(ร่าง) คุณลักษณะเฉพาะ
โครงการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของ
ระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช.

โดย
สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ
(สำนักงาน ป.ป.ช.)

๑. โครงการ

โครงการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช.

๒. หลักการและเหตุผล

ปัจจุบันการโจมตีหรือภัยคุกคามทางไซเบอร์จากผู้ไม่ประสงค์ดีได้มีเพิ่มขึ้นอย่างรวดเร็วและมีการพัฒนาอย่างต่อเนื่องในรูปแบบต่าง ๆ ที่มีความทันสมัยมากขึ้น และพบเหตุการณ์โจมตีเกิดขึ้นมากมายตลอดเวลา สำนักงาน ป.ป.ช. ได้ตระหนักถึงความสำคัญในการยกระดับเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ และเพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อธำรงข้อมูลสารสนเทศไว้ซึ่งคุณสมบัติความมั่นคงปลอดภัยด้านสารสนเทศตามมาตรฐานสากล ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความครบถ้วนของข้อมูล (Integrity) และการที่ระบบสามารถพร้อมให้บริการอยู่เสมอ (Availability) จึงจำเป็นต้องมีมาตรการหรือการดำเนินการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกหน่วยงาน หากเกิดขึ้นจะส่งผลกระทบต่อข้อมูลสารสนเทศที่สำคัญ และข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมไว้ตามอำนาจหน้าที่ขององค์กร

จากเหตุผลที่กล่าวข้างต้นทำให้สำนักงาน ป.ป.ช. มีความประสงค์จะดำเนินโครงการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช. เพื่อจัดจ้างผู้ที่มีความรู้ความเชี่ยวชาญในการตรวจสอบช่องโหว่ของระบบเทคโนโลยี เพื่อเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ รวมทั้งให้ความรู้เพื่อเสริมสร้างศักยภาพการปฏิบัติงานด้านเทคโนโลยีสารสนเทศสำหรับเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ และสร้างความตระหนักรู้ให้เจ้าหน้าที่ ป.ป.ช. ในการใช้งานเทคโนโลยีสารสนเทศเพื่อการปฏิบัติงานอย่างถูกต้องตามนโยบาย ระเบียบและข้อกำหนดต่าง ๆ ที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อไป

๓. วัตถุประสงค์

๓.๑ เพื่อยกระดับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓.๒ เพื่อตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช.

๓.๓ เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์จากผู้ไม่ประสงค์ดีซึ่งได้มีเพิ่มขึ้นอย่างรวดเร็วและมีการพัฒนาอย่างต่อเนื่องในรูปแบบต่าง ๆ ต่อระบบเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ช.

๓.๔ เพื่อเพิ่มประสิทธิภาพการบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ป.ป.ช. ธำรงไว้ซึ่งคุณสมบัติความมั่นคงปลอดภัยตามมาตรฐานสากล ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความครบถ้วนของข้อมูล (Integrity) และการที่ระบบสามารถพร้อมให้บริการอยู่เสมอ (Availability)

๓.๕ เพื่อพัฒนาศักยภาพด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ หรือผู้ที่เกี่ยวข้อง

/๔. ประโยชน์...

๔. ประโยชน์ที่คาดว่าจะได้รับ

๔.๑ การบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ป.ป.ช. มีประสิทธิภาพเพิ่มขึ้นและสอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔.๒ ความเสี่ยงจากภัยคุกคามทางไซเบอร์จากผู้ไม่ประสงค์ดีที่อาจจะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ช. ลดลง

๔.๓ เจ้าหน้าที่สำนักงาน ป.ป.ช. มีศักยภาพ มีความตระหนักรู้ ความสามารถในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเพิ่มขึ้น

๕. กลุ่มเป้าหมาย

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ

๖. คุณสมบัติของผู้เสนอราคา

๖.๑ มีความสามารถตามกฎหมาย

๖.๑.๒ ไม่เป็นบุคคลล้มละลาย

๖.๑.๓ ไม่อยู่ระหว่างเลิกกิจการ

๖.๑.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๖.๑.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๖.๑.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๖.๑.๗ เป็นบุคคลธรรมดาหรือนิติบุคคล ผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๖.๑.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงาน ป.ป.ช. ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๖.๑.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

๖.๑.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติ ดังนี้

(๑) การกำหนดสัดส่วนในการเข้าร่วมค้าของคู่สัญญา

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

(๒) กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

/ สำหรับ...

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

(๓) การยื่นข้อเสนอของกิจการร่วมค้า

(๓.๑) กรณีที่ข้อตกลงฯ กำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

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

๖.๑.๑๑ ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) กรมบัญชีกลาง

๖.๑.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศ ซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏ ในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไป ก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ ๑ ปีปฏิทิน เว้นแต่กรณีนิติบุคคลที่จัดตั้งขึ้น ตามกฎหมายไทย หากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคล ยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนอนั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก ๑ ปี ได้

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งตามกฎหมายไทย ซึ่งยังไม่มีการแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอไม่ต่ำกว่า ๒ ล้านบาท

(๓) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๖๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(๔) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมี แต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(๔.๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทย

/ แจ้งเวียน...

แจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๖๐ วัน

(๔.๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๖๐ วัน)

(๕) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทยตามข้อ ๖.๑.๑๒ (๒) (๓) และข้อ ๖.๑.๑๒ (๔.๒) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตรา ตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) จนถึงวันเสนอราคา

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

(๖) กรณีตามข้อ (๑) - ข้อ (๕) ไม่ใช้บังคับกับกรณีดังต่อไปนี้

(๖.๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

(๖.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย พ.ศ. ๒๔๘๓ และที่แก้ไขเพิ่มเติม

(๖.๓) งานจ้างก่อสร้างที่กรมบัญชีกลางได้ขึ้นทะเบียนผู้ประกอบการงานก่อสร้างแล้ว และงานจ้างก่อสร้างที่หน่วยงานของรัฐที่ได้มีการจัดทำบัญชีผู้ประกอบการงานก่อสร้างที่มีคุณสมบัติเบื้องต้นไว้แล้วก่อนวันที่พระราชบัญญัติการจัดซื้อจัดจ้างฯ มีผลใช้บังคับ

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

(๖.๕) การซื้ออสังหาริมทรัพย์และการเช่าอสังหาริมทรัพย์

(๖.๖) กรณีงานจ้างบริการหรืองานจ้างเหมาบริการกับบุคคลธรรมดา เช่น จ้างพนักงานขับรถ ครูชาวต่างชาติ พนักงานเก็บขยะ พนักงานบันทึกข้อมูล เป็นต้น

๖.๑.๑๓ ผู้เสนอราคาต้องมีผลงานการทดสอบเจาะระบบสารสนเทศให้แก่สถาบันการเงิน หน่วยงานภาครัฐ รัฐวิสาหกิจ หรือเอกชนอย่างน้อย ๑ โครงการ ในวงเงินไม่น้อยกว่า ๕ แสนบาท โดยเป็นสัญญาที่ทำมาไม่เกิน ๕ ปี นับถึงวันยื่นเสนอราคาทางระบบอิเล็กทรอนิกส์ โดยผู้เสนอราคาต้องส่งเอกสาร/หลักฐานแสดงถึงการทดสอบเจาะระบบสารสนเทศแล้วเสร็จ อย่างน้อยดังนี้

/ (๑) หนังสือ...

(๑) หนังสือรับรองผลงานของหน่วยงานนั้น ๆ โดยต้องมีหัวหน้าหน่วยงาน หรือผู้ทำการแทนหน่วยงานนั้นทำการรับรอง

(๒) สำเนาสัญญาจ้าง หรือหนังสือสั่งจ้างที่ปรากฏวงเงินสัญญา และขอบเขตงานการทดสอบเจาะระบบสารสนเทศ

ทั้งนี้ สำนักงาน ป.ป.ช. สงวนสิทธิ์ที่จะตรวจสอบวินิจฉัยข้อเท็จจริง โดยตรงจากผู้รับรองที่เสนอมานั้น

๖.๑.๑๔ ผู้เสนอราคาต้องมีบุคลากรหลักในโครงการ ดังต่อไปนี้

(๑) หัวหน้าโครงการ

<u>คุณสมบัติ</u>:

- สำเร็จการศึกษาระดับปริญญาตรี
- มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อย ๕ ปี
- มีประสบการณ์ในการบริหารโครงการตรวจสอบช่องโหว่ ประเมินและหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หน่วยงานภาครัฐ รัฐวิสาหกิจ หรือเอกชน
- ได้รับใบรับรอง (Certificate) และยังไม่หมดอายุนับถึงวันยื่นเสนอราคาทางระบบอิเล็กทรอนิกส์ อย่างน้อย ๑ รายการ ดังต่อไปนี้
  - CISSP (Certified Information Systems Security Professional)
  - CISA (Certified Information Systems Auditor)
  - CISM (Certified Information Security Manager)

(๒) บุคลากร/ทีมงานโครงการ (ผู้เชี่ยวชาญการทดสอบเจาะระบบฯ) อย่างน้อย ๓ คน

<u>คุณสมบัติ</u>

- สำเร็จการศึกษาระดับปริญญาตรี
- มีประสบการณ์ในการตรวจสอบช่องโหว่ ประเมินและหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หน่วยงานภาครัฐ รัฐวิสาหกิจ หรือเอกชน
- ได้รับใบรับรอง (Certificate) ระดับผู้เชี่ยวชาญ และยังไม่หมดอายุนับถึงวันยื่นเสนอราคาทางระบบอิเล็กทรอนิกส์อย่างน้อย ๑ รายการ ดังต่อไปนี้
  - EC-Council LPT (License Penetration Tester) Master
  - EC-Council Certified Security Analyst (ECSA)
  - Infosec Institute Certified Expert Penetration Tester (CEPT)
  - Offensive Security Certified Professional (OSCP)
  - Evasion Techniques and Breaching Defense (OSEP)
  - Offensive Security Web Expert (OSWE)
  - GIAC Penetration Tester (GPEN) และ GIAC Web Application Penetration Tester (GWAPT)
  - GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
  - Certified Simulated Attack (CCSAS)
  - Certified Web Application Tester (CCT Web App)

/ ➢ CREST ...

