ขอบเขตของงาน (Terms of Reference)
โครงการพัฒนาระบบเครือข่าย และจัดหาซอฟต์แวร์ เพื่อความมั่นคงปลอดภัย
ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

หลักการและเหตุผล

ตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนดให้จัดหาครุภัณฑ์คอมพิวเตอร์ใหม่ได้ โดยมีอายุการใช้งานไม่น้อยกว่า ๕ ปี ในการนี้ สำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) (สพพ.) จึงได้สำรวจครุภัณฑ์คอมพิวเตอร์ เมื่อเดือนกรกฎาคม ๒๕๖๔ แล้วพบว่า อุปกรณ์ป้องกันเครือข่าย (Firewall) มีอายุการใช้เกินกว่า ๕ ปี และ สพพ. มีการเช่าบริการ Co-Location สำหรับวางเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย ประกอบกับในปี ๒๕๖๕ ได้มีการดำเนินงานของโครงการ Front & Back Office เพื่อบูรณาการระบบเทคโนโลยีสารสนเทศของ สพพ. จึงมีความจำเป็นต้องจัดหาพื้นที่เช่าบริการวางเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายของโครงการ Front & Back Office รวมถึงเพิ่มประสิทธิภาพป้องกันการบุกรุกเว็บไซต์ของ สพพ. จำเป็นจะต้องมีการจัดหาอุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) ซอฟต์แวร์ป้องกันข้อมูลรั่วไหล หน่วยจัดเก็บข้อมูลและหน่วยความจำหลัก (Memory) สำหรับเครื่องคอมพิวเตอร์แม่ข่าย ทั้งนี้ ในการจัดหาอุปกรณ์ที่กล่าวจะทำให้การปฏิบัติงานมีความมั่นคงปลอดภัย มีความรวดเร็ว และมีประสิทธิภาพมากขึ้น

สพพ. ได้ดำเนินการตามแผนการดำเนินงานด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ กำหนดให้ สพพ. ดำเนินโครงการพัฒนาระบบเครือข่าย และอุปกรณ์ระบบเครือข่าย เพื่อความมั่นคงปลอดภัย เพื่อจัดหาอุปกรณ์ระบบเครือข่ายที่มีประสิทธิภาพ ประกอบด้วย อุปกรณ์ป้องกันเครือข่าย (Firewall) อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) ซอฟต์แวร์ป้องกันข้อมูลรั่วไหล หน่วยจัดเก็บข้อมูลและหน่วยความจำหลัก (Memory) สำหรับเครื่องคอมพิวเตอร์แม่ข่าย รวมถึงเช่าบริการ Co-Location สำหรับจัดเก็บอุปกรณ์เครือข่ายของโครงการ Front & Back Office

๑. วัตถุประสงค์

๑.๑ เพื่อจัดหาอุปกรณ์ระบบเครือข่ายที่มีประสิทธิภาพ ประกอบด้วย อุปกรณ์ป้องกันเครือข่าย (Firewall) อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) ซอฟต์แวร์ป้องกันข้อมูลรั่วไหล หน่วยจัดเก็บข้อมูลและหน่วยความจำหลัก (Memory) สำหรับเครื่องคอมพิวเตอร์แม่ข่าย รวมถึงเช่าบริการ Co-Location สำหรับจัดเก็บอุปกรณ์เครือข่ายของโครงการ Front & Back Office

๑.๒ เพื่อป้องกันการบุกรุกหรือการโจมตีจากผู้ไม่พึงประสงค์เข้าสู่ระบบเครือข่ายของ สพพ.

๑.๓ เพื่อจัดหาอุปกรณ์ป้องกันเครือข่าย (Firewall) ที่มีประสิทธิภาพสูงทดแทนเครื่องเดิม และเพื่อรองรับการปฏิบัติงานของระบบในปัจจุบันได้

๒. ขอบเขตการดำเนินงาน

๒.๑ ผู้ประสงค์จะเสนอราคาต้องติดตั้งและ/หรือตั้งค่าอุปกรณ์ที่เสนอในโครงการจัดหาเครื่องคอมพิวเตอร์แม่ข่าย และระบบเฝ้าระวังเครือข่าย เพื่อการบริหารงานอย่างต่อเนื่องและถูกต้อง พร้อมทั้งสามารถทำงานได้อย่างสมบูรณ์และมีประสิทธิภาพตรงตามความต้องการของ สพพ. ยกเว้น มีเหตุจำเป็นที่เกิดจากทาง สพพ. ไม่สามารถให้ดำเนินการติดตั้งและ/หรือตั้งค่าอุปกรณ์ได้

๒.๒ ผู้ประสงค์จะเสนอราคาต้องเสนอแผนการติดตั้ง ออกแบบอุปกรณ์หรือตั้งค่า พร้อมจัดทำ Diagram ให้ทาง สพพ. ก่อนดำเนินการ เพื่อให้ทาง สพพ. พิจารณา แก้ไข และอนุมัติแผนการก่อนเริ่มทำการติดตั้ง ภายใน ๑๕ วัน

๒.๓ ผู้ประสงค์จะเสนอราคาต้องจัดทำคู่มือการตั้งค่าอุปกรณ์และระบบงานในโครงการฯ ให้กับทาง สพพ.

๒.๔ ผู้ประสงค์จะเสนอราคามีหน้าที่รับผิดชอบค่าใช้จ่ายต่างๆ ที่เกิดขึ้นจากความผิดพลาด บกพร่อง รวมถึงประเมินความต้องการของระบบไม่ครบถ้วน ในการปฏิบัติงานของ สพพ.

๒.๕ ผู้ประสงค์จะเสนอราคาต้องบริหารจัดการระบบของโครงการฯ ให้สามารถทำงานร่วมกับระบบบริหารจัดการบัญชีผู้ใช้งาน (Active Directory) ที่ สพพ. ใช้งานอยู่ในปัจจุบันได้ โดยสามารถตั้งค่าให้สามารถใช้งานร่วมกันได้

๒.๖ ผู้ประสงค์จะเสนอราคาต้องจัดทำแผนการดำเนินการกรณีฉุกเฉินของระบบ แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อใช้เป็นกรอบหลักการและแนวทางปฏิบัติในการดำเนินธุรกิจอย่างต่อเนื่องภายใต้ภาวะวิกฤต ดังนี้

๒.๖.๑ ผู้ประสงค์จะเสนอราคาต้องจัดทำแผน BCP ของระบบ เพื่อรองรับกรณีงานที่ใช้บริการมีปัญหาหยุดชะงัก และไม่สามารถให้บริการได้อย่างต่อเนื่อง

๒.๖.๒ กรณีผู้ประสงค์จะเสนอราคามีการทดสอบแผน BCP ของระบบ ต้องแจ้งให้ สพพ. ทราบล่วงหน้าไม่น้อยกว่า ๑๕ วัน หาก สพพ. ประสงค์จะเข้าร่วมให้สามารถกระทำได้ และรายงานผลการทดสอบให้ สพพ. ทราบภายหลังการทดสอบเสร็จสิ้นไม่เกิน ๔๕ วัน

๒.๗ ผู้ประสงค์จะเสนอราคามีหน้าที่ให้ความร่วมมือกับ สพพ. ตามการร้องขอในการเตรียมความพร้อมของระบบ เพื่อให้สามารถดำเนินการติดตั้งระบบได้อย่างมีประสิทธิภาพทันต่อความต้องการ

๒.๘ ผู้ประสงค์จะเสนอราคาต้องทำการติดตั้ง อุปกรณ์ เพื่อเชื่อมระหว่าง สพพ. กับ ผู้ให้บริการ Colocation

<u>๓. คุณสมบัติผู้ประสงค์จะเสนอราคา</u>

๓.๑ ผู้ประสงค์จะเสนอราคาต้องเป็นนิติบุคคล ที่มีการจดทะเบียนก่อตั้งมาแล้วไม่น้อยกว่า ๓ ปี

