ชื่อโครงการ จ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services)

หน่วยงาน กองโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล สำนักดิจิทัลกรุงเทพมหานคร

ปีงบประมาณ พ.ศ. ๒๕๗๐

---

๑. หลักการและเหตุผล

ด้วยปัจจุบันมีภัยคุกคามทางไซเบอร์ต่าง ๆ ที่เกิดขึ้นมากมาย และเกิดขึ้นใหม่อย่างหลากหลายรูปแบบ ซึ่งกรุงเทพมหานครมีระบบเทคโนโลยีสารสนเทศที่ให้บริการประชาชน รวมถึงเจ้าหน้าที่ภายในหน่วยงานของกรุงเทพมหานครในการปฏิบัติงานอยู่มากมายและหลากหลาย

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๕ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๔ ซึ่งกำหนดไว้ ๓ องค์ประกอบ ได้แก่

๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. แผนการรับมือภัยคุกคามทางไซเบอร์

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้กำหนดให้กรุงเทพมหานครมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยกำหนดหน้าที่ตามมาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัย

จากเหตุผลดังกล่าวข้างต้น ทำให้กองโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล ดำเนินโครงการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) เพื่อช่วยให้รับรู้ถึงสถานการณ์ภัยคุกคามทางไซเบอร์ต่าง ๆ และระบุถึงเหตุการณ์ผิดปกติได้อย่างรวดเร็ว แม่นยำ และให้มีความพร้อมในการรับมือและสามารถตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้ทันท่วงที

๒. วัตถุประสงค์

๒.๑ กรุงเทพมหานครมีระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ต่อระบบเทคโนโลยีสารสนเทศของกรุงเทพมหานคร

๒.๒ ลดความเสี่ยงในการถูกโจมตีทางไซเบอร์ ซึ่งเป็นสาเหตุที่อาจทำให้เกิดความผิดตามกฎหมายทางด้านคอมพิวเตอร์ อาทิ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓. เป้าหมาย ...

๓. เป้าหมาย

กรุงเทพมหานครมีระบบสำหรับเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคาม หรือเหตุการณ์ผิดปกติ อันอาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและข้อมูลของกรุงเทพมหานคร

๔. ลักษณะโครงการ

ประเภทโครงการ

เป็นโครงการใหม่ และเป็นโครงการแผนยุทธศาสตร์

ความสอดคล้อง

เป็นโครงการที่สอดคล้องกับแผนปฏิบัติราชการกรุงเทพมหานคร ประจำปี ๒๕๗๐ ยุทธศาสตร์ที่ ๙ ด้านบริหารจัดการดี ประเด็นการพัฒนา ๙.๑ ระบบงาน เงิน คน ระเบียบ ที่มีประสิทธิภาพ (๓) พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัลให้สามารถรองรับการมุ่งสู่มหานครดิจิทัล ตัววัดผลหลัก OKR ๙๑xxx : เวลาตอบสนองต่อภัยคุกคาม

รูปแบบโครงการ

เป็นโครงการจ้างเหมาบริการ และเป็นโครงการแผนยุทธศาสตร์

๕. ระยะเวลาดำเนินการและสถานที่ดำเนินการ

ระยะเวลาดำเนินการตามสัญญา ๑๒ เดือน นับถัดจากวันที่ลงนามในสัญญา

๖. แผนปฏิบัติการ

ขั้นตอนการดำเนินงาน	ปีงบประมาณ พ.ศ.๒๕๖๙						
	พ.ศ.๒๕๖๙			พ.ศ. ๒๕๗๐			
	ส.ค.	ก.ย.	ต.ค.-ธ.ค.	ม.ค. - มี.ค.	เม.ย.-มิ.ย.	ก.ค.-ก.ย.	ต.ค.
๑. ขออนุมัติโครงการและรายละเอียดค่าใช้จ่าย	—						
๒. แต่งตั้งคณะกรรมการกำหนดขอบเขตการดำเนินงานจ้างเหมาบริการและขออนุมัติขอบเขตการดำเนินงานจ้างเหมาบริการ	—						
๓. ขออนุมัติจ้างเหมาบริการพร้อมแต่งตั้งคณะกรรมการตรวจรับและทำสัญญาจ้างเหมาบริการ		—					
๔. ที่ปรึกษาดำเนินการตามสัญญาจ้างและส่งมอบงานตามกำหนด			—	—	—	—	
๕. สรุปผลการดำเนินงานและจัดทำรายงานเสนอผู้บริหาร							—

๗. งบประมาณ...