- CREST Registered Penetration Tester (CRT)
- eLearnSecurity Certified Professional Penetration Tester (eCPPT)
- eLearnSecurity Web application Penetration Tester (eWPT)
- eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX)
- Certificate Red Team Professional (CRTP)

(๓) ผู้ประสานงานโครงการ อย่างน้อยจำนวน ๑ คน

<u>คุณสมบัติ</u>

- สำเร็จการศึกษาระดับปริญญาตรี
- มีประสบการณ์ในการทำงานในการประสานงานโครงการอย่างน้อย ๑ ปี

๗. ระยะเวลาดำเนินโครงการ

ระยะเวลาดำเนินการ ๒๗๐ วัน นับถัดจากวันลงนามในสัญญา

๘. ขอบเขตการดำเนินงาน

ผู้เสนอราคาต้องดำเนินการตามเงื่อนไขและขอบเขตการดำเนินงานของ สำนักงาน ป.ป.ช. อย่างน้อย ดังนี้

๘.๑ จัดทำแผนบริหารโครงการ (Project Plan) ประกอบด้วยอย่างน้อย ดังนี้

๘.๑.๑ แผนการดำเนินงานตามขอบเขตการดำเนินงานที่กำหนด

๘.๑.๒ แนวทางการดำเนินงาน ขั้นตอนการปฏิบัติงาน ความเสี่ยงและการบริหารความเสี่ยง เทคนิค ข้อมูลผู้ดำเนินงาน และข้อมูลอื่น ๆ ที่เกี่ยวข้องในการดำเนินงานตามขอบเขตการดำเนินงาน

๘.๒ ดำเนินการเพื่อตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช ประกอบด้วย

๘.๒.๑ ตรวจสอบช่องโหว่ (Vulnerability Assessment: VA) จำนวน ๒ ครั้ง ดังนี้

<u>๘.๒.๑.๑ ครั้งที่ ๑</u>

(๑) ตรวจสอบช่องโหว่ (VA) อุปกรณ์เครือข่าย (Network Equipment) เครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์ในระบบรักษาความปลอดภัยสารสนเทศ (Security Device) และอุปกรณ์อื่น ๆ ที่มีการเชื่อมต่ออินเทอร์เน็ต (Internet Facing) ของสำนักงาน ป.ป.ช. จำนวนไม่น้อยกว่า ๑๐๐ IP Address โดยใช้โปรแกรมประเภทที่มีลิขสิทธิ์ และผู้รับจ้างมีสิทธิ์ใช้โดยถูกต้องตามกฎหมาย ๑ โปรแกรม และ Open Source หรือ Freeware อย่างน้อย ๑ โปรแกรม ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ โดยการตรวจสอบช่องโหว่ดำเนินการจาก Internal ผ่าน Security Device และไม่ผ่าน Security Device

(๒) วิเคราะห์ จัดระดับความเสี่ยง และจัดทำข้อเสนอแนะแนวทางการปิดช่องโหว่ที่ตรวจพบ

(๓) จัดทำรายงานผลการตรวจสอบช่องโหว่ (VA) ตามรูปแบบรายงานผลการดำเนินงานตามข้อ ๘.๒.๓

/ (๔) ร่วมดำเนินการ...

(๔) ร่วมดำเนินการให้คำปรึกษากับผู้ดูแลระบบของสำนักงาน ป.ป.ช. เพื่อปิดช่องโหว่ตามผลการตรวจสอบช่องโหว่ (VA) ตามขอบเขตของงานและระยะเวลาการดำเนินการที่สำนักงาน ป.ป.ช. เห็นชอบ

๘.๒.๑.๒ ครั้งที่ ๒ (Revisit)

(๑) ตรวจสอบช่องโหว่ซ้ำ (Revisit Vulnerability Assessment) ตามข้อ ๘.๒.๑.๑ สอดคล้องตามผลการตรวจสอบช่องโหว่ (VA)

(๒) จัดทำรายงานตรวจสอบช่องโหว่ (VA) และผลการปิดช่องโหว่ครั้งที่ ๒ ตามรูปแบบรายงานผลการดำเนินงาน ตามข้อ ๘.๒.๓

๘.๒.๒ ทดสอบเจาะระบบ (Penetration Testing) ครอบคลุมการประเมินหรือทดสอบความมั่นคงปลอดภัยของโฮสต์ เครือข่าย และสถาปัตยกรรมของระบบเป้าหมาย จำนวน ๑๐ ระบบ ๘ IP และ API service ที่ให้บริการบน Server จำนวน ๓ IP ดังนี้

ที่	ชื่อระบบ	จำนวน IP Address
๑	ระบบแจ้งเบาะแสการทุจริต และติดตามสถานการณ์แจ้งเบาะแส	๑ IP Address
๒	ระบบ Q & A	
๓	ระบบการยื่นบัญชีแสดงรายการทรัพย์สินและหนี้สิน (Online Declaration System : ODS)	๑ IP Address
๔	ระบบการเปิดเผยบัญชีทรัพย์สินและหนี้สิน (DCS)	
๕	ระบบแจ้งทะเบียนผู้มีหน้าที่ยื่นบัญชีทรัพย์สินและหนี้สิน (ODRS) (สำหรับผู้แทนหน่วยงานต้นสังกัด)	๑ IP Address
๖	ระบบเปิดเผยผลการตรวจสอบทรัพย์สินและหนี้สิน ของสำนักงาน ป.ป.ช.	๑ IP Address
๗	ระบบทดสอบความรู้ธรรมาภิบาลออนไลน์	๑ IP Address
๘	ระบบการประเมินคุณธรรมและความโปร่งใสในการดำเนินงานของหน่วยงานภาครัฐระดับต่ำกว่ากรม (Integrity and Transparency Assessment of Public Service: ITAP)	๑ IP Address
๙	ระบบการประเมินคุณธรรมและความโปร่งใสในการดำเนินงานของหน่วยงานภาคเอกชนที่เป็นคู่ค้าคู่สัญญากับหน่วยงานภาครัฐ (Integrity and Transparency Assessment of Government Contractors: ITAGC)	
๑๐	ระบบพิพิธภัณฑ์ต้านโกง	๒ IP Address
๑๑	API service ที่ให้บริการบน Server	๓ IP Address

โดยดำเนินการทดสอบเจาะระบบ (Penetration Testing) จำนวน ๒ ครั้ง ดังนี้

๘.๒.๒.๑ ครั้งที่ ๑

(๑) ดำเนินการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบแบบ White Box ของระบบเป้าหมาย โดยจะต้องดำเนินการค้นหาช่องโหว่ในทุก ๆ หน้า ทุก ๆ ฟังก์ชัน ทุก ๆ Module ที่ใช้งาน และจะต้องค้นหาช่องโหว่ทั้งด้านเทคนิคและช่องโหว่ด้าน Business Logic และดำเนินการทดสอบเจาะระบบในรูปแบบผสมผสาน โดยการทดสอบด้วยการใช้เครื่องมือเจาะระบบแบบอัตโนมัติ (Automate Tool)

/ ทั้งแบบ ...

ทั้งแบบ Commercial Tool และแบบ Open-source Tool ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ(ผู้รับจ้างจะต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเองด้วย (Manual Test) มิให้ใช้เครื่องมืออัตโนมัติ (Automatic Test Tool) เพียงอย่างเดียว) เจาะจาก Internal ผ่าน Security Device และไม่ผ่าน Security Device อ้างอิงตาม Open Web Application Security Project (OWASP) Testing guide

(๒) ดำเนินการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของชุดคำสั่ง (Source Code Scanning) ของระบบเป้าหมายรวม Library อ้างอิงตาม OWASP Secure Coding Practices Quick Reference Guide ประกอบด้วยหัวข้อต่าง ๆ ดังนี้

(๒.๑) ตรวจสอบการนำเข้าข้อมูลทั้งหมด (Input Validation)

(๒.๒) ตรวจสอบการแสดงหรือส่งออกข้อมูลทั้งหมด (Output Validation)

(๒.๓) ตรวจสอบกลไกการยืนยันตัวตนและการจัดการรหัสผ่าน (Authentication and Password Management)

(๒.๔) ตรวจสอบการจัดการเซสชันของผู้ใช้งานหลังการยืนยันตัวตน (Session Management)

(๒.๕) ตรวจสอบการควบคุมการเข้าถึงระบบ (Access Control)

(๒.๖) ตรวจสอบการใช้งานการเข้ารหัสลับข้อมูล (Cryptographic Practices)

(๒.๗) ตรวจสอบการจัดการความผิดพลาดและการบันทึกล็อก (Error Handling and Logging)

(๒.๘) ตรวจสอบการรักษาความมั่นคงปลอดภัยข้อมูล (Data Protection)

(๒.๙) ตรวจสอบการรักษาความมั่นคงปลอดภัยของการสื่อสารข้อมูล (Communication Security)

(๒.๑๐) ตรวจสอบการตั้งค่าเครื่องแม่ข่าย (Server Configuration)

(๒.๑๑) การรักษาความมั่นคงปลอดภัยระบบฐานข้อมูล (Database Security)