๓.๒ ผู้ประสงค์จะเสนอราคาต้องมีทุนจดทะเบียนไม่น้อยกว่า ๑,๐๐๐,๐๐๐ บาท โดยมีหลักฐานการจดทะเบียนซึ่งกรมพัฒนาธุรกิจการค้ากระทรวงพาณิชย์ออกให้หรือรับรองไม่เกิน ๓ เดือน

๓.๓ ไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้ว

๓.๔ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ประสงค์จะเสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

๓.๕ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ประสงค์จะเสนอราคารายอื่นที่เข้าเสนอราคาให้แก่ สพพ. ณ วันประกาศ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการคัดเลือกครั้งนี้

๓.๖ บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญากับหน่วยงานของรัฐซึ่งได้ดำเนินการจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์ (e-Government Procurement : e-GP) ต้องลงทะเบียนในระบบอิเล็กทรอนิกส์ของกรมบัญชีกลางที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐ

๓.๗ ผู้ประสงค์จะเสนอราคาต้องเสนอรายชื่อผู้เชี่ยวชาญด้าน VMware ที่มี Certificate VMware Certificate Professional

๔. คุณสมบัติของอุปกรณ์/ระบบ

ในการดำเนินการตามขอบเขตของงาน ผู้ประสงค์จะเสนอราคาจะต้องดำเนินการจัดหาอุปกรณ์และระบบงาน โดยมีคุณลักษณะขั้นต่ำ ดังต่อไปนี้

๔.๑ อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) พร้อมติดตั้ง จำนวน ๒ เครื่อง

คุณลักษณะพื้นฐาน

๔.๑.๑ สามารถติดตั้งบนตู้ Rack ขนาด ๑๙ นิ้วได้

๔.๑.๒ เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance

๔.๑.๓ มีช่องต่อ Gigabit Ethernet RJ๔๕ ไม่น้อยกว่า ๑๒ ช่อง

๔.๑.๔ มีช่องต่อ Gigabit Ethernet SFP ไม่น้อยกว่า ๘ ช่อง

๔.๑.๕ มีช่องต่อ ๑๐G SFP+ ไม่น้อยกว่า ๒ ช่อง

๔.๑.๖ มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๕ ช่อง

๔.๑.๗ มี Firewall Throughput ไม่น้อยกว่า ๑๐Gbps และได้รับการรับรองมาตรฐานด้าน Firewall จาก ICSA Labs

๔.๑.๘ รองรับ Concurrent Sessions ไม่น้อยกว่า ๑,๕๐๐,๐๐๐ Session และ Sessions ใหม่ไม่น้อยกว่า ๕๖,๐๐๐ Session ต่อวินาที

๔.๑.๙ สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ อย่างน้อยดังนี้ Syn Flood, UDP Flood, ICMP Flood, TCP Port Scan, UDP Port Scan, DoS or DDoS, IP Fragment และ ICMP Sweep เป็นต้นได้

๔.๑.๑๐ มี IPS Throughput ไม่น้อยกว่า ๒.๖Gbps และได้รับการรับรองมาตรฐานด้าน IPS จาก ICSA Labs

๔.๑.๑๑ สามารถตรวจจับ Virus หรือ Malware ได้ โดยมี Threat Protection Throughput ไม่น้อยกว่า ๑Gbps และได้รับการรับรองมาตรฐานด้าน Antivirus จาก ICSA Labs

๔.๑.๑๒ สามารถตรวจสอบและป้องกันการเข้าถึง Web ตาม Categories และตาม URL ที่กำหนดได้

๔.๑.๑๓ สามารถตรวจสอบและป้องกับการเข้าถึง Application ได้ ไม่น้อยกว่า ๑,๐๐๐ รายการ

๔.๑.๑๔ มี IPSec VPN Throughput ได้ไม่น้อยกว่า ๑๑Gbps และได้รับการรับรองมาตรฐานด้าน IPSec จาก ICSA Labs

๔.๑.๑๕ สามารถทำ SSL VPN โดยรองรับผู้ใช้ SSL VPN ไม่น้อยกว่า ๕๐๐ ราย และได้รับการรับรองมาตรฐานด้าน SSL VPN จาก ICSA Labs

๔.๑.๑๖ สามารถ Authenticate ผู้ใช้งานแบบ Captive portal โดยตรวจสอบจาก Local user, LDAP และ RADIUS ได้

๔.๑.๑๗ สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้

๔.๑.๑๘ สามารถทำงานลักษณะ Transparent Mode และ NAT/Route ได้

๔.๑.๑๙ สามารถทำงานในลักษณะ Virtual Firewall หรือ Virtual Domain ได้อย่างน้อย ๑๐ ระบบ

๔.๑.๒๐ สามารถ Routing แบบ Static และ Dynamic Routing ได้

๔.๑.๒๑ มีความสามารถในการทำ Software-Defined Wan (SD-WAN) เพื่อเพิ่มประสิทธิภาพ WAN Link ดังนี้

(๑) Load balance WAN ตามสัดส่วนที่กำหนด

(๒) เลือกเส้นทาง WAN โดยตรวจสอบจาก Application

(๓) ตรวจสอบ WAN SLA โดยใช้ Latency, Jitter และ Packet loss

๔.๑.๒๒ มีความสามารถเป็น Wireless Controller รองรับการเชื่อมต่ออุปกรณ์ Access Point ที่อยู่ภายใต้เครื่องหมายการค้าเดียวได้ไม่น้อยกว่า ๖๔ ตัว

๔.๑.๒๓ สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย

๔.๑.๒๔ สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้

๔.๑.๒๕ สามารถใช้งานตามมาตรฐาน IPv๖ ได้

๔.๑.๒๖ มี Power Supply แบบ Redundant จำนวนไม่น้อยกว่า ๒ หน่วย

๔.๑.๒๗ เป็นอุปกรณ์ที่อยู่ในกลุ่ม Leader ของ Gartner Magic Quadrant for Network Firewall หรือใหม่กว่า

๔.๑.๒๘ สามารถยืนยันตัวตน แบบหลายชั้น (Multi-Factor Authentication) ด้วย Application Authenticator, E-mail หรือ SMS อย่างน้อย ๑ วิธี

๔.๑.๒๙ ผู้ประสงค์จะเสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่าย และได้รับการรับรองจากผู้ผลิตสาขาในประเทศไทยโดยตรงว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยใช้งานมาก่อน

๔.๑.๓๐ เพื่อป้องกันสินค้าลอกเลียนแบบ หรือสินค้าเก่านำมาประกอบใหม่บริษัทที่นำเสนอจะต้องได้รับ หนังสือรับรองผลิตภัณฑ์ และได้รับการแต่งตั้งเป็นตัวแทนอย่างเป็นทางการจากบริษัทผู้ผลิตฯ หรือสาขาของผู้ผลิตประจำในประเทศไทย

๔.๑.๓๑ อุปกรณ์จะต้องมีลิขสิทธิ์และเงื่อนไขการรับประกันเป็นเวลา ๑ ปี นับจากวันตรวจรับโครงการ ในกรณีที่เกิดปัญหาทางด้าน Hardware จะมีการติดต่อกลับภายใน ๔ ชั่วโมง (๔ Hours Response) โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ติดตั้งเครื่อง (On-Site Service)

๔.๒ อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) ขนาด ๔๘ ช่อง พร้อมติดตั้ง จำนวน ๑ เครื่อง

<u>คุณลักษณะพื้นฐาน</u>

๔.๒.๑ เป็นอุปกรณ์ทำหน้าที่ในการป้องกันด้าน Web Application หรือ Web Service โดยเฉพาะสามารถ ติดตั้งในตู้เก็บอุปกรณ์มาตรฐานขนาด ๑๙ นิ้ว ได้

