(ร่าง) ขอบเขตของงาน (Terms of Reference : TOR)
โครงการป้องกันภัยคุกคามของสำนักงานกิจการยุติธรรมและศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม ประจำปีงบประมาณ พ.ศ. ๒๕๖๘

.....

๑. ความเป็นมา

ปัจจุบันหน่วยงานของรัฐใช้เทคโนโลยีและระบบดิจิทัลเป็นกลไกหลักในการขับเคลื่อนการปฏิบัติงาน ทำให้เผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) มากขึ้น สำนักงานกิจการยุติธรรมและศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม DXC มีการให้บริการบุคลากรภายในสำนักงาน และดำเนินการพัฒนาระบบเพื่อยกระดับบริการของสำนักงานกิจการยุติธรรม และศูนย์ DXC ทั้งด้านอุปกรณ์ ด้านระบบบริการ และระบบรักษาความมั่นคงปลอดภัย ในการวางกรอบการกำกับดูแล โดยศูนย์ DXC ได้ดำเนินการขอรับรองมาตรฐาน ISO/IEC 27001:2022 การบริหารจัดการความเสี่ยงทั้งด้านบุคลากร กระบวนการและเครื่องมือหรือเทคโนโลยี เพื่อลดผลกระทบต่อผู้ใช้งานและหน่วยงานที่เกี่ยวข้องโดยรวม พร้อมทั้งรับประกันคุณภาพการให้บริการว่ามีความมั่นคงปลอดภัยขั้นสูง

สำนักงานกิจการยุติธรรม จึงได้กำหนดแผนการดำเนินงานและกำหนดแนวทางการบริหารจัดการความเสี่ยงด้านไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมี (Maturity Level) ให้สอดคล้องกับระดับความเสี่ยงตั้งต้นของตนเอง โดยปัจจุบันศูนย์ DXC ต้องดำเนินการเตรียมการรองรับนโยบายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เนื่องจากปัจจุบัน มีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนและเสียหายให้แก่ เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าเทคโนโลยี ทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อันเป็นการล่วงละเมิดทำได้โดยง่าย จึงจำเป็นที่หน่วยงานของรัฐจะต้องคุ้มครองข้อมูลต่าง ๆ ของประชาชน โดยในปีงบประมาณ พ.ศ. ๒๕๖๕ แผนการดำเนินงานของศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม DXC ที่ได้มีการวางแนวทางการขับเคลื่อนในระยะ ๓ ปี และเสนอคณะกรรมการพัฒนาการบริหารงานยุติธรรมแห่งชาติที่ได้รับความเห็นชอบให้ดำเนินการแล้วนั้น สำนักงานกิจการยุติธรรม กระทรวงยุติธรรม จึงมีโครงการสำคัญ เพื่อปฏิบัติตามกฎหมายและสร้างความมั่นใจในการให้บริการของภาครัฐ ภายใต้คุณภาพของการบริการและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม รวมถึงจัดหาโปรแกรมตรวจจับมัลแวร์ป้องกันการโจมตีชั้นสูงบนเครื่องผู้ใช้งาน และเครื่องการปฏิบัติงานของบุคลากรภายในสำนักงานกิจการยุติธรรม ซึ่งปัจจุบันและในอนาคตมีการพัฒนาบริการประชาชนในรูปแบบออนไลน์มากขึ้น แต่ด้วยภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ มีแนวโน้มเพิ่มสูงขึ้นทุกปี และมีการพัฒนารูปแบบอย่างต่อเนื่อง โดยเฉพาะมัลแวร์สายพันธุ์ใหม่ จึงพบว่า ระบบเว็บไซต์ และระบบเครือข่ายของหน่วยงานรัฐยังคงมีความเสี่ยงต่อการโจมตี จึงจำเป็นต้องจัดหาอุปกรณ์และระบบที่ทันสมัยเพื่อสามารถใช้ในการวิเคราะห์ รับมือ และจัดการภัยคุกคามทางเทคโนโลยี (ไซเบอร์) ที่เกิดขึ้นได้อย่างเหมาะสมทันท่วงที สร้างความน่าเชื่อถือให้กับระบบสารสนเทศของสำนักงานกิจการยุติธรรมต่อไป

๒. วัตถุประสงค์

๒.๑ เพื่อให้ระบบ DXC มีความมั่นคงปลอดภัยและเป็นไปตาม Standard หรือ Compliance ที่มีการระบุให้ทำการทดสอบเจาะระบบเป็นประจำอย่างน้อยทุก ๆ ๑ ปี และสามารถเข้าถึงข้อมูลแสดงระดับความมั่นคงปลอดภัยได้ในรูปแบบที่เหมาะสมสำหรับผู้บริหารและผู้จัดการระบบ

๒.๒ เพื่อปรับปรุงระบบรักษาความปลอดภัยทางด้านไซเบอร์ของสำนักงานกิจการยุติธรรม ให้มีประสิทธิภาพดีขึ้น และใช้เป็นเครื่องมือในการเพิ่มประสิทธิภาพการปฏิบัติงานให้กับผู้ดูแลระบบ โดยลดความเสี่ยง และผลกระทบจากภัยคุกคามทางด้านไซเบอร์ที่จะส่งผลต่อการดำเนินงานของสำนักงานกิจการยุติธรรม

๒.๓ จัดหาระบบป้องกันการโจมตีทางไซเบอร์บนเว็บไซต์ เพื่อให้เว็บไซต์ของสำนักงานกิจการยุติธรรม ปลอดภัยจากการฝังสคริปต์โฆษณา และการพนันออนไลน์

๒.๔ จัดหาสิทธิ์การใช้งานและติดตั้งระบบตรวจจับการโจมตีและตอบสนองภัยคุกคามขั้นสูง (Extended. Detection and Response - XDR) ตรวจจับภัยคุกคามได้แบบเรียลไทม์

๓. เป้าหมายของโครงการ

๓.๑ ระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม สามารถรองรับข้อกำหนดในกฎหมายของประเทศ และมาตรฐานด้านความมั่นคงปลอดภัย และมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

๓.๒ จัดหามาตรการพื้นฐานสำหรับเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ ระบบตรวจจับป้องกันการโจมตี และตอบสนองภัยคุกคามขั้นสูงที่ใช้ระบบอัตโนมัติ และเครื่องผู้ใช้งานของสำนักงานกิจการยุติธรรม

๓.๓ เตรียมความพร้อมศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC Service) ที่จะขยายบริการให้ประชาชน และทำรองรับการโจมตีทางไซเบอร์บนเว็บไซต์ เพื่อให้เว็บไซต์ของสำนักงานกิจการยุติธรรม ปลอดภัยจากการฝังสคริปต์โฆษณา และการพนันออนไลน์

๔. ประโยชน์ที่คาดว่าจะได้รับ

๔.๑ ด้านผลผลิต

๔.๑.๑ มีซอฟต์แวร์สำหรับเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ กรณีมัลแวร์เรียกค่าไถ่ (Ransomware) บนเครื่องให้บริการ และเครื่องผู้ใช้งานของสำนักงานกิจการยุติธรรม

๔.๑.๒ มีซอฟต์แวร์สำหรับป้องกันการโดนฝังสคริปต์โฆษณา และการพนันออนไลน์บนเว็บไซต์ของสำนักงานกิจการยุติธรรม (OJA) ศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) และศูนย์ปฏิบัติการฐานข้อมูลกระบวนการยุติธรรม (NJADC)

๔.๑.๓ การทดสอบเจาะระบบเพื่อสำรวจหาช่องโหว่ Web Application ของสำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) และการทดสอบสแกนหาช่องโหว่โดยใช้เครื่องมืออัตโนมัติ (Vulnerability Assessment) ของสำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยน

