข้อง มีประสบการณ์ทางด้านไซเบอร์ซีเคียวริตี้ไม่น้อยกว่า ๑ ปี และได้รับประกาศนียบัตร OSCP หรือ GPEN เป็นอย่างน้อย เพื่อทำหน้าที่ประเมินความเสี่ยงและทดสอบเจาะระบบตามแผนงาน ตรวจสอบยืนยันความถูกต้องของช่องโหว่ (Verify Findings) และคัดกรองผลลวง (False Positive) ออกจากรายงาน จัดทำรายงานผลการทดสอบทางเทคนิค ระบุรายละเอียดช่องโหว่ ระดับความรุนแรง และแนวทางการแก้ไขปัญหา ติดตามผลและดำเนินการทดสอบซ้ำ (Retest) เพื่อยืนยันความสมบูรณ์ของการแก้ไขช่องโหว่ตามรายงาน

๔.๔ ผู้ยื่นข้อเสนอต้องจัดให้มีบริการติดตั้งและส่งมอบระบบ Security Information and Event Management (SIEM) ให้กับกรมการพัฒนาชุมชนหลังจากจบสัญญาการว่าจ้างของโครงการ จำนวน ๑ ระบบ โดยมีรายละเอียด ดังนี้

๔.๔.๑ จัดให้มีบริการระบบ Security Information and Event Management (SIEM) ในรูปแบบติดตั้งใช้งานภายในหน่วยงาน (On-Premise) ให้กับทางกรมการพัฒนาชุมชน

/๔.๔.๒ จัดให้มี...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๔.๔.๒ จัดให้มีบริการเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์จัดเก็บข้อมูล ให้เพียงพอกับการใช้งานระบบระบบ Security Information and Event Management (SIEM) และดำเนินการติดตั้ง ณ ศูนย์ควบคุมระบบคอมพิวเตอร์ของกรมการพัฒนาชุมชน จำนวนไม่น้อยกว่า ๑ เครื่อง โดยมีรายละเอียดดังนี้

๑) มีหน่วยประมวลผลกลาง (CPU) แบบ ๑๐ แกนหลัก (๑๐ core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า ๒.๒ GHz จำนวนไม่น้อยกว่า ๑ หน่วย

๒) หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ ๖๔ bit มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันไม่น้อยกว่า ๑๓ MB

๓) มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR๔ หรือดีกว่า มีขนาดไม่น้อยกว่า ๑๖ GB

๔) สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID ๐, ๑, ๕

๕) มีหน่วยจัดเก็บข้อมูลชนิด SAS หรือ SATA ที่มีความเร็วรอบไม่น้อยกว่า ๑๐,๐๐๐ รอบต่อนาที ขนาดความจุไม่น้อยกว่า ๑ TB หรือ ชนิด Solid State Drive หรือดีกว่า ขนาดความจุไม่น้อยกว่า ๔๘๐ GB จำนวนไม่น้อยกว่า ๒ หน่วย

๖) มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๒ ช่อง

๗) มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย

๔.๔.๓ ระบบ Security Information and Event Management (SIEM) ต้องมีความสามารถอย่างน้อย ดังนี้

๑) มีความสามารถในการวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Log Data Analysis)

๒) มีความสามารถในการตรวจจับมัลแวร์ (Malware Detection)

๓) มีความสามารถในการตรวจจับช่องโหว่ (Vulnerability Detection)

๔) มีความสามารถในการเชื่อมต่อกับ Threat Intelligence Platform สำหรับดึงข้อมูลมาใช้ร่วมกับระบบ Security Information and Event Management (SIEM) เพื่อตรวจจับมัลแวร์ได้

๔.๔.๔ จัดให้มีบริการระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายที่รองรับการใช้งานที่เหมาะสม และดำเนินการติดตั้ง ให้สามารถทำงานได้อย่างมีประสิทธิภาพ

๔.๔.๕ บริการดูแล บำรุงรักษา เฝ้าระวัง และซ่อมแซมแก้ไขเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์จัดเก็บข้อมูล เป็นเวลาไม่น้อยกว่า ๒ ปี

๔.๔.๖ ผู้ยื่นข้อเสนอต้องจัดให้มีการถ่ายทอดองค์ความรู้การใช้งานเบื้องต้นสำหรับคณะทำงานและเจ้าหน้าที่ที่ดูแลรับผิดชอบระบบ Security Information and Event Management (SIEM) กรมการพัฒนาชุมชน

๔.๔.๗ ผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งในส่วนของซอฟต์แวร์ ฮาร์ดแวร์ และค่าลิขสิทธิ์ทั้งหมด

๔.๔.๘ เอกสาร คู่มือการใช้งาน ผังการทำงาน (Workflow) รายงานการตั้งค่าระบบ (Configuration) หรือโปรแกรมส่วนที่มีการพัฒนาเพิ่มเติม ปรับปรุง หรือดัดแปลง (Customization) ของระบบ Security Information and Event Management (SIEM) ตลอดจนข้อมูลต่างๆ ที่ผู้ยื่นข้อเสนอจัดทำขึ้นตามสัญญานี้ ให้ถือเป็นกรรมสิทธิ์และถือเป็นลิขสิทธิ์ของกรมการพัฒนาชุมชนหลังส่งมอบงาน

๔.๕ ผู้ยื่นข้อเสนอต้องจัดให้มีการถ่ายทอดองค์ความรู้ เทคโนโลยี และประสบการณ์ทางด้านไซเบอร์ซีเคียวริตี้ให้กับเจ้าหน้าที่ของกรมการพัฒนาชุมชน ดังนี้

