รายละเอียดคุณลักษณะเฉพาะของพัสดุ (Terms of Reference: TOR)

โครงการจัดหาทดแทนระบบคลาวด์เดิมของสำนักงานเศรษฐกิจการคลัง

---

1. ความเป็นมา

ระบบคลาวด์ของสำนักงานเศรษฐกิจการคลัง (สศค.) เป็นคลาวด์ระดับกรม (Agency Cloud) อยู่ในความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศ (ศทส.) เริ่มใช้งานในปี พ.ศ. 2560 เพื่อสนับสนุนภารกิจของ สศค. ในการเป็นหน่วยงานวิเคราะห์และเสนอแนะนโยบายเศรษฐกิจด้านการเงิน การคลัง และเศรษฐกิจระหว่างประเทศ รวมทั้งเป็นหน่วยงานติดตาม กำกับ ประเมินผล และรายงานผลการดำเนินนโยบายหรือมาตรการต่าง ๆ ที่เกี่ยวข้องกับกระทรวงการคลัง ซึ่งในช่วงที่มีการระบาดจนถึงหลังการระบาดของโรคติดเชื้อไวรัสโควิด 19 สศค. มีการประมวลผลข้อมูลมาตรการจำนวนมาก เช่น เราไม่ทิ้งกัน เราชนะ ชิมช้อปใช้ เป็นต้น ข้อมูลมาตรการเหล่านี้เป็นข้อมูลสำคัญและเป็นความลับ ต้องจำกัดการเข้าถึงจากผู้ไม่เกี่ยวข้อง และต้องการระบบประมวลผลความเร็วสูง ระบบคลาวด์ของ สศค. ได้สนับสนุนภารกิจดังกล่าวมาอย่างต่อเนื่อง

ในด้านเทคนิค ระบบคลาวด์ของ สศค. มีการปรับเปลี่ยนการทำงานจากระบบเครื่องคอมพิวเตอร์แม่ข่ายแบบเดิมไปสู่เครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Machine : VM) บนระบบ Cloud Computing ทำให้มีประสิทธิภาพดีขึ้นในด้านการบริหารจัดการระบบ การลดการใช้พื้นที่ในห้องเซิร์ฟเวอร์และประหยัดค่าไฟฟ้า โดยระบบคลาวด์ของ สศค. รองรับการสร้างและจัดการคอมพิวเตอร์เสมือน และมีการจัดการสิทธิ์ผู้เข้าใช้ระบบเพื่อความปลอดภัย ปัจจุบันมีการใช้งาน VM ในระบบคลาวด์เป็นจำนวน 161 VM โดยมีทั้ง VM สำหรับระบบงานภายในของ สศค. และ VM สำหรับจัดเก็บและประมวลผลข้อมูลมาตรการตามภารกิจของ สศค. มีการใช้ทรัพยากรจากระบบคลาวด์ทั้งสิ้น 1,047 vCPU RAM 4,014 GB และ Storage 102 TB และยังมีความต้องการใช้ทรัพยากร vCPU, RAM เพิ่มขึ้นในอัตรา 5% ต่อปี และ Storage เพิ่มขึ้นในอัตรา 10% ต่อปี ซึ่งเป็นไปตามภารกิจงานที่เพิ่มขึ้นตามนโยบายของรัฐบาล

ในด้านการใช้งาน ระบบคลาวด์เริ่มเกิดปัญหาการใช้งานเครื่อง VM เช่น การประมวลผลข้อมูลใช้เวลานานจนไม่ทันต่อการใช้งาน หรือเกิดการหยุดหยุดชะงักจนต้องรีสตาร์ทเครื่อง ปัญหาการใช้พื้นที่ Storage จนเต็มทำให้เครื่อง VM ล่ม ส่งผลให้เจ้าหน้าที่ สศค. ไม่สามารถเข้าถึงและประมวลผลข้อมูลใน VM เครื่องนั้นได้ การกู้คืนทำได้ยากและใช้เวลานาน ทำให้การดำเนินการตามมาตรการหยุดชะงัก การสร้าง VM ใหม่ต้องสร้างด้วยทรัพยากรเครื่องที่จำกัด เป็นต้น นอกจากนี้ยังมีปัญหาที่จากภัยคุกคามไซเบอร์ที่มากขึ้นเรื่อย ๆ เช่น VM บางเครื่องถูก Hack ส่งผลให้เว็บแอปพลิเคชันล่ม VM บางเครื่องติดไวรัส Ransomware เป็นต้น

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

ระบบคลาวด์ของ สศค. มีการใช้งานมานานเกิน 6 ปี ฮาร์ดแวร์ถึงจุด End of Life (EOL) แล้ว มีข้อจำกัดด้านพื้นที่การจัดเก็บข้อมูล และความเร็วในการประมวลผลไม่เพียงพอต่อการใช้งานในปัจจุบัน ซอฟต์แวร์ที่ทำงานเบื้องหลังเป็นเวอร์ชันเก่าทำให้ความเสถียรของระบบลดลง มีความเสี่ยงด้านภัยคุกคามไซเบอร์ ซึ่งหากระบบคลาวด์มีการหยุดชะงักจะทำให้เครื่อง VM ทุกเครื่องหยุดทำงานตามไปด้วย อาจส่งผลเสียต่อความสมบูรณ์ของข้อมูลและการดำเนินงานตามภารกิจของ สศค. ในอนาคตได้

2. วัตถุประสงค์

2.1 เพื่อจัดหาระบบคลาวด์ทดแทนระบบเดิม

2.1.1 เพื่อจัดหาฮาร์ดแวร์ ซอฟต์แวร์ และอุปกรณ์ที่เกี่ยวข้องสำหรับระบบคลาวด์

2.1.2 เพื่อจัดหาซอฟต์แวร์ และอุปกรณ์ที่เกี่ยวข้องสำหรับรักษาความปลอดภัยให้ระบบคลาวด์

2.1.3 เพื่อโอนย้ายระบบงานและข้อมูลไปทำงานบนระบบคลาวด์ใหม่

2.2 เพื่อเพิ่มประสิทธิภาพการทำงานของระบบงานภายในและการวิเคราะห์ข้อมูลตามภารกิจของ สศค.

3. คุณสมบัติผู้ยื่นข้อเสนอ

3.1 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลที่มีการจดทะเบียนก่อตั้งบริษัทมาแล้วไม่น้อยกว่า 5 ปี โดยมีหลักฐานการจดทะเบียน ณ กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ซึ่งออกเอกสารหรือรับรองการจดทะเบียนให้ไม่เกิน 3 เดือนนับถึงวันที่เสนอราคา โดยให้ยื่นขณะเข้าเสนอราคา

3.2 ผู้ยื่นข้อเสนอต้องมีผลงานในด้านระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ และเป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐตาม พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 อย่างน้อย 2 สัญญา มูลค่าของแต่ละสัญญาไม่น้อยกว่า 34,000,000 บาท (สามสิบสี่ล้านบาทถ้วน) ซึ่งผลงานนั้นต้องมีระยะเวลาไม่เกิน 5 ปี นับถัดจากวันสิ้นสุดในสัญญา และต้องแสดงหลักฐานเอกสารรับรองผลงาน และสำเนาสัญญาโดยให้ยื่นขณะเข้าเสนอราคา ทั้งนี้ สศค. สงวนสิทธิ์ที่จะตรวจสอบข้อเท็จจริงโดยตรงจากหน่วยงานตามเอกสารที่เสนอนั้น

3.3 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิต หรือตัวแทนจำหน่ายในประเทศไทย หรือบริษัทเจ้าของผลิตภัณฑ์ หรือจากบริษัทสาขาของเจ้าของผลิตภัณฑ์ในประเทศไทย และต้องได้รับการรับรองว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยใช้งานมาก่อน ยังอยู่ในสายการผลิต สนับสนุนการรับประกัน (Warranty) สนับสนุนทางด้านเทคนิคและบริการหลังการขาย โดยแนบสำเนาหนังสือแต่งตั้งและหนังสือรับรองสำหรับรายการที่ 4.1, 4.2, 4.3, 4.5, 4.6, 4.7 และ 4.8 ของรายละเอียดคุณลักษณะเฉพาะของพัสดุ (TOR) โดยให้ยื่นขณะเข้าเสนอราคา

3.4 ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายจากผู้ผลิต หรือตัวแทนจำหน่ายในประเทศไทย หรือบริษัทเจ้าของผลิตภัณฑ์ หรือจากบริษัทสาขาของเจ้าของผลิตภัณฑ์ในประเทศไทย และต้องได้รับการรับรองว่าได้รับการสนับสนุนการรับประกัน (Warranty) สนับสนุนทางด้านเทคนิคและบริการหลังการขาย โดยแนบสำเนา

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

หนังสือแต่งตั้งและหนังสือรับรองสำหรับรายการที่ 4.9.8 ของรายละเอียดคุณลักษณะเฉพาะของพัสดุ (TOR) โดยให้ยื่นขณะเข้าเสนอราคา

3.5 ผู้ยื่นข้อเสนอต้องมีเจ้าหน้าที่ด้านเทคนิคที่ได้รับหนังสือรับรอง (Certificate) ด้านระบบคอมพิวเตอร์แม่ข่ายเสมือนของผลิตภัณฑ์ไม่ต่ำกว่าระดับ Professional ตามรายการข้อ 4.3 ของรายละเอียดคุณลักษณะเฉพาะของพัสดุ (TOR) อย่างน้อย 1 คน และให้ปฏิบัติงานสนับสนุนการดำเนินงานตลอดระยะเวลาของโครงการและระยะเวลารับประกันของโครงการ พร้อมหลักฐานหนังสือรับรอง (Certificate) โดยให้ยื่นขณะเข้าเสนอราคา