ข้อมูลกระบวนการยุติธรรม (DXC) ซึ่งเป็นข้อกำหนดของ ISO/IEC 27001:2022 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔.๒ ด้านผลลัพธ์

๔.๒.๑ ระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม สามารถรองรับข้อกำหนดในกฎหมายของประเทศ และมาตรฐานด้านความมั่นคงปลอดภัย และมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

๔.๒.๒ ศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) มีการเตรียมความพร้อมด้านความมั่นคงปลอดภัยเพื่อขยายบริการให้ประชาชนในอนาคต

๕. <u>คุณสมบัติของผู้ยื่นข้อเสนอ</u>

๕.๑ มีความสามารถตามกฎหมาย

๕.๒ ไม่เป็นบุคคลล้มละลาย

๕.๓ ไม่อยู่ระหว่างเลิกกิจการ

๕.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๕.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๕.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๕.๗ เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๕.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอราคารายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานกิจการยุติธรรม ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๕.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

๕.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงานสิ่งของหรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้น ต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

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

๕.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

๑. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยหรือต่างประเทศซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ งบแสดงฐานะการเงิน ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ หมายถึง งบแสดงฐานะการเงินย้อนไปก่อนวันที่หน่วยงานของรัฐกำหนดให้เป็นวันยื่นข้อเสนอ ๑ ปีปฏิทิน เว้นแต่กรณีนิติบุคคบที่จัดตั้งขึ้นตามกฎหมายไทย หากวันยื่นข้อเสนอเป็นช่วงระยะเวลาที่กรมพัฒนาธุรกิจการค้ากำหนดให้นิติบุคคลยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ซึ่งจะอยู่ในช่วงเดือนมกราคม - เดือนพฤษภาคม ของทุกปี โดยนิติบุคคลที่เป็นผู้ยื่นข้อเสนอนั้นยังอยู่ในช่วงของการยื่นงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า คือ ช่วงเดือนมกราคม - เดือนพฤษภาคม กรณีนี้ให้สามารถยื่นงบแสดงฐานะการเงินย้อนไปอีก ๑ ปี ได้

๒. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๒ ล้านบาท

๓. สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอ ในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

๔. กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ สามารถดำเนินการได้ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย หรือบุคคลธรรมดาที่ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่ อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตาม

ประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือที่สำนักงานสาขารับรอง (กรณีได้มอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศหรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทย ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง จะเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทที่ธนาคารกลางต่างประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรองหรือสำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน

๕. กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ หรือบุคคลธรรมดาที่มิได้ถือสัญชาติไทยตามข้อ ๒ ข้อ ๓ และข้อ ๔ (๒) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารประกวดราคาในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e - GP) จนถึงวันเสนอราคา

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

๖. กรณีตาม ๑ - ๕ ยกเว้นสำหรับกรณี ดังต่อไปนี้

(๖.๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐภายในประเทศ

(๖.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย พ.ศ. ๒๔๘๓ และที่แก้ไขเพิ่มเติม

๕.๑๓ ผู้ยื่นข้อเสนอต้องได้รับการสนับสนุนทางเทคนิคโดยแสดงเอกสารรับรองการสนับสนุนทางเทคนิคตลอดอายุการรับประกันจากผู้ผลิตที่ระบุชื่อโครงการนี้มายื่นในวันนำเสนอราคา

๕.๑๔ ผู้ยื่นข้อเสนอต้องมีผลงาน ดังต่อไปนี้

๕.๑๔.๑ เคยมีผลงานขายพร้อมติดตั้งระบบการป้องกันบุกรุกทางไซเบอร์ เช่น Web Application Firewall และระบบตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยและภัยคุกคามพร้อมทำการตอบสนอง (Extended Detection and Response)

๕.๑๔.๒ เคยมีผลงานในการทำ Gap Analysis และผลงานในการวิเคราะห์ช่องโหว่และทดสอบเจาะระบบ กับหน่วยงานภาครัฐหรือหน่วยงานเอกชนที่มีความน่าเชื่อถือ

โดยมีมูลค่าผลงานรวมทั้งหมดไม่น้อยกว่า ๓,๘๐๐,๐๐๐ บาท (สามล้านแปดแสนบาทถ้วน) ย้อนหลังไม่เกิน ๕ ปี นับจากวันที่ยื่นข้อเสนอ โดยผู้ยื่นข้อเสนอต้องแนบสำเนาสัญญาคู่ฉบับหรือหนังสือรับรองการจ้างงานดังกล่าวมาพร้อมด้วย

๕.๑๕ ผู้ยื่นข้อเสนอต้องมีทีมงานในการดำเนินงานโครงการ ประกอบด้วย

๕.๑๕.๑ ผู้จัดการโครงการ (Project Manager) จำนวนอย่างน้อย ๑ คน โดยมีคุณสมบัติ ดังนี้

- มีวุฒิทางการศึกษาอย่างน้อยปริญญาตรี สาขาวิศวกรรมคอมพิวเตอร์ หรือสาขาวิทยาการคอมพิวเตอร์ หรือสาขาวิทยาศาสตร์คอมพิวเตอร์ หรือสาขาสารสนเทศศาสตร์
- มีอายุงานไม่น้อยกว่า ๕ ปี ในงานที่เกี่ยวข้องกับคอมพิวเตอร์
- มีประสบการณ์ในการเป็นผู้จัดการโครงการ (Project Manager) เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศไม่น้อยกว่า ๑ ปี และมีอย่างน้อย ๑ โครงการ ซึ่งมีมูลค่าไม่ต่ำกว่า ๑ ล้านบาท

๕.๑๕.๒ ผู้เชี่ยวชาญด้านทดสอบเจาะระบบ โดยมีประสบการณ์ในการทดสอบเจาะระบบไม่น้อยกว่า ๑๐ ปี จำนวนอย่างน้อย ๑ คน และจะต้องได้รับประกาศนียบัตรรับรองความสามารถตามข้อกำหนดอย่างใดอย่างหนึ่งดังนี้

- มีวุฒิทางการศึกษาอย่างน้อยปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ หรือวิศวกรรมคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้องด้านคอมพิวเตอร์
- มีประสบการณ์ที่เกี่ยวข้อง มีหน้าที่และความรับผิดชอบในโครงการอย่างน้อย ๑ โครงการ ซึ่งมีมูลค่าไม่ต่ำกว่า ๑ ล้านบาท
- ต้องได้รับการรับรอง หรือได้รับประกาศนียบัตรรับรองด้านความรู้ความสามารถทางด้านความมั่นคงปลอยภัยไซเบอร์จากหน่วยงานในระดับสากล อย่างใดอย่างหนึ่งดังนี้
  - GIAC Certified Network Penetration Testing (GPEN)
  - GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
  - OffSec Certified Professional (OSCP)
  - OffSec Certified Professional Plus (OSCP+)
  - Practical Network Penetration Tester (PNPT)
  - Certified Penetration Testing Specialist (CPTS)

๕.๑๕.๓ นักตรวจสอบช่องโหว่และนักทดสอบเจาะระบบ โดยมีประสบการณ์ ไม่น้อยกว่า ๓ ปี จำนวนอย่างน้อย ๒ คน และจะต้องได้รับประกาศนียบัตรรับรองความสามารถตามข้อกำหนดอย่างใดอย่างหนึ่งดังนี้

- มีวุฒิทางการศึกษาอย่างน้อยปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ หรือวิศวกรรมคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้องด้านคอมพิวเตอร์
- มีประสบการณ์ที่เกี่ยวข้อง มีหน้าที่และความรับผิดชอบในโครงการอย่างน้อย ๑ โครงการ ซึ่งมีมูลค่าไม่ต่ำกว่า ๑ ล้านบาท

