(ร่าง) ขอบเขตของงาน (Terms of Reference : TOR)
โครงการพัฒนาระบบรักษาความมั่นคงปลอดภัยสำนักงานกิจการยุติธรรม และศูนย์แลกเปลี่ยนข้อมูล กระบวนการยุติธรรม ประจำปี พ.ศ. ๒๕๖๗

.....

๑. ความเป็นมา

ปัจจุบันหน่วยงานของรัฐใช้เทคโนโลยีและระบบดิจิทัลเป็นกลไกหลักในการขับเคลื่อนการปฏิบัติงาน ทำให้เผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) มากขึ้น สำนักงานกิจการยุติธรรมและศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) มีการพัฒนาระบบและยกระดับบริการของสำนักงานกิจการยุติธรรมและศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) ทั้งด้านอุปกรณ์ ด้านระบบบริการ และระบบรักษาความมั่นคงปลอดภัยในการวางกรอบการกำกับดูแลด้วยการขอรับรองมาตรฐาน ISO/IEC 27001:2022 การบริหารจัดการความเสี่ยงทั้งด้านบุคลากร กระบวนการ และเครื่องมือหรือเทคโนโลยี เพื่อลดผลกระทบต่อผู้ใช้งานและหน่วยงานที่เกี่ยวข้องโดยรวม พร้อมทั้งรับประกันคุณภาพการให้บริการว่ามีความมั่นคงปลอดภัยขั้นสูง

สำนักงานกิจการยุติธรรม กระทรวงยุติธรรม จึงได้กำหนดแผนการดำเนินงานและกำหนดแนวทางการบริหารจัดการความเสี่ยงด้านไซเบอร์และมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยที่พึงมี (Maturity Level) ให้สอดคล้องกับระดับความเสี่ยงตั้งต้นของตนเอง โดยปัจจุบันสำนักงานกิจการยุติธรรมและศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) ต้องดำเนินการเตรียมการรองรับนโยบายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมาก จนสร้างความเดือดร้อน เสียหาย ให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดทำได้โดยง่าย จึงจำเป็นที่หน่วยงานของรัฐจะต้องคุ้มครองข้อมูลต่าง ๆ ของประชาชน โดยในปีงบประมาณ พ.ศ. ๒๕๖๗ สำนักงานกิจการยุติธรรม กระทรวงยุติธรรม จึงมีโครงการสำคัญเพื่อปฏิบัติตามกฎหมาย และสร้างความมั่นใจในการให้บริการของภาครัฐภายใต้คุณภาพของการบริการและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม รวมถึงจัดหาโปรแกรมตรวจจับมัลแวร์ป้องกันการโจมตีขั้นสูงบนเครื่องผู้ใช้งานและเครื่องการปฏิบัติงานของบุคลากรภายในสำนักงานกิจการยุติธรรม ซึ่งปัจจุบันและในอนาคตมีการพัฒนาบริการประชาชนในรูปแบบออนไลน์มากขึ้น แต่ด้วยภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศมีแนวโน้มเพิ่มสูงขึ้นทุกปี และมีการพัฒนารูปแบบอย่างต่อเนื่อง โดยเฉพาะมัลแวร์สายพันธุ์ใหม่ จึงพบว่าระบบเว็บไซต์และระบบเครือข่ายของหน่วยงานรัฐยังคงมีความเสี่ยงต่อการโจมตี จึงจำเป็นต้องจัดหาอุปกรณ์และระบบที่ทันสมัยเพื่อเพิ่มความสามารถในการวิเคราะห์ รับมือ และจัดการภัยคุกคามทางเทคโนโลยี (ไซเบอร์) ที่เกิดขึ้นได้อย่างเหมาะสม ทันท่วงที สร้างความน่าเชื่อถือให้กับระบบสารสนเทศของสำนักงานกิจการยุติธรรมและศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) ต่อไป

๒. วัตถุประสงค์

๒.๑ เพื่อให้มีความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์สำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) ให้เป็นไปตาม Standard หรือ Compliance ที่มีการระบุให้ทำการทดสอบเจาะระบบเป็นประจำทุกปี และสามารถแสดงระดับความมั่นคงปลอดภัยได้ในรูปแบบที่เหมาะสมสำหรับผู้บริหารและผู้จัดการดูแลระบบ

๒.๒ เพื่อมีมาตรการที่เหมาะสมสำหรับการรักษาความมั่นคงปลอดภัยข้อมูล ให้สามารถวางกลยุทธ์ในการจัดการความมั่นคงปลอดภัย และเชิงปฏิบัติการตอบโจทย์ทั้งข้อกำหนดในกฎหมายของประเทศและมาตรฐานด้านความมั่นคงปลอดภัยในระดับสากล

๒.๓ เพื่อจัดหาโปรแกรมตรวจจับมัลแวร์ป้องกันการโจมตีชั้นสูงบนเครื่องแม่ข่ายและเครื่องผู้ใช้งานของสำนักงานกิจการยุติธรรม

๒.๔ เพื่อเตรียมความพร้อมรองรับการพัฒนาและปรับปรุงงานตามนโยบาย รองรับมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS) ในขอบเขตบริการ DATA SERVICE ที่จะทำการขยายบริการให้แก่หน่วยงานภาครัฐ และประชาชนในอนาคต

๓. เป้าหมายของโครงการ

๓.๑ ศูนย์คอมพิวเตอร์สำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) สามารถรองรับข้อกำหนดในกฎหมายของประเทศและมาตรฐานด้านความมั่นคงปลอดภัย และมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

๓.๒ มีมาตรการพื้นฐานสำหรับเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ กรณีมัลแวร์เรียกค่าไถ่ (Ransomware) บนเครื่องให้บริการ และเครื่องผู้ใช้งานของสำนักงานกิจการยุติธรรม

