6.5.9 ต้องสามารถทำ Hardware-bases Access Control List และ filter packet บน protocol IPv4 ได้โดยกำหนด Source และ Destination ที่ระดับ IP, UDP, และ TCP ได้ไม่น้อยกว่า 256 รายการ

6.5.10 ต้องสามารจำกัด MAC address ที่จะใช้งานในแต่ละ port ได้

6.5.11 ต้องสามารถทำ Port Mirroring หรือ switch port analyzer หรือเทียบเท่า โดย

6.5.11.1 กำหนด Source port มากกว่า 1 port

6.5.11.2 กำหนด Source และ distribution Port ให้อยู่ต่างข้าม Switch ที่อยู่ใน Stack หรือ Clustering เดียวกันได้

6.5.12 ต้องทำงานตามมาตรฐานเหล่านี้ได้ (Compliance)

6.5.12.1 IEEE 802.3ad Link aggregation ได้ไม่น้อยกว่า 8 ports ต่อกลุ่ม และไม่น้อยกว่า 32กลุ่ม (ต่อ vc หรือ กลุ่มอุปกรณ์ หรือ stack)

6.5.12.2 IEEE 802.1x Network Identification (support guest VLAN หรือ quarantine VLAN) พร้อม Radius Authentication แบบ port-based และ multiple supplicant หรือเทียบเท่า

6.5.12.3 IEEE 802.1p Quality of Service

6.5.12.4 IEEE 802.1q VLAN

6.5.12.5 Spanning Tree Protocol ที่เป็นไปตามมาตรฐาน IEEE

6.5.13 สามารถแก้ไขค่า Configuration ผ่านทาง Console Port หรือ Serial Interface

6.5.14 มี SNMP agent (RFC1157 Compliance) ที่ใช้งานร่วมกับ Network Management ได้ตามมาตรฐานดังต่อไปนี้

6.5.14.1 MIB II

6.5.14.2 RMON

6.5.15 ต้องรายงาน error และ/หรือ warning และ/หรือ information และ/หรือ event ผ่านระบบ Syslog ได้

6.5.16 ต้องสามารถทำ Multicasting โดยใช้โปรโตคอล IGMP version 1 (RFC1112) หรือ IGMP version2 (RFC2236) หรือ IGMP Snooping ได้

6.5.17 ต้องแสดงผังการติดตั้ง Module /Interface ของอุปกรณ์ทุกชิ้น ตามรายการที่เสนอจริงเพื่อประการพิจารณา

6.5.18 ในแต่ละกลุ่มหรือแต่ละตัว ต้องมี Uplink ไปยัง Server Core Switch ที่ความเร็วไม่ต่ำกว่า 2x10 Gbps

6.5.19 อุปกรณ์ต้อง

6.5.19.1 ตั้งเวลาผ่านของระบบผ่าน Network Time Protocol (NTP) version3 (RFC1305) หรือ SNTP version4 (RFC2030) และต้องสามารถใช้งานร่วมกัน Authentication ได้

6.5.19.2 ต้องทำ Packet classification ด้วย Source/destination OP, Source หรือ Destination Application Port, 802.1p COS, และ DiffServ Code Point (DSCP) พร้อมกำหนดค่า Qos ได้โดยสามารถกำหนด Queue การให้บริการได้ไม่น้อยกว่า 8 queues ต่อพอร์ต

6.6 อุปกรณ์ป้องกันเครือข่าย (Firewall) มีข้อกำหนดคุณลักษณะขั้นต่ำ ดังนี้

6.6.1 เป็นอุปกรณ์ Firewall ชนิด Stateful Inspection firewall แบบ Appliance

6.6.2 มี Throughput ของ Firewall Inspection จำนวนไม่น้อยกว่า 10 Gbps

6.6.3 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 8 ช่อง และช่องแบบ 10Gigabit Ethernet ชนิด 10Gig-SR ไม่น้อยกว่า 2 ช่องพร้อมโมดูล 10Gigabit Ethernet ชนิด 10Gig-SR จำนวนไม่น้อยกว่า 2 ชุด

6.6.4 สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ อย่างน้อยดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoof, IP Address Sweep, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, TCP Fragment, ICMP Fragment เป็นต้นได้

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

6.6.6 สามารถทำงานลักษณะ Transparent Mode ได้

6.6.7 สามารถ Routing แบบ Static, Dynamic Routing ได้

6.6.8 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย

6.6.9 สามารถเก็บรายละเอียดและตรวจสอบพฤติกรรมการใช้งาน (Logging/Monitoring) โดยเก็บเป็น Syslog และรูปแบบกราฟฟิคได้

6.6.10 มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

6.6.11 สามารถรองรับ Max Concurrent Connections ไม่น้อยกว่า 4,000,000 Connections และรับ New Connections ได้ไม่น้อยกว่า 120,000 Connections/Sec.