(๒.๑๒) ตรวจสอบการจัดการไฟล์ของแอปพลิเคชัน (File Management)

(๒.๑๓) ตรวจสอบการจัดการหน่วยความจำของแอปพลิเคชัน (Memory Management)

(๓) วิเคราะห์ จัดระดับความเสี่ยง และจัดทำข้อเสนอแนะแนวทางการปิดช่องโหว่ที่ตรวจพบ

(๔) จัดทำรายงานผลทดสอบเจาะระบบ (Penetration Testing) ตามรูปแบบรายงานผลการดำเนินงานตามข้อ ๘.๒.๓

(๕) ร่วมดำเนินการให้คำปรึกษากับผู้ดูแลระบบของสำนักงาน ป.ป.ช. เพื่อปิดช่องโหว่ตามผลการทดสอบเจาะระบบ (Penetration Testing) ตามขอบเขตของงานและระยะเวลาการดำเนินการที่สำนักงาน ป.ป.ช. เห็นชอบ

<u>๘.๒.๒.๒ ครั้งที่ ๒ (Revisit)</u>

(๑) ทดสอบเจาะระบบซ้ำ (Revisit Penetration Testing) ตามข้อ ๘.๒.๒.๑ สอดคล้องตามผลการผลทดสอบเจาะระบบ

(๒) จัดทำรายงานทดสอบเจาะระบบ (Penetration Testing) และผลการปิดช่องโหว่ครั้งที่ ๒ ตามรูปแบบรายงานผลการดำเนินงานตามข้อ ๘.๒.๓

๘.๒.๓ จัดทำรายงานผลการวิเคราะห์และผลทดสอบตามข้อ ๘.๒.๑ และ ๘.๒.๒ พร้อมประเมินความเสี่ยง และข้อเสนอแนะเพื่อใช้ในการแก้ปัญหา และต้องมีหัวข้อแสดงข้อมูลเหล่านี้เป็นอย่างน้อย ดังนี้

(๑) บทสรุปสำหรับผู้บริหาร

/๘.๒.๓ จัดทำ...

๘.๒.๓ จัดทำรายงานผลการวิเคราะห์และผลทดสอบตามข้อ ๘.๒.๑ และ ๘.๒.๒ พร้อมประเมินความเสี่ยง และข้อเสนอแนะเพื่อใช้ในการแก้ปัญหา และต้องมีหัวข้อแสดงข้อมูลเหล่านี้เป็นอย่างน้อย ดังนี้

(๑) บทสรุปสำหรับผู้บริหาร

(๒) ระบบที่ทำการทดสอบ

(๓) วิธีการ และรายละเอียดในการทดสอบ

(๔) ประเภทของช่องโหว่ที่ดำเนินการทดสอบ

(๕) ผลการทดสอบเจาะระบบ (ช่องโหว่ที่ตรวจพบ)

(๖) ระดับความเสี่ยงช่องโหว่และผลกระทบที่อาจจะเกิดขึ้น

(๗) ช่วงวันเวลาที่ดำเนินการทดสอบ

(๘) แสดงภาพของการทดสอบระบบ (Screen Capture)

(๙) แนวทางและวิธีการแก้ไขจากผลการดำเนินการทดสอบ (ช่องโหว่ที่ตรวจพบ)

(๑๐) แนวทางและวิธีการเพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัยระบบสารสนเทศ

(๑๑) ประเมินค่าใช้จ่ายในการดำเนินการแก้ไข (ถ้ามี)

๘.๓ ให้คำแนะนำในการเตรียมความพร้อมเพื่อพัฒนางานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๘.๓.๑ ดำเนินการประเมินสถานการณ์ดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ปัจจุบันของสำนักงาน ป.ป.ช. โดยดำเนินการประเมินอย่างน้อยดังนี้

(๑) ตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review) เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย

(๒) ตรวจสอบนโยบายของ Firewall และ WAF เพื่อวิเคราะห์ความเหมาะสมของนโยบายและให้ข้อเสนอแนะเกี่ยวกับนโยบายที่จำเป็นของระบบสารสนเทศที่พัฒนาขึ้น

(๓) ตรวจสอบนโยบาย Security เพื่อประเมินความสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

(๔) วิเคราะห์ข้อมูล Log ของ SIEM (Security Information and Event Management)

๘.๓.๒ วิเคราะห์และจัดทำ Gap Analysis และข้อเสนอแนะการพัฒนางานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเตรียมความพร้อมในการดำเนินงานด้านศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยดำเนินการอย่างน้อยดังนี้

(๑) กำหนดกลยุทธ์และเป้าหมาย:

• ระบุความเสี่ยงและภัยคุกคามที่องค์กรอาจเผชิญ.

• กำหนดขอบเขตและเป้าหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับเป้าหมายของสำนักงาน ป.ป.ช.

• กำหนดโครงสร้างการทำงานของศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๘.๓.๓ ออกแบบและสร้างกระบวนการและขั้นตอน

• วิเคราะห์และให้ข้อเสนอแนะในการเลือกเทคโนโลยีที่เหมาะสมสำหรับการตรวจจับ, วิเคราะห์, และตอบสนองต่อภัยคุกคาม

• จัดทำข้อเสนอแนะการใช้งาน SIEM (Security Information and Event Management) เพื่อเชื่อมโยงข้อมูลและแจ้งเตือนเหตุการณ์ โดยออกแบบการรวบรวมและวิเคราะห์ข้อมูลรวมถึงการสร้าง Use Case สำหรับการตรวจจับภัยคุกคาม

/• พัฒนา...

• พัฒนากระบวนการตอบสนองต่อเหตุการณ์ (Incident Response Plan) ที่ชัดเจนและครอบคลุม

• กำหนดขั้นตอนการทำงาน (Standard Operating Procedures - SOP) สำหรับการดำเนินงานด้านศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

• จัดทำคู่มือการใช้งาน (Documentation) สำหรับบุคลากร ในการดำเนินงานด้านศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๘.๓.๔ จัดทำแนวทางพัฒนาทักษะ หลักสูตร ที่จำเป็นให้แก่บุคลากรที่ปฏิบัติงานด้านศูนย์ปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๘.๓.๕ จัดประชุมชี้แจงรายงานผลการศึกษาการเตรียมความพร้อมเพื่อพัฒนางานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ผู้ที่เกี่ยวข้อง

๘.๔ อบรม/สัมมนา โดยผู้เสนอราคาจะต้องดำเนินการบันทึกการอบรม และจัดทำเป็นไฟล์วีดีโอ สำหรับเผยแพร่ บันทึกลงสื่อจัดเก็บข้อมูล และรายงานการจัดอบรม/สัมมนา จำนวน ๓ ชุด โดยผู้เสนอราคาต้องรับผิดชอบค่าใช้จ่ายในเรื่องวิทยากร สถานที่ ค่าอาหารว่าง อาหารกลางวัน เครื่องดื่ม ค่าเอกสารประกอบการฝึกอบรม และอื่น ๆ ที่เกี่ยวข้องกับการจัดอบรม/สัมมนานี้ โดยกำหนดหลักสูตร ดังนี้

๘.๔.๑ หลักสูตรการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศสำหรับผู้บริหาร จำนวน ๑ ครั้ง ระยะเวลาไม่น้อยกว่า ๓ ชั่วโมง จำนวนผู้เข้าร่วมอบรมไม่น้อยกว่า ๑๕ คน

๘.๔.๒ หลักสูตรการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศสำหรับเจ้าหน้าที่ของหน่วยงาน จำนวนไม่น้อยกว่า ๑ ครั้ง ระยะเวลาครั้งละไม่น้อยกว่า ๓ ชั่วโมง จำนวนผู้เข้าร่วมอบรมรวมไม่น้อยกว่า ๑๐๐ คน

๘.๔.๓ หลักสูตรการตรวจสอบช่องโหว่ (VA) และการทดสอบเจาะระบบ (Penetration Testing) บนระบบจำลอง จำนวน ๑ ระบบ ระยะเวลาการอบรมวันละไม่น้อยกว่า ๖ ชั่วโมง อย่างน้อย ๓๐ ชั่วโมง จำนวนผู้เข้าร่วมอบรมไม่น้อยกว่า ๒๐ คน

๘.๔.๔ หลักสูตรการให้ความรู้ด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับผู้ดูแลระบบ ผู้รับผิดชอบ หรือผู้เกี่ยวข้องกับระบบสารสนเทศ จำนวน ๑ หลักสูตร ระยะเวลาการอบรมวันละไม่น้อยกว่า ๖ ชั่วโมง อย่างน้อย ๑๘ ชั่วโมง จำนวนผู้เข้าร่วมอบรมไม่น้อยกว่า ๓๐ คน

๘.๕ ต้องอนุญาตให้เจ้าหน้าที่ผู้ที่เกี่ยวข้อง เข้าร่วมสังเกตการทดสอบเจาะระบบเพื่อสร้างความตระหนักรู้ด้านภัยคุกคามที่อาจจะเกิดขึ้น

๘.๖ จัดประชุมนำเสนอผลการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช. ตามข้อ ๘.๒ และจัดทำรายงานผลการประชุม

๘.๗ เข้าร่วมประชุมเพื่อรายงานผลการดำเนินงานต่อคณะกรรมการ/คณะอนุกรรมการที่เกี่ยวข้อง

๘.๘ ผู้เสนอราคาต้องแจ้งเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ช. ให้ทราบทุกครั้งก่อนเข้าดำเนินงานในแต่ละขั้นตอน

๘.๙ การดำเนินงานต้องไม่ส่งผลกระทบหรือสร้างความเสียหายต่อระบบงาน หากเกิดความเสียหายผู้เสนอราคาต้องรับผิดชอบในการทำให้ระบบงานนั้นใช้งานได้เป็นปกติดังเดิม โดยไม่คิดค่าใช้จ่ายใด ๆ เพิ่มเติม

๘.๑๐ ผู้เสนอราคาต้องรับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงาน ป.ป.ช. ที่เกี่ยวข้องอย่างเคร่งครัด

/๘.๑๑ ผู้เสนอ...