- ต้องได้รับการรับรอง หรือได้รับประกาศนียบัตรรับรองด้านความรู้ความสามารถทางด้านความมั่นคงปลอยภัยไซเบอร์จากหน่วยงานในระดับสากล อย่างใดอย่างหนึ่งดังนี้

- GIAC Certified Network Penetration Testing (GPEN)
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- Offsec Certified Professional (OSCP)
- OffSec Certified Professional Plus (OSCP+)
- CREST Registered Penetration Tester (CRT)
- CREST Practitioner Security Analyst (CPSA)
- GIAC Web Application Penetration Tester (GWAPT)
- eLearnSecurity Certified Professional Penetration Tester (eCPPT)
- eLearnSecurity Web Application Penetration Tester (eWPT)
- Practical Network Penetration Tester (PNPT)
- Certified Penetration Testing Specialist (CPTS)

๕.๑๕.๔ ผู้เชี่ยวชาญซอฟต์แวร์ระบบตรวจจับและตอบสนองอัตโนมัติสำหรับบริหารจัดการโปรแกรมป้องกันไวรัสบนเครื่องลูกข่ายแบบรวมศูนย์ (Endpoint Detection and Response) จำนวนอย่างน้อย ๑ คน โดยมีคุณสมบัติ ดังนี้

- มีวุฒิทางการศึกษาอย่างน้อยปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ หรือวิศวกรรมคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้องด้านคอมพิวเตอร์
- มีประสบการณ์ที่เกี่ยวข้อง มีหน้าที่และความรับผิดชอบในโครงการอย่างน้อย ๑ โครงการ ซึ่งมีมูลค่าไม่ต่ำกว่า ๑ ล้านบาท
- มีใบรับรองผ่านการอบรม หรือได้รับ Certificate Endpoint Detection and Response

๕.๑๕.๕ ผู้เชี่ยวชาญซอฟต์แวร์ระบบป้องกันการโจมตีทางไซเบอร์บนเว็บไซต์ Web Application Firewall จำนวนอย่างน้อย ๑ คน โดยมีคุณสมบัติ ดังนี้

- มีวุฒิทางการศึกษาอย่างน้อยปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ หรือวิศวกรรมคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้องด้านคอมพิวเตอร์
- มีประสบการณ์ด้านการติดตั้ง การตั้งค่า และการบริการจัดการ Web Application Firewall อย่างน้อย ๑ โครงการ ซึ่งมีมูลค่าไม่ต่ำกว่า ๑ ล้านบาท
- มีใบรับรองผ่านการอบรม Web Application Firewall ที่เสนอในโครงการนี้

๖. ขอบเขตของงานที่จะดำเนินการจัดซื้อ

๖.๑ โปรแกรมป้องกันการโจมตีทางไซเบอร์บนเว็บไซต์ เพื่อให้เว็บไซต์ของสำนักงานกิจการยุติธรรมปลอดภัยจากการฝังสคริปต์โฆษณา และการพนันออนไลน์ จำนวน ๑ ลิขสิทธิ์ สำหรับ ๓ เว็บไซต์ โดยมีคุณลักษณะขั้นต่ำ หรือเทียบเท่า หรือดีกว่า ดังนี้

๖.๑.๑ เป็นผลิตภัณฑ์ที่ถูกจัดให้อยู่ใน Leader Quadrant ของ Gartner Magic Quadrant Web Application Firewall ปี ๒๐๒๒ หรือใหม่กว่าเป็นระบบ Cloud-WAF ที่ให้บริการในรูปแบบ Cloud Platform และสามารถใช้งานได้กับ Website จำนวน ๓ websites

๖.๑.๒ รองรับการใช้งานแบบ Data transfer ไม่น้อยกว่า 20 TB ต่อเดือน หรือแบบ 95 percentile cleaned-bandwidth ไม่น้อยกว่า 20 Mbps ต่อเดือน

๖.๑.๓ ต้องมี Data center หรือ Scrubbing Center หรือ Point of Presence ทั่วโลก ไม่น้อยกว่า ๕๐ แห่ง และอยู่ในประเทศไทยไม่น้อยกว่า ๑ แห่ง

๖.๑.๔ ระบบต้องได้รับการรับรองมาตรฐาน ISO 27001 และ SOC Type II เป็นอย่างน้อย

๖.๑.๕ สามารถป้องกันการโจมตีผ่านทางเว็บไซต์ตาม OWASP Web Application Top 10 เช่น Cryptographic Failures, Injection และ Server-Side Request Forgery ได้

๖.๑.๖ สามารถสร้างและกำหนดเงื่อนไข Web Firewall Policy แบบ Custom Security Rules ผ่าน Web UI ได้ เช่น Rate limit, Header value, URL, Parameter value, Method เป็นต้น

๖.๑.๗ สามารถกำหนด action ของ Rule ที่สร้างขึ้นมาเองได้ เช่น alert, block, require CAPTCHA, require Javascript และ log ได้

๖.๑.๘ สามารถตรวจจับและป้องกัน Backdoor ของเว็บไซต์ได้

๖.๑.๙ สามารถป้องกันการโจมตี DDoS attack Layer 3, Layer 4 และ Layer 7 ได้อัตโนมัติ โดยไม่มีผลกระทบต่อผู้ใช้งานปกติ หรือมี SLA สำหรับ DDoS mitigation ไม่เกิน ๓ วินาที

๖.๑.๑๐มีระบบ Bot Management โดยสามารถแยกกลุ่มของ Bots ที่เป็นกลุ่ม Good bots และกลุ่ม Bad bots ได้

๖.๑.๑๑มีระบบ Client classification โดยสามารถแสดงปริมาณ Bot และ Human และ Blocked Traffic พร้อมแสดงชื่อเครื่องมือของ Client ที่เรียกเข้ามาได้แบบ Real-time

๖.๑.๑๒ มีระบบป้องกัน Web DDoS attacks ที่ทำงานแบบอัตโนมัติ ไม่จำกัดจำนวนครั้ง และสามารถรองรับการโจมตีแบบ DDoS Volumetric Attacks ได้อย่างน้อย 6 Tbps โดยไม่ส่งผลกระทบต่อผู้ใช้งานปกติขณะเปิดระบบป้องกัน และไม่มีการคิดค่าบริการจากปริมาณการรับ-ส่งข้อมูลที่เกิดขึ้นจากการโจมตี

๖.๑.๑๓ สามารถทำ Client Side Detection เพื่อ Monitor การโจมตีข้อมูลฝั่งผู้ใช้งาน เช่น Skimming หรือ Magecart เป็นต้น

๖.๑.๑๔ สามารถทำ Delivery Policy เพื่อ Rewrite Request ได้ เช่น Redirect URL, Rewrite request URL, Rewrite request header, Remove request header, และ Remove request cookie

๖.๑.๑๕ สามารถ Cache Content ที่เป็น Static content ได้ และสามารถทำ Custom cache rule โดยระบุ URL ที่ต้องการได้

๖.๑.๑๖ สามารถทำ Tiered Caching หรือ Cache Shield ได้

๖.๑.๑๗ สามารถทำ Two-Factor Authentication กับ Web page ที่ต้องการได้ โดยผ่าน SMS หรือ Email หรือ Authenticator ได้อย่างน้อย ๕ ผู้ใช้งาน

๖.๑.๑๘ ระบบ Dashboard ต้องสามารถแสดงข้อมูล Traffic, Security และ Performance เช่น ประเทศต้นทางของผู้ใช้งาน และภัยคุกคามที่เกิดขึ้นกับเว็บไซต์ได้อย่างน้อย ๓๐ วัน ย้อนหลัง

๖.๑.๑๙ สามารถกำหนดสิทธิ์การเข้าใช้งาน Management Console โดยรองรับการทำ Two-Factor Authentication ผ่าน SMS หรือ Email หรือ Authentication

