

**ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่มีใขงานก่อสร้าง**

1. ชื่อโครงการ โครงการพัฒนาความพร้อมในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ	
2. หน่วยงานเจ้าของโครงการโครงการพัฒนากฎหมายและกลไกกำกับดูแลธุรกิจดิจิทัล.....	
3. วงเงินงบประมาณที่ได้รับจัดสรร๓๐,๐๐๐,๐๐๐ บาท บาท	
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ ๑๑ พ.ค. ๒๕๖๔	
เป็นเงิน๒๘,๕๐๐,๐๐๐..... บาท	
ราคา/หน่วย (ถ้ามี)	บาท
5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)	
5.1บริษัท ดาต้าวัน เอเชีย (ประเทศไทย) จำกัด.....	
5.2บริษัท เอซีอินโฟเทค จำกัด.....	
5.3บริษัท แพนเจอริน จำกัด.....	
6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน	
6.1นางสาวพลอย เจริญสม.....	
6.2นายสิริณัฐ ตั้งธรรมจิต.....	
6.3นางสาวพัทธนันท์ เต็มศิริวัฒน์.....	
6.4นายรุ่งวิทย์ จิตรส่องแสง.....	
6.5นายจักรพงษ์ ธนเกริกกวิน.....	

เนื่องด้วยราคาเฉลี่ยของแหล่งที่มาของราคากลาง (ราคาอ้างอิง) สูงกว่า วงเงินงบประมาณที่ได้รับจัดสรร
เจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคนเห็นว่าราคาต่ำสุดสามารถดำเนินการจัดซื้อจัดจ้างได้
จึงขอใช้ราคาต่ำสุดเป็นราคากลาง (ราคาอ้างอิง)

ETDA นางสาว www.etda.or.th	ขอบเขตของงาน (Terms of Reference : TOR)		จำนวน	๖ หน้า
	เรื่อง	จ้างพัฒนาความพร้อมในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ		
	จัดทำโดย	งานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	วันที่จัดทำ	๒๗ เม.ย. ๖๔

๑. ความเป็นมา

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๑ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ มีความมั่นคงปลอดภัยและเชื่อถือได้ โดยให้มีรายละเอียดตามที่กำหนดในประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม หรือตามกฎหมาย ประกาศ ระเบียบอื่น ๆ ตามที่ สพรอ. กำหนด

ต่อมา สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ สพรอ. ในฐานะหน่วยงานเลขานุการของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้รับความคิดเห็นจากหน่วยงานของรัฐที่มีความประสงค์จัดทำร่างหรือทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ครอบคลุมเนื้อหาตามที่กำหนด พบว่าหน่วยงานของรัฐบางแห่งมีข้อจำกัดในด้านงบประมาณ บุคลากร ฯลฯ และมีความประสงค์ขอสนับสนุนการจัดทำร่างหรือทบทวนนโยบายและแนวปฏิบัติดังกล่าว รวมถึงการสนับสนุนด้านเทคนิคในการรักษาความมั่นคงปลอดภัยไซเบอร์ สพรอ. จึงจัดทำโครงการพัฒนาความพร้อมในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ เพื่อส่งเสริมและสนับสนุนให้หน่วยงานของรัฐจัดทำร่างหรือทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศได้ ตลอดจนการสนับสนุนด้านเทคนิคในการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. วัตถุประสงค์

๒.๑ ตรวจสอบประเมินความมั่นคงปลอดภัยและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศทางเทคนิคให้แก่หน่วยงานของรัฐ จำนวนไม่น้อยกว่า ๘๐ กรณี

๒.๒ จัดทำร่างหรือทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ จำนวนไม่น้อยกว่า ๘๐ หน่วยงาน

๒.๓ ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของระบบบริการของหน่วยงานของรัฐ จำนวนไม่น้อยกว่า ๓๐ หน่วยงาน

๒.๔ ให้ความรู้หน่วยงานของรัฐในการดำเนินการตามมาตรการด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จัดการประชุมเชิงปฏิบัติการ และจัดการซ้อมรับมือภัยคุกคามทางไซเบอร์ โดยมีผู้เข้าร่วมไม่น้อยกว่า ๑๖๐ คน

