รายละเอียดขอบเขตงาน จ้างบำรุงรักษาระบบบริหารจัดการบริการเทคโนโลยีสารสนเทศ (IT Service Management (ITSM)) ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

1. หลักการและเหตุผล

ฝ่ายเทคโนโลยีสารสนเทศ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) มีหน้าที่ดูแลระบบเทคโนโลยีสารสนเทศที่ครอบคลุมทั้งระบบงาน (Application System) เครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย (Network) เพื่อให้บริการภายในและภายนอกหน่วยงานอย่างมีประสิทธิภาพและต่อเนื่อง จึงจำเป็นต้องดำเนินการบริหารจัดการและบำรุงรักษาเชิงรุก ตามแนวทาง IT Service Management (ITSM) โดยอิงมาตรฐาน ITIL, ISO/IEC 20000 และ ISO/IEC 27001 รวมถึงข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์และกฎหมายที่เกี่ยวข้อง โดยผู้เชี่ยวชาญเฉพาะด้านจากภายนอก ภายใต้การกำกับดูแลของฝ่ายเทคโนโลยีสารสนเทศ สสวท. เพื่อให้มั่นใจว่าระบบโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล สามารถรองรับการใช้งานได้อย่างมั่นคง ปลอดภัย และสอดคล้องกับนโยบายของหน่วยงาน

2. วัตถุประสงค์

เพื่อบริหารจัดการและบำรุงรักษาระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัลของ สสวท. อย่างมีประสิทธิภาพและต่อเนื่อง และดำเนินงานเป็นไปตามแนวทาง ITSM และมาตรฐานสากล ได้แก่ ITIL, ISO/IEC 20000, ISO/IEC 27001 รวมถึงข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ นโยบายคุ้มครองข้อมูลส่วนบุคคล และนโยบายความมั่นคงปลอดภัยสารสนเทศของ สสวท. และเพื่อสร้างความเชื่อมั่นของระบบ IT ภายในองค์กร ลดความเสี่ยงจากการหยุดชะงักของระบบ สามารถป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

3. คุณสมบัติของผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการ ผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

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 ผู้ยื่นข้อเสนอต้องมีผลงานประเภทเดียวกันกับงานรับจ้างในครั้งนี้ จำนวนไม่น้อยกว่า 1 ผลงาน วงเงินไม่น้อยกว่า 1,000,000 บาท (หนึ่งล้านบาทถ้วน) ในระยะเวลาไม่เกิน 2 ปี นับถัดจากวันสิ้นสุดภาระผูกพันตามสัญญา จนถึงวันที่ยื่นข้อเสนอ และเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ หรือหน่วยงานเอกชนที่สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) เชื่อถือ โดยยื่นสำเนาหนังสือรับรองผลงานและสำเนาสัญญาหรือใบสั่งซื้อ ซึ่งเป็นงานเดียวกัน

4. คุณสมบัติเฉพาะของผู้ยื่นข้อเสนอ

4.1 เป็นผู้มีประสบการณ์ในการบำรุงรักษาและบริหารโครงการด้านเทคโนโลยีสารสนเทศและการสื่อสาร มีความรู้ความสามารถในระบบสารสนเทศและการสื่อสาร สามารถให้คำปรึกษา แนะนำ ตรวจสอบประสานงาน และวิเคราะห์ปัญหา พร้อมเสนอแนวทางแก้ไขที่เกี่ยวข้องกับระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ซึ่งเป็นโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล

4.2 ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองจากทาง Microsoft ในการรับรองถึงการมีประสิทธิภาพในการให้บริการ (Solutions Partner Designations) ในด้าน Infrastructure (Azure) และ/หรือ Modern Work

4.3 ผู้ยื่นข้อเสนอต้องมีคณะผู้เชี่ยวชาญเฉพาะด้าน เพื่อปฏิบัติงานสนับสนุนต่างๆ (Back Office) อย่างน้อย 7 คน ที่มีประสบการณ์ทำงานในการบริหารจัดการระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ซึ่งเป็นโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ที่เกี่ยวข้องกับภาคผนวก 1 โดยมีหนังสือรับรองการทำงานและมีประกาศนียบัตรที่ยังไม่หมดอายุ ณ วันที่ยื่นข้อเสนอ ดังต่อไปนี้

1) Cisco Certified Network Associate (CCNA) หรือ Cisco Certified Network Professional (CCNP) อย่างน้อย 1 คน
2) Microsoft Certified Solutions Expert Cloud Platform and Infrastructure หรือ Microsoft Certified: Azure Solutions Architect Expert อย่างน้อย 1 คน
3) Microsoft Certified Solutions Expert Productivity หรือ Microsoft 365 Certified: Administrator Expert อย่างน้อย 1 คน
4) Microsoft 365 Certified: Security Administrator Associate หรือ Microsoft Certified: Security Operations Analyst Associate อย่างน้อย 1 คน
5) Microsoft Certified Cybersecurity Architect Expert อย่างน้อย 1 คน
6) Microsoft Certified Solutions Associate: SQL Server certification หรือ Microsoft Certified: Azure Database Administrator Associate อย่างน้อย 1 คน
7) Microsoft Certified: Power BI Data Analyst Associate อย่างน้อย 1 คน
8) Oracle Database Administrator Certification อย่างน้อย 1 คน
9) CompTIA Linux+ หรือ Red Hat Certified Engineer (RHCE) หรือ LINUX and GNU Certified Engineer (LCE) อย่างน้อย 1 คน
10) ITIL Expert Certification in IT Service Management หรือ ITIL Managing Professional (MP) อย่างน้อย 1 คน
11) Certified Project Management Professional (PMP) อย่างน้อย 1 คน

4.4 ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความเชี่ยวชาญ ด้านความมั่นคงปลอดภัยไซเบอร์ โดยต้องได้รับประกาศนียบัตร เช่น CompTIA Security+ หรือ Certified Information Systems Security Professional (CISSP) อย่างน้อย 1 คน เพื่อให้คำแนะนำทางด้านความมั่นคงปลอดภัยไซเบอร์

4.5 ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความเชี่ยวชาญ ด้านโครงสร้างพื้นฐานของ Cloud Computing โดยต้องได้รับประกาศนียบัตร เช่น Huawei Certified ICT Professional หรือ AWS Certified Solutions Architect – Associate อย่างน้อย 1 คน เพื่อให้คำแนะนำในการติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย การบริหารจัดการทรัพยากร การตั้งค่าด้านความปลอดภัย และการสำรองข้อมูล บน Cloud

4.6 ผู้ยื่นข้อเสนอต้องมีผู้เชียวชาญอย่างน้อย 1 คน และมีประสบการณ์อย่างน้อย 3 ปี ในการติดตั้งและบริหารจัดการ Linux Distribution เช่น Ubuntu, CentOS, Redhat ได้

4.7 ผู้ยื่นข้อเสนอต้องมีผู้เชียวชาญอย่างน้อย 1 คน และมีประสบการณ์อย่างน้อย 3 ปี ในการติดตั้งและบริหารจัดการระบบ Virtualization ของ VMware

4.8 ผู้ยื่นข้อเสนอต้องมีบุคลากรที่มีความเชี่ยวชาญ ด้านการบริหารความต่อเนื่องทางธุรกิจ BCM (Business Continuity Management) อย่างน้อย 1 คน

