

## รายละเอียดคุณลักษณะเฉพาะ ระบบเข้ารหัสฐานข้อมูล (Database Encryption)

### 1. ความเป็นมา

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จำเป็นต้องจัดเก็บและบริหารจัดการข้อมูลส่วนบุคคลและข้อมูลด้านสารสนเทศที่มีความสำคัญจำนวนมาก ซึ่งในปัจจุบันพบว่ามาตรการด้านการรักษาความมั่นคงปลอดภัยในการป้องกันข้อมูลยังไม่ครอบคลุมรอบด้าน เพื่อให้การดำเนินงานของ สสวท. เป็นไปตามกฎหมายและมาตรฐานสากล ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รวมถึงนโยบายด้านความมั่นคงปลอดภัยสารสนเทศของสำนักงานฯ พ.ศ. 2565 สสวท. จึงมีความจำเป็นต้องยกระดับมาตรฐานการรักษาความปลอดภัย

การดำเนินการดังกล่าวมีวัตถุประสงค์เพื่อรักษาความลับและความปลอดภัยของข้อมูลในสถานะหยุดนิ่ง (Data-at-rest) โดยอาศัยเทคโนโลยีการเข้ารหัสลับ (Encryption) และการจัดการกุญแจดิจิทัลรวมศูนย์ เพื่อป้องกันผลกระทบจากการถูกโจมตีทางไซเบอร์ และลดความเสี่ยงจากการละเมิดข้อมูล (Data Breach) ซึ่งจะช่วยสร้างความมั่นใจและความน่าเชื่อถือในการทำธุรกรรมดิจิทัลและการให้บริการสารสนเทศของ สสวท. ให้เป็นไปอย่างมั่นคงปลอดภัย

### 2. วัตถุประสงค์

เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศของ สสวท. ให้สอดคล้องกับกฎหมายและนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ โดยการจัดหาอุปกรณ์และซอฟต์แวร์สำหรับเข้ารหัสข้อมูลสำคัญในระดับฐานข้อมูลและโครงสร้างพื้นฐาน เพื่อป้องกันการรั่วไหลหรือการเข้าถึงข้อมูลโดยมิชอบ โดยมีการจัดหา ดังต่อไปนี้

รายการที่ 1 อุปกรณ์เข้ารหัสฐานข้อมูล (Hardware Security Module : HSM) จำนวน 1 เครื่อง

รายการที่ 2 ซอฟต์แวร์ระบบบริหารจัดการกุญแจเข้ารหัสฐานข้อมูลและใบรับรองอิเล็กทรอนิกส์ส่วนกลาง (Crypto Services Gateway : CSP) จำนวน 1 ระบบ

### 3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง



3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพขายงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน หรือหนังสือเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอ ในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

3.11 ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e - GP) ของกรมบัญชีกลาง

3.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ เป็นไปตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) ที่ 0405.2/ว124 ลงวันที่ 1 มีนาคม 2566

3.13 ผู้ยื่นข้อเสนอต้องมีผลงานจำหน่ายอุปกรณ์หรือระบบหรือซอฟต์แวร์ที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ จำนวน 1-2 ผลงาน วงเงินรวมกันไม่น้อยกว่า 1,600,000 บาท (หนึ่งล้านหกแสนบาทถ้วน) ใน

ระยะเวลาไม่เกิน 5 ปี จนถึงวันที่ยื่นข้อเสนอ และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือ หน่วยงานเอกชนที่ สถาบันส่งเสริมการสนธิวิทยาศาสตร์และเทคโนโลยี (สสวท.) เชื้อถือ โดยยื่นสำเนาหนังสือ รับรองผลงานและสำเนาสัญญาหรือใบสั่งซื้อ ซึ่งเป็นงานเดียวกัน

3.14 ผู้ยื่นข้อเสนอต้องจัดทำรายการวัสดุหรือครุภัณฑ์ที่ใช้ในงานจ้างซึ่งเป็นพัสดุที่ผลิตภายในประเทศ โดย ต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างนี้ (ถ้ามี)

3.15 ผู้ยื่นข้อเสนอต้องส่งมอบแผนการทำงานตลอดระยะเวลาตามสัญญา ภายใน 14 วัน นับถัดจากวันลง นามในสัญญา

### หลักฐานการยื่นข้อเสนอ

(1) ผู้ยื่นข้อเสนอต้องได้รับแต่งตั้งให้เป็นตัวแทนจำหน่ายอุปกรณ์ รายการที่ 1-2 ตามข้อกำหนดทาง เทคนิค จากเจ้าของผลิตภัณฑ์หรือตัวแทนจำหน่ายในประเทศไทย เพื่อแสดงถึงการสนับสนุนทางด้านเทคนิค เพื่อให้คำปรึกษาแนะนำการใช้งานในผลิตภัณฑ์ที่ได้นำเสนอ โดยจะต้องมีหนังสือรับรองตัวจริง มาประกอบการ พิจารณา (นับถัดจากวันที่ยื่นข้อเสนอในระบบของกรมบัญชีกลาง)