๓. คุณสมบัติผู้เสนอราคา

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ เป็นบุคคลธรรมดาหรือนิติบุคคล ผู้มีอาชีพรับจ้างทำงานที่จ้างในครั้งนี้

๓.๕ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๓.๖ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วนผู้จัดการ กรรมการ ผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๗ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ สพรอ. ณ วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการยื่นข้อเสนอครั้งนี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

๓.๑๐ ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e-GP) ของกรมบัญชีกลาง

๓.๑๑ ต้องยื่นรายการแสดงการเปรียบเทียบรายละเอียดขอบเขตของงานที่ สพรอ. ต้องการ กับรายละเอียดขอบเขตของงานที่เสนอว่าตรงกันหรือไม่ หากรายละเอียดขอบเขตของงานในเอกสารขัดแย้งกันเอง สพรอ. ขอสงวนสิทธิ์ที่จะพิจารณาในส่วนที่เป็นประโยชน์สูงสุดแก่ สพรอ.

๓.๑๒ ผู้ยื่นข้อเสนอต้องมีบุคลากรที่เป็นผู้เชี่ยวชาญเพื่อปฏิบัติงานจ้างครั้งนี้ โดยต้องได้รับประกาศนียบัตรที่ได้รับการยอมรับในระดับสากลด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งในวันที่ยื่นเสนอโครงการ ใบประกาศนียบัตรยังไม่หมดอายุ และมีอย่างน้อยกลุ่มละ ๑ ใบจากที่ระบุต่อไปนี้

กลุ่มที่ ๑

- ๓.๑๒.๑ GIAC Penetration Tester (GPEN)
- ๓.๑๒.๒ Offensive Security Certified Professional (OSCP)
- ๓.๑๒.๓ GIAC Web Application Penetration Tester (GWAPT)
- ๓.๑๒.๔ Offensive Security Certified Expert (OSCE)

กลุ่มที่ ๒

- ๓.๑๒.๕ Certified Information Systems Security Professional (CISSP)
- ๓.๑๒.๖ Certified Information Systems Auditor (CISA)
- ๓.๑๒.๗ ISMS Lead auditor
- ๓.๑๒.๘ ISMS Lead Implementor

๔. ขอบเขตของงาน

๔.๑ เข้าร่วมการประชุมกับเจ้าหน้าที่ สพรอ. อย่างน้อยเดือนละ ๑ ครั้ง หรือตามที่ สพรอ. กำหนด พร้อมจัดทำรายงานสรุปผลการประชุมทางไปรษณีย์อิเล็กทรอนิกส์ที่ สพรอ. กำหนดภายใน ๗ วันนับถัดจากวันประชุม

๔.๒ จัดทำรายงานแผนการดำเนินงานภายใน ๗ วันนับถัดจากวันลงนามในสัญญา ซึ่งประกอบด้วย

- (๑) สรุปข้อมูลทรัพยากรบุคคลและเวลาที่ต้องใช้ในการปฏิบัติงานตลอดทั้งโครงการ
- (๒) แผนการดำเนินงานตลอดทั้งโครงการ
- (๓) แนวทางการตรวจประเมินความมั่นคงปลอดภัยและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศทางเทคนิค รวมถึงแนวทางการแก้ไขปัญหาดังกล่าว

(๔) แนวทางการจัดทำร่างหรือทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐตามกฎหมายหรือมาตรฐานที่เกี่ยวข้อง

(๕) แนวทางการให้ความรู้หน่วยงานของรัฐในการดำเนินการตามมาตรการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

(๖) แนวทางการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของระบบบริการของหน่วยงานของรัฐ พร้อมจัดทำคู่มือประเมินความเสี่ยงดังกล่าว

๔.๓ ตรวจสอบประเมินความมั่นคงปลอดภัยและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศทางเทคนิค รวมถึงให้คำแนะนำในการแก้ไขปัญหาดังกล่าวแก่หน่วยงานของรัฐจำนวนไม่น้อยกว่า ๘๐ กรณี โดยให้มีรายละเอียดตามข้อกำหนดเกี่ยวกับการตรวจสอบประเมินฯ ที่ สฟทอ. กำหนด (เอกสารแนบ) เป็นอย่างน้อย

