แบบ บก.๐๖

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่าย
การจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

๑. ชื่อโครงการ การจ้างผู้ให้บริการเฝ้าระวังภัยคุกคามทางไซเบอร์ผ่านระบบควบคุมระยะไกลของ สำนักงาน กสทช.

๒. หน่วยงานเจ้าของโครงการ สำนักเทคโนโลยีสารสนเทศ (นบ.)

๓. วงเงินงบประมาณที่ได้รับจัดสรร

วงเงินงบประมาณ ๓,๐๐๐,๐๐๐.- บาท (สามล้านบาทถ้วน)

งบประมาณรายจ่าย ประจำปี ๒๕๖๙ รายจ่ายเกี่ยวกับการจัดการและบริหารองค์กร หมวดค่าใช้สอย รายการค่าจ้างเหมาบริการ ของสำนักเทคโนโลยีสารสนเทศ

๔. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ ๒ กุมภาพันธ์ ๒๕๖๙

เป็นเงิน ๒,๘๙๐,๐๐๐.- บาท (สองล้านแปดแสนเก้าหมื่นบาทถ้วน)

๕. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

๕.๑ อ้างอิงจากใบเสนอราคาบริษัท คลาวด์เซค เอเชีย จำกัด เลขที่ QUA๖๙๐๑๐๐๐๐๕ ลงวันที่ ๒๘ มกราคม ๒๕๖๙

๕.๒ อ้างอิงจากใบเสนอราคาบริษัท อี-ซี.โอ.พี (ประเทศไทย) จำกัด เลขที่ ECOPAS๒๐๒๕๑๐๒๐๐๒ ลงวันที่ ๒๘ มกราคม ๒๕๖๙

๕.๓ อ้างอิงจากใบเสนอราคาบริษัท มอนสเตอร์ คอนเนค จำกัด เลขที่ QT๒๐๒๖๐๑๐๐๒๙ ลงวันที่ ๒๘ มกราคม ๒๕๖๙

๖. รายชื่อผู้รับผิดชอบกำหนดราคากลาง

๖.๑ นายชัชชัย คำภักดี	ประธานกรรมการ	.....
๖.๒ นางสาวภัทรานี ฐิติกาล	กรรมการ	.....
๖.๓ นายวุฒิพงษ์ พันธ์โสภา	กรรมการและเลขานุการ	.....

ข้อกำหนดและขอบเขตของงาน (Terms of Reference : TOR)
จ้างผู้ให้บริการเฝ้าระวังภัยคุกคามทางไซเบอร์ผ่านระบบควบคุมระยะไกลของสำนักงาน กสทช.

๑. หลักการและเหตุผล

ภัยคุกคามทางไซเบอร์ในปัจจุบันมีการพัฒนาอย่างรวดเร็ว มีความซับซ้อนหลากหลายรูปแบบ และมีเป้าหมายที่ขยายวงกว้างขึ้น รวมถึงหน่วยงานภาครัฐและองค์กรกำกับดูแลที่มีบทบาทสำคัญต่อโครงสร้างพื้นฐานของประเทศ การรับมือกับภัยคุกคามเหล่านี้จำเป็นต้องอาศัยองค์ความรู้ ความเชี่ยวชาญเฉพาะทาง และประสบการณ์ในการวิเคราะห์ ตรวจจับ ป้องกัน และตอบสนองต่อเหตุการณ์ที่เปลี่ยนแปลงอยู่ตลอดเวลา การสร้างและรักษาทีมงานผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร (In-house) ที่มีทักษะและความสามารถจำเป็นต้องใช้ระยะเวลาในการสรรหา พัฒนา และมีค่าใช้จ่ายในการลงทุนด้านบุคลากรที่สูงมาก รวมถึงความท้าทายในการรักษาบุคลากรที่มีความสามารถให้อยู่กับองค์กรในระยะยาวทำได้ยาก เนื่องจากเป็นสาขาวิชาชีพที่เป็นที่ต้องการสูงในตลาด การให้ผู้เชี่ยวชาญจากภายนอกเข้ามาดูแลและประเมินความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร จะช่วยให้ได้รับมุมมองที่เป็นกลางและอิสระ ซึ่งอาจนำไปสู่การค้นพบช่องโหว่หรือจุดอ่อนที่ทีมงานภายในอาจมองข้ามไปได้ เป็นการเสริมสร้างความแข็งแกร่งให้กับระบบป้องกันโดยรวม อีกทั้งการนำเอาเทคโนโลยีในการตรวจสอบช่องโหว่จากภายนอกแบบตลอดเวลามาใช้เพื่อช่วยเสริมสร้างในการบริหารจัดการความมั่นคงปลอดภัยมีประสิทธิภาพมากขึ้นเป็นสิ่งที่จำเป็น

เพื่อให้การดำเนินงานของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) ในฐานะองค์กรกำกับดูแลภารกิจสำคัญด้านกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมของประเทศ ซึ่งมีการจัดการข้อมูลสารสนเทศและระบบเทคโนโลยีดิจิทัลจำนวนมาก เป็นไปด้วยความต่อเนื่อง มั่นคง ปลอดภัย และน่าเชื่อถือ สอดคล้องกับข้อกำหนดทางกฎหมายที่สำคัญ เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีระบบและบุคลากรผู้เชี่ยวชาญในการดูแล ตรวจสอบ เฝ้าระวัง และตอบสนองต่อภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้อย่างทันท่วงทีและมีประสิทธิภาพสูงสุด เพื่อปกป้องสินทรัพย์สารสนเทศที่สำคัญขององค์กร ข้อมูลของประชาชนผู้ใช้บริการ และรักษาไว้ซึ่งความเชื่อมั่นของสาธารณชน รวมถึงเพิ่มประสิทธิภาพในการบริหารจัดการทรัพยากรและยกระดับความเชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยการเข้าถึงความรู้ความสามารถ เทคโนโลยี และเครื่องมือที่ทันสมัยจากผู้รับจ้างภายนอกที่มีความเชี่ยวชาญเฉพาะทาง ซึ่งจะช่วยให้บริหารจัดการความเสี่ยงทางไซเบอร์ได้อย่างมีประสิทธิภาพสูงสุดภายใต้งบประมาณที่เหมาะสม

ดังนั้นการให้ผู้เชี่ยวชาญจากภายนอกเข้ามาดูแลและประเมินความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรจึงเป็นแนวทางที่สำคัญ เพราะจะช่วยให้ได้รับ มุมมองที่เป็นกลางและอิสระ ซึ่งอาจนำไปสู่การค้นพบช่องโหว่หรือจุดอ่อนที่ทีมงานภายในอาจมองข้ามไปได้ เป็นการเสริมสร้างความแข็งแกร่งให้กับระบบป้องกันโดยรวม ที่จำเป็นต้องมีผู้เชี่ยวชาญเพื่อป้องกัน ตรวจจับ และประเมินภัยคุกคามที่เกิดขึ้น โดยเฉพาะอย่างยิ่งสำหรับสำนักงาน กสทช. ในฐานะองค์กรกำกับดูแลภารกิจสำคัญด้านกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมของประเทศ ซึ่งมีการจัดการข้อมูลสารสนเทศและระบบเทคโนโลยีดิจิทัลจำนวนมาก