(2) ผู้ยื่นข้อเสนอหรือเจ้าของผลิตภัณฑ์หรือตัวแทนจำหน่ายในประเทศไทย ต้องมีศูนย์ที่บริการที่ได้รับ มาตรฐานบริการหลังการขายหรือมีกระบวนการ (Process) การให้บริการในภาพรวมตาม ISO 9001:2008 หรือ 2015

(3) ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความเชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ (Cybersecurity) โดยต้องได้ผ่านการฝึกอบรมหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ระดับผู้เชี่ยวชาญ ของ สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ ได้รับ Certificate ระดับสากล เช่น CompTIA Security+ เทียบเท่าหรือดีกว่า อย่างน้อย 1 คน

(4) ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความเชี่ยวชาญด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยต้องมีใบรับรองมาตรฐานวิชาชีพด้านการรักษาความปลอดภัยระบบสารสนเทศ ได้แก่ Certified Information Systems Security Professional (CISSP) หรือ Certified Information Security Manager (CISM) เทียบเท่าหรือดีกว่า อย่างน้อย 1 คน

(5) ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความเชี่ยวชาญด้านการบริหารจัดการฐานข้อมูล โดยต้องมีใบรับรอง ความเชี่ยวชาญ ระดับ Microsoft Certified: Database Administration เทียบเท่าหรือดีกว่า อย่างน้อย 1 คน หรือ บุคลากรที่มีความเชี่ยวชาญด้านการบริหารจัดการระบบปฏิบัติการ โดยต้องมีใบรับรองความเชี่ยวชาญ ระดับ Microsoft Certified: Administrator Associate เทียบเท่าหรือดีกว่า อย่างน้อย 1 คน

(6) ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความเชี่ยวชาญเฉพาะทางในผลิตภัณฑ์ที่นำเสนอ โดยต้องผ่านการ อบรมและได้รับใบรับรองความเชี่ยวชาญจากเจ้าของผลิตภัณฑ์ (Certified Engineer) ในด้านอุปกรณ์ Hardware

Security Module (HSM) หรือระบบ Key Management อย่างน้อย 1 คน เพื่อยืนยันความเชี่ยวชาญในการติดตั้งและปรับแต่งระบบตามมาตรฐานของเจ้าของผลิตภัณฑ์

(7) ผู้ยื่นข้อเสนอต้องเสนอข้อมูลทางด้านเทคนิคของครุภัณฑ์ ที่เสนอ โดยจัดทำเอกสารเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะครุภัณฑ์ที่กำหนดข้างต้นทั้งหมด กับรายละเอียดที่ผู้ยื่นข้อเสนอเสนอ โดยระบุเอกสารอ้างอิง แคตตาล็อก ให้ถูกต้อง และในเอกสารอ้างอิง แคตตาล็อก ต้องขีดเส้นใต้ หรือใช้ปากกาเน้นข้อความ ระบุหมายเลขข้อที่อ้างอิงให้ชัดเจน ทั้งนี้ต้องส่งมาพร้อมกับเอกสารแสดงคุณลักษณะ สสวท. ขอสงวนสิทธิ์ที่จะไม่พิจารณาผู้ยื่นข้อเสนอ หากไม่ปฏิบัติตามไม่ว่ากรณีใดๆ ทั้งสิ้นตามตัวอย่างด้านล่าง

#### ตัวอย่าง ตารางเปรียบเทียบ

รายละเอียดที่ สสวท. กำหนด	รายละเอียดที่ผู้ยื่นข้อเสนอ เสนอ	เอกสารอ้างอิง (ระบุเลขหน้า)
	* ต้องระบุเอกสารให้ชัดเจน ห้ามมี ไม่น้อยกว่า	

#### 4. รายละเอียดคุณลักษณะเฉพาะ

##### รายการที่ 1 อุปกรณ์เข้ารหัสฐานข้อมูล (Hardware Security Module : HSM) จำนวน 1 เครื่อง

เป็นอุปกรณ์ที่ถูกออกแบบมาเพื่อทำหน้าที่เป็น Hardware Security Module (HSM) โดยเฉพาะ มีคุณสมบัติดังนี้

1.1 ผ่านการรับรองความมั่นคงปลอดภัยตามมาตรฐาน FIPS 140-2 Level 3 ที่ใบรับรองยังมีผลบังคับใช้ (Active) หรือ มาตรฐาน FIPS 140-3 Level 3 รวมถึงมาตรฐาน eIDAS และ Common Criteria EAL4+ (หรือสูงกว่า)

1.2 อุปกรณ์ต้องมีเครื่องอ่านสมาร์ทการ์ดติดตั้งภายในตัวเครื่อง (Integrated Smart Card Reader) พร้อมสมาร์ทการ์ดสำหรับใช้ในการยืนยันตัวตนและการเข้าถึงอุปกรณ์ (Multi-factor Authentication) ตามนโยบายความปลอดภัย