๔.๔ จัดทำร่างหรือทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐตามกฎหมายหรือมาตรฐานที่เกี่ยวข้องให้หน่วยงานของรัฐจำนวนไม่น้อยกว่า ๘๐ หน่วยงาน และจัดทำคู่มือการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีผลการศึกษาแนวทางการดูแลความมั่นคงปลอดภัยตามกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และกฎหมายลำดับรองหรือ (ร่าง) กฎหมายลำดับรองที่เกี่ยวข้อง และศึกษามาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตาม ISO/IEC 27001:2013 และ NIST Cybersecurity Framework เป็นอย่างน้อย

๔.๕ ให้ความรู้หน่วยงานของรัฐในการดำเนินการตามมาตรการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยจัดกิจกรรมการประชุมเชิงปฏิบัติการให้กับหน่วยงานของรัฐ ในเรื่องที่เกี่ยวข้องกับการดำเนินการตามนโยบายและแนวปฏิบัติฯ และการประเมินความเสี่ยง และจัดซ้อมรับมือภัยคุกคามทางไซเบอร์ รวมกันแล้วจำนวนไม่น้อยกว่า ๑๖๐ คน ซึ่งสามารถดำเนินการได้ทั้งในรูปแบบออนไลน์และออฟไลน์ตามที่ตกลงกับ สฟทอ.

๔.๖ ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของระบบบริการของหน่วยงานของรัฐ จำนวนไม่น้อยกว่า ๓๐ หน่วยงาน โดยมีเนื้อหาเป็นไปตาม ISO/IEC 27005:2018 เป็นอย่างน้อย พร้อมจัดทำคู่มือประเมินความเสี่ยงเพื่อเป็นแนวทางให้กับหน่วยงานในการประเมินความเสี่ยงด้วยตนเองได้อย่างเหมาะสม

๔.๗ จัดทำและส่งรายงานผลการดำเนินการตามข้อ ๔.๓ - ๔.๖ ในรูปแบบรายงานตามที่ สฟทอ. กำหนด พร้อมสรุปผลการดำเนินการเป็นเอกสารนำเสนอ (Presentation)

๕. วงเงินในการจัดหา

วงเงินงบประมาณ เป็นจำนวนเงิน ๓๐,๐๐๐,๐๐๐ บาท (สามสิบล้านบาทถ้วน) และราคากลาง เป็นจำนวนเงิน ๒๘,๕๐๐,๐๐๐ บาท (ยี่สิบล้านห้าแสนบาทถ้วน)

๖. ระยะเวลาดำเนินการ

กำหนดระยะเวลาดำเนินการให้แล้วเสร็จภายใน ๑๘๐ (หนึ่งร้อยแปดสิบ) วัน นับถัดจากวันที่ลงนามในสัญญา

๗. สิ่งส่งมอบและกำหนดเวลาการส่งมอบ

ผู้รับจ้างจะต้องดำเนินการและส่งมอบงานตามขอบเขตของงานข้อ ๔ โดยแบ่งกำหนดระยะเวลาการดำเนินการและส่งมอบงานจ้างเป็นจำนวน ๔ (สี่) งวด ดังนี้

๗.๑ งวดที่ ๑ ดำเนินการและส่งมอบงานตามขอบเขตของงาน ข้อ ๔.๑ - ๔.๒, ๔.๔ ภายใน ๓๐ (สามสิบ) วัน นับถัดจากวันที่ลงนามในสัญญาหรือใบสั่งจ้าง ดังนี้

(๑) รายงานตามข้อ ๔.๑ และ ๔.๒

(๒) คู่มือการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามข้อ ๔.๔

๗.๒ งวดที่ ๒ ดำเนินการและส่งมอบงานตามขอบเขตของงาน ข้อ ๔.๑, ๔.๓ และ ๔.๔ ภายใน ๗๕ (เจ็ดสิบห้า) วัน นับถัดจากวันที่ลงนามในสัญญาหรือใบสั่งจ้าง ดังนี้

(๑) รายงานสรุปผลการประชุม ตามข้อ ๔.๑

(๒) ผลการตรวจประเมินฯ ตามข้อ ๔.๓ จำนวน ๔๐ (สี่สิบ) กรณี

(๓) ผลการจัดทำร่างหรือทบทวนนโยบายและแนวปฏิบัติฯ ตามข้อ ๔.๔ จำนวน ๔๐ (สี่สิบ) หน่วยงาน