๓.๓ เตรียมความพร้อมศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC Service) ที่จะขยายบริการให้แก่หน่วยงานภาครัฐ และประชาชนในอนาคต

๔. ประโยชน์ที่คาดว่าจะได้รับ

๔.๑ ด้านผลผลิต

๔.๑.๑ มีซอฟต์แวร์สำหรับเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ กรณีมัลแวร์เรียกค่าไถ่ (Ransomware) บนเครื่องให้บริการ และเครื่องผู้ใช้งานของสำนักงานกิจการยุติธรรม

๔.๑.๒ การทดสอบเจาะระบบเพื่อสำรวจหาช่องโหว่ Web Application ของสำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) และการทดสอบสแกนหาช่องโหว่โดยใช้เครื่องมืออัตโนมัติ (Vulnerability Assessment) ของสำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) ซึ่งเป็นข้อกำหนดของ ISO/IEC 27001:2022 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔.๑.๓ แนวทางปรับปรุงงานตามนโยบาย รองรับมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS) ในขอบเขตบริการ DATA SERVICE ที่จะทำการขยายบริการให้แก่หน่วยงานภาครัฐและประชาชนในอนาคต

๔.๒ ด้านผลลัพธ์

๔.๒.๑ ศูนย์คอมพิวเตอร์สำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) สามารถรองรับข้อกำหนดในกฎหมายของประเทศและมาตรฐานด้านความมั่นคงปลอดภัย และมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

๔.๒.๒ ศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) มีการเตรียมความพร้อมด้านความมั่นคงปลอดภัยเพื่อขยายบริการให้ประชาชนในอนาคต

๕. คุณสมบัติของผู้ยื่นข้อเสนอ

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 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สำนักงานกิจการยุติธรรม ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๕.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

๕.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงานสิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

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

๕.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๑ ล้านบาท

(๓) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่น

ข้อเสนอ ในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(๔) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ ๑ ใน ๔ ของมูลค่างบประมาณที่ยื่นข้อเสนอในครั้งนั้น (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน)

(๕) กรณีตาม (๑) - (๔) ยกเว้นสำหรับกรณีดังต่อไปนี้

(๕.๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(๕.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑

๕.๑๓ ผู้ยื่นข้อเสนอต้องเคยมีผลงานในการทำ Gap Analysis หรือผลงานในการวิเคราะห์ช่องโหว่และทดสอบเจาะระบบ กับหน่วยงานภาครัฐหรือหน่วยงานเอกชนที่มีความน่าเชื่อถือ โดยมีมูลค่าโครงการไม่น้อยกว่า ๑ ล้านบาท ย้อนหลังไม่เกิน ๕ ปี นับจากวันที่ยื่นข้อเสนอ โดยผู้ยื่นข้อเสนอต้องแนบสำเนาสัญญาคู่ฉบับหรือหนังสือรับรองการจ้างงานดังกล่าวมาพร้อมด้วย

๕.๑๔ ผู้ยื่นข้อเสนอต้องมีทีมงานในการดำเนินงานโครงการ ประกอบด้วย

๕.๑๔.๑ ผู้จัดการโครงการ (Project Manager) จำนวนอย่างน้อย ๑ คน โดยมีคุณสมบัติ ดังนี้

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

๕.๑๔.๒ ผู้เชี่ยวชาญด้านทดสอบเจาะระบบ โดยมีประสบการณ์ในการทดสอบเจาะระบบไม่น้อยกว่า ๑๐ ปี จำนวนอย่างน้อย ๑ คน และจะต้องได้รับประกาศนียบัตรรับรองความสามารถตามข้อกำหนดอย่างใดอย่างหนึ่งดังนี้

- มีวุฒิทางการศึกษาอย่างน้อยปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ หรือวิศวกรรมคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้องด้านคอมพิวเตอร์
- มีประสบการณ์ที่เกี่ยวข้อง มีหน้าที่และความรับผิดชอบในโครงการอย่างน้อย ๑ โครงการ ซึ่งมีมูลค่าไม่ต่ำกว่า ๑ ล้านบาท
- มีใบรับรองผ่านการอบรม หรือผ่านการสอบ หรือได้รับ Certificate อย่างใดอย่างหนึ่งดังนี้
  - GIAC Certified Network Penetration Testing (GPEN)
  - GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
  - Certified Offensive Security Certified (OSCP)

๕.๑๔.๓ นักตรวจสอบช่องโหว่และนักทดสอบเจาะระบบ โดยมีประสบการณ์ ไม่น้อยกว่า ๓ ปี จำนวนอย่างน้อย ๒ คน และจะต้องได้รับประกาศนียบัตรรับรองความสามารถตามข้อกำหนดอย่างใดอย่างหนึ่งดังนี้

- มีวุฒิทางการศึกษาอย่างน้อยปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ หรือวิศวกรรมคอมพิวเตอร์ หรือสาขาที่เกี่ยวข้องด้านคอมพิวเตอร์

- มีประสบการณ์ที่เกี่ยวข้อง มีหน้าที่และความรับผิดชอบในโครงการอย่างน้อย ๑ โครงการ ซึ่งมีมูลค่าไม่ต่ำกว่า ๑ ล้านบาท

- มีใบรับรองผ่านการอบรม หรือผ่านการสอบ หรือได้รับ Certificate อย่างใดอย่างหนึ่ง ดังนี้

  - GIAC Certified Network Penetration Testing (GPEN)
  - GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
  - Certified Offensive Security Certified (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)