1.3 มีประสิทธิภาพในการประมวลผลธุรกรรม (Transactions Per Second) ดังนี้

- คีย์แบบ RSA-2048: ไม่น้อยกว่า 580 ธุรกรรมต่อวินาที และสามารถขยายประสิทธิภาพได้ถึง 11,680 ธุรกรรมต่อวินาที ผ่านการอัปเกรด License โดยไม่ต้องเปลี่ยนตัวอุปกรณ์

- คีย์แบบ RSA-4096: ไม่น้อยกว่า 110 ธุรกรรมต่อวินาที และสามารถขยายประสิทธิภาพได้ถึง 2,050 ธุรกรรมต่อวินาที ผ่านการอัปเกรด License โดยไม่ต้องเปลี่ยนตัวอุปกรณ์



1.4 รองรับอัลกอริทึมในการเข้ารหัสตามมาตรฐานสากล ได้แก่

Asymmetric Algorithms: RSA, Diffie-Hellman และ DSA เป็นอย่างน้อย

Symmetric Algorithms: AES, Arcfour, ARIA, Camellia และ 3DES เป็นอย่างน้อย

Hashing/HMAC: MD5, RIPEMD160, SEED, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 และ Tiger เป็นอย่างน้อย

1.5 รองรับการเชื่อมต่อผ่าน Application Program Interface (API) มาตรฐาน ได้แก่ PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI/CNG และ nCore เป็นอย่างน้อย

1.6 รองรับการทำงานร่วมกับ REST API Web Services สำหรับการเข้ารหัส Encryption, Decryption, Signing, Verifying และ Key Generation โดยต้องเป็นโซลูชันจากผู้ผลิตรายเดียวกับอุปกรณ์

1.7 ใช้สถาปัตยกรรมการปกป้อง Application Keys โดยการเข้ารหัสด้วย Master Key ภายในอุปกรณ์ HSM (Security World) เพื่อเปลี่ยนเป็น Application Key Tokens และสามารถจัดเก็บไว้ภายนอกอุปกรณ์ (Client Host) ได้อย่างปลอดภัย

1.8 รองรับการสำรองข้อมูล (Backup) ของ Application Key Tokens ที่ถูกเข้ารหัสไว้แล้ว โดยไม่จำเป็นต้องติดตั้งอุปกรณ์ HSM เพิ่มเติมเพื่อการสำรองข้อมูล

1.9 รองรับการให้ผู้พัฒนาซอฟต์แวร์สามารถโหลดและรันโปรแกรม (Code Execution) ภายในพื้นที่ปลอดภัยของอุปกรณ์ ได้ ผ่านการอัปเดต License โดยไม่ต้องเปลี่ยนตัวอุปกรณ์

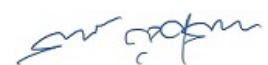
1.10 กรณีอุปกรณ์ชำรุดและต้องส่งคืนผู้ผลิต จะต้องไม่มีการเก็บ User Application Keys ไว้ภายในตัวเครื่อง (Zeroization/Host-stored Keys) เพื่อป้องกันข้อมูลรั่วไหล

1.11 มีช่องเชื่อมต่อเครือข่ายแบบ Gigabit Ethernet ไม่น้อยกว่า 2 พอร์ต และรองรับการทำงานในลักษณะ Failover และ Load Balancing เพื่อความต่อเนื่องในการให้บริการ

1.12 มีแหล่งจ่ายไฟแบบซ้ำซ้อน (Dual Hot-Swap Power Supplies) ที่สามารถเปลี่ยนได้โดยไม่ต้องหยุดการทำงานของอุปกรณ์

## รายการที่ 2 ซอฟต์แวร์ระบบบริหารจัดการกุญแจเข้ารหัสฐานข้อมูลและใบรับรองอิเล็กทรอนิกส์ส่วนกลาง (Crypto Services Gateway : CSP)

เป็นระบบที่ถูกออกแบบมาเพื่อเป็นศูนย์กลางการจัดการกุญแจเข้ารหัส (Cryptographic Key) และใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) โดยเฉพาะ มีคุณสมบัติดังนี้



2.1 สามารถติดตั้งบน On-premise, Private Cloud และ Public Cloud (เช่น AWS, Azure) ได้เป็น  
อย่างน้อย และรองรับการทำงานแบบ Cluster หรือ High Availability (Active-Active หรือ Active-Passive)  
โดยสามารถโอนถ่ายข้อมูลนโยบายและกุญแจระหว่างกันได้โดยอัตโนมัติ

2.2 ต้องรองรับการทำงานร่วมกับอุปกรณ์ Hardware Security Module (HSM) ยี่ห้อเดียวกัน และผ่าน  
มาตรฐาน FIPS 140-2 Level 3 ที่ไบร์รองยังมีผลบังคับใช้ (Active) หรือมาตรฐาน FIPS 140-3 Level 3 เพื่อใช้  
เป็นรากฐานความปลอดภัย (Hardware Root of Trust)