/๔.๕.๑ ผู้ยื่น...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๔.๕.๑ ผู้ยื่นข้อเสนอต้องจัดให้มีการถ่ายทอดองค์ความรู้ด้านการตระหนักรู้ภัยคุกคามทางด้านไซเบอร์ (Cybersecurity Awareness) ให้กับบุคลากรของกรมการพัฒนาชุมชน โดยมีรายละเอียดอย่างน้อย ดังนี้

๑) ถ่ายทอดองค์ความรู้ด้านการตระหนักรู้ภัยคุกคามทางด้านไซเบอร์

๒) ถ่ายทอดองค์ความรู้อย่างน้อยปีละ ๑ ครั้ง โดยแต่ละครั้งมีระยะเวลาไม่น้อยกว่า ๓ ชั่วโมง

๓) รูปแบบการถ่ายทอดองค์ความรู้เป็นแบบ Hybrid

๔) หัวข้อในการถ่ายทอดองค์ความรู้อย่างน้อย ดังต่อไปนี้

๔.๑) ความหมายและความสำคัญของ Cybersecurity Awareness

๔.๒) ความหมายและวิธีการล่อลวงเชิงจิตวิทยา (Social Engineering)

๔.๓) การตั้งค่ารหัสผ่านสำหรับบัญชีผู้ใช้งานให้มีความปลอดภัย

๔.๔) การใช้งานอินเทอร์เน็ตให้มีความปลอดภัย

๔.๕) การรักษาความปลอดภัยให้กับข้อมูลขององค์กร

๔.๖) การตอบสนองต่อเหตุการณ์ภัยคุกคามทางด้านไซเบอร์เบื้องต้น

๔.๕.๒ ผู้ยื่นข้อเสนอต้องจัดให้มีการถ่ายทอดองค์ความรู้จากเหตุภัยคุกคามที่ตรวจพบจากศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC) ให้กับบุคลากรของกรมการพัฒนาชุมชน โดยมีรายละเอียดเป็นอย่างน้อย ดังนี้

๑) จัดให้มีการถ่ายทอดองค์ความรู้ อย่างน้อย ๓ เดือน ๑ ครั้ง โดยมีรายละเอียด ดังนี้

๑.๑) เนื้อหาการถ่ายทอดองค์ความรู้ มีเนื้อหาจากสถิติและรูปแบบการโจมตีที่ตรวจพบโดยศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ และรูปแบบภัยคุกคามที่มีแนวโน้มเกิดขึ้นในอนาคต

๑.๒) การถ่ายทอดองค์ความรู้เน้นไปที่การตอบสนองหรือรับมือต่อภัยคุกคามทางด้านไซเบอร์

๑.๓) ระยะเวลาในการถ่ายทอดองค์ความรู้ไม่น้อยกว่า ๓ ชั่วโมง

๑.๔) รูปแบบการถ่ายทอดองค์ความรู้เป็นแบบ On-site โดยใช้สถานที่การถ่ายทอดองค์ความรู้ของกรมการพัฒนาชุมชน

๒) จัดให้มีการถ่ายทอดองค์ความรู้ ที่มีเนื้อหาจากผลสรุปบริการทดสอบเจาะระบบและตรวจสอบช่องโหว่ ตามข้อ ๔.๓.๑๖ โดยมีรายละเอียดเป็นอย่างน้อย ดังนี้

๒.๑) เนื้อหาการถ่ายทอดองค์ความรู้ ที่มีเนื้อหาจากผลสรุปบริการทดสอบเจาะระบบและตรวจสอบช่องโหว่ ที่ตรวจพบตามรอบของการทดสอบ

๒.๒) การถ่ายทอดองค์ความรู้เน้นไปที่แนวทางการปิดช่องโหว่ (Remediation) และการรับมือกับภัยคุกคามทางด้านไซเบอร์ (Incident Response)

๒.๓) จัดการถ่ายทอดองค์ความรู้อย่างน้อยปีละ ๒ ครั้ง แต่ละครั้งมีระยะเวลาไม่น้อยกว่า ๓ ชั่วโมง

๒.๔) รูปแบบการจัดการถ่ายทอดองค์ความรู้เป็นแบบออนไซต์ (On-site) โดยใช้สถานที่การถ่ายทอดองค์ความรู้ของกรมการพัฒนาชุมชน

กรมการพัฒนาชุมชน

/๕. กำหนด...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๕. กำหนดเวลาส่งมอบพัสดุ

ผู้ยื่นข้อเสนอต้องดำเนินงานตามข้อ ๔ ขอบเขตของงาน และส่งมอบการให้บริการศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ ภายใน ๓๖๕ วัน นับถัดจากวันลงนามในสัญญา โดยกำหนดการส่งมอบงานออกเป็น ๓ งวด ซึ่งแต่ละงวดต้องส่งมอบงานในรูปแบบของเอกสาร (Hard Copy) และเอกสารอิเล็กทรอนิกส์ (Soft Copy) จำนวนอย่างละ ๒ ชุด ตามงวดงานให้แก่กรมการพัฒนาชุมชน ดังนี้