๕.๑๔.๔ 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

๖. <u>ขอบเขตของงานที่จะดำเนินการจัดจ้าง</u>

๖.๑ ซอฟต์แวร์ระบบตรวจจับและตอบสนองอัตโนมัติสำหรับบริหารจัดการโปรแกรมป้องกันไวรัสบนเครื่องลูกข่ายแบบรวมศูนย์ (Endpoint Detection and Response) โดยมีลิขสิทธิ์ถูกต้องตามกฎหมายสำหรับเครื่องลูกข่าย จำนวน ๑๘๐ ลิขสิทธิ์ โดยมีคุณลักษณะขั้นต่ำ หรือเทียบเท่า หรือดีกว่าดังนี้

๖.๑.๑ เป็นโปรแกรมในการตรวจจับภัยคุกคามขั้นสูงและตอบสนองอัตโนมัติ สามารถบริหารจัดการผ่านทางเว็บอินเตอร์เฟส (Web UI) ได้

๖.๑.๒ สามารถตรวจจับเหตุการณ์ด้านความปลอดภัย (Endpoint Incident Detection) จากการสังเกตการณ์กิจกรรมต่าง ๆ (Activity) ของเครื่องลูกข่าย, การละเมิดนโยบาย, การตรวจจับด้วยตัวบ่งชี้ Indicators of Compromise (IoCs) หรือ Suspicious Object ได้

๖.๑.๓ สามารถตรวจสอบเหตุการณ์ด้านความปลอดภัย (Investigate Incident หรือ Alerts) ตรวจสอบตามประวัติระยะเวลาของการเริ่มต้นของเหตุการณ์หลักทั้งหมดของเครื่องลูกข่าย เช่น การแพร่กระจาย, การเพิ่มสิทธิ์ เป็นต้น

๖.๑.๔ สามารถทำการจำกัดและตอบสนองต่อเหตุการณ์ (Incident Containment and Response) โดยการจำกัดเหตุการณ์บนเครื่องลูกข่าย และทำการตอบสนอง การแก้ไขเหตุการณ์ เช่น กำจัดไฟล์มัลแวร์, กู้คืนไฟล์ เป็นต้น

๖.๑.๕ สามารถทำการเก็บข้อมูลระยะไกลจากเครื่องลูกข่ายแบบ real-time ได้แก่ Process creation, Process changes, Registry persistence, File system modifications และ Network connections ได้

๖.๑.๖ สามารถสร้างรายงานเหตุการณ์ (Event) ได้อัตโนมัติด้วยความสามารถของการสแกน IoC (Indicator of Compromise), process หรือการตรวจสอบเหตุการณ์ที่ต้องสงสัยด้วย Detection Models จากเจ้าของผลิตภัณฑ์ ที่ผิดปกติบนเครื่องลูกข่าย

๖.๑.๗ สามารถนำ External IoC (Indicator of Compromise) หรือ STIX file จากภายนอกมาสแกนหา process หรือ Files ที่ผิดปกติบนเครื่องลูกข่ายได้

๖.๑.๘ สามารถกำหนดค่าการตอบสนองต่อเหตุการณ์อัตโนมัติได้ ดังนี้

๖.๑.๘.๑ Prevent file execution สามารถป้องกันการทำงานของไฟล์ที่ผิดปกติ เมื่อตรวจพบจาก IoC (Indicator of Compromise), process หรือวัตถุต้องสงสัย (Suspicious Object) ที่ผิดปกติบนเครื่องลูกข่าย และจะถูกเพิ่มไปยัง blacklist เพื่อป้องกัน process ดังกล่าว

๖.๑.๘.๒ Performing host isolation สามารถใช้คำสั่งระยะไกลในการแยกเครื่องลูกข่ายที่ผิดปกติออกจากเครือข่าย เมื่อตรวจพบจาก IoC (Indicator of Compromise) process หรือการแจ้งเตือน (Alerts) ที่ผิดปกติบนเครื่องลูกข่ายนั้น

๖.๑.๘.๓ Quarantine/recovery of objects ทำการสั่งให้กักกัน และย้ายไฟล์ที่ผิดปกติ หรือไฟล์ต้องสงสัย ที่เครื่องลูกข่ายไว้ รวมถึงสามารถปลดการกักกันหรือย้ายไฟล์กลับ (Restore file)

๖.๑.๘.๔ มีความสามารถ File deletion ทำการสั่งให้ลบไฟล์ที่ผิดปกติที่เครื่องลูกข่าย

๖.๑.๘.๕ Terminate processes ทำการสั่งให้หยุดการทำงานของ process ผิดปกติบนเครื่องลูกข่ายที่ตรวจพบ

๖.๑.๙ สามารถกำหนดนโยบายการป้องกัน (Prevention) การใช้งาน files, scripts, office document ในการเรียกใช้จากเครื่องลูกข่ายได้

๖.๑.๑๐ สามารถทำการกำหนดค่า Whitelisting ที่อนุญาตให้ยกเว้นการวิเคราะห์ ในระดับ networks, host address, users และ application ได้

๖.๑.๑๑ สามารถทำงานร่วมกับ SIEM ในการ export event หรือส่ง Syslog ในรูปแบบ CEF format ได้

๖.๑.๑๒ สามารถติดตั้งโปรแกรม Agent และทำงานบน Microsoft Windows Operating System บนเครื่อง workstation และ Server ได้ เช่น Windows 11/Windows 10/ Windows 8.1 x32,x64/ Windows 7 x32,x64, Windows Server 2019 และ Windows Server 2016, Windows Server 2012/R2 x64, Windows Server 2008 R2 x64 ได้เป็นอย่างน้อย