2.3 สามารถทำหน้าที่เป็น Root CA และ Issuing CA เพื่อสร้างและบริหารจัดการวงจรชีวิตของไบร์รอง  
อิเล็กทรอนิกส์ภายในองค์กรได้

2.4 มีระบบ Discovery Scanner สำหรับค้นหาไบร์รองอิเล็กทรอนิกส์ผ่านระบบเครือข่าย และรองรับ  
การนำเข้าไบร์รองแบบ Manual หรือแบบกลุ่ม (Bulk Import) ได้

2.5 สามารถแสดงรายละเอียดของไบร์รอง ได้แก่ Location, Type, Algorithms และวันหมดอายุ พร้อม  
ระบบแจ้งเตือนอัตโนมัติเมื่อใกล้หมดอายุผ่านทาง Email

2.6 สามารถทำหน้าที่เป็น Key Management Server (KMS) ตามมาตรฐาน KMIP เพื่อบริหารจัดการ  
กุญแจเข้ารหัสจากศูนย์กลาง

2.7 สามารถเชื่อมต่อกับระบบฐานข้อมูลเพื่อปกป้องกุญแจที่ใช้ในการเข้ารหัสฐานข้อมูลแบบ TDE  
(Transparent Data Encryption) โดยเฉพาะ Microsoft SQL Server และ Oracle ได้

2.8 สามารถเชื่อมต่อกับระบบ Public Cloud Provider (AWS, Azure, GCP) เพื่อบริหารจัดการกุญแจใน  
รูปแบบ BYOK (Bring Your Own Key) หรือ HYOK (Hold Your Own Key) และรองรับการหมุนเวียนกุญแจ  
(Key Rotation) แบบอัตโนมัติ

2.9 รองรับการทำ Data Tokenization และการเข้ารหัสข้อมูลประเภท Structured Data ผ่าน REST  
API โดยต้องรองรับเทคนิค Format Preserving Encryption (FPE) เพื่อรักษาความยาวและรูปแบบเดิมของข้อมูล

2.10 สามารถเข้ารหัสข้อมูลในระดับ Disk Partition-level พร้อมกำหนดสิทธิ์การเข้าถึงข้อมูล (Access  
Control List: ACL) ได้

2.11 สามารถทำหน้าที่เป็น Secret Management เพื่อบริหารจัดการข้อมูลความลับ เช่น API Key และ  
Password ของระบบงานต่างๆ

2.12 มีระบบ Role-based Access Control (RBAC) เพื่อกำหนดสิทธิ์ผู้ใช้งาน และรองรับการทำงานแบบ  
Multi-tenancy เพื่อแยกส่วนการบริหารจัดการ (Separation of Duties) ของแต่ละหน่วยงานภายในให้เป็นอิสระ  
ต่อกัน



2.13 สามารถตรวจสอบสถานะความมั่นคงปลอดภัยของไบบ์รองและกุญแจตามมาตรฐาน Compliance Template สากล (เช่น NIST) และสามารถสร้าง Custom Template ตามความต้องการของได้

2.14 สามารถสร้างรายงาน (User-defined Report) แบบตั้งเวลาล่วงหน้า และบริหารจัดการระบบผ่าน Web Browser (Browser-based User Interface) ได้

### คุณสมบัติเพิ่มเติม

1. ติดตั้งอุปกรณ์และระบบตามที่เสนอ ให้สามารถทำงานร่วมกับระบบฐานข้อมูลเดิมและระบบเครือข่ายเดิมหรือระบบที่เกี่ยวข้องได้อย่างสมบูรณ์ พร้อมทำการทดสอบ การใช้งานร่วมกับ Application ผ่าน API ตามที่ สสวท. กำหนด

2. รวบรวมข้อมูลและกำหนดนโยบายการจัดการวงจรชีวิตกุญแจเข้ารหัส (Key Lifecycle Management Policy) ให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของ สสวท. ปี 2565 และ กฎหมาย ข้อบังคับ ประกาศ ของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ (สกมช.) หรือ มาตรฐาน NIST

3. จัดทำคู่มือการใช้งาน คู่มือผู้ดูแลระบบ และคู่มือการกู้คืนระบบ (Disaster Recovery Guide) ที่มีรายละเอียดขั้นตอนการสำรองและกู้คืนกุญแจอย่างชัดเจน พร้อมทั้งจัดทำรายงานผลการทดสอบระบบ (UAT Report) ที่ครอบคลุมหัวข้อการทดสอบการกู้คืนระบบ (Disaster Recovery Test) เพื่อพิสูจน์และยืนยันว่าระบบ และกุญแจเข้ารหัสที่สำรองไว้สามารถกู้คืนมาใช้งานได้จริงตามขั้นตอนที่ระบุในคู่มือ


4. ดำเนินการฝึกอบรมการใช้งานและการบริหารจัดการระบบให้แก่เจ้าหน้าที่ผู้ดูแลระบบ เพื่อให้สามารถปฏิบัติงานและกู้คืนระบบเบื้องต้นได้ ระยะเวลาไม่น้อยกว่า 1 วัน