๒. วัตถุประสงค์

๒.๑ เพื่อเสริมสร้างความมั่นคงปลอดภัยของระบบสารสนเทศและข้อมูลสำคัญของสำนักงาน กสทช. ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทุกรูปแบบ ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล การเปลี่ยนแปลงแก้ไขข้อมูลโดยมิชอบ และความเสียหายต่อระบบเทคโนโลยีสารสนเทศที่สำคัญขององค์กร

Proof

๒.๒ เพื่อให้การดำเนินงานของสำนักงาน กสทช. เป็นไปอย่างต่อเนื่องและมีเสถียรภาพ สร้างความเชื่อมั่นว่าระบบเทคโนโลยีสารสนเทศที่สนับสนุนภารกิจหลักของ สำนักงาน กสทช. สามารถทำงานได้อย่างต่อเนื่อง

๒.๓ เพื่อให้การปฏิบัติงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงาน กสทช. เป็นไปตามกฎหมาย ข้อกำหนด และมาตรฐานสากล ดำเนินการให้สอดคล้องกับ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และมาตรฐานอื่น ๆ ที่เกี่ยวข้อง เพื่อยกระดับการกำกับดูแลที่ดี

๒.๔ เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการทรัพยากรและยกระดับความเชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงาน กสทช. โดยการเข้าถึงความรู้ความสามารถ เทคโนโลยี และเครื่องมือที่ทันสมัยจากผู้รับจ้างภายนอกที่มีความเชี่ยวชาญเฉพาะทาง ทำให้สามารถบริหารจัดการความเสี่ยงทางไซเบอร์ได้อย่างมีประสิทธิภาพสูงสุดภายใต้งบประมาณที่เหมาะสม

๓. คุณสมบัติของผู้ยื่นข้อเสนอ

ผู้ยื่นข้อเสนอต้องมีคุณสมบัติพื้นฐานที่กำหนด ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ และระบบการจัดซื้อจัดจ้างภาครัฐ (Electronic Government Procurement : e-GP) ตามที่กำหนดในเอกสารประกวดราคาจ้าง ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

๔. ขอบเขตการดำเนินงาน

ผู้รับจ้างต้องเฝ้าระวังตอบสนองและเสนอแนวทางแก้ไขต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Monitoring Services) เป็นระยะเวลา ๑๒ เดือน โดยมีรายละเอียดดังนี้

๔.๑ บริการเฝ้าระวังภัยคุกคาม วิเคราะห์ความเกี่ยวโยงของเหตุการณ์และภัยคุกคามทางไซเบอร์จากระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (Security Information and Event Management : SIEM) ที่สำนักงาน กสทช. มีการใช้งานอยู่ในปริมาณ ๕,๐๐๐ EPS และแก้ไขเหตุการณ์ร่วมกับสำนักงาน กสทช. เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดการดำเนินงานต่อไปนี้

๔.๑.๑ บริการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Monitoring Services) ผ่านช่องทางการเฝ้าระวังระยะไกล (Remote)

๔.๑.๒ แจ้งเตือนภัยคุกคามและเสนอแนวแก้ไขให้กับเจ้าหน้าที่ของสำนักงาน กสทช. ตามข้อกำหนดระดับการให้บริการ (Service Level Agreement : SLA) ในข้อ ๔.๕

๔.๑.๓ ประสานงานกับเจ้าหน้าที่ของสำนักงาน กสทช. ในการดำเนินการจำกัดความเสียหาย (Containment) ในกรณี Critical เช่น การตัดอุปกรณ์ที่ติดเชื้อมัลแวร์ออกจากเครือข่าย จัดภัยคุกคาม (Eradication) และกู้คืนระบบ (Recovery)การป้องกันเพื่อไม่ให้เกิดเหตุซ้ำ

๔.๑.๔ จัดให้มีเจ้าหน้าที่เพื่อดำเนินการเฝ้าระวังภัยคุกคามและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Security Monitoring Services) ระดับ ๑ และระดับ ๒ และ ผู้เชี่ยวชาญ (Security Analyst) ดำเนินการปรับแต่ง Use Cases ของการเฝ้าระวังให้เหมาะสมกับภัยคุกคามที่เกิดขึ้นมาใหม่ ตลอดระยะเวลาสัญญา

๔.๑.๕ จัดทำรายงานประจำสัปดาห์ (Weekly Report) และรายงานประจำเดือน (Monthly Report) รวมทั้งนำส่งรายงานให้แก่สำนักงาน กสทช. ภายในระยะเวลาที่กำหนด โดยมีรายงานอย่างน้อยดังต่อไปนี้

๔.๑.๕.๑ รายงานประจำสัปดาห์ (Weekly Report) ผู้รับจ้างต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ สำนักงาน กสทช. ผ่านช่องทาง e-mail โดยมีรายละเอียดของรายงานดังนี้อย่างน้อย

Proof

(ก.) สรุปการแจ้งเตือนเหตุการณ์ผิดปกติหรือภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารตาม Service Level Agreement (SLA) โดยมีการจัดระดับความรุนแรง

(ข.) สรุปสถานะการดำเนินการบริหารจัดการภัยคุกคามที่พบหรือความผิดปกติที่กระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Incident Management) ที่เกิดขึ้นในแต่ละสัปดาห์ที่ผ่านมา

๔.๑.๕.๒ รายงานประจำเดือน (Monthly Report) ผู้รับจ้างต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ สำนักงาน กสทช. ผ่านช่องทาง e-mail โดยมีรายละเอียดของรายงานดังต่อไปนี้อย่างน้อย

(ก.) บทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security Monitoring) ในแต่ละเดือน

(ข.) สรุปเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เกิดขึ้นในแต่ละเดือน โดยมีการจัดระดับความรุนแรง และวิเคราะห์ผลกระทบต่อการดำเนินธุรกิจของสำนักงาน กสทช.

(ค.) สรุปการแจ้งเตือนเหตุการณ์ผิดปกติหรือภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตาม Service Level Agreement (SLA) และสรุปสถานะการดำเนินการบริหารจัดการภัยคุกคามที่พบหรือความผิดปกติที่กระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Incident Management) ที่เกิดขึ้นในแต่ละเดือน

(ง.) อัพเดทข้อมูลข่าวสารเกี่ยวกับภัยคุกคามร้ายแรงด้านความปลอดภัยสารสนเทศ (Security News) ที่เกิดขึ้นในแต่ละเดือน (ถ้ามี)

๔.๒ ผู้รับจ้างต้องจัดให้มีเจ้าหน้าที่ปฏิบัติงาน ดังนี้

๔.๒.๑ เจ้าหน้าที่ปฏิบัติงาน CSOC ระดับ ๑ มีหน้าที่ดังต่อไปนี้

๔.๒.๑.๑ เฝ้าระวังเหตุการณ์ภัยคุกคามทุกวัน ตลอด ๒๔ ชั่วโมง

๔.๒.๑.๒ ตรวจสอบ วิเคราะห์ เพื่อคัดแยกและประเมินความรุนแรงของเหตุการณ์ภัยคุกคามที่เกิดขึ้น

๔.๒.๑.๓ คัดแยกการแจ้งเตือน และเหตุการณ์ภัยคุกคามที่เป็น False Positive Alerts/Incidents

๔.๒.๑.๔ เก็บรวบรวมข้อมูลเกี่ยวกับการแจ้งเตือน และ เหตุการณ์ภัยคุกคามที่เกิดขึ้น พร้อมทั้งการบันทึกข้อมูลเหตุการณ์และผลการวิเคราะห์ลงบนระบบ Case Management และอัพเดตสถานะของเหตุการณ์ในระบบ