๔.๒.๒ มี Throughput ของ Next Generation Firewall (NGFW) ไม่น้อยกว่า ๕Gbps (มีความเร็วในการส่งผ่านข้อมูล (Throughput) ไม่น้อยกว่า ๕๐๐Mbps (๕Gbps) หรือรองรับการส่งผ่านข้อมูลได้ไม่น้อยกว่า ๕,๐๐๐ Transactions ต่อวินาที)

๔.๒.๓ มีระบบป้องกันภัยคุกคาม Threat Prevention โดยมี Throughput ไม่น้อยกว่า ๔.๒Gbps

๔.๒.๔ สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser หรือ CLI ได้เป็นอย่างน้อย

๔.๒.๕ มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) อย่างน้อยดังนี้

(๑) มีพอร์ตชนิด ๑๐/๑๐๐/๑๐๐๐ Base-T จำนวนไม่น้อยกว่า ๖ ช่อง และสามารถรองรับการทำ Hardware Bypass ได้จำนวน ๑ คู่

(๒) มีพอร์ตชนิด ๑G SFP จำนวนไม่น้อยกว่า ๒ ช่อง

๔.๒.๖ สามารถทำ Routing แบบ Static, Dynamic Routing ได้

๔.๒.๗ สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้

๔.๒.๘ สามารถปรับเทียบเวลา (Time Synchronization) กับอุปกรณ์ภายนอกได้

๔.๒.๙ สร้างและจัดเก็บรายงาน (Report) ในรูปแบบ PDF Format เป็นอย่างน้อย และสามารถตั้งเวลาส่งรายงาน (Report) รายวัน/ สัปดาห์/ เดือน ได้ (สามารถทำรายงานการถูกโจมตีได้ในรูปแบบ HTML หรือ PDF หรือ XLS หรือดีกว่า)

๔.๒.๑๐ สามารถใช้งานตามมาตรฐาน IPv๖ ได้

๔.๒.๑๑ สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย

๔.๒.๑๒ สามารถป้องกันการโจมตี Denial of Service (DoS) หรือ Distributed Denial of Service (DDoS) รูปแบบต่างๆ เช่น SYN Flood, UDP Flood, DNS Flood, ICMP Flood, ICMPv๖ Flood, Port Scan, Teardrop Attack, LAND Attack, IP Fragment และ Smurf Attack ได้เป็นอย่างน้อย

๔.๒.๑๓ ระบบที่นำเสนอต้องสามารถใช้งานป้องกัน APT (Advance Persistent Threat) ด้วยเทคโนโลยี Cloud-Based Sandbox Threats Analysis โดยใช้ ตรวจจับ Botnet, Remote Access Trojan และ Malware ได้เป็นอย่างน้อย หรือเสนออุปกรณ์เสริมภายนอกที่มีฟังก์ชันการทำงานในลักษณะเดียวกันเพื่อให้การทำงานสมบูรณ์

๔.๒.๑๔ มีฟังก์ชันในการใช้งาน IPS โดยต้องสามารถทำงานแบบ Signatures Database ร่วมกับ Cloud Based Analysis Engine และได้รับการรับรองโดย Common Vulnerabilities And Exposures (CVE)

๔.๒.๑๕ อุปกรณ์สามารถหรือเสนอระบบเพิ่มเติมสำหรับการทำ Risk Assessment ที่สามารถสแกนช่องโหว่ภายในระบบ โดยสามารถตรวจสอบช่องโหว่ประเภท Operating System หรือ System Vulnerabilities

๔.๒.๑๖ สามารถตรวจจับพฤติกรรมการใช้งาน Web Application ของผู้ที่เข้ามาใช้บริการ Web Application บนเครื่องคอมพิวเตอร์แม่ข่ายต่างๆ ได้

๔.๒.๑๗ อุปกรณ์ที่นำเสนอจะต้องสามารถทำงานแบบ In-Line (Bridge) หรือ Transparent และ Span-Mode (Monitor) สำหรับตรวจสอบพฤติกรรมได้เป็นอย่างน้อย

๔.๒.๑๘ อุปกรณ์สามารถหรือเสนอระบบเพิ่มเติมสำหรับป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)

(๑) ได้รับการรับรองหรือทดสอบจาก NSS Labs ระดับ “Recommended” เทียบเท่า หรือดีกว่า ในหัวข้อการทดสอบ Web Application Firewall

(๒) มีความสามารถในการทำงานและปกป้อง Web Application ต่างๆ ได้ โดยรองรับ HTTPS หรือ SSL ได้เป็นอย่างน้อย

(๓) รองรับการป้องกันการถูกโจมตีด้วยวิธีต่างๆ ได้อย่างน้อยหรือเทียบเท่าดังนี้

- Cross-site Scripting
- Cookie Poisoning หรือ Cookie-Based Attack หรือ Cookie Manipulation
- Buffer Overflow
- SQL Injection

๔.๒.๑๙ มีซอฟต์แวร์หรือเสนอซอฟต์แวร์เพิ่มเติมสำหรับติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่สามารถทำงานร่วมกับอุปกรณ์รักษาความปลอดภัยเครือข่าย (Firewall) ที่เสนอผ่านระบบเครือข่ายได้ โดยมีคุณสมบัติอย่างน้อยดังนี้

(๑) เป็นซอฟต์แวร์ประเภท Endpoint Protection ที่สามารถทำงานทั้งในลักษณะ Endpoint Protection และ Endpoint Detection and Response (EDR) ได้ภายใน Agent เดียว โดยมีลิขสิทธิ์การใช้งานไม่น้อยกว่า ๑ ปี

(๒) รองรับการติดตั้งและทำงานร่วมกับระบบปฏิบัติการ (OS) และมีจำนวนลิขสิทธิ์การติดตั้ง (License) อย่างน้อยดังต่อไปนี้

- Microsoft Windows Server ๒๐๐๘R๒/๒๐๑๒/๒๐๑๖ หรือดีกว่า จำนวน ๓๐ ลิขสิทธิ์

(๓) สามารถบริหารจัดการผ่านทาง HTTPS ได้

(๔) สามารถตั้งกำหนดการตรวจสอบไวรัส (Virus Scan) ในลักษณะการตั้งเวลา (Scheduled) ได้

(๕) สามารถทำ Network Isolation หรือ Device Isolating ได้

(๖) มี Engine ในการตรวจจับไวรัสที่ทำงานในลักษณะ AI-based หรือ Machine Learning ได้

๔.๒.๒๐ เป็นผลิตภัณฑ์ที่ผ่านการทดสอบหรือถูกบรรจุรายชื่อเครื่องหมายการค้าของผลิตภัณฑ์อยู่ใน Magic Quadrant ของ Gartner ด้านอุปกรณ์ Enterprise Network Firewalls เป็นอย่างน้อย

๔.๒.๒๑ ได้รับการรับรองหรือทดสอบจาก Cyber Ratings ระดับ “AAA” สำหรับ Rating ในด้านการทดสอบ NGFW หรือ Enterprise Firewall เป็นอย่างน้อย

๔.๒.๒๒ ผู้ประสงค์จะเสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายและได้รับการรับรองจากผู้ผลิตสาขาในประเทศไทยโดยตรงว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยใช้งานมาก่อน เพื่อป้องกันสินค้าลอกเลียนแบบ หรือสินค้าเก่านำมาประกอบใหม่บริษัทที่นำเสนอจะต้องได้รับ หนังสือรับรองผลิตภัณฑ์

๔.๒.๒๓ การรับประกันสินค้าจากเจ้าของผลิตภัณฑ์ทั้งในส่วนของ Hardware และ Software รวมทั้ง สิทธิในการอัพเดทฐานข้อมูลของอุปกรณ์ที่เสนอเป็นเวลาไม่น้อยกว่า ๑ ปี นับจากวันตรวจรับโครงการ

๔.๓ เช่าใช้บริการพื้นที่วางเครื่องคอมพิวเตอร์แม่ข่ายของสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) กับผู้ให้บริการ Co-Location