ธอ แนฟอร์ม

๘.๑๑ ผู้เสนอราคาจะต้องปฏิบัติตามนโยบาย มาตรการ ระเบียบวิธีปฏิบัติ และคู่มือการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO ๒๗๐๐๑ ของสำนักเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ช. และกฎหมายอื่น ๆ ที่เกี่ยวข้อง

๙. ข้อกำหนดในการตรวจรับงานและการส่งมอบงาน

ผู้เสนอราคา จะต้องส่งมอบเอกสารตามรายการทั้งหมดให้ถูกต้องและครบถ้วนตามที่กำหนด พร้อมบันทึกลงสื่อจัดเก็บข้อมูล อย่างน้อยจำนวน ๓ ชุด ตามงวดงาน ดังต่อไปนี้

งวดที่ ๑ ส่งมอบงาน ข้อ ๘.๑ ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา

งวดที่ ๒ ส่งมอบงาน ภายใน ๑๕๐ วัน นับถัดจากวันลงนามในสัญญา ตามขอบเขตการดำเนินงานตามหัวข้อ ๘.๒ ได้แก่ ข้อ ๘.๒.๑.๑ และข้อ ๘.๒.๒.๑

งวดที่ ๓ ส่งมอบงาน ภายใน ๒๗๐ วัน นับถัดจากวันลงนามในสัญญา ตามขอบเขตการดำเนินงานตามหัวข้อต่าง ๆ ดังนี้

(๑) รายงานผลการดำเนินงานตามขอบเขตการดำเนินงานตามหัวข้อ ๘.๒ ได้แก่ ข้อ ๘.๒.๑.๒ และข้อ ๘.๒.๒.๒

(๒) รายงานผลการดำเนินตามขอบเขตงาน ข้อ ๘.๓

(๓) รายงานผลการดำเนินงานตามขอบเขตงาน ข้อ ๘.๔

๑๐. เงื่อนไขการจ่ายเงิน

การชำระเงินตามจำนวนในสัญญาแบ่งเป็น ๒ งวด ภายหลังจากที่คณะกรรมการตรวจการจ้างได้ตรวจรับรายงานต่าง ๆ ที่ต้องส่งมอบถูกต้องเรียบร้อยแล้ว ดังนี้

งวดที่ ๑ ชำระค่าจ้างจำนวนร้อยละ ๔๐ ของวงเงินตามสัญญาจ้าง เมื่อสำนักงาน ป.ป.ช. ได้ตรวจรับงานงวดที่ ๑ และงานงวดที่ ๒ เรียบร้อยแล้ว

งวดที่ ๒ ชำระค่าจ้างจำนวนร้อยละ ๖๐ ของวงเงินตามสัญญาจ้าง เมื่อสำนักงาน ป.ป.ช. ได้ตรวจรับงานงวดที่ ๓ เรียบร้อยแล้ว

๑๑. การรักษาข้อมูล

ผู้เสนอราคาต้องเก็บรักษาข้อมูลสำนักงาน ป.ป.ช. และข้อมูลส่วนบุคคลไว้เป็นความลับ และไม่เปิดเผยให้บุคคลภายนอกทราบ ทั้งนี้ หากมีการฝ่าฝืนผู้เสนอราคาจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นและตามที่กฎหมายกำหนดและต้องลงนาม "สัญญาที่จะไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) และข้อตกลงในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) และการปฏิบัติตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ" ทั้งนี้ร่างสัญญาดังกล่าวมีรายละเอียดตามภาคผนวกที่แนบท้ายร่างขอบเขตของงาน (Terms of Reference : TOR) ฉบับนี้

๑๒. เกณฑ์การพิจารณา

๑๒.๑ หากผู้เสนอราคารายใดมีคุณสมบัติไม่ถูกต้องตามข้อกำหนด หรือยื่นหลักฐานการเสนอราคาไม่ถูกต้อง หรือไม่ครบถ้วนตามข้อกำหนด แล้วคณะกรรมการประกวดราคาจะไม่รับพิจารณาข้อเสนอของผู้เสนอราคารายนั้น เว้นแต่เป็นข้อผิดพลาดหรือผิดหลงเพียงเล็กน้อยหรือผิดพลาดมาจากเงื่อนไขของเอกสารประกวดราคาในส่วนที่มิใช่สาระสำคัญ ทั้งนี้ เฉพาะในกรณีที่พิจารณาเห็นว่าจะเป็นประโยชน์ต่อสำนักงาน ป.ป.ช. เท่านั้น

/๑๒.๒ สำนักงาน...

๑๒.๒ สำนักงาน ป.ป.ช. สงวนสิทธิ์ไม่พิจารณาราคาของผู้เสนอราคา โดยไม่มีการผ่อนผันในกรณีเสนอรายละเอียดแตกต่างไปจากเงื่อนไขที่กำหนดในเอกสารประกวดราคาที่เป็นสาระสำคัญ หรือมีผลทำให้เกิดความได้เปรียบเสียเปรียบแก่ผู้เสนอราคารายอื่น

๑๒.๓ สำนักงาน ป.ป.ช. ทรงไว้ซึ่งสิทธิที่จะไม่รับราคาต่ำสุดหรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดก็ได้ และอาจพิจารณาเลือกในจำนวน หรือขนาด หรือเฉพาะรายการหนึ่งรายการใด หรืออาจจะยกเลิกการประกวดราคา โดยไม่พิจารณาจัดจ้างเลยก็ได้ สุดแต่จะพิจารณา และให้ถือว่าการตัดสินของสำนักงาน ป.ป.ช. เป็นเด็ดขาด ผู้เสนอราคาจะเรียกร้องค่าเสียหายใด ๆ มิได้ รวมทั้งสำนักงาน ป.ป.ช. จะพิจารณายกเลิกการประกวดราคา และลงโทษผู้เสนอราคาเป็นผู้ทิ้งงาน ไม่ว่าจะเป็นผู้เสนอราคาที่ได้รับคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่เชื่อได้ว่าการเสนอราคากระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ หรือใช้ชื่อบุคคลธรรมดา หรือนิติบุคคลอื่นมาเสนอราคาแทน เป็นต้น

๑๒.๔ ในกรณีที่ปรากฏข้อเท็จจริงภายหลังจากการประกวดราคาว่า ผู้เสนอราคาที่มีสิทธิได้รับการคัดเลือกเป็นผู้เสนอราคาที่มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่น หรือเป็นผู้เสนอราคาที่กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม สำนักงาน ป.ป.ช. มีอำนาจที่จะตัดรายชื่อผู้เสนอราคาที่มีสิทธิได้รับการคัดเลือกดังกล่าว และสำนักงาน ป.ป.ช. จะพิจารณาลงโทษผู้เสนอราคารายนั้นเป็นผู้ทิ้งงาน

๑๒.๕ ข้อเสนอโครงการต้องประกอบด้วยเนื้อหาที่แสดงถึงความรู้ความสามารถด้านตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศ โดยเสนอในรูปแบบที่มีการแสดงการเปรียบเทียบระหว่างข้อเสนอกับคุณสมบัติหรือเงื่อนไขในส่วนต่าง ๆ ตามที่สำนักงาน ป.ป.ช. ได้กำหนดไว้

๑๒.๖ สำนักงาน ป.ป.ช. จะพิจารณาตัดสินโดยใช้เกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (เกณฑ์ราคาประกอบเกณฑ์อื่น) ซึ่งพิจารณาให้คะแนนการประเมินค่าประสิทธิภาพต่อราคา (Price Performance) โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนด ดังนี้ ราคาที่เสนอเป็นร้อยละ ๓๐ และข้อเสนอทางเทคนิคหรือข้อเสนออื่นเพิ่มเติม ร้อยละ ๗๐ (รายละเอียดตามภาคผนวก ๑)

๑๒.๗ ผู้เสนอราคาต้องนำเสนอการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศ ประกอบด้วย

(๑) แผนการดำเนินงาน ขั้นตอนการดำเนินงาน และขั้นตอนการประเมินความเสี่ยง เช่น การจำแนกความเสี่ยง คำอธิบายความเสี่ยง และรูปแบบรายงานผลการวิเคราะห์และผลการทดสอบเจาะระบบสารสนเทศ

(๒) Methodology กระบวนการ เครื่องมือ เทคนิค หรือวิธีการที่ใช้ในการประเมินความมั่นคงปลอดภัยและตรวจสอบค้นหาช่องโหว่ของระบบสารสนเทศ และชุดคำสั่ง (Source Code) และแนวทางการบริหารการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงจากภัยคุกคามคอมพิวเตอร์ที่อาจจะเกิดขึ้น

(๓) แนวคิดการบริหารจัดการศูนย์ปฏิบัติการด้านความปลอดภัย (Security Operations Center: SOC)

ตามวันและเวลาที่สำนักงาน ป.ป.ช. กำหนด ทั้งนี้หากผู้เสนอราคาไม่เข้าร่วมการนำเสนอ สำนักงาน ป.ป.ช. จะไม่พิจารณารายละเอียดและข้อเสนอของผู้เสนอราคารายนั้น

๑๓. รายละเอียดเอกสารประกอบการพิจารณาการเข้าเสนอราคา

ผู้เสนอราคาต้องจัดทำเอกสารยื่นข้อเสนอราคา และจะต้องยื่นผ่านระบบจัดซื้อจัดจ้างฯ (e-GP) ไม่อนุญาตให้มีการขอส่งเอกสารเพิ่มเติมในภายหลังไม่ว่ากรณีใด ๆ นับจากวันที่ให้ยื่นข้อเสนอราคายื่นผ่านระบบจัดซื้อจัดจ้างฯ (e-GP) เว้นแต่คณะกรรมการพิจารณาผลได้พิจารณาแล้วเห็นควรขอเอกสารเพิ่มเติม เพื่อความชัดเจนในการพิจารณา ได้แก่

/๑๓.๑ ตาราง...