๖.๑.๑๓ โปรแกรม Agent สามารถทำงานร่วมกับผลิตภัณฑ์ป้องกันไวรัสยี่ห้ออื่นได้ และสามารถทำงานร่วมกับซอฟต์แวร์ที่มีอยู่เดิมของสำนักงานกิจการยุติธรรมได้เป็นอย่างดี โดยไม่กระทบกับการใช้งานระบบ

๖.๑.๑๔ โปรแกรมติดตั้งบนเครื่องลูกข่าย (EDR Agent) มี anti-malware engine ในการสแกนไฟล์แบบ Real-time โดยมีความสามารถในการวิเคราะห์และตรวจสอบภัยคุกคามจากการเรียนรู้พฤติกรรมการทำงานของไฟล์ด้วยเทคโนโลยี Machine Learning

๖.๑.๑๕ สามารถทำการจัดเก็บข้อมูลไว้ในเครื่องลูกข่ายเป็นระยะเวลาไม่น้อยกว่า ๓ สัปดาห์ เมื่อไม่ได้เชื่อมโยงกับระบบโปรแกรมบริหารจัดการจากส่วนกลาง

๖.๑.๑๖ โปรแกรมบนเครื่องลูกข่าย (EDR Agent) ทำงานตอบสนองต่อเหตุการณ์อัตโนมัติได้ดังนี้

๖.๑.๑๖.๑ รวบรวมข้อมูลเกี่ยวกับภัยการคุกคามและบริบทการคุกคามจาก EDR Agent ของเครื่องคอมพิวเตอร์ปลายทาง (Data Collection)

๖.๑.๑๖.๒ เพิ่มการแสดงผลข้อมูลในการตรวจสอบ (Threat development chain) หรือ Observable Graph และแสดงผลการตรวจสอบเหตุการณ์จากข้อมูลที่รวบรวมมาจากโปรแกรมติดตั้งบนเครื่องลูกข่าย (EDR Agent) ได้

๖.๑.๑๖.๓ ส่งข้อมูลที่เกี่ยวข้องไปที่โปรแกรมบริหารศูนย์กลางสำหรับการสร้างภาพข้อมูลรวมถึงข้อมูลการโจมตีและสาเหตุหลัก (Root-cause)

๖.๑.๑๖.๔ สามารถสแกนหา IoC (Indicator of Compromise), process หรือวัตถุต้องสงสัย (Suspicious Object) บนเครื่องลูกข่ายและสามารถดำเนินการตอบสนองกับ IoC (Indicator of Compromise) process หรือวัตถุต้องสงสัย (Suspicious Object) เหล่านั้น

๖.๑.๑๖.๕ สามารถรองรับการทำงานร่วมกับ Sandbox product โดย EDR Agent สามารถรองรับการส่งไฟล์ต้องสงสัยไปตรวจสอบที่ Sandbox ได้

๖.๑.๑๖.๖ ข้อมูลเหตุการณ์ที่เกี่ยวข้องกับการตรวจหาพฤติกรรมที่ต้องสงสัยจำพวกภัยคุกคามจะถูกส่งไปที่โปรแกรมบริหารศูนย์กลางเพื่อเพิ่มในการวิเคราะห์และการตอบสนอง

๖.๑.๑๗ สามารถกำหนดค่าการตอบสนองต่อเหตุการณ์อัตโนมัติ ได้ดังนี้

๖.๑.๑๗.๑ Kill Process หรือ Terminate Process

๖.๑.๑๗.๒ Quarantine หรือ recover the object

๖.๑.๑๗.๓ Delete the file

๖.๑.๑๘ สามารถส่งรายงานเหตุการณ์ที่ผิดปกติ (Incident Information card) หรือการแจ้งเตือนเหตุการณ์ต้องสงสัย (Alert) แบบอัตโนมัติ โดยมีข้อมูลดังนี้

๖.๑.๑๘.๑ Attack execution map หรือ threat visualization หรือ workbench alerts

๖.๑.๑๘.๒ Incident events (registered artifact file/ process details/ URL/ information/ registry modification, etc.) หรือ Highlighted objects

๖.๑.๑๘.๓ Host information (name, ip address, MAC address, list of users, OS, domain controller role, etc.)

๖.๑.๑๙ ลิขสิทธิ์ในนาม สำนักงานกิจการยุติธรรม

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

๖.๑.๒๑ จัดฝึกอบรมการใช้งานระบบ โดยจัดหาวิทยากร สถานที่ พร้อมเอกสารการฝึกอบรมให้กับเจ้าหน้าที่ที่เกี่ยวข้องจำนวนอย่างน้อย ๕ คน โดยผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งสิ้น

๖.๒ ซอฟต์แวร์ระบบตรวจจับและตอบสนองอัตโนมัติสำหรับบริหารจัดการโปรแกรมป้องกันไวรัสสำหรับเครื่องลูกข่ายแบบรวมศูนย์ (Endpoint Detection and Response) โดยมีลิขสิทธิ์ถูกต้องตามกฎหมายสำหรับเครื่องแม่ข่าย จำนวน ๑ เครื่อง โดยมีคุณลักษณะขั้นต่ำหรือเทียบเท่า หรือดีกว่าดังนี้

๖.๒.๑ คุณสมบัติของโปรแกรมบริหารจัดการ สามารถรองรับการติดตั้ง หรือใช้งานในรูปแบบใดรูปแบบหนึ่ง ดังต่อไปนี้

๖.๒.๑.๑ หากซอฟต์แวร์ระบบที่เสนอเป็นรูปแบบ On-Premise ระบบที่เสนอจะต้องรองรับการติดตั้งโปรแกรมบริหารจัดการบนเครื่อง Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8 และ Windows 10 ได้เป็นอย่างน้อย และรองรับการใช้งานกับ Database Microsoft SQL Server หรือ My SQl หรือดีกว่าได้