๗. งบประมาณ

ประมาณการงบประมาณ

รายละเอียด/กิจกรรม	จำนวน (หน่วย)	ราคา (บาท)	กฎหมายระเบียบที่เกี่ยวข้อง
๑. จ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) ประกอบด้วย	๑ บริการ		ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างภาครัฐและการบริหารพัสดุภาครัฐ พ.ศ.๒๕๖๐
- ค่าบริการระบบจัดเก็บข้อมูลและวิเคราะห์ความปลอดภัย (SIEM)		๘,๗๙๕,๔๐๐	
- ค่าบริหารจัดการและตอบสนองต่อภัยคุกคามอัตโนมัติ (SOAR)		๗,๐๖๒,๐๐๐	
- ระบบติดตามข่าวสารภัยคุกคามไซเบอร์ (Threat Intelligence)		๕,๐๐๗,๖๐๐	
- บริการพื้นที่จำลองสำหรับการทดสอบไฟล์และโปรแกรม เพื่อยืนยันความปลอดภัยและภัยคุกคามอื่น ๆ (Sandbox Security)		๔,๔๙๔,๐๐๐	
- บริการเฝ้าระวังภัยคุกคามทางไซเบอร์ (CSOC)		๒,๒๓๐,๘๐๐	
- บริการทำสถานการณ์โจมตีในรูปแบบ Social Engineering		๖,๘๐๕,๒๐๐	
- บริการป้องกันการโจมตีเว็บไซต์ (Web Application Firewall)		๑,๖๐๕,๐๐๐	
รวมทั้งสิ้น		๓๖,๐๐๐,๐๐๐	

เบิกจ่ายจากงบประมาณประจำปี พ.ศ. ๒๕๗๐ แผนงานบริหารงานกรุงเทพมหานคร ผลผลิตระบบเทคโนโลยีสารสนเทศและการสื่อสาร งบรายจ่ายอื่น รายการจ้างเหมาบริการระบบความมั่นคงปลอดภัยและการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Managed Services) จำนวน ๓๖,๐๐๐,๐๐๐.- บาท (สามสิบหกล้านบาทถ้วน)

๘. ความเสี่ยงของโครงการและแนวการบริหารความเสี่ยง

ความเสี่ยง	การประเมินความเสี่ยง			แนวทางการบริหารความเสี่ยง
	โอกาสที่จะเกิด	ผลกระทบ	ระดับของความเสี่ยง	
การจัดหาไม่เป็นไปตามแผนที่กำหนดไว้	๓	๓	สูง	๑. ควบคุมกิจกรรมตามแผนที่กำหนด ๒. มีการรายงานความคืบหน้าของโครงการให้ผู้บริหารทราบ
การดำเนินการตามสัญญาไม่เป็นไปตามแผนที่กำหนดไว้	๒	๒	ปานกลาง	๑. ประชุมเตรียมความพร้อมก่อนเริ่มสัญญา ๒. ควบคุมกิจกรรมตามแผนที่กำหนด

๙. ประโยชน์ที่คาดว่าจะได้รับ ...

๙. ประโยชน์ที่คาดว่าจะได้รับ

๙.๑ สามารถตรวจจับและเฝ้าระวังภัยคุกคามทางไซเบอร์ ได้อย่างทันท่วงที

๙.๓ สามารถแจ้งเตือนภัยคุกคามทางไซเบอร์ใหม่ และภัยคุกคามเหตุการณ์ผิดปกติได้อย่างมีประสิทธิภาพ

๙.๒ หากเกิดเหตุการณ์ถูกโจมตีทางไซเบอร์ สามารถวิเคราะห์สาเหตุ และพิสูจน์หลักฐานภัยคุกคามที่เกิดขึ้นได้อย่างมีประสิทธิภาพ

๑๐. การติดตามประเมินผล

๑๐.๑. ตัวชี้วัดความสำเร็จ

ตัวชี้วัด	ค่าเป้าหมาย	ประเภทตัวชี้วัด	วิธีการคำนวณ/เครื่องมือในการใช้วัด	ระยะเวลา
ร้อยละความสำเร็จในการจัดหา	๑๐๐	ผลผลิต	การส่งมอบงานและการตรวจรับงาน เครื่องมือในการใช้วัด ใบตรวจรับมอบงาน	๑๒ เดือน

๑๐.๒ การติดตามความก้าวหน้า

มีการรายงานความก้าวหน้าการดำเนินโครงการเป็นรายเดือน

๑๐.๓ การประเมินผลโครงการ

สามารถดำเนินการบริหารจัดการกระบวนการที่เกี่ยวข้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้อย่างมีประสิทธิภาพ

ลงชื่อ.....ผู้เสนอโครงการ

ลงชื่อ.....ผู้อนุมัติโครงการ