4.9 ผู้ยื่นข้อเสนอต้องเป็นผู้ได้รับการรับรองมาตรฐาน ISO/IEC 20000 และ ISO/IEC 27001เพื่อการบริการที่มีคุณภาพและปลอดภัย

4.10 ผู้ยื่นข้อเสนอต้องจัดให้มีเจ้าหน้าที่ปฏิบัติงานประจำ ณ สสวท. จำนวน 2 คน โดยมีวุฒิการศึกษาขั้นต่ำระดับปริญญาตรี ในสาขาคอมพิวเตอร์ เทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง และมีประสบการณ์ด้านการดูแลระบบคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย ไม่น้อยกว่า 3 ปี โดยแบ่งเป็น

4.10.1 เจ้าหน้าที่ด้านระบบโครงสร้างพื้นฐาน จำนวน 1 คน ต้องมีความรู้ความสามารถในหัวข้อดังต่อไปนี้

1) เจ้าหน้าที่ด้านระบบโครงสร้างพื้นฐาน (Infrastructure System)

- ระบบสำรองข้อมูล (Backup/Restore, Replication, High Availability - HA)
- ระบบปฏิบัติการ Windows Server (ตั้งแต่เวอร์ชัน 2012 R2 ถึง 2022)
- ระบบ Active Directory / LDAP
- ระบบ DHCP (IPv4/IPv6)
- ระบบ DNS (IPv4/IPv6)
- ระบบจดหมายอิเล็กทรอนิกส์ Microsoft Exchange Server 2019 และ Microsoft Office 365 (Email Service)
- ระบบรักษาความปลอดภัย Trend Micro (Enterprise Security Suite)
- ระบบ Mail Security (IMSVA Version 9)
- ระบบ File Server Resource Manager (บน Windows Server 2022)
- ระบบฐานข้อมูลส่วนกลาง เช่น Microsoft SQL Server

- ระบบ Web Server เช่น IIS, Apache, หรือ NginX

2) ด้าน Microsoft 365

- ระบบ AD Sync เช่น Microsoft Entra Connect
- การบริหารจัดการระบบ Microsoft Office 365
- การใช้งาน Microsoft Enterprise Mobility + Security (EMS)

3) ด้านระบบ Linux Server

- รองรับ Linux Distributions ได้แก่ Ubuntu, CentOS และ Red Hat
- การจัดการระบบ Security Patch
- การใช้งาน Docker และการบริหารจัดการ Containers

4.10.2 เจ้าหน้าที่ด้านระบบเครือข่าย จำนวน 1 คน ต้องมีความรู้ความสามารถดังต่อไปนี้

- ระบบ DHCP (IPv4/IPv6)
- ระบบ DNS (IPv4/IPv6)
- ระบบ Wireless และโครงสร้างพื้นฐานเครือข่าย (LAN/WAN)
- ระบบ RADIUS Server
- การบริหารจัดการ Network & Internet Security
- ระบบ Wireless Security
- การใช้งานและบริหารระบบ Network Monitoring Tools
- การใช้งาน Endpoint Security Solution

5. ขอบเขตการดำเนินงาน

ผู้ยื่นข้อเสนอต้องสามารถให้คำปรึกษา แนะนำ สนับสนุน และประสานงานในการตรวจสอบ วิเคราะห์ และแก้ไขปัญหาที่เกิดขึ้นกับระบบเครือข่ายและเครื่องแม่ข่าย ซึ่งเป็นโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล เพื่อให้ระบบสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ทั้งนี้ ต้องดำเนินงานภายใต้แนวทางของ IT Service Management (ITSM) ตามกรอบมาตรฐาน ITIL โดยเฉพาะกระบวนการ Incident Management, Problem Management, Change Management และ Configuration Management และเป็นไปตามมาตรฐาน ISO/IEC 20000 และ ISO/IEC 27001 รวมถึงต้องปฏิบัติตามประกาศและแนวทางที่เกี่ยวข้องกับ การรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเสริมสร้างความน่าเชื่อถือ ลดความเสี่ยง และป้องกันเหตุการณ์ด้านความปลอดภัยที่อาจส่งผลกระทบต่อการให้บริการ

5.1. ผู้ยื่นข้อเสนอต้องเสนอแผนการดำเนินงานบำรุงรักษาระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามเอกสารภาคผนวก 1 โดยมีหัวข้ออย่างน้อยต่อไปนี้

1) โครงสร้างของคณะทำงานของผู้ยื่นข้อเสนอ ระบุชื่อ นามสกุล รูปถ่าย หนังสือรับรองการทำงาน และคุณสมบัติ

2) แผนการดำเนินงาน ในการจัดทำหรือปรับปรุง Access Control ด้าน Account Management ตามนโยบายด้านความปลอดภัยของ สสวท. และ มาตรฐานสากล

3) แผนการสำรองและกู้คืน ระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล

4) ระบบ Call Center ที่สามารถติดต่อได้ 24 ชั่วโมง พร้อมรายชื่อบุคลากร ตำแหน่ง e-mail หมายเลขโทรศัพท์และที่ตั้งที่สามารถติดต่อได้

5) แผนการถ่ายโอน (Transition Plan) ในการถ่ายโอนงานจาก สสวท. หรือ จากผู้รับจ้างเดิม การถ่ายทอดความรู้ (Solution and Knowledge Transfer) แก่ บุคลากร สสวท. โดยผู้มีความรู้ความชำนาญในงานที่จ้างเกี่ยวกับการตรวจสอบ การตรวจซ่อม การบำรุงรักษา และการ configuration ตามภาคผนวก 1 โดยการฝึกอบรมในขณะปฏิบัติงาน เอกสารคู่มือขั้นตอนการ ปฏิบัติงาน (Procedure) วิธีการปฏิบัติงาน (Work Instruction) คู่มือการทำงาน (Manual) ระเบียบปฏิบัติที่เกี่ยวข้องกับการทำงาน (Rules & Regulation)

5.2. ดำเนินการประชุมก่อนการดำเนินการ (Kick off Meeting) เพื่อนำเสนอแผนการดำเนินงานตลอดสัญญา แผนการทำงานตามขอบเขตการดำเนินงานต่างๆ งานที่ต้องส่งในการประชุมแต่ละเดือน การตรวจรับแต่ละงวดงานและกำหนดเวลาในการดำเนินการต่างๆ

5.3. เจ้าหน้าที่ (Front Office) 2 คน ประจำ ณ สสวท. ระหว่างเวลา 8.00 - 17.00 น. ทุกวัน (ยกเว้นวันหยุดราชการตามประกาศของ สสวท.) โดยปฏิบัติงานประจำวัน ดังต่อไปนี้

1) ต้องตรวจสอบสถานะการทำงานเบื้องต้นและสถานะ Log ของระบบตามภาคผนวก 1

2) ต้องตรวจสถานะการเชื่อมต่อ VPN ระบบสารสนเทศและเว็บไซต์ ตามที่ สสวท. กำหนด จากเครือข่ายภายนอก สสวท. เช่น 4G/5G อย่างน้อย 2 ครั้ง ต่อวัน (09:00 น. และ 13:00 น.)