๖.๒.๑.๒ หากซอฟต์แวร์ระบบที่เสนอเป็นรูปแบบคลาวด์ (Cloud) ระบบที่เสนอต้องให้บริการในรูปแบบ Software as a Services (SaaS) ที่มี Web-Based Management เพื่อใช้ในการบริหารจัดการเครื่องลูกข่าย

๖.๒.๒ สามารถบริหารจัดการความปลอดภัยบนเครื่องคอมพิวเตอร์ลูกข่าย โดยประกอบไปด้วยเทคโนโลยีทางด้าน Anti-Malware, Personal Firewall, Intrusion Detections/Vulnerability Protection และ Web Reputation and Application Control ได้เป็นอย่างน้อย

๖.๒.๓ สามารถทำการ update virus/spyware pattern แบบ incremental update เพื่อลดภาระในระบบเครือข่ายได้

๖.๒.๔ สามารถแสดงรายงานของไฟล์ที่ถูกสำรอง (Backup หรือ Central Quarantine Restore) ข้อมูลไว้หากถูกลบได้จากโปรแกรมสำหรับบริหารจัดการจากศูนย์กลางและสามารถสั่งคืนค่าไฟล์ดังกล่าวได้จากโปรแกรมสำหรับบริหารจัดการจากศูนย์กลาง

๖.๒.๕ สามารถตรวจสอบรายละเอียดของโปรแกรมและอุปกรณ์ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการติดตั้งโปรแกรมป้องกันไวรัสที่เสนอ และอยู่บนระบบเครือข่ายเดียวกัน และสามารถออกรายงานโดยผู้ดูแลระบบได้ (Inventory Report)

๖.๒.๖ สามารถทำการกู้คืนและสำรองฐานข้อมูลของเครื่องแม่ข่ายเพื่อป้องกันในกรณีระบบเกิดการเสียหาย (Backup-Restore) หรือหากระบบบริหารจัดการรูปแบบคลาวด์ (Cloud) ระบบจะต้องมีการแจ้งเตือนเกี่ยวกับการปรับปรุงไปยังผู้ดูแลระบบได้

๖.๒.๗ สามารถนำเข้า (import) รายละเอียดผู้ใช้งานจากกลุ่มที่ได้สร้างเอาไว้จากระบบ Active Directory (AD) ของสำนักงานกิจการยุติธรรมเพื่อนำมาแบ่งกลุ่มการใช้งานตัวโปรแกรมสำหรับบริหารจัดการจากศูนย์กลางได้

๖.๒.๘ สามารถบริหารจัดการ และกำหนดนโยบายให้กับ Mobile device หรือเครื่องคอมพิวเตอร์โน้ตบุ๊ก ที่ติดตั้งโปรแกรมป้องกันไวรัสลงไปได้

๖.๒.๙ สามารถสร้างรายงาน ในรูปแบบ PDF, XLS และ HTML ได้

๖.๒.๑๐ สามารถติดตั้งโปรแกรมสำหรับบริหารจัดการจากศูนย์กลางบนเครื่องคอมพิวเตอร์แม่ข่ายได้หลายเครื่อง และสามารถทำงานร่วมกันได้ หรือเป็นซอฟต์แวร์ระบบตรวจจับและตอบสนองอัตโนมัติสำหรับบริหารจัดการโปรแกรมป้องกันไวรัสสำหรับเครื่องลูกข่ายแบบรวมศูนย์รูปแบบคลาวด์ (Cloud) ได้

๖.๒.๑๑ สามารถบริหารจัดการและการกำหนดนโยบายการทำงานของโปรแกรมป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์ลูกข่ายได้เป็นอย่างน้อย โดยบริหารจัดการผ่านโปรแกรมสำหรับบริหารจัดการจากศูนย์กลางเดียวกัน

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

๖.๒.๑๓ จัดฝึกอบรมการใช้งานระบบ โดยจัดหาวิทยากร สถานที่ พร้อมเอกสารการฝึกอบรมให้กับเจ้าหน้าที่ที่เกี่ยวข้องจำนวนอย่างน้อย ๕ คน โดยผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งสิ้น

๖.๓ ซอฟต์แวร์ระบบตรวจสอบและป้องกันภัยคุกคามขั้นสูง (Advance Persistent Threats) สำหรับเครื่องลูกข่ายแบบรวมศูนย์ จำนวน ๑๘๐ ลิขสิทธิ์ โดยมีคุณลักษณะขั้นต่ำ หรือเทียบเท่า หรือดีกว่าดังนี้

๖.๓.๑ มีระบบปฏิบัติการเสมือนสำหรับตรวจสอบและป้องกันภัยคุกคามขั้นสูง สำหรับเครื่องคอมพิวเตอร์ลูกข่ายแบบรวมศูนย์ ในรูปแบบใดรูปแบบหนึ่ง ดังต่อไปนี้

๖.๓.๑.๑ หากระบบที่เสนอเป็นรูปแบบ Sandbox (On-Premise) จะต้องติดตั้งมาพร้อมกับ Microsoft License key อย่างน้อยดังนี้

๖.๓.๑.๑.๑ Windows XP หรือ Windows 7

๖.๓.๑.๑.๒ Windows 10 หรือ Windows 11

๖.๓.๑.๒ หากระบบที่เสนอเป็นรูปแบบ Cloud Sandbox จะต้องมาพร้อมกับระบบปฏิบัติการเสมือน อย่างน้อยดังนี้

๖.๓.๑.๒.๑ Windows XP หรือ Windows 7

๖.๓.๑.๒.๒ Windows 10 หรือ Windows 11

๖.๓.๒ ระบบต้องสามารถวิเคราะห์พฤติกรรมของภัยคุกคามเพื่อตรวจจับกิจกรรมที่เป็นอันตรายและเป้าหมายของการโจมตีภายในองค์กรได้

