

เอกสารนำเสนอ
คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ของ ปค.



โครงการผู้ให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ของ
กรมการปกครอง (Security Operation Center : SOC)
ประจำปีงบประมาณ พ.ศ. 2569
งบประมาณ 3,959,000 บาท

ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง
กรมการปกครอง กระทรวงมหาดไทย
ธันวาคม 2567

สารบัญ

แบบรายงานสรุปโครงการเพื่อพิจารณาความเหมาะสมของคุณลักษณะเฉพาะ หน้า

เอกสารเกณฑ์มาตรฐานราคากลาง

ภาคผนวก ก.

ส่วนที่ 1 : บทสรุปโครงการ

1. ชื่อโครงการและหน่วยงานที่รับผิดชอบ	1
2. วัตถุประสงค์และเป้าหมายของโครงการ	1
3. หน้าที่ความรับผิดชอบของหน่วยงาน	1
4. ระบบงาน	2
5. การเตรียมบุคลากรผู้ปฏิบัติโครงการ	2
6. วงเงินค่าใช้จ่าย และแหล่งที่มาของเงิน	2

ส่วนที่ 2 : รายละเอียดโครงการที่เสนอขออนุมัติ

1. ชื่อโครงการ	4
2. ส่วนราชการ	4
3. หน่วยงาน	4
4. ระบบงานที่ขออนุมัติ	6
4.1 วัตถุประสงค์และเป้าหมาย	6
4.2 รายละเอียดอุปกรณ์คอมพิวเตอร์ที่ขออนุมัติ	
4.3 ค่าใช้จ่าย	6
4.4 ระยะเวลาดำเนินงาน	7
5. ผลประโยชน์ที่คาดว่าจะได้รับ	7

ใบเสนอราคา (คู่เทียบ)

ภาคผนวก ข.

รายละเอียดอุปกรณ์คอมพิวเตอร์

ภาคผนวก ค.

ภาคผนวก ก.

แบบรายงานสรุปโครงการเพื่อพิจารณาความเหมาะสมของมูลค่างานและราคา (ก่อนการจัดทำ)

☒ เสนอคณะกรรมการฯ ของ มท. เพื่อพิจารณาให้ความเห็นชอบในหลักการ

☐ เสนอคณะกรรมการฯ ของ ปค. เพื่อพิจารณาให้ความเห็นชอบในหลักการ (ได้รับความเห็นชอบในหลักการจากคณะกรรมการฯ ของ ปค. ในการประชุมครั้งที่ เมื่อวันที่)

ชื่อ : โครงการผู้ให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ของกรมการปกครอง (Security Operation Center : SOC) ประจำปีงบประมาณ พ.ศ. 2569

รวมวงเงินโครงการ จำนวนเงิน 3,959,000 บาท

ส่วนที่เป็นอุปกรณ์คอมพิวเตอร์ จำนวนเงิน 3,584,500 บาท

ชื่อหน่วยงาน ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง

ส่วนที่เป็นอุปกรณ์คอมพิวเตอร์

กรณีตรงตามเกณฑ์ของกระทรวงดิจิทัลฯ หรือเกณฑ์ที่ส่วนราชการอื่นประกาศกำหนด

ลำดับ	รายการ	ชื่อ (ตามเกณฑ์ MICT)	ราคา MICT	ราคาอ้างอิง	จำนวน	วงเงินรวม

กรณีไม่มีราคาตามเกณฑ์ของกระทรวงดิจิทัลฯ หรือเกณฑ์ที่ส่วนราชการอื่นประกาศกำหนด

ลำดับ	รายการ	การสืบราคาจากท้องตลาด รวมทั้งเว็บไซต์ต่างๆ (เปรียบเทียบอย่างน้อย 3 ราย/ 3 ยี่ห้อ รวมทั้งเว็บไซต์อย่างน้อย 1 เว็บไซต์)			จำนวน	วงเงินรวม	หมายเหตุ
		PTT Digital Solution Co.,LTD. โพรซ์ จำกัด	บ. ไอ ซู เอ็มคอนน์ บ. โซ ซิเคียว จำกัด	รวมทั้งหมดเว็บไซต์ (อย่างน้อย 1 เว็บไซต์)			
1	ระบบเก็บรวบรวมและวิเคราะห์ข้อมูลความปลอดภัยทางเครือข่าย	1,712,000.00	1,712,000.00		1	1,712,000.00	
2	บริการตรวจจับและตอบสนองต่อภัยคุกคามไซเบอร์ (EDR)	3,745.00	4,066.00		100	374,500.00	
3	ระบบบริหารจัดการ Web Application Firewall on cloud (Cloud-WAF)	107,000.00	107,000.00		3	321,000.00	
4	บริหารจัดการ CSOC Monitoring	588,500.00	609,900.00		1	588,500.00	
5	เจ้าหน้าที่ผู้เชี่ยวชาญ ระดับ 1 ตลอด 24 ชม.	588,500.00	609,900.00		1	588,500.00	
รวมจำนวนเงินที่ไม่เป็นไปตามเกณฑ์ราคากลางๆ						3,584,500.00	

ส่วนที่เป็นอุปกรณ์อื่นๆ

ลำดับ	รายการ			จำนวนเงิน	จำนวน	จำนวนเงินรวม
1	ค่าติดตั้ง			3,745,200	1 งาน	374,500
						ภาษีมูลค่าเพิ่ม 7%

ส่วนที่ 1 บทสรุปโครงการ

1. ชื่อโครงการและหน่วยงานที่รับผิดชอบ

ชื่อโครงการ : โครงการผู้ให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ของ
กรมการปกครอง (Security Operation Center : SOC) ประจำปีงบประมาณ พ.ศ. 2569
หน่วยงานที่รับผิดชอบ : ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง กระทรวงมหาดไทย

2. วัตถุประสงค์และเป้าหมายของโครงการ

2.1 วัตถุประสงค์

- 1) เพื่อให้มีเครื่องมือและบุคคลในการเฝ้าระวังภัยคุกคามทางไซเบอร์ตลอด ๒๔ ชั่วโมง
- 2) เพื่อเพิ่มประสิทธิภาพด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร
ให้เป็นไปตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- 3) เพื่อให้มีการเฝ้าระวัง วิเคราะห์ แก้ไขปัญหา และป้องกันภัยคุกคามทางไซเบอร์
จากผู้เชี่ยวชาญเฉพาะด้าน
- 4) เพื่อป้องกันความเสียหายและลดผลกระทบที่จะเกิดขึ้นจากภัยคุกคาม พร้อมบริหารจัดการ
เหตุการณ์ความมั่นคงปลอดภัยให้ระบบสามารถให้บริการได้อย่างต่อเนื่องและมี
ประสิทธิภาพ
- 5) เพื่อมีแผนรับมือภัยคุกคามทางไซเบอร์

2.2 เป้าหมาย

จัดหาระบบเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ของกรมการปกครอง อย่างมี
ประสิทธิภาพให้เป็นไปตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

3. หน้าที่ความรับผิดชอบของหน่วยงาน (ศสป.)

ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง มีอำนาจหน้าที่เสนอแนะนโยบายและจัดทำแผน
แม่บทกลยุทธ์ และแผนปฏิบัติการเทคโนโลยีสารสนเทศ รวมทั้งกำกับ ติดตาม และประเมินผล บริหารและ
พัฒนาระบบสารสนเทศ ศึกษา วิเคราะห์ ออกแบบ และประยุกต์ใช้นวัตกรรมระบบสารสนเทศเพื่อพัฒนาการ
บริหารงานของศูนย์ปฏิบัติการกรม และเป็นศูนย์กลางเครือข่ายข้อมูลสารสนเทศเพื่อการบริหารราชการระดับ
อำเภอ พัฒนาศักยภาพและจัดทำหลักสูตรฝึกอบรมด้านการใช้เทคโนโลยีสารสนเทศ ตลอดจนปฏิบัติงาน
เลขานุการคณะกรรมการข้อมูลสารสนเทศกรมการปกครอง และงานอื่น ๆ ที่ได้รับมอบหมาย แบ่งโครงสร้าง
ภายในออกเป็น 1 ฝ่าย 4 กลุ่มงาน ได้แก่

- 1) ฝ่ายบริหารงานทั่วไป
- 2) กลุ่มงานวิเคราะห์และพัฒนาระบบ
- 3) กลุ่มงานปฏิบัติการและประมวลผลข้อมูล
- 4) กลุ่มงานพัฒนาการเรียนรู้และบูรณาการระบบสารสนเทศ
- 5) กลุ่มงานขับเคลื่อนการบริหารงานปกครองแบบดิจิทัล