6.6.12 มีความเร็วในการทำงาน IPS Throughput ได้ไม่ต่ำกว่า 8 Gbps

6.6.13 มีความเร็วในการทำงาน IPsec VPN ได้ไม่ต่ำกว่า 4Gbps

6.6.14 มีความสามารถในการป้องกันการบุกรุก (Intrusion Prevention) โดยสามารถ update ฐานข้อมูลการรุก (Attack Signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติ ตลอดระยะของการรับประกัน

6.6.15 สามารถป้องกันการเข้าถึง Web site โดยกำหนดแยกตามประเภทของ Web site (Web Categories) ได้โดยมีสิทธิในการเข้าตรวจสอบฐานข้อมูลประเภทของ Web site ได้ตลอดระยะของการรับประกัน

6.6.16 สามารถทำการตรวจสอบผู้ใช้ (User Authentication) กับฐานข้อมูลผู้ใช้ภายในตัวอุปกรณ์ผู้ใช้ RADIUS, LDAP และ Windows Active Directory ได้เป็นอย่างน้อย

6.6.17 สามารถ Identification และ Control Application ได้

6.6.18 สามารถทำ High Availability (HA) แบบ Active-Active หรือ Active-Standby โดยไม่ต้องเสียค่าใช้จ่ายเพิ่ม

6.6.19 สามารถทำรายงานการถูกโจมตีได้ในรูปแบบ HTML หรือ PDF หรือดีกว่า

6.6.20 สามารถใช้งานตามมาตรฐาน IPv4 และ IPv6 ได้

6.6.21 อุปกรณ์ต้องได้รับมาตรฐาน FCC หรือ UL หรือ CUL หรือ CB ได้เป็นอย่างน้อย

6.7 อุปกรณ์เก็บข้อมูลจราจรคอมพิวเตอร์มีข้อกำหนดคุณลักษณะขั้นต่ำ ดังนี้

6.7.1 เป็นอุปกรณ์ Appliance หรืออุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices, ระบบปฏิบัติการ, ระบบ appliances, ระบบเครือข่าย และระบบฐานข้อมูล เป็นต้น โดยสามารถแสดงผลอยู่ภายใต้รูปแบบ (format) เดียวกันได้

6.7.2 มีระบบการเข้ารหัสข้อมูลเพื่อใช้ยืนยันความถูกต้องของข้อมูลที่จัดเก็บตามมาตรฐาน MD5 หรือ SHA-1 หรือดีกว่า

6.7.3 สามารถเก็บ Log File ในรูปแบบ Syslog ของอุปกรณ์ เช่น Router, Switch, Firewall, VPN, Server เป็นต้น ได้

6.7.4 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้

6.7.5 สามารถจัดเก็บ log file ได้ถูกต้อง ตรงตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

6.7.6 สามารถทำการสำรองข้อมูล (Data Backup) ไปยังอุปกรณ์จัดเก็บข้อมูลภายนอก เช่น Tape หรือ DVD หรือ External Storage เป็นต้น ได้

6.7.7 สามารถจัดเก็บข้อมูลเหตุการณ์ต่อวินาที (Events per Seconds) ได้ไม่น้อยกว่า 20,000 eps

6.7.8 มี Interface 10/100/1000Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 2 ช่อง โดยทั้ง 2 ช่อง ต้องเป็น Network Interface

6.7.9 อุปกรณ์มีหน่วยเก็บข้อมูล Hard Disk ความจุไม่น้อยกว่า 4TB หลังทำ RAID 1 หรือ RAID 5 หรือดีกว่า

6.7.10 อุปกรณ์มีสิทธิในการรับข้อมูลจราจรฯ จากอุปกรณ์ประเภทเครือข่ายได้ไม่น้อยกว่า 1,000 อุปกรณ์

6.7.11 สามารถกำหนดสิทธิและระดับความสำคัญให้กับผู้ดูแลระบบฯ ที่จะเข้ามาใช้งานอุปกรณ์เก็บข้อมูลจราจรนี้ได้ สามารถกำหนดได้ว่ามีสิทธิในการอ่านอย่างเดียว (read-only administrator) หรือ สิทธิในการทำ Report อย่างเดียว

6.7.12 อุปกรณ์ต้องได้รับมาตรฐาน FCC หรือ UL หรือ EN หรือ CE เป็นอย่างน้อย

6.8 ระบบบริหารจัดการ IP Management (DHCP & IPAM) มีข้อกำหนดคุณลักษณะขั้นต่ำ ดังนี้

6.8.1 ระบบที่เสนอในโครงการต้องสามารถ บริหารจัดการ DHCP และ IP Address Management โดยเฉพาะ

6.8.2 ต้องสามารถจัดการ/ให้บริการระบบ DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol) และ IPAM (IP Address Management) ได้เป็นอย่างน้อย

6.8.3 ต้องมี Network Interface แบบ Ethernet RJ-45 ความเร็ว 10/100/1000 Mbps จำนวนไม่น้อยกว่า 4 Ports

6.8.4 ต้องสามารถบริหารจัดการ IP Address (IP Address Management) ทั้งระบบ IPv4 และ IPv6 โดยมีความสามารถในการตรวจสอบสถานะของ IP Address ที่มีการแจกให้ใช้งานในเครือข่ายได้