๗.๓ งวดที่ ๓ ดำเนินการและส่งมอบงานตามขอบเขตของงาน ข้อ ๔.๑, ๔.๔ และ ๔.๖ ภายใน ๑๒๐ (หนึ่งร้อยยี่สิบ) วัน นับถัดจากวันที่ลงนามในสัญญาหรือใบสั่งจ้าง ดังนี้

(๑) รายงานสรุปผลการประชุม ตามข้อ ๔.๑

(๒) ผลการตรวจประเมินฯ ตามข้อ ๔.๓ จำนวน ๔๐ (สี่สิบ) กรณี

(๓) ผลการจัดทำร่างหรือทบทวนนโยบายและแนวปฏิบัติฯ ตามข้อ ๔.๔ จำนวน ๔๐ (สี่สิบ) หน่วยงาน

(๔) ผลการให้ความรู้ ประชุมเชิงปฏิบัติการ และจัดซ้อมรับมือภัยคุกคามทางไซเบอร์ ตามข้อ ๔.๕

๗.๔ งวดที่ ๔ ดำเนินการและส่งมอบงานตามขอบเขตของงาน ข้อ ๔.๑, ๔.๖ - ๔.๗ ทั้งหมด ภายใน ๑๘๐ (หนึ่งร้อยแปดสิบ) วัน นับถัดจากวันที่ลงนามในสัญญาหรือใบสั่งจ้าง

โดยงานทั้ง ๔ งวดต้องส่งมอบในรูปแบบโดยส่งมอบเป็นไฟล์อิเล็กทรอนิกส์ในรูปแบบ Microsoft Word, Microsoft PowerPoint และ PDF บันทึกในสื่อบันทึกข้อมูลแบบ USB จำนวน ๒ ชุด หรือตามที่ สพรอ. กำหนด

๘. เงื่อนไขการจ่ายเงิน

สพรอ. จะจ่ายเงินค่าจ้างให้แก่ผู้รับจ้าง โดยแบ่งเป็น ๔ (สี่) งวด ดังนี้

งวดที่ ๑ อัตราร้อยละ ๒๐ (ยี่สิบ) ของค่าจ้าง เมื่อผู้รับจ้างได้ดำเนินการและส่งมอบงานตามสิ่งส่งมอบ ข้อ ๗.๑ และคณะกรรมการตรวจรับได้ตรวจรับงานจ้างครบถ้วนถูกต้องแล้ว

งวดที่ ๒ อัตราร้อยละ ๓๐ (สามสิบ) ของค่าจ้าง เมื่อผู้รับจ้างได้ดำเนินการและส่งมอบงานตามสิ่งส่งมอบ ข้อ ๗.๒ และคณะกรรมการตรวจรับได้ตรวจรับงานจ้างครบถ้วนถูกต้องแล้ว

งวดที่ ๓ อัตราร้อยละ ๔๐ (สี่สิบ) ของค่าจ้าง เมื่อผู้รับจ้างได้ดำเนินการและส่งมอบงานตามสิ่งส่งมอบ ข้อ ๗.๓ และคณะกรรมการตรวจรับได้ตรวจรับงานจ้างครบถ้วนถูกต้องแล้ว

งวดที่ ๔ อัตราร้อยละ ๑๐ (สิบ) ของค่าจ้าง เมื่อผู้รับจ้างได้ดำเนินการและส่งมอบงานตามสิ่งส่งมอบ ข้อ ๗.๔ และคณะกรรมการตรวจรับได้ตรวจรับงานจ้างครบถ้วนถูกต้องแล้ว

ทั้งนี้ ค่าจ้างที่ สพรอ. จะจ่ายตามข้อนี้ ได้รวมค่าใช้จ่ายและค่าภาษีอากร รวมทั้งภาษีมูลค่าเพิ่ม (ถ้ามี) ไว้ด้วยแล้ว