4. ระบบงาน

4.1 ปัญหาและอุปสรรค

ปัจจุบันความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้นสร้างความเสียหายเป็นวงกว้างทั้งด้านการให้บริการผ่านระบบสารสนเทศ ด้านความเสี่ยงในการสูญเสียข้อมูลที่สำคัญ กระทั่งการให้บริการและภาพลักษณ์ความไว้วางใจของประชาชนต่อองค์กร จึงจำเป็นต้องมีผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามทางไซเบอร์ เพื่อช่วยให้สามารถรับรู้ถึงสถานการณ์ภัยคุกคามต่างๆ ได้อย่างครอบคลุม และระบุถึงเหตุการณ์ผิดปกติได้อย่างรวดเร็วแม่นยำ เพื่อการตอบสนองได้อย่างทันทั่วถึงไปจนถึงวิเคราะห์ข้อมูลเชิงลึก การประเมินความเสี่ยงด้านสารสนเทศเพื่อเป็นข้อมูลในการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขององค์กร ให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ต่อไป

4.2 ลักษณะการขออนุมัติ

เป็นการจัดหาระบบระวังความมั่นคงปลอดภัยทางไซเบอร์ของกรมการปกครอง (Security Operation Center : SOC)

5. การเตรียมบุคลากรผู้ปฏิบัติโครงการ

การดำเนินโครงการจะใช้บุคลากรที่มีตำแหน่งงานและความรู้ด้านคอมพิวเตอร์ ซึ่งมีอยู่เดิม 10 คน และมีแผนเพิ่มบุคลากรที่เกี่ยวข้องเพื่อเพิ่มประสิทธิภาพความเข้มแข็งของโครงสร้างอัตรากำลังของ ศสป. รวมทั้งจัดให้มีการฝึกอบรมด้านคอมพิวเตอร์ให้กับผู้ปฏิบัติงานและผู้บริหารระดับต่าง ๆ ให้มีความรู้สามารถทำงานได้ดังนี้

5.1 สามารถวิเคราะห์กำหนดคุณลักษณะของอุปกรณ์เครื่อง จัดระบบติดตั้งเชื่อมโยงระบบเครื่องคอมพิวเตอร์ ศึกษาวิเคราะห์ออกแบบเกี่ยวกับชุดคำสั่งระบบ ชุดคำสั่งประยุกต์ รวมทั้งการเขียนคู่มืออธิบายการใช้คำสั่งต่าง ๆ ให้คำปรึกษาแนะนำการอบรมเกี่ยวกับวิทยาการคอมพิวเตอร์ด้านต่าง ๆ แก่บุคลากรหรือหน่วยงาน ติดตามความก้าวหน้าของเทคโนโลยีสมัยใหม่

5.2 สามารถควบคุม ดูแล ซ่อมแซม ตรวจสอบการทำงาน แก้ไขปัญหาการใช้งานของระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ระบบเครือข่ายสื่อสาร รวมทั้งระบบสนับสนุนต่าง ๆ เพื่อให้ระบบงานสามารถทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ

6. วงเงินค่าใช้จ่าย และแหล่งที่มาของเงิน

ใช้งบประมาณรายจ่าย ประจำปีงบประมาณ พ.ศ. 2569 แผนงาน : ยุทธศาสตร์พัฒนาบริการประชาชนและการพัฒนาประสิทธิภาพภาครัฐ ผลผลิต : โครงการสนับสนุนการบูรณาการงานในพื้นที่เพื่อพัฒนาประสิทธิภาพภาครัฐ กิจกรรมหลัก : สนับสนุนการปฏิบัติงานของอำเภอ โครงการผู้ให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ของกรมการปกครอง (Security

Operation Center : SOC) ประจำปีประมาณ พ.ศ. 2569 งบลงทุน หมวดค่าครุภัณฑ์คอมพิวเตอร์สูง
กว่า 1 ล้านบาท จำนวน 3,959,000 บาท ประกอบด้วย

6.1 ระบบจัดเก็บรวบรวมและวิเคราะห์ข้อมูลความปลอดภัยทางเครือข่ายคอมพิวเตอร์ (SIEM)

จำนวน 1 ระบบ เป็นเงิน 1,712,000 บาท

6.2 บริการตรวจจับและตอบสนองต่อภัยคุกคามไซเบอร์ (EDR) 100 ครั้ง ๆ ละ 3,745 บาท เป็นเงิน
374,500 บาท

6.3 ระบบบริหารจัดการ Web Application Firewall on cloud (Cloud-WAF) จำนวน 3 ระบบ ๆ
ละ 107,000 บาท เป็นเงิน 321,000 บาท

6.4 บริหารจัดการ CSOC Monitoring เป็นเงิน 588,500 บาท

6.5 เจ้าหน้าที่ผู้เชี่ยวชาญ ระดับ1 ตลอด 24 ชั่วโมง ณ สถานที่ของผู้ให้บริการ เป็นเงิน 588,500 บาท

6.6 ค่าติดตั้ง เป็นเงิน 374,500 บาท

ส่วนที่ 2 รายละเอียดโครงการที่เสนอขออนุมัติ

1. ชื่อโครงการ

1.1 ชื่อโครงการ : โครงการผู้ให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ของ
กรมการปกครอง (Security Operation Center : SOC) ประจำปีงบประมาณ พ.ศ. 2569

2 ความสอดคล้องกับยุทธศาสตร์ระดับชาติ/หน่วยงาน

- 1.2.1 ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561 – 2580)
- 1.2.2 แผนแม่บทภายใต้ยุทธศาสตร์ชาติ (พ.ศ. 2566 – 2580) (ฉบับแก้ไขเพิ่มเติม)
- 1.2.3 แผนการปฏิรูปประเทศ : ด้านการบริหารราชการแผ่นดิน
- 1.2.4 แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 : มิติที่ 4
- 1.2.5 แผนพัฒนารัฐบาลดิจิทัลของไทย พ.ศ. 2566 – 2570 : ยุทธศาสตร์ที่ 1 – ยุทธศาสตร์ที่ 4
- 1.2.6 นโยบายรัฐบาล : ด้านที่ 8. การพัฒนาและส่งเสริมการใช้ประโยชน์จากวิทยาศาสตร์ฯ
- 1.2.7 แผนปฏิบัติราชการของกระทรวงมหาดไทย พ.ศ. 2566 – 2570
- 1.2.8 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- 1.2.9 ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

2. ส่วนราชการ

2.1 ชื่อส่วนราชการ

ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง กระทรวงมหาดไทย

2.2 สถานที่ตั้ง

ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง อาคาร 3 ชั้น 2 วังไชยา

ถนนนครสวรรค์ แขวงถนนนครไชยศรี เขตดุสิต กรุงเทพฯ 10300

2.3 หัวหน้าส่วนราชการ

นายไชยวัฒน์ จุนถิระพงศ์ อธิบดีกรมการปกครอง

2.4 ผู้รับผิดชอบโครงการ

นายก่อเกียรติ แก้วกึ่ง ผู้อำนวยการศูนย์สารสนเทศเพื่อการบริหารงานปกครอง

3. หน่วยงาน

3.1 หน้าที่ความรับผิดชอบของหน่วยงาน

อำนาจหน้าที่เสนอแนะนโยบายและจัดทำแผนแม่บท กลยุทธ์ และแผนปฏิบัติการ

เทคโนโลยีสารสนเทศ กำกับ ติดตาม และประเมินผล บริหารและพัฒนาระบบสารสนเทศ ศึกษา วิเคราะห์
ออกแบบ และประยุกต์ใช้นวัตกรรมระบบสารสนเทศเพื่อพัฒนาการบริหารงานของศูนย์ปฏิบัติการกรม

และเป็นศูนย์กลางเครือข่ายข้อมูลสารสนเทศเพื่อการบริหารราชการระดับอำเภอ พัฒนาศักยภาพและจัดทำ
หลักสูตรฝึกอบรมด้านการใช้เทคโนโลยีสารสนเทศ

3.2 แผนภูมิการแบ่งส่วนราชการ



3.3 ปัญหาและอุปสรรค ปัจจุบันความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้นสร้างความเสียหายเป็นวงกว้างทั้งด้านการให้บริการผ่านระบบสารสนเทศ ด้านความเสี่ยงในการสูญเสียข้อมูลที่สำคัญ กระทับกับการให้บริการและภาพลักษณ์ความไว้วางใจของประชาชนต่อองค์กร จึงจำเป็นอย่างยิ่งที่ต้องมีผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ เพื่อช่วยให้สามารถรับรู้ถึงสถานการณ์ภัยคุกคามต่างๆ ได้อย่างครอบคลุม และระบุถึงเหตุการณ์ผิดปกติได้อย่างรวดเร็วแม่นยำเพื่อการตอบสนองได้อย่างทันท่วงทีไปจนถึงวิเคราะห์ข้อมูลเชิงลึก การประเมินความเสี่ยงด้านสารสนเทศเพื่อเป็นข้อมูลในการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขององค์กร ให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ต่อไป