<u>คุณลักษณะพื้นฐาน</u>

๔.๓.๑ ผู้ให้บริการ Co-Location จะต้องจัดเตรียมพื้นที่ภายในศูนย์คอมพิวเตอร์ที่เหมาะสม พร้อมด้วยระบบสื่อสารข้อมูล และสิ่งจำเป็นทุกอย่างที่เกี่ยวข้อง เพื่อรองรับชุดอุปกรณ์คอมพิวเตอร์ของ สพพ. จำนวนไม่น้อยกว่า ๕U

๔.๓.๒ ผู้ให้บริการ Co-Location จะต้องจัดเตรียมอุปกรณ์ปลายทางพร้อมสายสัญญาณต่างๆ สำหรับระบบสื่อสารข้อมูลความเร็วสูงที่เสนอ โดยจะต้องสามารถเชื่อมต่อเข้ากับอุปกรณ์ของ สพพ. ได้

๔.๓.๓ ผู้ให้บริการ Co-Location จะต้องจัดเตรียมพื้นที่ภายในศูนย์คอมพิวเตอร์ โดยจะต้องเป็นตู้ Rack เดียวกับที่ สพพ. ใช้บริการอยู่ปัจจุบัน เพื่อรองรับการปฏิบัติงานอย่างต่อเนื่อง และมีประสิทธิภาพ

๔.๓.๔ ผู้ให้บริการ Co-Location จะต้องจัดหา Public IP Address IPv๔ ให้จำนวนไม่น้อยกว่า ๘ IP

๔.๓.๕ ผู้ให้บริการ Co-Location จะต้องจัดหา Public IP Address IPv๖ ให้จำนวนไม่น้อยกว่า ๑๖ IP

๔.๓.๖ ผู้ให้บริการ Co-Location ต้องมีระบบอินเทอร์เน็ตแบบ Shared Domestic Bandwidth ขนาดความเร็วอย่างน้อย ๔๐Gbps เพื่อให้เครื่องคอมพิวเตอร์แม่ข่ายสามารถใช้งานอินเตอร์เน็ตได้

๔.๓.๗ ผู้ให้บริการ Co-Location ต้องมีระบบอินเทอร์เน็ตแบบ Shared international Bandwidth ขนาดความเร็วอย่างน้อย ๔Gbps เพื่อให้เครื่องคอมพิวเตอร์แม่ข่ายสามารถใช้งานอินเตอร์เน็ตได้

๔.๓.๘ ช่อง (Port) สำหรับการเชื่อมต่อแบบ ๑๐/๑๐๐/๑๐๐๐Mbps ไม่น้อยกว่า ๒ Port ที่สามารถเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตได้

๔.๓.๙ สพพ. สามารถที่จะดำเนินการเปลี่ยนแปลงหรือเพิ่มเติมหรืออุปกรณ์เข้าไปในตู้ได้ตลอดระยะเวลาการให้บริการโดยผู้ให้บริการ Co-Location จะต้องช่วยเหลือสนับสนุนและอำนวยความสะดวกในการดำเนินการดังกล่าว โดยไม่สามารถเรียกร้อง หรือคิดค่าใช้จ่ายใดๆ เพิ่มเติมได้ ยกเว้น กรณีเป็นอุปกรณ์ที่ทางผู้ให้บริการจัดหาเพิ่มเติมนอกเหนือจากสัญญาสามารถคิดค่าบริการเพิ่มเติมจากสัญญาได้

๔.๓.๑๐ ผู้ให้บริการ Co-Location ต้องมีคุณสมบัติ ดังนี้

(๑) ระบบไฟฟ้าภายในศูนย์คอมพิวเตอร์ (Power System)

(๒) ระบบปรับอากาศภายในศูนย์คอมพิวเตอร์ (Air Conditioning System)

(๓) ระบบดับเพลิงอัตโนมัติ (Fire Prevention System)

(๔) ระบบรักษาความปลอดภัย (Security)

๔.๓.๑๑ ระยะเวลาในการเช่าใช้บริการ

ระยะเวลา ๑๒ เดือน นับถัดจากคณะกรรมการตรวจรับได้เห็นชอบการตรวจรับเรียบร้อยแล้ว

๔.๔ ซอฟต์แวร์แม่ข่ายเสมือน (Server Virtualization) จำนวน ๒ ชุด

<u>คุณลักษณะพื้นฐาน</u>

๔.๔.๑ รองรับการบริหารจัดการผ่าน Browser ได้

๔.๔.๒ รองรับการแบ่งทรัพยากรของ Host ออกเป็นเครื่องคอมพิวเตอร์เสมือน (Virtual Machine) ได้มากกว่า ๑๐๐ เครื่องคอมพิวเตอร์เสมือน

๔.๔.๓ รองรับการกำหนดหน่วยความจำให้กับเครื่องคอมพิวเตอร์เสมือน (Virtual Machine) ได้สุงสุดไม่น้อยกว่า ๒TB

๔.๔.๔ สามารถกำหนดพื้นที่ Disk Space ให้คอมพิวเตอร์เสมือนในแบบ Thin Provisioning ได้

๔.๔.๕ สามารถย้าย disk file ของคอมพิวเตอร์เสมือนข้าม Storage ได้ โดยไม่ก่อให้เกิดความเสียหายต่องานที่ทำบนเครื่องคอมพิวเตอร์เสมือน (Virtual Machine) หรือส่งผลต่อผู้ใช้งานที่ใช้บริการอยู่

๔.๔.๖ สามารถย้ายเครื่องคอมพิวเตอร์เสมือน (Virtual Machine) ข้ามเครื่อง Server เมื่อต้องการบำรุงรักษาเครื่อง Server โดยไม่ก่อให้เกิดความเสียหายต่องานที่ทำบนเครื่องคอมพิวเตอร์เสมือน (Virtual Machine) หรือส่งผลต่อผู้ใช้งานที่ใช้บริการอยู่

๔.๔.๗ รองรับการ Restart เครื่องคอมพิวเตอร์เสมือน (Virtual Machine) ในแบบอัตโนมัติ เมื่อ Hardware หรือระบบปฏิบัติการหยุดการทำงาน หรือเกิดความเสียหายได้

๔.๔.๘ สามารถกำหนดให้เครื่องคอมพิวเตอร์ (Virtual Machine) เข้าถึงช่องทางการติดต่อสื่อสารได้ เช่น Fiber Channel (FC), iSCSI เป็นต้น

๔.๔.๙ สามารถกำหนดให้ application ทำงานได้ต่อเนื่องโดยไม่ทำให้เกิดความเสียหายหรือหยุดให้บริการ (Fault Tolerance) เมื่อเกิดความเสียหายของ Hardware โดยสามารถกำหนด Virtual CPU ได้สูงสุด ไม่น้อยกว่า ๒ vCPU ต่อ ๑ เครื่องคอมพิวเตอร์เสมือน

๔.๔.๑๐ สามารถกำหนด virtual CPUs per virtual machine ได้สูงสุด ไม่น้อยกว่า ๑๒๘ Virtual CPUs

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

๔.๔.๑๒ มีระบบช่วยแบ่งเบาการทำงานด้านโปรแกรมป้องกันไวรัสคอมพิวเตอร์ โดยไม่ต้องติดตั้ง agent บนเครื่องคอมพิวเตอร์เสมือน

๔.๔.๑๓ มีลิขสิทธิ์ใช้งานถูกต้องตามกฎหมาย สำหรับเครื่องแม่ข่ายที่มีหน่วยประมวลผล ไม่น้อยกว่า ๒ หน่วย

๔.๕ หน่วยจัดเก็บข้อมูล สำหรับเครื่องคอมพิวเตอร์แม่ข่าย พร้อมติดตั้ง จำนวน ๑๐ หน่วย