3) บริหารจัดการระบบ Monitoring ระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ที่ สสวท. ใช้งาน ด้วยโปรแกรมที่ผู้รับจ้างจัดหามาไว้เพื่อสนับสนุนการบริหารจัดการ

4) ตรวจสอบสถานะการ จัดส่ง/รับจดหมายอิเล็กทรอนิกส์ไปยังระบบจดหมายอิเล็กทรอนิกส์ ทั้งจากภายนอกและภายใน อย่างน้อย 3 ครั้ง ต่อวัน (09:00 น. 13:00 น. และ 16:00 น.)

5) ตรวจสอบและรายงานผล การทำงานของระบบ Endpoint Antivirus Solutions

6) ตรวจสอบการแจ้งเตือนภัยคุกคามจาก ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (SOC) และทำการป้องกันภัยคุกคามต่างๆ ตามที่ได้รับแจ้ง รวมถึงรายงานผลการป้องกันให้ สสวท. รับทราบ

7) ในกรณีที่เป็นการแก้ไขปัญหาต่อเนื่องและมีความจำเป็น ต้องสามารถปฏิบัติงานนอกเวลาทำการได้เป็นครั้งคราว โดยไม่มีค่าใช้จ่ายใดๆ เพิ่มเติม

8) ในกรณีนอกเวลาทำการ จะต้องสามารถให้บริการแบบ On-call หรือ On-site ได้ โดยการปฏิบัติงานนอกเวลาทำการ สสวท. ไม่เกิน 12 วัน เช่น เมื่อเกิดเหตุฉุกเฉินระดับวิกฤต อันส่งผลต่อการให้บริการของระบบโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล หรือ เมื่อมีการบำรุงรักษาระบบต่างๆ เช่น ระบบไฟฟ้า ระบบไฟฟ้าสำรอง ระบบเครื่องปรับอากาศ ของ สสวท. หรือ อาคารสิริภิญโญ ซึ่งอาจจะส่งผลต่อการให้บริการของระบบต่างๆ จะต้องเข้าปฏิบัติงานที่อาคารสิริภิญโญได้ทันที

5.4. ต้องดำเนินการตรวจสอบระบบที่เกี่ยวข้องและทำรายงานสรุป ส่ง สสวท. เดือนละ 1 ครั้ง ดังนี้

1) Active Directory: ทำการตรวจสอบรายการคอมพิวเตอร์และรายการบัญชีผู้ใช้งาน ที่ไม่มีการใช้งานเกิน 30 วัน (หรือตามที่ สสวท. กำหนด) เพื่อพิจารณาและผู้รับจ้างดำเนินการ ลบ (Delete) หรือ ปิด (Disable) ผู้ใช้งาน ตามคำแนะนำของผู้รับจ้างที่ผ่านความเห็นชอบจาก สสวท. หรือตามที่ สสวท. กำหนด

2) File Server: ทำการตรวจสอบสิทธิ์ของผู้ใช้งานบน Shared Folder และปริมาณการใช้งาน File Server เพื่อให้เจ้าของสิทธิ์ในแต่ละ Folder ทำการตรวจสอบการใช้งานต่างๆ ว่าถูกต้องหรือไม่

3) Mail Server: ตรวจสอบ Blacklist Server ไม่น้อยกว่า 80 ฐานข้อมูล โดยจะต้องตรวจสอบ IP Blacklist และแจ้งเตือนทันทีที่ IP ถูก Blacklist โดยต้องรายงานเมื่อ IP ติด Blacklist และเมื่อ IP กลับสู่สถานะปกติ (Delist) และ ทำการตรวจสอบบัญชีผู้ใช้งาน Mailbox ที่ไม่มีการใช้งานเกิน 30 วัน หรือตามที่ สสวท. กำหนด

4) Network: ตรวจสอบอุปกรณ์เครือข่าย รวมถึง Port ที่ไม่ได้ถูกใช้งาน เพื่อให้ สสวท. พิจารณาและผู้รับจ้างดำเนินการ ปิด (Disable) Port ตามข้อเสนอแนะของผู้รับจ้างที่ผ่านความเห็นชอบจาก สสวท. หรือตามที่ สสวท. กำหนด

5) Centralize Log: ตรวจสอบระบบบริหารจัดการข้อมูล Log File แบบศูนย์กลาง ให้สามารถจัดเก็บ Log ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ฉบับที่ 2)

6) Patch Management Lifecycle: บริหารจัดการ Patch และช่องโหว่แบบเป็นระบบ เพื่อให้มีการอัปเดตอย่างสม่ำเสมอ

5.5. การจัดการฐานข้อมูล (Database Management) ต้องบริหารจัดการระบบฐานข้อมูลส่วนกลาง ดังนี้

1) ดำเนินการตรวจสอบการทำงานของเครื่องแม่ข่าย Oracle Database 10g, Oracle Database 12c และ MS SQL ทุก Version ที่ สสวท. ใช้งาน ให้สามารถให้บริการได้

2) ตรวจสอบการทำงานโดยรวมของระบบการจัดการฐานข้อมูลของคลังข้อมูล ได้แก่ การใช้งาน Disk, Index, Statistics และ Session ต่างๆ

3) ปรับแต่งประสิทธิภาพ (Tuning)

4) ประสานงานการแก้ไขปัญหาที่เกี่ยวข้องกับระบบจัดการฐานข้อมูล

5.6. ผู้รับจ้างต้องดำเนินการจัดเก็บและบริหารจัดการข้อมูลของระบบเครือข่าย และเครื่องแม่ข่าย คอมพิวเตอร์ ซึ่งเป็นส่วนหนึ่งของโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ให้เป็นไปตามแนวทาง การบริหารจัดการทรัพย์สิน IT (IT Asset Management – ITAM) ภายใต้แนวปฏิบัติของ ITIL Framework โดย ดำเนินการจัดทำรายงานสถานะของระบบสารสนเทศที่มีอยู่ในปัจจุบัน (Existing Report) อย่างน้อย 2 ครั้ง (เดือนที่ 3 และเดือนที่ 11) นับถัดจากวันที่ได้รับหนังสือแจ้งให้เริ่มงาน

5.7. ต้องสามารถบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย ที่ใช้ระบบปฏิบัติการ Linux โดยสามารถ

1) Update Patch หรือ Upgrade OS ได้

2) การสำรองและกู้คืนข้อมูลระบบ

3) วางแผนการทำ Disaster Recovery ตามที่ สสวท. กำหนด

4) การให้คำแนะนำในการบริหารจัดการระบบ Docker Containers

5.8. กู้คืนระบบต่างๆ เมื่อเกิดปัญหาเกิดขึ้น ตามมาตรฐาน ITIL Service Support โดยดำเนินการดังต่อไปนี้

1) รับทราบปัญหาเหตุขัดข้องทางระบบแจ้งเตือน หรือ สสวท. แจ้งเหตุขัดข้อง

2) วิเคราะห์หาสาเหตุของปัญหาที่แท้จริงและแนวทางการกู้ระบบให้ใช้งานได้ตามปกติ และจัดทำรายงานสรุปการแก้ไขปัญหาที่เกิดขึ้น (Incident Report)

3) ดำเนินการกู้คืนให้ระบบสามารถใช้งานได้ตามปกติ หากระบบดังกล่าวเสียหายไม่สามารถกู้คืนได้ จะต้องติดตั้งระบบใหม่ให้ใช้งานได้ดังเดิม

