รายละเอียดขอบเขตงาน

จ้างบำรุงรักษาระบบบริหารจัดการบริการเทคโนโลยีสารสนเทศ (IT Service Management (ITSM))

ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

1. หลักการและเหตุผล

ฝ่ายเทคโนโลยีสารสนเทศ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) มีหน้าที่ดูแลรับผิดชอบโครงสร้างพื้นฐานดิจิทัลที่สำคัญ ประกอบด้วย ระบบสารสนเทศ ระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่ายทั้ง On-premise และ คลาวด์กลางภาครัฐ (GDCC) รวมถึงระบบฐานข้อมูล Microsoft SQL Server และระบบสนับสนุนการทำงานร่วมกัน Microsoft 365 เพื่อให้บริการแก่บุคลากรได้อย่างต่อเนื่อง

เพื่อให้การบริหารจัดการเป็นไปอย่างมีประสิทธิภาพภายใต้มาตรฐานสากลและสอดคล้องกับสถาปัตยกรรมเทคโนโลยีที่เปลี่ยนแปลงไป สสวท. จึงมีความจำเป็นต้องจัดหาผู้เชี่ยวชาญที่มีความรู้ความสามารถเฉพาะด้านในการบริหารจัดการเชิงรุกตามแนวทาง IT Service Management (ITSM) และการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อรองรับการขับเคลื่อนพันธกิจของสถาบันให้มีความมั่นคง ปลอดภัย และสอดคล้องกับกฎหมายที่เกี่ยวข้อง

2. วัตถุประสงค์

2.1 เพื่อดำเนินการบริหารจัดการบริการเทคโนโลยีสารสนเทศ รวมถึงระบบคลาวด์ภาครัฐ (GDCC) ฐานข้อมูล และระบบสนับสนุนการทำงานร่วมกัน ตามแนวทาง ITSM และมาตรฐานสากล (ITIL, ISO/IEC 20000, ISO/IEC 27001) โดยเน้นการยกระดับความมั่นคงปลอดภัยไซเบอร์ตามนโยบายและแนวปฏิบัติของสถาบัน

2.2 เพื่อสร้างความเชื่อมั่นในระบบสารสนเทศ ลดความเสี่ยงจากการหยุดชะงักของระบบงาน (Business Interruption) และเพิ่มขีดความสามารถในการป้องกัน ตรวจสอบ และรับมือกับภัยคุกคามทางไซเบอร์ต่อโครงสร้างพื้นฐานดิจิทัลของสถาบันได้อย่างมีประสิทธิภาพและทันท่วงที

2.3 เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศสอดคล้องกับกฎหมายและระเบียบที่เกี่ยวข้อง ได้แก่ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)

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 เป็นผู้มีประสบการณ์ในการบริหารโครงการด้านเทคโนโลยีสารสนเทศและการสื่อสาร มีความรู้ความสามารถในระบบสารสนเทศและการสื่อสาร สามารถให้คำปรึกษา แนะนำ ตรวจสอบ ประสานงาน และวิเคราะห์ปัญหา พร้อมเสนอแนวทางแก้ไขที่เกี่ยวข้องกับระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ซึ่งเป็นโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล

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

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

4.4 ผู้ยื่นข้อเสนอต้องจัดให้มีคณะผู้เชี่ยวชาญเฉพาะด้าน (Back Office) เพื่อปฏิบัติงานสนับสนุน ไม่น้อยกว่า 9 คน (บุคลากร 1 คนสามารถถือครองประกาศนียบัตรได้มากกว่า 1 รายการ) โดยต้องมีหนังสือรับรองการทำงานและมีประกาศนียบัตรที่ยังไม่หมดอายุ ณ วันที่ยื่นข้อเสนอ ครอบคลุมทักษะดังต่อไปนี้

1) ด้านความมั่นคงปลอดภัย ต้องได้รับประกาศนียบัตร CISSP (Certified Information Systems Security Professional) เพื่อให้คำแนะนำเชิงกลยุทธ์และการบริหารความเสี่ยง อย่างน้อย 1 คน

2) ด้านระบบเครือข่าย ต้องได้รับประกาศนียบัตร CCNP อย่างน้อย 1 คน

3) ด้านโครงสร้างพื้นฐานคลาวด์และ Microsoft 365 ต้องได้รับประกาศนียบัตร Azure Solutions Architect Expert หรือ Azure Administrator Associate หรือ Microsoft 365 Certified: Administrator Expert อย่างน้อย 1 คน

4) ด้านระบบปฏิบัติการ Linux ต้องมีประสบการณ์ไม่น้อยกว่า 3 ปี ในการบริหารจัดการ Linux (เช่น Ubuntu, RedHat) และได้รับประกาศนียบัตร CompTIA Linux+ หรือ RHCE หรือเทียบเท่า อย่างน้อย 1 คน

5) ด้านระบบเสมือน (Virtualization) ต้องมีประสบการณ์ไม่น้อยกว่า 3 ปี ในการบริหารจัดการระบบ VMware โดยเฉพาะ อย่างน้อย 1 คน

6) ด้านฐานข้อมูล ต้องมีความรู้ความชำนาญในการบริหารจัดการฐานข้อมูล SQL Server อย่างน้อย 1 คน

7) ด้านการวิเคราะห์ข้อมูล ต้องได้รับประกาศนียบัตร Microsoft Certified: Power BI Data Analyst Associate อย่างน้อย 1 คน

8) ด้านการบริหารจัดการโครงการ ต้องได้รับประกาศนียบัตร PMP (Project Management Professional) เพื่อทำหน้าที่วางแผนและควบคุมภาพรวมการดำเนินงาน อย่างน้อย 1 คน

9) ด้านมาตรฐานการให้บริการไอที (ITIL Specialist) ต้องได้รับประกาศนียบัตร ITIL 4 (Foundation หรือสูงกว่า) เพื่อกำกับดูแลกระบวนการ ITSM ให้เป็นไปตามมาตรฐาน อย่างน้อย 1 คน

10) ด้านความต่อเนื่องทางธุรกิจ (BCM Specialist) ต้องมีความเชี่ยวชาญและประสบการณ์ด้านการบริหารความต่อเนื่องทางธุรกิจ (BCM) และการจัดทำแผนกู้คืนระบบ (DR Plan) อย่างน้อย 1 คน

4.5 ผู้ยื่นข้อเสนอต้องจัดให้มีเจ้าหน้าที่ปฏิบัติงานประจำ ณ สสวท. จำนวน 2 คน โดยต้องมีวุฒิการศึกษาขั้นต่ำระดับปริญญาตรี ในสาขาคอมพิวเตอร์ เทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง และมีประสบการณ์ด้านการดูแลระบบคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายไม่น้อยกว่า 3 ปี โดยแบ่งตามความเชี่ยวชาญดังนี้

1) เจ้าหน้าที่ด้านระบบโครงสร้างพื้นฐาน (Infrastructure System Administrator) ต้องมีความรู้ความเชี่ยวชาญและสามารถบริหารจัดการระบบต่างๆ ดังนี้