๑๓.๑ ตารางการเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะตามข้อกำหนดของ สำนักงาน ป.ป.ช. กับที่เสนอเป็นข้อ ๆ ในแต่ละรายการอย่างละเอียดโดยพิมพ์เป็นเอกสารประกอบการนำเสนอ พร้อมทั้งบ่งชี้ในแต่ละรายการอย่างครบถ้วนและชัดเจน

๑๓.๒ เอกสารแสดงถึงผลงานการทดสอบเจาะระบบสารสนเทศให้แก่สถาบันการเงิน หน่วยงานภาครัฐ รัฐวิสาหกิจ หรือเอกชนอย่างน้อย ๑ โครงการ ในวงเงินไม่น้อยกว่า ๕ แสนบาท โดยเป็นสัญญาที่ทำมาไม่เกิน ๕ ปี นับถึงวันยื่นเสนอราคาทางระบบอิเล็กทรอนิกส์ โดยผู้เสนอราคาต้องส่งเอกสาร/หลักฐานแสดงถึงการทดสอบเจาะระบบสารสนเทศแล้วเสร็จ อย่างน้อยดังนี้

๑) หนังสือรับรองผลงานของหน่วยงานนั้น ๆ โดยต้องมีหัวหน้าหน่วยงาน หรือผู้ทำการแทนหน่วยงานนั้นทำการรับรอง

๒) สำเนาสัญญาจ้าง หรือหนังสือสั่งจ้างที่ปรากฏวงเงินสัญญา และขอบเขตงานการทดสอบเจาะระบบสารสนเทศ

๑๓.๓ รายชื่อของหัวหน้าโครงการ บุคลากร/ทีมงานโครงการ (ผู้เชี่ยวชาญเพื่อทดสอบเจาะระบบสารสนเทศ) และผู้ประสานงานโครงการ พร้อมสำเนาเอกสารหลักฐานคุณวุฒิ ปริญญาบัตร/ประกาศนียบัตรความเชี่ยวชาญ ประวัติการทำงาน ใบรับรอง (Certificate)

๑๓.๔ เอกสารทางด้านเทคนิคเพื่อแสดงคุณลักษณะเฉพาะตามที่ได้กำหนดไว้ ดังนี้

๑) แผนการดำเนินงาน ขั้นตอนการดำเนินงาน และขั้นตอนการประเมินความเสี่ยง เช่น การจำแนกความเสี่ยง คำอธิบายความเสี่ยง และรูปแบบรายงานผลการวิเคราะห์และผลการทดสอบเจาะระบบสารสนเทศ

๒) Methodology กระบวนการ หรือวิธีการที่ใช้ในการประเมินความมั่นคงปลอดภัยและตรวจสอบค้นหาช่องโหว่ของระบบสารสนเทศ และชุดคำสั่ง (Source Code) และแนวทางการบริหารการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงจากภัยคุกคามคอมพิวเตอร์ที่อาจจะเกิดขึ้น

๓) แนวคิดการบริหารจัดการศูนย์ปฏิบัติการด้านความปลอดภัย (Security Operations Center: SOC)

๑๔. วงเงินในการจัดหา (เงินงบประมาณ)

๕,๑๙๓,๑๐๐.๐๐ บาท (ห้าล้านหนึ่งแสนเก้าหมื่นสามพันหนึ่งร้อยบาทถ้วน)

๑๕. หน่วยงานที่รับผิดชอบและสถานที่ติดต่อ

สำนักเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ช.

สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติมหรือเสนอแนะวิจารณ์ หรือแสดงความคิดเห็นโดยเปิดเผยตัวได้ที่

๑) ทางไปรษณีย์

ส่งถึง เลขาธิการคณะกรรมการ ป.ป.ช.

สำนักงาน ป.ป.ช. เลขที่ ๓๖๑ ถ. นนทบุรี ต. ท่าทราย อ. เมืองนนทบุรี

จ. นนทบุรี ๑๑๐๐๐

๒) โทรศัพท์ ๐-๒๕๒๘-๔๘๐๐ ต่อ ๓๐๓๑

๓) โทรสาร ๐-๒๕๒๘-๔๙๘๒

๔) อีเมล egp๒๓_nac@nacc.go.th

ภาคผนวก ๑

หลักเกณฑ์การพิจารณาข้อเสนอด้านเทคนิค

โครงการตรวจสอบหาช่องโหว่ ประเมิน และหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ช.

๑. สำนักงาน ป.ป.ช. จะพิจารณาคุณสมบัติของผู้เสนอราคา หากคุณสมบัติไม่เป็นไปตามหลักเกณฑ์ที่กำหนดไว้ สำนักงาน ป.ป.ช. จะไม่พิจารณาข้อเสนอทางเทคนิค

๒. ในการเสนอราคาครั้งนี้ สำนักงาน ป.ป.ช. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance)

๓. สำนักงาน ป.ป.ช. จะพิจารณาให้คะแนนการประเมินค่าประสิทธิภาพต่อราคา (Price Performance) โดยพิจารณาให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนด คือ

(๑) ราคาที่เสนอราคา (Price) เป็นตัวแปรหลักบังคับ น้ำหนักร้อยละ ๓๐

(๒) คุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อทางสำนักงาน ป.ป.ช. น้ำหนักร้อยละ ๗๐

โดยกำหนดให้มีน้ำหนักรวมทั้งหมด เท่ากับร้อยละ ๑๐๐

๔. สำนักงาน ป.ป.ช. จะพิจารณาจากผู้เสนอราคาที่ได้รับคะแนนข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ๆ สูงสุดและเรียงลำดับคะแนนต่อไปเป็นอันดับที่ ๒ ๓ ตามลำดับ และขอสงวนสิทธิคัดเลือกผู้เสนอราคาที่มีคะแนนข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ๆ และเสนอราคาภายในวงเงินที่กำหนด หากผู้เสนอราคามีคะแนนข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ๆ เท่ากันจะพิจารณาจากข้อเสนอด้านราคาเป็นลำดับถัดไป

๕. เกณฑ์การพิจารณาข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ๆ (คะแนนเต็ม ๑๐๐ คะแนน)

สำนักงาน ป.ป.ช. จะพิจารณาข้อเสนอด้านเทคนิคหรือข้อเสนออื่น ๆ ของผู้เสนอราคาเฉพาะที่มีคุณสมบัติและหลักฐานเอกสารถูกต้อง โดยมีเกณฑ์การพิจารณา ดังนี้

หลักเกณฑ์การให้คะแนน	คะแนน
(๑) ผลงานที่ผ่านมา	๒๐ คะแนน
(๒) บุคลากร/ทีมงาน	๓๐ คะแนน
(๓) ข้อเสนอจัดกิจกรรมซ้อมรับมือภัยคุกคามทางไซเบอร์ (Cyber Drill) โดยวิธี Email Phishing	๒๐ คะแนน
(๔) การนำเสนอข้อเสนอโครงการ	๓๐ คะแนน
รวม	**๑๐๐ คะแนน**

หมายเหตุ : สำนักงาน ป.ป.ช. จะนำคะแนนทั้ง ๒ ตัวแปรหลักมาคำนวณเป็นร้อยละ เพื่อพิจารณาผลต่อไป

/โดยมีรายละเอียด...

โดยมีรายละเอียดหลักเกณฑ์การให้คะแนน ดังต่อไปนี้

(๑) ผลงานที่ผ่านมา ๒๐ คะแนน

การพิจารณาในส่วนนี้พิจารณาจากจำนวนโครงการที่มีลักษณะที่เกี่ยวข้องกับการทดสอบเจาะระบบสารสนเทศ และได้รับการยอมรับด้านคุณภาพงาน โดยสำนักงาน ป.ป.ช. **พิจารณาจากหนังสือรับรองผลงานของหน่วยงาน โดยต้องมีหัวหน้าหน่วยงาน หรือผู้ทำการแทนหน่วยงานนั้นทำการรับรอง และสำเนาสัญญาจ้าง หรือหนังสือสั่งจ้างที่ปรากฏวงเงินสัญญา และขอบเขตงานการทดสอบเจาะระบบสารสนเทศ ซึ่งแสดงถึงการทดสอบเจาะระบบสารสนเทศแล้วเสร็จ** ทั้งนี้ สำนักงาน ป.ป.ช. สงวนสิทธิ์ที่จะตรวจสอบวินิจฉัยข้อเท็จจริง โดยตรงจากผู้รับรอง

หลักเกณฑ์การให้คะแนน	สูตรการคำนวณ	คะแนน
๑) ผลงานการทดสอบเจาะระบบสารสนเทศให้แก่หน่วยงานภาครัฐ รัฐวิสาหกิจ หรือเอกชนในวงเงินไม่น้อยกว่า ๕ แสนบาท โดยเป็นสัญญาจ้างฯ ที่ทำมาไม่เกิน ๕ ปี นับถึงวันยื่นซองเสนอราคา (จำนวนโครงการ)	จำนวนโครงการ x ๑	ไม่เกิน ๕ คะแนน
๒) ผลงานการทดสอบเจาะระบบสารสนเทศให้แก่สถาบันการเงินภายในประเทศ ในวงเงินไม่น้อยกว่า ๕ แสนบาท โดยเป็นสัญญาจ้างฯ ที่ทำมาไม่เกิน ๕ ปี นับถึงวันยื่นซองเสนอราคา (จำนวนโครงการ)	จำนวนโครงการ x ๓	ไม่เกิน ๑๕ คะแนน
รวม		**๒๐ คะแนน**