งวดที่	รายละเอียดการส่งมอบงาน	อ้างถึงข้อขอบเขตการดำเนินงาน
๑	รายงานผลการศึกษา วิเคราะห์รายละเอียดความต้องการ แผนการดำเนินงาน โครงสร้างและรายละเอียดของระบบศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC) แผนปฏิบัติการโครงการฯ แผนบริหารความเสี่ยง วิธีการ ขั้นตอน และรายละเอียดกิจกรรมอื่นๆ	๔.๑
	รายงานผลการศึกษา วิเคราะห์ข้อมูล ออกแบบ และจัดทำแผนโครงสร้างระบบศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC) ที่ครอบคลุมและเชื่อมโยงระบบต่างๆให้ถูกต้องเป็นปัจจุบัน	๔.๒
	รายงานศูนย์บริการปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operations Center : CSOC)	๔.๓
	เอกสารสรุปการถ่ายทอดองค์ความรู้	๔.๕.๒
๒	รายงานการให้บริการศูนย์บริการปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operations Center : CSOC)	๔.๓.๗ - ๔.๓.๑๕
	เอกสารสรุปการถ่ายทอดองค์ความรู้	๔.๕.๑ - ๔.๕.๒
๓	รายงานการให้บริการศูนย์บริการปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operations Center : CSOC)	๔.๓.๗ - ๔.๓.๑๕
	รายงานระบบ Security Information and Event Management (SIEM) ให้กับกรมการพัฒนาชุมชน	๔.๔
	เอกสารสรุปการถ่ายทอดองค์ความรู้	๔.๕.๒

๖. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลผู้ชนะการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ กรมการพัฒนาชุมชน ใช้หลักเกณฑ์ราคาประกอบเกณฑ์อื่นในการพิจารณาผู้ชนะการยื่นข้อเสนอ โดยจะพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักรวมเท่ากับร้อยละ ๑๐๐ โดยมีหลักเกณฑ์ ดังนี้

๖.๑ พิจารณาตามราคาที่ยื่นข้อเสนอ (Price) กำหนดน้ำหนักเท่ากับร้อยละ ๔๐ (๑๐๐ คะแนน)

๖.๒ พิจารณาตามข้อเสนอทางเทคนิคและข้อเสนออื่นๆ ที่เป็นประโยชน์ต่อทางราชการ กำหนดน้ำหนักเท่ากับร้อยละ ๖๐ (๑๐๐ คะแนน) โดยพิจารณาจากหลักเกณฑ์ ดังนี้

กรมการพัฒนาชุมชน

/๖.๒.๑ การเสนอ...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๖.๒.๑ การเสนองานมีความสอดคล้อง ชัดเจน และครบถ้วนตามขอบเขตการดำเนินงานและเนื้อหาที่กรมการพัฒนาชุมชนกำหนด รวมถึงมีการอธิบายรายการที่อ้างถึงตามเอกสารที่เสนออย่างชัดเจนและง่ายต่อการตรวจสอบ (ตามรายละเอียดคุณลักษณะเฉพาะฯ ข้อ ๔) ให้น้ำหนักร้อยละ ๒๐ ดังนี้

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน	วิธีการให้คะแนน
๑. เอกสาร/หลักฐานมีความสอดคล้องตามขอบเขตของงาน ครบถ้วน ชัดเจน และง่ายต่อการตรวจสอบ อย่างโดดเด่น	๑๐๐	เอกสารหลักฐานต่าง ๆ ที่ผู้ยื่นข้อเสนอยื่นมา ซึ่งจัดทำในรูปแบบ PDF File และต้องจัดทำในรูปแบบตารางเปรียบเทียบคุณสมบัติข้อกำหนดทางเทคนิคโดยจะพิจารณาจากความสอดคล้องกับขอบเขตของงานอย่างถูกต้อง ครบถ้วน ชัดเจน ง่ายต่อการตรวจสอบ และมีคุณลักษณะเฉพาะของพัสดุเป็นไปตามที่กำหนดไว้ในประกาศ	คณะกรรมการจะพิจารณาจากเอกสารและหลักฐานต่าง ๆ ที่ผู้ยื่นข้อเสนอได้เสนอมา โดยการให้คะแนนจะคิดจากผู้ยื่นข้อเสนอที่นำเสนองานได้ดีที่สุด เรียงลำดับลงมา
๒. เอกสาร/หลักฐานมีความสอดคล้องตามขอบเขตของงาน ครบถ้วน ชัดเจน และง่ายต่อการตรวจสอบ แต่ไม่โดดเด่น	๕๐		
๓. เอกสาร/หลักฐานไม่มีความสอดคล้องตามขอบเขตของงาน	๐		

๖.๒.๒ ประสบการณ์การทำงานและผลงานที่ผ่านมาของผู้ยื่นข้อเสนอที่เกี่ยวข้องกับงานที่จะจ้างในครั้งนี้ ซึ่งเป็นคู่สัญญาโดยตรงกับหน่วยงานราชการ หรือรัฐวิสาหกิจ หรือหน่วยงานเอกชนภายในประเทศไทย (ตามรายละเอียดคุณลักษณะเฉพาะฯ ข้อ ๓.๑๓) ให้น้ำหนักร้อยละ ๑๐ แบ่งเป็น