3.6 ผู้ยื่นข้อเสนอต้องมีเจ้าหน้าที่ด้านเทคนิคที่ได้รับหนังสือรับรอง (Certificate) คือ Certified Information Systems Security Professional (CISSP) หรือ CompTIA Advanced Security Practitioner (CompTIA CASP+) อย่างน้อย 1 คน พร้อมหลักฐานหนังสือรับรอง (Certificate) โดยให้ยื่นขณะเข้าเสนอราคา

3.7 เจ้าหน้าที่ด้านเทคนิคของผู้ยื่นข้อเสนอตามข้อ 3.5 และ ข้อ 3.6 สามารถเป็นบุคคลเดียวกันหรือต่างบุคคลก็ได้ ทั้งนี้ จะต้องมีคุณสมบัติครบถ้วนตามที่กำหนดในข้อ 3.5 และ ข้อ 3.6

4. รายละเอียดคุณลักษณะเฉพาะและข้อกำหนด

ผู้ยื่นข้อเสนอจะต้องเสนอรายการอุปกรณ์และระบบ พร้อมการปรับตั้งค่า (Configuration) และติดตั้งอุปกรณ์และระบบ ณ ห้องเซิร์ฟเวอร์ของ สศค. หรือสถานที่ตามที่ สศค. กำหนด ดังนี้

ลำดับที่	รายการ	จำนวน	หน่วย
1	อุปกรณ์กระจายสัญญาณ	2	ชุด
2	เครื่องคอมพิวเตอร์แม่ข่าย	8	ชุด
3	ซอฟต์แวร์ระบบคอมพิวเตอร์แม่ข่ายเสมือน	1	ชุด
4	ซอฟต์แวร์ระบบปฏิบัติการ	1	ชุด
5	ระบบตรวจจับการโจมตีและตอบสนองต่อภัยคุกคามไซเบอร์	150	ชุด
6	อุปกรณ์รักษาความปลอดภัย	2	ชุด
7	ระบบบริการจัดการรหัสผ่านและบริหารจัดการเซสชั่น	1	ระบบ
8	ระบบประเมินและตรวจสอบช่องโหว่ภายในเครือข่าย	1	ระบบ
9	การย้ายระบบ	1	งาน

รายละเอียดคุณลักษณะอุปกรณ์ของโครงการฯ มีดังนี้

4.1 อุปกรณ์กระจายสัญญาณ จำนวน 2 ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังนี้

4.1.1 เป็นอุปกรณ์สวิตช์ที่สามารถทำงานในระดับ Layer 2 และ Layer 3 ได้

4.1.2 มีขนาดของ Switching Capacity ไม่น้อยกว่า 4.0 Tbps (full-duplex)

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

4.1.3 มีความสามารถในการส่งข้อมูล (Throughput) ได้ไม่น้อยกว่า 3.0 Bpps (full-duplex)

4.1.4 มีพอร์ตแบบ 10/25 Gigabit Ethernet (SFP28) จำนวนไม่น้อยกว่า 48 พอร์ต พร้อม Transceiver Module

4.1.5 มีพอร์ตแบบ 100 Gigabit Ethernet (QSFP28) จำนวนไม่น้อยกว่า 4 พอร์ต พร้อม Transceiver Module

4.1.6 มีพอร์ตสำหรับบริหารจัดการตัวอุปกรณ์แบบ RJ45 Console และ Management Port

4.1.7 สนับสนุนจำนวน MAC Address ได้สูงสุดไม่น้อยกว่า 256,000 Addresses

4.1.8 สามารถรองรับจำนวน VLAN ได้ไม่น้อยกว่า 4000 VLAN

4.1.9 สนับสนุน IP Multicast เช่น IGMPv1/v2/v3 ได้เป็นอย่างน้อย

4.1.10 สนับสนุนการทำ Quality of Service (QoS) และ ACL ได้

4.1.11 สนับสนุน Routing แบบ OSPF และ BGP ได้เป็นอย่างน้อย

4.1.12 สนับสนุนการทำ Link aggregation ตามมาตรฐาน IEEE 802.3ad ได้อย่างน้อย 16 พอร์ตต่อหนึ่งกลุ่ม

4.1.13 สนับสนุนมาตรฐานดังต่อไปนี้ได้ IEEE 802.1d, IEEE 802.1w, IEEE 802.1S และ RPVST+ ได้

4.1.14 อุปกรณ์ทำงานตามมาตรฐานแบบ IEEE 802.1x และรองรับการทำ Authentication ผ่าน Radius ได้

4.1.15 สามารถบริหารจัดการได้ดังต่อไปนี้ Command Line Interface (CLI), Telnet, SNMP และ SSH เป็นต้น

4.1.16 สนับสนุนการ Monitor ของ Traffic แบบ sFlow ได้

4.1.17 สนับสนุนการทำ L2 VXLAN (Static VXLAN, BGP EVPN) ได้เป็นอย่างน้อย

4.1.18 อุปกรณ์สามารถติดตั้งบนตู้ Rack ได้

4.1.19 สามารถรองรับระบบไฟฟ้าแบบ 100-240 VAC ความถี่ 50/60 Hz ได้

4.1.20 มี Power supply สามารถทำงานทดแทนแบบ Redundant ได้

4.1.21 สามารถทำงานได้ที่อุณหภูมิ 0 ถึง 45 องศาเซลเซียส ได้

4.1.22 ได้รับมาตรฐานจาก FCC, UL, EN, VCCI และ RoHS เป็นอย่างน้อย

4.1.23 สามารถทำงานแบบ High Availability (HA) แบบ Active – Active หรือ Active – Standby ได้

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

4.2 เครื่องคอมพิวเตอร์แม่ข่าย จำนวน 8 ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังนี้

4.2.1 สามารถติดตั้งซอฟต์แวร์ระบบจัดเก็บข้อมูลแบบเสมือนสำหรับระบบแม่ข่ายคอมพิวเตอร์เสมือนที่เสนอในโครงการแบบ Hyper Converged Infrastructure (HCI) ได้

4.2.2 มีหน่วยประมวลผลกลาง (CPU) แบบ 28 แกนหลัก (28 Core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะ มีความเร็วสัญญาณนาฬิกาพื้นฐานไม่น้อยกว่า 2 GHz จำนวนไม่น้อยกว่า 2 หน่วย

4.2.3 หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ 64 bit มีความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันไม่น้อยกว่า 52.5 MB

4.2.4 มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR5 หรือดีกว่า มีขนาดรวมไม่น้อยกว่า 1024 GB รองรับการใส่ memory ได้สูงสุดไม่น้อยกว่า 8 TB และมีจำนวนช่องใส่ Memory ไม่น้อยกว่า 32 DIMM Slots

4.2.5 มีหน่วยจัดเก็บข้อมูล M.2 SSD แบบ Hot Plug หรือ Hot-Swap ที่มีความจุไม่น้อยกว่า 480 GB จำนวน 2 หน่วย สามารถทำ Hardware RAID1 ได้

4.2.6 มีหน่วยจัดเก็บข้อมูลแบบ SSD SAS Mixed use แบบ Hot Plug หรือ Hot-Swap ที่มีความจุไม่น้อยกว่า 800GB จำนวนไม่น้อยกว่า 2 หน่วย

4.2.7 มีหน่วยจัดเก็บข้อมูลแบบ SSD SAS RI แบบ Hot Plug หรือ Hot-Swap ที่มีความจุไม่น้อยกว่า 3.84 TB จำนวนไม่น้อยกว่า 10 หน่วย

4.2.8 มีจอ LCD แสดงสถานะการทำงานที่ด้านหน้า ซึ่งสามารถทราบถึงความผิดปกติของระบบได้จาก Error Code บน LCD Display

4.2.9 สามารถจัดการเครื่องแม่ข่ายผ่าน micro-USB port

4.2.10 มีส่วนเชื่อมต่อกับระบบเครือข่ายแบบ Gigabit Ethernet จำนวนไม่น้อยกว่า 2 ports

4.2.11 มีส่วนเชื่อมต่อแบบ Ethernet ที่มีความเร็วไม่น้อยกว่า 10/25Gb ชนิด SFP28 จำนวนไม่น้อยกว่า 4 ports พร้อม module ชนิด SFP+ ไม่น้อยกว่า 4 unit

4.2.12 มีหน่วยจ่ายกระแสไฟฟ้าภายในเครื่อง (Power Supply) ขนาดไม่น้อยกว่า 1,400 Watt จำนวน 2 ชุด มีคุณสมบัติทำงานทดแทนกันได้โดยอัตโนมัติ (Redundant) และสามารถถอดเปลี่ยนได้ทันทีแม้ไม่เกิดปัญหาใด ๆ (Hot Plug หรือ Hot Swap)

4.2.13 ตัวเครื่องคอมพิวเตอร์แม่ข่ายที่เสนอจะต้องเป็นรุ่นที่ได้รับการออกแบบเพื่อติดตั้งบน Rack โดยเฉพาะ ขนาดไม่เกิน 2U พร้อมอุปกรณ์ Rack ในการติดตั้ง

4.2.14 สามารถใช้งานกับระบบปฏิบัติการและ Hypervisor อย่างน้อย ดังนี้ Microsoft Windows Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, VMware ESXi

4.2.15 มีตัวช่วยควบคุมการเข้าถึงระบบเพื่อรองรับการจัดการเครื่องแม่ข่ายจากระยะไกล โดยไม่ต้องติดตั้ง (Agent-free) หรือเสนอ software เพิ่มเติม

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

4.2.16 มีโปรแกรมช่วยในการควบคุมระบบ (System Management) และมีความสามารถอย่างน้อยดังนี้

4.2.16.1 สามารถควบคุม Power On, Power Off, System Reset, Power Cycle และ Graceful Shutdown ได้