- บริหารจัดการ Windows Server (เวอร์ชัน 2012 R2 ถึง 2022) และ Linux (Ubuntu, CentOS, Red Hat) รวมถึงการจัดการ Security Patch และการใช้งาน Docker/Container
- บริหารจัดการ Active Directory, LDAP, DHCP และ DNS (ทั้ง IPv4 และ IPv6)
- บริหารจัดการ Microsoft Exchange Server 2019, Microsoft Office 365 และ
- บริหารจัดการระบบรักษาความปลอดภัย Trend Micro, Mail Security (IMSVA) และการตั้งค่าความปลอดภัยบน Microsoft EMS
- บริหารจัดการระบบสำรองข้อมูล (Backup/Restore, Replication, HA), ระบบฐานข้อมูล SQL Server, File Server Resource Manager และ Web Server (IIS, Apache, Nginx)

2) เจ้าหน้าที่ด้านระบบเครือข่าย (Network Administrator) ต้องมีความรู้ความเชี่ยวชาญและสามารถบริหารจัดการระบบต่างๆ ดังนี้

- บริหารจัดการโครงสร้างพื้นฐานเครือข่าย LAN/WAN และระบบ Wireless Network
- บริหารจัดการระบบ DHCP, DNS (ทั้ง IPv4 และ IPv6), RADIUS Server และระบบ Wireless Security
- บริหารจัดการความมั่นคงปลอดภัยเครือข่าย (Internet Security) และการใช้งาน Endpoint Security Solution
- บริหารจัดการและใช้งานเครื่องมือตรวจสอบประสิทธิภาพเครือข่าย (Network Monitoring Tools) เพื่อเฝ้าระวังและแก้ไขปัญหาได้อย่างทันท่วงที

5. ขอบเขตการดำเนินงาน

ผู้ยื่นข้อเสนอต้องสามารถให้คำปรึกษา แนะนำ สนับสนุน และประสานงานในการตรวจสอบ วิเคราะห์ และแก้ไขปัญหาที่เกิดขึ้นกับระบบโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ซึ่งครอบคลุมถึงระบบเครือข่าย เครื่องคอมพิวเตอร์แม่ข่ายทั้งภายในหน่วยงาน (On-premise) และระบบคลาวด์กลางภาครัฐ (GDCC) ระบบบริหารจัดการฐานข้อมูล (Microsoft SQL Server) และระบบสนับสนุนการทำงานร่วมกัน (Microsoft 365) เพื่อให้ระบบสารสนเทศทั้งหมดสามารถให้บริการได้อย่างต่อเนื่อง มีเสถียรภาพ และมีประสิทธิภาพสูงสุด

ทั้งนี้ การดำเนินงานต้องอยู่ภายใต้แนวทาง IT Service Management (ITSM) ตามกรอบมาตรฐาน ITIL โดยเน้นกระบวนการหลัก ได้แก่ Incident Management, Problem Management, Change Management, Request Fulfillment และ Configuration Management ให้เป็นไปตามมาตรฐานสากล ISO/IEC 20000 และ ISO/IEC 27001 รวมถึงต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศของ สสวท. และประกาศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) และการคุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อยกระดับความน่าเชื่อถือ ลดความเสี่ยงจากภัยคุกคาม และป้องกันเหตุการณ์ที่อาจส่งผลกระทบต่อความพร้อมใช้งานของระบบงานสำคัญ โดยมีรายละเอียดการดำเนินงานดังนี้

5.1 ผู้ยื่นข้อเสนอต้องเสนอแผนการดำเนินงาน (Project Plan) โดยมีรายละเอียด ดังนี้

1) โครงสร้างคณะทำงาน (Organization Chart) ระบุชื่อ-นามสกุล รูปถ่าย หนังสือรับรองการทำงาน และคุณสมบัติของบุคลากรทุกคนที่จะปฏิบัติงานในโครงการให้ชัดเจน

2) การติดต่อประสานงาน (Communication & Support) จัดให้มีระบบ Call Center หรือช่องทางติดต่อที่สามารถให้บริการได้ 24 ชั่วโมง พร้อมระบุรายชื่อบุคลากร ตำแหน่ง อีเมล หมายเลขโทรศัพท์ และสถานที่ตั้งที่สามารถติดต่อได้จริง

3) แผนการโอนย้ายงานและถ่ายทอดความรู้ (Transition & Knowledge Transfer Plan) ผ่านการฝึกอบรมขณะปฏิบัติงาน (On-the-job Training) รวมถึงการจัดทำเอกสารคู่มือประกอบการทำงาน เช่น ขั้นตอนการปฏิบัติงาน (Procedure), วิธีการปฏิบัติงาน (Work Instruction), คู่มือการใช้งาน (Manual) และระเบียบปฏิบัติต่างๆ (Rules & Regulations)

4) แผนการบริหารจัดการสิทธิ์เข้าถึง (Access Control & Account Management) แนวทางการจัดทำหรือปรับปรุงระบบการจัดการบัญชีผู้ใช้งานตามนโยบายความปลอดภัยของ สสวท. และมาตรฐานสากล

5) แผนการสำรองข้อมูลและแนวทางการกู้คืนระบบเครือข่ายและเครื่องแม่ข่าย (Backup & Disaster Recovery Plan)

5.2 ผู้ยื่นข้อเสนอต้องจัดการประชุมเริ่มงาน ในรูปแบบ Onsite ณ สสวท. เพื่อนำเสนอบุคลากรที่จะปฏิบัติงานในโครงการทั้งหมด พร้อมระบุบทบาทความรับผิดชอบของแต่ละบุคคลให้ชัดเจน, แผนการดำเนินงานโดยละเอียดตลอดอายุสัญญา (Project Roadmap) รวมถึงขั้นตอนและวิธีการปฏิบัติงานตามขอบเขตงาน (Scope of

Work) และ กำหนดรายละเอียดของงานและรายงาน (Deliverables) ที่ต้องจัดส่งในการประชุมติดตามงานประจำเดือน

5.3 เจ้าหน้าที่ประจำ จำนวน 2 คน ต้องปฏิบัติงาน ณ สสวท. ระหว่างเวลา 08:00 – 17:00 น. (หรือตามเวลาทำการที่ สสวท. กำหนด) โดยมีขอบเขตภาระงานดังนี้

1) การตรวจสอบและเฝ้าระวังระบบประจำวัน (Daily Operations)

- Health Check ตรวจสอบสถานะการทำงานเบื้องต้นและตรวจสอบ Log ของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายตามภาคผนวก 1 พร้อมสรุปรายงานประจำวัน

- Connectivity Check ทดสอบการเชื่อมต่อ VPN ระบบสารสนเทศ และเว็บไซต์ จากเครือข่ายภายนอก อย่างน้อยวันละ 2 ครั้ง (เวลา 09:00 น. และ 13:00 น.)

- Email System Check ตรวจสอบสถานะการรับ-ส่งจดหมายอิเล็กทรอนิกส์ทั้งภายในและภายนอกองค์กร อย่างน้อยวันละ 3 ครั้ง (เวลา 09:00 น., 13:00 น. และ 16:00 น.)