๔.๒.๑.๕ การยับยั้ง หรือ บรรเทาเหตุการณ์ภัยคุกคามที่เกิดขึ้นเบื้องต้น ตามวิธีการที่ผู้ว่าจ้างกำหนด

๔.๒.๑.๖ ทำการยกระดับ (Escalation) เหตุการณ์ภัยคุกคาม โดยการแจ้งเตือนไปยังทีมงานระดับถัดไปตามกระบวนการที่กำหนด

๔.๒.๒ เจ้าหน้าที่ปฏิบัติงาน CSOC ระดับ ๒ มีหน้าที่ดังต่อไปนี้

๔.๒.๒.๑ เฝ้าระวังเหตุการณ์ภัยคุกคามทุกวัน ตลอด ๒๔ ชั่วโมง

๔.๒.๒.๒ ทำการตรวจสอบเชิงลึกและหาสาเหตุของเหตุการณ์ภัยคุกคามที่เกิดขึ้น

๔.๒.๒.๓ ทำการตรวจหาขอบเขตผลกระทบที่เกิดขึ้น

Proof

๔.๒.๒.๔ ทำการรวบรวมการแจ้งเตือนหรือเหตุการณ์ภัยคุกคามที่เหมือนกันเป็นหนึ่งเหตุการณ์ (Correlation)

๔.๒.๒.๕ ทำการระบุภัยคุกคาม หรือช่องโหว่ที่เกิดขึ้นจากเหตุการณ์ภัยคุกคาม

๔.๒.๒.๖ ทำการตรวจสอบเชิงรุกเพิ่มเติมจากเหตุการณ์ภัยคุกคามที่เกิดขึ้น

๔.๒.๒.๗ ให้คำแนะนำในการแก้ไขปัญหาที่เกิดขึ้น หรือช่องโหว่และการฟื้นฟูความเสียหายที่เกิดขึ้น

๔.๒.๒.๘ ทำการวิเคราะห์การจราจรเครือข่าย (Network Traffic) หรือ บันทึก (Log) ที่ต้องสงสัย

๔.๒.๒.๙ จัดทำรายงานเกี่ยวกับเหตุการณ์ภัยคุกคามที่เกิดขึ้น แบบลงรายละเอียดกับเหตุการณ์กับคุกคาม ตั้งแต่เริ่มต้นตรวจพบยับยั้ง ฟื้นฟู แก้ไข ไปจนถึงสรุปบทเรียนที่เกิดขึ้นจากเหตุการณ์ภัยคุกคาม

๔.๒.๓ ผู้เชี่ยวชาญ (Security Analyst) มีหน้าที่ดังนี้

๔.๒.๓.๑ นำและประสานงานการตอบสนองต่อภัยคุกคามในระดับ Critical ที่ถูกยกระดับ (Escalated) จากระดับ L2

๔.๒.๓.๒ ทำการตรวจสอบเชิงลึก (Forensic Analysis) ในกรณีที่จำเป็นต้องมีการตรวจสอบเชิงลึกเพื่อหาหลักฐานเพิ่มเติม

๔.๒.๓.๓ ประสานงานกับเจ้าหน้าที่ของสำนักงาน กสทช. เพื่อกำจัดภัยคุกคาม (Eradication) และกู้คืนระบบ (Recovery) ให้กลับมาใช้งานได้ตามปกติ

๔.๒.๓.๔ จัดทำรายงานเหตุการณ์โดยละเอียดเมื่อเกิดภัยคุกคามในระดับ Critical (Incident Reports) ที่ระบุผลการวิเคราะห์, ข้อสรุป, และข้อเสนอแนะสำหรับการดำเนินการต่อไป

๔.๒.๓.๕ ดำเนินการทำ Threat Hunting เพื่อค้นหาภัยคุกคามที่ยังไม่ถูกตรวจจับภายในเครือข่าย

๔.๓ ผู้รับจ้างจะต้องประสานงานกับเจ้าหน้าที่ของสำนักงาน กสทช. เพื่อจัดการเหตุการณ์ (Incident Ticket) ผ่านทางระบบบริหารจัดการ (Incident Management) ของระบบ SIEM ที่ทางสำนักงาน กสทช. ใช้งาน ดังนี้

๔.๓.๑ การรับและบันทึกเหตุการณ์ (Incident Logging and Ticketing)

๔.๓.๑.๑ ประเภทของเหตุการณ์ (Incident Type) เช่น Malware, Phishing, DDoS, Unauthorized Access

๔.๓.๑.๒ ระดับความรุนแรง (Severity Level) เช่น Critical, High, Medium, Low

๔.๓.๑.๓ แหล่งที่มาของภัยคุกคาม (Source IP/Hostname)

๔.๓.๑.๔ เป้าหมายของภัยคุกคาม (Destination IP/Hostname)

๔.๓.๑.๕ เวลาที่เกิดเหตุการณ์ (Timestamp)

๔.๓.๑.๖ ข้อมูล Log ที่เกี่ยวข้อง

๔.๓.๒ การวิเคราะห์และตรวจสอบ (Analysis and Investigation)

๔.๓.๒.๑ วิเคราะห์ความสัมพันธ์ของข้อมูล (Log Correlation) จากหลายแหล่งที่มาเพื่อหาความเชื่อมโยงของเหตุการณ์และระบุต้นตอของปัญหา

๔.๓.๒.๒ ตรวจสอบเชิงลึก (Forensic Analysis) ในกรณีที่จำเป็นต้องมีการตรวจสอบเชิงลึกเพื่อหาหลักฐานเพิ่มเติม

๔.๓.๒.๓ ระบุผลกระทบ (Impact Assessment) ประเมินผลกระทบของเหตุการณ์ต่อระบบและข้อมูล

๔.๓.๓ การตอบสนองและแก้ไข (Response and Remediation) ในกรณี Critical

Proof

๔.๓.๓.๑ ดำเนินการตาม Playbook หรือขั้นตอนการตอบสนองต่อเหตุการณ์แต่ละประเภทอย่างชัดเจน

๔.๓.๓.๒ จำกัดความเสียหาย (Containment) ไม่ให้ลุกลามไปยังส่วนอื่นๆ ของระบบ

๔.๓.๓.๓ กำจัดภัยคุกคาม (Eradication) ของภัยคุกคามออกจากระบบ

๔.๓.๓.๔ กู้คืนระบบ (Recovery) และข้อมูลให้กลับมาใช้งานได้ตามปกติ

๔.๓.๔ การติดตามและรายงานผล (Monitoring and Reporting)

๔.๓.๔.๑ ติดตามสถานะของ Ticket อย่างสม่ำเสมอ

๔.๓.๔.๒ แจ้งเตือนผู้ที่เกี่ยวข้องเมื่อมีความคืบหน้าหรือเมื่อเหตุการณ์ได้รับการแก้ไขแล้ว

๔.๓.๔.๓ จัดทำรายงานสรุปเหตุการณ์หลังจากการแก้ไขเสร็จสิ้น โดยระบุสาเหตุ ผลกระทบ และแนวทางการป้องกันในอนาคต

๔.๓.๕ การปรับปรุงและพัฒนา (Improvement and Development)