4) ในกรณีที่มีปัญหา ไม่สามารถแก้ไขได้โดยเจ้าหน้าที่ (Front Office) ผู้รับจ้างจะต้องให้ผู้เชี่ยวชาญ ดำเนินการตรวจสอบ ให้คำแนะนำและแก้ไขระบบที่ขัดข้องให้แล้วเสร็จตาม Service Level Agreement (SLA)

5) ในกรณีปัญหาเกิดจากการชำรุดของเครื่องคอมพิวเตอร์แม่ข่าย, อุปกรณ์เครือข่าย, ระบบเครือข่ายที่ให้บริการ สสวท. จะจัดหาและแจ้งไปยังผู้รับจ้างอีกครั้งว่าได้จัดหาให้เรียบร้อยแล้ว และผู้รับจ้างดำเนินการกู้คืนระบบที่ขัดข้องให้แล้วเสร็จตาม Service Level Agreement (SLA) โดยจะเริ่มต้นนับเวลาใหม่ หรือขยายเวลา ให้ตามที่ สสวท. เห็นชอบ

หมายเหตุ ระยะเวลาการแจ้งเหตุขัดข้องและการนับเวลา SLA

การแจ้งเหตุขัดข้องสามารถดำเนินการได้ตลอดเวลา ผ่านอีเมล โทรศัพท์ หรือระบบแจ้งเตือนที่ สสวท. ตกลงไว้กับผู้รับจ้าง อย่างไรก็ตาม การนับเวลาเพื่อกำหนด SLA จะเริ่มต้นในช่วงวันจันทร์–เสาร์ เวลา 08.00–16.30 น. เท่านั้น ตัวอย่าง: หากมีการแจ้งเหตุขัดข้องในวันเสาร์ เวลา 18.00 น. จะเริ่มนับเวลา SLA ตั้งแต่วันจันทร์ เวลา 08.00 น.

6) ในกรณีที่เป็นการแก้ไขปัญหาต่อเนื่อง ต้องสามารถปฏิบัติงานนอกเวลาทำการได้ โดยไม่มีค่าใช้จ่ายใดๆ เพิ่มเติม

5.9. การกู้คืนระบบต่างๆ ตามภาคผนวก 1 ต้องดำเนินงานอย่างน้อยดังนี้

1) จัดทำแผนปฏิบัติงานสำรองและกู้คืน ที่ได้รับการตรวจสอบและรับรองจากผู้เชี่ยวชาญ

2) จัดทำคู่มือสำรองและกู้คืน และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

3) ร่วมกับผู้พัฒนาระบบงานสารสนเทศ (ระบบบริหารจัดการงาน MIS, ระบบบริหารงานบุคคล, ระบบงานสารบรรณ) เพื่อจัดทำแผนปฏิบัติงานกู้คืน ระบบงานและข้อมูล พร้อมทดสอบการกู้คืน อย่างน้อย 1 ครั้ง ตามที่ สสวท. กำหนด

4) ทดสอบการกู้คืนระบบจดหมายอิเล็กทรอนิกส์ และ ระบบจัดเก็บไฟล์สำหรับองค์กร (File Server) อย่างน้อย ระบบละ 2 ครั้ง โดย สสวท. เป็นผู้กำหนดช่วงเวลาดำเนินการทดสอบ (ภายในเดือนที่ 9) นับถัดจากวันที่ได้รับหนังสือแจ้งให้เริ่มงาน โดยต้องมีผู้เชี่ยวชาญด้านแผนบริหารความต่อเนื่องทางธุรกิจตรวจสอบและรับรอง ตลอดทุกขั้นตอนในการปฏิบัติงาน

5.10. บำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล อย่างน้อย 2 ครั้ง (เดือนที่ 6 และเดือนที่ 11) นับถัดจากวันที่ได้รับหนังสือแจ้งให้เริ่มงาน

5.11. ปรับแต่งประสิทธิภาพ (Tuning) ของระบบต่างๆ ตามเอกสารภาคผนวก 1 ให้มีประสิทธิภาพสามารถทำงานได้อย่างต่อเนื่อง รวมถึงการปฏิบัติตามมาตรฐานความปลอดภัยสารสนเทศ หรือ ตามที่ สสวท. กำหนด เช่น การเพิ่มความปลอดภัยให้ระบบจดหมายอิเล็กทรอนิกส์ ด้วยมาตรฐานสากล และ ระบบ Cloud ของ สสวท. ซึ่งรวมถึง Microsoft Office 365 และ Microsoft Azure

5.12. ตรวจสอบการทำงานของระบบบริการรับส่ง E-mail (Microsoft Exchange Server 2019) อย่างน้อยดังนี้

1) ตรวจสอบสุขภาพระบบ (Service Health) และประสิทธิภาพการทำงานของระบบ

2) ตรวจสอบ Message Queue และการทำงานของระบบ Mail Flow

3) ตรวจสอบ Audit Log และ Security Log เพื่อตรวจจับเหตุการณ์ผิดปกติ

5.13. ต้องดำเนินการจัดทำระบบเสมือนจริง ตามที่ สสวท. กำหนด เพื่อป้องกัน ผลกระทบจากภัยคุกคามทางไซเบอร์อย่างน้อย 2 กรณี (Case) และ จัดทำแนวปฏิบัติในการรับมือเหตุการณ์ดังกล่าว ตามที่ สสวท. กำหนด

5.14. ให้ผู้เชี่ยวชาญ ที่ผู้รับจ้างจัดหามาเป็นกรณีพิเศษ ในการดำเนินการจัดทำภาระงานอื่น ที่ไม่ได้กำหนดในขอบเขตงาน จำนวน 10 วัน โดย สสวท. จะแจ้งรายละเอียดเบื้องต้นของงานที่ต้องการ ปรับแต่งประสิทธิภาพ โดยหลังจากได้รับแจ้ง ผู้รับจ้างต้องดำเนินการจัดประชุมและนำเสนอกับ สสวท. เพื่อรายงานผลการวิเคราะห์และผลกระทบในการปรับปรุง เพื่อให้ทาง สสวท. พิจารณา ทั้งนี้ หาก สสวท. พิจารณา

เห็นชอบให้ดำเนินการดังกล่าว ผู้รับจ้างต้องติดตั้งและจัดทำให้ระบบที่เกี่ยวข้องทำงานได้ตามข้อตกลงนี้ โดย สสวท. จะเป็นผู้รับผิดชอบในการจัดหาเครื่องคอมพิวเตอร์แม่ข่าย ลิขสิทธิ์ซอฟต์แวร์เพิ่มเติมที่เกิดขึ้น

5.15. ให้คำแนะนำ ร่วมวิเคราะห์ และปรับปรุงกระบวนการทำงานที่เกี่ยวข้องกับระบบเครือข่าย เครื่องแม่ข่าย และระบบรักษาความปลอดภัยสารสนเทศ ซึ่งเป็นโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ให้สอดคล้องกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยของ สสวท. ตามภาคผนวก 2 (เช่น นโยบายการควบคุมการเข้าถึง การสำรองข้อมูล การเตรียมความพร้อมกรณีฉุกเฉิน เป็นต้น)