3.4 บุคลากรด้านระบบสารสนเทศศูนย์สารสนเทศเพื่อการบริหารงานปกครอง

- | | |
|---------------------------------------|------------|
| 1. นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ | จำนวน 1 คน |
| 2. เจ้าพนักงานปกครองชำนาญการ | จำนวน 1 คน |
| 3. นักวิชาการคอมพิวเตอร์ชำนาญการ | จำนวน 8 คน |
| 4. นักวิชาการคอมพิวเตอร์ปฏิบัติการ | จำนวน 1 คน |
| 5. เจ้าหน้าที่ปกครองชำนาญงาน | จำนวน 1 คน |
| 6. เจ้าหน้าที่ธุรการชำนาญงาน | จำนวน 3 คน |

7. เจ้าหน้าที่เครื่องคอมพิวเตอร์ ชำนาญงาน	จำนวน 1 คน
7. พนักงานราชการ	จำนวน 6 คน
8. ลูกจ้างเหมาบริการ	จำนวน 1 คน
รวม	จำนวน 23 คน

4. ระบบงานที่ขออนุมัติ

4.1 วัตถุประสงค์ และเป้าหมาย

4.1.1 วัตถุประสงค์

- 1) เพื่อให้มีเครื่องมือและบุคคลในการเฝ้าระวังภัยคุกคามทางไซเบอร์ตลอด ๒๔ ชั่วโมง
- 2) เพื่อเพิ่มประสิทธิภาพด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร ให้เป็นไปตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- 3) เพื่อให้มีการเฝ้าระวัง วิเคราะห์ แก้ไขปัญหา และป้องกันภัยคุกคามทางไซเบอร์จากผู้เชี่ยวชาญเฉพาะด้าน
- 4) เพื่อป้องกันความเสียหายและลดผลกระทบที่จะเกิดขึ้นจากภัยคุกคาม พร้อมบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยให้ระบบสามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ
- 5) เพื่อมีแผนรับมือภัยคุกคามทางไซเบอร์

4.1.2 เป้าหมาย

- 4.1.2.1 ตัวชี้วัดเชิงปริมาณ จัดหาระบบเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ของกรมการปกครอง จำนวน 1 ระบบ
- 4.1.2.2 ตัวชี้วัดเชิงคุณภาพ เพื่อเพิ่มประสิทธิภาพของเครือข่ายและระบบสารสนเทศของกรมการปกครองในการปฏิบัติงานของบุคลากร

4.2 รายละเอียดอุปกรณ์คอมพิวเตอร์ที่ขออนุมัติ

เอกสารแนบ 1

4.3 ค่าใช้จ่าย

ลำดับ	รายการ	จำนวน	ราคา/บาท	รวม/บาท
1	ระบบจัดเก็บรวบรวมและวิเคราะห์ข้อมูลความปลอดภัยทางเครือข่าย	1 ระบบ	1,712,000	1,712,000
2	บริการตรวจจับและตอบสนองต่อภัยคุกคามไซเบอร์ (EDR)	100 ครั้ง	3,745	374,500
3	ระบบบริหารจัดการ Web Application Firewall on cloud (Cloud-WAF)	3 ระบบ	107,000	321,000

4	บริหารจัดการ CSOC Monitoring	1 ระบบ	588,500	588,500
5	เจ้าหน้าที่ผู้เชี่ยวชาญ ระดับ1 ตลอด 24 ชม.	-	588,500	588,500
6	ค่าติดตั้ง		374,500	374,500
		รวม		3,959,000

4.4 ระยะเวลาดำเนินงาน 365 วัน

5. ผลประโยชน์ที่คาดว่าจะได้รับ

5.1 กรมการปกครองมีการป้องกันความเสียหายและลดผลกระทบที่จะเกิดขึ้นจากภัยคุกคาม ส่งผลให้ระบบสารสนเทศสามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ

5.2 กรมการปกครองมีการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรอย่างมีประสิทธิภาพ โดยเป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

5.3 มีผู้เชี่ยวชาญเฉพาะด้านช่วยตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ โดยมีการทำแผนที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ และรายงานต่างๆ ให้กับกรมการปกครอง

ภาคผนวก ข.

QUOTATION

Company Name : กรมการปกครอง กระทรวงมหาดไทย
 Attention : อธิบดีกรมการปกครอง
 Address : ถนนรัชฎาภิเศก แขวงวัดราชบพิธ เขตพระนคร กทม. 10200
 Mobile : TEL - E-Mail :
 Project Name : โครงการศูนย์ปฏิบัติการศูนย์ ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ของกรมการปกครอง
 (Security Operation Center : SOC) ประจำปีงบประมาณ พ.ศ. 2569

Quotation No. : i2/SD/6711-03
 Project ID : P605
 Issue Date : 6 พ.ย. 67
 Valid Till : 5 ม.ค. 68

No.	Description	Qty	Unit price	Total Price
1	ระบบจัดเก็บรวบรวมและวิเคราะห์ข้อมูลความปลอดภัยทางเครือข่ายคอมพิวเตอร์ (SIEM)	1	1,722,700.00	1,722,700.00
2	บริการตรวจจับและตอบสนองต่อภัยคุกคามไซเบอร์ (EDR)	100	4,066.00	460,600.00
3	ระบบบริหารจัดการ Web Application Firewall on cloud(Cloud-WAF)	3	107,000.00	321,000.00
4	CSOC Monitoring	1	609,900.00	609,900.00
5	เจ้าหน้าที่ผู้เชี่ยวชาญ ระดับ 1 ให้บริการ 24 ชั่วโมง ทุกวัน ณ สถานที่ของผู้ให้บริการ	1	609,900.00	609,900.00
6	ค่าติดตั้ง	1	395,900.00	395,900.00
	(ราคานี้ได้รวมภาษีมูลค่าเพิ่มแล้ว)			
สี่ล้านหนึ่งหมื่นสองพันห้าร้อยบาทถ้วน			ยอดรวม (Sub Total)	4,012,500.00
Terms and Conditions :			ภาษีมูลค่าเพิ่ม (Vat7%)	
1) Delivery Within			จำนวนเงินสุทธิ (Net Total)	4,012,500.00
2) Term of Payment				
3) Price Validity	60 Days			
4) Warranty				
Remark :			เสนอราคา	PC
			(Ms.Pimpatra Luaeirojane)	
			ตำแหน่ง	Assitant Director
			เบอร์ติดต่อ	062-5152956

PTT Digital Solution Co.,LTD.

555/1 ศูนย์เอนเนอร์ยี่คอมเพล็กซ์ อาคารเอ ชั้น 4-5

ถนนวิภาวดีรังสิต แขวงจตุจักร เขตจตุจักร

กรุงเทพมหานคร 10900 (สำนักงานใหญ่)

เลขประจำตัวผู้เสียภาษี 0-1055-49076-49-6



ใบเสนอราคา / Quotation

โครงการ /Project : โครงการผู้ให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ของกรมการปกครอง

(Security Operation Center : SOC) ประจำปีงบประมาณ พ.ศ. 2569

บริษัท /Company : กรมการปกครอง กระทรวงมหาดไทย

เรียน /Contact : อธิบดีกรมการปกครอง

โทรศัพท์ /Tel :

E-mail :

เลขที่/No : QUO242738

วันที่ /Date : 6 พ.ย. 67

จาก /From : ธิติมา ศรีเจริญ

E-mail : thitima.s@pttdigital.com

โทรศัพท์ /Tel : 095-3681944

1	ระบบจัดเก็บรวบรวมและวิเคราะห์ข้อมูลความปลอดภัยทางเครือข่ายคอมพิวเตอร์ (SIEM)	1	1,712,000.00	1,712,000.00
2	บริการตรวจจับและตอบสนองต่อภัยคุกคามไซเบอร์ (EDR)	100	3,745.00	374,500.00
3	ระบบบริหารจัดการ Web Application Firewall on cloud(Cloud-WAF)	3	107,000.00	321,000.00
4	CSOC Monitoring	1	588,500.00	588,500.00
5	เจ้าหน้าที่ผู้เชี่ยวชาญ ระดับ1 ให้บริการตลอด 24 ชั่วโมง ทุกวัน ณ สถานที่ของผู้ให้บริการ	1	588,500.00	588,500.00
6	ค่าติดตั้ง	1	374,500.00	374,500.00
(ราคานี้รวมภาษีมูลค่าเพิ่มแล้ว)				
		ราคารวม / Total		3,959,000.00
		ภาษีมูลค่าเพิ่ม / Vat 7%		
		ราคารวม Vat 7%		3,959,000.00

Term and Condition / ระยะเวลาและเงื่อนไข

การบริการ /Service :

การชำระเงิน /Payment :

การยืนยันราคา /Validity : 60 วัน

เงื่อนไขอื่นๆ /Others Condition :

PTT Digital Solution Co.,LTD. หวังเป็นอย่างยิ่งว่าจะได้รับการพิจารณาจากท่าน

If you have any question please do not hesitate to call us. We look forward to hearing from you in the near future.

Order Confirmation By Customer

.....
(.....)