(๑) จำนวนสัญญา ให้น้ำหนักร้อยละ ๕ โดยมีเกณฑ์การให้คะแนน ดังนี้

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน	วิธีการให้คะแนน
๑. จำนวนสัญญาที่มีวงเงินไม่น้อยกว่าร้อยละ ๕๐ ของวงเงินงบประมาณหรือวงเงินที่ประมาณการที่จะจัดซื้อจัดจ้างในครั้งนั้น มากที่สุด อันดับที่ ๑	๑๐๐	เอกสารที่ผู้ยื่นข้อเสนอ ได้ยื่นเสนอมา จะต้องมีหนังสือรับรองผลงานและสำเนาสัญญาที่มีวงเงินเกินร้อยละ ๕๐ ของวงเงินงบประมาณหรือวงเงินที่ประมาณการในงานรับจ้างที่มีลักษณะเดียวกันกับงานที่ประกวดราคาจ้างด้วยวิธีการทางอิเล็กทรอนิกส์ครั้งนี้ที่ดำเนินการเสร็จเรียบร้อยแล้ว โดยจะพิจารณาเฉพาะจำนวนสัญญาที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐหรือเอกชนที่ผู้ว่าจ้างเชื่อถือกำหนด	คณะกรรมการจะพิจารณาเปรียบเทียบจากเอกสารที่ยื่นมาและการให้คะแนนคิดจากผู้ยื่นข้อเสนอที่นำเสนองานได้ดีที่สุดและครบถ้วนสมบูรณ์มากที่สุด เรียงลำดับลงมา
๒. จำนวนสัญญาที่มีวงเงินไม่น้อยกว่าร้อยละ ๕๐ ของวงเงินงบประมาณหรือวงเงินที่ประมาณการที่จะจัดซื้อจัดจ้างในครั้งนั้น มากที่สุด อันดับที่ ๒	๗๕		
๓. จำนวนสัญญาที่มีวงเงินไม่น้อยกว่าร้อยละ ๕๐ ของวงเงินงบประมาณหรือวงเงินที่ประมาณการที่จะจัดซื้อจัดจ้างในครั้งนั้น มากที่สุด อันดับที่ ๓	๕๐		
๔. จำนวนสัญญาที่มีวงเงินไม่น้อยกว่าร้อยละ ๕๐ ของวงเงินงบประมาณหรือวงเงินที่ประมาณการที่จะจัดซื้อจัดจ้างในครั้งนั้น มากที่สุด อันดับที่ ๔ ลงมา	๒๕		

/(๒) มูลค่า...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

(๒) มูลค่าของวงเงินสัญญา ให้น้ำหนักร้อยละ ๕ โดยมีเกณฑ์การให้คะแนน ดังนี้

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน	วิธีการให้คะแนน
๑. วงเงินสัญญารวม ของวงเงินงบประมาณหรือวงเงินที่ประมาณการที่จะจัดซื้อจัดจ้างในครั้งนั้น มากที่สุด อันดับที่ ๑	๑๐๐	เอกสารที่ผู้ยื่นข้อเสนอยื่นมาโดยจะต้องมีหนังสือรับรองผลงานและสำเนาสัญญาที่มีวงเงินเกินร้อยละ ๕๐ ของวงเงินงบประมาณหรือวงเงินที่ประมาณการที่จะจัดซื้อจัดจ้างในครั้งนั้น และเป็นวงเงินงบประมาณในงานรับจ้างที่มีลักษณะเดียวกันกับงานที่ประกวดราคาจ้างด้วยวิธีการทางอิเล็กทรอนิกส์ครั้งนี้ที่ดำเนินการเสร็จเรียบร้อยแล้ว โดยจะพิจารณาเฉพาะวงเงินสัญญาที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐหรือเอกชนที่ผู้ว่าจ้างเชื่อถือกำหนด กรณีที่เสนอมาหลายสัญญา โดยจะพิจารณาจากวงเงินสัญญารวมสูงสุด	คณะกรรมการจะพิจารณาเปรียบเทียบจากเอกสารที่ยื่นมาและการให้คะแนนคิดจากผู้ยื่นข้อเสนอที่นำเสนองานได้ดีที่สุดและครบถ้วนสมบูรณ์มากที่สุด เรียงลำดับลงมา
๒. วงเงินสัญญารวม ของวงเงินงบประมาณหรือวงเงินที่ประมาณการที่จะจัดซื้อจัดจ้างในครั้งนั้น มากที่สุด อันดับที่ ๒	๗๕		
๓. วงเงินสัญญารวม ของวงเงินงบประมาณหรือวงเงินที่ประมาณการที่จะจัดซื้อจัดจ้างในครั้งนั้น มากที่สุด อันดับที่ ๓	๕๐		
๔. วงเงินสัญญารวม ของวงเงินงบประมาณหรือวงเงินที่ประมาณการที่จะจัดซื้อจัดจ้างในครั้งนั้น มากที่สุด อันดับที่ ๔ ลงมา	๒๕		

๖.๒.๓ ข้อเสนองานบริการเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ เป็นไปตามที่กำหนดไว้ในขอบเขตการดำเนินงาน เพื่อทำหน้าที่เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ ตลอด ๒๔ ชั่วโมง (ตามรายละเอียดคุณลักษณะเฉพาะฯ ข้อ ๔.๓) ให้น้ำหนักร้อยละ ๒๕ ดังนี้

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน	วิธีการให้คะแนน
๑. มีรายละเอียดศูนย์ปฏิบัติการความปลอดภัยระบบเครือข่าย ที่ให้บริการเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ ถูกต้อง ครบถ้วน	๑๐๐	เอกสารหลักฐานที่แสดงถึงศูนย์ปฏิบัติการความปลอดภัยระบบเครือข่าย (Security Operations Center : SOC) ที่ผ่านมาตรฐาน ISO ๒๗๐๐๑ พร้อมให้บริการเฝ้าระวังภัยคุกคาม ตลอด ๒๔ ชั่วโมง รูปแบบและรายละเอียดการให้บริการ โดยการให้คะแนนจะคิดจากผู้ที่มีการเสนองานได้ดีที่สุด ความถูกต้องครบถ้วนสมบูรณ์ เรียงลำดับลงมา	คณะกรรมการจะพิจารณเปรียบเทียบจากเอกสารและหลักฐานต่าง ๆ ที่ผู้ยื่นข้อเสนอได้เสนอมา โดยการให้คะแนนจะคิดจากผู้ยื่นข้อเสนอที่นำเสนองานได้ดีที่สุดและความครบถ้วนสมบูรณ์มากที่สุด เรียงลำดับลงมา
๒. มีรายละเอียดศูนย์ปฏิบัติการความปลอดภัยระบบเครือข่าย ที่ให้บริการเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ แต่ยังขาดองค์ประกอบสำคัญบางรายการไม่ครอบคลุม	๕๐		
๓. ไม่มีรายละเอียดศูนย์ปฏิบัติการความปลอดภัยระบบเครือข่าย	๐		