4.2.16.2 สามารถใช้งาน Virtual Console ผ่าน HTML5 และ รองรับการใช้งาน Virtual Media เช่น CD/DVD, Map Removable Disk ได้เป็นอย่างน้อย

4.2.16.3 สามารถป้องกัน การแก้ไข Configuration และ Firmware ของตัวเครื่องได้

4.2.16.4 System Management รองรับการจัดการ Server และ Monitor อุปกรณ์ Networking, Storage รวมถึง Third-Party

4.2.16.5 System Management รองรับการทำ Integrations กับ Third-party เช่น Microsoft System Center, VMware vCenter and vRealize Operation Manager ได้เป็นอย่างน้อย และรองรับการเชื่อมต่อกับ Third-party เช่น IBM Tivoli และ Nagios ได้เป็นอย่างน้อย

4.3 ซอฟต์แวร์ระบบคอมพิวเตอร์แม่ข่ายเสมือน แบบ Open License ที่มีลิขสิทธิ์รองรับการใช้งานไม่น้อยกว่า 2 ปี จำนวน 1 ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังนี้

4.3.1 มีระบบบริหารจัดการสำหรับคอมพิวเตอร์เสมือน ซึ่งมีความสามารถดังนี้

4.3.1.1 มีระบบ Single Sign-On เพื่อ Login เพียงครั้งเดียว ในกรณีที่มีระบบบริหารส่วนกลางสำหรับคอมพิวเตอร์เสมือนมากกว่า 1 ระบบ

4.3.1.2 มี API สำหรับการเชื่อมต่อกับ Third-Party Tools ต่าง ๆ ได้

4.3.2 มีระบบเครื่องคอมพิวเตอร์แม่ข่ายเสมือน ซึ่งมีคุณลักษณะอย่างน้อยดังนี้

4.3.2.1 มี API สำหรับการเชื่อมต่อกับ Third-Party Backup Software, Multipath Software

4.3.2.2 สามารถทำ High Availability (HA) โดยทำการ Restart คอมพิวเตอร์เสมือนได้โดยอัตโนมัติในกรณีที่ Hardware หรือ Operating System มีปัญหา โดยสามารถกำหนดลำดับการ Restart ของคอมพิวเตอร์เสมือน

4.3.2.3 สามารถจัดการพื้นที่ Disk บน Shared Storage ให้คอมพิวเตอร์เสมือนแบบ Thin Provisioning ได้

4.3.2.4 สามารถทำการย้ายคอมพิวเตอร์เสมือนข้ามไปมาระหว่าง Server ทั้งภายในคลัสเตอร์เดียวกันและต่างคลัสเตอร์ได้โดยไม่กระทบการทำงานของผู้ใช้งาน

4.3.2.5 สามารถทำงานแบบ Fault Tolerance เพื่อให้ Application ทำงานต่อเนื่องในกรณีที่ Hardware ของ Server มีปัญหา โดยรองรับการทำงาน (Workload) ที่ 8 Virtual CPUs

4.3.2.6 สามารถย้ายไฟล์ดิสก์ของคอมพิวเตอร์เสมือนข้ามไปมาระหว่าง Storage ได้โดยไม่มีผลกระทบกับผู้ใช้งาน

4.3.2.7 สามารถสร้างคอมพิวเตอร์แม่ข่ายเสมือนให้ใช้งานหน่วยความจำได้มากกว่าหน่วยความจำที่มีอยู่จริงบนเครื่องคอมพิวเตอร์แม่ข่าย (Memory Overcommitment)

4.3.2.8 มีระบบช่วยแบ่งเบาการทำงานของโปรแกรมป้องกันไวรัสคอมพิวเตอร์โดยไม่ต้องติดตั้ง Agent บนคอมพิวเตอร์เสมือน หรือเสนอระบบป้องกันภัยบุกรุก แบบ Virtual IPS

4.3.2.9 สามารถทำการ Replicate คอมพิวเตอร์เสมือนข้ามศูนย์คอมพิวเตอร์ได้ โดยมีค่า RPO (Recovery Point Objective) ไม่เกิน 15 นาที

4.3.2.10 สามารถตรวจสอบปัญหาที่จะเกิดขึ้นกับ Server ล่วงหน้า แล้วทำการย้ายคอมพิวเตอร์เสมือนไปที่ Server อื่น เพื่อไม่ให้มีผลกระทบกับผู้ใช้งาน (Proactive HA)

4.3.2.11 สามารถใช้งานกับ Reliable Memory เพื่อเพิ่มความเสถียรให้กับระบบโดยการนำส่วนที่สำคัญในการทำงาน เช่น Hypervisor เก็บใน Memory แบบ Reliable ในขณะใช้งาน

4.3.2.12 สามารถกำหนด Bandwidth (QoS) ในการใช้ Network และ Storage บนคอมพิวเตอร์เสมือนได้

4.3.2.13 สามารถทำ Load Balance หรือ Balance resource การใช้งาน Storage โดยการย้ายพื้นที่เก็บข้อมูลคอมพิวเตอร์เสมือนไปยัง Storage ที่เหมาะสมได้โดยอัตโนมัติ

4.3.2.14 สามารถทำการย้ายคอมพิวเตอร์เสมือนข้ามไปมาระหว่าง Server และข้ามระบบบริหารส่วนกลางได้โดยไม่กระทบการทำงานของผู้ใช้งาน

4.3.2.15 มีเครื่องมือในการวางแผนจัดการการอัพเดทเวอร์ชันของ Hypervisor, Patch, Driver และ Firmware โดยอ้างอิงกับ Hardware บน Server ที่ใช้ติดตั้งระบบแม่ข่ายคอมพิวเตอร์เสมือน

4.3.2.16 มีลิขสิทธิ์ถูกต้องรองรับการใช้งานครอบคลุมจำนวนหน่วยประมวลผลกลาง (Processor Core) ไม่น้อยกว่า 448 Cores

4.3.3 มีระบบจัดเก็บข้อมูลแบบเสมือนสำหรับระบบแม่ข่ายคอมพิวเตอร์เสมือน ซึ่งมีคุณลักษณะอย่างน้อยดังนี้

4.3.3.1 สามารถบริหารจัดการระบบจัดเก็บข้อมูลแบบเสมือน ได้โดยตรงจากระบบบริหารส่วนกลางสำหรับคอมพิวเตอร์เสมือนในรูปแบบ HTML5

4.3.3.2 เป็นระบบที่มีชุดควบคุมหรือจัดการทำงานในระดับ Kernel ของ Hypervisor

4.3.3.3 สามารถนำ SSD บน Server มาสร้างเป็น Shared Storage สำหรับเครื่องคอมพิวเตอร์เสมือน

4.3.3.4 สามารถใช้ Solid-State Drive (SSD) ที่มีอยู่บน Server มาทำ Cache เพื่อช่วยเพิ่มความเร็วในการเขียนและอ่านข้อมูล

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

4.3.3.5 สามารถกำหนด Storage Policy เช่น รูปแบบ RAID, จำนวน Disk ที่ Stripe, Thin Provisioning, Cache Reservation ให้ VM แต่ละ VM ได้

4.3.3.6 สามารถกำหนดกลุ่มของ Server เพื่อจัดการ Availability ในระดับ Rack Server ได้

4.3.3.7 สามารถกำหนดปริมาณการใช้งาน (QoS – Quality of Service) Storage ของ VM แต่ละ VM ได้ โดยกำหนดในนโยบาย Storage ของ VM

4.3.3.8 สามารถใช้งานเป็น Cloud Native Storage บน Container และสนับสนุนเครื่องมือที่ใช้ในการ Monitor ต่าง ๆ เช่น Prometheus

4.3.3.9 สามารถลดปริมาณของข้อมูลที่เขียนโดยการทำ Deduplication (ลดการซ้ำซ้อน) และ Compression (การบีบอัด) ข้อมูล

4.3.3.10 สามารถสร้าง Storage ของ VM ให้มีลักษณะแบบ Erasure Coding

4.3.3.11 มีลิขสิทธิ์ถูกต้องครอบคลุมความจุ Raw Capacity ที่เสนอตามข้อ 4.2 เครื่องคอมพิวเตอร์แม่ข่าย จำนวน 8 ชุด

4.4 ซอฟต์แวร์ระบบปฏิบัติการ Microsoft Windows Server Datacenter จำนวน 1 ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังนี้

เป็นลิขสิทธิ์ Microsoft Windows Server Datacenter เวอร์ชันล่าสุดสำหรับเครื่องคอมพิวเตอร์แม่ข่าย โดยรองรับหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า 280 แกนหลัก (280 Core) ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

4.5 ระบบตรวจจับการโจมตีและตอบสนองต่อภัยคุกคามไซเบอร์ จำนวน 150 ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังนี้

4.5.1 เป็นระบบหรือเป็น Platform ที่ออกแบบมาสำหรับป้องกันการโจมตีแบบ Extended Detection and Response (XDR) มาโดยเฉพาะ

4.5.2 มีโครงสร้างการบริหารจัดการแบบ Multi-tenant SaaS เพื่อให้สามารถบริหารจัดการ Policy ของแต่ละ Site ได้ตามที่กำหนด

4.5.3 สามารถกำหนดสิทธิ์สำหรับควบคุมการเข้าถึงระบบ (RBAC) ของแต่ละ User ได้

4.5.4 สามารถเก็บข้อมูลภัยคุกคามที่ตรวจพบได้ไม่น้อยกว่า 365 วัน

4.5.5 สามารถติดตั้ง Agent บนระบบปฏิบัติการของเครื่องคอมพิวเตอร์ปลายทาง (Endpoint) ดังนี้ Windows, Windows Server, MacOS, Linux, Container Platforms และ VDI ได้เป็นอย่างน้อย