<u>คุณลักษณะพื้นฐาน</u>

๔.๕.๑ หน่วยจัดเก็บข้อมูล Hot swap hard disk drives แบบ SAS Hot-plug ชนิด ๒.๕” สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) ยี่ห้อ DELL รุ่น R๖๔๐ ซึ่ง สพพ. ใช้งานอยู่ในปัจจุบัน ขนาดความจุไม่น้อยกว่า ๑.๒TB ที่มีความเร็วในการทำงานอย่างน้อย ๗,๒๐๐ รอบต่อนาที (rpm) หรือดีกว่า จำนวนไม่น้อยกว่า ๒ หน่วย

๔.๕.๒ หน่วยจัดเก็บข้อมูล Hot swap hard disk drives แบบ SAS Hot-plug ชนิด ๒.๕” สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) ยี่ห้อ DELL รุ่น R๗๔๐ ซึ่ง สพพ. ใช้งานอยู่ในปัจจุบัน ขนาดความจุไม่น้อยกว่า ๑.๒TB ที่มีความเร็วในการทำงานอย่างน้อย ๗,๒๐๐ รอบต่อนาที (rpm) หรือดีกว่า จำนวนไม่น้อยกว่า ๒ หน่วย

๔.๕.๓ หน่วยจัดเก็บข้อมูล Hot swap hard disk drives แบบ Solid State Drive หรือดีกว่า ชนิด ๒.๕” สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) ยี่ห้อ DELL รุ่น R๗๔๐ ซึ่ง สพพ. ใช้งานอยู่ในปัจจุบัน ขนาดความจุไม่น้อยกว่า ๔๘๐GB จำนวนไม่น้อยกว่า ๒ หน่วย

๔.๕.๔ หน่วยจัดเก็บข้อมูล Hot swap hard disk drives แบบ SAS Hot-plug ชนิด ๒.๕” สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) ยี่ห้อ IBM รุ่น System X๓๒๕๐ M๕ ซึ่ง สพพ. ใช้งานอยู่ในปัจจุบัน มีความจุไม่น้อยกว่า ๑.๒TB จำนวนไม่น้อยกว่า ๒ หน่วย

๔.๕.๕ หน่วยจัดเก็บข้อมูล Hot swap hard disk drives แบบ Solid State Drive หรือดีกว่า ชนิด ๒.๕” สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) ยี่ห้อ IBM รุ่น System X๓๒๕๐ M๕ ซึ่ง สพพ. ใช้งานอยู่ในปัจจุบัน ขนาดความจุไม่น้อยกว่า ๔๘๐GB จำนวนไม่น้อยกว่า ๒ หน่วย

๔.๖ หน่วยความจำหลัก (Memory) สำหรับเครื่องคอมพิวเตอร์แม่ข่าย พร้อมติดตั้ง จำนวน ๘ หน่วย

<u>คุณลักษณะพื้นฐาน</u>

๔.๖.๑ หน่วยความจาหลัก (Memory) ชนิด DDR๔ หรือดีกว่า สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) ยี่ห้อ IBM รุ่น System X๓๒๕๐ M๕ ซึ่ง สพพ. ใช้งานอยู่ในปัจจุบัน ขนาดไม่น้อยกว่า ๖๔GB จำนวนไม่น้อยกว่า ๔ หน่วย

๔.๖.๒ หน่วยความจาหลัก (Memory) ชนิด DDR๔ หรือดีกว่า สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) ยี่ห้อ DELL รุ่น R๖๔๐ ซึ่ง สพพ. ใช้งานอยู่ในปัจจุบัน ขนาดไม่น้อยกว่า ๖๔GB จำนวนไม่น้อยกว่า ๔ หน่วย

๔.๗ ซอฟต์แวร์สำหรับสำรองข้อมูลที่ศูนย์คอมพิวเตอร์สำรอง จำนวน ๒ ชุด

<u>คุณลักษณะพื้นฐาน</u>

๔.๗.๑ สามารถสำรองและกู้คืนข้อมูลบนระบบ VMware vSphere โดยไม่จำเป็นต้องติดตั้ง Agent บนเครื่องคอมพิวเตอร์เสมือน

๔.๗.๒ สามารถกู้คืนข้อมูลในระดับไฟล์บน Guest OS ที่มีระบบปฏิบัติการประเภท Windows, Linux, Mac, BSD และ Solaris

๔.๗.๓ สามารถสำรองและกู้คืนข้อมูลในระดับ Application บนเครื่องคอมพิวเตอร์เสมือน (Granular Recovery) ได้โดยไม่จำเป็นต้องติดตั้ง Agent ซึ่งต้องรองรับ Application อย่างน้อยดังต่อไปนี้ Microsoft SQL Server, Microsoft SharePoint, Microsoft Active Directory, Microsoft Exchange และ Oracle

๔.๗.๔ สามารถสำรองข้อมูลเครื่องคอมพิวเตอร์เสมือนแบบ Synthetic Full Backup ซึ่งช่วยลดระยะเวลาในการสำรองข้อมูล

๔.๗.๕ สามารถสำรองข้อมูลเครื่องคอมพิวเตอร์เสมือนแบบ Forever Incremental Backup ได้ นั่นคือทำ Full Backup แค่ครั้งแรกครั้งเดียว ครั้งต่อๆ มาทำแค่ Incremental Backup โดยไม่จำเป็นต้องย้อนมาทำ Full Backup อีก

๔.๗.๖ สามารถลดความซ้ำซ้อน (Deduplication) หรือบีบอัด (Compression) ข้อมูลที่ทำการสำรองได้ด้วยซอฟต์แวร์ที่เสนอ

๔.๗.๗ สามารถสำรองข้อมูลเครื่องคอมพิวเตอร์เสมือนแบบ Image Backup แต่เลือกไฟล์หรือโฟลเดอร์ที่ต้องการจะ Exclude ได้

๔.๗.๘ สามารถควบคุมการสำรองข้อมูลโดยการกำหนดค่า Maximum Latency ของ Production Storage ที่ต้องการได้ เพื่อให้การสำรองข้อมูลไม่ส่งผลกระทบต่อระบบงานหลักมากเกินไป

๔.๗.๙ สามารถตรวจสอบความสมบูรณ์ของข้อมูลที่ได้สำรองไว้ (Backup Verification) โดยการจำลองการกู้คืนข้อมูลแบบอัตโนมัติได้ ซึ่งในกระบวนการนี้ต้องสามารถออกรายงานเพื่อแสดงผลลัพธ์ของการตรวจสอบได้ด้วย

๔.๗.๑๐ สามารถสร้างสภาพแวดล้อมจำลอง เพื่อนำมาทดสอบเครื่องคอมพิวเตอร์เสมือนที่ทำการ Backup ไว้ โดยไม่ส่งผลกับระบบงาน Production (On-Demand Sandbox)

๔.๗.๑๑ สามารถ Replicate ข้อมูลเครื่องคอมพิวเตอร์เสมือนไปยังไซต์สำรอง โดยไม่จำเป็นต้องติดตั้ง Agent และสามารถ FailOver และ FailBack เครื่องคอมพิวเตอร์เสมือนได้

๔.๗.๑๒ สามารถกำหนดแผนการกู้คืนระบบที่ไซต์สำรองไว้ล่วงหน้า ช่วยให้ผู้ดูแลระบบสามารถกู้คืนระบบได้แบบ ๑-Click

๔.๗.๑๓ รองรับการกู้คืนข้อมูลในระดับ VM และไฟล์ใน Guest OS จาก Snapshot ของ Storage

๔.๗.๑๔ รองรับการสำรองข้อมูลไปยัง Tape Drive, Tape Library หรือ VTL

๔.๗.๑๕ รองรับการใช้งานร่วมกับ vSphere Web Client

๔.๗.๑๖ สามารถบริหารจัดกลางจากส่วนกลางได้ (Centralize Management)