5.16. ในกรณีเกิดเหตุการณ์ที่สร้างความเสียหายแก่ ระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล เช่น การโจมตีทางไซเบอร์ (Cyber Attack) ที่อาจเกิดขึ้นกับระบบเครือข่ายและข้อมูลอิเล็กทรอนิกส์ จะต้องส่งผู้เชี่ยวชาญ ดำเนินการตรวจสอบ ให้คำแนะนำแก้ไขระบบ ให้กลับมาใช้งานตามปกติ รวมถึงช่วยวิเคราะห์หาสาเหตุของการบุกรุกและวิธีการป้องกันการเกิดซ้ำ

5.17. ร่วมตรวจสอบช่องโหว่ของระบบ (Vulnerability Assessment and Penetration Testing) โดยผู้เชี่ยวชาญ ซึ่ง สสวท. เป็นผู้จัดหา เพื่อประเมินความเสี่ยงด้วยการทดสอบเจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่างๆ โดยผู้รับจ้าง จะเป็นผู้ดำเนินการปิดช่องโหว่ ตามคำแนะนำของผู้เชี่ยวชาญ

5.18. การถ่ายทอดความรู้ (Solution and Knowledge Transfer) ผู้รับจ้างต้องถ่ายทอดองค์ความรู้ให้กับ สสวท. โดยผู้มีความรู้ความชำนาญในงานที่จ้างเกี่ยวกับการตรวจสอบ ตรวจซ่อม บำรุงรักษา และการ Configuration โดยมีรายละเอียดดังนี้

1) จัดประชุมเพื่อนำเสนอผลการดำเนินงาน ข้อคิดเห็น และข้อเสนอแนะต่อ สสวท.

2) ทุกการประชุมต้องมีหัวหน้าโครงการของผู้รับจ้างเข้าร่วม พร้อมผู้เชี่ยวชาญ (Back Office) ที่เกี่ยวข้องตามที่ สสวท. กำหนด

5.19. การถ่ายโอนงานจากผู้รับจ้างรายเดิม

1) จัดส่งแผนการถ่ายโอนงานล่วงหน้าไม่น้อยกว่า 5 วันทำการก่อนเริ่มสัญญา

2) จัดส่งผู้จัดการโครงการ ผู้เชี่ยวชาญ (Back Office) และเจ้าหน้าที่ (Front Office) เพื่อดำเนินการถ่ายโอนงานจากผู้รับจ้างรายเดิมภายในระยะเวลาดังกล่าว

5.20. การถ่ายโอนงานให้ผู้รับจ้างรายใหม่ ผู้รับจ้างต้องเตรียมเอกสารและดำเนินการถ่ายโอนงานให้รายใหม่ ดังนี้

1) สรุปรายละเอียดงาน กิจกรรม และหน้าที่ของเจ้าหน้าที่ (Front Office) และผู้เชี่ยวชาญ (Back Office) แยกตามรายวัน รายเดือน และรายไตรมาส พร้อมเอกสารส่งมอบตามงวดงาน

2) จัดทำรายงานสถานะระบบสารสนเทศ (Existing Report) และภาพรวมระบบเครือข่าย/เครื่องแม่ข่าย ณ วันสิ้นสุดสัญญา

3) ให้ความร่วมมือและคำแนะนำในกระบวนการถ่ายโอนงานอย่างน้อย 5 วันทำการ

5.21. ผู้ยื่นข้อเสนอต้องมีระบบหรือแอปพลิเคชันที่ใช้สนับสนุนการดำเนินงาน ดังนี้

1) ระบบบริหารจัดการบริการ IT (ITSM) และ CMDB ต้องรองรับมาตรฐาน ITIL เพื่อบริหารจัดการ IT Asset Management และ กระบวนการให้บริการ IT อย่างเป็นระบบ สามารถแจ้งขอรับบริการผ่าน Workflow ที่ติดตามการรับเรื่องและการแก้ไขปัญหาได้ (IT Incident Management) เช่น iTop

2) ระบบตรวจสอบประสิทธิภาพเครือข่ายและเซิร์ฟเวอร์ (Network & Server Monitoring) เพื่อใช้ตรวจสอบการทำงานของเครื่องแม่ข่ายจริง/เสมือน และอุปกรณ์โครงสร้างพื้นฐาน ของระบบตามภาคผนวก 1 พร้อมติดตามสถานะ ระบุและวิเคราะห์ปัญหา รวมถึงแจ้งเตือนผ่านอีเมลเมื่อเกิดเหตุขัดข้อง เช่น Zabbix

3) ระบบตรวจสอบช่องโหว่ของระบบเครือข่ายและระบบคอมพิวเตอร์ (Vulnerability Assessment Tools) โดยสามารถสแกนพอร์ต, ตรวจหา service ที่เปิดใช้งาน, ตรวจหาช่องโหว่เบื้องต้น และให้คำแนะนำในการอุดช่องโหว่ เช่น OpenVAS (Open Vulnerability Assessment System)

4) ระบบตรวจสอบประสิทธิภาพแอปพลิเคชันและเว็บไซต์ (Application Performance Monitoring) ให้บริการแบบ Cloud ทำงานตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์ (24x7) พร้อมส่งอีเมลแจ้งเตือนเมื่อระบบมีปัญหา เช่น https://www.site24x7.com/ หรือ https://uptimerobot.com/

5) ระบบตรวจสอบการรับส่งอีเมลและสถานะ IP ของ Email Server (Blacklist Monitor) ตรวจสอบ IP กับ DNS-based Blacklists อย่างน้อย 80 รายการ ตรวจทุกวัน พร้อมแจ้งเตือนทางอีเมลเมื่อพบว่า IP ถูก Blacklist และเมื่อกลับเข้าสู่สถานะปกติ (Delist) เช่น https://mxtoolbox.com/

5.22. บริหารจัดการติดตามควบคุมผู้รับจ้างรายอื่นที่มีสัญญาบำรุงรักษาอุปกรณ์/ระบบ กับ สสวท. เพื่อให้อุปกรณ์/ระบบในสัญญาทำงานได้ตามปกติ และตามนโยบายของ สสวท.

5.23. ผู้ยื่นข้อเสนอต้องจัดทำรายการวัสดุหรือครุภัณฑ์ที่ใช้ในงานจ้าง ซึ่งเป็นพัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างนี้ (ถ้ามี)

6. ระยะเวลาการดำเนินงาน 12 เดือน นับถัดจากวันที่ได้รับหนังสือแจ้งให้เริ่มงาน

7. วงเงินงบประมาณ 2,200,000 บาท (สองล้านสองแสนบาทถ้วน) (รวมภาษีมูลค่าเพิ่ม) ดังนี้

งบประมาณปี 2568 เป็นเงิน 550,000 บาท

งบประมาณปี 2569 เป็นเงิน 1,650,000 บาท

8. หลักเกณฑ์และสิทธิในการพิจารณาราคา ในการพิจารณาผลการยื่นข้อเสนอครั้งนี้ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จะพิจารณาตัดสิน โดยใช้หลักเกณฑ์ราคา เพียงอย่างเดียว และ การพิจารณาผู้ชนะการยื่นข้อเสนอ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) จะพิจารณาจากราคารวม (รวมภาษีมูลค่าเพิ่มแล้ว) ที่เสนอราคาต่ำสุด

9. เอกสารในโครงการ ผู้รับจ้างต้องจัดทำเอกสารและรายงานต่างๆ ดังนี้

9.1 รายงานการปฏิบัติงานประจำเดือน มีรายละเอียดดังนี้

1) บันทึกการปฏิบัติงานรายวัน ของเจ้าหน้าที่ (Front Office) ประจำ ณ สสวท.