4.5.6 ระบบที่นำเสนอต้องมี Maintenance Token หรือ Passphrase เพื่อป้องกันการถอนการติดตั้งโปรแกรมได้

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

4.5.7 ระบบที่นำเสนอต้องสามารถตรวจจับและป้องกันภัยคุกคามที่โจมตีบนเครื่องคอมพิวเตอร์ปลายทาง จากภัยคุกคามต่าง ๆ ได้ เช่น Known and unknown malware, Trojans, Hacking tools, Ransomware, Memory exploits, Script misuse และ Bad macros ได้เป็นอย่างน้อย

4.5.8 สามารถสั่งทำ Full Disk Scan ผ่านหน้าบริหารการจัดการ เพื่อค้นหาภัยคุกคามบนเครื่องคอมพิวเตอร์ปลายทาง

4.5.9 สามารถสืบค้นข้อมูลพฤติกรรมต้องสงสัย (Investigation and Hunting) และนำเสนอข้อมูลดังต่อไปนี้ได้เป็นอย่างน้อย

4.5.9.1 แสดงความสัมพันธ์ของแต่ละ Process ที่ต้องสงสัย (Process relationship)

4.5.9.2 แสดงข้อมูลตามลำดับเหตุการณ์ (Event Timeline)

4.5.9.3 จำแนกพฤติกรรมการโจมตีที่สอดคล้องตาม MITRE ATT&CK

4.5.9.4 สามารถจัดกลุ่มของข้อมูลตามประเภทได้ เช่น Processes, Indicators, Files, Network Actions, Registry, Logins เป็นต้น

4.5.9.5 สามารถ Custom Rules ในการตรวจจับเพิ่มเติมได้

4.5.10 สามารถทำการเก็บหลักฐานหรือข้อมูลการโจมตีที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ปลายทางเพื่อตรวจสอบย้อนหลังได้ไม่น้อยกว่า 14 วัน สำหรับค่าต่าง ๆ ในการค้นหา และรองรับการขยายในการเก็บข้อมูลได้ไม่น้อยกว่า 365 วัน

4.5.11 สามารถทำการกู้คืนระบบ (Rollback) ของคอมพิวเตอร์ปลายทาง โดยสามารถทำงานร่วมกับ Windows VSS snapshot เมื่อถูกโจมตีจาก Ransomware หรือ Malicious และรองรับการกู้คืนระบบแบบอัตโนมัติผ่านหน้าบริหารการจัดการ โดยไม่จำเป็นต้องเขียน Script เพื่อใช้ในการกู้คืน

4.5.12 สามารถทำ Remote Shell เพื่อให้ผู้ดูแลระบบ เข้ามาช่วยตรวจสอบการโจมตี และรวบรวมข้อมูลช่วยประหยัดเวลาในการช่วยเหลือได้อย่างมีประสิทธิภาพ

4.5.13 ระบบสามารถทำงานควบคุม Network Connectivity หรือ Firewall Control เพื่อควบคุมการเชื่อมต่อของคอมพิวเตอร์ปลายทางได้ โดยสามารถทำงานได้บนระบบปฏิบัติการทั้ง Windows, MacOS และ Linux ได้เป็นอย่างน้อย

4.5.14 สามารถควบคุมการใช้งานอุปกรณ์ (Device Control) เช่น Removable Media ผ่าน USB และ Bluetooth บนเครื่องคอมพิวเตอร์ปลายทางได้

4.5.15 ระบบสามารถแสดงรายการ Application ที่ติดตั้งบนเครื่องคอมพิวเตอร์ปลายทาง ผ่านหน้าบริหารการจัดการ รวมถึงตรวจสอบช่องโหว่บน Application ได้

4.5.16 ระบบสามารถควบคุมดำเนินการเครื่องคอมพิวเตอร์ปลายทางจากศูนย์กลางได้ หลังการถูกโจมตี เช่น Kill Process, Quarantine และ Remediate เพื่อทำการลบไฟล์อันตราย หรือไฟล์แปลกปลอม และค่าระบบที่ถูกเปลี่ยนแปลงโดยภัยคุกคาม

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

4.5.17 ระบบสามารถออกรายงานในรูปแบบต่าง ๆ ดังต่อไปนี้

4.5.17.1 Executive Insights

4.5.17.2 Applications Insights

4.5.17.3 Threats Insights

4.6 อุปกรณ์รักษาความปลอดภัย จำนวน 2 ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังนี้

4.6.1 เป็นอุปกรณ์ Next Generation Firewall แบบ Appliance ที่มี Module Slots อย่างน้อย 1 Slot และสามารถติดตั้งใน Rack ขนาด 19 นิ้วได้

4.6.2 มีอินเตอร์เฟสแบบ 10 Gigabit Ethernet แบบ SFP+ ไม่น้อยกว่า 4 พอร์ต พร้อม Transceiver SFP+ แบบ Single Mode

4.6.3 มีอินเตอร์เฟสแบบ Copper Ethernet 10/100/1000 หรือดีกว่า ไม่น้อยกว่า 8 พอร์ต

4.6.4 สามารถใช้งานได้บนเครือข่าย IPv4 และ IPv6 ได้

4.6.5 มี Throughput สำหรับการทำงาน Firewall ไม่น้อยกว่า 80 Gbps

4.6.6 มี Throughput สำหรับการตรวจสอบ NGIPS ได้ไม่น้อยกว่า 5 Gbps

4.6.7 มีความสามารถในการรองรับการเชื่อมต่อ Concurrent Connections หรือ Concurrent Sessions ไม่น้อยกว่า 17,000,000 Connections หรือ Session และรับการเชื่อมต่อ New TCP Connections หรือ New TCP Sessions ได้ไม่น้อยกว่า 350,000 เป็นอย่างน้อย

4.6.8 สามารถทำ Automatic Anti-Spoofing ให้อัตโนมัติ

4.6.9 สามารถทำงานในลักษณะ High Availability (HA) หรือ Clustering Firewall แบบ Active-Active หรือ Active-Standby

4.6.10 สามารถทำ Application Control ได้

4.6.11 สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่าง ๆ อย่างน้อย ดังนี้ Syn Flood หรือ UDP Flood หรือ ICMP Flood หรือ RST Flood, IP Address Spoofing, Port Scan, DoS หรือ DDoS, Teardrop Attack หรือ Land Attack หรือ IP Fragment หรือ ICMP Fragment เป็นต้นได้

4.6.12 สามารถทำ Server Load Balancing ได้

4.6.13 สามารถทำการตรวจสอบการโจมตีได้หลายลักษณะ เช่น Full-Steam Deep Inspection, Dynamic Context Detection, Vulnerability Exploit Detection, Anti-Botnet และสามารถทำการ Custom Fingerprinting ได้เป็นอย่างน้อย

4.6.14 มีสิทธิในการทำ Virtual Contexts ได้ไม่น้อยกว่า 10 Virtual และรองรับการขยายไม่น้อยกว่า 100 Virtual ได้ในอนาคต

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

4.6.15 มีระบบบริหารจัดการแบบส่วนกลาง (Centralize Management) จำนวน 1 ระบบ โดยมีคุณสมบัติอย่างน้อยดังนี้

4.6.15.1 เป็นอุปกรณ์ หรือระบบซอฟต์แวร์ที่สามารถติดตั้งได้บนระบบปฏิบัติการ Windows หรือ Linux ได้ โดยทำหน้าที่ในการบริหารจัดการอุปกรณ์รักษาความปลอดภัย (Next Generation Firewall)

4.6.15.2 มีระบบในการจัดเก็บข้อมูล Traffic Log ของอุปกรณ์ที่เสนอในโครงการ โดยสามารถจัดเก็บข้อมูล Log Records หรือ Collector Rate ได้ไม่น้อยกว่า 100,000 Records Per Second

4.6.15.3 สามารถทำ Policy Validation และ Policy Snapshots ได้เพื่อง่ายต่อการตรวจสอบความถูกต้องของ Policy ก่อนการ Deploy Policies จริงเพื่อป้องกันความผิดพลาดในการใช้งานได้ พร้อมทั้งสามารถสร้าง Policy แบบ Jump Rule ได้เพื่อเพิ่มประสิทธิภาพการทำงานของอุปกรณ์ให้ดียิ่งขึ้น

4.6.15.4 สามารถแสดงแผนภาพสถานะของการทำงานในลักษณะ Geo-locations, Networks Diagrams, Real-Time System Status และ Top-Rate Statistics ได้เป็นอย่างน้อย

4.6.15.5 สามารถทำการ Customize Dashboard หรือ Overview ข้อมูล Real-Time System Status และ Top-Rate Statistics ได้ และสามารถตั้ง Threshold เพื่อแจ้งเตือนเมื่อค่าเกินที่กำหนดได้

4.6.15.6 สามารถ Filtering Log ด้วยการ Drag and Dropping Log จาก Fields ได้ และสามารถสร้าง Rule จาก Log ได้

4.6.15.7 สามารถทำการแสดง Log Analysis ในรูปแบบแผนภาพการโจมตี (Log Visualization) เช่น Attack Analysis, Network Application and Client Executable Usage และสามารทำ Log Aggregations ได้เป็นอย่างน้อย

4.6.15.8 มีระบบการทำ Fail-Safe ทั้งในส่วนของ Policy Upload และ Remote Upgrade Firmware เพื่อป้องกันความผิดพลาดในกรณีที่มีการ Upload ข้อมูลที่ไม่สมบูรณ์ไปอุปกรณ์

4.6.15.9 มีระบบ Incident Management เพื่อช่วยผู้ดูแลระบบแก้ไขปัญหา

4.6.15.10 สามารถตรวจสอบ และติดตามสถานการณ์ทำงานของอุปกรณ์อื่น ๆ ได้ เช่น Router หรือ Switch เป็นต้น และสามารถทำการรับข้อมูล เช่น Log, NetFlow มาทำการวิเคราะห์ร่วมกันกับอุปกรณ์ที่เสนอในโครงการได้