๔.๗.๑๗ มีเครื่องมือสำหรับเฝ้าสังเกต, ออกรายงานรวมไปถึงทำ Capacity planning สำหรับระบบเครื่องคอมพิวเตอร์เสมือน

๔.๗.๑๘ รองรับการทำงานกับระบบคอมพิวเตอร์เสมือนได้ทั้ง VMware vSphere และ Microsoft Hyper-V

๔.๗.๑๙ สามารถทำงานร่วมกับระบบสำรองข้อมูลสำหรับเครื่องคอมพิวเตอร์เสมือนเพื่อดูสถานะและออกรายงานที่เกี่ยวกับการทำสำรองข้อมูลได้

๔.๗.๒๐ สามารถเฝ้าสังเกตระบบคอมพิวเตอร์เสมือนและแสดงผลการทำงานได้แบบ Real Time ตลอด ๒๔x๗ โดยไม่จำเป็นต้องติดตั้ง Agent บนเครื่องคอมพิวเตอร์เสมือน

๔.๗.๒๑ สามารถแสดงข้อมูลระบบได้ โดยต้องเก็บข้อมูลย้อนหลังได้ไม่น้อยกว่า ๗ วัน

๔.๗.๒๒ สามารถออกรายงานที่แสดงถึงอัตราการเปลี่ยนแปลงของข้อมูลที่เกิดขึ้นกับเครื่องคอมพิวเตอร์เสมือนได้

๔.๗.๒๓ สามารถแจ้งเตือนผ่านทางอีเมล์ในกรณีที่เกิดเหตุการณ์ต่างๆ กับระบบเครื่องคอมพิวเตอร์เสมือนได้

๔.๗.๒๔ สามารถออกรายงานแสดงการใช้งาน CPU, Memory และ Network ของเครื่องคอมพิวเตอร์เสมือนได้

๔.๗.๒๕ สามารถปรับแต่งการออกรายงาน โดยผู้ดูแลระบบสามารถออกแบบและเลือกข้อมูลที่ต้องการให้แสดงในรายงานได้เอง

๔.๗.๒๖ สามารถแสดงข้อมูลเกี่ยวกับการขยายหรือการเพิ่มขึ้นของระบบเครื่องคอมพิวเตอร์เสมือน เพื่อวิเคราะห์แนวโน้มและประเมินความต้องทรัพยากรที่ต้องใช้ในอนาคตได้

๔.๗.๒๗ สามารถแสดงข้อมูลเพื่อสนับสนุนการทำ What-if Analysis ในกรณีที่จำเป็นต้องมีการปรับเปลี่ยนองค์ประกอบของระบบคอมพิวเตอร์เสมือนได้

๔.๗.๒๘ สามารถออกรายงานเพื่อแสดงม้วนเทปที่ใช้ในการสำรองข้อมูลสำหรับระบบเครื่องคอมพิวเตอร์เสมือนได้

๔.๗.๒๙ สามารถออกรายงานเพื่อแสดงม้วนเทปที่ใช้ในการสำรองข้อมูลสำหรับระบบเครื่องคอมพิวเตอร์เสมือนได้

๔.๗.๓๐ มี Dashboard สำหรับแสดงข้อมูลภาพรวมของระบบคอมพิวเตอร์เสมือน

๔.๘ ซอฟต์แวร์ป้องกันข้อมูลรั่วไหล (Data Loss Prevention) จำนวนไม่น้อยกว่า ๖๐ ผู้ใช้

<u>คุณลักษณะพื้นฐาน</u>

๔.๘.๑ โปรแกรมป้องกันข้อมูลรั่วไหล (Data Loss Prevention) ที่สามารถควบคุมกิจกรรมการรับส่งข้อมูล (Protection) และค้นหาตรวจสอบ (Discovery) การใช้งานข้อมูลของเครื่องคอมพิวเตอร์จากส่วนกลาง

๔.๘.๒ โปรแกรมบริหารจัดการจากส่วนกลางสามารถติดตั้งได้บนระบบปฏิบัติการ MS Windows Server ๒๐๑๒ หรือสูงกว่า

๔.๘.๓ โปรแกรมบริหารจัดการจากส่วนกลางสามารถรองรับฐานข้อมูลการใช้งาน ดังนี้ MS SQL Server ๒๐๑๒ หรือสูงกว่า, MS SQL Express ๒๐๑๖ หรือสูงกว่า, Azure SQL ได้

๔.๘.๔ โปรแกรมบริหารจัดการสามารถบริหารจัดการเครื่องลูกข่ายได้ดังนี้ MS Windows ๗/๘.๑/๑๐ ทั้ง ๓๒/๖๔-bit และ macOS ๑๐.๑๐ หรือสูงกว่า

๔.๘.๕ สามารถกำหนดนโยบายการป้องกันข้อมูลได้หลายระดับ เช่น Log only, Log only and notify, Log and Block ได้

๔.๘.๖ สามารถกำหนดนโยบายป้องกันตัวเองให้กับเครื่องลูกข่ายในการป้องกันการถอดถอนโปรแกรมการซ่อนโปรเซสและโฟเดอร์ (Hide processes and folders) และกำหนดรหัสผ่านสำหรับ Local Administration โปรแกรมให้กับเครื่องลูกข่ายได้

๔.๘.๗ สามารถป้องกันการรั่วไหลของข้อมูลได้หลากหลายช่องทาง (Data channeled protected) ตามที่กำหนดดังต่อไปนี้ได้

(๑) การส่งข้อมูล ผ่านทางระบบ Internet ได้แก่ http/https, FTP/FTPS, P๒P ได้

(๒) การส่งข้อมูล ผ่านทางระบบ E-mail ได้แก่ Webmail, POP๓/IMAP, SMTP ได้

(๓) การส่งข้อมูล ผ่านทางระบบ File Sharing and Social Media ได้แก่ Facebook, Twitter, Send Anywhere, WeTransfer ได้

(๔) การส่งข้อมูล ผ่านทาง Cloud ได้แก่ Box, Dropbox, Google Drive, OneDrive, SharePoint ได้

(๕) การส่งข้อมูล ผ่านทาง Microsoft ๓๖๕ ได้แก่ Exchange Online, SharePoint Online ได้

(๖) การส่งข้อมูลผ่านทาง Instant Messaging Applications ได้แก่ Teams, Skype, Slack ได้

(๗) การส่งข้อมูลผ่านทาง Removable Storage ได้แก่ USB, Memory cards, External drives, Optional discs ได้

(๘) การส่งข้อมูล ผ่านทาง Media ได้แก่ Printers, CD, DVD, Blu-ray ได้

(๙) การส่งข้อมูลผ่านทางการเชื่อมต่อ Connections ได้แก่ Bluetooth, Firewire

(๑๐) การใช้งานระบบ Operations เช่น Copy/Paste, Drag and Drop และ Screen Capture ได้

๔.๘.๘ สามารถทำสำเนาเหตุการณ์ (Shadow Copy) เก็บหลักฐานสำหรับเหตุการณ์โดยการสร้างสำเนาข้อมูลที่รั่วไหล โดยสำเนามีการเข้ารหัสและสามารถเก็บรักษาไว้ใน Local Computer

๔.๘.๙ สามารถแสดงรายงานการค้นหา วิเคราะห์ข้อมูล (Discovery) แบบ Real-Time ตามที่กำหนดดังต่อไปนี้

(๑) Application การเข้าใช้งานโปรแกรมต่างๆ บนเครื่องลูกข่าย

(๒) Device การเชื่อมต่อ Devices ต่างๆ บนเครื่องลูกข่าย เช่น USB, Mass Storage, Hard Drive, CD/DVD, Windows Portable Device, Printer, LPT, Transfer Cable, Camera/Scanner ได้

(๓) Web sites การเข้าถึงและเข้าใช้งานเว็บไซต์ต่างๆ โดยสามารถแสดง URL ที่เปิดใช้งานได้