Date :

Authorized Signature

(ดิวิมา ศรีเจริญ)

Date :





SOSECURE

บริษัท โซ ซีเคียว จำกัด (สำนักงานใหญ่)
99/10 ซอย 01 กาญจนภิเษก 5 แขวงอโศก เขตสายไหม จังหวัด
กรุงเทพมหานคร 10220
เลขประจำตัวผู้เสียภาษี 0105561088491
โทร. 021650660
เบอร์มือถือ 0615645294 สำนักงาน / 0642416429 บัญชี
<https://www.sosecure.co.th/>

ลูกค้า

กรมการปกครอง กระทรวงมหาดไทย (สำนักงานใหญ่)
กรมการปกครอง (วังไชยา) ชั้น 2 เลขที่ 442 ถนนนครสวรรค์ แขวงสี่แยก
มหานาค เขตดุสิต กรุงเทพฯ 10300

ใบเสนอราคา

เลขที่ QT2024110019
วันที่ 06/11/2024
ผู้ขาย sirikarn meanghom

ชื่องาน Blue Team : CSOC SERVICE (โครงการผู้ให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ของกรมการปกครอง (Security Operation Center : SOC) ประจำปีงบประมาณ พ.ศ. 2569)
ผู้ติดต่อ อธิบดีกรมการปกครอง

#	รายละเอียด	จำนวน	ราคาต่อหน่วย	ส่วนลด	มูลค่า
1	ระบบจัดเก็บรวบรวมและวิเคราะห์ข้อมูลความปลอดภัยทางเครือข่ายคอมพิวเตอร์ (SIEM)	1	1,712,000.00		1,712,000.00
2	ค่าบริการตรวจจับและตอบสนองต่อภัยคุกคามไซเบอร์ (EDR)	1	428,000.00		428,000.00
3	ระบบบริหารจัดการ Web Application Firewall on Cloud (Cloud-WAF)	1	385,200.00		385,200.00
4	CSOC Monitoring	1	599,200.00		599,200.00
5	เจ้าหน้าที่ผู้เชี่ยวชาญ ระดับ 1 ให้บริการ 24 ชั่วโมง ทุกวัน -ปฏิบัติงาน ณ สถานที่ของผู้ให้บริการ	1	599,200.00		599,200.00
6	ค่าติดตั้ง	1	385,200.00		385,200.00

(ราคานี้ได้รวมภาษีมูลค่าเพิ่มเรียบร้อยแล้ว)

(สี่ล้านหนึ่งแสนแปดพันแปดร้อยบาทถ้วน)

รวมเป็นเงิน 4,108,800.00 บาท
ภาษีมูลค่าเพิ่ม 0% 0.00 บาท
จำนวนเงินรวมทั้งสิ้น 4,108,800.00 บาท

หมายเหตุ

ข้อบัญญัติ โซ ซีเคียว จำกัด
ธนาคารกสิกรไทย สาขาคริสต์ส ดีไซน์ เซ็นเตอร์
เลขที่บัญชี 041 1 40243 6

ในนาม กรมการปกครอง กระทรวงมหาดไทย

ในนาม บริษัท โซ ซีเคียว จำกัด



ผู้สั่งซื้อสินค้า

วันที่

ผู้อนุมัติ

06/11/2024

วันที่

ภาคผนวก ค.

ขอบเขตงาน (Term of Reference : TOR)

โครงการผู้ให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ของกรมการปกครอง (Security Operation Center : SOC) ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

๑. หลักการและเหตุผล

ด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งมีผลบังคับใช้เมื่อวันที่ ๒๘ พฤษภาคม ๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

กรมการปกครองเป็นหน่วยงานภาครัฐที่ต้องปฏิบัติตามพระราชบัญญัติและประกาศข้างต้น ประกอบกับกรมการปกครองโดนภัยคุกคามทางไซเบอร์ตลอดเวลาหลากหลายรูปแบบ และมีปริมาณในการโจมตีสูงมาก ภัยคุกคามดังกล่าว สร้างความเสียหายในวงกว้างทั้งด้านการให้บริการผ่านระบบสารสนเทศ ไปจนถึงการจารกรรมข้อมูล ซึ่งอาจจะก่อให้เกิดความเสียหายที่อาจจะประเมินมูลค่าไม่ได้ กระทั่งกับภาพลักษณ์ความไว้วางใจของประชาชนต่อกรมการปกครอง จึงจำเป็นต้องมีการเฝ้าระวังภัยคุกคามได้อย่างทั่วถึงตลอด ๒๔ ชั่วโมง และมีผู้เชี่ยวชาญในการวิเคราะห์ แก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามทางไซเบอร์ เพื่อช่วยให้กรมการปกครองสามารถรับรู้ถึงสถานการณ์ภัยคุกคามต่างๆ ระบุถึงเหตุการณ์ผิดปกติได้อย่างรวดเร็วแม่นยำเพื่อการตอบสนองได้อย่างทันท่วงที ไปจนถึงวิเคราะห์ข้อมูลเชิงลึก ตรวจสอบหาช่องโหว่ของระบบสารสนเทศ การประเมินความเสี่ยงด้านสารสนเทศ เพื่อเป็นข้อมูลในการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ของกรมการปกครอง ให้เป็นไปตามพระราชบัญญัติและประกาศข้างต้นต่อไป

๒. วัตถุประสงค์

- ๒.๑ เพื่อให้มีเครื่องมือและบุคคลในการเฝ้าระวังภัยคุกคามทางไซเบอร์ตลอด ๒๔ ชั่วโมง
- ๒.๒ เพื่อให้มีการ วิเคราะห์ แก้ไขปัญหา และป้องกันภัยคุกคามทางไซเบอร์จากผู้เชี่ยวชาญเฉพาะด้าน
- ๒.๓ เพื่อเพิ่มประสิทธิภาพด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรให้เป็นไปตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- ๒.๔ เพื่อป้องกันความเสียหายและลดผลกระทบที่จะเกิดขึ้นจากภัยคุกคาม พร้อมบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยให้ระบบสามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ

๓. ประโยชน์...

๓. ประโยชน์ที่คาดว่าจะได้รับ

๓.๑ กรมการปกครองมีการป้องกันความเสียหายและลดผลกระทบที่จะเกิดขึ้นจากภัยคุกคาม ส่งผลให้ระบบสารสนเทศสามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ

๓.๒ กรมการปกครองมีการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรอย่างมีประสิทธิภาพ โดยเป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔. ระยะเวลาดำเนินงาน

เริ่มตั้งแต่ ๑ ตุลาคม ๒๕๖๘ ถึง ๓๐ กันยายน ๒๕๖๙ (รวม ๑๒ เดือน)

๕. วงเงินงบประมาณ / ราคาากลาง

๕.๑ เงินงบประมาณประจำปี พ.ศ.๒๕๖๙ เป็นจำนวนเงินทั้งสิ้น ๔,๐๐๐,๐๐๐ บาท (สี่ล้านบาทถ้วน)

๕.๒ ราคาากลางเป็นจำนวนเงิน ๓,๙๕๙,๐๐๐ บาท (สามล้านเก้าแสนห้าหมื่นเก้าพันบาทถ้วน)

๖. หน่วยงานผู้รับผิดชอบ

ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง ถนนนครสวรรค์ แขวงสีแยกมทานาค เขตดุสิต กทม. ๑๐๓๐๐

๗. คุณสมบัติของผู้ยื่นข้อเสนอ

๗.๑ มีความสามารถตามกฎหมาย

๗.๒ ไม่เป็นบุคคลล้มละลาย

๗.๓ ไม่อยู่ระหว่างเลิกกิจการ

๗.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนด ตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๗.๕ ไม่เป็นบุคคลซึ่งถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๗.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๗.๗ ผู้ยื่น...

๗.๗ ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว โดยต้องนำหลักฐานเป็นหนังสือมาแสดงในวันยื่นข้อเสนอ

๗.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่กรมการปกครอง ณ วันประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๗.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นนั้น

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

๗.๑๑ ผู้ยื่นข้อเสนอต้องมีผลงานในการให้บริการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยให้บริการตลอด ๒๔ ชั่วโมงต่อวัน ๗ วันต่อสัปดาห์ (๒๔/๗) ซึ่งเป็นผลงานที่แล้วเสร็จไม่เกิน ๓ ปี นับถึงวันยื่นข้อเสนออย่างน้อย ๒ โครงการ ซึ่งมีมูลค่าของโครงการละไม่น้อยกว่า ๑,๙๐๐,๐๐๐ บาท (หนึ่งล้านเก้าแสน บาทถ้วน) ทั้งนี้ผู้ยื่นข้อเสนอต้องแสดงหนังสือรับรองและสำเนาสัญญาการให้บริการฯ และรายละเอียดงาน ที่ได้รับการจ้างในครั้งนั้น พร้อมกับการยื่นข้อเสนอด้วย

๘. หลักเกณฑ์ในการพิจารณาผลการยื่นข้อเสนอ จะพิจารณาตัดสินโดยใช้หลักเกณฑ์ราคา

๙. ข้อกำหนดทั่วไป

๙.๑ ผู้ยื่นข้อเสนอจะต้องจัดหาบุคลากรในการดำเนินโครงการดังนี้

๙.๑.๑ ผู้จัดการโครงการ อย่างน้อย ๑ คน คุณสมบัติดังนี้

๙.๑.๑.๑ คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี

๙.๑.๑.๒ มีประสบการณ์ในตำแหน่งผู้จัดการโครงการที่เกี่ยวกับศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศ หรือตำแหน่งที่เกี่ยวข้อง มาแล้วไม่น้อยกว่า ๕ ปี

๙.๑.๑.๓ ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ Certified Information Systems Security Professional (CISSP) และ Certified Information Security Manager (CISM) และ Certified Information Systems Auditor (CISA)

๙.๑.๒ ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ ระดับ ๓ (Tier ๓) อย่างน้อย ๑ คน คุณสมบัติดังนี้

๙.๑.๒.๑ คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี

๙.๑.๒.๒ มีประสบการณ์...