- Security Monitoring ตรวจสอบสถานะการทำงานของระบบ Endpoint Antivirus Solutions และติดตามการแจ้งเตือนภัยคุกคามจากศูนย์ CSOC เพื่อดำเนินการป้องกันและระงับเหตุตามขั้นตอน พร้อมรายงานผลให้ สสวท. ทราบทันที

2) บริหารจัดการและเฝ้าระวังระบบเครือข่ายและเครื่องแม่ข่ายผ่านระบบ Monitoring ตามที่นำเสนอในโครงการ เพื่อให้มั่นใจว่าโครงสร้างพื้นฐานด้านดิจิทัลทำงานได้อย่างมีประสิทธิภาพตลอดเวลา

3) การปฏิบัติงานนอกเวลาทำการ (Overtime & Emergency Support) ในกรณีที่มีการแก้ไขปัญหาค้างคาหรือมีความจำเป็นเร่งด่วน ต้องสามารถปฏิบัติงานต่อเนื่องจนกว่าปัญหาจะคลี่คลาย โดยไม่มีค่าใช้จ่ายเพิ่มเติม ในกรณีนอกเวลาทำการ ต้องสามารถให้บริการในรูปแบบ On-call หรือ On-site เข้าปฏิบัติงาน ณ อาคารสิริภิญโญ ได้ทันทีเมื่อเกิดเหตุวิกฤต (เช่น ระบบล่ม, ภัยคุกคามทางไซเบอร์) หรือเมื่อมีการบำรุงรักษาระบบโครงสร้างพื้นฐานของอาคาร (เช่น ระบบไฟฟ้า, เครื่องปรับอากาศ) ที่ส่งผลกระทบต่อระบบไอที โดยกำหนดเพดานการปฏิบัติงานนอกเวลาทำการไม่เกิน 12 วันต่อปี (หรือตามที่ตกลงในสัญญา)

5.4 ต้องดำเนินการตรวจสอบสถานะระบบที่เกี่ยวข้อง และจัดทำรายงานสรุปผลการดำเนินงานเสนอต่อ สสวท. อย่างน้อยเดือนละ 1 ครั้ง โดยมีรายละเอียดดังนี้

1) ตรวจสอบและรายงานรายการคอมพิวเตอร์และบัญชีผู้ใช้งานที่ไม่มีการใช้งาน (Inactive) เกิน 30 วัน เพื่อให้ สสวท. พิจารณาสั่งการ ลบ (Delete) หรือ ปิดกั้น (Disable) ตามความเหมาะสม

2) ตรวจสอบและรายงานบัญชี Mailbox ที่ไม่มีการใช้งานเกิน 30 วัน พร้อมทั้งตรวจสอบสถานะ IP กับฐานข้อมูล DNS-based Blacklists (ไม่น้อยกว่า 80 รายการ) หากพบสถานะผิดปกติ ต้องแจ้งเตือนทันทีและรายงานผลการดำเนินการแก้ไขจนกว่าจะกลับสู่สถานะปกติ (Delist)

3) ตรวจสอบและรายงานสิทธิ์การเข้าถึง (Permissions) บน Shared Folder และปริมาณการใช้

พื้นที่จัดเก็บข้อมูล เพื่อให้เจ้าของข้อมูล (Data Owner) ตรวจสอบความถูกต้องและบริหารจัดการพื้นที่ได้อย่างมีประสิทธิภาพ

4) ตรวจสอบสถานะอุปกรณ์เครือข่าย (Network Assets) และพอร์ตเชื่อมต่อ (Port) ที่ไม่มีการใช้งาน เพื่อให้ สสวท. พิจารณาสั่งการ ปิด (Disable) ตามมาตรการความมั่นคงปลอดภัย

5) ตรวจสอบระบบจัดเก็บ Log File แบบศูนย์กลาง (Centralized Log) ให้มีความพร้อมใช้งานและจัดเก็บข้อมูลได้ครบถ้วน ถูกต้องตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่บังคับใช้อยู่ในปัจจุบัน

6) รายงานสถานะการบริหารจัดการแพตช์ (Patch) และการปิดช่องโหว่ของระบบปฏิบัติการและซอฟต์แวร์ต่างๆ ให้เป็นปัจจุบันอย่างสม่ำเสมอตามวงจรการบริหารจัดการที่ได้มาตรฐาน

5.5 การจัดการฐานข้อมูล (Database Management) ผู้ยื่นข้อเสนอต้องบริหารจัดการและบำรุงรักษาระบบฐานข้อมูลส่วนกลาง (On-premise และ GDCC) ดังนี้

1) ติดตามสถานะการทำงานของ Microsoft SQL Server ให้พร้อมใช้งาน มีเสถียรภาพ และปลอดภัยอย่างต่อเนื่อง

2) เฝ้าระวังและจัดการพื้นที่จัดเก็บข้อมูล (Disk), Index, Statistics และ Session เพื่อป้องกันปัญหาด้านประสิทธิภาพ (Performance Bottleneck)

3) วิเคราะห์และทำ Tuning ระบบฐานข้อมูลและชุดคำสั่ง (Query) ให้ทำงานรวดเร็ว พร้อมจัดทำรายงานสรุปผลการปรับปรุงอย่างสม่ำเสมอ

4) ดำเนินการสำรองข้อมูล (Backup) ทดสอบการกู้คืน (Recovery) บริหารจัดการสิทธิ์การเข้าถึงและติดตั้ง Patch ความปลอดภัยตามนโยบายของ สสวท.

5) วิเคราะห์และแก้ไขปัญหาที่เกี่ยวข้องกับระบบฐานข้อมูลร่วมกับผู้ที่เกี่ยวข้อง ให้กลับมาใช้งานได้ตามระดับการให้บริการ (SLA) ที่กำหนด

5.6 ผู้ยื่นข้อเสนอต้องบริหารจัดการข้อมูลสินทรัพย์ดิจิทัล (IT Asset Management) ซึ่งครอบคลุมทั้งอุปกรณ์ระบบเครือข่าย, เครื่องแม่ข่าย (On-premise และ GDCC), ระบบฐานข้อมูล และสิทธิ์การใช้งานซอฟต์แวร์ (License) ต่างๆ ให้เป็นไปตามแนวทาง ITIL โดยต้องจัดทำรายงานบัญชีสถานะสินทรัพย์ดิจิทัลและระบบสารสนเทศ (Existing Asset Report) ที่เป็นปัจจุบัน อย่างน้อย 2 ครั้ง (ภายในเดือนที่ 3 และเดือนที่ 11) นับถัดจากวันที่ได้รับหนังสือแจ้งให้เริ่มงาน เพื่อใช้ในการวางแผนบริหารจัดการและปรับปรุงระบบให้มีความมั่นคงปลอดภัย

5.7 ผู้ยื่นข้อเสนอต้องบริหารจัดการระบบปฏิบัติการ Linux ให้ทำงานได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย ดังนี้

1) ดำเนินการ Update Patch และ Upgrade ระบบปฏิบัติการ (OS) ให้เป็นเวอร์ชันปัจจุบันเพื่อปิดช่องโหว่และเพิ่มประสิทธิภาพ ทั้งนี้ ในกรณีที่เป็นระบบปฏิบัติการที่มีระบบงานประยุกต์ (Application) จาก

ผู้พัฒนารายอื่นติดตั้งอยู่ โดยต้อง วิเคราะห์ ตรวจสอบความพร้อม และประสานงานร่วมกับผู้พัฒนารายนั้นๆ เพื่อวางแผนการดำเนินงานและทดสอบอย่างรัดกุมก่อนเริ่มดำเนินการ