5. ดำเนินการตรวจสอบบำรุงรักษาระบบ (Preventive Maintenance) และให้คำปรึกษาทางเทคนิคตลอด ระยะเวลารับประกันตามเงื่อนไขที่กำหนด โดยมีรายละเอียดการดำเนินการดังนี้

5.1 ดำเนินการเข้าตรวจสอบอุปกรณ์และระบบ ณ สถานที่ติดตั้ง อย่างน้อยทุก 6 เดือน เพื่อให้ เครื่องและระบบอยู่ในสภาพที่ใช้งานได้เป็นปกติและมีประสิทธิภาพ พร้อมดำเนินการอัปเดตซอฟต์แวร์หรือ Patch ความปลอดภัยล่าสุดตามความเหมาะสม

5.2 จัดทำรายงานตรวจสอบสถานะความสมบูรณ์ของอุปกรณ์ (Health Check) และรายงาน ประสิทธิภาพการทำงานของระบบ (Performance Report) เพื่อแสดงค่าสถิติการใช้งานและเสถียรภาพของระบบ

5.3 จัดทำรายงานสรุปผลการให้บริการและสถานะระบบในรูปแบบรายเดือน (Monthly Report) โดยจัดส่งเป็นไฟล์เอกสารอิเล็กทรอนิกส์ (PDF)



## 5. หลักเกณฑ์และสิทธิในการพิจารณาราคา

ในการพิจารณาผลการยื่นข้อเสนอประกวดราคาอิเล็กทรอนิกส์ครั้งนี้ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จะพิจารณาตัดสิน โดยใช้หลักเกณฑ์ราคา เพียงอย่างเดียว และ การพิจารณาผู้ชนะการยื่นข้อเสนอ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จะพิจารณาจาก ราคารวม (รวมภาษีมูลค่าเพิ่มแล้ว) ที่เสนอราคาต่ำสุด

6. วงเงินงบประมาณ จำนวน 3,300,000 บาท (สามล้านสามแสนบาทถ้วน) รวมภาษีมูลค่าเพิ่ม

## 7. ระยะเวลาดำเนินการ

ส่งมอบพร้อมติดตั้งตามที่ สสวท. กำหนด ภายใน 90 วัน นับถัดจากวันลงนามในสัญญา ดังนี้

7.1 ส่งมอบแผนการทำงานตลอดระยะเวลาตามสัญญา ภายใน 14 วัน นับถัดจากวันลงนามในสัญญา

7.2 ก่อนการส่งมอบบริษัท จะต้องทำหนังสือแจ้งกำหนดการส่งมอบล่วงหน้าไม่น้อยกว่า 7 วันทำการ

7.3 ผู้เสนอราคาต้องทำการติดตั้งอุปกรณ์พร้อมสายสัญญาณระหว่างอุปกรณ์ที่เสนอการจัดซื้อครั้งนี้ ให้สามารถใช้งานร่วมกับระบบเครือข่ายของ สสวท ได้เป็นอย่างดี

7.4 ส่งมอบเอกสาร รูปแบบการติดตั้งระบบพร้อมอุปกรณ์ทั้งหมด (Configuration) พร้อมเอกสารแสดงรายละเอียดของอุปกรณ์ โดยระบุชนิด ยี่ห้อ รุ่น จำนวน และ Serial Number ในรูปแบบเอกสารอิเล็กทรอนิกส์ (PDF)

8. การส่งมอบงานและการชำระเงิน ชำระเงิน 100% เมื่อ สสวท. ได้ทดสอบการใช้งานและตรวจรับเรียบร้อยแล้ว

## 9. รายละเอียดการรับประกัน การบำรุงรักษา

9.1 ต้องมีการให้บริการถึงสถานที่ติดตั้ง (On-site Service) ตลอดระยะเวลาการรับประกัน 1 ปี โดยมีรายละเอียดดังนี้

- Response Time: เมื่อได้รับแจ้งเหตุผิดปกติ ผู้รับจ้างต้องตอบสนองปัญหาภายใน 2 ชั่วโมง (ทางโทรศัพท์, อีเมล หรือวีโมท) เพื่อวิเคราะห์ปัญหาเบื้องต้น

- On-site Service: ในกรณีที่จำเป็นต้องเข้าแก้ไข ณ สถานที่ติดตั้ง ผู้รับจ้างต้องดำเนินการให้ถึงสถานที่ภายใน วันทำการถัดไป (Next Business Day) โดยไม่จำกัดจำนวนครั้งตลอดระยะเวลารับประกัน

- Service Level: บริการครอบคลุมเวลาทำการ (8x5) เป็นอย่างน้อย แต่สำหรับกรณีปัญหาในระดับวิกฤต (Critical Issue) ที่ส่งผลกระทบต่อการใช้งานข้อมูลหลัก ต้องพร้อมให้คำปรึกษาและแก้ไขจนกว่าระบบจะกลับมาทำงานได้ตามปกติ