4.6.15.11 สามารถออกรายงานแบบ Schedule Report ได้ เช่น รายงาน Botnet Daily Summary, Inspection Alert Summary, Evasion Summary, Vulnerability Summary และ Application & Web Security Summary เป็นอย่างน้อย

4.6.15.12 สามารถทำงานร่วมกับระบบบริหารจัดการระบบรักษาความปลอดภัย (Security Management Center) ที่ สศค. ใช้งานอยู่ในปัจจุบัน

4.6.16 มีลิขสิทธิ์การใช้งานไม่น้อยกว่า 2 ปี

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

4.7 ระบบบริการจัดการรหัสผ่านและบริหารจัดการเซสชั่น จำนวน 1 ระบบ โดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังนี้

4.7.1 เป็นระบบที่ถูกออกแบบมาสำหรับทำหน้าที่ในการบริหารจัดการรหัสผ่านและควบคุมสิทธิหรือเซสชั่น (Session) ในการเข้าถึงเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายในลักษณะ Privileged Access Management (PAM) โดยเฉพาะ

4.7.2 สามารถทำการระบบบริหารจัดการผ่านทาง Web Browser ได้

4.7.3 รองรับทำงานในลักษณะ High availability (HA) แบบ Active-Standby หรือ Active-Active ได้

4.7.4 มีสิทธิในการบริหารจัดการผู้ใช้งานหรือ Privileged Account หรือ Admin User ได้ไม่น้อยกว่า 20 User และบริหารจัดการอุปกรณ์ได้ไม่น้อยกว่า 300 อุปกรณ์ โดยเป็นสิทธิการใช้งานในลักษณะ Perpetual License

4.7.5 สามารถทำการควบคุมการขอใช้และเปลี่ยน Password ของระบบหรืออุปกรณ์ต่าง ๆ เช่น Windows, Linux, Unix, Router และ Network Switch ได้เป็นอย่างน้อย

4.7.6 สามารถทำการนำเข้าบัญชีผู้ใช้งานจากระบบ Active Directory และ LDAP เข้ามายังระบบ Privileged Access Management ได้

4.7.7 สามารถกำหนดสิทธิผู้ใช้งานของ PAM Users ในการเข้าถึงเครื่องแม่ข่ายและอุปกรณ์เครือข่าย ในระดับสิทธิต่าง ๆ ของเครื่องแม่ข่ายและอุปกรณ์เครือข่ายนั้น ๆโดยวิธีการ Map Users หรือ Shared Accounts Password Management (SAPM) ได้เป็นอย่างน้อย

4.7.8 สามารถทำการควบคุมและติดตามการเข้าถึงระบบหรืออุปกรณ์ปลายทาง (Session Management) ได้ ผ่าน SSH, Telnet, RDP, VNC, HTTP หรือ HTTPS, SFTP หรือ Database Connections (SQL) ได้เป็นอย่างน้อย

4.7.9 ในกรณีที่มีการใช้งานผ่าน RDP และ VNC และ SSH หรือ Telnet ระบบต้องสามารถทำการบันทึกการใช้งาน (Session Record) ในลักษณะ Video Record และสามารถทำการดูย้อนหลัง (Video Playback) ได้

4.7.10 มีระบบ Object Character Recognition (OCR) เพื่อใช้ในการค้นหา Keywords หรือ Commands ที่ทำการบันทึกใน Session Record ได้

4.7.11 สามารถกำหนดนโยบาย Policy Key Definition ในการควบคุมชุดคำสั่งที่สำคัญสำหรับผู้ใช้งาน เช่น ชุดคำสั่งต้องห้าม (Black Key) และชุดคำสั่งที่สามมารถใช้งานได้ (White Key) ได้เป็นอย่างน้อย

4.7.12 มีระบบในการขออนุมัติใช้ชุดคำสั่ง (Managerial Approval For Command) เช่น ขออนุมัติใช้งานชุดคำสั่งต้องห้าม (Black Key) และ สามารถทำการกำหนดระยะเวลาในการใช้งาน (Managerial Approval Reservation) ได้เป็นอย่างน้อย

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

4.7.13 สามารถตรวจสอบการใช้งาน Session ในลักษณะ Active Session ได้ โดยผู้ดูแลระบบสามารถทำการปิดหรือระงับการใช้งาน Session ที่ไม่ต้องการได้ เช่น Kill Session และ Kill Session with Logoff ได้เป็นอย่างน้อย

4.7.14 สามารถทำการ Monitor Session ที่ต้องการแบบ Real Time ในลักษณะ Wire to Session ได้

4.7.15 สามารถทำการค้นหาข้อมูลการเข้าใช้งานของ อุปกรณ์ หรือ Session นั้น ๆ ได้ เช่น ทำการค้นหาจาก Device Group, IP, Host Name, Protocol, User Name, Client IP, Command, Policy Name, Time Start และ Time Stop ได้เป็นอย่างน้อย

4.7.16 สามารถทำ Two Factor Authentication (2FA) ร่วมกับ Mobile Application สำหรับการเข้าใช้งานระบบได้

4.7.17 รองรับการทำ Jump Host ได้ไม่น้อยกว่า 20 Jump Host

4.7.18 สามารถงานในลักษณะ SSH Proxy, SFTP Proxy, RDP Proxy, HTTP หรือ HTTPS Proxy ในตัวเองได้โดยไม่ต้องพึ่งพาระบบ External Jump Host ได้

4.7.19 สามารถทำ Task Automation ในลักษณะ Workflow โดยรองรับการออกแบบการทำงานของ Task เช่น Pre-check, Execution และ Post-check ได้ หรือสามารถทำ Job Scheduler สำหรับการ Run Jobs หรือ Tasks ได้อัตโนมัติ

4.8 ระบบประเมินและตรวจสอบช่องโหว่ภายในเครือข่าย จำนวน 1 ระบบ โดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังนี้

4.8.1 โปรแกรมที่นำเสนอต้องถูกออกแบบมาเพื่อทำหน้าที่ตรวจสอบและประเมินความเสี่ยงจากช่องโหว่ (Vulnerability) โดยเฉพาะ

4.8.2 สามารถทำการตรวจหาช่องโหว่ในระบบได้แบบไม่จำกัดจำนวน IP Address

4.8.3 สามารถบริหารจัดการได้ผ่าน Web Based GUI แบบ HTTPS

4.8.4 สามารถทำการตรวจสอบ (Scan) ได้หลากหลาย เช่น แบบ Non-Credentialed หรือ Credentialed ได้เป็นอย่างน้อย

4.8.5 สามารถตรวจสอบช่องโหว่ภายในระบบเครือข่ายผ่าน IPv4 หรือ IPv6 ได้

4.8.6 สามารถทำการตรวจสอบช่องโหว่ของอุปกรณ์เครือข่าย เช่น Cisco, Juniper, HP, F5 และ SonicWall ได้

4.8.7 สามารถทำการตรวจสอบช่องโหว่ของระบบฐานข้อมูลได้ เช่น Oracle หรือ SQL Server หรือ MySQL ได้

4.8.8 สามารถตรวจสอบช่องโหว่ของระบบปฏิบัติการคอมพิวเตอร์ เช่น Windows, MacOS, Linux ได้

4.8.9 สามารถทำการตั้งเวลาการ Scan ล่วงหน้าได้

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

4.8.10 มี Templates สำหรับทำการตรวจสอบ Compliance และ Configuration อย่างน้อย 400 Templates

4.8.11 มีระบบ Threat Detection เช่น สามารถตรวจสอบ Backdoor, Malware หรือ Botnet ได้เป็นอย่างน้อย

4.8.12 มีฐานข้อมูลของช่องโหว่ (Plugin) ไม่น้อยกว่า 150,000 Plugins

4.8.13 มีฐานข้อมูลของช่องโหว่ที่ครอบคลุมมาตรฐาน Common Vulnerabilities and Exposures (CVE) ไม่น้อยกว่า 60,000 CVE IDs

4.8.14 สามารถอัพเดทฐานข้อมูลของช่องโหว่ได้โดยอัตโนมัติ

4.8.15 สามารถทำการ Scan ในการหาช่องโหว่โดยอ้างอิงมาตรฐานด้านความปลอดภัย เช่น SCAP หรือ CIS หรือ PCI ได้

4.8.16 สามารถจัดลำดับความรุนแรงของช่องโหว่ตามมาตรฐาน Common Vulnerability Scoring System (CVSS) ได้

4.8.17 สามารถออกรายงานในรูปแบบ PDF หรือ HTML หรือ CSV formats ได้

4.8.18 มีลิขสิทธิ์การใช้งานอย่างน้อย 2 ปี

4.9 การย้ายระบบ จำนวน 1 งาน โดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังนี้

4.9.1 สำรวจระบบงานที่ติดตั้งบนที่อยู่ในระบบคลาวด์เดิมของ สศค. ดังนี้

4.9.1.1 พื้นที่ติดตั้งอุปกรณ์และการเชื่อมต่อ

4.9.1.2 รายระเอียด IP Address ของแต่ละอุปกรณ์และระบบ

4.9.1.3 ค่า Policy และ Flow การทำงานของระบบ

4.9.2 ตรวจสอบสถานะการทำงานของระบบที่อยู่ในระบบคลาวด์เดิมของ สศค. ว่า Virtual มีเปิดหรือปิดการใช้งาน

4.9.3 จัดทำ Check List และทดสอบการทำงานของระบบต่างๆ ที่อยู่ในระบบคลาวด์เดิมของ สศค.