2) บริหารจัดการการสำรองข้อมูล (Backup) และทดสอบการกู้คืนข้อมูลระบบ (Recovery) ให้พร้อมใช้งานเมื่อเกิดเหตุขัดข้อง

3) ร่วมวางแผนและดำเนินการทดสอบแผนกู้คืนระบบจากภัยพิบัติ (Disaster Recovery Plan) ให้สอดคล้องตามมาตรฐานและนโยบายที่ สสวท. กำหนด

4) ให้คำปรึกษา แนะนำ และบริหารจัดการระบบ Docker Containers เพื่อรองรับการทำงานของระบบงานประยุกต์ รวมถึงการใช้งาน GitLab เพื่อบริหารจัดการการตั้งค่าระบบและสนับสนุนกระบวนการส่งมอบระบบงาน (Deployment)

5.8 ผู้ยื่นข้อเสนอต้องดำเนินการกู้คืนระบบเมื่อเกิดปัญหาตามมาตรฐาน ITIL และระดับการให้บริการ (SLA) ที่กำหนด ดังนี้

1) รับทราบและตอบรับเหตุขัดข้องทันทีที่ได้รับแจ้งจากระบบเฝ้าระวังอัตโนมัติ หรือจากเจ้าหน้าที่ สสวท. ผ่านช่องทางที่ตกลงกัน

2) วิเคราะห์สาเหตุที่แท้จริง (Root Cause) และดำเนินการกู้คืนระบบให้กลับมาใช้งานได้ตามปกติ หากระบบเสียหายจนไม่สามารถกู้คืนได้ ต้องดำเนินการติดตั้งระบบใหม่ให้มีสถานะและข้อมูลพร้อมใช้งานดังเดิม พร้อมจัดทำรายงานสรุปการแก้ไขปัญหา (Incident Report)

3) กรณีเจ้าหน้าที่ประจำ (Front Office) ไม่สามารถแก้ไขปัญหาได้ จะต้องจัดให้มีผู้เชี่ยวชาญ (Back Office) เข้าดำเนินการตรวจสอบและแก้ไขให้แล้วเสร็จตาม SLA

4) หากปัญหาเกิดจากฮาร์ดแวร์ชำรุด สสวท. จะเป็นผู้จัดหาอุปกรณ์ทดแทน เมื่ออุปกรณ์พร้อมใช้งาน จะต้องดำเนินการกู้คืนระบบให้แล้วเสร็จตาม SLA โดยจะเริ่มนับเวลาใหม่หรือขยายเวลาให้ตามที่ สสวท. เห็นชอบ

5) กรณีเป็นการแก้ไขปัญหาที่วิกฤตหรือต่อเนื่อง จะต้องสามรถปฏิบัติงานนอกเวลาทำการจนกว่าจะแก้ไขปัญหาแล้วเสร็จ โดยไม่มีค่าใช้จ่ายเพิ่มเติม

หมายเหตุ: เกณฑ์การนับเวลาตามระดับการให้บริการ (SLA)

ต้องสามารถแจ้งได้ตลอด 24 ชั่วโมง ผ่านอีเมล โทรศัพท์ หรือระบบแจ้งซ่อม (Ticketing System) โดยจะเริ่มต้นนับเวลาในช่วงวันจันทร์ – เสาร์ เวลา 08.00 – 16.30 น.

* ตัวอย่าง: หากได้รับแจ้งเหตุในวันเสาร์ เวลา 18.00 น. จะเริ่มนับเวลาตาม SLA ตั้งแต่วันจันทร์ เวลา 08.00 น. เป็นต้นไป (ยกเว้นกรณีเหตุวิกฤตที่ส่งผลกระทบวงกว้าง สสวท. อาจขอให้ดำเนินการแก้ไขทันทีตามความเหมาะสม)

5.9 ผู้ยื่นข้อเสนอต้องดำเนินการบริหารจัดการแผนและทดสอบการกู้คืนระบบตามภาคผนวก 1 อย่างน้อย ดังนี้

1) จัดทำและปรับปรุง แผนปฏิบัติงาน (Work Instruction) และ คู่มือการสำรองและกู้คืนข้อมูล (Backup & Recovery) ให้เป็นปัจจุบัน โดยต้องครอบคลุมทั้งระบบ On-premise, Cloud GDCC, ฐานข้อมูล MS SQL และ Microsoft365 และผ่านการรับรองจากผู้เชี่ยวชาญที่เกี่ยวข้อง

2) ประสานงานร่วมกับผู้พัฒนาระบบงานสารสนเทศ (เช่น MIS, บริหารงานบุคคล, สารบรรณ) เพื่อจัดทำแผนและทดสอบกู้คืนระบบงานและฐานข้อมูลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าระบบสามารถทำงานร่วมกันได้อย่างสมบูรณ์

3) ทดสอบกู้คืนข้อมูลระบบ Microsoft 365 (เช่น Exchange Online, SharePoint/OneDrive) และ File Server อย่างน้อยระบบละ 2 ครั้ง ภายในเดือนที่ 9 นับถัดจากวันที่เริ่มงาน โดย สสวท. เป็นผู้กำหนดช่วงเวลา

4) การทดสอบในข้อ 2 และ 3 ต้องดำเนินการภายใต้การกำกับดูแล ตรวจสอบ และรับรองโดยผู้เชี่ยวชาญด้าน Business Continuity Plan (BCP) หรือผู้ดูแลระบบที่เกี่ยวข้อง ตลอดทุกขั้นตอน เพื่อให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัย

5.10 ผู้ยื่นข้อเสนอต้องบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) ระบบโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล อย่างน้อย 2 ครั้ง (ภายในเดือนที่ 6 และเดือนที่ 11) นับถัดจากวันที่ได้รับหนังสือแจ้งให้เริ่มงาน โดยมีขอบเขตการดำเนินงาน ดังนี้

1) ตรวจสอบสภาพการทำงาน (Health Check) ของอุปกรณ์และระบบปฏิบัติการให้พร้อมใช้งาน และจัดทำรายงานผลการตรวจสอบพร้อมข้อเสนอแนะในการปรับปรุงประสิทธิภาพ

2) ในกรณีที่อุปกรณ์หรือซอฟต์แวร์อยู่ภายใต้การรับประกัน (MA) ของบริษัทอื่น ผู้ยื่นข้อเสนอต้องเป็นผู้ประสานงาน กำกับดูแล และร่วมตรวจสอบการทำงานกับบริษัทเหล่านั้น เพื่อให้การบำรุงรักษาเชิงป้องกันเป็นไปตามมาตรฐานที่ สสวท. กำหนด

3) ประสานงานกับผู้ดูแล อุปกรณ์ต่างๆ เพื่อดำเนินการ Update Firmware หรือ Patch ตามรอบการบำรุงรักษา โดยต้องมีการสำรองข้อมูลการตั้งค่า (Configuration Backup) และแผนถอยกลับ (Rollback Plan) ทุกครั้งก่อนเริ่มดำเนินการ