๙.๑.๒.๒ มีประสบการณ์ทำงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศในตำแหน่ง Security analyst ระดับ ๓ (Tier ๓) และ Digital forensic มาแล้วไม่น้อยกว่า ๓ ปี

๙.๑.๒.๓ ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ GIAC Certified Forensic Analyst (GCFA)

๙.๑.๓ ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ ระดับ ๒ (Tier ๒) อย่างน้อย ๒ คน คุณสมบัติดังนี้

๙.๑.๓.๑ คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี

๙.๑.๓.๒ มีประสบการณ์ทำงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศในตำแหน่ง Security analyst ระดับ ๒ (Tier ๒) มาแล้วไม่น้อยกว่า ๒ ปี

๙.๑.๓.๓ ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ EC-Council Certified Security Analyst (ECSA) และ Certified CompTIA Cybersecurity Analyst (CySA+) และ CompTIA Advanced Security Practitioner (CASP+) หรือ Certified Ethical Hacker (CEH)

๙.๑.๔ ผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยต่อภัยคุกคามไซเบอร์ ระดับ ๑ (Tier ๑) อย่างน้อย ๔ คน คุณสมบัติดังนี้

๙.๑.๔.๑ คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี

๙.๑.๔.๒ มีประสบการณ์ทำงานในศูนย์ปฏิบัติการเฝ้าระวังภัยคุกคามทางด้านความปลอดภัยสารสนเทศในตำแหน่ง Security analyst ระดับ ๑ (Tier ๑) มาแล้วไม่น้อยกว่า ๒ ปี

๙.๑.๔.๓ ได้รับประกาศนียบัตรรับรองคุณวุฒิด้านความปลอดภัยสารสนเทศ Certified CompTIA Security +

๙.๑.๕ เจ้าหน้าที่ตอบสนองภัยคุกคาม (Incident Response) หรือผู้บัญชาการทีม SOC (Team Lead) อย่างน้อย ๑ คน คุณสมบัติดังนี้

๙.๑.๕.๑ คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี

๙.๑.๕.๒ ได้รับประกาศนียบัตรรับรองคุณวุฒิมีประกาศนียบัตรด้านความปลอดภัยสารสนเทศ GIAC Certified Incident Handler Certification (GCIH) และ EC-Council Certified Incident Handler (ECIH)

๙.๑.๖ เจ้าหน้าที่ตรวจสอบภัยคุกคามเชิงรุก (Threat Hunting) อย่างน้อย ๑ คน คุณสมบัติดังนี้

๙.๑.๖.๑ คุณวุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี

๙.๑.๖.๒ ได้รับ...

๙.๑.๖.๒ ได้รับประกาศนียบัตรรับรองคุณวุฒิมีประกาศนียบัตรด้านความปลอดภัยสารสนเทศ MITRE ATT&CK for Threat Hunting and Detection Engineering Certification และ CompTIA Advanced Security Practitioner (CASP+) และ CompTIA Security Analytics Professional (CSAP)

๙.๒ คุณสมบัติของศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (Security Operation Center: SOC)

๙.๒.๑ ต้องได้รับการรับรองระบบบริหารจัดการรักษาความมั่นคงปลอดภัยสารสนเทศ ISO ๒๗๐๐๑ Information Security Management System: ISMS

๙.๒.๒ ต้องได้รับการรับรองตามมาตรฐานการบริหารความต่อเนื่องทางธุรกิจ ISO ๒๒๓๐๑ และต้องมีแผนรองรับเหตุฉุกเฉิน BCP Plan โดยมีศูนย์ปฏิบัติการสำรอง เพื่อที่จะได้ทำงานแทนได้ทันที ในกรณีที่ศูนย์ปฏิบัติการหลักไม่สามารถทำงานได้

๙.๒.๓ ต้องมีห้องเฉพาะ (Dedicated Room) ที่เป็นศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ (Cybersecurity Operations Center)

๑๐. คุณลักษณะเฉพาะของการให้บริการ

๑๐.๑ ผู้ยื่นข้อเสนอจะต้องเสนอบริการระบบจัดเก็บรวบรวมและวิเคราะห์ข้อมูลความปลอดภัยทางเครือข่ายคอมพิวเตอร์ (SIEM) เพื่อจัดเก็บรวบรวมและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์จากอุปกรณ์เครือข่ายและรักษาความมั่นคงปลอดภัยของกรมการปกครอง โดยมีคุณสมบัติดังนี้

๑๐.๑.๑ เป็นบริการที่ถูกออกแบบมา เพื่อวิเคราะห์ข้อมูลทางด้านการรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ หรือ Security Information and Event Management (SIEM) โดยเฉพาะ

๑๐.๑.๒ ผู้ให้บริการจะต้องใช้ผลิตภัณฑ์ระบบเฝ้าระวังภัยคุกคามทางไซเบอร์ SIEM ที่อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for Security Information and Event Management (SIEM) ปี ๒๐๒๔ สามารถรองรับปริมาณการรับ Log จำนวน ๒,๐๐๐ EPS หรือ ๑๐๐ GB/Day

๑๐.๑.๓ สามารถจัดเก็บข้อมูล Log จากอุปกรณ์ในระบบเครือข่ายคอมพิวเตอร์ (Log Source) ของกรมการปกครอง ได้อย่างน้อยดังนี้

- (๑) อุปกรณ์ Firewall รองรับการใช้งานของหน่วยงานส่วนกลาง จำนวน ๑ ชุด
- (๒) อุปกรณ์ WAF จำนวน ๑ ชุด
- (๓) อุปกรณ์ Authentication จำนวน ๑ ชุด
- (๔) อุปกรณ์ VPN จำนวน ๑ ชุด
- (๕) เครื่องคอมพิวเตอร์แม่ข่าย Active Directory (AD Server) จำนวน ๑ ชุด

๑๐.๑.๔ สามารถ...

๑๐.๑.๔ สามารถจัดเก็บข้อมูล Log ตามอุปกรณ์ที่ระบุในโครงการ และมีพื้นที่จัดเก็บข้อมูลได้ไม่น้อยกว่า ๙๐ วัน

๑๐.๑.๕ สามารถ Export ข้อมูล Log ในรูปแบบ XML หรือ CSV ได้

๑๐.๑.๖ สามารถค้นหา (Search) ข้อมูล Log ด้วย Keyword หรือ Full Text ได้จากชื่อเครื่องคอมพิวเตอร์, ชื่อผู้ใช้, IP Address, ช่วงวัน และช่วงเวลา เป็นอย่างน้อย

๑๐.๑.๗ สามารถวิเคราะห์พฤติกรรมการใช้งานของผู้ใช้งาน โดยตรวจสอบและแจ้งเตือนภัยคุกคาม ได้อย่างน้อยดังนี้

- Compromised Account
- Shared User Credentials
- Brute Force
- Data Transfer Volume
- Lateral Movement
- Suspicious Privileged Activity

๑๐.๑.๘ สามารถปรับแต่ง (Customization) การแสดงผล (Dashboard), รายงาน (Report), การแจ้งเตือน (Alert) และ การสร้างความสัมพันธ์ของข้อมูล (Correlation) ของภัยคุกคามได้

๑๐.๑.๙ สามารถแจ้งเตือน (Alert) เหตุการณ์ด้านความปลอดภัยและ ความผิดปกติในเครือข่ายให้ผู้ดูแลระบบ โดยมีรูปแบบเหตุการณ์อย่างน้อย ดังนี้

- (๑) Port Scanning
- (๒) Brute Force Attack
- (๓) DDoS Attack
- (๔) Botnet
- (๕) Malware Outbreak

๑๐.๑.๑๐ สามารถสร้างรายงาน (Report) ได้อย่างน้อย ดังนี้

- (๑) Compliance เช่น ISO ๒๗๐๐๑ หรือ ISO ๒๗๐๐๒
- (๒) Top ๑๐ Event เช่น Source IP Address, Destination IP Address, Alert/Incident ได้

๑๐.๑.๑๑ สามารถ Export รายงานในรูปแบบ PDF และ CSV ได้

๑๐.๑.๑๒ สามารถทำงานบนเครือข่าย IPv4 และ IPv6

๑๐.๑.๑๓ สามารถทำงานร่วมกับระบบ Network Time Protocol ได้

๑๐.๒ ผู้ยื่น...