๙. อัตราค่าปรับ

เมื่อครบกำหนดส่งมอบงานตามที่กำหนด ถ้าผู้รับจ้างไม่ส่งมอบงานจ้าง หรือส่งมอบล่าช้า หรือส่งมอบไม่ถูกต้อง หรือไม่ครบจำนวน หรือไม่เป็นไปตามที่ตกลงกันไว้แก่ สพรอ. ผู้รับจ้างจะต้องชำระค่าปรับให้ สพรอ. เป็นรายวันเป็นจำนวนเงินตายตัวในอัตราร้อยละ ๐.๑๐ (ศูนย์จุดหนึ่งศูนย์) ของราคางานจ้าง แต่จะต้องไม่ต่ำกว่าวันละ ๑๐๐ บาท (หนึ่งร้อยบาทถ้วน) นับถัดจากวันครบกำหนดส่งมอบตามสัญญาจนถึงวันที่ผู้รับจ้างได้ส่งมอบงานจ้างให้แก่ สพรอ. จนถูกต้องครบถ้วน

๑๐. การรักษาความลับ

๑๐.๑ ผู้รับจ้างจะต้องจัดเก็บรักษาข้อมูลต่าง ๆ ที่เกี่ยวกับการดำเนินงานที่ผู้รับจ้างได้รับจาก สฟทอ. และข้อมูลต่าง ๆ ที่ผู้รับจ้างได้จัดทำขึ้นเนื่องจากการดำเนินงานตามสัญญาเป็นอย่างเป็นความลับของ สฟทอ. ซึ่งต่อไปในสัญญานี้เรียกว่า “ข้อมูลที่เป็นความลับ” โดยผู้รับจ้างต้องหามาตรการในการจัดเก็บข้อมูลที่เป็นความลับให้มิดชิด รวมทั้งไม่เปิดเผย หรือเผยแพร่ หรือกระทำด้วยวิธีการใดให้บุคคลอื่นใดที่มีใช้คู่สัญญาภายใต้สัญญานี้ หรือมิใช่บุคคลที่ สฟทอ. ได้อนุญาตเป็นลายลักษณ์อักษรให้มีส่วนเกี่ยวข้องที่จะรับทราบข้อมูลที่เป็นความลับภายใต้สัญญานี้ ได้ทราบถึงข้อมูลที่เป็นความลับดังกล่าว เว้นแต่จะเป็นการเปิดเผยข้อมูลดังกล่าวให้แก่เจ้าหน้าที่ผู้ปฏิบัติงานของผู้รับจ้างที่ต้องเกี่ยวข้องโดยตรงกับข้อมูลดังกล่าวเท่านั้น และผู้รับจ้างจะต้องจัดให้เจ้าหน้าที่ผู้ปฏิบัติงานดังกล่าวได้ผูกพันและปฏิบัติตามเงื่อนไขในการรักษาข้อมูลที่เป็นความลับเช่นว่านั้นด้วย

๑๐.๒ หากผู้รับจ้างมิได้ปฏิบัติตามข้อ ๑๐.๑ ผู้รับจ้างจะต้องรับผิดชอบต่อ สฟทอ. หรือบุคคลอื่นที่เป็นเจ้าของข้อมูลที่เป็นความลับนั้นในความเสียหายใด ๆ ที่เกิดขึ้นเนื่องจากการที่ข้อมูลที่เป็นความลับดังกล่าวได้ถูกเปิดเผยไม่ว่าทั้งหมดหรือแต่บางส่วน และ สฟทอ. มีสิทธิบอกเลิกสัญญาได้ทันที

๑๐.๓ ผู้รับจ้างจะยังคงต้องผูกพันตามข้อกำหนดเกี่ยวกับการรักษาข้อมูลที่เป็นความลับตามข้อ ๑๐.๑ ต่อไป ตราบที่ข้อมูลที่เป็นความลับดังกล่าวยังคงเป็นความลับอยู่ แม้ว่าการจ้างตามสัญญานี้ได้สิ้นสุดลงแล้วไม่ว่าด้วยเหตุใดก็ตาม

๑๑. หลักเกณฑ์การพิจารณา

ใช้เกณฑ์ราคาและเกณฑ์คุณภาพประกอบกัน โดย สฟทอ. ขอสงวนสิทธิ์ในการพิจารณาคัดเลือกโดยเรียงลำดับจากผู้ที่ได้รับคะแนนรวมสูงสุด ดังนี้