5.11 ผู้ยื่นข้อเสนอต้องดำเนินการปรับแต่งประสิทธิภาพ (Tuning) และเสริมความมั่นคงปลอดภัย (Hardening) ให้แก่ระบบเครือข่าย เครื่องแม่ข่ายทั้ง On-premise และ Cloud (GDCC) ระบบฐานข้อมูล รวมถึงระบบ Microsoft 365 และ Microsoft Azure ให้ทำงานได้อย่างต่อเนื่อง มีเสถียรภาพ และปลอดภัยตามมาตรฐานสากล ISO/IEC 27001 มาตรฐานความปลอดภัยทางไซเบอร์ และนโยบายของ สสวท. อย่างเคร่งครัด

5.12 ผู้ยื่นข้อเสนอต้องตรวจสอบสถานะการทำงานของระบบจดหมายอิเล็กทรอนิกส์ (Microsoft Exchange Server 2019 และ Microsoft 365) โดยครอบคลุมการตรวจสอบสุขภาพระบบ (Service Health), ประสิทธิภาพการทำงาน, ระบบการรับส่งอีเมล (Mail Flow & Message Queue) รวมถึงการตรวจสอบ Audit Log และ Security Log เพื่อเฝ้าระวังและป้องกันเหตุการณ์ผิดปกติหรือภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ

5.13 ผู้ยื่นข้อเสนอต้องดำเนินการจัดทำสถานการณ์จำลองภัยคุกคามไซเบอร์ (Cyber Threat Simulation/Tabletop Exercise) เพื่อป้องกันและลดผลกระทบจากภัยคุกคามตามความเสี่ยงสำคัญของ สสวท. อย่างน้อย 2 กรณี (Cases) โดยต้องดำเนินการตามขั้นตอนและกระบวนการดังนี้

1) วิเคราะห์ความเสี่ยงที่สำคัญ (เช่น Ransomware, Data Breach หรือ Cloud Service Disruption) เพื่อออกแบบสถานการณ์จำลองตามแนวทางของ สกมช.

2) จัดทำขั้นตอนการปฏิบัติงานมาตรฐาน (Standard Operating Procedures: SOP) หรือ Playbook ในการตรวจจับ (Detect), การยับยั้ง (Containment) และการกู้คืนระบบ (Recovery) สำหรับแต่ละกรณีที่กำหนด

3) ดำเนินการซ้อมรับมือเหตุการณ์ (Cyber Incident Response Exercise) ร่วมกับเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อทดสอบความเข้าใจในบทบาทหน้าที่และความสมบูรณ์ของแนวปฏิบัติที่จัดทำขึ้น

4) จัดทำรายงานสรุปผลการซ้อม (Post-Incident Report/After Action Review) พร้อมข้อเสนอแนะในการปรับปรุงโครงสร้างพื้นฐานและมาตรการรักษาความปลอดภัยของ สสวท. ให้มีความมั่นคงปลอดภัยยิ่งขึ้น

5.14 ผู้ยื่นข้อเสนอต้องจัดให้มีผู้เชี่ยวชาญเฉพาะด้านเพื่อรองรับการปฏิบัติงานกรณีพิเศษ การแก้ไขเหตุการณ์ผิดปกติที่นอกเหนือจากขอบเขตงานปกติ หรือการดำเนินการภาระงานอื่นที่เกี่ยวข้องกับโครงสร้างพื้นฐานดิจิทัลตามที่ สสวท. มอบหมาย รวมจำนวนไม่น้อยกว่า 10 วันทำการ (Man-Days) โดยเมื่อได้รับแจ้งรายละเอียดงานจาก สสวท. แล้ว จะต้องดำเนินการวิเคราะห์ ประเมินผลกระทบ และจัดประชุมนำเสนอแนวทางการดำเนินงานเพื่อให้ สสวท. พิจารณาเห็นชอบก่อนเริ่มดำเนินการ ทั้งนี้ ในการติดตั้งและปรับแต่งระบบที่เกี่ยวข้องให้สามารถทำงานได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัยตามข้อตกลง โดย สสวท. จะเป็นผู้รับผิดชอบจัดหาเครื่องคอมพิวเตอร์แม่ข่ายและลิขสิทธิ์ซอฟต์แวร์เพิ่มเติมที่จำเป็น (หากมี)

5.15 ผู้ยื่นข้อเสนอต้องให้คำแนะนำ ร่วมวิเคราะห์ และปรับปรุงกระบวนการทำงานด้านโครงสร้างพื้นฐานดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ ให้สอดคล้องกับนโยบาย สสวท. (ภาคผนวก 2) มาตรฐานสากล (เช่น ISO/IEC 27001, NIST) และกฎหมายที่เกี่ยวข้อง (พ.ร.บ. ไซเบอร์ฯ และ PDPA) ครอบคลุมทั้งการควบคุมการเข้าถึง, การบริหารจัดการสินทรัพย์, การสำรองข้อมูล และการเตรียมความพร้อมรับมือเหตุฉุกเฉิน (BCP)

ทั้งนี้ ในกรณีที่การวิเคราะห์หรือปรับปรุงกระบวนการดังกล่าวมีความซับซ้อน หรือจำเป็นต้องใช้ผู้เชี่ยวชาญเฉพาะด้านเพิ่มเติม สสวท. มีสิทธิ์พิจารณาให้ผู้รับจ้างดำเนินการ ได้รับการสนับสนุนจากผู้เชี่ยวชาญกรณีพิเศษ ตามที่กำหนดไว้ในข้อ 5.14 เพื่อให้การดำเนินงานเป็นไปตามมาตรฐานสากลอย่างมีประสิทธิภาพ

5.16 ในกรณีเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่สร้างความเสียหายต่อโครงสร้างพื้นฐานดิจิทัลและข้อมูลอิเล็กทรอนิกส์ ผู้ยื่นข้อเสนอต้องจัดส่งผู้เชี่ยวชาญเข้าดำเนินการสนับสนุน สสวท. ทันทีเพื่อปฏิบัติงานตามแนวทางของ สกมช. ดังนี้

1) ให้คำแนะนำและดำเนินการร่วมกับ สสวท. ในการระงับการแพร่กระจายของภัยคุกคาม แก้ไขช่องโหว่ และกู้คืนระบบให้กลับมาให้บริการตามปกติอย่างเร่งด่วน

2) ดำเนินการวิเคราะห์หาสาเหตุที่แท้จริงของการบุกรุก (Root Cause Analysis) รวมถึงการเก็บรวบรวมพยานหลักฐานดิจิทัลที่เกี่ยวข้องตามหลักการพิสูจน์หลักฐานดิจิทัล (Digital Forensics)

3) จัดทำรายงานสรุปเหตุการณ์ (Incident Report) พร้อมเสนอแนะมาตรการปรับปรุงระบบและวิธีการป้องกันเพื่อไม่ให้เกิดเหตุการณ์ซ้ำเดิม

4) สนับสนุนข้อมูลและประสานงานร่วมกับหน่วยงานภายนอกหรือหน่วยงานกำกับดูแล (เช่น สกมช. หรือ สพธอ.) ตามที่ สสวท. มอบหมาย