(๔) Print แสดงการใช้งานการปริ้นข้อมูลต่างๆ เช่น ชื่อไฟล์ (Document Name), จำนวนหน้าที่ปริ้น, ปริ้นสี หรือขาวดำ

(๕) E-mail แสดงข้อมูลการใช้งาน E-mail เช่น Send/Received, Subject, Contains Attachments ได้

(๖) Files แสดงรายละการการเข้าถึงไฟล์ต่างๆ ได้ เช่น Open, Move, Delete, Create, Rename, Copy, FTP Transfer, Web Download/Upload, IM-Send File ได้เป็นอย่างน้อย

๔.๘.๑๐ สามารถทำการแบ่งหมวดหมู่ของข้อมูล (Data Categories) เพื่อระบุข้อมูลที่สำคัญในการจัดทำนโยบายการป้องกันข้อมูล (DLP Policy) ดังนี้

(๑) Sensitive Content เช่น credit cards number, custom regular expressions และ keywords

(๒) Exiting classification (metadata), classification identifier และ Tag identifier

(๓) Context rules ต่างๆ เช่น Application categories (Output files), Web (Specified Domain), Path Rules กำหนด Specified Folders

(๔) File properties ได้แก่ File Extensions เป็นต้น

๔.๘.๑๑ สามารถทำการแจ้งเตือนเมื่อผู้ใช้อาจละเมิดนโยบาย (Display Notification) ของข้อมูลที่ละเอียดอ่อน (Sensitive Data) ได้

๔.๘.๑๒ ผู้ประสงค์จะเสนอราคาต้องมีหนังสือแต่งตั้งการเป็นตัวแทนจำหน่ายและได้รับการรับรองจากผู้ผลิตสาขาในประเทศไทยโดยตรงว่าอุปกรณ์ที่เสนอเป็นอุปกรณ์ใหม่ ไม่เคยใช้งานมาก่อน

๔.๘.๑๓ บริษัทที่นำเสนอจะต้องได้รับหนังสือรับรองผลิตภัณฑ์ และได้รับการแต่งตั้งเป็นตัวแทนอย่างเป็นทางการจากบริษัทผู้ผลิตฯ หรือสาขาของผู้ผลิตประจำในประเทศไทย เพื่อป้องกันสินค้าลอกเลียนแบบหรือสินค้าเก่านำมาประกอบใหม่

๕. ระยะเวลาดำเนินการ

๙๐ วัน นับถัดจากวันลงนามในสัญญา

๖. งบประมาณ

วงเงินงบประมาณ ๒,๒๐๐,๐๐๐ บาท (สองล้านสองแสนบาทถ้วน) รวมภาษีมูลค่าเพิ่ม ๗% และค่าใช้จ่ายอื่นๆ ไว้ด้วยแล้ว

๗. การส่งมอบ

ผู้รับจ้างต้องดำเนินการส่งมอบอุปกรณ์ และ/หรือ เอกสารตามระยะเวลา ดังต่อไปนี้

๗.๑ **ส่วนที่ ๑** : ส่งมอบภายใน ๑๕ วัน นับถัดจากวันลงนามในสัญญา ประกอบด้วย แผนการดำเนินงาน (Inception Report) และจัดทำ Diagram ระบบที่ให้บริการสำหรับ สพพ. เป็นแบบ Visio โดยระบุรายละเอียดแต่ละ VM รวมถึงระบบภายใน สพพ. จำนวนไม่น้อยกว่า ๗ ชุด

๗.๒ **ส่วนที่ ๒** : ส่งมอบภายใน ๖๐ วัน นับถัดจากวันลงนามในสัญญา ประกอบด้วย ส่งมอบอุปกรณ์ทั้งหมดของโครงการฯ

๗.๓ **ส่วนที่ ๓** : ติดตั้งและฝึกอบรม ภายใน ๙๐ วัน นับถัดจากวันลงนามในสัญญา ประกอบด้วย

๗.๓.๑ ติดตั้งอุปกรณ์และระบบงานทั้งหมดในโครงการฯ พร้อมโอนถ่ายข้อมูลระบบเทคโนโลยีสารสนเทศบนอุปกรณ์เครือข่ายเดิม ไปยังอุปกรณ์เครือข่ายเครื่องใหม่

๗.๓.๒ จัดทำเอกสารระบุอุปกรณ์ ซอฟต์แวร์ คู่มือ หรือสิ่งอื่นใดที่จะตรวจรับ โดยระบุชนิด ยี่ห้อ จำนวน หมายเลขประจำอุปกรณ์ (Serial Number) สถานที่ติดตั้ง หรือรายละเอียดอื่นใดที่จำเป็นในการตรวจรับให้กับ สพพ. รวมถึงรายงานผลการติดตั้งและทดสอบอุปกรณ์และระบบงานในโครงการฯ ในรูปแบบเอกสาร จำนวนไม่น้อยกว่า ๗ ชุด และในรูปแบบ Flash Drive จำนวนไม่น้อยกว่า ๒ ชุด ดังนี้

(๑) รายงานสรุปผลการติดตั้งและทดสอบอุปกรณ์และระบบงานในโครงการฯ

(๒) คู่มือการใช้งานและดูแลรักษาอุปกรณ์ในโครงการฯ

(๓) เอกสารแสดงรายละเอียดสถานที่ติดตั้ง Data center พร้อมเบอร์ติดต่อ Call Center

๗.๓.๓ ผู้รับจ้างดำเนินการฝึกอบรมให้แก่ผู้ดูแลระบบ จำนวนไม่น้อยกว่า ๒ คน โดยทางผู้รับจ้างจะต้องเป็นผู้รับผิดชอบค่าใช้จ่ายในด้านต่างๆ เช่น ค่าวิทยากร ค่าเอกสารประกอบการฝึกอบรม ค่าอาหารว่าง และเครื่องดื่ม เป็นต้น

๘. การติดตั้งและการทดสอบอุปกรณ์/ระบบ

๘.๑ จัดทำแผนการติดตั้งก่อนเข้าดำเนินการติดตั้งอุปกรณ์/ระบบ

๘.๒ ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ และซอฟต์แวร์ ณ สพพ. และสถานที่ผู้รับจ้างให้บริการที่เสนอมาโดยไม่คิดค่าใช้จ่ายเพิ่มเติม

๘.๓ ติดตั้งระบบปฏิบัติการให้เป็นแบบ ๖๔bits พร้อมการปรับปรุง Service Pack และ Patch ข้อบกพร่อง ให้ทันสมัย

๘.๔ ปรับปรุงระบบ Active Directory ให้สามารถใช้งานบนระบบปฏิบัติการที่นำเสนอได้

๘.๕ อุปกรณ์ทุกรายการที่เสนอ จะต้องเป็นของใหม่ไม่เคยถูกใช้งานมาก่อน มีคุณภาพดี เป็นที่น่าเชื่อถือ มีความมั่นคงแข็งแรง และถูกต้องตามมาตรฐานก่อนที่จะนำไปติดตั้งหรือทดสอบ

๘.๖ ผู้รับจ้างต้องติดตั้งอุปกรณ์ในโครงการฯ อย่างถูกต้อง และสามารถทำงานได้อย่างสมบูรณ์ตรงตามความต้องการของ สพพ.

