รายละเอียดงานจ้างเหมาบริการระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และบริการเฝ้าระวังและวิเคราะห์ภัยคุกคามทางคอมพิวเตอร์
(Log Management Service and Security Monitoring Service)

1. เงื่อนไขในการดำเนินงาน

ข้อกำหนดเงื่อนไขเกี่ยวกับความต้องการทั่วไปของสถาบันวิจัยแสงซินโครตรอน (องค์การมหาชน) หรือ สซ. ความต้องการทั่วไปของ สซ. คือ ระบบเก็บบันทึกการใช้งานเครือข่ายสื่อสารคอมพิวเตอร์และบริการเฝ้าระวังและวิเคราะห์ภัยคุกคามทางคอมพิวเตอร์ ของ สซ. สำหรับเก็บบันทึกข้อมูลจราจรทางคอมพิวเตอร์ที่ถูกส่งผ่านระบบเครือข่ายสื่อสาร เพื่อเป็นไปตามข้อบังคับทางกฎหมายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 พร้อมทั้งเพื่อให้มีการเฝ้าระวังและวิเคราะห์ภัยคุกคาม โดยมีสัญญาการทำงาน 12 เดือน

2. ข้อกำหนดเงื่อนไขเกี่ยวกับคุณลักษณะเฉพาะของบริการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และบริการเฝ้าระวังและวิเคราะห์ภัยคุกคามทางคอมพิวเตอร์

2.1 บริการจัดเก็บข้อมูลข้อมูลจราจรทางคอมพิวเตอร์ของ สซ. มีคุณลักษณะดังนี้

2.1.1 จัดเตรียมระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ เป็นระยะเวลา 90 วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และรองรับปริมาณข้อมูลจราจรทางคอมพิวเตอร์จำนวน 1 GB ต่อวัน โดยไม่จำกัดจำนวนอุปกรณ์กำเนิดข้อมูลจราจรทางคอมพิวเตอร์ (Log Source)

2.1.2 อุปกรณ์ที่นำมาติดตั้งเพื่อดำเนินการจัดเก็บข้อมูลจราจรจะต้องจัดเก็บ log file ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 โดยได้รับรองมาตรฐานการจัดเก็บและรักษาความปลอดภัยของ log file ที่ได้มาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ. 4003.1-2552)

2.1.3 มีการเข้ารหัสข้อมูลระหว่างการจัดส่งไปยังศูนย์จัดเก็บข้อมูลของผู้ให้บริการ

2.1.4 มีบริการสำรองข้อมูล (Backup Log) 1 สำเนา โดยจัดเก็บไว้ที่ศูนย์สำรองข้อมูลของผู้ให้บริการ (DR Site) ซึ่งผ่านการรับรองมาตรฐานสากลด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2013)

2.1.5 มีระบบค้นหา (Searching) ข้อมูลหรือย้อนหลังกลับดูข้อมูลตามวันเวลาที่ต้องการได้

2.1.6 มีระบบการพิสูจน์ตัวตนโดยใช้ 2 Factor Authentication เช่น Tokens ในการเข้าใช้ระบบค้นหา (Searching)

2.1.7 มีการจัดทำรายงานประจำวัน โดยสรุปปริมาณข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บ

2.1.8 บริการตรวจสอบสถานะการส่งข้อมูลจราจรทางคอมพิวเตอร์ พร้อมแจ้งเตือนไปยังเจ้าหน้าที่ที่เกี่ยวข้องผ่านทางระบบไปรษณีย์อิเล็กทรอนิกส์ (E-Mail) ในกรณีที่อุปกรณ์ไม่อาจส่งข้อมูลมายังสถานที่จัดเก็บข้อมูลได้ ภายในระยะเวลา 4 ชั่วโมง

2.1.9 บริการให้คำปรึกษาผ่านทางอีเมลและโทรศัพท์ในวันทำการ 8x5 (ตลอด 8 ชั่วโมง 5 วันทำการ)

2.2 บริการเฝ้าระวังและวิเคราะห์ภัยคุกคามทางคอมพิวเตอร์มีคุณลักษณะดังนี้

2.2.1 เป็นศูนย์เฝ้าระวังภัยคุกคาม (Security Operation Center) ที่ให้บริการวิเคราะห์ความเกี่ยวโยงของเหตุการณ์และภัยคุกคามด้านความปลอดภัยสารสนเทศ (Security Monitoring) จากข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของเครื่องแม่ข่าย อุปกรณ์เครือข่ายและระบบงานต่าง ๆ ทุกวัน ตลอด 24 ชั่วโมง