5.17 ผู้ยื่นข้อเสนอต้องให้ความร่วมมือและสนับสนุนผู้เชี่ยวชาญที่ สสวท. จัดหามา ในการตรวจสอบช่องโหว่และทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing: VAPT) เพื่อค้นหาจุดอ่อนและความเสี่ยงของโครงสร้างพื้นฐานดิจิทัล โดยผู้ยื่นข้อเสนอมีหน้าที่ดำเนินการปิดช่องโหว่ (Remediation) หรือปรับแต่งการตั้งค่าระบบตามคำแนะนำในรายงานผลการตรวจสอบให้แล้วเสร็จภายในระยะเวลาที่กำหนด ทั้งนี้ ต้องมีการวิเคราะห์ผลกระทบและวางแผนการดำเนินการร่วมกับ สสวท. เพื่อมิให้กระทบต่อการให้บริการของระบบงาน

5.18 การถ่ายทอดความรู้และการถ่ายโอนงาน (Knowledge Transfer)

1) ต้องถ่ายทอดองค์ความรู้ด้านการบริหารจัดการ การบำรุงรักษา และการตั้งค่าระบบ (Configuration) ให้แก่เจ้าหน้าที่ สสวท. โดยต้องจัดประชุมนำเสนอสรุปผลการดำเนินงานและข้อเสนอแนะเป็นระยะ ทั้งนี้ หัวหน้าโครงการและผู้เชี่ยวชาญ (Back Office) ต้องเข้าร่วมประชุมเพื่อตอบข้อซักถามตามที่ สสวท. กำหนด

2) การรับโอนงานจากผู้รับจ้างรายเดิม (Transition-In) ต้องจัดส่งแผนการรับโอนงานล่วงหน้าไม่น้อยกว่า 5 วันทำการก่อนเริ่มสัญญา และจัดให้มีผู้จัดการโครงการพร้อมทีมงาน (Front Office & Back Office) เข้าดำเนินการรับถ่ายทอดข้อมูลและสิทธิ์ในการเข้าถึงระบบจากผู้รับจ้างรายเดิมให้ครบถ้วนภายในกรอบเวลาดังกล่าว

3) การส่งมอบงานให้ผู้รับจ้างรายใหม่ (Transition-Out) เมื่อสิ้นสุดสัญญา ผู้รับจ้างต้องให้ความร่วมมือในการถ่ายโอนงานให้รายใหม่อย่างน้อย 5 วันทำการ โดยต้องดำเนินการสรุปรายละเอียดภาระงาน คู่มือการปฏิบัติงานของเจ้าหน้าที่ จัดทำรายงานสรุปสถานะระบบสารสนเทศ (Existing Report) และแผนผังโครงสร้างระบบ (Network/System Diagram) ฉบับล่าสุด ณ วันสิ้นสุดสัญญา รวมถึงส่งมอบเอกสารประกอบการดำเนินงาน ข้อมูลการตั้งค่าระบบ (Configuration) ทั้งหมดในรูปแบบไฟล์อิเล็กทรอนิกส์ (PDF) และส่งคืนทรัพย์สินทั้งหมดให้แก่ สสวท. ให้ครบถ้วน

5.19 ผู้ยื่นข้อเสนอต้องจัดให้มีเครื่องมือและระบบสนับสนุนการดำเนินงาน เพื่อใช้สนับสนุนการปฏิบัติงานตลอดอายุสัญญา โดยมีรายละเอียดดังนี้

1) ระบบบริหารจัดการบริการไอที (ITSM & CMDB) ต้องรองรับมาตรฐาน ITIL เพื่อใช้บริหารจัดการสินทรัพย์ (IT Asset Management) และกระบวนการให้บริการอย่างเป็นระบบ มีระบบ Workflow สำหรับจัดการเหตุขัดข้อง (Incident Management) ที่สามารถติดตามสถานะการแก้ไขปัญหาได้ตั้งแต่เริ่มต้นจนจบ

2) ระบบเฝ้าระวังและแจ้งเตือน (Infrastructure Monitoring) ต้องสามารถตรวจสอบประสิทธิภาพและสถานะการทำงานของเครื่องแม่ข่าย (Physical/Virtual Server) และอุปกรณ์เครือข่ายตามภาคผนวก 1 ได้แบบเรียลไทม์ พร้อมระบบแจ้งเตือน (Alerting) ผ่านอีเมลหรือช่องทางที่ สสวท. กำหนดเมื่อเกิดเหตุขัดข้อง

3) ระบบตรวจเช็กช่องโหว่ (Vulnerability Assessment Tools) ต้องสามารถสแกนพอร์ต (Port Scanning) ตรวจสอบบริการที่เปิดใช้งาน และค้นหาช่องโหว่เบื้องต้นของระบบเครือข่ายและเครื่องแม่ข่าย พร้อมรายงานแนวทางแก้ไข (Remediation Guide) เพื่อความมั่นคงปลอดภัย

4) ระบบตรวจสอบประสิทธิภาพจากภายนอก (Application & Website Monitoring) ต้องเป็นระบบ Cloud-based ที่ตรวจสอบสถานะเว็บไซต์และแอปพลิเคชันจากภายนอกได้ตลอด 24 ชั่วโมง ทุกวัน (24x7) พร้อมแจ้งเตือนทันทีเมื่อระบบไม่สามารถเข้าถึงได้

5) ระบบตรวจสอบสถานะบัญชีดำ (Blacklist Monitoring) ต้องสามารถตรวจสอบสถานะ IP Address ของระบบอีเมลกับฐานข้อมูล DNS-based Blacklists ระดับสากลอย่างน้อย 80 รายการเป็นประจำทุกวัน และแจ้งเตือนเมื่อพบสถานะผิดปกติหรือเมื่อได้รับการถอนชื่อออก (Delist)

6) ระบบบริหารจัดการซอร์สโค้ดและชุดคำสั่ง (Source Control Management & CI/CD) เพื่อใช้ในการจัดเก็บและบริหารจัดการชุดคำสั่ง (Script), ไฟล์การตั้งค่าระบบ (Configuration Files) ของเครื่องแม่ข่ายและอุปกรณ์เครือข่าย ให้เป็นระเบียบและสามารถตรวจสอบประวัติการแก้ไขย้อนหลังได้ รวมถึงสนับสนุนกระบวนการส่งมอบและติดตั้งระบบงาน (Deployment) บนระบบ Docker และ Container ให้มีความรวดเร็วและแม่นยำ

เงื่อนไขการดำเนินการและการใช้งาน

1) ต้องนำเสนอรายละเอียดของเครื่องมือและระบบสนับสนุนทั้งหมด รวมถึงกำหนดสิทธิ์การเข้าใช้งาน (Dashboard/Admin Access) ในวันประชุมเริ่มงาน (Kick-off Meeting) เพื่อให้ สสวท. พิจารณาเห็นชอบก่อนเริ่มดำเนินการติดตั้งหรือใช้งาน

2) ซอฟต์แวร์และเครื่องมือทั้งหมดต้องเป็นเวอร์ชันที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย (Licensed Software) หรือเป็นซอฟต์แวร์รหัสเปิด (Open Source) ที่ไม่มีข้อจำกัดในการใช้งานเชิงพาณิชย์ และต้องไม่ละเมิดลิขสิทธิ์ของผู้อื่น โดยผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่ายที่เกิดขึ้นทั้งหมดตลอดอายุสัญญา