๖.๑.๒๐ สามารถทำ Sub-tenant หรือ Sub-account เพื่อแบ่งกลุ่มการบริหารจัดการเว็บไซต์ และ Admin user แยกกันได้

๖.๑.๒๑ สามารถส่ง Log ผ่านทาง API หรือ SFTP Server หรือ AWS S3 เพื่อจัดเก็บ Log ร่วมกับระบบ SIEM ที่มีอยู่ได้ โดยสามารถเลือกส่งในรูปแบบ CEF และ W3C และ LEEF ได้ หรือสามารถเข้าไปเก็บ Log ผ่าน API ได้

๖.๑.๒๒ สามารถกำหนดสิทธิ์การเข้าใช้งาน Management Console แบบ Role base ให้กับแต่ละ Administrator User ได้

๖.๑.๒๓ มี Real-time Dashboard โดยต้องสามารถแสดงข้อมูล ปริมาณ Requests, Cached Request, Bandwidth, PoP, Response time, Top Sources, Top URL และ Sample event ได้เป็นอย่างน้อย

๖.๑.๒๔ มีฐานข้อมูล IP Reputation สำหรับค้นหาและป้องกัน Bad reputation IP ตามระดับความเสี่ยงและประเภทของความเสี่ยงได้ เช่น TOR IP และ Anonymous Proxy IP

๖.๑.๒๕ มีรายงานสรุปการใช้งาน (Summary Report) แบบรายสัปดาห์ หรือ แบบรายเดือน

๖.๑.๒๖ สามารถจัดเก็บ Audit Event หรือ Trail หรือ Activity ได้ไม่น้อยกว่า ๗ ปี ตามมาตรฐาน SOX หรือหากระบบที่เสนอไม่สามารถจัดเก็บได้ตามข้อกำหนดดังกล่าว สามารถเสนอระบบจัดเก็บเพิ่มเติม (Log retention) โดยระยะเวลาจัดเก็บไม่น้อยกว่า ๗ ปี และหน่วยงานไม่เสียค่าใช้จ่ายเพิ่มเติม

๖.๑.๒๗ ลิขสิทธิ์ในนาม สำนักงานกิจการยุติธรรม

๖.๑.๒๘ จัดทำคู่มือการติดตั้งระบบ (Configuration) และจัดทำคู่มือการใช้งานระบบ (User Guide) โดยจัดพิมพ์เป็นเล่ม จำนวน ๕ เล่มพร้อม Soft Copy ทั้งในรูปแบบของ File Word และ PDF ลงใน Flash Drive จำนวน ๒ ชุด

๖.๑.๒๙ จัดฝึกอบรมการใช้งานระบบ โดยจัดหาวิทยากร สถานที่ พร้อมเอกสารการฝึกอบรมให้กับเจ้าหน้าที่ที่เกี่ยวข้อง จำนวนอย่างน้อย ๕ คน โดยผู้ขายเป็นผู้รับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งสิ้น

๖.๑.๓๐ ต้องได้รับการสนับสนุนทางเทคนิค โดยแสดงเอกสารรับรองการสนับสนุนทางเทคนิคตลอดอายุการรับประกันจากผู้ผลิตที่ระบุชื่อโครงการนี้มายื่นในวันนำเสนอราคา

๖.๑.๓๑ ในกรณีที่โปรแกรมเกิดความขัดข้องทำให้ไม่สามารถให้บริการได้อย่างถาวร หรือบริษัทผู้ให้การบริการเกิดปัญหาจนไม่สามารถให้บริการ หรือสนับสนุนผู้ขายจะต้องทำการจัดหาและติดตั้งโปรแกรมที่มีคุณสมบัติเทียบเท่ากันหรือดีกว่า เพื่อมาติดตั้งแทนโปรแกรมเดิมที่ได้เสนอมา โดยระยะเวลาของลิขสิทธิ์จะต้องมีระยะเวลา ๑ ปี นับตั้งแต่วันที่ติดตั้งให้กับสำนักงานกิจการยุติธรรม

๖.๒ โปรแกรมตรวจจับการโจมตีและตอบสนองภัยคุกคามขั้นสูง บนเครื่องลูกข่ายและเครื่องแม่ข่าย จำนวน ๑๘๐ ลิขสิทธิ์ ระยะเวลา ๑ ปี โดยมีคุณลักษณะขั้นต่ำหรือเทียบเท่า หรือดีกว่า ดังนี้

๖.๒.๑ ระบบป้องกัน, ตรวจจับ และโต้ตอบภัยคุกคามเพื่อเสริมสร้างความปลอดภัยให้กับเครื่องลูกข่าย และเครื่องคอมพิวเตอร์แม่ข่าย จำนวน ๑ ระบบ มีคุณลักษณะอย่างน้อย ดังต่อไปนี้

๖.๒.๑.๑ ต้องรองรับและสามารถป้องกัน Malware, Spyware, rootkit และ virus บนระบบปฏิบัติการ Windows 10, Windows 11, MacOS, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 และ Windows Server 2022 ได้

๖.๒.๑.๒ มีระบบบริหารจัดการได้ Software as a service เพื่อความยืดหยุ่นและบริหารจัดการ โปรแกรมป้องกันไวรัสจากส่วนกลาง ผ่านทาง web console เดียวได้

๖.๒.๑.๓ สามารถตรวจสอบ Malware แบบอ้างอิงจากฐานข้อมูล (Signature) และแบบวิเคราะห์พฤติกรรมอย่างน้อยดังนี้

- Virtual Patching หรือ Intrusion Prevention (HIPS)
- Behavior Monitoring และ Ransomware Protection
- ตรวจจับภัยคุกคามได้ทั้งแบบ Pre-Execute และ Runtime โดยใช้ Machine Learning

๖.๒.๑.๔ สามารถป้องกันช่องโหว่ทางเครือข่าย โดยที่ไม่จำเป็นต้องทำการติดตั้ง patches บนระบบปฏิบัติการเหล่านั้นจริงได้ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการ patches โดยที่ยังไม่ได้ทำการทดสอบการใช้งาน

๖.๒.๑.๕ สามารถป้องกัน Ransomware ด้วยพฤติกรรม และสามารถกู้คืนไฟล์เอกสารที่ถูกโจมตีด้วย Ransomware ได้โดยอัตโนมัติ

๖.๒.๑.๖ สามารถทำการป้องกันอันตรายที่มาจากทางเว็บไซต์ต่างๆ (Web Threats) ได้

๖.๒.๑.๗ มีความสามารถในการกำหนดสิทธิ์การใช้งาน เช่น Read, Read and Execute ให้กับอุปกรณ์ USB Storage devices และสามารถอนุญาตให้ใช้งาน USB Storage รวมถึงสามารถกำหนดเงื่อนไขสำหรับ Non-Storage Device ไม่ให้ใช้งานได้ เช่น Bluetooth adapter, IEEE 1394 interface, Print screen key เป็นต้น

๖.๒.๑.๘ ระบบป้องกันไวรัสบนเครื่องลูกข่ายสามารถป้องกันการหยุดการทำงานและถอดถอนการติดตั้ง โดยใช้รหัสผ่านได้

๖.๒.๑.๙ สามารถทำการป้องกันโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาตได้ (Application Control) ที่สามารถกำหนด Rule ได้ หรือเสนอระบบ Application Control เพิ่มเติม

๖.๒.๑.๑๐ สามารถทำการ Update ฐานข้อมูลไวรัส (pattern) จากเครื่องแม่ข่าย หรือจาก Cloud ของผลิตภัณฑ์ได้ โดยตรงในกรณีที่มีการนำเครื่องลูกข่ายไปใช้นอกระบบเครือข่าย และสามารถทำการ Update ฐานข้อมูลไวรัส (pattern) แบบ Incremental ได้เพื่อลดจำนวนขนาดในการ Download ฐานข้อมูล