๔.๓.๕.๑ ปรับปรุง Rule ของ SIEM ให้สามารถตรวจจับภัยคุกคามใหม่ๆ ได้อย่างมีประสิทธิภาพ

๔.๓.๕.๒ พัฒนา Playbook/Response action ให้ทันสมัยและสอดคล้องกับสถานการณ์ปัจจุบัน

๔.๔ ผู้รับจ้างต้องฝึกอบรมและถ่ายทอดองค์ความรู้พัฒนาศักยภาพแก่บุคลากรของสำนักงาน กสทช. ให้มีความรู้ความสามารถในการปฏิบัติงานด้าน Cybersecurity Operations ตั้งแต่ระดับพื้นฐานจนถึงระดับเชี่ยวชาญ เพื่อสร้างความยั่งยืนและความมั่นคงปลอดภัยทางไซเบอร์ให้กับองค์กรในระยะยาว โดยใช้การฝึกอบรมในรูปแบบ การฝึกอบรมภาคปฏิบัติ (On-the-Job Training) ในลักษณะร่วมกันทำงานโดยให้คำแนะนำกับเจ้าหน้าที่ของ สำนักงาน กสทช. ที่เป็นการปฏิบัติงานทั่วไปของเจ้าหน้าที่ระดับที่ ๑ (SOC Analyst - Tier ๑) และเจ้าหน้าที่ระดับที่ ๒ (Incident Responder / Threat Analyst - Tier ๒) ในกรณีที่เกิดเหตุการณ์ที่เกี่ยวข้องกับการจัดการระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (Security Information and Event Management: SIEM) ที่สำนักงาน กสทช. มีการใช้งานอยู่ และการฝึกอบรมในห้องเรียน (Classroom Training) หลักสูตรขั้นสูงสำหรับผู้เชี่ยวชาญ จำนวน ๑ ครั้งเป็นเวลา ๔ วัน

๔.๔.๑ เจ้าหน้าที่ระดับที่ ๑ (SOC Analyst - Tier ๑) มีเนื้อหาการอบรมแบบ On-the-Job Training ดังนี้

๔.๔.๑.๑ ความเข้าใจใน Security Log ประเภทต่างๆ (Firewall, IPS/IDS, Proxy, Endpoint, OS, etc.)

๔.๔.๑.๒ การใช้งานเครื่องมือ SIEM และ SOAR ในระดับผู้ใช้งาน (Monitoring Dashboards, Search Query, Alert Handling)

๔.๔.๑.๓ กระบวนการจัดการเหตุการณ์เบื้องต้น (Initial Incident Triage) ตาม Playbook

๔.๔.๑.๔ ความรู้พื้นฐานเกี่ยวกับภัยคุกคามที่พบบ่อย (Common Threats) เช่น Phishing, Malware, Ransomware

๔.๔.๑.๕ การใช้งาน Threat Intelligence Platform เบื้องต้นเพื่อตรวจสอบ Indicators of Compromise (IoCs)

๔.๔.๒ เจ้าหน้าที่ระดับที่ ๒ (Incident Responder / Threat Analyst - Tier ๒) มีเนื้อหาการอบรมแบบ On-the-Job Training ดังนี้

๔.๔.๒.๑ การวิเคราะห์ Log เชิงลึก (Deep-dive Log Analysis)

๔.๔.๒.๒ กระบวนการตอบสนองต่อเหตุการณ์ (Incident Response Lifecycle)

๔.๔.๒.๓ การวิเคราะห์มัลแวร์เบื้องต้น (Basic Malware Analysis)

Proof

๔.๔.๒.๔ การใช้ Threat Intelligence เพื่อการวิเคราะห์และคาดการณ์

๔.๔.๒.๕ การทำความเข้าใจและปฏิบัติตาม Playbook ในการตอบสนองต่อเหตุการณ์ประเภทต่าง ๆ

๔.๔.๒.๖ การเริ่มต้นทำ Threat Hunting จากสมมติฐานเบื้องต้น

๔.๔.๓ จัดการฝึกอบรมในห้องเรียน (Classroom Training) หลักสูตรขั้นสูงสำหรับผู้เชี่ยวชาญโดยมีเนื้อหาการอบรม จำนวน ๔ วัน ไม่น้อยกว่า ๒ คน ดังนี้

๔.๔.๓.๑ เทคนิคการทำ Threat Hunting ขั้นสูง

๔.๔.๓.๒ การทำ Digital Forensics และ Memory Analysis เบื้องต้น

๔.๔.๓.๓ หลักการทำ Reverse Engineering มัลแวร์

๔.๔.๓.๔ การพัฒนา Use Case และกฎการตรวจจับ (Detection Rule) บน SIEM

๔.๔.๓.๕ การพัฒนาและปรับปรุง Incident Response Playbook

๔.๔.๓.๖ การทำความเข้าใจและวิเคราะห์เทคนิคของแฮกเกอร์ตามกรอบ MITRE ATT&CK Framework

๔.๕ คุณภาพการให้บริการ

ผู้รับจ้างต้องให้บริการเฝ้าระวังตอบสนองและเสนอแนวทางแก้ไขต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Monitoring Services) ตามขอบเขตของงานนี้ด้วยคุณภาพและประสิทธิภาพตามข้อกำหนดระดับการให้การ (Service Level Agreement : SLA) ดังนี้

ระดับความรุนแรงของปัญหา	สถานการณ์	ช่องทางการให้บริการ	ระยะเวลาการแจ้งเตือน
Critical	ผลกระทบรุนแรงกับ Critical Asset ในระดับวงกว้าง ทำให้การทำงานสำคัญหยุดชะงัก	บริการแก้ไขปัญหาแบบ Remote Access/Onsite	แจ้งเตือนภายใน ๓๐ นาที และเสนอแนวทางแก้ไขเหตุการณ์ผิดปกติหรือภัยคุกคามด้านเทคโนโลยีสารสนเทศภายใน ๔ ชั่วโมง
High	ผลกระทบกับหลายระบบพร้อมๆกัน ถึงแม้ระบบสำคัญยังใช้การได้	บริการแก้ไขปัญหาแบบ Remote Access/Onsite	แจ้งเตือนภายใน ๑ ชั่วโมง และเสนอแนวทางแก้ไขเหตุการณ์ผิดปกติหรือภัยคุกคามด้านเทคโนโลยีสารสนเทศภายใน ๘ ชั่วโมง
Medium	ตรวจพบเจอพฤติกรรมที่ผิดปกติที่อาจลุกลามหรือรุนแรงมากขึ้นถ้าไม่ตรวจสอบ	บริการแก้ไขปัญหาแบบ Remote Access/Onsite	แจ้งเตือนภายใน ๓ ชั่วโมง และเสนอแนวทางแก้ไขเหตุการณ์ผิดปกติหรือภัยคุกคามด้านเทคโนโลยีสารสนเทศภายใน ๒๔ ชั่วโมง
Low	ตรวจพบเจอเหตุการณ์แต่ไม่พบการเชื่อมโยงหรือทำให้เชื่อได้ว่าเหตุการจะลุกลาม	บริการแก้ไขปัญหาแบบ Remote Access/Onsite	แจ้งเตือนภายใน ๖ ชั่วโมง และเสนอแนวทางแก้ไขเหตุการณ์ผิดปกติหรือภัยคุกคามด้านเทคโนโลยีสารสนเทศ ภายใน ๑ สัปดาห์