9.2 ตลอดระยะเวลาประกัน สสวท. ต้องได้รับสิทธิ์ในการอัปเดตซอฟต์แวร์และเฟิร์มแวร์ให้เป็นเวอร์ชันใหม่ (New Release/Version) หรือการติดตั้งโปรแกรมแก้ไขช่องโหว่ (Security Patch) โดยผู้รับจ้างต้องเป็นผู้ดำเนินการอัปเดตให้ตามที่สำนักงานฯ ร้องขอ โดยต้องไม่มีค่าใช้จ่ายเพิ่มเติม และต้องมีการทดสอบหรือวางแผนการดำเนินงานเพื่อไม่ให้ส่งผลกระทบต่อการทำงานของระบบเดิมที่เกี่ยวข้อง

9.3 รับประกันความชำรุดบกพร่องของอุปกรณ์และซอฟต์แวร์เป็นเวลา 1 ปี นับถัดจากวันตรวจรับงานงวดสุดท้าย ในกรณีที่พบ Bug หรือความผิดพลาดของซอฟต์แวร์ ผู้รับจ้างต้องดำเนินการแก้ไขหรือหาแนวทางบรรเทาปัญหา (Workaround) ให้แล้วเสร็จภายใน 1 วันทำการ หากอุปกรณ์ HSM ชำรุดและไม่สามารถซ่อมแซมได้ภายใน 24 ชั่วโมง นับจากวันที่เข้าตรวจสอบ ผู้รับจ้างต้องจัดหาอุปกรณ์สำรองที่มีคุณสมบัติไม่ต่ำกว่าเดิมมาติดตั้งให้ใช้งานทดแทนชั่วคราว เพื่อให้ระบบการเข้ารหัสข้อมูลของสำนักงานฯ ทำงานได้อย่างต่อเนื่อง



ตารางแสดงวงเงินงบประมาณที่ได้จัดสรรและราคากลาง (ราคาอ้างอิง)  
ในการจัดซื้อจัดจ้างที่มีใช้งานก่อสร้าง

1. ชื่อโครงการ จัดซื้ออุปกรณ์เข้ารหัสฐานข้อมูล (Database Encryption)  
งบลงทุน ประจำปีงบประมาณ 2569  
รหัสกิจกรรม 408220100  
หน่วยงานเจ้าของโครงการ.....ฝ่ายเทคโนโลยีสารสนเทศ.....
2. วงเงินงบประมาณที่ได้รับจัดสรร..... 3,300,000..... บาท (สามล้านสามแสนบาทถ้วน)
3. วันที่กำหนดราคากลาง (ราคาอ้างอิง)..... 12 มีนาคม 2569 .....  
เป็นเงิน..... 3,300,000..... บาท (สามล้านสามแสนบาทถ้วน)
4. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
  - 4.1 ใบเสนอราคา บริษัท ซีเคียวร์ เซอร์ฟ จำกัด เลขที่ Q#250717-0010-C วันที่ 12 มีนาคม 2569
  - 4.2 ใบเสนอราคา บริษัท อีเทอร์นิตี้ จำกัด เลขที่ 260162 วันที่ 12 มีนาคม 2569
  - 4.3 ใบเสนอราคา บริษัท เน็ตแคร์ โซลูชันส์ จำกัด เลขที่ NCS\_26PC80117 วันที่ 11 มีนาคม 2569
5. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน ประกอบด้วย
  - 5.1 นายภากร กุลสุภกร





## SECURE SERVE CO.LTD.

1/18 Soi Ramintra 14 Yak 11/1,Tharaeng Bangkhen  
Bangkok 10220 Thailand

เลขที่ประจำตัวผู้เสียภาษี : 0105554065634

โทรศัพท์ : 02-170-6104-5 E-mail : info@secureserve.co.th

QUOTATION

## ผู้ซื้อ

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี  
เลขที่ 924 ถนนสุขุมวิท แขวงพระโขนง เขตคลองเตย กรุงเทพฯ 10110

เลขที่ประจำตัวผู้เสียภาษี : 994000165633

ชื่อผู้ติดต่อ Khun Pakorn Kulsupakorn

โทรศัพท์ 02-392-4021

E-mail pkuls@ipst.ac.th

วิธีจัดส่ง จัดส่ง

ที่อยู่จัดส่ง เลขที่ 924 ถนนสุขุมวิท แขวงพระโขนง เขต  
คลองเตย กรุงเทพฯ 10110

โครงการ -

## ใบเสนอราคา

เลขที่ Q#250717-0010-C  
วันที่ 12 มี.ค. 2569  
วันที่ยื่นราคา 13 มี.ย. 2569  
เงื่อนไขการชำระเงิน เครดิต 30 วัน  
Salesperson Manop Keamapiruck  
โทรศัพท์ 0868357544  
E-mail manop@secureserve.co.th