๖.๒.๑.๑๑ สามารถกำหนดสิทธิ์ของผู้ดูแลระบบในระดับที่แตกต่างกันด้วยสิทธิ์ที่ต่างกันได้ (Role-based Administration)

๖.๒.๑.๑๒ สามารถสั่งงาน Isolate endpoint, remote shell, remote custom script, collect file, dump process memory, terminate process, add to block list และ submit file to Sandbox เพื่อตอบสนองต่อภัยคุกคามที่พบได้

๖.๒.๑.๑๓ สามารถออกรายงานการทำงานในรูปแบบ PDF และ CSV ได้เป็นอย่างน้อย

๖.๒.๑.๑๔ สามารถส่งไฟล์ที่ต้องสงสัย เพื่อไปวิเคราะห์ยังระบบ Sandbox as a Service โดยมีจำนวนการส่งไม่น้อยกว่า จำนวน agent ที่ติดตั้งในโครงการนี้เป็นอย่างน้อย

๖.๒.๑.๑๕ มีกระบวนการในการลบตัวอย่าง (sample) หรือไฟล์ต้องสงสัยออกไปจากระบบได้ หลังจากทำการวิเคราะห์ผ่าน Sandbox แล้ว

๖.๒.๑.๑๖ ข้อมูลที่ได้รับจากการวิเคราะห์ด้วยระบบ Sandbox จะต้องประกอบด้วยข้อมูล ดังนี้

- ระดับความรุนแรง
- File ต้องสงสัย
- File Hash
- File Path ที่ตรวจพบ
- Detection Name
- ประเภทของ File ต้องสงสัย
- ประเภทของของภัยคุกคาม

๖.๒.๑.๑๗ ผลรายงานหลังการวิเคราะห์ (Report) จะต้องถูกเก็บไว้บนระบบของเจ้าของผลิตภัณฑ์ เป็นเวลาอย่างน้อย ๑๘๐ วัน

๖.๒.๑.๑๘ มีระบบตรวจจับและโต้ตอบต่อภัยคุกคามข้ามเลเยอร์ (Extended Detection and Response) เพื่อการค้นหาและวิเคราะห์ภัยคุกคามที่มาจากหลายทิศทางแบบเชิงลึก

๖.๒.๑.๑๙ ระบบสามารถทำการเก็บข้อมูลหลักฐานต่าง ๆ ของเครื่องคอมพิวเตอร์ (Forensic Analysis) เพื่อตรวจสอบเหตุการณ์การทำงานของมัลแวร์ได้ย้อนหลังไม่น้อยกว่า ๓๐ วัน โดยมีการเก็บข้อมูลไว้บนบริการที่ได้รับมาตรฐาน ISO 27001 และ ISO 27017 เป็นอย่างน้อย

๖.๒.๑.๒๐ ตรวจสอบสิ่งที่เกิดขึ้น เช่น file, process, network communication, registry, task scheduler และ user activity ได้

๖.๒.๑.๒๑ วิเคราะห์ Flow การทำงานของมัลแวร์ โดยสร้างเป็นแผนภาพที่แสดง Root Cause Analysis หรือ Execution Profile ได้

๖.๒.๑.๒๒ สามารถแสดงข้อมูลการตรวจจับภัยคุกคาม โดยทำการแสดง MITRE ATT&CK Framework ของภัยคุกคามที่ตรวจพบได้

๖.๒.๑.๒๓ มีการทำงาน sweeping จากข้อมูลที่บันทึก โดยใช้ Threat Intelligence จากเจ้าของผลิตภัณฑ์เองและ External Source และสามารถเพิ่มแหล่งข้อมูลจาก STIX file, CSV file, TAXII Feeds, MISP เพื่อค้นหาการโจมตีที่เกิดขึ้นในองค์กรได้

๖.๒.๑.๒๔ แสดงการแจ้งเตือนที่สอดคล้องกับ Detection Models เพื่อทำการวิเคราะห์หาต้นเหตุที่แท้จริง และผลกระทบ (Root Cause and Impact Analysis) ซึ่งจะช่วยให้เข้าใจขอบเขตและความรุนแรงการแจ้งเตือนได้

๖.๒.๑.๒๕ มีหน้าจอแสดงการจัดลำดับความสำคัญและแจ้งเตือน เพื่อเพิ่มความสามารถในการมองเห็น ได้แก่ ดูรายละเอียดการดำเนินการเพิ่มเติม (Execution Profile), ระบุขอบเขตของผลกระทบ (Identify the Scope of Impact) และดำเนินการโต้ตอบ (Response Actions)

๖.๒.๑.๒๖ มีการแสดงแผนภาพการโจมตี (Observable Graph) เพื่อช่วยทำความเข้าใจเรื่องราวของการโจมตี และดูการกระทำของภัยคุกคามที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ได้

๖.๒.๑.๒๗ มี Public API เพื่อทำงานร่วมกับ SIEM และ SOAR ได้

๖.๒.๑.๒๘ เจ้าของผลิตภัณฑ์ถูกจัดอันดับให้อยู่ในกลุ่ม Leaders ของ Gartner Magic Quadrant ในกลุ่มผลิตภัณฑ์ Endpoint Protection Platforms ปี ๒๐๒๓ หรือ KuppingerCole XDR Leadership Compass Report ปี ๒๐๒๔ หรือปีล่าสุด หรือปีล่าสุดทั้งสองรายงาน

๖.๒.๑.๒๙ ผู้ขายต้องได้รับการสนับสนุนทางเทคนิค โดยแสดงเอกสารรับรองการสนับสนุนทางเทคนิคตลอดอายุการรับประกันจากผู้ผลิตที่ระบุชื่อโครงการนี้มายื่นในวันนำเสนอราคา

๖.๒.๒ อุปกรณ์ตรวจจับและวิเคราะห์ภัยคุกคามขั้นสูงในระดับเครือข่าย เพื่อเพิ่มประสิทธิภาพในการตรวจจับภัยคุกคามขั้นสูงในระดับเครือข่ายของเครื่องแม่ข่าย จำนวน ๑ ชุด โดยมีคุณลักษณะขั้นต่ำหรือเทียบเท่า หรือดีกว่า ดังนี้

๖.๒.๒.๑ เป็นอุปกรณ์ Hardware Appliance ออกแบบมาสำหรับระบบตรวจจับค้นหา แจ้งเตือน และรายงานอันตรายจากภัยต่าง ๆ (Threats) ในระบบเครือข่ายให้กับผู้ดูแลระบบได้

๖.๒.๒.๒ ระบบที่นำเสนอต้องมี Data Interface แบบ Ethernet 10/100/1000 ไม่ต่ำกว่า ๓ interfaces โดยไม่รวมกับ Management Interface

๖.๒.๒.๓ อุปกรณ์ที่นำเสนอต้องสามารถรองรับ Throughput ได้ไม่น้อยกว่า 500 Mbps

๖.๒.๒.๔ สามารถรับข้อมูล Traffic ด้วยวิธี Mirror หรือ SPAN จากอุปกรณ์ Network เช่น Switch, Router ได้ หรือเสนออุปกรณ์อื่นๆ เพิ่มเติมได้ โดยระบบอุปกรณ์ที่เสนอจะต้องรองรับ Throughput ในการตรวจสอบได้ไม่น้อยกว่า 500 Mbps

๖.๒.๒.๕ รองรับการตรวจหาภัยคุกคามจากกระแสข้อมูล (Traffic) ได้จาก Protocol CIFS/SMB, SMTP, POP3, HTTP และ DNS ได้เป็นอย่างน้อย และสามารถตรวจค้นการใช้งานโปรแกรมประยุกต์ต่างๆ เช่น Instant Messaging, Peer-to-peer, และ Streaming media ได้