๖.๓.๓ ระบบสามารถตรวจสอบไฟล์โดยรองรับขนาดไฟล์สูงสุดได้อย่างน้อยดังนี้

๖.๓.๓.๑ หากระบบที่เสนอเป็นรูปแบบ Sandbox (On-Premise) ระบบต้องสามารถตรวจสอบไฟล์โดยรองรับขนาดไฟล์สูงสุด ๑๐๐ MB

๖.๓.๓.๒ หากระบบที่เสนอเป็นรูปแบบ Cloud Sandbox ระบบต้องสามารถตรวจสอบไฟล์โดยรองรับขนาดไฟล์สูงสุด ๖๐ MB

๖.๓.๔ ระบบสามารถตรวจสอบไฟล์ในแบบอัตโนมัติ (Automated Mode) และแบบตามความต้องการของผู้ใช้งาน (Manual Mode) ได้

๖.๓.๕ ระบบต้องมีฐานข้อมูลภัยคุกคามสำหรับตรวจสอบไฟล์ และสามารถปรับปรุงฐานข้อมูลให้เป็นปัจจุบันอยู่เสมอในแบบอัตโนมัติและแบบปรับปรุงเองได้ หรือหากระบบที่เสนอเป็นรูปแบบ Cloud Sandbox ระบบต้องสามารถปรับปรุงฐานข้อมูลให้เป็นปัจจุบันอยู่เสมอในแบบอัตโนมัติได้

๖.๓.๖ ระบบต้องรองรับการปรับปรุงฐานข้อมูลระบบ Sandbox ในรูปแบบ HTTP หรือ HTTPS หรือรองรับการปรับปรุง (Update) จากเจ้าของผลิตภัณฑ์อัตโนมัติได้

๖.๓.๗ ระบบต้องสามารถทำงานร่วมกับระบบตรวจจับและตอบสนองอัตโนมัติภายใต้ผลิตภัณฑ์ชื่อเดียวกันได้ เพื่อทำการประเมินภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้อย่างสมบูรณ์แบบ

๖.๓.๘ รองรับการประเมินภัยคุกคามในหลายระดับ (Multi-level Assessment) หรือการประเมินระดับความรุนแรงของภัยคุกคาม (Severity level) และการวิเคราะห์พฤติกรรมของไฟล์หรือวัตถุที่อาจเป็นภัยคุกคาม

๖.๓.๙ หากระบบ Sandbox ที่เสนอเป็นรูปแบบ Sandbox (On-Premise) ระบบจะต้องมีอินเทอร์เฟซเครือข่ายเฉพาะในตัวสำหรับตรวจสอบการมีปฏิสัมพันธ์ที่เป็นอันตรายจากวัตถุที่เข้ามาจากอินเทอร์เน็ต

๖.๓.๑๐ ระบบต้องสามารถจำลองการทำงานของผู้ใช้ หรือแสดงผลกระบวนการตรวจสอบภัยคุกคาม (Process Graph) กรณีต้องการตรวจสอบภัยคุกคามที่สงสัยได้

๖.๓.๑๑ ระบบต้องสามารถตรวจสอบและต่อต้านเทคนิคการหลบเลี่ยงของมัลแวร์สมัยใหม่จากการตรวจสอบของ Sandbox (Sandbox bypass หรือ Evasion resistance) ที่ใช้ได้อย่างมีประสิทธิภาพ

๖.๓.๑๒ ลิขสิทธิ์ในนาม สำนักงานกิจการยุติธรรม

๖.๓.๑๓ ติดตั้งซอฟต์แวร์ลิขสิทธิ์บนระบบเดิมของสำนักงานกิจการยุติธรรม หรือบนระบบคลาวด์ (Cloud) ของเจ้าของผลิตภัณฑ์ที่นำเสนอ ให้สามารถทำงานได้อย่างปลอดภัยและมีประสิทธิภาพ

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

๖.๓.๑๕ จัดฝึกอบรมการใช้งานระบบ โดยจัดหาวิทยากร สถานที่ พร้อมเอกสารการฝึกอบรมให้กับเจ้าหน้าที่ที่เกี่ยวข้องจำนวนอย่างน้อย ๕ คน โดยผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งสิ้น

๖.๔ ดำเนินการทดสอบเจาะระบบและสแกนหาช่องโหว่ระบบรักษาความปลอดภัยสำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) ประจำปี ๒๕๖๗ โดยผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยดำเนินการทดสอบเจาะระบบ (Annual Penetration Test) โดยดำเนินการดังนี้

๖.๔.๑ ผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยดำเนินการทดสอบเจาะระบบเพื่อสำรวจหาช่องโหว่ Web Application ของสำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) จำนวน ๒ ระบบ โดยอ้างอิงแนวทางการเจาะระบบตามมาตรฐานสากล อย่างน้อยดังนี้

- OWASP Top 10 เวอร์ชั่นล่าสุด
- CWE TOP 25 Most Dangerous Software Weaknesses เวอร์ชั่นล่าสุด

๖.๔.๒ ผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยดำเนินการทดสอบเจาะระบบสำนักงานกิจการยุติธรรม (OJA) ผ่านเครือข่ายจากภายนอก (External Network Penetration Test) และผ่านระบบเครือข่ายภายใน (Internal Network Penetration Test) จำนวนทั้งสิ้นไม่เกิน ๕๐ IP Address ระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) ผ่านเครือข่ายจากภายนอก (External Network Penetration Test) และผ่านระบบเครือข่ายภายใน (Internal Network Penetration Test) จำนวนทั้งสิ้นไม่เกิน ๘๐ IP Address