2) บันทึกการปฏิบัติงานรายวัน ของผู้เชี่ยวชาญ (Back Office) (ถ้ามี)

3) สถิติและปริมาณการใช้งาน Storage ของเครื่อง File Server ทุกเครื่อง

4) รายการเครื่องคอมพิวเตอร์ รายการบัญชีผู้ใช้งาน รายการจดหมายอิเล็คทรอนิกส์ ที่ไม่ถูกใช้งานเกิน 30 วัน หรือตามที่ สสวท. กำหนด

5) การตรวจสอบการทำงานของระบบบริการรับส่ง E-mail

6) การสำรองข้อมูลและการกู้คืนข้อมูล (ถ้ามี)

7) การปฏิบัติตามเอกสารการแจ้งเตือนคำแนะนำ ในการป้องกันแก้ไขภัยคุกคามทางไซเบอร์ (ถ้ามี)

8) การปรับปรุงการตั้งค่าระบบ ตามนโยบายหรือ สสวท. กำหนด (ถ้ามี)

9) การบริหารจัดการติดตามควบคุมบริษัทที่มีสัญญาบำรุงรักษาระบบ/อุปกรณ์ เครื่องคอมพิวเตอร์แม่ข่าย กับ สสวท. (ถ้ามี)

10) การให้คำปรึกษา จัดการ/ดำเนินการปรับแต่งประสิทธิภาพ (Tuning) ระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล (ถ้ามี)

11) การวิเคราะห์การทำงานของระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีและการสื่อสาร สสวท. (ถ้ามี)

9.2 รายงานอื่นๆ ตามงวดงาน

9.2.1 แผนปฏิบัติงานสำรองและกู้คืนระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามภาคผนวก 1 ที่ได้รับการตรวจสอบและรับรองจากผู้เชี่ยวชาญ (2 ฉบับ)

9.2.2 รายงานสถานะของระบบสารสนเทศที่มีอยู่ในปัจจุบัน (Existing Report) (2 ฉบับ)

9.2.3 รายงานการบำรุงรักษาเชิงป้องกัน (2 ฉบับ)

9.2.4 รายงานการดำเนินการจัดทำระบบเสมือนจริงตามที่ สสวท. กำหนด จากภัยคุกคามทางไซเบอร์อย่างน้อย 2 กรณี

9.2.5 รายงานการวิเคราะห์และปรับแต่งประสิทธิภาพ (Tuning) ระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีและการสื่อสาร สสวท. (2 ฉบับ)

9.2.6 แผนปฏิบัติงานกู้คืนระบบงานและข้อมูลที่ สสวท. ได้มอบหมายให้สำรองระบบและข้อมูล (1 ฉบับ)

9.2.7 รายงานผลการทดสอบ การกู้คืนร่วมกับผู้พัฒนาระบบงาน ตามที่ สสวท. กำหนด ในข้อ 8.2.6 (1 ฉบับ)

9.2.8 คู่มือสำรองและกู้คืนระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามภาคผนวก 1 หรือ ตามที่ สสวท. กำหนด เช่น ระบบ Active Directory ระบบ Internet DNS Server Messaging และ ระบบ Wireless System ระบบ Network infrastructure (2 ฉบับ)

9.2.9 รายงานผลการทดสอบการกู้คืน ระบบจดหมายอิเล็กทรอนิกส์ และระบบ File Server 1 ฉบับ

9.2.10 คู่มือการถ่ายทอดความรู้ (Solution Transfer) 1 ฉบับ

10. การส่งมอบงานและการจ่ายเงิน จ่ายเงินจำนวนร้อยละ 25 ของวงเงินสัญญา จำนวน 4 งวด ดังนี้

งวดที่ 1 เมื่อผู้รับจ้างส่งแผนการดำเนินงานบำรุงรักษาระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามเอกสารภาคผนวก 1 ภายใน 5 วัน นับถัดจากวันลงนามในสัญญา และ บำรุงรักษา ตั้งแต่ เดือนที่ 1 – เดือนที่ 2 และส่งมอบรายงาน ตามข้อ 9.1 และ 9.2 รายงานอื่นๆ ตามงวดงาน และคณะกรรมการตรวจรับเรียบร้อยแล้ว ดังนี้

1) แผนปฏิบัติงานสำรองและกู้คืนระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามภาคผนวก 1 ที่ได้รับการตรวจสอบและรับรองจากผู้เชี่ยวชาญ (ฉบับที่ 1)

2) รายงานสถานะของระบบสารสนเทศที่มีอยู่ในปัจจุบัน (Existing Report) (ฉบับที่ 1)

3) แผนปฏิบัติงานกู้คืนระบบงานและข้อมูลที่ สสวท. ได้มอบหมายให้สำรองระบบและข้อมูล

4) รายการวัสดุหรือครุภัณฑ์ที่ใช้ในงานจ้าง ซึ่งเป็นพัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างนี้ (ถ้ามี)

โดยจัดส่งในรูปแบบเอกสารไฟล์อิเล็กทรอนิกส์ PDF จำนวน 1 ชุด

งวดที่ 2 เมื่อผู้รับจ้างบำรุงรักษา ตั้งแต่ เดือนที่ 3 – เดือนที่ 6 และส่งมอบรายงาน ตามข้อ 9.1 และ 9.2 รายงานอื่นๆ ตามงวดงาน และคณะกรรมการตรวจรับเรียบร้อยแล้ว ดังนี้

1) รายงานการบำรุงรักษาเชิงป้องกัน (ฉบับที่ 1)

2) รายงานการวิเคราะห์และปรับแต่งประสิทธิภาพ (Tuning) ระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีและการสื่อสาร สสวท. (ฉบับที่ 1)

3) คู่มือสำรองและกู้คืนระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามภาคผนวก 1 หรือ ตามที่ สสวท. กำหนด เช่น ระบบ Active Directoryระบบ Internet DNS Server Messaging และ ระบบ Wireless System ระบบ Network infrastructure (ฉบับที่ 1)

โดยจัดส่งในรูปแบบเอกสารไฟล์อิเล็กทรอนิกส์ PDF จำนวน 1 ชุด

งวดที่ 3 เมื่อผู้รับจ้างบำรุงรักษา ตั้งแต่ เดือนที่ 7 – เดือนที่ 9 และส่งมอบรายงาน ตามข้อ 9.1 และ 9.2 รายงานอื่นๆ ตามงวดงาน และคณะกรรมการตรวจรับเรียบร้อยแล้ว ดังนี้

1) แผนปฏิบัติงานสำรองและกู้คืนระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามภาคผนวก 1 ที่ได้รับการตรวจสอบและรับรองจากผู้เชี่ยวชาญ (ฉบับที่ 2)

2) รายงานผลการทดสอบ การกู้คืนร่วมกับผู้พัฒนาระบบงาน ตามที่ สสวท. กำหนด ในข้อ 9.2.6

3) รายงานผลการทดสอบการกู้คืน ระบบจดหมายอิเล็กทรอนิกส์ และระบบ File Server 1 ฉบับ

โดยจัดส่งในรูปแบบเอกสารไฟล์อิเล็กทรอนิกส์ PDF จำนวน 1 ชุด

งวดที่ 4 เมื่อผู้รับจ้างบำรุงรักษา ตั้งแต่ เดือนที่ 10 – เดือนที่ 12 และส่งมอบรายงาน ตามข้อ 9.1 และ 9.2 รายงานอื่นๆ ตามงวดงาน และคณะกรรมการตรวจรับเรียบร้อยแล้ว ดังนี้