Proof

ทั้งนี้ ระยะเวลาที่กำหนดดังกล่าวข้างต้น ให้ยึดถือรายการบันทึก (Log) ในระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (Security Information and Event Management : SIEM)

๕. บุคลากรของผู้รับจ้าง

บุคลากรของผู้รับจ้างต้องจัดให้มีเจ้าหน้าที่ที่มีความรู้ความชำนาญเพื่อดำเนินงานตามขอบเขตงาน โดยมีคุณสมบัติอย่างน้อย ดังนี้

๕.๑ เจ้าหน้าที่ปฏิบัติงาน CSOC ระดับ ๑ ไม่น้อยกว่า ๓ คน โดยได้รับใบรับรองด้านความมั่นคงปลอดภัยไซเบอร์หรือประกาศนียบัตรอย่างน้อย ๑ ใบ ดังนี้

- CompTIA Sec+ หรือ
- CompTIA CySA+

๕.๒ เจ้าหน้าที่ปฏิบัติงาน CSOC ระดับ ๒ ไม่น้อยกว่า ๓ คน โดยได้รับใบรับรองด้านความมั่นคงปลอดภัยไซเบอร์หรือประกาศนียบัตรอย่างน้อย ๑ ใบ ดังนี้

- CompTIA CASP+ หรือ
- CompTIA Security X

๕.๓ ผู้เชี่ยวชาญ ที่ได้รับใบรับรองหรือประกาศนียบัตรด้านความมั่นคงปลอดภัยไซเบอร์ โดยต้องมีคุณสมบัติรวมกันอย่างน้อยดังนี้

- LogRhythm Platform Administrator (LRPA) หรือ LogRhythm Security Analyst (LRSA)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certification Certified Information Systems Auditor (CISA)

๖. กำหนดการส่งมอบพัสดุ

ภายในระยะเวลา ๓๖๕ วัน นับจากลงนามในสัญญา

๗. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

สำนักงาน กสทช. จะพิจารณาคัดเลือกข้อเสนอโดยใช้เกณฑ์ราคา

๘. วงเงินที่ใช้ในการจัดหา

ภายในวงเงินงบประมาณ ๓,๐๐๐,๐๐๐.- บาท (สามล้านบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่มและค่าใช้จ่ายทั้งปวงไว้แล้ว โดยเบิกจ่ายจากงบประมาณรายจ่ายประจำปี ๒๕๖๙ สำนักเทคโนโลยีสารสนเทศ รายจ่ายเกี่ยวกับการจัดการและบริหารองค์กร หมวดค่าใช้สอย รายการค่าจ้างเหมาบริการ

๙. งวดงานและการจ่ายเงิน

สำนักงาน กสทช. จะจ่ายเงินค่าจ้างเมื่อผู้รับจ้างส่งมอบงานตามงวดงานที่กำหนดและคณะกรรมการตรวจรับพัสดุได้ตรวจรับเรียบร้อยแล้วโดยมีรายละเอียดดังต่อไปนี้ (แต่ละงวดจำนวน ๔ ชุด) พร้อมบันทึกข้อมูลแบบ Thumb Drive จำนวน ๑ ชุด (ไฟล์ Word และ PDF)

งวดที่ ๑ จ่ายร้อยละ ๒๕ ของค่าจ้างตามสัญญา เมื่อส่งมอบรายงานตามข้อ ๔.๑.๕.๑ และข้อ ๔.๑.๕.๒ ภายใน ๙๐ วัน นับถัดจากวัน ลงนามในสัญญา

งวดที่ ๒ จ่ายร้อยละ ๒๕ ของค่าจ้างตามสัญญา เมื่อส่งมอบรายงานตามข้อ ๔.๑.๕.๑ และข้อ ๔.๑.๕.๒ ภายใน ๑๘๐ วัน นับถัดจากวัน ลงนามในสัญญา

Proof

งวดที่ ๓ จ่ายร้อยละ ๒๕ ของค่าจ้างตามสัญญา เมื่อส่งมอบรายงานตามข้อ ๔.๑.๕.๑ และข้อ ๔.๑.๕.๒ ภายใน ๒๗๐ วัน นับถัดจากวัน ลงนามในสัญญา

งวดที่ ๔ จ่ายร้อยละ ๒๕ ของค่าจ้างตามสัญญา เมื่อส่งมอบรายงานตามข้อ ๔.๑.๕.๑ และข้อ ๔.๑.๕.๒ ภายใน ๓๖๕ วัน นับถัดจากวัน ลงนามในสัญญา

๑๐. อัตราค่าปรับ

๑๐.๑ หากผู้ว่าจ้างพบว่าผู้รับจ้างไม่ดำเนินงานให้เป็นไปตามข้อกำหนดขอบเขตของงาน (สัญญา) ต้องชำระค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๑ ของค่าจ้างตามสัญญา นับถัดจากวันที่ผู้จ้างตรวจพบและได้แจ้งให้ทราบแล้ว จนถึงวันที่ดำเนินงานหรือแก้ไขการดำเนินงานให้ถูกต้องครบถ้วน

๑๐.๒ กรณีที่ผู้รับจ้างไม่สามารถดำเนินงานให้เป็นไปตามข้อกำหนดคุณภาพการบริการ (Service Level Agreement : SLA) ตามข้อ ๔.๕ ผู้รับจ้างต้องยินยอมให้คิดค่าปรับเป็นรายชั่วโมงในอัตราร้อยละ ๐.๐๓๕ ของค่าจ้างตามสัญญา นับจากเวลาที่ครบกำหนดจนถึงเวลาที่ผู้รับจ้างดำเนินการแจ้งเตือนเหตุการณ์หรือกำหนดเวลาเสนอแนวทางแก้ไข แล้วเสร็จแล้วแต่กรณี

๑๐.๓ กรณีที่ผู้รับจ้างไม่สามารถตอบสนองและเสนอแนวทางแก้ไขเหตุการณ์ผิดปกติหรือภัยคุกคามด้านเทคโนโลยีสารสนเทศ ที่ได้รับความเสียหาย ต้องยินยอมให้คิดค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๑ ของค่าจ้างตามสัญญา นับถัดจากวันที่ครบกำหนดจนถึงวันที่แก้ไขเหตุการณ์ผิดปกติหรือภัยคุกคามด้านเทคโนโลยีสารสนเทศแล้วเสร็จ

๑๑. การปฏิบัติตามกฎหมายที่เกี่ยวข้อง

๑๑.๑ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ชนะ หรือผู้ได้รับการคัดเลือก จะต้องต้องดำเนินการดังนี้

๑๑.๑.๑ ปฏิบัติให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กฎหมาย ระเบียบ ข้อบังคับต่าง ๆ ที่เกี่ยวข้อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงาน กสทช. ฉบับล่าสุด ซึ่งรวมถึงหลักการวิศวกรรมความมั่นคงปลอดภัย (แบบฟอร์มความต้องการด้านความมั่นคงปลอดภัยของระบบทางด้านเทคนิค (System Security Requirement)

๑๑.๑.๒ กรณีมีการใช้บริการคลาวด์ (Cloud) ต้องปฏิบัติตามข้อกำหนดด้านการใช้บริการคลาวด์ (Cloud Security Requirement) ตามที่ผู้ว่าจ้างกำหนด

๑๑.๑.๓ ตรวจสอบความมั่นคงปลอดภัยของซอร์สโค้ด (Source Code Scanning) และดำเนินการแก้ไขก่อนนำระบบขึ้นให้บริการ