๖.๒.๒.๖ สามารถตรวจจับการโจมตี แบบ APT (Advanced Persistent Threats), Malware, Ransomware และ Document Exploits ได้

๖.๒.๒.๗ มีระบบที่สามารถตรวจสอบไฟล์ที่ต้องสงสัยและวิเคราะห์พฤติกรรมของไฟล์โดยใช้ระบบ Sandbox โดยไม่ส่งตัวอย่างไฟล์ต้องสงสัยไปยังภายนอก หรือเสนออุปกรณ์ Sandbox เพิ่มเติมเพื่อให้เป็นไปตามข้อกำหนด

๖.๒.๒.๘ รองรับการวิเคราะห์ด้วย Sandbox ในข้อกำหนด ๖.๒.๒.๗ สำหรับไฟล์ประเภท Executable และ Microsoft Office เป็นอย่างน้อย

๖.๒.๒.๙ Sandbox มี Operating System สำหรับวิเคราะห์ไฟล์ต้องสงสัย ได้อย่างน้อย ดังนี้ Windows, Linux

๖.๒.๒.๑๐ สามารถตรวจสอบ Websites หรือ URL ที่ User พยายามเข้าใช้งานโดยใช้เทคโนโลยี Threat Intelligence บน Cloud ได้

๖.๒.๒.๑๑ สามารถดูการกระทำของภัยคุกคามที่เกิดขึ้นบนเครือข่าย (Network Analytics) เช่น Command and Control และ Lateral movement ได้

๖.๒.๒.๑๒ สามารถทำ Network Analytics ด้วย Machine Learning เพื่อทำ Threat Correlation ในการโจมตี โดยเก็บรวบรวมข้อมูลย้อนหลังได้อย่างน้อย ๖ เดือน เพื่อหาจุดตั้งต้นในการเข้ามาของการโจมตี Timeline ในการโจมตีผู้ใช้งานที่มีผลกระทบ รวมทั้งช่องทางที่ภัยคุกคามติดต่อสื่อสารได้

๖.๒.๒.๑๓ สามารถแสดงข้อมูลการตรวจจับภัยคุกคาม เช่น Timestamp, Source host, Destination host, Interested host, Threat description, Detection name, Threat, Detection type, MITRE ATT&CK Framework, Protocol, Detection severity, Attack phase, Virtual analyser risk level, Direction และ notable object ได้

๖.๒.๒.๑๔ มี Template ในการสร้าง Advanced report, Executive report, Host severity report, Summary report และ Threat detection report รวมทั้งสามารถ Export ออกมาในรูปแบบ PDF ได้

๖.๒.๒.๑๕ สามารถทำการเชื่อมต่อกับระบบตรวจจับและโต้ตอบต่อภัยคุกคามข้ามเลเยอร์ (Extended Detection and Response) เพื่อรับการแชร์ข้อมูลภัยคุกคามที่ตรวจค้นพบใหม่ (Suspicious object list synchronization) ระหว่างกันได้ และสามารถแชร์ข้อมูลดังกล่าวไปยังระบบรักษาความปลอดภัยบนเครื่องคอมพิวเตอร์ลูกข่าย และคอมพิวเตอร์แม่ข่ายที่เสนอในโครงการได้อย่างมีประสิทธิภาพ

๖.๒.๒.๑๖ ผลิตภัณฑ์ที่เสนอจะต้องเป็นผลิตภัณฑ์ภายใต้เจ้าของหรือแบรนด์เดียวกันกับระบบที่เสนอในข้อ ๖.๒.๑

๖.๒.๒.๑๗ อุปกรณ์ที่เสนอจะต้องมีสาขาของเจ้าของผลิตภัณฑ์ตั้งอยู่ในประเทศไทยเพื่อรองรับบริการหลังการขายและสนับสนุนทางเทคนิค พร้อมแสดงเอกสารรับรองการสนับสนุนทางเทคนิคตลอดอายุการรับประกันจากผู้ผลิตที่ระบุชื่อโครงการนี้มายื่นในวันนำเสนอราคา

๖.๒.๓ ลิขสิทธิ์ในนามสำนักงานกิจการยุติธรรม

๖.๒.๔ จัดทำคู่มือการติดตั้งระบบ (Configuration) และจัดทำคู่มือการใช้งานระบบ (User Guide) โดยจัดพิมพ์เป็นเล่ม จำนวน ๕ เล่มพร้อม Soft Copy ทั้งในรูปแบบของ File Word และ PDF ลงใน Flash Drive จำนวน ๒ ชุด

๖.๒.๕ จัดฝึกอบรมการใช้งานระบบ โดยจัดหาวิทยากร สถานที่ พร้อมเอกสารการฝึกอบรมให้กับเจ้าหน้าที่ที่เกี่ยวข้อง จำนวนอย่างน้อย ๕ คน โดยผู้ซื้อเป็นผู้รับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งสิ้น

๖.๒.๖ ในกรณีที่โปรแกรมเกิดความขัดข้องทำให้ไม่สามารถให้บริการได้อย่างถาวร หรือบริษัทผู้ให้การบริการเกิดปัญหาจนไม่สามารถให้บริการหรือสนับสนุน ผู้ขายจะต้องทำการจัดหาและติดตั้งโปรแกรมที่มีคุณสมบัติเทียบเท่ากันหรือดีกว่า เพื่อมาติดตั้งแทนโปรแกรมเดิมที่ได้เสนอมา โดยระยะเวลาของลิขสิทธิ์จะต้องมีระยะเวลา ๑ ปี นับตั้งแต่วันที่ติดตั้งให้กับสำนักงานกิจการยุติธรรม

๖.๓ ดำเนินการทดสอบเจาะระบบและสแกนหาช่องโหว่ระบบรักษาความปลอดภัยสำนักงานกิจการยุติธรรม ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ โดยผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัย ดำเนินการทดสอบเจาะระบบ (Annual Penetration Test) โดยดำเนินการดังนี้

๖.๓.๑ ผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยดำเนินการทดสอบเจาะระบบ เพื่อสำรวจหาช่องโหว่ Web Application ของระบบแลกเปลี่ยนกระบวนการยุติธรรมและ Web Application หรือระบบงานภายในที่มีความสำคัญของสำนักงานกิจการยุติธรรม โดยอ้างอิงแนวทางการเจาะระบบตามมาตรฐานสากลอย่างน้อย ดังนี้ OWASP Web Application Top 10 เวอร์ชันล่าสุด และ SANS/CWE TOP 25 Most Dangerous Software Errors เวอร์ชันล่าสุด

๖.๓.๒ ผู้ดำเนินการเจาะระบบและทดสอบสแกนหาช่องโหว่จะต้องเป็นบุคคลตามที่ผู้ขายระบุในข้อเสนอ หากบุคคลดังกล่าวไม่สามารถดำเนินการได้ ผู้ขายจะต้องหาบุคลากรที่มีคุณสมบัติเทียบเท่าหรือสูงกว่าเพื่อดำเนินการแทน โดยจะต้องได้รับความเห็นชอบจากให้สำนักงานกิจการยุติธรรมก่อนเริ่มดำเนินการ

๖.๓.๓ ผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยดำเนินการทดสอบเจาะระบบสำนักงานกิจการยุติธรรมผ่านเครือข่ายจากภายนอก (External Network Penetration Test) และผ่านระบบเครือข่ายภายใน (Internal Network Penetration Test) จำนวนทั้งสิ้นไม่เกินกว่า ๕๐ IP Address ตามที่สำนักงานกิจการยุติธรรมกำหนด