1) รายงานการบำรุงรักษาเชิงป้องกัน (ฉบับที่ 2)

2) รายงานสถานะของระบบสารสนเทศที่มีอยู่ในปัจจุบัน (Existing Report) (ฉบับที่ 2)

3) รายงานการดำเนินการจัดทำระบบเสมือนจริงตามที่ สสวท. กำหนด จากภัยคุกคามทางไซเบอร์อย่างน้อย 2 กรณี

4) รายงานการวิเคราะห์และปรับแต่งประสิทธิภาพ (Tuning) ระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีและการสื่อสาร สสวท. (ฉบับที่ 2)

5) คู่มือสำรองและกู้คืนระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามภาคผนวก 1 หรือ ตามที่ สสวท. กำหนด เช่น ระบบ Active Directoryระบบ Internet DNS Server Messaging และ ระบบ Wireless System ระบบ Network infrastructure (ฉบับที่ 2)

6) คู่มือการถ่ายทอดความรู้ (Solution Transfer)

โดยจัดส่งในรูปแบบเอกสารไฟล์อิเล็กทรอนิกส์ PDF จำนวน 1 ชุด

11. การรับประกันผลงาน

ผู้รับจ้างตกลงบำรุงรักษาระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอ โดยให้มีเวลาระบบเครือข่ายและเครื่องแม่ข่ายขัดข้องรวมตามเกณฑ์การคำนวณเวลาขัดข้อง ไม่เกินเดือนละ 4 (สี่) ชั่วโมง หรือร้อยละ 0.55 (ศูนย์จุดห้าห้า) ของเวลาใช้งานทั้งหมดของคอมพิวเตอร์ของเดือนนั้น แล้วแต่ตัวเลขใดจะมากกว่ากัน มิฉะนั้นผู้รับจ้างต้องยอมให้ สสวท. คิดค่าปรับเป็นรายชั่วโมง ในอัตราร้อยละ 0.025 ของราคาตามสัญญาต่อชั่วโมงในช่วงเวลาที่ไม่สามารถใช้งานได้ในส่วนที่เกินกว่ากำหนดเวลาขัดข้องข้างต้น โดยเศษของชั่วโมงนับเป็น 1 ชั่วโมง

12. การให้บริการ

ในกรณีที่ผู้รับจ้างไม่เข้ามาซ่อมแซมแก้ไขภายในเวลาที่กำหนด หรือไม่สามารถดำเนินการซ่อมแซมแก้ไข ผู้รับจ้างยินยอมให้คิดค่าปรับเป็นรายชั่วโมง (เศษของชั่วโมงให้นับเป็น 1 (หนึ่ง) ชั่วโมง) ในอัตราร้อยละ 0.1 (ศูนย์จุดหนึ่ง) ของค่าจ้างบำรุงรักษา (รายงวด) ตามสัญญา นับจากเวลาที่ครบกำหนดจนถึงเวลาที่ผู้รับจ้างได้เริ่มการซ่อมแซมแก้ไข หรือจนถึงเวลาที่ผู้รับจ้างดำเนินการซ่อมแซมแก้ไขแล้ว เสร็จแล้วแต่กรณี ทั้งนี้ หากผู้รับจ้างไม่ดำเนินการดังกล่าว สสวท. มีสิทธิ์จ้างบุคคลภายนอกทำการซ่อมแซมแก้ไข โดยผู้รับจ้างจะต้องออกค่าใช้จ่ายในการจ้างบุคคลภายนอกซ่อมแซมแก้ไขแทน สสวท. ทั้งสิ้นการจ้างบริการบำรุงรักษาตามสัญญานี้

13. ความรับผิดของผู้รับจ้าง

กรณีผู้รับจ้างส่งมอบงานล่าช้ากว่าที่กำหนดในสัญญา หรือผู้รับจ้างไม่สามารถทำงานให้แล้วเสร็จตามเวลาที่กำหนดไว้ในสัญญา และสสวท. ยังไม่บอกเลิกสัญญา ผู้รับจ้างจะต้องชำระค่าปรับให้แก่ สสวท. เป็นรายวันในอัตราร้อยละ 0.10 ของราคาค่าจ้างตามสัญญา จนกว่าผู้รับจ้างจะส่งมอบงานให้แก่สสวท. ครบถ้วน

14. ข้อสงวนสิทธิ์

14.1 สสวท. สามารถขอเปลี่ยนแปลงบุคลากรหลัก ตามที่ระบุไว้ในข้อเสนอได้โดยไม่มีเงื่อนไข

14.2 ผู้รับจ้างไม่มีสิทธิ์เปลี่ยนแปลงบุคลากรหลัก ตลอดระยะเวลาดำเนินการโดยไม่ได้รับความเห็นชอบจาก สสวท.

14.3 ข้อมูลและเอกสารใดๆ ที่ สสวท. ได้รับทราบหรือได้รับจากหน่วยงานลูกค้าของ สสวท. และ/หรือ จาก สสวท. รวมทั้งผลงานที่ส่งมอบ ผู้ยื่นข้อเสนอต้องถือเป็นความลับ ไม่นำไปเผยแพร่ให้บุคคลใดทราบเป็นอันขาด เว้นแต่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจาก สสวท.

14.4 สสวท. ขอสงวนสิทธิ์ในการยกเลิกการจ่ายเงินทันที และ/หรือเรียกเงินคืน หากผู้ยื่นข้อเสนอไม่สามารถดำเนินการได้ตามข้อกำหนดและเงื่อนไข (TOR) ข้อหนึ่งข้อใดของสัญญาจ้างในโครงการนี้ โดยที่ผู้ยื่นข้อเสนอจะไม่ขอ

เรียกร้องสิทธิรวมทั้งค่าใช้จ่ายใดๆ จาก สสวท. ยกเว้นการไม่สามารถดำเนินการได้ดังกล่าวเป็นผลมาจากข้อจำกัดของ สสวท.

15. เงื่อนไขอื่นๆ สสวท. แบ่งสำนักงาน ออกเป็น 3 ที่ ดังนี้

15.1 สำนักงานหลัก อาคารสิริภิญโญ เลขที่ 475 ชั้น 9 ถนนศรีอยุธยา แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400

15.2 สำนักงานย่อย อาคารศูนย์บริการวิทยาศาสตร์เพื่อสุขภาพ (อาคาร 6) เลขที่ 928 ถนนสุขุมวิท แขวงพระโขนง เขตคลองเตย กรุงเทพฯ 10110

15.3 สำนักงานย่อย องค์การค้าของ สกสค. เลขที่ 2249 อาคาร 19 โรงพิมพ์คุรุสภาลาดพร้าว แขวงสะพานสอง เขตวังทองหลาง กรุงเทพมหานคร 10310

ตัวอย่างตารางเปรียบเทียบข้อกำหนด สสวท.