(๒) บุคลากร/ทีมงาน ๓๐ คะแนน

การพิจารณาในส่วนนี้ประกอบด้วยหัวข้อการประเมิน ดังนี้

(๒.๑) คุณสมบัติและประสบการณ์ของหัวหน้าโครงการ (๑๕ คะแนน)

หลักเกณฑ์การให้คะแนน	สูตรการคำนวณ	คะแนน
๑) มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยระบบเครือข่ายสื่อสารและความปลอดภัยคอมพิวเตอร์อย่างน้อย ๕ ปี	**จำนวนปีประสบการณ์** ตั้งแต่ ๗ ปีขึ้นไป ๕ คะแนน ตั้งแต่ ๖ ปีขึ้นไป ๓ คะแนน ตั้งแต่ ๕ ปีขึ้นไป ๑ คะแนน	ไม่เกิน ๕ คะแนน
๒) มีประสบการณ์ในการบริหารโครงการตรวจสอบช่องโหว่ ประเมินและหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หน่วยงานภาครัฐ รัฐวิสาหกิจ หรือเอกชน	**จำนวนโครงการ** ๑ โครงการ ๑ คะแนน ๒ โครงการ ๓ คะแนน ๓ โครงการ ๕ คะแนน ตั้งแต่ ๔ โครงการขึ้นไป ๑๐ คะแนน	ไม่เกิน ๑๐ คะแนน
รวม		**๑๕ คะแนน**

หมายเหตุ : กรณีมีประสบการณ์ในการบริหารโครงการตรวจสอบช่องโหว่ ประเมินและหาจุดอ่อนของระบบเทคโนโลยีสารสนเทศของสถาบันการเงินจะได้รับคะแนนเพิ่ม ๓ คะแนน

/(๒.๒) คุณสมบัติ ...

(๒.๒) คุณสมบัติและประสบการณ์ของทีมงาน (ผู้เชี่ยวชาญเพื่อทดสอบเจาะระบบสารสนเทศ) (๑๕ คะแนน)

คะแนน: คำนวณจากคะแนนเฉลี่ยของบุคลากร/ทีมงานทั้งหมด

หลักเกณฑ์การให้คะแนน	สูตรการคำนวณ	คะแนน
๑) มีประสบการณ์ในการตรวจสอบช่องโหว่ ประเมิน และหาจุดอ่อนระบบเทคโนโลยีสารสนเทศของสถาบันการเงิน หน่วยงานภาครัฐ รัฐวิสาหกิจ เอกชน หรือหน่วยงานที่น่าเชื่อถือ ไม่เกิน ๓ ปีที่ผ่านมา	**<u>จำนวนโครงการ</u>** ๑ โครงการ ๑ คะแนน ๒ โครงการ ๓ คะแนน ตั้งแต่ ๓ โครงการขึ้นไป ๕ คะแนน	ไม่เกิน ๕ คะแนน
๒) ใบรับรอง (Certificate) ตามที่กำหนด	**จำนวนใบรับรอง** (Certificate) X ๒.๕	ไม่เกิน ๑๐ คะแนน
รวม		**๑๕ คะแนน**

<u>หมายเหตุ</u> กรณีมีประสบการณ์ในการตรวจสอบช่องโหว่ ประเมิน และหาจุดอ่อนระบบเทคโนโลยีสารสนเทศของสถาบันการเงินจะได้รับคะแนนเพิ่ม ๓ คะแนน

(๓) ข้อเสนอจัดกิจกรรมซ้อมรับมือภัยคุกคามทางไซเบอร์ (Cyber Drill) โดยวิธี Email Phishing (๒๐ คะแนน)

- มี<u>เสนอ</u> จัดกิจกรรมซ้อมรับมือภัยคุกคามทางไซเบอร์ (Cyber Drill) โดยวิธี Email Phishing ได้ ๒๐ คะแนน

- <u>ไม่มีเสนอ</u> จัดกิจกรรมซ้อมรับมือภัยคุกคามทางไซเบอร์ (Cyber Drill) โดยวิธี Email Phishing ได้ ๐ คะแนน

ทั้งนี้ กรณีที่ผู้เสนอราคาต้องการเสนอการจัดกิจกรรมดังกล่าวให้ระบุข้อเสนอการจัดกิจกรรมในเอกสารประกอบการพิจารณาการเข้าเสนอราคา

(๔) ข้อเสนอโครงการ ๓๐ คะแนน

๔.๑ แผนการดำเนินงาน ขั้นตอนการดำเนินงาน และขั้นตอนการประเมินความเสี่ยง เช่น การจำแนกความเสี่ยง คำอธิบายความเสี่ยง และรูปแบบรายงานผลการวิเคราะห์และผลการทดสอบเจาะระบบสารสนเทศ (๑๐ คะแนน)

๔.๒ Methodology กระบวนการ เครื่องมือ เทคนิค หรือวิธีการที่ใช้ในการประเมินความมั่นคงปลอดภัยและตรวจสอบค้นหาช่องโหว่ของระบบสารสนเทศ และชุดคำสั่ง (Source Code) และแนวทางการบริหารการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงจากภัยคุกคามคอมพิวเตอร์ที่อาจจะเกิดขึ้น (๑๐ คะแนน)

๔.๓ แนวคิดการบริหารจัดการศูนย์ปฏิบัติการด้านความปลอดภัย (Security Operations Center: SOC) (๑๐ คะแนน)

/๑. แผนการดำเนินงาน ...

หลักเกณฑ์การให้คะแนน	คะแนน
๑. แผนการดำเนินงาน ขั้นตอนการดำเนินงาน และการประเมินความเสี่ยง เช่น การจำแนกความเสี่ยง คำอธิบายความเสี่ยง และรูปแบบรายงานผลการวิเคราะห์และผลการทดสอบเจาะระบบสารสนเทศให้กับสำนักงาน ป.ป.ช. สื่อถึงความเข้าใจในระดับใด - ไม่มีการนำเสนอ ได้ ๐ คะแนน - นำเสนอได้เข้าใจพอใช้ ได้ ๓ คะแนน - นำเสนอได้เข้าใจดี ได้ ๖ คะแนน - นำเสนอได้เข้าใจดีมาก ได้ ๑๐ คะแนน	๑๐
๒. Methodology กระบวนการ เครื่องมือ เทคนิค หรือวิธีการที่ใช้ในการประเมินความมั่นคงปลอดภัยและตรวจสอบค้นหาช่องโหว่ของระบบสารสนเทศ และชุดคำสั่ง (Source Code) และแนวทางการบริหารการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงจากภัยคุกคามคอมพิวเตอร์ที่อาจจะเกิดขึ้นสื่อถึงความเข้าใจในระดับใด - ไม่มีการนำเสนอ ได้ ๐ คะแนน - นำเสนอได้เข้าใจพอใช้ ได้ ๓ คะแนน - นำเสนอได้เข้าใจดี ได้ ๖ คะแนน - นำเสนอได้เข้าใจดีมาก ได้ ๑๐ คะแนน	๑๐
๓. แนวคิดการบริหารจัดการศูนย์ปฏิบัติการด้านความปลอดภัย (Security Operations Center: SOC) สื่อถึงความเข้าใจในระดับใด - ไม่มีการนำเสนอ ได้ ๐ คะแนน - นำเสนอได้เข้าใจพอใช้ ได้ ๓ คะแนน - นำเสนอได้เข้าใจดี ได้ ๖ คะแนน - นำเสนอได้เข้าใจดีมาก ได้ ๑๐ คะแนน	๑๐

ปัญหาขัดแย้งหรือการตีความ

ในกรณีที่มีความจำเป็นต้องตีความข้อใด หรือมีข้อความใดที่ขัดแย้งในการประกาศเสนอราคา หรือเอกสารเสนอราคา หรือในเอกสารอื่นใดก็ตาม ซึ่งมีความจำเป็นต้องวินิจฉัยเพื่อให้การเสนอราคาครั้งนี้เป็นไปด้วยความเรียบร้อยบรรลุวัตถุประสงค์ของสำนักงาน ป.ป.ช. สำนักงาน ป.ป.ช. สงวนสิทธิ์ที่จะเป็นผู้ตีความและวินิจฉัยข้อขัดแย้ง คำวินิจฉัยนี้ให้ถือเป็นอันเด็ดขาดและถึงที่สุด

สัญญาที่จะไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) และข้อตกลงในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) และการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สัญญาฉบับนี้ทำขึ้น ณ .....
วันที่.....ระหว่า ง "สำนักงาน ป.ป.ช."
โดย.....ซึ่งต่อไปนี้ เรียกว่า **"ผู้ให้ข้อมูล"** ฝ่ายหนึ่ง
กับ.....โดย.....
ซึ่งต่อไปนี้ เรียกว่า **"ผู้รับข้อมูล"** อีกฝ่ายหนึ่ง ทั้งสองฝ่ายได้ตกลงกัน โดยมีความตกลงดังต่อไปนี้