4.9.4 ทำการ Backup ค่า Configuration หรือ Virtual ที่อยู่ในระบบคลาวด์เดิมของ สศค. ก่อนที่จะมีการโอนย้ายระบบ

4.9.5 ดำเนินการโอนย้ายระบบงานที่อยู่ในระบบคลาวด์เดิมของ สศค. ไปยังระบบคลาวด์คอมพิวเตอร์ใหม่ที่เสนอ จำนวนอย่างน้อย 17 ระบบ ดังนี้

4.9.5.1 ระบบ Web Portal

4.9.5.2 ระบบบริหารจัดการโครงสร้างองค์กร (Staff Directory)

4.9.5.3 ระบบบริหารจัดการวัสดุและครุภัณฑ์

4.9.5.4 ระบบจองรถยนต์

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

4.9.5.5 ระบบจองห้องประชุม

4.9.5.6 เว็บไซต์สำนักงานเศรษฐกิจการคลัง

4.9.5.7 เว็บไซต์ 1359.go.th

4.9.5.8 ระบบสารบรรณอิเล็กทรอนิกส์

4.9.5.9 ระบบแบบฟอร์มอิเล็กทรอนิกส์ (e-Form)

4.9.5.10 ระบบลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature)

4.9.5.11 ระบบสร้างและจัดเก็บเอกสารกลางอิเล็กทรอนิกส์

4.9.5.12 ระบบการลงเวลาและการลาอิเล็กทรอนิกส์

4.9.5.13 ระบบ Mail

4.9.5.14 ระบบ Active Directory

4.9.5.15 ระบบการคำนวณและเผยแพร่อัตราเงินชดเชยค่าภาษีสินค้าส่งออกที่ผลิตในราชอาณาจักร

4.9.5.16 ระบบ PDPA

4.9.5.17 ระบบบริหารจัดการฐานข้อมูลกลางด้านเศรษฐกิจการคลัง ระยะที่ 2 (DOC Phase II)

4.9.5.18 ดำเนินการย้าย VM ระบบอื่นที่ทำงานบนระบบคลาวด์เดิมของ สศค. ไปจัดเก็บบนระบบคลาวด์ในโครงการ

4.9.6 ทำการทดสอบตาม Check List เดิมระบบต่างๆ ที่อยู่ในระบบคลาวด์คอมพิวเตอร์ใหม่ที่เสนอ

4.9.7 Monitor การทำงานของระบบงานต่างๆ หลังจากมีการย้ายมาอยู่ในระบบคลาวด์คอมพิวเตอร์ใหม่ที่เสนอ

4.9.8 ผู้ชนะการประกวดราคาต้องติดตั้งระบบสารบรรณอิเล็กทรอนิกส์ แบบฟอร์ม ระบบลงนามอิเล็กทรอนิกส์ และระบบจัดเก็บค้นหาเอกสารกลางอิเล็กทรอนิกส์ (ผลิตภัณฑ์ Infoma รุ่น WebFlow และผลิตภัณฑ์ Infoma รุ่น WebForm) ที่ สศค. ใช้งานอยู่ บนเครื่องแม่ข่ายที่จัดเตรียมใหม่ และโอนย้ายข้อมูลดัชนีไฟล์เอกสารแนบทั้งหมดพร้อมตรวจสอบ ตามรายละเอียดดังนี้

4.9.8.1 ผู้ชนะการประกวดราคาต้องติดตั้งโปรแกรมระบบสารบรรณอิเล็กทรอนิกส์แบบฟอร์ม ระบบลงนามอิเล็กทรอนิกส์ และ ระบบจัดเก็บค้นหาเอกสารกลางอิเล็กทรอนิกส์พร้อมสิทธิ์การใช้งาน (License) บนเครื่องแม่ข่ายที่จัดเตรียมไว้

4.9.8.2 ผู้ชนะการประกวดราคาต้องตรวจสอบข้อมูลความพร้อมและจำนวนข้อมูลก่อนการโอน, โอนย้ายข้อมูล ดัชนี ไฟล์เอกสารแนบมาติดตั้งบนเครื่องแม่ข่ายที่จัดเตรียมไว้ และทดสอบระบบ

4.9.8.3 ผู้ชนะการประกวดราคาต้องจัดทำรายงานการติดตั้งระบบสารบรรณอิเล็กทรอนิกส์สำหรับการติดตั้งบนเครื่องแม่ข่ายใหม่

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

4.9.8.4 ผู้ชนะการประกวดราคาต้องจัดทำรายงานสรุปจำนวนข้อมูลดัชนี และจำนวนไฟล์เอกสารแนบ โดยเปรียบเทียบข้อมูลก่อนการโอนและหลังการโอนย้ายข้อมูลระบบสารบรรณอิเล็กทรอนิกส์

5. กำหนดเวลาส่งมอบพัสดุ

ผู้ชนะการประกวดราคาจะต้องส่งมอบอุปกรณ์และติดตั้งอุปกรณ์พร้อมซอฟต์แวร์ทั้งหมด ให้แล้วเสร็จภายใน 240 วัน นับถัดจากวันลงนามในสัญญา โดยแบ่งการส่งมอบงานเป็น 4 งวด ดังนี้

งวดที่ 1: ภายใน 30 วัน นับถัดจากวันลงนามในสัญญา โดยมีงานที่ต้องดำเนินการ ดังนี้

- ส่งมอบแผนการดำเนินงานของโครงการ
- ส่งมอบรายงานการออกแบบสถานที่ติดตั้งคอมพิวเตอร์ รวมทั้งระบบอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วย แผนผังตำแหน่งการติดตั้งอุปกรณ์ แผนผังการเชื่อมต่อของระบบ

งวดที่ 2: ภายใน 180 วัน นับถัดจากวันลงนามในสัญญา โดยมีงานที่ต้องดำเนินการ ดังนี้

- ส่งมอบอุปกรณ์ที่จะติดตั้งตามข้อ 4.1, 4.2 และ 4.6
- ส่งมอบรายงานผลสรุปการศึกษา วิเคราะห์และผลสำรวจความต้องการของผู้ใช้งานของระบบเครือข่าย

งวดที่ 3: ภายใน 210 วัน นับถัดจากวันลงนามในสัญญา โดยมีงานที่ต้องดำเนินการ ดังนี้

- ส่งมอบรายงานการติดตั้งอุปกรณ์และระบบที่ติดตั้งสำเร็จแล้วตามข้อ 4. รายละเอียดคุณลักษณะเฉพาะและข้อกำหนด
- ส่งมอบรายงานการทดสอบอุปกรณ์และระบบส่งมอบ License ของอุปกรณ์และซอฟต์แวร์ของระบบ

งวดที่ 4: ภายใน 240 วัน นับถัดจากวันลงนามในสัญญา โดยมีงานที่ต้องดำเนินการ ดังนี้

- จัดการฝึกอบรมเจ้าหน้าที่ และส่งมอบรายงานการฝึกอบรมเจ้าหน้าที่
- ส่งมอบเอกสารหรือคู่มือปฏิบัติงานสำหรับผู้ใช้ (User Manual)
- ส่งมอบเอกสารหรือคู่มือปฏิบัติงานสำหรับเจ้าหน้าที่ดูแลระบบ พร้อม Username และ Password สำหรับบริหารจัดการ
- นำระบบที่สมบูรณ์แล้วทั้งหมดในโครงการออกปฏิบัติงานจริง

6. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการยื่นข้อเสนอครั้งนี้ สศค. จะพิจารณาตัดสินจากเกณฑ์ราคาโดยใช้ราคาต่ำสุด เป็นผู้ชนะการประกวดราคา

7. วงเงินงบประมาณ/วงเงินที่ได้รับจัดสรร

เบิกจ่ายจากงบประมาณปี พ.ศ. 2568 วงเงินงบประมาณ 69,646,000 บาท (หกสิบเก้าล้านหกแสนสี่หมื่นหกพันบาทถ้วน) รวมภาษีมูลค่าเพิ่มแล้ว

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

8. งวดงานและการจ่ายเงิน

สศค. จะชำระเงิน โดยแบ่งออกเป็น 4 งวด ดังนี้

<u>งวดที่ 1:</u> เป็นจำนวนเงินในอัตราร้อยละ 5 ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและได้รับการตรวจรับงานงวดที่ 1 เสร็จ สิ้นสมบูรณ์

<u>งวดที่ 2:</u> เป็นจำนวนเงินในอัตราร้อยละ 30 ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและได้รับการตรวจรับงานงวดที่ 2 เสร็จสิ้นสมบูรณ์

<u>งวดที่ 3:</u> เป็นจำนวนเงินในอัตราร้อยละ 45 ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและได้รับการตรวจรับงานงวดที่ 3 เสร็จสิ้นสมบูรณ์

<u>งวดที่ 4:</u> เป็นจำนวนเงินในอัตราร้อยละ 20 ของวงเงินตามสัญญา ภายหลังที่ได้ทำการส่งมอบและได้รับการตรวจรับงานงวดที่ 4 เสร็จสิ้นสมบูรณ์

9. อัตราค่าปรับ

กรณีที่ผู้ชนะการประกวดราคาไม่สามารถส่งมอบพัสดุได้ตามเงื่อนไขที่กำหนดไว้ในเอกสารนี้ ผู้ชนะการประกวดราคาจะต้องเสียค่าปรับให้ในอัตราร้อยละ 0.2 ของมูลค่าตามสัญญาต่อวัน