๑๑.๑ ราคาที่เสนอ ให้น้ำหนักร้อยละ ๑๐ (สิบ)

๑๑.๒ ผลงานที่ผ่านมา หรือ ความน่าเชื่อถือของผู้เสนอราคา ให้น้ำหนักร้อยละ ๙๐ (เก้าสิบ)

การพิจารณาข้อเสนอตามขอบเขตของงาน ผู้ที่ผ่านการพิจารณาตามเกณฑ์ จะต้องได้รับคะแนนรวมไม่น้อยกว่า ๘๐ (แปดสิบ) คะแนน จากคะแนนรวม ๑๐๐ (หนึ่งร้อย) คะแนน ตามหลักเกณฑ์การพิจารณา ดังนี้

ลำดับ	รายละเอียด	น้ำหนัก (ร้อยละ)	คะแนนต่อข้อ (๑๐๐)	คะแนนรวม (๑๐๐)
๑	ราคาที่เสนอ	๑๐		
๒	จำนวนใบประกาศนียบัตรเฉลี่ยต่อบุคลากรตามคุณสมบัติผู้เสนอราคาข้อ ๓.๑๒	๒๐		
๓	ผลงาน (รายงาน) ที่ผ่านมาเกี่ยวกับการดำเนินการตรวจประเมินความมั่นคงปลอดภัยและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศทางเทคนิค โดยคำนวณเป็นคะแนน ดังนี้ ๓.๑. รายงานมีการอ้างอิงตามระเบียบวิธี (Methodology) ตามเอกสารแนบ และหากเป็นระบบที่เกี่ยวข้องกับหน่วยงานภาครัฐ จะมีการคิดคะแนนเพิ่มพิเศษ โดยรายงานที่นำเสนอข้างต้นต้องมี จำนวนไม่เกิน ๒ ระบบ	๕๐		

	ต่อประเภทของระบบสารสนเทศ ดังนี้ (คะแนนเต็ม ๓๐) (๑) Web Application (คะแนนเต็ม ๑๕) (๒) Mobile Application (คะแนนเต็ม ๑๕) ๓.๒. ตัวอย่างเอกสาร (Template) รายงานที่มีการอ้างอิงตามระเบียบวิธี (Methodology) (คะแนนเต็ม ๑๐) (๑) ข้อมูลการจราจรทางคอมพิวเตอร์ (Log) (คะแนนเต็ม ๕) (๒) เครื่องคอมพิวเตอร์ติดโปรแกรม ไม่พึงประสงค์ (Malware) (คะแนนเต็ม ๕)			
๔	ผลงานที่ผ่านมา และข้อเสนอแนวทางการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	๒๐		
๕	ผลงานที่ผ่านมา และข้อเสนอแนวทางการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ	๑๐		
คะแนนรวมทั้งหมด		๑๐๐		

หมายเหตุ

๑. คะแนนที่ผู้เสนอราคาได้รับ = (คะแนน*น้ำหนัก) / ๑๐๐

๒. ประเมินคะแนนจากราคาที่เสนอ = ๑๐๐ - ((ผลต่างราคาของผู้เสนอ กับ ราคาผู้เสนอราคาต่ำสุด / ราคาผู้เสนอราคาต่ำสุด)* ๑๐๐)

ทั้งนี้ ผู้เสนอราคาจะต้องส่งข้อเสนอด้านเทคนิคและด้านผลงานเพื่อประกอบการพิจารณาให้กับ สฟธ. และนำเสนอ Presentation ไม่เกิน ๖๐ (หกสิบ) นาที ณ สฟธ. อาคารเดอะไนน์ ทาวเวอร์แกรนด์ พระรามเก้า (อาคารบี) ชั้น ๒๐ เลขที่ ๓๓/๔ ถนนพระราม ๙ แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพฯ ๑๐๓๑๐ เพื่อประกอบการพิจารณา

ข้อกำหนดเกี่ยวกับการตรวจประเมินความมั่นคงปลอดภัย

และวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศทางเทคนิค

(สำหรับโครงการพัฒนาความพร้อมในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ)