/๖.๓.๔ ข้อเสนอ...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๖.๒.๔ ข้อเสนอการบริการหลังการขาย การสนับสนุนด้านเทคนิคภายหลังสิ้นสุดการรับประกัน (ตามรายละเอียดคุณลักษณะเฉพาะฯ ข้อ ๔.๔.๕ และ ข้อ ๑๐) ให้น้ำหนักร้อยละ ๒๕ ดังนี้

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน	วิธีการให้คะแนน
๑. ข้อเสนอการบริการดูแล การรับประกันอุปกรณ์และเอกสารหรือหนังสือรับรองที่บ่งบอกว่าได้รับการสนับสนุนทางเทคนิค ที่ชัดเจนเป็นรูปธรรมและมีประโยชน์กับทางราชการอย่างโดดเด่น	๑๐๐	เอกสารที่ผู้ยื่นข้อเสนอได้ยื่นมา โดยจะพิจารณาจากเอกสารที่บ่งบอกว่ามีความรอบรู้และเชี่ยวชาญในผลิตภัณฑ์ หนังสือรับรองการให้บริการหลังการขายหรือบริการบำรุงรักษา การสนับสนุนด้านเทคนิคจากเจ้าของผลิตภัณฑ์หรือสาขาของบริษัทเจ้าของผลิตภัณฑ์ที่อยู่ในประเทศไทย ระยะเวลา ๑ ปี ที่นำเสนอสอดคล้อง น่าสนใจ ตามขอบเขตของงานและวัตถุประสงค์มากที่สุด	คณะกรรมการจะพิจารณาเปรียบเทียบจากเอกสารและหลักฐานต่าง ๆ ที่ผู้ยื่นข้อเสนอได้เสนอมา โดยการให้คะแนน จะคิดจากผู้ยื่นข้อเสนอที่นำเสนองานได้ดีที่สุด เรียงลำดับลงมา
๒. ข้อเสนอการบริการดูแล การรับประกันอุปกรณ์และเอกสารหรือหนังสือรับรองที่บ่งบอกว่าได้รับการสนับสนุนทางเทคนิค ที่ชัดเจนเป็นรูปธรรมและมีประโยชน์กับทางราชการแต่ไม่โดดเด่น	๕๐		
๓. ไม่ข้อเสนอการบริการซ่อมบำรุงรักษาระบบและอุปกรณ์ตามที่กำหนดไว้	๐		

๖.๒.๕ ความเหมาะสมและการวางแผนในการดำเนินงานตามขอบเขตการดำเนินงานที่กำหนดไว้ ซึ่งเชื่อได้ว่าสามารถดำเนินงานได้ตรงตามวัตถุประสงค์โครงการ และแผนบริหารความเสี่ยงในการบริหารโครงการ (ตามรายละเอียดคุณลักษณะเฉพาะฯ ข้อ ๔.๑) ให้น้ำหนักร้อยละ ๑๐ ดังนี้

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน	วิธีการให้คะแนน
๑. มีการจัดทำแผนการดำเนินงานที่มีความละเอียด ครบถ้วน ชัดเจน สามารถดำเนินการได้จริง	๑๐๐	เอกสารหลักฐานที่ผู้ยื่นข้อเสนอยื่นมา โดยจะพิจารณาจากการนำขอบเขตของงานที่กำหนดไว้มาจัดทำแผนและวิธีการในการดำเนินงานที่สอดคล้องกับระยะเวลาดำเนินงานโครงการได้ชัดเจน เข้าใจง่าย และเป็นรูปธรรมมากที่สุด	คณะกรรมการจะพิจารณาจากเอกสารและหลักฐานต่าง ๆ ที่ผู้ยื่นข้อเสนอ ได้เสนอมา โดยการให้คะแนน จะคิดจากผู้ยื่นข้อเสนอที่นำเสนองานได้ดีที่สุด เรียงลำดับลงมา
๒. มีการจัดทำแผนการดำเนินงาน แต่ไม่ละเอียด หรือไม่ครบถ้วน ไม่ชัดเจน	๕๐		
๓. ไม่มีการจัดทำแผนการดำเนินงาน	๐		

/๖.๓.๖ โครงสร้าง...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๖.๒.๖ โครงสร้างการบริหารโครงการ ความพร้อมด้านบุคลากร และคุณสมบัติของบุคลากรที่ใช้ในการดำเนินงานมีความเหมาะสม รวมถึงมีทักษะความชำนาญและประสบการณ์การทำงานเกี่ยวข้องกับงานจ้างในครั้งนี้ (ตามรายละเอียดคุณลักษณะเฉพาะฯ ข้อ ๔.๓.๑๗) ให้น้ำหนักร้อยละ ๑๐ ดังนี้