ข้อ ๑ คำนิยาม

"ข้อมูล" หมายความถึง บรรดาข้อความ เอกสาร ข้อมูล ตลอดจนรายละเอียดทั้งปวงที่เป็นของผู้ให้ข้อมูล ทั้งที่อยู่ในความควบคุมหรือครอบครองแม้จะไม่เป็นที่รับรู้ของสาธารณชนโดยทั่วไป และไม่ว่าจะอยู่ในรูปแบบหรือสื่อแบบใด ไม่ว่าจะถูกทำซ้ำ แก้ไข ดัดแปลง โดยผู้รับข้อมูลหรือไม่

"ข้อมูลส่วนบุคคล" หมายความถึง ข้อมูลเกี่ยวกับบุคคล ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ข้อ ๒ วัตถุประสงค์

ผู้รับข้อมูลและผู้ให้ข้อมูลตกลงที่จะให้มีการรักษาข้อมูลเป็นความลับตามสัญญาฉบับนี้ ภายใต้โครงการหรือกิจกรรมหรือสัญญาจ้างหรือบันทึกข้อตกลง ที่.....
.....เรื่อง..... .....
.....ลงวันที่..... ระหว่างสำนักงาน ป.ป.ช.
กับ..... .....
เพื่อให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ซึ่งต่อไปนี้ในสัญญาฉบับนี้ เรียกว่า "กิจกรรมตามสัญญา"

ข้อ ๓ การรักษาข้อมูลเป็นความลับ

๓.๑ ผู้รับข้อมูลตกลงว่าจะรักษาข้อมูลและเก็บข้อมูลไว้เป็นความลับโดยครบถ้วนและเคร่งครัด ผู้รับข้อมูลจะต้องไม่เปิดเผยข้อมูลหรือทำการอื่นใดในทำนองเดียวกันไม่ว่าทั้งหมดหรือบางส่วน ตลอดระยะเวลาตามกิจกรรมตามสัญญาและตลอดไป

๓.๒ ผู้รับข้อมูลตกลงจะไม่เปิดเผยข้อมูลไม่ว่าทั้งหมดหรือแต่บางส่วนต่อบุคคลอื่นหรือองค์กรใดทราบโดยมิได้รับอนุญาตเป็นหนังสือจากผู้ให้ข้อมูล เว้นแต่กรณีจำต้องเปิดเผยตามกฎหมาย คำสั่งศาลหรือเจ้าพนักงานของรัฐ หรือหน่วยงานที่มีอำนาจกำกับดูแลที่อาศัยอำนาจตามกฎหมาย

/๓.๓ ...

๓.๓ ผู้รับข้อมูลตกลงที่จะควบคุมมิให้พนักงาน ลูกจ้าง ผู้รับจ้าง หรือตัวแทนของตนล่วงรู้หรือสามารถเข้าถึงข้อมูลนั้น เว้นแต่บุคคลเหล่านั้น ได้รับมอบหมายหรือมีหน้าที่เกี่ยวข้อง หรือมีความจำเป็นในการเข้าถึงข้อมูล และตกลงที่จะควบคุมบุคคลเหล่านั้น มิให้เปิดเผยข้อมูลไม่ว่าด้วยวิธีการใด ๆ และไม่ว่าทั้งทางตรงและทางอ้อมแก่บุคคลอื่นใด

๓.๔ ผู้รับข้อมูลตกลงใช้มาตรการที่เหมาะสมในการเก็บรักษาข้อมูล เพื่อป้องกันมิให้ข้อมูลถูกนำไปใช้โดยมิได้รับอนุญาตหรือถูกเปิดเผยแก่บุคคลใด โดยผู้รับข้อมูลต้องใช้มาตรการการเก็บรักษาข้อมูลในระดับเดียวกันกับที่ผู้รับข้อมูลใช้กับข้อมูลของตน และต้องไม่น้อยกว่าระดับที่วิญญูชนที่ประกอบวิชาชีพเช่นนั้น พึงรักษาข้อมูลของตน โดยเฉพาะข้อมูลส่วนบุคคลที่ต้องดำเนินการเก็บรักษาข้อมูล ส่วนบุคคลให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๓.๕ ผู้รับข้อมูลตกลงที่จะปฏิบัติตามประกาศสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔ ตลอดจนกฎหมาย ระเบียบ หลักเกณฑ์ วิธีการ หรือเงื่อนไขเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศซึ่งใช้บังคับทั้งที่ใช้บังคับอยู่ ณ วันทำสัญญา รวมถึงที่ได้มีการแก้ไขในอนาคต

๓.๖ ผู้รับข้อมูลตกลงที่จะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสม ทั้งในเชิงองค์กรและเชิงเทคนิค ตามประกาศที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดและเป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดในสัญญาฉบับนี้

๓.๗ ผู้รับข้อมูลตกลงที่จะดำเนินการตามข้อ ๓ แห่งสัญญาฉบับนี้ ตลอดระยะเวลาตามกิจกรรมตามสัญญา และตลอดไป

ข้อ ๔ การเปิดเผยข้อมูล

ผู้ให้ข้อมูลและผู้รับข้อมูล ตกลงให้เปิดเผยข้อมูลที่ผู้รับข้อมูลได้รับจากผู้ให้ข้อมูลตามสัญญาฉบับนี้ ในกรณีดังต่อไปนี้

๔.๑ ข้อมูลที่อยู่ในการรับรู้ การครอบครอง หรือการควบคุม ไม่ว่าด้วยวิธีใดของผู้รับข้อมูลที่ได้รับข้อมูลเหล่านั้นมาโดยชอบด้วยกฎหมาย ก่อนที่จะได้รับข้อมูลนั้นจากผู้ให้ข้อมูล

๔.๒ ข้อมูลที่เป็นที่รับรู้กันโดยทั่วไปหรือที่เป็นการรู้กันอย่างแพร่หลายในเวลาที่ได้รับข้อมูลนั้น ซึ่งไม่ได้เป็นผลมาจากการละเมิดหรือผิดเงื่อนไข ข้อกำหนดตามกิจกรรมตามสัญญาโดยผู้รับข้อมูล

๔.๓ ข้อมูลที่ผู้รับข้อมูลได้รับรู้มาจากบุคคลอื่นที่มีสิทธิให้ข้อมูลและไม่มีหน้าที่ต้องปกปิดข้อมูลตามสัญญาฉบับนี้

๔.๔ ข้อมูลที่เป็นข้อมูลสาธารณะอันประชาชนทั่วไปเข้าถึงข้อมูลได้

/๔.๕ ...

๔.๕ ข้อมูลที่ต้องเปิดเผยตามกฎหมาย ตามคำสั่งศาลหรือเจ้าพนักงานของรัฐหรือหน่วยงานที่มีอำนาจกำกับดูแลที่อาศัยอำนาจตามกฎหมาย โดยผู้รับข้อมูลต้องมีหนังสือแจ้งให้ผู้ให้ข้อมูลได้ทราบถึงข้อกฎหมายตามกฎหมาย หรือคำสั่งดังกล่าว พร้อมทั้งหมายศาลหรือคำสั่งของเจ้าพนักงานของรัฐอื่นใด ก่อนดำเนินการเปิดเผยข้อมูลดังกล่าว

๔.๖ ข้อมูลที่เปิดเผยโดยได้รับความเห็นชอบเป็นหนังสือจากผู้ให้ข้อมูลเป็นลายลักษณ์อักษรก่อนที่ผู้รับข้อมูลจะเปิดเผยข้อมูลนั้น

ข้อ ๕ ข้อกำหนดและการใช้ข้อมูล

๕.๑ ผู้รับข้อมูลตกลงใช้ข้อมูลและข้อมูลส่วนบุคคล เฉพาะแต่การใดเพื่อให้บรรลุวัตถุประสงค์ที่กำหนดไว้ในสัญญาเท่านั้น

๕.๒ ผู้รับข้อมูลตกลงจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing) ทั้งหมดที่ประมวลผลในขอบเขตของกิจกรรมตามสัญญาและตกลงส่งมอบบันทึกรายการดังกล่าวให้แก่ผู้ให้ข้อมูลก่อนการประมวลผลข้อมูลหรือเมื่อมีการเปลี่ยนแปลงในกระบวนการประมวลผลข้อมูลทันทีที่ผู้ให้ข้อมูลร้องขอ

๕.๓ ผู้รับข้อมูลตกลงที่จะดำเนินการเพื่อช่วยเหลือผู้ให้ข้อมูลในการดำเนินการตามคำร้องขอที่เจ้าของข้อมูลส่วนบุคคลแจ้งต่อผู้ให้ข้อมูลที่เป็นการใช้สิทธิตามกฎหมายของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในขอบเขตของกิจกรรมตามสัญญา

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลต่อผู้รับข้อมูลโดยตรงนั้น ผู้รับข้อมูลตกลงจะดำเนินการแจ้งและส่งคำร้องขอดังกล่าวให้ผู้ให้ข้อมูลทันที โดยผู้รับข้อมูลจะตกลงที่จะไม่ดำเนินการตามคำร้องขอดังกล่าวเว้นแต่จะได้รับมอบหมายจากผู้ให้ข้อมูลเป็นลายลักษณ์อักษรให้ดำเนินการแทนผู้ให้ข้อมูล

ข้อ ๖ การทำซ้ำหรือดัดแปลง และทำให้เสียรูปซึ่งข้อมูล

๖.๑ ผู้รับข้อมูลตกลงที่จะไม่ทำซ้ำหรือดัดแปลงข้อมูลและข้อมูลส่วนบุคคลและตกลงที่จะควบคุมมิให้พนักงาน ลูกจ้าง ผู้รับจ้าง หรือตัวแทนของตนกระทำการดังกล่าวเช่นเดียวกัน

๖.๒ ผู้รับข้อมูลจะทำซ้ำหรือดัดแปลงข้อมูลและข้อมูลส่วนบุคคลมิได้ เว้นแต่เป็นการทำซ้ำหรือดัดแปลงเพื่อใช้ตามวัตถุประสงค์ที่กำหนดไว้ในสัญญาฉบับนี้ และกิจกรรมตามสัญญา

๖.๓ ผู้รับข้อมูลตกลงจะไม่กระทำการวิศวกรรมย้อนกลับ ถอดรหัส หรือกระทำการอื่นใดที่ให้เกิดผลในลักษณะเดียวกันต่อข้อมูล รวมทั้งไม่เคลื่อนย้าย พิมพ์ทับ หรือทำให้เสียรูปซึ่งสัญลักษณ์ที่แสดงเครื่องหมายสิทธิบัตร ลิขสิทธิ์ เครื่องหมายการค้า ตราสัญลักษณ์และเครื่องหมายอื่นใดที่แสดงความเป็นกรรมสิทธิ์ของต้นฉบับหรือสำเนาของข้อมูลที่ได้รับจาก ผู้ให้ข้อมูล

/ข้อ ๗ ...