๖.๔.๓ ดำเนินการทดสอบสแกนหาช่องโหว่โดยใช้เครื่องมืออัตโนมัติ (Vulnerability Assessment) ของเครื่องแม่ข่ายระบบสำนักงานกิจการยุติธรรม (OJA) จำนวนทั้งสิ้นไม่เกิน ๕๐ IP Address และระบบศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC) จำนวนทั้งสิ้นไม่เกิน ๑๐๐ IP Address พร้อมเสนอวิธีแก้ไขช่องโหว่ให้ทางสำนักงานกิจการยุติธรรมพิจารณา เพื่อเห็นชอบให้แก้ไขช่องโหว่ ในกรณีที่ไม่สามารถปิดช่องโหว่ที่พบได้หรือการปิดช่องโหว่แล้วมีผลกระทบรุนแรงจนทำให้ระบบไม่สามารถให้บริการได้ ให้เสนอแนวทางลดความเสี่ยงลดผลกระทบที่เกิดขึ้น

๖.๔.๔ วิเคราะห์และจัดทำเอกสารรายงานผลการทดสอบเจาะระบบ โดยจัดทำเอกสารรูปแบบของเอกสาร (Hard Copy) จำนวน ๕ ชุด และรูปแบบไฟล์เอกสาร (Soft Copy) ทั้งในรูปแบบของ File Word และ PDF ลงใน Flash Drive จำนวน ๒ ชุด โดยเอกสารดังกล่าวประกอบด้วยหัวข้ออย่างน้อยดังต่อไปนี้ บทสรุปสำหรับผู้บริหาร (Executive Summary) และรายละเอียดเชิงเทคนิคของผลการทดสอบ

๖.๔.๕ ทดสอบเจาะระบบซ้ำและดำเนินการทดสอบสแกนหาช่องโหว่ซ้ำเพื่อตรวจสอบผลการแก้ไขและจัดทำเอกสารรายงานผลการทดสอบเจาะระบบครั้งที่ ๒

๖.๔.๖ เข้าร่วมประชุมเพื่อหารือและให้คำปรึกษาเพื่อจัดทำแนวทางและวิธีการดำเนินการปิดช่องโหว่ อย่างน้อย ๒ ครั้ง ตามรายงานผลการทดสอบเจาะระบบ (Penetration Testing Report) และรายงานผลการทดสอบสแกนหาช่องโหว่โดยใช้เครื่องมืออัตโนมัติ (Vulnerability Assessment Report) ของสำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC)

๖.๕ ดำเนินการจัดการเพื่อเตรียมความพร้อมรองรับการพัฒนาและปรับปรุงงานตามนโยบายรองรับมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS) ในขอบเขตบริการ DATA SERVICE โดยดำเนินการดังนี้

๖.๕.๑ ที่ปรึกษาดำเนินการจัดทำแผนงานโครงการ (Project Plan) สำหรับระบบมาตรฐานว่าด้วยการบริหารการบริการด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS) ในขอบเขตของระบบงาน DXC Service ที่ติดตั้ง ณ สำนักงานกิจการยุติธรรม จำนวน ๔ ระบบ ประกอบไปด้วย ระบบสืบค้นประวัติการกระทำความผิด, บริการ API Portal, ระบบบริการ

ตนเอง (Self Service System) และระบบแสดงผลข้อมูลด้านยาเสพติดและสถานการณ์ด้านกระบวนการยุติธรรม หรือระบบอื่นที่สำนักงานกิจการยุติธรรมกำหนด

๖.๕.๒ ให้คำปรึกษาและสนับสนุนในการทบทวนเอกสาร รวมไปถึงปรับปรุงกระบวนการให้เป็นไปตามมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS) อย่างน้อยดังนี้

๖.๕.๒.๑ นโยบายและข้อปฏิบัติที่สอดคล้องกับระบบมาตรฐานว่าด้วยการบริหารการบริการด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS)

๖.๕.๒.๒ เอกสารอื่น ๆ ที่เกี่ยวข้องกับระบบมาตรฐานว่าด้วยการบริหารการบริการด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS) เช่น Service Catalogue and Service Level Management, Configuration Management

๖.๕.๓ ให้คำปรึกษาและสนับสนุนในการทบทวนการประเมินความเสี่ยง กระบวนการและมาตรฐานการให้บริการต่าง ๆ ที่มีความสำคัญต่อระบบมาตรฐานว่าด้วยการบริหารการบริการด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS) อย่างน้อยดังนี้

๖.๕.๓.๑ การประเมินความเสี่ยง (Risk Assessment)

๖.๕.๓.๒ การแก้ไขความเสี่ยง (Risk Treatment)

๖.๕.๔ ดำเนินการสรุปผล และข้อเสนอในการเตรียมความพร้อมรองรับการพัฒนาและปรับปรุงงานตามนโยบายรองรับมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS)

๖.๕.๕ ดำเนินการจัดการฝึกอบรมระบบมาตรฐานว่าด้วยการบริหารการบริการด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS) ให้กับเจ้าหน้าที่สำนักงานกิจการยุติธรรม จำนวนไม่น้อยกว่า ๕ คน

๗. กำหนดเวลาส่งมอบพัสดุ

๑๘๐ วัน นับถัดจากวันลงนามในสัญญา

๘. พื้นที่การดำเนินการ

สำนักงานกิจการยุติธรรม อาคารรัฐประศาสนภักดี ชั้น ๙ ศูนย์ราชการเฉลิมพระเกียรติฯ ๘๐ พรรษา ถนนแจ้งวัฒนะ หลักสี่ กรุงเทพมหานคร