๑๐.๒ ผู้ยื่นข้อเสนอจะต้องจัดให้มีการบริการตรวจจับและตอบสนองต่อภัยคุกคามไซเบอร์ สำหรับเครื่องคอมพิวเตอร์ (Endpoint Detection and Response Service) จำนวน ๑๐๐ เครื่อง โดยมี คุณสมบัติดังต่อไปนี้

๑๐.๒.๑ เป็น Platform ที่มีความสามารถในการตรวจหาภัยคุกคามที่เกิดขึ้นในองค์กร (Threat Hunting) และหาข้อมูลความเกี่ยวข้องของภัยคุกคามที่เกิดขึ้น (Investigation) ของเครื่อง คอมพิวเตอร์ที่ติดตั้ง Agent Software ได้

๑๐.๒.๒ สามารถติดตั้งบนเครื่องคอมพิวเตอร์ ไม่น้อยกว่า ๑๐๐ เครื่อง ที่ใช้ระบบปฏิบัติการ Windows Server ๒๐๑๒, Windows Server ๒๐๑๖, Windows Server ๒๐๑๙, Windows Server ๒๐๒๒, Windows ๑๐/๑๑, MacOS, Linux, Ubuntu และ CentOS ได้เป็นอย่างดีน้อย

๑๐.๒.๓ มีความสามารถในการป้องกันภัยคุกคาม ดังนี้

๑๐.๒.๓.๑ ป้องกันการโจมตีที่ช่องโหว่ของระบบ (Exploit Prevention)

๑๐.๒.๓.๒ ป้องกันมัลแวร์ หรือไวรัส (Malware Prevention หรือ Antivirus)

๑๐.๒.๓.๓ ป้องกันการโจมตีของมัลแวร์ระดับสูง ที่ใช้เทคนิคโจมตีแบบไม่ใช้ไฟล์ (Fileless Attacks)

๑๐.๒.๓.๔ ป้องกันการโจมตีโดยใช้เทคนิคของ (AI-based local analysis engine) หรือ Machine Learning

๑๐.๒.๓.๕ ป้องกันการโจมตีโดยใช้การวิเคราะห์พฤติกรรม (Behavior)

๑๐.๒.๓.๖ ป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware Protection)

๑๐.๒.๔ มีระบบบริหารจัดการอยู่บน Cloud management (SaaS) และการเชื่อมต่อ ระหว่าง Agent กับ Cloud Management และเข้ารหัสแบบ TLS-Encrypted เพื่อความปลอดภัย ใช้งาน ผ่านทาง Web Console โดยมีการยืนยันตัวตนด้วย MFA ได้

๑๐.๒.๕ มีความสามารถทำการตัดการเชื่อมต่อของระบบเครือข่าย (Network Containment) หรือแยกเครื่องคอมพิวเตอร์ที่มีความเสี่ยงจากภัยคุกคามออกจากระบบเครือข่าย (Isolate) บนเครื่องที่มีการติดตั้ง Agent Software

๑๐.๒.๖ สามารถนำข้อมูลการแจ้งเตือนภัยคุกคามพร้อมแสดงข้อมูล MITRE ATT&CK Framework ของแต่ละรายการแจ้งเตือน

๑๐.๒.๗ สามารถค้นหาข้อมูลการใช้งาน Source IP Address, Domain และ Event ที่ เกี่ยวข้องกับข้อมูลการใช้งาน (Activity) ได้

๑๐.๒.๘ บริการที่นำเสนอต้องถูกรับรองโดย Gartner Magic Quadrant™ for Endpoint Protection Platforms ปี ๒๐๒๓ ในกลุ่มผู้นำ (Leaders) หรือ The Forrester Wave™: Endpoint Security, Q๔ ๒๐๒๓ ในกลุ่มผู้นำ (Leaders)

๑๐.๒.๙ ผู้ยื่น...

๑๐.๒.๙ เจ้าของผลิตภัณฑ์ต้องได้รับการจัดอันดับให้อยู่ในกลุ่ม Leaders Performers ของ The Forrester Wave™: Endpoint Security, Q๔ ๒๐๒๓

๑๐.๒.๙ ผู้ให้บริการต้องตั้งค่าการส่ง Log จากระบบ EDR ไปยังระบบ SIEM ที่นำเสนอในโครงการได้

๑๐.๒.๑๐ ผู้ให้บริการต้องมีผู้เชี่ยวชาญด้านการบริหารจัดการ EDR ที่ได้รับประกาศนียบัตรจากเจ้าของผลิตภัณฑ์อย่างน้อย ๑ คน

๑๐.๓ ผู้ยื่นข้อเสนอจะต้องจัดให้มีการบริการ Web Application Firewall on Cloud (Cloud-WAF) สำหรับป้องกันจำนวน ๒ เว็บไซต์ โดยมีคุณสมบัติดังต่อไปนี้

๑๐.๓.๑ บริการที่นำเสนอต้องเป็นระบบ Cloud-WAF ที่ให้บริการในรูปแบบ Cloud Platform

๑๐.๓.๒ บริการที่นำเสนอต้องมี Datacenter หรือ Scrubbing Center ทั่วโลก รวมไม่น้อยกว่า ๔๐ แห่ง

๑๐.๓.๓ บริการที่นำเสนอต้องรองรับการใช้งาน Clean-Bandwidth ๒ Mbps แบบ ๙๕ percentile

๑๐.๓.๔ บริการที่นำเสนอต้องได้รับการรับรองมาตรฐาน PCI DSS, ISO ๒๗๐๐๑ และ SOC ๒ Type ๒ เป็นอย่างน้อย

๑๐.๓.๕ บริการที่นำเสนอต้องสามารถป้องกันการโจมตีผ่านทางเว็บไซต์ ตาม TOP ๑๐ OWASP เช่น Cross-side Request Forgery (CSRF), Server-side Request Forgery (SSRF), Cross Site Scripting (XSS), Injection Flaws, Command Execution, Database Sabotage, Stealth Commanding, Client Side Protection (Detection) ได้

๑๐.๓.๖ บริการที่นำเสนอต้องสามารถสร้างและกำหนดเงื่อนไข Web Firewall Policy ผ่าน Web UI ได้

๑๐.๓.๗ บริการที่นำเสนอต้องสามารถตรวจจับและป้องกันการโจมตีที่ส่งผลกระทบต่อ Application Programming Interface (API Protection) ได้

๑๐.๓.๘ บริการที่นำเสนอต้องสามารถป้องกันการโจมตี DDoS attack Layer ๓, Layer ๔ และ Layer ๗ ได้อัตโนมัติ

๑๐.๓.๙ บริการที่นำเสนอต้องมี Real-time Dashboard โดยต้องสามารถแสดงข้อมูล ปริมาณ Requests, Bandwidth, Top Sources, Top URL ได้เป็นอย่างน้อย

๑๐.๓.๑๐ บริการที่นำเสนอต้องมีฐานข้อมูล IP Reputation สำหรับค้นหาประวัติ ระดับความเสี่ยง และประเภทกลุ่มเป้าหมายที่ถูกโจมตี ของ IP ที่ต้องสงสัยได้

๑๐.๓.๑๑ ผู้ยื่น...

๑๐.๓.๑๑ บริการที่นำเสนอต้องสามารถทำ Delivery Policy เพื่อ Rewrite Request ได้ เช่น Redirect URL, Rewrite request URL, Rewrite request header, Remove request header, Rewrite request cookie และ Remove request cookie

๑๐.๓.๑๒ บริการที่นำเสนอต้องสามารถทำ Delivery Policy เพื่อ Rewrite Response ได้ เช่น Rewrite response header, Remove response header และ Rewrite response code

๑๐.๓.๑๓ บริการที่นำเสนอต้องมีระบบหรือบริการวิเคราะห์การโจมตีที่เกิดขึ้นโดยอัตโนมัติ (Analytics) ที่แสดงผลข้อมูลในเชิงวิเคราะห์ได้อย่างน้อย ดังต่อไปนี้

๑๐.๓.๑๓.๑ แสดงการจัดกลุ่มและบ่งบอกถึงประเภทการโจมตีที่เกิดขึ้น (Correlated incidents) พร้อมระบุระดับความรุนแรงของเหตุการณ์ (Severity) ให้โดยอัตโนมัติ

๑๐.๓.๑๓.๒ แสดงอัตราการป้องกันต่อการโจมตีที่เกิดขึ้น (Blocked rate) โดยอัตโนมัติ

๑๐.๓.๑๓.๓ แสดงแนวโน้มการโจมตีที่เกิดขึ้น (Event and Incident) โดยอัตโนมัติ

๑๐.๓.๑๓.๔ แสดงและเลือกดูข้อมูลในช่วงเวลาที่กำหนด โดยต้องสามารถดูย้อนหลังได้ไม่ต่ำกว่า ๓๐ วัน