10. การกำหนดระยะเวลารับประกันความชำรุดบกพร่อง

10.1 ผู้ชนะการประกวดราคาตกลงรับประกันความชำรุดบกพร่องหรือขัดข้องของคอมพิวเตอร์และการติดตั้งตามสัญญาเป็นเวลา 1 ปี ในรายการ 4.1, 4.2, 4.4, 4.5, 4.7 และ 2 ปี ในรายการ 4.3, 4.6, 4.8 นับถัดจากวันที่ สศค. ได้รับมอบคอมพิวเตอร์ทั้งหมดโดยถูกต้องครบถ้วนตามสัญญา และดำเนินการตรวจรับโครงการเสร็จสิ้นสมบูรณ์แล้ว โดยการรับประกันค่าแรงพร้อมอะไหล่ และบริการ ณ สถานที่ติดตั้ง (Onsite Service Warranty) โดยไม่คิดมูลค่าใด ๆ ทั้งสิ้น

ถ้าภายในระยะเวลาดังกล่าวคอมพิวเตอร์ชำรุดบกพร่องหรือขัดข้อง หรือใช้งานไม่ได้ทั้งหมดหรือแต่บางส่วน หรือเกิดความชำรุดบกพร่องหรือขัดข้องจากการติดตั้ง เว้นแต่ความชำรุดบกพร่องหรือขัดข้องดังกล่าวเกิดขึ้นจากความผิดของ สศค. ซึ่งไม่ได้เกิดขึ้นจากการใช้งานตามปกติ ผู้ชนะการประกวดราคาจะต้องจัดการซ่อมแซมแก้ไขให้เสร็จเรียบร้อยและอยู่ในสภาพใช้การได้ดีดังเดิม โดยต้องเริ่มจัดการซ่อมแซมแก้ไขภายใน 2 ชั่วโมง ด้วยการ Online/Remote หรือ On-site นับถัดจากที่ได้รับแจ้งจาก สศค. โดยไม่คิดค่าใช้จ่ายใด ๆ จาก สศค. ทั้งสิ้น

กรณีผู้ชนะการประกวดราคาไม่สามารถ แก้ไข หรือซ่อมแซม หรือเปลี่ยนใหม่ได้ภายใน 6 ชั่วโมง ผู้ชนะการประกวดราคาต้องนำเครื่องสำรองที่มีประสิทธิภาพทัดเทียมกันหรือดีกว่ามาใช้งานแทนภายใน 10 ชั่วโมง จนกว่าจะแก้ไขหรือซ่อมแซมหรือเปลี่ยนใหม่ ให้แล้วเสร็จสมบูรณ์

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

กรณีที่ผู้ชนะประกวดราคาไม่สามารถจัดหาเครื่องสำรองที่มีประสิทธิภาพทัดเทียมกันหรือดีกว่ามาใช้งานแทนได้ สศค. มีสิทธิที่จะทำการนั้นเองหรือจ้างผู้อื่นทำการนั้นแทนผู้ชนะการประกวดราคา โดยผู้ชนะการประกวดราคาต้องออกค่าใช้จ่ายเองทั้งสิ้นแทน สศค.

10.2 ผู้ชนะการประกวดราคามีหน้าที่บำรุงรักษาและซ่อมแซมแก้ไขคอมพิวเตอร์ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอตลอดระยะเวลาดังกล่าวตามข้อ 10.1 ด้วยค่าใช้จ่ายของผู้ชนะการประกวดราคา โดยให้มีเวลาคอมพิวเตอร์ขัดข้องรวมตามเกณฑ์การคำนวณเวลาขัดข้องไม่เกินเดือนละ 12 ชั่วโมง หรือร้อยละ 1.67 ของเวลาใช้งานทั้งหมดของคอมพิวเตอร์ของเดือนนั้น แล้วแต่ตัวเลขใดจะมากกว่ากัน มิฉะนั้นผู้ชนะการประกวดราคาต้องยอมให้ สศค. คิดค่าปรับเป็นรายชั่วโมง ในอัตราร้อยละ 0.035 ของราคาคอมพิวเตอร์ทั้งหมดตามสัญญาในช่วงเวลาที่ไม่สามารถใช้คอมพิวเตอร์ได้ในส่วนที่เกินกว่ากำหนดเวลาขัดข้องข้างต้น

เกณฑ์การคำนวณเวลาขัดข้องของคอมพิวเตอร์ ตามข้อ 10.2 ให้เป็นดังนี้

- กรณีที่คอมพิวเตอร์เกิดขัดข้องพร้อมกันหลายหน่วย ให้นับเวลาขัดข้องของหน่วยที่มีตัวถ่วงมากที่สุดเพียงหน่วยเดียว

- กรณีความเสียหายอันสืบเนื่องมาจากความขัดข้องของคอมพิวเตอร์แตกต่างกัน เวลาที่ใช้ในการคำนวณค่าปรับจะเท่ากับเวลาขัดข้องของคอมพิวเตอร์หน่วยนั้นคูณด้วยตัวถ่วง

โดยพิจารณาจากบัญชีของ สศค. โดยมีเกณฑ์การคำนวณนับชั่วโมงและค่าตัวถ่วงเป็นดังนี้

ก. จำนวนชั่วโมงที่ขัดข้องในขณะใดขณะหนึ่งเท่ากับค่าสูงสุดของจำนวนชั่วโมงที่ขัดข้องในขณะนั้นของระบบคอมพิวเตอร์แต่ละระบบ คูณด้วยค่าตัวถ่วง

จำนวนชั่วโมง = ค่าสูงสุด (ชั่วโมงที่ขัดข้อง x ค่าตัวถ่วง)

เศษชั่วโมงนับเป็น 1 ชั่วโมง

ข. ค่าปรับ = ร้อยละ 0.035 x (ผลรวมจำนวนชั่วโมง - 12) x มูลค่าตามสัญญาซื้อฯ

ค. กำหนดค่าตัวถ่วงของระบบคอมพิวเตอร์

ลำดับที่	รายการ	ค่าตัวถ่วง
1	อุปกรณ์กระจายสัญญาณ	1
2	เครื่องคอมพิวเตอร์แม่ข่าย	1
3	ซอฟต์แวร์ระบบคอมพิวเตอร์แม่ข่ายเสมือน	1
4	ซอฟต์แวร์ระบบปฏิบัติการ	1
5	ระบบตรวจจับการโจมตีและตอบสนองต่อภัยคุกคามไซเบอร์	1
6	อุปกรณ์รักษาความปลอดภัย	1
7	ระบบบริการจัดการรหัสผ่านและบริหารจัดการเซสชั่น	1
8	ระบบประเมินและตรวจสอบช่องโหว่ภายในเครือข่าย	1

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

ลำดับที่	รายการ	ค่าตัวถ่วง
9	การย้ายระบบ	-

10.3 ผู้ชนะการประกวดราคาจะต้องชำระค่าปรับตามข้อ 10.2 ให้แก่ สศค. ภายใน 7 วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจาก สศค. หากผู้ชนะการประกวดราคาไม่ชำระค่าปรับตามที่ได้รับแจ้งจาก สศค. ภายในเวลาที่กำหนด สศค. มีสิทธิบังคับเอาจากหลักประกันการปฏิบัติตามสัญญาได้

การที่ สศค. ทำการนั้นเอง หรือให้ผู้อื่นทำการนั้นแทนผู้ชนะการประกวดราคา ไม่ทำให้ผู้ชนะการประกวดราคาหลุดพ้นจากความรับผิดตามสัญญา หากผู้ชนะการประกวดราคา ไม่ชดใช้ค่าใช้จ่ายหรือค่าเสียหายตามที่ สศค. เรียกร้อง สศค. มีสิทธิบังคับจากหลักประกันการปฏิบัติตามสัญญาได้

10.4 เมื่อเกิดเหตุขัดข้อง สศค. สามารถแจ้งเหตุได้ตลอด 24 ชั่วโมง โดยช่องทางดังต่อไปนี้

10.4.1 ติดต่อผ่าน E-mail

10.4.2 ติดต่อผ่านโทรศัพท์สายด่วน (Hotline/Helpdesk/Call Center) หรือโทรศัพท์เคลื่อนที่

10.4.3 ติดต่อผ่าน Instant messaging

10.5 คุณสมบัติของอะไหล่ ชิ้นส่วน หรืออุปกรณ์ใด ๆ ที่ใช้ในการเปลี่ยนหรือทดแทนชั่วคราว

10.5.1 กรณีเปลี่ยนอะไหล่ ชิ้นส่วน หรืออุปกรณ์ใด ๆ ที่ใช้ในการเปลี่ยน ต้องมีคุณสมบัติไม่ด้อยกว่าอะไหล่ ชิ้นส่วน หรืออุปกรณ์เดิมในทุกกรณี และต้องเป็นของใหม่ที่ยังไม่เคยผ่านการใช้งานมาก่อน และสามารถใช้งานร่วมกับระบบเดิมได้เป็นอย่างดี โดยต้องเป็นอะไหล่จากเจ้าของผลิตภัณฑ์โดยตรง

10.5.2 กรณีที่อะไหล่ ชิ้นส่วน หรืออุปกรณ์ใด ๆ เพื่อนำมาใช้ทดแทนชั่วคราว ต้องมีคุณสมบัติไม่ด้อยกว่าอะไหล่ ชิ้นส่วน หรืออุปกรณ์เดิมในทุกกรณี และสามารถใช้งานร่วมกับระบบเดิมได้โดยไม่ก่อให้เกิดปัญหาใด ๆ

10.6 เมื่อมีการตรวจสอบ/แก้ไขใด ๆ ผู้ชนะการประกวดราคาต้องส่งรายงานให้ สศค. ทุกครั้งภายใน 3 วันทำการนับจากวันที่ได้ดำเนินการแล้วเสร็จ โดยระบุวัน เวลา สถานที่ อาการ สาเหตุ การตรวจสอบ/แก้ไข และสถานภาพสุดท้ายของอุปกรณ์ และในกรณีที่เกิดความล่าช้าในการตรวจสอบแก้ไข ผู้ชนะการประกวดราคาจะต้องส่งรายงานความคืบหน้าให้ สศค. ทราบเป็นระยะจนกว่าจะดำเนินการแล้วเสร็จ