ข้อ ๗ ทรัพย์สินทางปัญญา

ผู้ให้ข้อมูลและผู้รับข้อมูลตกลงกันว่าสัญญาฉบับนี้ ไม่มีผลเป็นการโอนสิทธิหรือการอนุญาตให้ใช้สิทธิ ไม่ว่าโดยตรงหรือโดยอ้อม ให้แก่ผู้รับข้อมูลที่ได้รับข้อมูล ซึ่งสิทธิบัตร ลิขสิทธิ์ การออกแบบ เครื่องหมายการค้า ตราสัญลักษณ์ รูปประดิษฐ์อื่นใด ชื่อทางการค้า ความลับทางการค้า หรือสิทธิอื่นใดภายใต้กฎหมายว่าด้วยทรัพย์สินทางปัญญา ไม่ว่าจดทะเบียนไว้ตามกฎหมายหรือไม่ก็ตาม หรือสิทธิอื่นใดของผู้ให้ข้อมูลซึ่งปรากฏอยู่หรือนำมาทำซ้ำไว้ในข้อมูล

ทั้งนี้ ผู้รับข้อมูลรวมถึงบุคคลที่เกี่ยวข้องกับข้อมูลตกลงจะไม่ยื่นขอรับสิทธิหรือขอจดทะเบียนใด ๆ ตามกฎหมายว่าด้วยทรัพย์สินทางปัญญา ตลอดจนไม่นำไปใช้ โดยไม่ได้รับการอนุญาตเป็นหนังสือจากผู้ให้ข้อมูลเกี่ยวกับรายละเอียดข้อมูลหรือส่วนหนึ่งส่วนใด

ข้อ ๘ เหตุละเมิดต่อข้อมูลและข้อมูลส่วนบุคคล

๘.๑ กรณีที่มีเหตุอันถือว่าเป็นความเสี่ยงที่จะก่อให้เกิดเหตุละเมิด หรือรับทราบข้อเท็จจริงอันเป็นพฤติการณ์ใด ๆ แก่ข้อมูลและข้อมูลส่วนบุคคลของผู้ให้ข้อมูลที่กระทำต่อการรักษาความมั่นคงปลอดภัยของข้อมูลนั้น ทั้งในส่วนของการประมวลผลภายใต้กิจกรรมตามสัญญา ซึ่งจะก่อให้เกิดความเสียหาย ลบ ทำลาย สูญหาย แก้ไข เปลี่ยนแปลง เข้าถึง ใช้ เปิดเผย หรือด้วยวิธีการใด ๆ อันเป็นการมิชอบด้วยกฎหมายนั้น ผู้รับข้อมูลตกลงที่จะแจ้งผู้ให้ข้อมูลทราบทันที

๘.๒ กรณีที่พบว่ามีเหตุละเมิดต่อข้อมูลและข้อมูลส่วนบุคคล ภายใต้กิจกรรมตามสัญญานั้น ผู้รับข้อมูลตกลงที่จะใช้มาตรการตามที่เหมาะสมในการระบุสาเหตุของการละเมิดและป้องกันเหตุละเมิดดังกล่าวมิให้เกิดซ้ำ รวมทั้งต้องแจ้งรายละเอียดตามขอบเขตที่กฎหมายกำหนด ภายใน ๔๘ ชั่วโมงนับแต่เกิดเหตุละเมิดต่อผู้ให้ข้อมูลอันประกอบไปด้วยรายละเอียดของเหตุละเมิด รวมถึงประเภทของข้อมูลและเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิดและผลกระทบที่ได้รับ ตลอดจนมาตรการตอบสนองอื่น ๆ เพื่อบรรเทาผลกระทบความเสียหายทั้งในส่วนข้อมูลที่ถูกละเมิดและข้อมูลอื่น ๆ ที่เกี่ยวข้อง

๘.๓ ผู้รับข้อมูลตกลงให้ผู้ให้ข้อมูลใช้สิทธิทางศาลเพื่อขอให้ศาลมีคำสั่งใด ๆ ให้ผู้รับข้อมูลยับยั้งการกระทำการใด ๆ หรือกระทำการใด ๆ ที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามสัญญาฉบับนี้ไม่ว่าข้อใดข้อหนึ่ง

ข้อ ๙ การชดใช้ค่าเสียหาย

๙.๑ กรณีที่ผู้รับข้อมูล พนักงาน ลูกจ้าง ผู้รับจ้างหรือตัวแทนของตนฝ่าฝืนหรือไม่ปฏิบัติตามสัญญาฉบับนี้ไม่ว่าข้อใดข้อหนึ่งนั้น ผู้รับข้อมูลตกลงจะชดใช้ค่าเสียหาย โดยสิ้นเชิงให้แก่ผู้ให้ข้อมูลและ/หรือบุคคลที่มีสิทธิในการใช้ข้อมูลของผู้ให้ข้อมูลที่ได้รับความเสียหาย โดยต้องชดใช้ค่าเสียหายภายใน ๓๐ (สามสิบ) วัน นับแต่วันที่ได้รับแจ้งเป็นหนังสือจากผู้ให้ข้อมูล

/๙.๒ ...

๙.๒ กรณีที่ผู้ให้ข้อมูลใช้สิทธิทางศาลอันเนื่องมาจากการกระทำที่ผู้รับข้อมูลฝ่าฝืนหรือไม่ปฏิบัติตามสัญญาฉบับนี้ไม่ว่าข้อใดข้อหนึ่งหรือผู้ให้ข้อมูลได้รับความเสียหายจากการกระทำเช่นว่านั้น ผู้รับข้อมูลตกลงเป็นผู้รับผิดชอบค่าใช้จ่าย ๆ ต่างที่เกิดขึ้นในการดำเนินการดังกล่าว

ข้อ ๑๐ การส่งคืน ลบ หรือการทำลายข้อมูล

๑๐.๑ เมื่อกิจกรรมตามสัญญาได้เสร็จสิ้นลงตามวัตถุประสงค์ผู้รับข้อมูลตกลงส่งมอบข้อมูลตลอดจนสำเนาของข้อมูลที่ได้ทำซ้ำขึ้นไม่ว่าในรูปแบบใดที่ผู้รับข้อมูลได้รับและจัดทำขึ้นคืนให้แก่ผู้ให้ข้อมูลภายในระยะเวลาที่ผู้ให้ข้อมูลแจ้งเป็นหนังสือแก่ผู้รับข้อมูล

๑๐.๒ ผู้รับข้อมูลตกลงจะลบหรือทำลายข้อมูลและข้อมูลส่วนบุคคล ที่ถูกจัดเก็บไว้ในคอมพิวเตอร์ หรืออุปกรณ์อื่นใดที่ใช้จัดเก็บข้อมูล ตลอดจนที่ทำซ้ำไว้และจัดเก็บด้วยวิธีการอื่นใด (ถ้ามี) ตลอดจนดำเนินการอื่นตามที่ได้รับแจ้งเป็นหนังสือจากผู้ให้ข้อมูล รวมถึงต้องไม่กระทำการอื่นใดอันเป็นการใช้ข้อมูลและข้อมูลส่วนบุคคลที่ได้รับจากผู้ให้ข้อมูลทันที

ข้อ ๑๑ การบังคับใช้

๑๑.๑ หากผู้รับข้อมูลกระทำการฝ่าฝืนหรือผิดสัญญาฉบับนี้ข้อหนึ่งข้อใดผู้รับข้อมูลตกลงให้ผู้ให้ข้อมูลดำเนินการเรียกร้องตามข้อสัญญาและดำเนินการตามกฎหมายได้ทันที

๑๑.๒ กรณีที่ปรากฏในภายหลังว่าส่วนหนึ่งส่วนใดของสัญญาฉบับนี้เป็นโมฆะให้ถือว่าข้อกำหนดส่วนที่เป็นโมฆะไม่มีผลบังคับในสัญญานี้ และข้อกำหนดอื่นที่เหลืออยู่ในสัญญาฉบับนี้ยังคงใช้บังคับได้และมีผลอยู่อย่างสมบูรณ์

ทั้งนี้ สัญญาฉบับนี้ อยู่ภายใต้การบังคับใช้และตีความตามกฎหมายไทย

สัญญาฉบับนี้ทำขึ้นสองฉบับ มีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความโดยละเอียดทั้งหมด จึงได้ลงลายมือชื่อพร้อมทั้งประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยานและคู่สัญญาต่างยึดถือไว้ฝ่ายละหนึ่งฉบับ

ลงชื่อ..... ผู้ให้ข้อมูล	ลงชื่อ..... ผู้รับข้อมูล
(.....)	(.....)
ลงชื่อ.....พยาน	ลงชื่อ.....พยาน
(.....)	(.....)