ลำดับ รายละเอียด	จำนวน	หน่วย	ราคา/หน่วย	มูลค่า
✂️ โครงการระบบเข้ารหัสฐานข้อมูล (Database Encryption)				
✂️ Appliance : Entrust HSM				
1 NH2096-B : nShield 5c Base	1.00	Set	1,775,000.00	1,775,000.00
2 PM Standard : Standard Support	1.00	Set	0.00	0.00
3 AC2050 : nShield Connect Rack Mounting Rails	1.00	Set	0.00	0.00
4 M-030099-L ; nShield Connect Keyboard	1.00	Set	0.00	0.00
5 AC3381LRemote : Admin Ready Cards v2.0 - Pack of 5	1.00	Set	0.00	0.00
6 PM Standard : Standard Support	1.00	Set	0.00	0.00
7 OP3176-WSOP-E : Web Services Option Pack	1.00	Set	0.00	0.00
8 SW2068C-W-E : Security World s/w for Windows	1.00	Set	0.00	0.00
✂️ Software : Entrust CSP				
9 SUB-CSP-KM-STD : Entrust CSP Standard -Key Control on Premise - Subscription License	1.00	Set	1,308,000.00	1,308,000.00
10 SUB-CSP-PKIH-STD : Entrust CSP Standard -PKI HUB Appliance CA - On Premise Subscription License	1.00	Set	0.00	0.00
11 SUB-PKIH-CERTSE : ntrust PKI Hub Production Certificates	50.00	Set	0.00	0.00
12 Platinum Support(22%) : Support based on quantities above	1.00	Set	0.00	0.00
13 PS-CSP-BASE-X : Deployment of Base CSP Compliance Manager Appliance - Professional Services	1.00	Set	0.00	0.00

**SECURE SERVE CO.LTD.**1/18 Soi Ramintra 14 Yak 11/1,Tharaeng Bangkhen  
Bangkok 10220 Thailand

เลขที่ประจำตัวผู้เสียภาษี : 0105554065634

โทรศัพท์ : 02-170-6104-5 E-mail : info@secureserve.co.th

QUOTATION

**ผู้ซื้อ**สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี  
เลขที่ 924 ถนนสุขุมวิท แขวงพระโขนง เขตคลองเตย กรุงเทพฯ 10110**ใบเสนอราคา**

เลขที่	Q#250717-0010-C
วันที่	12 มี.ค. 2569
วันที่ยื่นราคา	13 มี.ย. 2569
รวมเป็นเงิน	3,083,000.00
VAT 7 %	215,810.00
จำนวนเงินรวมก่อน VAT	3,083,000.00
<hr/>	
จำนวนเงินรวมทั้งหมด THB	3,298,810.00
(สามล้านสองแสนเก้าหมื่นแปดพันแปดร้อยสิบบาทถ้วน)	

## รายละเอียดการชำระเงิน

## หมายเหตุ

- ยื่นราคา 90 วัน
- กำหนดส่งมอบงาน 120 วัน

ผู้เสนอราคา	ผู้อนุมัติใบเสนอราคา	ผู้ยืนยันการสั่งซื้อ
 Manop Keamapiruck 11 มี.ค. 2569	 Supatthan Petyoi 11 มี.ค. 2569	..... / /

Netcare Solutions Co.,Ltd. 160/232-3 ITF Silom Palace Building, 14th Fl., Silom Rd.,

Quotation No. : NCS\_26PC80117

Suriyawong, Bangrak, Bangkok 10500 Tel :0-2634-0422-23 Fax : 02-234-5297

Contract : The Institute for the Promotion of Teaching Science and Technology

Date: 11 มีนาคม พ.ศ.2569

475 Siriphinyo Building, 9th Floor, Sri Ayutthaya Road, Phaya Thai Subdistrict, Ratchathewi District, Bangkok 10400

บริษัท NetCare Solutions มีความยินดีขอเสนอราคา เพื่อโปรดพิจารณา ดังนี้ :

รายการ Item	Description	จำนวน Quantity	หน่วย Unit	จำนวน Unit Price	ราคารวม Total Amount
	<b>Appliance Entrust HSM</b>	1	system	1,855,000.00	1,855,000.00
1	NH2096-B : nShield 5c Base	1	ea.		
2	PM Standard : Standard Support	1	ea.		
3	AC2050 : nShield Connect Rack Mounting Rails	1	ea.		
4	M-030099-L ; nShield Connect Keyboard	1	ea.		
5	SW2068C-W-E : Security World s/w for Windows	1	ea.		
6	OP3176-WSOP-E : Web Services Option Pack	1	ea.		
7	AC3381LRemote : Admin Ready Cards v2.0 - Pack of 5	1	ea.		
8	PM Standard : Standard Support	1	ea.		
	<b>Software : Entrust CSP</b>	1	system	1,326,000.00	1,326,000.00
9	SUB-CSP-KM-STD : Entrust CSP Standard -Key Control on Premise - Subscription License	1	ea.		
		1	ea.		
10	SUB-CSP-PKIH-STD : Entrust CSP Standard -PKI HUB Appliance CA - On Premise Subscription License	1	ea.		
11	SUB-PKIH-CERTSE : ntrust PKI Hub Production Certificates	50	ea.		
12	PS-CSP-BASE-X : Deployment of Base CSP Compliance Manager Appliance - Professional Services	1	ea.		
13	Platinum Support (22%) : Support based on quantities above	1	ea.		