5.20 ผู้ยื่นข้อเสนอต้องดำเนินการประสานงาน ติดตาม และกำกับดูแลการทำงานของผู้รับจ้างรายอื่น ที่มีสัญญาบำรุงรักษาอุปกรณ์หรือระบบกับ สสวท. เพื่อควบคุมให้การปฏิบัติงานและการแก้ไขปัญหาเป็นไปตามนโยบายของ สสวท. รวมถึงเป็นไปตามเงื่อนไขการรับประกันและระดับการให้บริการ (SLA) ที่กำหนดไว้ เพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่องและมีเสถียรภาพ

5.21 ผู้ยื่นข้อเสนอต้องจัดทำรายการวัสดุหรือครุภัณฑ์ที่ใช้ในงานจ้าง ซึ่งเป็นพัสดุที่ผลิตภายในประเทศ โดยต้องใช้ไม่น้อยกว่าร้อยละ 60 ของมูลค่าพัสดุที่จะใช้ในงานจ้างนี้ (ถ้ามี)

6. ระยะเวลาการดำเนินงาน 12 เดือน นับถัดจากวันที่ได้รับหนังสือแจ้งให้เริ่มงาน

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

งบประมาณปี 2569 เป็นเงิน 550,000 บาท

งบประมาณปี 2570 เป็นเงิน 1,650,000 บาท

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

9. เอกสารในโครงการ จะต้องจัดทำเอกสารและรายงานต่างๆ 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 รายการจดหมายอิเล็กทรอนิกส์ ที่ไม่ถูกใช้งานเกิน 30 วัน หรือตามที่ สสวท. กำหนด

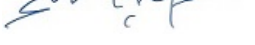
5) การตรวจสอบการทำงานของระบบบริการรับส่ง E-mail

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 9.2.6 (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 เมื่อผู้รับจ้างส่งแผนการดำเนินงานการบริหารจัดการและบำรุงรักษาระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามเอกสารภาคผนวก 1 ภายใน 5 วัน นับถัดจากวันลงนามในสัญญาและปฏิบัติงานตามขอบเขตของงาน ตั้งแต่ เดือนที่ 1 – เดือนที่ 3 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 เมื่อผู้รับจ้างปฏิบัติงานตามขอบเขตของงาน เดือนที่ 4 – 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 เมื่อผู้รับจ้างปฏิบัติงานตามขอบเขตของงาน ตั้งแต่ เดือนที่ 7 – เดือนที่ 9 และส่งมอบรายงานตามข้อ 9.1 และ 9.2 รายงานอื่นๆ ตามงวดงาน และคณะกรรมการตรวจรับเรียบร้อยแล้ว ดังนี้

1) แผนปฏิบัติงานสำรองและกู้คืนระบบเครือข่ายและเครื่องแม่ข่ายคอมพิวเตอร์ที่ให้บริการโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล ตามภาคผนวก 1 ที่ได้รับการตรวจสอบและรับรองจากผู้เชี่ยวชาญ (ฉบับที่ 2)

2) รายงานผลการทดสอบ การกู้คืนร่วมกับผู้พัฒนาระบบงาน ตามที่ สสวท. กำหนด ในข้อ 9.2.7

3) รายงานผลการทดสอบการกู้คืน ระบบจดหมายอิเล็กทรอนิกส์ และระบบ File Server 1 ฉบับ โดยจัดส่งในรูปแบบเอกสารไฟล์อิเล็กทรอนิกส์ PDF จำนวน 1 ชุด

งวดที่ 4 เมื่อผู้รับจ้างปฏิบัติงานตามขอบเขตของงาน ตั้งแต่ เดือนที่ 10 – เดือนที่ 12 และส่งมอบรายงานตามข้อ 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. การให้บริการและค่าปรับ

ผู้รับจ้างต้องบริหารจัดการระบบโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล (ซึ่งครอบคลุมถึงระบบเครือข่าย, เครื่องแม่ข่ายทั้ง On-premise และ GDCC, ระบบฐานข้อมูล MS SQL และระบบ Microsoft 365) ให้มีประสิทธิภาพ มั่นคงปลอดภัย และพร้อมใช้งานอย่างต่อเนื่อง โดยมีเกณฑ์การให้บริการและความรับผิดดังนี้

11.1 ผู้รับจ้างต้องบริหารจัดการมิให้ระบบขัดข้องรวมเกินกว่า 4 (สี่) ชั่วโมงต่อเดือน หรือร้อยละ 0.55 ของเวลาใช้งานทั้งหมดในเดือนนั้น (แล้วแต่ตัวเลขใดจะมากกว่ากัน) หากระบบขัดข้องเกินกว่ากำหนด ผู้รับจ้างยินยอมให้ สสวท. คิดค่าปรับเป็นรายชั่วโมงในอัตราร้อยละ 0.025 ของราคาค่าจ้างรวมตามสัญญาต่อชั่วโมง สำหรับเวลาที่ไม่สามารถใช้งานได้ในส่วนที่เกินกำหนด (เศษของชั่วโมงนับเป็น 1 ชั่วโมง)

11.2 ในกรณีที่เกิดเหตุขัดข้องหรือได้รับการแจ้งซ่อม หากผู้รับจ้างไม่เข้าดำเนินการตรวจสอบหรือแก้ไขภายในเวลาที่กำหนดในขอบเขตงาน (TOR) หรือไม่สามารถแก้ไขให้แล้วเสร็จตามกำหนดผู้รับจ้างยินยอมให้คิดค่าปรับเป็นรายชั่วโมงในอัตราร้อยละ 0.1 ของค่าจ้างรายงวด นับจากเวลาที่ครบกำหนดจนถึงเวลาที่เริ่มการแก้ไขหรือจนกว่าจะแก้ไขแล้วเสร็จ (เศษของชั่วโมงนับเป็น 1 ชั่วโมง) หากผู้รับจ้างไม่ดำเนินการ สสวท. มีสิทธิ์จ้างบุคคลภายนอกมาดำเนินการแทน โดยผู้รับจ้างต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นจริงทั้งหมด

11.3 ในกรณีที่ผู้รับจ้างส่งมอบรายงานประจำงวด หรือผลการดำเนินงานล่าช้ากว่าที่กำหนดในสัญญา และ สสวท. ยังไม่บอกเลิกสัญญา ผู้รับจ้างต้องชำระค่าปรับให้แก่ สสวท. เป็นรายวันในอัตราร้อยละ 0.1 ของราคาค่าจ้างรวมตามสัญญา นับถัดจากวันที่ครบกำหนดส่งมอบจนถึงวันที่ส่งมอบงานให้แก่ สสวท. ครบถ้วนถูกต้อง

12. ข้อสงวนสิทธิ์

12.1 สสวท. สามารถขอเปลี่ยนแปลงบุคลากรหลัก ตามที่ระบุไว้ในข้อเสนอได้โดยไม่มีเงื่อนไข

12.2 ผู้รับจ้างไม่มีสิทธิ์เปลี่ยนแปลงบุคลากรหลัก ตลอดระยะเวลาดำเนินการ โดยไม่ได้รับความเห็นชอบจาก สสวท.