รายละเอียดข้อกำหนดของ สสวท.	ข้อเสนอของผู้รับจ้าง	เอกสารอ้างอิง (ระบุเลขหน้า)	หมายเหตุ
4.2 ผู้ยื่นข้อเสนอต้องมีหนังสือรับรองจากทาง Microsoft ในการรับรองถึงการมีประสิทธิภาพในการให้บริการ (Solutions Partner Designations) ในด้าน Infrastructure (Azure) และ/หรือ Modern Work	หนังสือหรือจดหมายรับรองจากบริษัทหน่วยงานที่สามารถออกใบรับรองได้	หนังสือรับรองหรือเอกสารรับรอง ระบุเลขข้อ (ทำแถบสีหรือเครื่องหมายให้ชัดเจน)	
4.7 ผู้ยื่นข้อเสนอต้องมีผู้เชียวชาญอย่างน้อย 1 คน และมีประสบการณ์อย่างน้อย 3 ปี ในการติดตั้งและบริหารจัดการระบบ Virtualization ของ VMware	หนังสือรับรองจากบริษัทผู้ยื่นข้อเสนอหรือหน่วยงานที่สามารถออกใบรับรองได้	หนังสือรับรองหรือเอกสารรับรอง ระบุเลขข้อ (ทำแถบสีหรือเครื่องหมายให้ชัดเจน)	

ภาคผนวก 1 รายการระบบต่างๆ

การปรับแต่งประสิทธิภาพ (Tuning) ระบบต่างๆ ให้มีความปลอดภัย มีประสิทธิภาพ สามารถทำงานได้อย่างต่อเนื่อง และตรงกับนโยบาย เช่น นโยบายด้านความปลอดภัยของ สสวท. กฎหมาย และ ข้อกำหนดจากหน่วยงานด้านความปลอดภัยที่บังคับใช้ก่อนและระหว่างสัญญาจ้าง)

ระบบ	ระบบย่อย	SLA (ชั่วโมง)
Active Directory	Active Directory Design and Maintenance	4
	AD Integrated DNS Servers and DHCP Server	4
	Group Policy implementation for standard administrative purpose	6
	Active Directory logging and auditing	6
	Active Directory Backup for critical restore	6
	Azure Active Directory	4
Internet DNS Server	External DNS Servers, Caching DNS Server	6
Messaging	Messaging Secure Design plan and implementation (SMTP relay and others)	4
	Spam and Antivirus for Mailbox design	6
	Messaging design for fault tolerance	6
	Microsoft Exchange additional feature : OWA, RPC over HTTP, Push Mail, MAPI over HTTP	6
	Mail Storage Backup and restore	6
	Microsoft Office 365 integration with on-premises environments (Exchange 2019)	4
	ติดตั้ง SSL Certificate (สสวท. เป็นผู้จัดหา SSL Certificate)	2
	Message logging and achieving for audit purpose	6
Microsoft Team	ที่ สสวท. ใช้งาน	4
Microsoft Office 365	Office 365 Education Plan A1 สำหรับองค์กร ที่ สสวท. ใช้งาน	4
TrendMicro™ (Smart Protection™ Suites.)	Master-Client antivirus design and implementation	4
	Virus signature update with master antivirus server	6
	Schedule scan design and implementation On Server and Clients	6
WSUS Server	WSUS update (windows update)	6
Wireless System	Aruba Controller & Aruba AP (Aruba 7030) EDUROAM	6

ระบบ	ระบบย่อย	SLA (ชั่วโมง)
Network infrastructure WAN	view check and design all related equipment but configuration /implement from core switch to internal)	-
	Zone design and maintenance	-
	VLAN design Implement: maintenance	6
Public key infrastructure (PKI) maintenance	Certificate Authority Maintenance	6
	Certificate Enrollment & Service Certificate maintenance	6
	การใช้งาน PKI กับเครื่องลูกข่ายที่ต้องการรักษาความปลอดภัยระดับสูง	2
Central File Server	Home directory implementation/Maintenance	4
	Disk Quota implementation/MA	6
	SAN Storage design and maintenance	6
	Volume Shadow copy service Maintenance	6
	File server Backup and restore implementation/MA	6
	Critical logging with confidential file	6
SSL Certificate	ติดตั้ง SSL บนระบบที่เกี่ยวข้องในภาคผนวก 1 รวมถึง ระบบอื่นๆ ตามที่ สสวท. กำหนด และบริหารจัดการการใช้งาน SSL Certificate (สสวท. เป็นผู้จัดหา SSL Certificate)	2
Incident Case	หากต้องการขยาย SLA ให้อยู่ในดุลพินิจ สสวท.	24
Request Case (Urgent)	หากต้องการขยาย SLA ให้อยู่ในดุลพินิจ สสวท.	4
Request Case (Not Urgent)	ตามที่ตกลงร่วมกันกับ สสวท.	-

หมายเหตุ สสวท. มีเครื่องมือ ดังนี้

1. Virtual Machine

   1.1 VMware vCenter Server 6/7 สำหรับบริหารจัดการ Virtualization Machine
2. Trend Micro Smart Protection Complete จำนวน 70 agent
3. Backup

   3.1 CA Arcserve (Backup Disk to Tape) Version 16.5R

   3.2 Arcserve UDP (Backup Disk to Disk) Version 5.0.1897

   3.3 Windows Server Backup Feature

   3.4 ซอฟต์แวร์สำรองข้อมูลสำหรับ VM (Veeam Backup)
4. Monitoring Tool

   4.1 Manage Engine Version 12 ประกอบด้วยซอฟต์แวร์ย่อยคือ

   - Appliance Manager Professional Edition, EventLog Analyzer Premium for 80 Host/App
   - Exchange Reporter Plus Professional Edition for 500 mail boxes

4.2 Solarwinds Version 6.1.7601.65536 (Network Monitoring) ประกอบด้วยซอฟต์แวร์ย่อย - Orion, NPM, NTA, IVIM

5. Aruba Wireless Controller Management
6. Crowdstrike EDR
7. Forescout Network Access Control
8. iTop
9. Zabbix

ภาคผนวก 2 นโยบายและแนวปฏิบัติในการปฏิบัติงาน

1. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564
2. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2565
3. นโยบายการสำรองข้อมูลและการเตรียมความพร้อมในกรณีฉุกเฉิน
4. แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ตามประกาศของ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) และ กมช. ที่ อ้างอิงตาม สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้แก่
    4.1 แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
    4.2 การประเมินความเสียงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
    4.3 แผนการรับมือภัยคุกคามทางไซเบอร์
    4.4 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline)
5. แผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2567
6. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
7. ปฏิบัติตามประกาศที่เกี่ยวข้อง เช่น
    7.1 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566
    7.2 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566
    7.3 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566
    7.4 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗
    7.5 รวมถึงประกาศหรือกฎหมายต่างๆ ที่เกี่ยวข้อง ที่มีการประกาศระหว่างสัญญา

ร่างรายชื่อคณะกรรมการ

จ้างบำรุงรักษาระบบบริหารจัดการบริการเทคโนโลยีสารสนเทศ (IT Service Management (ITSM)) ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

คณะกรรมการพิจารณาผล

นางสาวปลื้มฤดี	ชาติวันชัย	ประธานกรรมการ
นายพีรพัฒน์	ผิวผา	กรรมการ
นายภากร	กุลศุภกร	กรรมการ

คณะกรรมการตรวจรับ

นายถนิม	ทิพย์ผ่อง	ประธานกรรมการ
นายรชต	ทรงอยู่	กรรมการ
นางสาวอภิวรรณ	วิรัชสกุลทิพย์	กรรมการ