๑๑.๒ กรณีที่ขอบเขตของงานเกี่ยวข้องกับการประมวลผล (เก็บรวบรวม ใช้ เปิดเผย) ข้อมูลส่วนบุคคลผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้ชนะ หรือผู้ได้รับการคัดเลือก ต้องดำเนินการตามเงื่อนไขและรายละเอียดตามที่กำหนดไว้ในข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) กับสำนักงาน กสทช. (ตามภาคผนวก)

๑๒. เงื่อนไขอื่นๆ

๑๒.๑ ข้อมูลของสำนักงาน กสทช. ถือเป็นความลับของทางราชการ ห้ามมิให้นำไปเผยแพร่

๑๒.๒ การกระทำการใดๆ ของทีมงานผู้รับจ้างอันอาจจะก่อผลให้เกิดความเสียหายต่อระบบที่เสนอ ผู้รับจ้างจะต้องแจ้งและได้รับอนุญาตจากเจ้าหน้าที่ผู้รับผิดชอบของสำนักงาน กสทช. ก่อนสำนักงานสำนักงาน กสทช. สงวนสิทธิ์ในการตรวจสอบข้อเท็จจริงที่เสนอ หากพบว่าไม่สามารถดำเนินการได้ตามที่ระบุสำนักงาน กสทช. จะยกเลิกสัญญาและเรียกร้องค่าเสียหายจากผู้รับจ้างหรือคู่สัญญา

๑๒.๓ สำนักงาน กสทช. ขอสงวนสิทธิ์ในการยกเลิกประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ได้ในทุกขั้นตอน เพื่อประโยชน์ของสำนักงาน กสทช. เป็นสำคัญ โดยถือว่าการตัดสินของสำนักงาน กสทช.เป็นเด็ดขาด และผู้ยื่น

ข้อเสนอจะเรียกร้องค่าเสียหายใด ๆ มิได้ ทั้งนี้ สำนักงาน กสทช. จะพิจารณายกเลิกการดำเนินการจัดจ้างและลงโทษผู้ยื่นข้อเสนอเป็นผู้ทิ้งงาน ไม่ว่าจะเป็นผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกหรือไม่ก็ตาม หากมีเหตุที่เชื่อถือได้ว่าการยื่นข้อเสนอกระทำการโดยไม่สุจริต เช่น การเสนอเอกสารอันเป็นเท็จ การใช้ชื่อบุคคลธรรมดา หรือนิติบุคคลอื่นมายื่นข้อเสนอแทน เป็นต้น

๑๒.๔ ผู้รับจ้างต้องส่งรายงานผลการใช้พัสดุที่ผลิตในประเทศ พร้อมเหตุผลความจำเป็นที่ไม่ได้เป็นไปตามแผน (ถ้ามี) เพื่อให้คณะกรรมการตรวจรับพัสดุตรวจสอบด้วย

๑๒.๕ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกจะต้องจัดทำแผนการดำเนินงานให้บรรลุความสำเร็จตามขอบเขตของงานภายในระยะเวลาที่กำหนดตามสัญญา โดยแสดงรายละเอียดแผนการดำเนินการและร้อยละของความสำเร็จของงานแต่ละเดือน ส่งให้คณะกรรมการตรวจรับพัสดุ ภายใน ๑๕ วัน นับถัดจากวันลงนามในสัญญา เพื่อกำกับและติดตามความก้าวหน้าในผลการดำเนินงาน ทั้งนี้ แผนการดำเนินงานดังกล่าว สำนักงาน กสทช. ถือเป็นส่วนหนึ่งของสัญญา

Proof

ภาคผนวก

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล
(Data Processing Agreement : DPA) กับสำนักงาน กสทช.

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล ("ข้อตกลง") นี้ จัดทำขึ้นเพื่อให้สอดคล้องกับหน้าที่ของสำนักงาน กสทช. และ ผู้ประมวลผลข้อมูลส่วนบุคคลตามมาตรา ๔๐ วรรคสามและมาตรา ๓๗ (๒) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และข้อ ๖ ของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และถือเป็นส่วนหนึ่งของ (ให้ระบุว่าเป็นงานตามขอบเขตของงาน) ซึ่งสำนักงาน กสทช. มีฐานะเป็น "ผู้ควบคุมข้อมูลส่วนบุคคล" และ ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก มีฐานะเป็น "ผู้ประมวลผลข้อมูลส่วนบุคคล" ซึ่งเป็นผู้ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผย ("ประมวลผล") ข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของสำนักงาน กสทช. โดยผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการเพื่อวัตถุประสงค์ดังต่อไปนี้

๑. <u>เพื่อดูแล ตรวจสอบ เฝ้าระวัง และตอบสนองต่อภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้อย่างทันท่วงทีและมีประสิทธิภาพสูงสุด เพื่อปกป้องสินทรัพย์สารสนเทศที่สำคัญขององค์กร ข้อมูลของประชาชนผู้ใช้บริการ</u>

๒. <u>เพื่อเสริมสร้างความมั่นคงปลอดภัยของระบบสารสนเทศและข้อมูลสำคัญของสำนักงาน กสทช. ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทุกรูปแบบ ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล การเปลี่ยนแปลงแก้ไขข้อมูลโดยมิชอบ และความเสียหายต่อระบบเทคโนโลยีสารสนเทศที่สำคัญขององค์กร</u>

โดยข้อมูลส่วนบุคคลที่มีการประมวลผลตามวัตถุประสงค์ข้างต้น ประกอบด้วย

๑. <u>ชื่อ นามสกุล เบอร์โทรศัพท์ อีเมล IP address ข้อมูลผู้ใช้งานแอปพลิเคชั่นของรัฐ หรือข้อมูลของประชาชนผู้ใช้บริการ เป็นต้น</u>

๒. <u>ประเภทไฟล์เอกสาร/ประเภทไฟล์อิเล็กทรอนิกส์</u>

๓. <u>ข้อมูลอื่นใดที่อาจมีความจำเป็นเพื่อให้บรรลุวัตถุประสงค์ตามขอบเขตงานในบันทึกข้อตกลงความร่วมมือสัญญาหลัก</u>

การควบคุมดูแลการประมวลผลข้อมูลส่วนบุคคลที่สำนักงาน กสทช. มอบหมายหรือแต่งตั้งให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการ ซึ่งจะต้องดำเนินการตามหน้าที่และความรับผิดชอบตามขอบเขตงานในบันทึกข้อตกลงความร่วมมือสัญญาหลัก และดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชกฤษฎีกา ระเบียบ และประกาศ ที่ออกตามความในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงนี้ รวมเรียกว่า "กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล" ทั้งที่มีผลใช้บังคับอยู่นับแต่วันที่มีการทำ บันทึกข้อตกลงความร่วมมือสัญญาหลัก และที่จะมีการแก้ไขเพิ่มเติมในภายหลัง โดยผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งต่อไปนี้เรียกว่า "ผู้ประมวลผลข้อมูลส่วนบุคคล" ต้องดำเนินงานตามบันทึกข้อตกลงความร่วมมือสัญญาหลัก ในส่วนของข้อมูลตามที่กำหนดในวัตถุประสงค์ข้างต้น ให้เป็นไปตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล มีรายละเอียดดังนี้

๑. ผู้ประมวลผลข้อมูลส่วนบุคคลรับทราบว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดยจะดำเนินการตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย

๒. ผู้ประมวลผลข้อมูลส่วนบุคคลจะกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้จำกัดเฉพาะบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงนี้เท่านั้น และจะ

Proof

ดำเนินการเพื่อให้บุคคลดังกล่าวทำการประมวลผลและรักษาความลับของข้อมูลส่วนบุคคลตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้

๓. ผู้ประมวลผลข้อมูลส่วนบุคคลจะควบคุมดูแลให้บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และดำเนินการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ของการดำเนินการตามขอบเขตงานในบันทึกข้อตกลงความร่วมมือสัญญาหลัก หรือที่แก้ไขเพิ่มเติมในภายหลัง โดยจะไม่ทำซ้ำ คัดลอก ทำสำเนา บันทึกภาพข้อมูลส่วนบุคคลไม่ว่าทั้งหมดหรือแต่บางส่วนเป็นอันขาด เว้นแต่เป็นไปตามเงื่อนไขของขอบเขตงานในบันทึกข้อตกลงความร่วมมือสัญญาหลัก หรือที่แก้ไขเพิ่มเติมในภายหลัง หรือกฎหมายที่เกี่ยวข้องที่กำหนดไว้เป็นประการอื่น

๔. ผู้ประมวลผลข้อมูลส่วนบุคคลจะดำเนินการเพื่อช่วยเหลือหรือสนับสนุนสำนักงาน กสทช. ในการตอบสนองต่อคำร้องที่เจ้าของข้อมูลส่วนบุคคลแจ้งต่อสำนักงาน กสทช. ในการตอบสนองต่อคำร้องที่เจ้าของข้อมูลส่วนบุคคลแจ้งต่อสำนักงาน กสทช. อันเป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในขอบเขตงานในบันทึกข้อตกลงความร่วมมือสัญญาหลัก ในกรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิดังกล่าวต่อผู้ประมวลผลข้อมูลส่วนบุคคลโดยตรง ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องดำเนินการแจ้งและส่งคำร้องดังกล่าวให้แก่สำนักงาน กสทช. ทันที โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่เป็นผู้ตอบสนองต่อคำร้องดังกล่าว เว้นแต่สำนักงาน กสทช. จะได้มอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเฉพาะเรื่องที่เกี่ยวข้องกับคำร้องดังกล่าว

๕. ผู้ประมวลผลข้อมูลส่วนบุคคลจะจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing) ทั้งหมดที่ผู้ประมวลผลข้อมูลส่วนบุคคลประมวลผลในขอบเขตงานในบันทึกข้อตกลงความร่วมมือสัญญาหลัก และจะดำเนินการส่งมอบบันทึกรายการดังกล่าวให้แก่สำนักงาน กสทช. ภายใน ๓๐ วันนับถัดจากวันลงนามในสัญญา หรือเมื่อสำนักงาน กสทช. ร้องขอเป็นลายลักษณ์อักษร

๖. ผู้ประมวลผลข้อมูลส่วนบุคคลจะจัดให้มีและคงไว้ซึ่งมาตรการรักษาความมั่นคงปลอดภัยสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเหมาะสมทั้งมาตรการเชิงองค์กรและเชิงเทคนิค รวมถึงมาตรการทางกายภาพที่จำเป็นตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕ และตามประกาศสำนักงาน กสทช. เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงาน กสทช. รวมถึงที่ได้มีการแก้ไขเพิ่มเติมในอนาคต โดยคำนึงถึงระดับความเสี่ยงตามลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดในขอบเขตงานในบันทึกข้อตกลงความร่วมมือสัญญาหลัก เป็นสำคัญ เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิด อุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือไม่ชอบด้วยกฎหมาย เป็นต้น โดยต้องจัดให้มีมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะหรือประเภทของข้อมูลส่วนบุคคล ลักษณะ ประเภท หรือสถานะของเจ้าของข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

Proof

๗. เว้นแต่กฎหมายที่เกี่ยวข้องจะบัญญัติไว้เป็นประการอื่น ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องส่งคืนข้อมูลส่วนบุคคลให้กับสำนักงาน กสทช. หรือดำเนินการลบ ทำลาย ยกเลิกการเข้าถึง หรือทำให้เป็นข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ ทั้งนี้ ตามที่สำนักงาน กสทช. กำหนดโดยทันทีเมื่อการดำเนินการประมวลผลตามวัตถุประสงค์ของขอบเขตงานในบันทึกข้อตกลงความร่วมมือสัญญาหลัก เสร็จสิ้นลง โดยผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องควบคุมดูแล ตรวจสอบ และรับรองว่าข้อมูลส่วนบุคคลดังกล่าวจะไม่อยู่ในความครอบครองของตนเองและของบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคลอีกต่อไป

๘. เหตุแห่งการละเมิดข้อมูลส่วนบุคคล

๘.๑ ในกรณีที่ ผู้ประมวลผลข้อมูลส่วนบุคคลได้ทราบหรือมีเหตุอันควรทราบว่ามีเหตุแห่งการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น ภายใน ๒๔ ชั่วโมงนับแต่ทราบหรือมีเหตุอันควรทราบถึงเหตุแห่งการละเมิดข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการดังต่อไปนี้

(ก) ให้ข้อมูลที่จำเป็นแก่สำนักงาน กสทช. เพื่อให้สำนักงาน กสทช. สามารถปฏิบัติหน้าที่ภายใต้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและทันภายในระยะเวลาที่กฎหมายกำหนด เช่น ลักษณะของเหตุแห่งการละเมิดข้อมูลส่วนบุคคล ประเภทและจำนวนโดยประมาณของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากเหตุแห่งการละเมิด และรายละเอียดของเจ้าของข้อมูลส่วนบุคคลดังกล่าว ผลกระทบที่อาจเกิดขึ้นได้จากเหตุแห่งการละเมิด มาตรการที่ได้ดำเนินการแล้วหรือที่จะเสนอให้ดำเนินการและมาตรการที่จะเยียวยาผลกระทบที่อาจเกิดขึ้นจากเหตุแห่งการละเมิดข้อมูลส่วนบุคคลนั้น

(ข) ให้ความร่วมมืออย่างเต็มที่กับสำนักงาน กสทช. และดำเนินการใด ๆ ตามที่สำนักงาน กสทช. กำหนดเพื่อช่วยในการดำเนินการตรวจสอบ บรรเทา และเยียวยาความเสียหายอันเกิดจากเหตุแห่งการละเมิดข้อมูลส่วนบุคคลนั้น

๘.๒ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องไม่เปิดเผยเหตุแห่งการละเมิดข้อมูลส่วนบุคคลให้แก่บุคคลอื่นใดทราบโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช. ก่อน เว้นแต่กรณีที่เป็นการปฏิบัติตามกฎหมาย

๘.๓ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องชดใช้บรรดาค่าใช้จ่ายที่เกิดขึ้นจริงในการดำเนินการใด ๆ เพื่อจัดการเหตุแห่งการละเมิดข้อมูลส่วนบุคคลให้แก่สำนักงาน กสทช. หากปรากฏว่า ผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลของ ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลช่วงที่อยู่ในความรับผิดชอบของตนเป็นผู้ก่อให้เกิดเหตุแห่งการละเมิดข้อมูลส่วนบุคคลดังกล่าวนั้น

๙. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

๙.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลรับรองและยืนยันว่าจะไม่ส่งหรือโอน หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลภายใต้ขอบเขตงานใน บันทึกข้อตกลงความร่วมมือสัญญาหลัก ไปยังต่างประเทศโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช.