๑. ผู้รับจ้างต้องจัดทำแผนการดำเนินงานภาพรวมของขอบเขตงานรวมถึงข้อมูลที่เกี่ยวข้องอื่น ๆ ในบริการตรวจประเมินความมั่นคงปลอดภัยและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศทางเทคนิค โดยประกอบด้วยรายละเอียดดังต่อไปนี้

๑.๑ บทสรุปสำหรับผู้บริหาร (Executive Summary) รายละเอียดภาพรวมของงานตรวจประเมินฯ

๑.๒ ขอบเขตงานตรวจประเมินฯ

๑.๒.๑ ข้อมูลสรุปทรัพยากรคนและเวลา (Man-Day) ที่ต้องใช้ในการปฏิบัติงาน ตามข้อ ๒

๑.๒.๒ ข้อมูลวิธีการ ขั้นตอน และเครื่องมือที่ใช้ในการปฏิบัติงานอย่างละเอียด ตามข้อ ๒

๑.๒.๓ เกณฑ์ที่ใช้ในการประเมินระดับความเสี่ยง (Risk Rating) ที่พบจากการตรวจประเมินฯ ตามข้อ ๒

๑.๓ รายชื่อผู้ปฏิบัติงาน ตำแหน่ง และข้อมูลการติดต่อของผู้ที่เกี่ยวข้อง

๑.๔ ตัวอย่างเอกสาร (Template) ที่เกี่ยวข้องกับการตรวจประเมินฯ ดังนี้

๑.๔.๑ เอกสารใบคำร้องขอรับบริการสำหรับการตรวจประเมินฯ ตามข้อ ๒

๑.๔.๒ เอกสารขออนุญาตก่อนการตรวจประเมินฯ ตามข้อ ๒ สำหรับแจ้งให้ผู้รับบริการตรวจประเมินฯ รับทราบ

๑.๔.๓ เอกสารแสดงรายละเอียดก่อนดำเนินการตรวจประเมินฯ ตามข้อ ๓

๑.๔.๔ เอกสารรายงานผลการตรวจประเมินฯ ตามข้อ ๖

๒. ผู้รับจ้างต้องดำเนินการตรวจประเมินความมั่นคงปลอดภัยและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศทางเทคนิค ได้ตลอด ๒๔ ชั่วโมง โดยไม่เว้นวันหยุดราชการและวันหยุดนักขัตฤกษ์ ตามที่ได้รับแจ้งจาก สฟธอ. รวมทั้งสิ้นจำนวนไม่น้อยกว่า ๘๐ กรณี (ระบบสารสนเทศ) โดย สฟธอ. จะพิจารณาเลือกจากระบบสารสนเทศดังต่อไปนี้

๒.๑ Web Application

๒.๒ Mobile Application

๒.๓ วิเคราะห์เหตุการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ ดังต่อไปนี้เป็นอย่างน้อย

๒.๓.๑ ข้อมูลการจราจรทางคอมพิวเตอร์ (Log) ของระบบสารสนเทศ

๒.๓.๒ เครื่องคอมพิวเตอร์ติดโปรแกรมไม่พึงประสงค์ (Malware)

ทั้งนี้ ผู้รับจ้างต้องดำเนินการตรวจประเมินฯ แต่ละกรณีอีกครั้ง (Revisit) ภายหลังจากมีการแก้ไขปัญหาด้านความมั่นคงปลอดภัยระบบสารสนเทศและเมื่อได้รับแจ้งจาก สฟธอ. แล้ว โดยไม่มีการคิดค่าใช้จ่ายเพิ่มเติม เพื่อยืนยันผลการแก้ปัญหาดังกล่าว

๓. ก่อนดำเนินการตรวจประเมินความมั่นคงปลอดภัยและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศทางเทคนิค ตามข้อ ๒ ผู้รับจ้างต้องจัดส่งแผนและรายละเอียดการปฏิบัติงานตามที่สพธอ. กำหนด ซึ่งประกอบไปด้วยรายละเอียดอย่างน้อยดังต่อไปนี้

๓.๑ ชื่อ-นามสกุล และหมายเลขโทรศัพท์ติดต่อของบุคลากรที่ปฏิบัติงานตรวจประเมินฯ

๓.๒ ช่วงเวลาที่ปฏิบัติงานตรวจประเมินฯ ระบบสารสนเทศ

๓.๓ รายละเอียดระบบสารสนเทศที่ตรวจประเมินฯ เช่น โดเมน หมายเลขไอพีแอดเดรส และชื่อระบบสารสนเทศ