2.2.2 บริการที่นำเสนอจะต้องเป็นระบบที่ออกแบบมาเพื่อใช้ในการวิเคราะห์ความเกี่ยวโยงของเหตุการณ์ด้านความปลอดภัยสารสนเทศ SIEM (Security Information and Event Management) โดยเฉพาะ

2.2.3 บริการสามารถรองรับการวิเคราะห์ข้อมูลจราจรจากอุปกรณ์ต้นทางได้ 1 Data Source (วิเคราะห์ข้อมูลจราจรจาก อุปกรณ์ Palo Alto Networks ที่ทาง สซ. ติดตั้งและใช้งานอยู่)

2.2.4 สามารถแจ้งเตือนไปยังผู้ดูแลระบบได้แบบอัตโนมัติ (Real-time Alert) ในกรณีที่เกิดภัยคุกคามหรือเป็นการใช้งานปกติของระบบแต่มีพฤติกรรมที่น่าสงสัย เช่น การล็อกอินเข้าระบบไม่สำเร็จเป็นจำนวนมาก เป็นต้น

2.2.5 บริการวิเคราะห์ปัญหาที่เกิดจากภัยคุกคาม โดยให้คำปรึกษาและวิเคราะห์เชิงลึก (Incident Report) ซึ่งประกอบไปด้วยแผนภูมิรูปภาพแสดงสรุปเหตุการณ์อย่างละเอียด (Correlation Graph) พร้อมทั้งแนวทางในการป้องกันปัญหาทางด้านความปลอดภัยที่อาจจะเกิดขึ้นได้อีกในอนาคต โดยจัดเป็นรูปแบบของรายงาน จำนวนไม่เกิน 4 ครั้งต่อเดือน แบบภาษาไทย

2.2.6 มีผู้เชี่ยวชาญทำหน้าที่ปรับแต่งและกำหนดค่าการทำงานของระบบวิเคราะห์ความเกี่ยวโยงของเหตุการณ์และเฝ้าระวังภัยคุกคามทางคอมพิวเตอร์

2.2.7 มีผู้เชี่ยวชาญให้คำปรึกษาเกี่ยวกับระบบวิเคราะห์ความเกี่ยวโยงของเหตุการณ์และเฝ้าระวังภัยคุกคามทางคอมพิวเตอร์

2.3 ข้อกำหนดเงื่อนไขเกี่ยวกับการรับประกันหรือการให้บริการ

2.3.1 ในกรณีที่ระบบฯ ติดตั้งหรืออุปกรณ์ที่ผู้เสนอราคาจัดหาเกิดชำรุดหรือขัดข้อง ผู้เสนอราคาจะต้องดำเนินการซ่อมแซมแก้ไขให้แล้วเสร็จภายในระยะเวลา 2 วัน กรณีที่ไม่สามารถแก้ไขให้สามารถใช้งานได้ ภายในระยะเวลาที่กำหนด หากปัญหาเกิดจากอุปกรณ์ ผู้เสนอราคาจะต้องนำอุปกรณ์ที่มีประสิทธิภาพเท่าเทียมกันหรือดีกว่านำมาติดตั้งเพื่อให้งานทดแทน ให้ใช้งานจนกว่าผู้เสนอราคา จะทำการแก้ไขอุปกรณ์นั้น ๆ แล้วเสร็จ

2.3.2 ผู้เสนอราคาต้องมีบริการรับแจ้ง (Help Desk Center) ณ ที่ทำการของผู้เสนอราคา และให้บริการรับแจ้งปัญหาจากผู้ใช้งานตลอดเวลาการปฏิบัติงานวันเวลาราชการ โดยแจ้งให้ทราบถึงหมายเลขโทรศัพท์ที่ สซ. สามารถติดต่อได้ ในวันยื่นเอกสารสอบราคา

2.3.3 ผู้เสนอราคาจะต้องจัดเจ้าหน้าที่ให้คำแนะนำเกี่ยวกับวิธีการใช้งาน การบำรุงรักษาและแนะนำวิธีการแก้ไขปัญหาที่เกิดขึ้นในระหว่างการส่งมอบระบบด้วย

3. **ข้อกำหนดเงื่อนไขเกี่ยวกับการชำระเงิน**

สช. จะจ่ายชำระค่าบริการเป็นรายเดือนๆ จำนวน 12 เดือน โดยเริ่มจ่ายชำระค่าเช่าบริการเมื่อดำเนินการติดตั้งเสร็จเรียบร้อย และคณะกรรมการตรวจรับพัสดุฯ ของ สช. ได้ทำการตรวจรับถูกต้องครบถ้วนตามสัญญาเรียบร้อยแล้ว

ลงชื่อ.....ผู้กำหนดคุณลักษณะ

(.....)