เกณฑ์การพิจารณา	คะแนน	วิธีการประเมิน	วิธีการให้คะแนน
๑. มีเอกสารหรือหลักฐานด้านโครงสร้างการบริหารโครงการและคุณสมบัติของบุคลากรที่แสดงถึงความพร้อมด้านบุคคลากรตามขอบเขตของงาน อย่างโดดเด่น	๑๐๐	เอกสารที่ผู้ยื่นข้อเสนอได้ยื่นเสนอมา โดยจะพิจารณาจากโครงสร้างทีมงาน จำนวนบุคลากร และจำนวนใบรับรองความรู้ความสามารถของบุคลากร ประสบการณ์การทำงานตามระยะเวลาการทำงาน ที่มีลักษณะงานสอดคล้องหรือใกล้เคียงกับลักษณะงานจ้างในครั้งนี้ และวัตถุประสงค์ของโครงการมากที่สุด	คณะกรรมการจะพิจารณาเปรียบเทียบจากเอกสารและหลักฐานต่าง ๆ ที่ผู้ยื่นข้อเสนอ ได้เสนอมา โดยการให้คะแนนจะคิดจากผู้ยื่นข้อเสนอที่นำเสนองานได้ดีที่สุดและความครบถ้วนสมบูรณ์มากที่สุด เรียงลำดับลงมา
๒. มีเอกสารหรือหลักฐานด้านโครงสร้างการบริหารโครงการและคุณสมบัติของบุคลากรที่แสดงถึงความพร้อมด้านบุคคลากรตามขอบเขตของงาน แต่ไม่โดดเด่น	๕๐		
๓. ไม่มีเอกสารหรือหลักฐานด้านโครงสร้างการบริหารโครงการและคุณสมบัติของบุคลากรที่แสดงถึงความพร้อมด้านบุคคลากรตามขอบเขตของงาน	๐		

๗. วงเงินงบประมาณ

งบประมาณที่ใช้ในการดำเนินงานโครงการเพิ่มประสิทธิภาพการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และการเฝ้าระวังภัยคุกคาม (CDDSOC) ภายในงบประมาณ ๙,๘๕๐,๐๐๐ บาท (เก้าล้านแปดแสนห้าหมื่นบาทถ้วน) ซึ่งเป็นราคาที่รวมค่าอุปกรณ์หรือระบบงานทุกรายการ ค่าติดตั้ง ค่าดำเนินการ และภาษีมูลค่าเพิ่ม ตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว

๘. งวดงานและการจ่ายเงิน

ในการจัดจ้างครั้งนี้ กำหนดระยะเวลา ๓๖๕ วัน กรมการพัฒนาชุมชนกำหนดจ่ายเงินค่าจ้างตามสัญญา เมื่อผู้ยื่นข้อเสนอปฏิบัติตามข้อตกลงในสัญญาครบถ้วน พร้อมจัดส่งมอบเอกสารการส่งมอบงานให้ถูกต้องครบถ้วนตามสัญญา และคณะกรรมการตรวจรับพัสดุ ได้พิจารณาตรวจรับเป็นที่เรียบร้อยแล้ว โดยแบ่งการเบิกจ่ายงบประมาณตามงวด ดังนี้

งวดที่ ๑ กำหนดชำระเป็นเงิน ร้อยละ ๖๐ ของวงเงินตามสัญญา ภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา เมื่อผู้ยื่นข้อเสนอได้ดำเนินการแล้วเสร็จและส่งมอบงานตามเงื่อนไข ตามรายละเอียดคุณลักษณะเฉพาะข้อ ๔.๑ - ๔.๓ และ ๔.๕.๒

งวดที่ ๒ กำหนดชำระเป็นเงิน ร้อยละ ๓๐ ของวงเงินตามสัญญา ภายใน ๒๔๐ วัน นับถัดจากวันลงนามในสัญญา เมื่อผู้ยื่นข้อเสนอได้ดำเนินการแล้วเสร็จและส่งมอบงานตามเงื่อนไข ตามรายละเอียดคุณลักษณะเฉพาะข้อ ๔.๓.๗ - ๔.๓.๑๕ และ ๔.๕.๑ - ๔.๕.๒

งวดที่ ๓ (งวดสุดท้าย) กำหนดชำระเป็นเงิน ร้อยละ ๑๐ ของวงเงินตามสัญญา ภายใน ๓๖๕ วัน นับถัดจากวันลงนามจากวันลงนามในสัญญา เมื่อผู้ยื่นข้อเสนอได้ดำเนินการแล้วเสร็จและส่งมอบงานตามเงื่อนไข ตามรายละเอียดคุณลักษณะเฉพาะข้อ ๔.๓.๗ - ๔.๓.๑๕, ๔.๔ และ ๔.๕.๒

/๙. อัตรา...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๙. อัตราค่าปรับ

ในกรณีที่ผู้ยื่นข้อเสนอไม่สามารถให้บริการศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Operations Center : CSOC) ตามเงื่อนไขที่กำหนดไว้ในเอกสารนี้ ผู้ยื่นข้อเสนอต้องยินยอมให้กรมการพัฒนาชุมชนปรับเป็นรายวันในอัตราร้อยละ ๐.๑๐ ของมูลค่าของสัญญาทั้งหมด และรับผิดชอบค่าเสียหายต่าง ๆ ของกรมการพัฒนาชุมชนที่เกิดขึ้น ในกรณีที่ไม่สามารถให้บริการบำรุงรักษาได้ตามข้อกำหนด จนถึงวันที่ผู้ยื่นข้อเสนอสามารถให้บริการได้ตามข้อกำหนด

๑๐. การกำหนดระยะเวลารับประกันความชำรุดบกพร่อง

๑๐.๑ ผู้ยื่นข้อเสนอจะต้องรับประกันความชำรุดบกพร่องหรือเสียหายของงาน โดยตรวจเช็คระบบงานที่เกี่ยวข้องทั้งหมด ๓ เดือนต่อครั้ง เพื่อให้อยู่ในสภาพที่ใช้งานได้ดีดังเดิมตลอดอายุสัญญา และระยะเวลารับประกันผลงานอย่างน้อย ๑ ปี ซึ่งระยะเวลาที่รับประกันจะเริ่มนับจากวันที่คณะกรรมการตรวจรับพัสดุได้รับมอบงานและตรวจรับเรียบร้อยแล้วตามเงื่อนไขสัญญา