๘.๗ ตรวจสอบการทำงานของอุปกรณ์ร่วมกันระหว่างผู้รับจ้างและ สพพ. ในวันที่ส่งมอบอุปกรณ์

๘.๘ ผู้รับจ้างต้องเสนอแผนการทดสอบอุปกรณ์ในโครงการฯ ให้กับ สพพ. พิจารณาก่อนล่วงหน้าอย่างน้อย ๗ วัน ประกอบด้วยการทดสอบดังนี้

๘.๘.๑ การทดสอบอุปกรณ์ตามคุณสมบัติที่นำเสนอ

๘.๘.๒ การทดสอบการทำงานร่วมกันกับอุปกรณ์ และ/หรือ ระบบงานเดิม

๘.๙ ผู้รับจ้างจะต้องเป็นผู้ดำเนินการทดสอบอุปกรณ์ทั้งหมด โดย สพพ. จะเป็นเพียงผู้ตรวจสอบความถูกต้องเท่านั้น

๘.๑๐ ในระหว่างที่ทำการทดสอบอุปกรณ์ในโครงการฯ หากอุปกรณ์ใดได้รับความเสียหายระหว่างการทดสอบ และ/หรือ เกิดจากความบกพร่องของบุคลากรของผู้รับจ้าง ผู้รับจ้างจะต้องทำการซ่อมแซม แก้ไขหรือเปลี่ยนแทน โดยไม่คิดค่าใช้จ่ายใดๆ จาก สพพ.

๙. การชำระเงิน

สพพ. จะชำระเงินเป็นงวดเดียว เมื่อคณะกรรมการตรวจรับ ได้เห็นชอบการตรวจรับงานตามข้อ ๗ และข้อ ๘ เรียบร้อยแล้ว

๑๐. การรับประกันความชำรุด บกพร่อง ให้บริการตรวจสอบ และซ่อมแซมแก้ไข (Preventive Maintenance)

๑๐.๑ การให้บริการบำรุงรักษาและซ่อมแซมแก้ไขอุปกรณ์และระบบงานใต้โครงการฯ ผู้รับจ้างต้องทำการบำรุงรักษาซ่อมแซมแก้ไขอุปกรณ์ และระบบให้อยู่ในสภาพที่ใช้งานได้ดีดังเดิมตลอดระยะเวลาที่รับประกัน โดยระยะเวลาที่รับประกันจะเริ่มนับตั้งแต่วันถัดจากวันที่ตรวจรับงานเรียบร้อยแล้ว เป็นระยะเวลา ๑ ปี

๑๐.๒ การแจ้งเหตุในกรณีมีเหตุชำรุดบกพร่องหรือความขัดข้องของอุปกรณ์ ผู้รับจ้างต้องสามารถรับแจ้งได้ทุกวัน ทั้งทางโทรศัพท์ และโทรศัพท์เคลื่อนที่ โดยหลังจากที่ผู้รับจ้างได้รับแจ้งเหตุแล้ว จะต้องตอบกลับภายใน ๑ ชั่วโมง

๑๐.๓ การแจ้งเหตุในกรณีมีเหตุชำรุดบกพร่องหรือความขัดข้องของอุปกรณ์ ผู้รับจ้างต้องสามารถรับแจ้งได้ทุกวัน ทางจดหมายอิเล็กทรอนิกส์ (E-mail) โดยหลังจากที่ผู้รับจ้างได้รับแจ้งเหตุแล้ว จะต้องตอบกลับภายใน ๒๔ ชั่วโมง

๑๐.๔ ระหว่างรับประกันผลงาน ผู้รับจ้างต้องจัดส่งบุคลากรเข้าดำเนินการบำรุงรักษาอุปกรณ์และระบบ เป็นประจำในภาวะปกติอย่างน้อยปีละ ๔ ครั้ง ทุกๆ ๓ เดือน ตลอดระยะเวลารับประกัน โดยต้องแจ้งให้ทราบก่อนล่วงหน้าทุกครั้งที่เข้าดำเนินการอย่างน้อย ๑๕ วัน และจะต้องจัดส่งเอกสารสรุปผลภายในสัปดาห์แรกของเดือนถัดไป

๑๐.๕ การซ่อมแซม แก้ไข อุปกรณ์ในโครงการฯ

๑๐.๕.๑ ในกรณีที่อุปกรณ์ในโครงการ เกิดขัดข้อง หรือไม่สามารถใช้งานได้ ไม่ว่าจะติดตั้งอยู่ ณ สถานที่ใดตามที่กำหนดในสัญญา ความชำรุดนี้มิได้เกิดจากความผิดของ สพพ. ผู้รับจ้างต้องเริ่มจัดการซ่อมแซมแก้ไขให้อยู่ในสภาพดีได้ดังเดิม โดยไม่คิดค่าใช้จ่ายใดๆ จาก สพพ. ทั้งนี้ ต้องเริ่มจัดการซ่อมแซมแก้ไขหลังจากที่ได้รับแจ้งจาก สพพ. หรือผู้ที่ได้รับมอบหมายจาก สพพ. ภายใน ๑ วัน หากไม่สามารถเริ่มจัดการซ่อมแซมแก้ไขภายในเวลาดังกล่าว ผู้รับจ้างต้องถูกปรับในอัตราวันละ ๕๐๐ บาท (ห้าร้อยบาทถ้วน) ถ้าการซ่อมแซมแก้ไขไม่แล้วเสร็จภายใน ๓ วันทำการนับแต่เริ่มทำการซ่อมแซมแก้ไข ผู้รับจ้างต้องนำอุปกรณ์ หรือเครื่องสำรองที่มีประสิทธิภาพทัดเทียมกันมาให้ใช้แทนไปจนกว่าจะซ่อมแซมแล้วเสร็จสมบูรณ์ หากไม่สามารถนำอุปกรณ์ หรือเครื่องสำรองมาใช้แทนได้ ผู้รับจ้างต้องถูกปรับในอัตราวันละ ๑,๐๐๐ บาท (หนึ่งพันบาทถ้วน) นับตั้งแต่วันที่ ๔ เป็นต้นไป

๑๐.๕.๒ ในกรณีที่อุปกรณ์ในโครงการ เกิดขัดข้องไม่สามารถแก้ไขได้ในระยะเวลาภายใน ๓๐ วัน ผู้รับจ้างจะต้องจัดหาอุปกรณ์ใหม่มาทดแทนอุปกรณ์ที่ชำรุดเดิม

๑๐.๖ ในกรณีที่อุปกรณ์ หรือ ระบบ ในโครงการเกิดขัดข้อง ทำให้ไม่สามารถใช้งานได้ ผู้รับจ้างจะต้องให้คำแนะนำ คำปรึกษา หรือจัดส่งเจ้าหน้าที่เข้ามาให้บริการแก้ไขปัญหาที่ สพพ. ตามที่ร้องขอ โดยจะต้องพิจารณาปัญหาร่วมกับผู้รับผิดชอบของ สพพ. และกำหนดระยะเวลาในการแก้ไขปัญหาให้เสร็จสิ้นที่เหมาะสมร่วมกัน

๑๐.๗ กรณีที่มีเหตุสุดวิสัยทำให้เกิดความล่าช้าในการบริการ/การแก้ไขอุปกรณ์หรือระบบ เนื่องจากเกิดปัญหาที่ไม่สามารถแก้ไขได้ ทางผู้รับจ้างจะต้องรายงานความคืบหน้าต่อ สพพ. จนกว่าจะแก้ไขแล้วเสร็จ

๑๐.๘ หลังจากที่แก้ไขปัญหาใน ข้อ ๑๐.๗ เรียบร้อยแล้ว ผู้รับจ้างจะต้องส่งรายงานการซ่อมแซมแก้ไขปัญหาให้ทราบ ภายใน ๕ วันทำการ นับจากวันที่ตรวจสอบ/แก้ไขปัญหาแล้วเสร็จ

๑๑. เงื่อนไขการปรับ

ในกรณีที่ผู้รับจ้างไม่สามารถดำเนินงานได้ตามเงื่อนไขที่กำหนดไว้ในเอกสารนี้ ผู้รับจ้างจะต้องเสียค่าปรับในอัตราร้อยละ ๐.๐๒ ของมูลค่าสัญญาทั้งหมดต่อวัน หรือไม่น้อยกว่า ๑๐๐ บาทต่อวัน จนกว่าอุปกรณ์/หรือระบบฯ จะสามารถทำงานได้ตามปกติโดยเศษของวันจะถือเป็นหนึ่งวันเต็ม