๙. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สำนักงานกิจการยุติธรรมจะพิจารณาจากราคารวม ตัดสินโดยใช้หลักเกณฑ์ราคาต่ำสุด หากปรากฏว่ามีผู้เสนอราคาต่ำสุดเท่ากันหลายราย จะพิจารณาราคาต่ำสุดของผู้ที่เสนอราคาในลำดับแรกเป็นผู้ชนะการยื่นข้อเสนอ

๑๐. วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร

๔,๕๐๐,๐๐๐.- บาท (สี่ล้านห้าแสนบาทถ้วน)

๑๑. งวดงานและการจ่ายเงิน

สำนักงานกิจการยุติธรรมจะจ่ายเงินเป็นรายงวด ตามงวดการส่งมอบงาน จำนวน ๔ งวด ดังนี้

งวดที่ ๑ ร้อยละ ๓๐ ของวงเงินตามสัญญา เมื่อผู้รับจ้างดำเนินการส่งมอบงาน 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. แผนการดำเนินงานโครงการพัฒนาระบบรักษาความมั่นคงปลอดภัยสำนักงานกิจการยุติธรรมและศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม ประจำปี พ.ศ. ๒๕๖๗

๒. แผนงานโครงการ (Project Plan) สำหรับระบบมาตรฐานว่าด้วยการบริหารการบริการด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS) ในขอบเขตระบบ DXC Service (TOR ข้อ ๖.๕.๑)

๓. สัญญาการรักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement)

๔. รายงานผลการทดสอบเจาะระบบ (Penetration Testing Report) ครั้งที่ ๑ ของสำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC)

๕. รายงานผลการทดสอบสแกนหาช่องโหว่โดยใช้เครื่องมืออัตโนมัติ (Vulnerability Assessment Report) : ครั้งที่ ๑ ของสำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC)

งวดที่ ๒ ร้อยละ ๓๕ ของวงเงินตามสัญญา เมื่อผู้รับจ้างดำเนินการส่งมอบงาน ภายใน ๖๐ 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. ซอฟต์แวร์ระบบตรวจจับและตอบสนองอัตโนมัติสำหรับบริหารจัดการโปรแกรมป้องกันไวรัสสำหรับเครื่องลูกข่ายแบบรวมศูนย์ (Endpoint Detection and Response) โดยมีลิขสิทธิ์ถูกต้องตามกฎหมายสำหรับเครื่องลูกข่าย จำนวน ๑๘๐ ลิขสิทธิ์ (TOR ข้อ ๖.๑)

๒. ซอฟต์แวร์ระบบตรวจจับและตอบสนองอัตโนมัติสำหรับบริหารจัดการโปรแกรมป้องกันไวรัสสำหรับเครื่องลูกข่ายแบบรวมศูนย์ (Endpoint Detection and Response) โดยมีลิขสิทธิ์ถูกต้องตามกฎหมายสำหรับเครื่องแม่ข่าย ๑ เครื่อง จำนวน ๑ ลิขสิทธิ์ (TOR ข้อ ๖.๒)

๓. ซอฟต์แวร์ระบบตรวจสอบและป้องกันภัยคุกคามขั้นสูง (Advance Persistent Threats) สำหรับเครื่องลูกข่ายแบบรวมศูนย์ จำนวน ๑๘๐ ลิขสิทธิ์ (TOR ข้อ ๖.๓)

งวดที่ ๓ ร้อยละ ๓๐ ของวงเงินตามสัญญา เมื่อผู้รับจ้างดำเนินการส่งมอบงาน ภายใน ๑๒๐ 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. การจัดการฝึกอบรมระบบมาตรฐานว่าด้วยการบริหารการบริการด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS) ให้กับเจ้าหน้าที่สำนักงานกิจการยุติธรรม จำนวนไม่น้อยกว่า ๕ คน (TOR ข้อ ๖.๕.๕)

๒. เอกสารเกี่ยวกับการออกแบบ พัฒนา และปฏิบัติใช้กระบวนการ รวมไปถึงปรับปรุงเนื้อหาเอกสารให้เหมาะสมกับบริบทขององค์กรและภัยคุกคามในปัจจุบัน ประกอบด้วย

๒.๑ Service Catalogue and Service Level Management
๒.๒ Asset Management
๒.๓ Configuration Management
๒.๔ Demand and Capacity management
๒.๕ Service design Transition
๒.๖ Change Management

๒.๗ Service Request Management
๒.๘ Incident Management
๒.๙ Problem Management

งวดที่ ๔ ร้อยละ ๕ ของวงเงินตามสัญญา เมื่อผู้รับจ้างดำเนินการส่งมอบงาน 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 (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC)

๒. รายงานผลการทดสอบสแกนหาช่องโหว่โดยใช้เครื่องมืออัตโนมัติ (Vulnerability Assessment Report) : ครั้งที่ ๒ ของสำนักงานกิจการยุติธรรม (OJA) และศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC)

๓. รายงานสรุปผล และข้อเสนอในการเตรียมความพร้อมรองรับการพัฒนาและปรับปรุงงานตามนโยบายรองรับมาตรฐาน ISO/IEC 20000-1:2018 (Service Management System : SMS) (TOR ข้อ ๖.๕.๔)

๑๒. <u>อัตราค่าปรับ</u>

๑๒.๑ กรณีที่ผู้รับจ้างนำงานที่รับจ้างไปจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจากสำนักงานจะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนร้อยละ ๑๐ ของวงเงินของงานจ้างช่วงนั้น

๑๒.๒ กรณีที่ผู้รับจ้างปฏิบัติผิดสัญญาจ้างนอกเหนือจากข้อ ๑๒.๑ จะกำหนดค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๑๐ ของราคาค่าจ้าง