เงื่อนไขการเสนอราคา/conditions :

- 1 การชำระเงิน/Payment Term : 30 Days after sign Invoice
- 2 กำหนดยืนราคา/Price Validity : 90 Days
- 3 กำหนดส่งมอบ/Delivery Date : 120 Days

**Total** 3,181,000.00

**Vat 7%** 222,670.00

**Grand Total** 3,403,670.00

ลายมือชื่อผู้มีอำนาจลงนามพร้อมประทับตราสำคัญ

Authorized Signature with co's Seal



ผู้เสนอราคา/By

ลงชื่อ/Signature



คุณประเสริฐ เจริญบงกชกร

# ETERNITY Quote / ใบเสนอราคา :

No.E260162 - The Institute for the Promotion of Teaching Science and Technology



ETERNITY

Sales Person : Ms.Naratachadha Wongaphiphan  
Email: naratachadha.wo@eterthailand.com M: 080-518-8789

**Billing Address** : สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี  
**Shipping Address** : 924 ถนนสุขุมวิท แขวงพระโขนง เขตคลองเตย กรุงเทพฯ 10110  
**Contact Person** : K. Pakorn Kulsapakorn (pkuls@ipst.ac.th)

**Payment Term** : 30 Days  
**Delivery Date** : 120 Days  
**Page no.** : 1 of 1  
**Quote Date** : 12-Mar-2026

Thank you for the opportunity to provide you with the following quotation

## Price Summary :

Description:	Qty:	Unit Price Ex VAT:	Total Price:
<b>1</b> <b>Appliance : Entrust HSM</b> NH2096-B : nShield 5c Base PM Standard : Standard Support AC2050 : nShield Connect Rack Mounting Rails M-030099-L ; nShield Connect Keyboard AC3381LRemote : Admin Ready Cards v2.0 - Pack of 5 PM Standard : Standard Support OP3176-WSOP-E : Web Services Option Pack SW2068C-W-E : Security World s/w for Windows	1 1 1 1 1 1 1 1	1,810,000.00	1,810,000.00
<b>2</b> <b>Software : Entrust CSP</b> SUB-CSP-KM-STD : Entrust CSP Standard -Key Control on Premise - Subscription License SUB-CSP-PKIH-STD : Entrust CSP Standard -PKI HUB Appliance CA - On Premise Subscription License SUB-PKIH-CERTSE : ntrust PKI Hub Production Certificates Platinum Support (22%) : Support based on quantities above PS-CSP-BASE-X : Deployment of Base CSP Compliance Manager Appliance - Professional Services	1 1 1 50 1 1	1,350,000.00	1,350,000.00
จำนวนเงินรวมก่อน VAT			3,160,000.00
VAT 7 %			221,200.00
รวมเป็นเงินทั้งสิ้น			3,381,200.00


### Payment Information:

\*\* ส่งจ่ายโอนนาม บริษัท อีเทอริตี้ จำกัด ธนาคารทหารไทยธนชาติ จำกัด (มหาชน) บัญชีเลขที่ 029-2-74069-3 สาขาปากเกร็ด

If this quote meets with your approval please contact me to discuss placing an order. We hope the above offer will serve your requirement and we look forward to your kind

**Remarks:** มีราคาเป็นเวลา 90 วัน

สามล้านสามแสนแปดหมื่นหนึ่งพันสองร้อยบาทถ้วน

  
(Ms.Naratachadha Wongaphiphan)  
Date : \_\_\_/\_\_\_/\_\_\_

Eternity Authorized Signature (Chop & Sign) :

We agree and accept to order as in this quotation.

Date : \_\_\_/\_\_\_/\_\_\_

Customer Authorized Signature (Chop & Sign) :

Eternity Company Limited.

99/306, M.4, Bangpleeyai, Banglee, Samutprakarn 10540 Tel : +662 171-9063 Fax : +662 171-9202 Tax ID : 0115556016690

รายชื่อคณะกรรมการ  
งานจัดซื้ออุปกรณ์เข้ารหัสฐานข้อมูล (Database Encryption)

คณะกรรมการพิจารณางานจัดซื้อจัดจ้าง

- |                  |                |               |
|------------------|----------------|---------------|
| 1. นายภากร       | กุลศุภกร       | ประธานกรรมการ |
| 2. นายนवल        | กาบแก้ว        | กรรมการ       |
| 3. นางสาวอภิวรรณ | วิรัชสกุลทิพย์ | กรรมการ       |

รายชื่อคณะกรรมการตรวจรับ

- |                    |              |               |
|--------------------|--------------|---------------|
| 1. นายพีรพัฒน์     | ผิวผา        | ประธานกรรมการ |
| 2. นายสุประดิษฐ์   | รุ่งศรี      | กรรมการ       |
| 3. นางสาวรัฐานันท์ | พันทวีศักดิ์ | กรรมการ       |