๖.๓.๔ ดำเนินการทดสอบสแกนหาช่องโหว่โดยใช้เครื่องมืออัตโนมัติ (Vulnerability Assessment) ของสำนักงานการยุติธรรม จำนวนทั้งสิ้นไม่เกินกว่า ๑๐๐ IP Address ตามที่สำนักงานกิจการยุติธรรมกำหนด พร้อมเสนอวิธีแก้ไขช่องโหว่ให้ทางสำนักงานกิจการยุติธรรม พิจารณาเพื่อเห็นชอบให้แก้ไขช่องโหว่ ในกรณีที่ไม่สามารถปิดช่องโหว่ที่พบได้หรือการปิดช่องโหว่แล้วมีผลกระทบรุนแรง จนทำให้ระบบไม่สามารถให้บริการได้ ให้เสนอแนวทางลดความเสี่ยงลดผลกระทบที่เกิดขึ้น

๖.๓.๕ วิเคราะห์และจัดทำเอกสารรายงานผลการทดสอบเจาะระบบ และเอกสารรายงานผลการสแกนหาช่องโหว่ โดยจัดทำเอกสารรูปแบบของเอกสาร (Hard Copy) จำนวน ๕ ชุด และรูปแบบไฟล์เอกสาร (Soft Copy) ทั้งในรูปแบบของ File Word และ PDF ลงใน Flash Drive จำนวน ๒ ชุด โดยเอกสารดังกล่าวประกอบด้วยหัวข้ออย่างน้อย ดังต่อไปนี้

๖.๓.๔.๑ บทสรุปสำหรับผู้บริหาร (Executive Summary)

๖.๓.๔.๒ ขอบเขตการดำเนินงาน

๖.๓.๔.๓ เกณฑ์ในการประเมินระดับความรุนแรงของช่องโหว่

๖.๓.๔.๔ สรุปผลการทดสอบและสรุปช่องโหว่ที่มีความเสี่ยงสูง

๖.๓.๔.๕ รายละเอียดช่องโหว่ที่ตรวจพบ

๖.๓.๔.๖ แนวทางการแก้ไข

๖.๓.๖ เมื่อสำนักงานกิจการยุติธรรมดำเนินการปิดช่องโหว่ตามระยะเวลาที่กำหนด ต้องดำเนินการตรวจสอบผลการปิดช่องโหว่ ครั้งที่ ๒ ด้วยเทคนิค และวิธีการเดิมพร้อมจัดทำและนำเสนอรายงานให้สำนักงานกิจการยุติธรรมทราบก่อนสิ้นสุดสัญญา โดยมีหัวข้อดังต่อไปนี้เป็นอย่างน้อย ประกอบด้วย ๑.) จำนวนช่องโหว่ที่ได้รับการแก้ไข ๒.) ช่องโหว่ที่ยังมีอยู่ และ ๓.) ช่องโหว่ใหม่ที่ได้รับการค้นพบจากการทดสอบเจาะระบบและการทดสอบสแกนหาช่องโหว่ ครั้งที่ ๒

๖.๓.๗ เข้าร่วมประชุมเพื่อหารือและให้คำปรึกษาหารือเพื่อจัดทำแนวทางดำเนินการปิดช่องโหว่ อย่างน้อย ๒ ครั้ง ตามรายงานผลการทดสอบ

๗. <u>กำหนดเวลาส่งมอบพัสดุ</u>

๑๘๐ วัน นับถัดจากวันลงนามในสัญญา

๘. <u>พื้นที่การดำเนินการ</u>

สำนักงานกิจการยุติธรรม อาคารรัฐประศาสนภักดี ชั้น ๙ ศูนย์ราชการเฉลิมพระเกียรติฯ ๘๐ พรรษา ถนนแจ้งวัฒนะ หลักสี่ กรุงเทพมหานคร

๙. <u>หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ</u>

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สำนักงานกิจการยุติธรรมจะพิจารณาจากราคารวม ตัดสินโดยใช้หลักเกณฑ์ราคาต่ำสุด หากปรากฏว่ามีผู้เสนอราคาต่ำสุดเท่ากันหลายราย จะพิจารณาราคาต่ำสุดของผู้ที่เสนอราคาในลำดับแรกเป็นผู้ชนะการยื่นข้อเสนอ

๑๐. <u>วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร</u>

๗,๗๐๐,๐๐๐.- บาท (เจ็ดล้านเจ็ดแสนบาทถ้วน)

๑๑. งวดงานและการจ่ายเงิน

สำนักงานกิจการยุติธรรมจะจ่ายเงินเป็นรายงวด ตามงวดการส่งมอบงาน จำนวน ๓ งวด ดังนี้

งวดที่ ๑ ร้อยละ ๓๕ ของวงเงินตามสัญญา เมื่อผู้ขายดำเนินการส่งมอบงาน ภายใน ๓๐ วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบเอกสารรูปแบบของเอกสาร (Hard Copy) จำนวน ๕ ชุด และรูปแบบไฟล์เอกสาร (Soft Copy) ทั้งในรูปแบบของ File Word และ PDF ลงใน Flash Drive จำนวน ๒ ชุด และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว ดังรายการต่อไปนี้

๑. แผนการดำเนินงานโครงการป้องกันภัยคุกคามของสำนักงานกิจการยุติธรรม และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม ประจำปีงบประมาณ พ.ศ. ๒๕๖๘

๒. สัญญาการรักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement)

๓. รายงานผลการทดสอบเจาะระบบ (Penetration Testing Report) ครั้งที่ ๑ ของสำนักงานกิจการยุติธรรม

๔. รายงานผลการทดสอบสแกนหาช่องโหว่โดยใช้เครื่องมืออัตโนมัติ (Vulnerability Assessment Report) : ครั้งที่ ๑ ของสำนักงานกิจการยุติธรรม

งวดที่ ๒ ร้อยละ ๕๐ ของวงเงินตามสัญญา เมื่อผู้ขายดำเนินการส่งมอบงาน ภายใน ๙๐ วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบเอกสารรูปแบบของเอกสาร (Hard Copy) จำนวน ๕ ชุด และรูปแบบไฟล์เอกสาร (Soft Copy) ทั้งในรูปแบบของ File Word และ PDF ลงใน Flash Drive จำนวน ๒ ชุด และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว ดังรายการต่อไปนี้

๑. โปรแกรมป้องกันการโจมตีทางไซเบอร์บนเว็บไซต์ เพื่อให้เว็บไซต์ของสำนักงานกิจการยุติธรรมปลอดภัยจากการฝังสคริปต์โฆษณาและ การพนันออนไลน์ จำนวน ๑ ลิขสิทธิ์ สำหรับ ๓ เว็บไซต์ (TOR ข้อ ๖.๑)

๒. โปรแกรมตรวจจับการโจมตีและตอบสนองภัยคุกคามขั้นสูงบนเครื่องลูกข่ายและเครื่องแม่ข่าย จำนวน ๑๘๐ ลิขสิทธิ์ (TOR ข้อ ๖.๒.๑)

๓. อุปกรณ์ตรวจจับและวิเคราะห์ภัยคุกคามขั้นสูงในระดับเครือข่าย เพื่อเพิ่มประสิทธิภาพในการตรวจจับภัยคุกคามขั้นสูงในระดับเครือข่าย ของเครื่องแม่ข่าย จำนวน ๑ ชุด (TOR ข้อ ๖.๒.๒)

๔. คู่มือการติดตั้งระบบ (Configuration) และจัดทำคู่มือการใช้งานระบบ (User Guide) สำหรับโปรแกรมป้องกันการโจมตีทางไซเบอร์บนเว็บไซต์ (TOR ข้อ ๖.๑.๒๘)

๕. คู่มือการติดตั้งระบบ (Configuration) และจัดทำคู่มือการใช้งานระบบ (User Guide) (TOR ข้อ ๖.๒.๔) สำหรับโปรแกรมตรวจจับการโจมตีและตอบสนองภัยคุกคามขั้นสูง (TOR ข้อ ๖.๒.๑)