๓.๔ ชื่อ-นามสกุล และหมายเลขโทรศัพท์ติดต่อของบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศที่ตรวจประเมินฯ

๔. ผู้รับจ้างต้องสามารถดำเนินการตรวจประเมินความมั่นคงปลอดภัยและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศทางเทคนิค ตามข้อ ๒ ณ สถานที่ตรวจประเมินฯ ได้ (Onsite Service) ตามที่ได้รับแจ้งจาก สพธอ.

๕. ผู้รับจ้างต้องปฏิบัติตามระเบียบวิธี (Methodology) โดยมีรายละเอียด ดังต่อไปนี้

๕.๑ กระบวนการดำเนินงาน ตามข้อ ๒.๑ (Web Application) ต้องปฏิบัติตามระเบียบวิธีอย่างน้อยดังนี้

๕.๑.๑ OWASP Web Security Testing Guide

๕.๑.๒ OWASP Top 10 2017

๕.๑.๓ NIST SP800-115

๕.๒ กระบวนการดำเนินงาน ตามข้อ ๒.๒ (Mobile Application) ต้องปฏิบัติตามระเบียบวิธีอย่างน้อยดังนี้

๕.๒.๑ OWASP Mobile Top 10 2016

๕.๒.๒ Mobile Security Testing Guide (MSTG)

๕.๒.๓ NIST SP800-115

๕.๓ กระบวนการดำเนินงาน ตามข้อ ๒.๓ (วิเคราะห์เหตุการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์) ต้องปฏิบัติตามระเบียบวิธีอย่างน้อยดังนี้

๕.๓.๑ NIST.SP.800-61r2 (Computer Security Incident Handling Guide)

๕.๓.๒ NIST SP800-115

๖. ผู้รับจ้างต้องจัดทำรายงานผล (Report) และจัดทำรายงานสำหรับนำเสนอ (Presentation) ผลการตรวจประเมินความมั่นคงปลอดภัยและวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศทางเทคนิค ตามข้อ ๒ ในแต่ละเป้าหมาย โดยรายงานประกอบด้วยรายละเอียดอย่างน้อยดังนี้

๖.๑ บทสรุปผู้บริหาร (Executive Summary)

๖.๒ ข้อมูลผู้ปฏิบัติงาน

๖.๓ การประเมินระดับความเสี่ยง (Risk Rating)

๖.๔ ขอบเขตการปฏิบัติงานและช่วงเวลาที่ตรวจประเมินฯ

๖.๕ รายละเอียดของเป้าหมาย

๖.๖ รายละเอียดวิธีการและขั้นตอนการตรวจประเมินฯ

๖.๗ รายละเอียดผลการตรวจประเมินฯ

๖.๘ ข้อเสนอแนะและแนวทางการแก้ไข

๖.๙ ผลการตรวจประเมิน Revisit (กรณีที่ได้รับแจ้งจาก สพอ.)

๗. ผู้รับจ้างต้องดำเนินงาน ตามข้อ ๒ และข้อ ๖ ตามที่ได้รับแจ้งจาก สพอ. ให้แล้วเสร็จ โดยแบ่งเป็น ๒ กรณี ดังนี้

๗.๑ กรณีที่ต้องดำเนินงานแบบเร่งด่วน ต้องจัดทำรายงานผลฉบับร่าง ประกอบด้วยข้อ ๖.๑,

๖.๓, ๖.๕, ๖.๗, ๖.๘ และ ๖.๙ (ถ้ามี) ให้แล้วเสร็จภายใน ๓ วัน และต้องจัดทำรายงานผล

ฉบับสมบูรณ์ ตามข้อ ๖ ให้แล้วเสร็จภายใน ๑๐ วัน นับถัดจากวันที่ได้รับแจ้งจาก สพอ.

กรณีที่ต้องดำเนินงานแบบปกติ ต้องจัดทำรายงานผลฉบับสมบูรณ์ ตามข้อ ๖ ให้แล้วเสร็จภายใน ๑๑ วัน นับถัดจากวันที่ได้รับแจ้งจาก สพอ.