๑๐.๓.๑๔ บริการที่นำเสนอต้องถูกรับรองโดย Gartner Magic Quadrant Web Application Firewall ปี ๒๐๒๒ ในกลุ่มผู้นำ (Leader) หรือ SPARK Matrix™: Web Application Firewall, Q๔ ๒๐๒๓ ในกลุ่ม Technology Leader

๑๐.๔ บริการ CSOC monitoring ศูนย์กลางของผู้ให้บริการ เพื่อเฝ้าระวังและตรวจจับ พร้อมทั้งรับมือกับภัยคุกคามทางไซเบอร์ โดยพึ่งพาการวิเคราะห์ เชื่อมโยง และประสานการทำงานกับระบบภายในองค์กร

๑๐.๕ ให้เจ้าหน้าที่เฝ้าระวัง มาปฏิบัติงานตามสถานที่และเวลา ตลอดระยะเวลาของสัญญา ณ ศูนย์เฝ้าระวังภัยคุกคาม (SOC) ของผู้ให้บริการ ตลอด ๒๔ ชั่วโมง ต่อวัน / ๗ วันต่อสัปดาห์ (๒๔/๗)

๑๑. ข้อกำหนดของการให้บริการ

๑๑.๑ ผู้ให้บริการต้องจัดประชุมร่วมกับเจ้าหน้าที่ของกรมการปกครอง เพื่อเตรียมการติดตั้งและตั้งค่า (Configuration) ของอุปกรณ์ในโครงการ

๑๑.๒ ผู้ให้บริการต้องดำเนินการติดตั้งและตั้งค่า (Configuration) ของอุปกรณ์ในโครงการให้เป็นไปตาม ข้อ ๑๐.๑ - ๑๐.๓ แล้วเสร็จภายใน ๓๐ วัน นับถัดจากวันเริ่มสัญญา

๑๑.๓ ผู้ให้บริการต้องดำเนินงานด้านบริการตรวจจับและเฝ้าระวังภัยคุกคามทางไซเบอร์ของกรมการปกครองครอบคลุมรายการอุปกรณ์ ทั้งนี้ระหว่างสัญญากรมการปกครองสงวนสิทธิ์ในการปรับเปลี่ยนระบบหรืออุปกรณ์ในการเฝ้าระวังภัยคุกคามได้ตามความต้องการ โดยมีรายการอุปกรณ์ทั้งหมดตามข้อ ๑๐.๑ ถึงข้อ ๑๐.๓ ซึ่งต้องมีการดำเนินงานอย่างน้อยดังต่อไปนี้

ขอบเขตงาน (Term of Reference : TOR) โครงการจ้างผู้ให้บริการศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ กรมการปกครอง
(Security Operation Center : SOC) ประจำปีงบประมาณ พ.ศ.๒๕๖๘

๑๑.๓.๑ ดำเนินการรับแจ้งภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ ให้สามารถรองรับการทำ Incident Management and Change Management และสามารถทำงานร่วมกับระบบ SIEM ในการบริหารจัดการศูนย์ SOC ได้

๑๑.๓.๒ ดำเนินการวิเคราะห์เหตุการณ์ผิดปกติทางด้านบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต ในเรื่องที่เกี่ยวข้องกับความผิดปกติของภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ (Security Monitoring) พร้อมให้คำปรึกษาและร่วมกับการปกครองในการแก้ไขอุปกรณ์ที่เกี่ยวข้องเพื่อหาแนวทางการป้องกันไม่ให้เกิดเหตุการณ์ขึ้นอีก

๑๑.๓.๓ ดำเนินการตั้งค่าระบบเฝ้าระวังภัยคุกคามไซเบอร์ของกรมการปกครอง ให้สามารถแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยผ่านทางระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) ของกรมการปกครอง หรือช่องทางที่กรมการปกครองกำหนด

๑๑.๓.๔ ดำเนินการแจ้งเตือนเมื่อตรวจพบภัยคุกคามหรือการบุกรุกระบบเทคโนโลยีสารสนเทศ และให้คำปรึกษาพร้อมนำเสนอวิธีการแก้ปัญหาเฉพาะกิจให้แก่กรมการปกครอง โดยจัดแบ่งตามระดับความสำคัญดังนี้

๑๑.๓.๔.๑ เมื่อพบว่ามีระดับความรุนแรงตั้งแต่ระดับสูงขึ้นไป จะต้องดำเนินการแจ้งให้กรมการปกครองทราบทันทีทางโทรศัพท์เคลื่อนที่ของผู้ประสานงานของกรมการปกครอง (Mobile Phone) หรือระบบการสื่อสารอื่น ๆ ที่เหมาะสมและบันทึกในรายงานเฝ้าระวังภัยคุกคามทางไซเบอร์ (Incident Report)

๑๑.๓.๔.๒ เมื่อพบว่ามีระดับความรุนแรงตั้งแต่ระดับปานกลางจนถึงระดับต่ำ จะต้องดำเนินการแจ้งกรมการปกครอง ทางระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือช่องทางที่กรมการปกครองกำหนด และบันทึกในรายงานเฝ้าระวังภัยคุกคามทางไซเบอร์ (Incident Report)

๑๑.๓.๕ ดำเนินการตั้งค่าระบบเฝ้าระวังภัยคุกคามไซเบอร์ของกรมการปกครองให้สามารถกำหนดเงื่อนไขรูปแบบการเฝ้าระวังและตรวจจับภัยคุกคาม (Use Case) ตามที่ได้ทำการประเมินและตกลงร่วมกับทางกรมการปกครองได้ไม่น้อยกว่า ๕ Use Case พร้อมจัดทำรายงานสรุปรูปแบบการเฝ้าระวังและตรวจจับภัยคุกคาม

(Use Case) ส่งภายใน ๙๐ นับถัดจากวันเริ่มสัญญา

๑๑.๓.๖ ดำเนินการแจ้งข่าวสารที่เกี่ยวข้องกับระบบรักษาความปลอดภัยระบบคอมพิวเตอร์และเครือข่ายที่เกิดขึ้น โดยมีรายละเอียดอย่างน้อยดังนี้

- (๑) รายชื่อ และคุณลักษณะของมัลแวร์ (Malware)
- (๒) ช่องโหว่ใหม่ (Vulnerability) ของอุปกรณ์ในระบบเครือข่าย (Network Equipment)
- (๓) ช่องโหว่ใหม่ (Vulnerability) ของระบบปฏิบัติการ (Operating System)
- (๔) ช่องโหว่ใหม่ (Vulnerability) ของระบบฐานข้อมูลหลัก (Database)

(๕) ช่องโหว่ใหม่ (Vulnerability) ของระบบและอุปกรณ์ต่าง ๆ ที่ผู้รับจ้างเห็นว่าจะก่อให้เกิดผลเสียหายต่อการดำเนินงานของกรมการปกครอง โดยข่าวสารดังกล่าวประกอบด้วยเนื้อหาที่สำคัญ เช่น คำอธิบายโดยย่อ (Overview) คำอธิบายอย่างละเอียด (Description) ผลกระทบ (Impact) ระบบที่ได้รับผลกระทบ (System Affected) ทางแก้ไข (Solution) (ถ้ามี) อ้างอิง (Reference) เป็นต้น

๑๑.๔ ผู้ให้บริการต้องบริหารจัดการและตอบสนองต่อเหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคามทางไซเบอร์สำหรับเครื่องคอมพิวเตอร์ (Incident Response) โดยต้องจัดให้มีการดำเนินงานอย่างน้อยดังต่อไปนี้

๑๑.๔.๑ เข้าดำเนินการตรวจสอบและวิเคราะห์เหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคามทางไซเบอร์ในขั้นต้น เช่น ระบุผลลัพธ์การวิเคราะห์ (Analyst Verdict) กำหนดสถานะของเหตุการณ์ (Incident Status) ระบุรายละเอียดเพิ่มเติม (Incident Note)

๑๑.๔.๒ แจ้งเตือนและประสานงานไปยังเจ้าหน้าที่หรือหน่วยงานที่รับผิดชอบ

๑๑.๔.๓ สนับสนุนและตอบสนองต่อเหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคาม ระบุ ยับยั้ง หรือยุติกระบวนการที่เป็นอันตรายต่อระบบ โดยต้องดำเนินการอย่างน้อยดังนี้

๑๑.๔.๓.๑ ระบุขอบเขตของผลกระทบที่เกิดจากภัยคุกคามดังกล่าว

๑๑.๔.๓.๒ ทำการแยกเครื่อง Endpoint ที่เป็นอันตรายออกจากระบบ เพื่อหลีกเลี่ยงการแพร่กระจายไปสู่เครื่องอื่น ๆ

๑๑.๔.๓.๓ ทำการระบุ ยับยั้ง หรือ ยุติกระบวนการที่เป็นอันตรายต่อระบบ

๑๑.๔.๓.๔ ทำการกำจัด ลบ หรือล้างไฟล์ที่เกี่ยวข้องกับภัยคุกคามดังกล่าว ในกรณีที่เครื่องได้รับผลกระทบจะต้องดำเนินการกู้คืนกลับสู่สภาพปกติ

๑๑.๔.๔ ดำเนินการปรับปรุงการตั้งค่าของอุปกรณ์ที่เกี่ยวข้องในระบบ รวมถึงการกำหนด Blacklist หรือ Whitelist Asset ต่าง ๆ

๑๑.๔.๕ ผู้ให้บริการต้องดำเนินงานภายใต้ SLA (Service Level Agreement) ที่กำหนดสำหรับบริการเฝ้าระวังและตอบสนองต่อเหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคามทางไซเบอร์ โดยอ้างอิงตามภาคผนวก ก.