๖. คู่มือการติดตั้งระบบ (Configuration) และจัดทำคู่มือการใช้งานระบบ (User Guide) (TOR ข้อ ๖.๒.๔) สำหรับอุปกรณ์ตรวจจับและวิเคราะห์ภัยคุกคามขั้นสูงในระดับเครือข่าย (TOR ข้อ ๖.๒.๒)

งวดที่ ๓ ร้อยละ ๑๕ ของวงเงินตามสัญญา เมื่อผู้ขายดำเนินการส่งมอบงาน ภายใน ๑๘๐ วัน นับถัดจากวันลงนามในสัญญา โดยส่งมอบเอกสารรูปแบบของเอกสาร (Hard Copy) จำนวน ๕ ชุด และรูปแบบไฟล์เอกสาร (Soft Copy) ทั้งในรูปแบบของ File Word และ PDF ลงใน Flash Drive จำนวน ๒ ชุด และคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้ว ดังรายการต่อไปนี้

๑. รายงานผลการทดสอบเจาะระบบ (Penetration Testing Report) ครั้งที่ ๒ ของสำนักงานกิจการยุติธรรม

๒. รายงานผลการทดสอบสแกนหาช่องโหว่โดยใช้เครื่องมืออัตโนมัติ (Vulnerability Assessment Report) : ครั้งที่ ๒ ของสำนักงานกิจการยุติธรรม

๓. รายงานผลการฝึกอบรม (TOR ข้อ ๖.๑.๒๙ และ ๖.๒.๕)

๔. รายงานสรุปผลการดำเนินโครงการ

๑๒. <u>อัตราค่าปรับ</u>

ค่าปรับตามแบบสัญญาซื้อขายแนบท้ายเอกสารประกวดราคาอิเล็กทรอนิกส์นี้ หรือข้อตกลง ซื้อขายเป็นหนังสือ ให้คิดในอัตราร้อยละ ๐.๒๐ ของราคาค่าสิ่งของที่ยังไม่ได้รับมอบต่อวัน

๑๓. <u>การรับประกันผลงาน</u>

ผู้ขายจะต้องรับประกันความชำรุดบกพร่องของอุปกรณ์ ซอฟต์แวร์และระบบ ดังนี้

๑๓.๑ โปรแกรมป้องกันการโจมตีทางไซเบอร์บนเว็บไซต์ เพื่อให้เว็บไซต์ของสำนักงานกิจการยุติธรรมปลอดภัยจากการฝังสคริปต์โฆษณาและการพนันออนไลน์ จำนวน ๑ ลิขสิทธิ์ สำหรับ ๓ เว็บไซต์ ตาม TOR ข้อ ๖.๑ เป็นระยะเวลาไม่น้อยกว่า ๑ ปี หลังจากส่งมอบ

๑๓.๒ ระบบป้องกัน, ตรวจจับ และโต้ตอบภัยคุกคามเพื่อเสริมสร้างความปลอดภัยให้กับเครื่องลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่าย จำนวน ๑ ระบบ ตาม TOR ข้อ ๖.๒.๑ เป็นระยะเวลาไม่น้อยกว่า ๑ ปี หลังจากส่งมอบ

๑๓.๓ อุปกรณ์ตรวจจับและวิเคราะห์ภัยคุกคามขั้นสูงในระดับเครือข่าย เพื่อเพิ่มประสิทธิภาพในการตรวจจับภัยคุกคามขั้นสูงในระดับเครือข่ายของเครื่องแม่ข่าย จำนวน ๑ ชุด ตาม TOR ข้อ ๖.๒.๒ เป็นระยะเวลาไม่น้อยกว่า ๑ ปี หลังจากส่งมอบ

๑๓.๔ ในกรณีที่มีข้อผิดพลาดอันเนื่องมาจากการติดตั้งอุปกรณ์ ซอฟต์แวร์ ที่เสนอมาในโครงการนี้ ผู้ขายต้องประสานกับสำนักงานกิจการยุติธรรมเพื่อดำเนินการแก้ไขและปรับปรุง ให้สามารถทำงานได้อย่างถูกต้องโดยเร็ว และให้เสร็จภายใน ๑๕ วัน นับแต่วันที่ได้รับแจ้งจากสำนักงานกิจการยุติธรรม โดยไม่ทำให้ระบบงานชะงักหรือเกิดความเสียหายแก่ทางราชการ

๑๓.๕ สามารถแจ้งเหตุได้ทุกวันทำการ ทั้งทางโทรศัพท์พื้นฐาน โทรศัพท์เคลื่อนที่ หรือจดหมายอิเล็กทรอนิกส์ (Email) และจะต้องดำเนินการชี้แจงรายละเอียด หรือปัญหา หรือแนวทางการแก้ไขภายใน ๔ ชั่วโมง หลังจากที่ได้รับการแจ้งเหตุแล้ว

๑๓.๖ หลังจากผู้ขายรับทราบปัญหาแล้ว ให้ดำเนินการประสานกับสำนักงานกิจการยุติธรรมเพื่อแก้ไขปัญหาเพื่อให้ระบบอยู่ในสภาพที่ใช้งานได้ดี ตามปกติพร้อมทั้งรายงานให้สำนักงานกิจการยุติธรรมทราบทุกครั้ง ภายใน ๕ วันทำการนับจากวันที่ตรวจสอบ/แก้ไขแล้วเสร็จ ยกเว้นกรณีที่มีความจำเป็นเร่งด่วน หากไม่ดำเนินการจะเสียหายกับราชการอย่างร้ายแรง สำนักงานกิจการยุติธรรมขอให้ผู้ขายเข้าดำเนินการแก้ไขทันที

๑๔. ข้อสงวนสิทธิ์

๑๔.๑ สำนักงานจะมีการลงนามในสัญญาหรือข้อตกลงหรือเป็นหนังสือต่อเมื่อพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๘ มีผลใช้บังคับ และได้รับจัดสรรงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๘ จากสำนักงานงบประมาณแล้ว และกรณีที่หน่วยงานของรัฐไม่ได้รับจัดสรรงบประมาณเพื่อการจัดซื้อจัดจ้างในครั้งดังกล่าว หน่วยงานของรัฐสามารถยกเลิกการจัดซื้อจัดจ้างได้

๑๔.๒ สำนักงานกิจการยุติธรรมสงวนสิทธิ์ที่จะบอกเลิกสัญญาซื้อขาย ในกรณีที่ผู้ขายไม่อาจทำสัญญาซื้อขายตามที่ได้เจรจาตกลงหรือมีเหตุจำเป็นอื่นๆ ที่เป็นอุปสรรคซึ่งทำให้ไม่สามารถดำเนินการซื้อขายได้ ให้ถือว่าเป็นอันยกเลิกไป ผู้ขายไม่มีสิทธิ์โต้แย่งและเรียกร้องค่าเสียหายใด ๆ ทั้งสิ้น

๑๔.๓ สำนักงานกิจการยุติธรรมขอสงวนสิทธิ์ในการเปลี่ยนแปลงบุคลากรหลักตามที่ระบุไว้ในข้อเสนอทั้งนี้ เพื่อประโยชน์ของราชการเป็นสำคัญ และจะต้องดำเนินการโดยไม่มีเงื่อนไข ยกเว้นได้รับการยินยอมจากผู้ซื้อ

๑๔.๔ ลิขสิทธิ์ในเอกสารทุกฉบับ ต้องเป็นกรรมสิทธิ์ของสำนักงานกิจการยุติธรรมและขอสงวนสิทธิ์มิให้ผู้ขายนำไปใช้ในกิจกรรมอื่นโดยไม่ได้รับการยินยอมจากสำนักงานกิจการยุติธรรม