๑๐.๒ การรับประกันความชำรุดบกพร่องของงาน หรือความเสียหายของงาน ได้แก่ การบำรุงรักษา การให้บริการแก้ไข การสนับสนุนด้านเทคนิค ณ สถานที่ติดตั้งระบบงาน (On site) หรือโปรแกรมควบคุมระยะไกลให้แล้วเสร็จโดยเร็วที่สุดแบบไม่มีเงื่อนไข และไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้นตลอดระยะเวลาการรับประกัน

๑๐.๓ กรมการพัฒนาชุมชนจะต้องสามารถแจ้งเหตุชำรุดบกพร่อง หรือความขัดข้องของระบบงาน หรือติดต่อเพื่อปรึกษาทางด้านเทคนิค ได้ตลอด ๒๔ ชั่วโมง ตั้งแต่วันจันทร์ถึงวันอาทิตย์ ผ่านทางโทรศัพท์ อีเมล และแอปพลิเคชันไลน์ ทั้งนี้ ให้เป็นไปตามข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่กำหนดไว้

๑๑. การยื่นเอกสารเสนอราคา

ผู้ยื่นข้อเสนอต้องมีคุณสมบัติครบถ้วนตามข้อ ๓ และจัดทำข้อเสนอทางเทคนิค ซึ่งต้องดำเนินงานดังนี้

๑๑.๑ การยื่นเอกสารเสนอราคา ผู้ยื่นข้อเสนอต้องทำตารางเปรียบเทียบรายละเอียดข้อกำหนดโครงการเพิ่มประสิทธิภาพการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และการเฝ้าระวังภัยคุกคาม ที่เสนอเป็นรายข้อ ตั้งแต่ข้อ ๓ คุณสมบัติของผู้ยื่นข้อเสนอ ถึงข้อสุดท้าย รวมถึงภาคผนวก โดยใช้ตัวอย่างแบบฟอร์มการเปรียบเทียบตามตารางที่ ๑ ในกรณีที่ต้องมีการอ้างอิงถึงข้อความอื่นในเอกสารที่เสนอมา ผู้ยื่นข้อเสนอจะต้องระบุให้ชัดเจน พร้อมทั้งให้หมายเหตุหรือขีดเส้นใต้ หรือระบายสี พร้อมเขียนข้อกำกับไว้ให้ตรงกัน เพื่อให้ง่ายต่อการตรวจสอบกับเอกสารเปรียบเทียบ ซึ่งคณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ถือเป็นสาระสำคัญในการพิจารณาการประกวดราคา

ตารางที่ ๑ ตารางเปรียบเทียบคุณสมบัติข้อกำหนดทางเทคนิค

อ้างถึงข้อ	ข้อกำหนดที่ต้องการ	ข้อกำหนดที่นำเสนอ	เปรียบเทียบ	เอกสารอ้างอิง
ระบุหัวข้อให้ตรงกับหัวข้อที่ระบุในรายละเอียดคุณลักษณะเฉพาะของพัสดุ	ให้คัดลอกคุณสมบัติขอบเขตการดำเนินงานคุณลักษณะเฉพาะที่ทางราชการกำหนด	ให้ระบุคุณสมบัติขอบเขตการดำเนินงานคุณลักษณะเฉพาะของพัสดุที่ผู้ยื่นข้อเสนอ	ให้ระบุตรงตามข้อกำหนด หรือดีกว่าข้อกำหนด	ให้ระบุหรืออ้างถึงเอกสารในข้อเสนอที่อ้างอิง

๑๑.๒ ผู้ยื่นข้อเสนอต้องส่งแคตตาล็อก หรือรายละเอียดคุณลักษณะเฉพาะของพัสดุทุกรายการที่เสนอเพื่อใช้ประกอบการพิจารณา โดยกรมการพัฒนาชุมชน จะเก็บไว้เป็นเอกสารของทางราชการ ทั้งนี้ เอกสารที่ยื่นเสนอมาหากเป็นสำเนารูปถ่ายจะต้องรับรองสำเนาถูกต้องโดยผู้มีอำนาจทำนิติกรรมแทนนิติบุคคล

/๑๑.๓ ผู้ยื่น...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๑๑.๓ ผู้ยื่นข้อเสนอต้องศึกษา/ตรวจดูและทำความเข้าใจขอบเขตการดำเนินงาน รายละเอียดคุณลักษณะเฉพาะ เงื่อนไขและข้อกำหนดทั้งหมดอย่างละเอียดถี่ถ้วน และไม่ว่ากรณีใด ๆ ผู้ยื่นข้อเสนอจะยกขึ้นมาเป็นข้ออ้างโดยอาศัยเหตุจากการละเลยไม่ทำความเข้าใจในเอกสารดังกล่าว หรืออ้างความสำคัญผิดในความหมายของข้อมูลความในขอบเขตการดำเนินงานและข้อกำหนดนั้นไม่ได้

๑๑.๔ การยื่นเสนอราคาในครั้งนี้ กรมการพัฒนาชุมชน ทรงไว้ซึ่งสิทธิที่จะพิจารณาว่า ผู้ยื่นข้อเสนอที่มีข้อเสนอถูกต้องตรงตามความต้องการที่ระบุไว้ในเอกสารขอบเขตการดำเนินงานและข้อกำหนด โดยคณะกรรมการฯ สามารถยกเลิกการเสนอราคา โดยผู้ยื่นข้อเสนอยินยอมที่จะไม่ร้องเรียนและเรียกร้องค่าเสียหายใด ๆ กับกรมการพัฒนาชุมชน