๑๑.๕ ตรวจสอบและตั้งค่า Configuration อุปกรณ์เครือข่ายและรักษาความมั่นคงปลอดภัยของกรมการปกครองและเครื่องคอมพิวเตอร์ และติดตั้งใช้งานอุปกรณ์หรือโปรแกรมที่เกี่ยวข้องให้มีการส่งข้อมูลจราจรทางคอมพิวเตอร์ (Logs) จากอุปกรณ์และเครื่องคอมพิวเตอร์ ที่กำหนดไว้ในข้อ ๑๐.๑ ถึง ๑๐.๓ ไปยังระบบ Security Operation Center (SOC) ของผู้ให้บริการได้อย่างครบถ้วนสมบูรณ์

๑๑.๖ ดำเนินการจัดทำรายงานเฝ้าระวังภัยคุกคามทางไซเบอร์ (Incident Report) เป็นประจำทุกวันตลอดระยะเวลาสัญญา โดยจัดส่งทางระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือ Shared File Cloud Services หรือช่องทาง Social Media อื่นๆ ตามที่กรมการปกครองกำหนด และรวบรวมสรุปส่งเอกสารของเดือน ให้กรมการปกครองภายในวันที่ ๑๕ ของเดือนถัดไป โดยต้องครอบคลุมเนื้อหาอย่างน้อยดังต่อไปนี้

(๑) ระบุประเภทของภัยคุกคาม

(๒) วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

- (๓) ระบุต้นทาง (Attacker) และปลายทาง (Target)
- (๔) ภาพการเชื่อมโยงเหตุการณ์ภัยคุกคามที่เกิดขึ้น
- (๕) รายละเอียดเหตุการณ์และพฤติกรรมทั้งหมด
- (๖) ให้คำแนะนำพร้อมขั้นตอนการดำเนินการแก้ไขเชิงเทคนิคและแนวทางในการป้องกันไม่ให้เกิดเหตุการณ์เดิมซ้ำอีก
- (๗) ระบุระดับความรุนแรง (Severity) ตาม Service Level Agreement (SLA) ดังรายละเอียดภาคผนวก ก.

๑๑.๗ ดำเนินการจัดทำรายงานประจำเดือนเป็นประจำทุกเดือนตลอดระยะสัญญาโดยจัดส่งทางระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือ Shared File Cloud Services หรือช่องทาง Social Media อื่น ๆ ตามที่กรมการปกครองกำหนด และส่งเอกสารให้กรมการปกครองภายในวันที่ ๑๕ ของเดือนถัดไป โดยมีรายละเอียดของรายงานเป็นอย่างน้อย ดังนี้

(๑) บทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังภัยคุกคาม ความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security Monitoring) ในแต่ละเดือน

(๒) สรุปเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีการจัดระดับความรุนแรง ประเภทของภัยคุกคามและความเชื่อมโยงของแต่ละภัยคุกคาม โดยสรุปสถานะการดำเนินการบริหารจัดการภัยคุกคามที่พบหรือความผิดปกติที่กระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกิดขึ้นในแต่ละเดือน

(๓) รายงานการปฏิบัติงานของผู้ปฏิบัติงานประจำ SOC ณ สถานที่ของผู้ให้บริการ โดยมีรายละเอียดในแต่ละช่วงเวลาของผู้ให้บริการ (๒๔x๗)

(๔) รายงานสถานะและประสิทธิภาพในภาพรวมของระบบที่ให้บริการ ตามข้อ ๑๐.๑ - ๑๐.๓

(๕) รายงานสรุปข่าวสารตามข้อ ๑๑.๓.๗

๑๑.๑๒ ผู้รับจ้างต้องลบบัญชีของผู้ใช้และช่องทางการเข้าถึงระบบการให้บริการในโครงการของบุคลากรที่ไม่เกี่ยวข้องกับโครงการออกทั้งหมดเมื่อมีการเปลี่ยนตัวบุคลากรในโครงการ

๑๒. ข้อมูลที่เป็นความลับและการรักษาความลับ

๑๒.๑ ผู้รับจ้างต้องรักษาข้อมูลของผู้ว่าจ้างไว้เป็นความลับ

๑๒.๒ ผู้รับจ้างจะต้องไม่เปิดเผยข้อมูลอันเป็นความลับใดๆ หรือข้อมูลอื่นใดทั้งหมดหรือบางส่วนที่ได้รับหรือรับรู้มาจากผู้ว่าจ้าง ให้ผู้อื่นทราบโดยมิได้รับความยินยอมจากผู้ว่าจ้าง หากผู้รับจ้างนำไปเปิดเผยจะต้องรับผิดชอบตามกฎหมาย

๑๒.๓ ผู้รับจ้างต้องให้บุคลากรของผู้รับจ้างทุกคนในโครงการลงนามหนังสือรับรองไม่เปิดเผยข้อมูลอันเป็นความลับใดๆ หรือข้อมูลอื่นใดทั้งหมดหรือบางส่วนที่ได้รับรู้มาจากการปกครอง ให้ผู้อื่นทราบโดย

มิได้รับความยินยอมจากผู้ว่าจ้าง หากผู้รับจ้างนำไปเปิดเผย จะต้องรับผิดชอบตามกฎหมาย โดยจัดทำหนังสือรับรองให้การคุ้มครองภายใน ๓๐ วัน นับถัดจากวันเริ่มสัญญา (ภาคผนวก ข.)

๑๓. ข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑๓.๑ ผู้รับจ้างต้องดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ว่าจ้างเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

๑๓.๒ จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ว่าจ้างทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

๑๓.๓ ผู้รับจ้างต้องจัดทำ และเก็บรักษาบันทึกการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activity: RoPA) ไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด โดยมีรายละเอียดที่บันทึกใน RoPA อย่างน้อยตามมาตรา ๓๙ แห่งพระราชบัญญัติดังกล่าว เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบได้ ซึ่งจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

๑๓.๔ ผู้รับจ้างต้องลงนามในบันทึกข้อตกลงการประมวลผลข้อมูลส่วนบุคคลร่วมกับผู้ว่าจ้าง เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้รับจ้างให้เป็นไปตามพระราชบัญญัตินี้ โดยจัดทำข้อตกลงดังกล่าวในวันลงนามในสัญญา (ภาคผนวก ค.)

๑๕. ค่าจ้างและการจ่ายเงิน

กรมการปกครอง จะจ่ายค่าจ้างซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่น ๆ และค่าใช้จ่ายทั้งปวงด้วยแล้วให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้รับจ้าง โดยแบ่งเป็นงวดจำนวน ๑๒ งวดๆ ละ ๑ เดือน

ภาคผนวก ก.

Service Level Agreement (SLA)

SLA สำหรับบริการเฝ้าระวังและตอบสนองต่อเหตุการณ์ที่อยู่ในข่ายเป็นภัยคุกคามทางไซเบอร์

ระดับความรุนแรง (Severity)	เวลาในการวิเคราะห์และแจ้งเตือน กรมการปกครอง (Detection & Investigation) (เครื่องคอมพิวเตอร์และอุปกรณ์ใน ศูนย์สารสนเทศที่ดิน)	เวลาในการวิเคราะห์และแจ้งเตือน กรมการปกครอง (Detection & Investigation) (เครื่องคอมพิวเตอร์และอุปกรณ์ลูก ข่าย)
สูงมาก (Very High)	๓๐ นาที	๑ ชั่วโมง
สูง (High)	๒ ชั่วโมง	๔ ชั่วโมง
ปานกลาง (Medium)	๔ ชั่วโมง	๖ ชั่วโมง
ต่ำ (Low)	๒๔ ชั่วโมง	๔๘ ชั่วโมง
* Threat Response SLA หมายถึง เวลานั้นนับตั้งแต่ได้รับการแจ้งเตือนจากระบบตรวจจับ จนกระทั่งได้ทำการวิเคราะห์ภัยคุกคามและแจ้งเตือน พร้อมให้ข้อมูลประกอบเพิ่มเติมกับกรมการปกครอง		