๙.๒ ในกรณีที่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช. แล้ว ผู้ประมวลผลข้อมูลส่วนบุคคลสามารถส่งหรือโอน หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลภายใต้ขอบเขตงานในบันทึกข้อตกลงความร่วมมือสัญญาหลัก ไปยังต่างประเทศได้ ทั้งนี้ การส่งหรือโอน หรืออนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลดังกล่าวจะต้องกระทำภายใต้บทบัญญัติของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งเป็นลายลักษณ์อักษรของสำนักงาน กสทช. เท่านั้น โดย ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องเข้าทำข้อตกลงเพิ่มเติมหรือจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลบังคับใช้

๑๐. การให้บริการช่วง

๑๐.๑ ภายใต้หน้าที่และขอบเขตงานที่กำหนดใน บันทึกข้อตกลงความร่วมมือสัญญาหลัก ผู้ประมวลผลข้อมูลส่วนบุคคล ไม่สามารถว่าจ้างหรือแต่งตั้งบุคคลภายนอกเป็นผู้ประมวลผลข้อมูลส่วนบุคคลช่วงเพื่อทำการประมวลผลข้อมูลส่วนบุคคลตามขอบเขตงานใน บันทึกข้อตกลงความร่วมมือสัญญาหลัก ในนามของสำนักงาน กสทช. ได้ เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากสำนักงาน กสทช. ก่อน

Proof

๑๐.๒ ในกรณีที่ ผู้ประมวลผลข้อมูลส่วนบุคคลได้รับอนุญาตให้สามารถว่าจ้างผู้ประมวลผลข้อมูลส่วนบุคคลช่วงได้ตามข้อ ๑๐.๑ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดทำข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคลช่วงเป็นลายลักษณ์อักษร โดยกำหนดขอบเขตเนื้อหาและหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลช่วงให้สอดคล้องกับหน้าที่และความรับผิดชอบของ ผู้ประมวลผลข้อมูลส่วนบุคคลตามข้อตกลงนี้

ในกรณีที่สำนักงาน กสทช. ร้องขอเป็นลายลักษณ์อักษร ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการตรวจสอบการปฏิบัติหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลช่วงในส่วนที่เกี่ยวกับข้อมูลส่วนบุคคลที่ได้รับจากสำนักงาน กสทช. และจัดทำผลการตรวจสอบ รวมทั้งส่งมอบผลการตรวจสอบให้แก่สำนักงาน กสทช. ในกรณีที่ปรากฏว่าผู้ประมวลผลข้อมูลส่วนบุคคลช่วงไม่ปฏิบัติตามหรือมีเหตุอันควรเชื่อว่าผู้ประมวลผลข้อมูลส่วนบุคคลช่วงอาจไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรืออาจก่อให้เกิดความเสียหายต่อสำนักงาน กสทช. ไม่ว่าในกรณีใด ๆ สำนักงาน กสทช. อาจขอให้ ผู้ประมวลผลข้อมูลส่วนบุคคลเปลี่ยนผู้ประมวลผลข้อมูลส่วนบุคคลช่วงได้ทันที โดยสำนักงาน กสทช. ไม่ต้องรับผิดในความเสียหายหรือค่าใช้จ่ายใด ๆ อันเกิดจากการเปลี่ยนผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

๑๑.การตรวจสอบ

๑๑.๑ ในกรณีที่สำนักงาน กสทช. มีการร้องขอเป็นลายลักษณ์อักษร ผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการส่งมอบข้อมูลที่จำเป็นทั้งหมดให้แก่สำนักงาน กสทช. เพื่อเป็นการปฏิบัติหน้าที่ตามข้อตกลงนี้

๑๑.๒ ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงอนุญาตให้สำนักงาน กสทช. และบุคคลที่ได้รับมอบหมายจากสำนักงาน กสทช. เข้าตรวจสอบการปฏิบัติหน้าที่ของ ผู้ประมวลผลข้อมูลส่วนบุคคลในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลภายใต้ข้อตกลงนี้ โดยสำนักงาน กสทช. จะแจ้งให้ ผู้ประมวลผลข้อมูลส่วนบุคคลทราบล่วงหน้าเป็นลายลักษณ์อักษรไม่น้อยกว่า ๗ วัน และ ผู้ประมวลผลข้อมูลส่วนบุคคลตกลงให้ความร่วมมือแก่สำนักงาน กสทช. และบุคคลที่ได้รับมอบหมายจากสำนักงาน กสทช. ในการเข้าตรวจสอบดังกล่าวข้างต้น

๑๒.การชดใช้และการเยียวยา

ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องชดใช้ค่าเสียหายหรือค่าใช้จ่ายใด ๆ ให้แก่สำนักงาน กสทช. ในกรณีที่เกิดความเสียหาย การสูญหาย การเรียกร้อง ค่าเสียหาย ความรับผิดทางแพ่ง โทษปรับทางปกครอง หรือค่าใช้จ่ายใด ๆ ที่เกิดขึ้นต่อบุคคลภายนอก หรือในกรณีที่สำนักงาน กสทช. จะต้องรับผิดอันเนื่องมาจากการไม่ปฏิบัติตามข้อใดข้อหนึ่งภายใต้ข้อตกลงนี้หรือตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือการละเมิดคำรับรองและรับประกันของ ผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลที่ได้รับมอบหมายจากผู้ประมวลผลข้อมูลส่วนบุคคลให้ปฏิบัติหน้าที่ประมวลผลข้อมูลส่วนบุคคล ผู้รับจ้างช่วง ผู้ประมวลผลข้อมูลส่วนบุคคลช่วง หรือตัวแทนของ ผู้ประมวลผลข้อมูลส่วนบุคคล

๑๓.การบอกกล่าว

บรรดาคำบอกกล่าวหรือการติดต่อสื่อสารใด ๆ ตามข้อตกลงนี้ ให้ทำเป็นลายลักษณ์อักษร โดยให้ส่งโดยบุคคล หรือไปรษณีย์ หรือโทรสาร ไปยังสถานที่ของผู้รับตามที่ระบุไว้ในข้อตกลงนี้ หรือตามที่ได้รับแจ้งเปลี่ยนแปลงจากผู้รับ (ถ้ามี) คำบอกกล่าวหรือการติดต่อสื่อสารทั้งหลายจะถือว่าผู้รับได้รับแล้วเมื่อคำบอกกล่าวหรือการติดต่อสื่อสารนั้นไปถึงสถานที่นั้นแล้ว

๑๔. หน้าที่และความรับผิดของผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตามข้อตกลงนี้จะสิ้นสุดลงนับแต่วันที่การปฏิบัติงานตามขอบเขตงานใน บันทึกข้อตกลงความร่วมมือสัญญาหลัก เสร็จสิ้น หรือวันที่ ผู้ประมวลผลข้อมูลส่วนบุคคลและสำนักงาน กสทช. ได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิกการดำเนินการตามขอบเขตงานนี้แล้วแต่กรณีใดจะเกิดขึ้นก่อน โดยคู่สัญญาตกลงจะไม่โอนสิทธิเรียกร้องตามข้อตกลงนี้ให้แก่บุคคลอื่น