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

12.4 สสวท. ขอสงวนสิทธิ์ในการยกเลิกการจ่ายเงินทันที และ/หรือเรียกเงินคืน หากผู้ยื่นข้อเสนอไม่สามารถดำเนินการได้ตามข้อกำหนดและเงื่อนไข (TOR) ข้อหนึ่งข้อใดของสัญญาจ้างในโครงการนี้ โดยที่ผู้ยื่นข้อเสนอจะไม่ขอเรียกร้องสิทธิรวมทั้งค่าใช้จ่ายใดๆ จาก สสวท. ยกเว้นการไม่สามารถดำเนินการได้ดังกล่าวเป็นผลมาจากข้อจำกัดของ สสวท.

13. เงื่อนไขอื่นๆ สสวท. แบ่งสำนักงาน ออกเป็น 3 ที่ ดังนี้

1) สำนักงานหลัก อาคารสิริภิญโญ เลขที่ 475 ชั้น 9 ถนนศรีอยุธยา แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ 10400

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

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

ตัวอย่างตารางเปรียบเทียบข้อกำหนด สสวท.

รายละเอียดข้อกำหนดของ สสวท.	ข้อเสนอ	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

ผู้รับจ้างต้องดำเนินการบริหารจัดการ บำรุงรักษา และปรับแต่งประสิทธิภาพ (Tuning) รวมถึงเสริมความมั่นคงปลอดภัย (Hardening) ให้แก่ระบบต่างๆ ตามรายการที่กำหนดในภาคผนวกนี้ เพื่อให้ระบบโครงสร้างพื้นฐานดิจิทัลสามารถให้บริการได้อย่างต่อเนื่อง มีเสถียรภาพ และมีประสิทธิภาพสูงสุด ทั้งนี้ การดำเนินงานต้องสอดคล้องกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศของ สสวท. และเป็นไปตามกฎหมายที่เกี่ยวข้อง

ตารางระดับการให้บริการ (SLA)

หมวดหมู่ระบบงาน	รายการระบบและกิจกรรมการปฏิบัติงาน	SLA (ชั่วโมง)
1. Identity & Directory	Active Directory (On-premise): บำรุงรักษา, จัดการ GPO, Backup, Auditing	4
	Microsoft Entra ID (Azure AD): บริหารจัดการบัญชี และตรวจสอบสถานะการ Sync	4
	Core Network Services: บริหารจัดการ DNS (Internal/External) และ DHCP	2
2. Messaging & Collaboration	Microsoft Exchange Server 2019: Mail Flow, Storage Management, Database Health	4
	Microsoft 365 (Exchange Online/Teams): บริหารจัดการสิทธิ์และ Service Health	4
	Mail Security: บริหารจัดการ Spam Filter, Relay Server และ Blacklist Monitoring	2
3. DevOps & Configuration	GitLab Self-Managed: Source Control, User Access, Backup และการดูแลระบบ	4
	Configuration as Code: การจัดเก็บและปรับปรุง Script/Config บน GitLab	6
4. Cloud & Virtualization	VMware vSphere (vCenter/ESXi): การบริหารจัดการ VM และ Cluster Health	4
	GDCC (Government Cloud): บริหารจัดการทรัพยากรบน Cloud กลางภาครัฐ	4
5. Security & Protection	Endpoint Security (Antivirus/EDR): การอัปเดต Signature และ Remediation	4
	SSL Certificate: การติดตั้งและต่ออายุ SSL (เมื่อได้รับไฟล์จาก สสวท.)	2
	Network Access Control (NAC): การควบคุมการเข้าถึงระบบเครือข่าย (Forescout)	4
6. Infrastructure & Network	Network Infrastructure: บำรุงรักษาอุปกรณ์ Switch, Wireless Controller/AP	6
	Windows / Linux Server: การ Patching, Hardening และการจัดการ OS	6
7. Data & Storage	File Server & SAN Storage: การจัดการ Quota, Permission และ Shadow Copy	6
	Backup & Recovery: การสำรองข้อมูลตามรอบ และการทดสอบกู้คืน (Restore Test)	6
8. Monitoring & Support	Monitoring Tools: การตั้งค่าระบบเฝ้าระวัง (Solarwinds/Zabbix) และระบบแจ้งเตือน	4
	ITSM (iTop): การจัดการ Asset Inventory (CMDB) และบันทึก Ticket	8

หมายเหตุ รายการเครื่องมือและซอฟต์แวร์สนับสนุนที่ สสวท. มีอยู่ (Existing Tools)

1. Virtualization: VMware vCenter Server เวอร์ชัน 6 และ 7
2. Security & EDR: Trend Micro Smart Protection, Crowdstrike EDR และ Forescout Network Access Control
3. Backup Solutions: CA Arcserve (Disk to Tape), Arcserve UDP (Disk to Disk), Windows Server Backup และ Veeam Backup
4. Monitoring Tools: Manage Engine (EventLog Analyzer, Exchange Reporter Plus), Solarwinds และ Zabbix
5. Management & Source Control: Aruba Wireless Controller Management, iTop และ GitLab

ภาคผนวก 2 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยดิจิทัล

ผู้รับจ้างต้องศึกษา ทำความเข้าใจ และถือปฏิบัติงานให้สอดคล้องกับกฎหมาย ระเบียบ ประกาศ และนโยบายที่เกี่ยวข้องอย่างเคร่งครัด ดังนี้

1. กฎหมายและประกาศระดับกระทรวง

1.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) การบริหารจัดการข้อมูลส่วนบุคคลที่อยู่ในระบบสารสนเทศของ สสวท.

1.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

2. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) และ สกมช.

ผู้รับจ้างต้องปฏิบัติตามมาตรฐานขั้นต่ำและแนวทางที่ สกมช. กำหนด ได้แก่

2.1 มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 เพื่อวางรากฐานความปลอดภัยพื้นฐาน

2.2 มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

2.3 มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 (Cloud Cybersecurity Standard) เพื่อการดูแลระบบ GDCC และ คลาวด์อื่นๆ

2.4 มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

2.5 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) สำหรับการดูแลเว็บไซต์ภายใต้ความรับผิดชอบของ สสวท.

3. แผนและแนวทางปฏิบัติงานด้านไซเบอร์ (Cybersecurity Framework)

3.1 แผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2567 และแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

3.2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Risk Assessment) ตามวงรอบที่กำหนด

3.3 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) และขั้นตอนการปฏิบัติงานมาตรฐาน (SOP/Playbook)

4. นโยบายและแนวปฏิบัติภายใน สสวท.

4.1 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2565 ของ สสวท.

4.2 นโยบายการสำรองข้อมูลและการเตรียมความพร้อมในกรณีฉุกเฉิน เพื่อความต่อเนื่องทางธุรกิจ (BCP)

5. การเปลี่ยนแปลงกฎหมายและประกาศในอนาคต

ผู้รับจ้างมีหน้าที่ติดตาม ปรับปรุงกระบวนการทำงาน และปฏิบัติตามกฎหมาย ประกาศ หรือหลักเกณฑ์ใหม่ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล ที่มีการประกาศใช้ระหว่างอายุสัญญาจ้าง โดยไม่มีค่าใช้จ่ายเพิ่มเติม