๑๒. เงื่อนไขการติดตั้งและข้อกำหนดอื่น ๆ

๑๒.๑ ผู้ยื่นข้อเสนอต้องทำการศึกษาระบบเครือข่ายคอมพิวเตอร์ของกรมการพัฒนาชุมชนที่มีอยู่เดิมและจัดทำแผนการติดตั้งระบบงานและอุปกรณ์ในโครงการฯ ให้กรมการพัฒนาชุมชน พิจารณาก่อนเข้าดำเนินการติดตั้ง และอุปกรณ์ที่ผู้ยื่นข้อเสนอนำเสนอต้องสามารถใช้งานร่วมกับระบบเครือข่ายคอมพิวเตอร์ของกรมการพัฒนาชุมชนได้เป็นอย่างดี หากมีค่าใช้จ่ายใด ๆ เกิดขึ้นเพิ่มเติมในภายหลัง เพื่อทำให้ระบบทำงานได้เหมือนเดิม ผู้ยื่นข้อเสนอต้องเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมด

๑๒.๒ การติดตั้งระบบงานและอุปกรณ์คอมพิวเตอร์ ผู้ยื่นข้อเสนอต้องจัดหาอุปกรณ์อื่น ๆ ที่จำเป็นในการดำเนินงานนี้จนแล้วเสร็จ และส่งมอบงานตามโครงการ หากในระหว่างการติดตั้งต้องจัดหาอุปกรณ์ใดเพิ่มเติม เพื่อให้ระบบทำงานร่วมกันได้ ผู้ยื่นข้อเสนอต้องเป็นผู้จัดหาและรับผิดชอบค่าใช้จ่ายทั้งหมด

๑๒.๓ อุปกรณ์ทุกรายการที่เสนอ จะต้องรับประกันความชำรุดบกพร่องหรือเสียหาย อันเนื่องมาจากตัวอุปกรณ์เอง ตลอดระยะเวลาดำเนินโครงการฯ โดยไม่มีค่าใช้จ่ายใด ๆ ทั้งสิ้น

๑๒.๔ กรมการพัฒนาชุมชน ทรงไว้ซึ่งสิทธิในการปรับปรุงรูปแบบ แผนการดำเนินงานและแผนปฏิบัติการโครงการ รวมทั้งปรับเปลี่ยนแผนงานให้สอดคล้องกับสถานการณ์ และผู้ยื่นข้อเสนอพร้อมแก้ไข ตามที่กรมการพัฒนาชุมชน เห็นสมควร เพื่อความเหมาะสมอันเป็นประโยชน์แก่ทางราชการ

๑๓. สถานที่ดำเนินการ

ศูนย์ควบคุมระบบคอมพิวเตอร์ (Data Center) ชั้น ๕ กรมการพัฒนาชุมชน ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพมหานคร

๑๔. การขอสงวนสิทธิ์และข้อกำหนดอื่น ๆ

๑๔.๑ กรมการพัฒนาชุมชน ขอสงวนสิทธิ์ในการพิจารณาผู้ชนะการเสนอราคาตามหลักเกณฑ์ราคาประกอบเกณฑ์อื่น เพื่อประโยชน์สูงสุดของราชการ

๑๔.๒ กรมการพัฒนาชุมชน ขอสงวนสิทธิ์ในการตรวจสอบและพิจารณาคัดเลือกผู้ยื่นข้อเสนอเฉพาะผู้ที่ผ่านคุณสมบัติเบื้องต้นในการจัดซื้อจัดจ้างของกรมการพัฒนาชุมชน

๑๔.๓ ผู้ยื่นข้อเสนอต้องควบคุมดูแลและรับผิดชอบบุคลากรของผู้ยื่นข้อเสนอ ให้ปฏิบัติตามกฎระเบียบ ประกาศ หรือข้อกำหนดของกรมการพัฒนาชุมชน

๑๔.๔ ผู้ยื่นข้อเสนอต้องเก็บรักษาความลับของข้อมูลที่เกี่ยวข้องในการปฏิบัติงานของกรมการพัฒนาชุมชน โดยจัดทำเป็นข้อตกลงการประมวลผลข้อมูล (Data Processing Agreement : DPA) ซึ่งห้ามมิให้ผู้ยื่นข้อเสนอนำข้อมูลไปเผยแพร่หรือดำเนินการใดเกี่ยวกับข้อมูล โดยมิได้รับความยินยอมจากกรมการพัฒนาชุมชน หากกรมการพัฒนาชุมชน พบว่ามีการกระทำดังกล่าว และมีความเสียหายที่เกิดขึ้นจากการรั่วไหลของข้อมูล คู่สัญญาจะต้องรับผิดชอบในความเสียหายที่เกิดขึ้น จากการดำเนินงานของคู่สัญญาทุกกรณี

๑๔.๕ ข้อตกลงนี้ให้ถือเป็นส่วนหนึ่งของสัญญา อันเป็นเงื่อนไขที่กรมการพัฒนาชุมชน บอกเลิกสัญญาเรียกค่าเสียหาย หรือปรับสินไหม รวมทั้งการดำเนินคดีทั้งในทางแพ่งและอาญาทุกประเภท

/๑๕. หน่วยงาน...

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....

๑๕. หน่วยงานที่รับผิดชอบ

ศูนย์สารสนเทศเพื่อการพัฒนาชุมชน กรมการพัฒนาชุมชน

๑๖. สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติม

เพื่อขอทราบข้อมูลเพิ่มเติม

กลุ่มงานพัสดุ กองคลัง กรมการพัฒนาชุมชน

ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ อาคารรัฐประศาสนภักดี ชั้น ๕

ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

โทรศัพท์ ๐-๒๑๔๑-๖๓๔๒, ๐-๒๑๔๑-๖๒๙๕, ๐-๒๑๔๑-๖๒๘๓

โทรสาร ๐-๒๑๔๓-๘๙๒๗

กรมการพัฒนาชุมชน

ลงชื่อ..... ลงชื่อ..... ลงชื่อ.....