10.7 หากเกิดความเสียหายใด ๆ ซึ่งก่อให้เกิดความชำรุดบกพร่องหรือเกิดความสูญเสีย หรือความเสียหายแก่ทรัพย์สินของ สศค. อันเป็นผลสืบเนื่องมาจากการกระทำหรือละเว้นการกระทำของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาต้องรับผิดชอบชดใช้ค่าเสียหายแก่ สศค. ตามจำนวนที่เสียหายจริงภายในระยะเวลาที่ สศค.กำหนด

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

11. การเสนอราคา

ผู้ยื่นข้อเสนอต้องยื่นเอกสารผ่านระบบ e-GP ของกรมบัญชีกลาง โดยผู้ยื่นข้อเสนอต้องนำเสนอรายละเอียดเป็นตารางการเปรียบเทียบคุณสมบัติ ตามรูปแบบดังนี้

คุณลักษณะเฉพาะและข้อกำหนด (งานซื้อ) ที่ สศค. กำหนด	คุณสมบัติที่ผู้ยื่นข้อเสนอ เสนอ	เปรียบเทียบคุณสมบัติ หรือขอบเขตการดำเนินงานที่ผู้ยื่นข้อเสนอ เสนอ	เอกสารอ้างอิง
ให้คัดลอกคุณสมบัติที่ สศค. กำหนด หรือขอบเขตการดำเนินงานที่ สศค. กำหนด	ให้ระบุคุณสมบัติที่ผู้ยื่นข้อเสนอเสนอ พร้อมทั้งระบุยี่ห้อและรุ่น	ให้ระบุจุดที่ดีกว่า หรือเทียบเท่า	ให้ระบุเอกสารอ้างอิงหรือหนังสือรับรองจากผู้ผลิต (ถ้ามี)

ผู้ยื่นข้อเสนอจะต้องเสนอกำหนดยืนราคาไม่น้อยกว่า 90 วัน นับแต่วันที่ยืนยันราคาสุดท้าย โดยภายในกำหนดยืนราคา ผู้ยื่นข้อเสนอหรือผู้มีสิทธิเสนอราคาจะต้องรับผิดชอบราคาที่ตนได้เสนอไว้และจะถอนการเสนอราคามิได้

12. การติดตั้งและทดสอบอุปกรณ์ในโครงการ

12.1 ผู้ชนะการประกวดราคาต้องติดตั้งอุปกรณ์ในโครงการ ณ ห้องเซิร์ฟเวอร์ของ สศค. หรือสถานที่ตามที่ สศค. กำหนดอย่างถูกต้องครบถ้วน และการปรับตั้งค่า (Configuration) ของอุปกรณ์และระบบพร้อมทดสอบการทำงานของอุปกรณ์และระบบ

12.2 ในกรณีผลการทดสอบการทำงานของอุปกรณ์ในโครงการ ยังไม่สามารถทำงานได้อย่างถูกต้องครบถ้วนตามวัตถุประสงค์ของโครงการ ผู้ชนะการประกวดราคาจะต้องทำการปรับปรุงแก้ไขเพื่อให้การทดสอบผ่านเงื่อนไขตามข้อกำหนดดังกล่าว

12.3 ในระหว่างที่ทำการทดสอบระบบ หากอุปกรณ์ใดของสำนักงาน หรือหน่วยงานที่เกี่ยวข้องได้รับความเสียหายระหว่างการทดสอบ และส่งผลให้เกิดข้อบกพร่องของระบบคอมพิวเตอร์ในโครงการอื่น ๆ โดยความเสียหายที่เกิดขึ้นระหว่างการทดสอบนั้นเกิดจากความบกพร่องของบุคลากรของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาจะต้องทำการซ่อมแซม แก้ไขหรือเปลี่ยนแทนโดยไม่คิดค่าใช้จ่ายใด ๆ จาก สศค.

12.4 ในระหว่างดำเนินโครงการ ผู้ชนะการประกวดราคาต้องรับผิดชอบเรื่องการขนย้ายขยะมูลฝอยและเศษวัสดุออกจากพื้นที่ทุกครั้ง รวมทั้งการปรับสภาพพื้น ผนังห้องเซิร์ฟเวอร์ของ สศค. หรือสถานที่ตามที่ สศค. กำหนดให้อยู่ในสภาพดีดังเดิม หากมีค่าใช้จ่ายเกิดขึ้น ผู้ชนะการประกวดราคาต้องเป็นผู้รับผิดชอบทั้งหมด

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

13. การฝึกอบรม

ผู้ชนะการประกวดราคาต้องจัดการฝึกอบรมเจ้าหน้าที่ของ สศค. พร้อมคู่มือและเอกสารประกอบการฝึกอบรม โดยต้องดำเนินการฝึกอบรมให้แล้วเสร็จภายใน 240 วัน นับถัดจากวันลงนามในสัญญา

ผู้ชนะการประกวดราคาต้องรับผิดชอบค่าวิทยากร ค่าอาหารกลางวัน ค่าอาหารว่าง และค่าเอกสารตลอดการฝึกอบรม โดยต้องอบรมหลักสูตรเจ้าหน้าที่ผู้ดูแลระบบคลาวด์และอุปกรณ์ที่เกี่ยวข้อง ระยะเวลา 2 วัน วันละไม่น้อยกว่า 6 ชั่วโมง จำนวนอย่างน้อย 5 คน และหลักสูตรเจ้าหน้าที่ใช้งานระบบ ระยะเวลา 1 วัน วันละไม่น้อยกว่า 6 ชั่วโมง จำนวนอย่างน้อย 10 คน

14. การสนับสนุนของ สศค.

สศค. จะอำนวยความสะดวกให้กับบริษัทผู้ชนะการประกวดราคา เพื่อให้การดำเนินงานเรียบร้อยและมีประสิทธิภาพ ดังนี้

14.1 ประสานงานและดำเนินการจัดเจ้าหน้าที่อำนวยความสะดวกในการให้ข้อมูลเกี่ยวกับระบบความปลอดภัยของระบบเครือข่าย ระบบคลาวด์เดิมของ สศค. และอื่น ๆ ที่เกี่ยวข้อง

14.2 อนุญาตให้บริษัทผู้ชนะการประกวดราคาสามารถใช้และสามารถส่งข้อมูลผ่านระบบเครือข่ายสื่อสารของ สศค. ตามความเหมาะสม

15. การรักษาความลับของข้อมูล

ผู้ชนะการประกวดราคาต้องรักษาข้อมูลที่เกี่ยวข้องกับโครงการหรือข้อมูลของ สศค. ไว้เป็นความลับตลอดไป ไม่ว่าจะอยู่ในรูปแบบใด ที่ได้รับมาอย่างเคร่งครัด และจะต้องไม่เปิดเผยข้อมูลดังกล่าวไม่ว่าทั้งหมดหรือแต่บางส่วนให้ผู้อื่นทราบโดยปราศจากความยินยอมเป็นลายลักษณ์อักษรของเจ้าของข้อมูลไม่ว่าโดยทางตรงหรือทางอ้อม หากผู้แทน ช่างหรือลูกจ้างของผู้ชนะการประกวดราคาจงใจหรือประมาทเลินเล่อ กระทำหรืองดเว้นการกระทำใด ๆ ที่เป็นการเปิดเผยข้อมูลที่เกี่ยวข้องกับโครงการหรือข้อมูลของ สศค. อันก่อให้เกิดความเสียหายต่อ สศค. หรือบุคคลอื่น ผู้ชนะการประกวดราคาจะต้องชดใช้ค่าเสียหายที่เกิดขึ้นทั้งหมดให้แก่ สศค. หรือบุคคลที่ได้รับความเสียหาย และถือว่าข้อพิจารณาของ สศค. ถือเป็นการสิ้นสุด จะร้องขอต่อไปไม่ได้

16. การละเมิดลิขสิทธิ์หรือสิทธิบัตรเกี่ยวกับคอมพิวเตอร์

ในกรณีที่บุคคลภายนอกกล่าวอ้างหรือใช้สิทธิ์เรียกร้องใด ๆ ว่าการละเมิดสิทธิ์ หรือสิทธิบัตรเกี่ยวกับคอมพิวเตอร์ และ/หรือ Software ที่เสนอ โดย สศค. มิได้แก้ไขหรือดัดแปลงไปจากเดิม ผู้ชนะการประกวดราคาจะต้องดำเนินการทั้งปวงเพื่อให้การกล่าวอ้างหรือการเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว หากผู้ชนะการประกวดราคามิอาจกระทำได้ และ สศค. ต้องรับผิดชดใช้ค่าเสียหายต่อบุคคลภายนอก เนื่องจากผลแห่งการละเมิดลิขสิทธิ์หรือสิทธิบัตรดังกล่าว ผู้ชนะการประกวดราคาต้องเป็นผู้ชำระค่าเสียหายและค่าใช้จ่ายรวมทั้งค่าฤชาธรรมเนียม และค่าทนายความแทน สศค. ทั้งนี้ สศค. จะแจ้งให้ผู้ชนะการประกวดราคาทราบเป็นลายลักษณ์อักษรเมื่อได้มีการกล่าวอ้างหรือใช้สิทธิ์เรียกร้องดังกล่าวโดยไม่ชักช้า

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ

17. หน่วยงานที่รับผิดชอบดำเนินการ

ศูนย์เทคโนโลยีสารสนเทศ สำนักงานเศรษฐกิจการคลัง

โทรศัพท์ 0-2273-9020 ต่อ 3706

อีเมล itproject@fpo.go.th

.....ประธานกรรมการ .....กรรมการ .....กรรมการ .....กรรมการ

.....กรรมการ .....กรรมการ .....กรรมการและเลขานุการ