6.8.5 ต้องสามารถทำการแจก IP Address ได้ทั้งแบบ Dynamic Allocation และ Address Reservation หรือเทียบเท่า

6.8.6 ต้องสามารถกำหนด Scope และ Range ในการแจก IP Address และสามารถทำ Access Control List (ACL) หรือ สามารถกำหนด Policy กับอุปกรณ์ (BYOD) ที่ทำการ request IP ได้ หรือ DHCP Filter ในการควบคุมการแจก IP address ได้

6.8.7 ต้องสามารถทำ DHCP Failover ได้ เพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่องในกรณีที่ระบบหลักเกิดปัญหา

6.8.8 รองรับการทำงานร่วมกับ DHCP Platform อื่นๆ ได้ เช่น DHCP ISC หรือ Microsoft ได้ในอนาคต

6.8.9 ต้องมีระบบปฏิบัติการที่ถูก Hardened แล้ว (Operating System Hardening)

6.8.10 ต้องสามารถทำงานบนระบบเครือข่ายแบบ IPv4 และ IPv6 ได้

6.8.11 ต้องสามารถบริหารจัดการอุปกรณ์ในรูปแบบ Graphical User Interface (GUI) ผ่าน Web Browser ได้

6.8.12 ต้องสามารถ Export รายงานออกมาในรูปแบบของ PDF และ CSV ได้ และสามารถ Custom report ได้

6.8.13 รองรับการทำ HA (High Availability) สำหรับ Management แบบ Active-Passive ได้ในอนาคต

6.8.14 รองรับการบริหารจัดการแบบรวมศูนย์ (Centralized Management) ได้ในอนาคต โดยไม่ต้องเปลี่ยนอุปกรณ์ หรือ Activate License เพิ่มเติม

6.8.15 ต้องเป็นอุปกรณ์แบบ Rack mountable ซึ่งสามารถติดตั้งใน Rack มาตรฐาน 19 นิ้วได้

6.8.16 ผลิตภัณฑ์ที่เสนอต้องได้รับมาตรฐานความปลอดภัย UL, FCC, CE และ RoHS เป็นอย่างน้อย

6.9 ซอฟต์แวร์ (Software) บริหารจัดการเครือข่าย มีข้อกำหนดคุณลักษณะขั้นต่ำ ดังนี้

6.9.1 สามารถตั้งค่าการบริหารจัดการอุปกรณ์เครือข่ายต่างๆ ผ่านโปรโตคอล SNMP version 1, 2 และ 3, Telnet และ SSH ได้เป็นอย่างน้อย

6.9.2 สนับสนุนการบริหารจัดการอุปกรณ์เครือข่ายในหลายๆ ผลิตภัณฑ์ (3rd party)

6.9.3 สามารถบริหารจัดการอุปกรณ์เครือข่ายได้ทั้งแบบมีสาย (Switch, Router) ที่เสนอในโครงการได้ทั้งหมด และไม่น้อยกว่า 200 อุปกรณ์

6.9.4 ผู้ดูแลสามารถ login เพื่อเข้าใช้งานระบบบริหารจัดการเครือข่ายคอมพิวเตอร์ที่ เสนอได้ผ่านทาง Web Browser จากเครื่อง PC หรือ Laptop หรือ Notebook หรือ Tablet ได้

6.9.5 สนับสนุนการค้นหาอุปกรณ์แบบอัตโนมัติ (Auto Discovery) ได้

6.9.6 สนับสนุนการ Import และ Export รายการอุปกรณ์ผ่าน CSV File ได้

6.9.7 สามารถกำหนดการทำงานในรูปแบบของ Task Scheduling ได้

6.9.8 สนับสนุนการบริการจัดการอุปกรณ์แบบกลุ่ม (Multiple Devices Using Batch Operations) ได้ เช่นการกำหนด SNMP , Telnet หรือ Pooling interval สำหรับอุปกรณ์แต่ละกลุ่มได้

6.9.9 สามารถบริหารจัดการระบบเครือข่ายเสมือน (VLAN) และ Access Control List (ACL) หรือ Policy ได้เป็นอย่างน้อย

6.9.10 สามารถตั้งค่า (Customization) เครื่องมือ แบบ Widget หรือ Dashboard ในการบริหารจัดการได้

6.9.11 สามารถจัดเก็บ (Backup) คัดลอกข้อมูลกลับ (Restore) ระบบปฏิบัติการ (Firmware) และ Configuration ของอุปกรณ์ได้

6.9.12 สามารถแสดงภาพการต่อเชื่อมอุปกรณ์เครือข่าย Topology Map และ สามารถจัดกลุ่มอุปกรณ์ในแผนภาพได้ เช่นการทำ Sub-View ของ Topology Map

6.9.13 สามารถแสดงสถานะของอุปกรณ์ผ่านทางสี ใน Topology Map ได้

6.9.14 สามารถแสดงภาพเสมือนจริงของอุปกรณ์เครือข่าย (Device View) ได้

6.9.15 สนับสนุนการบริหารจัดการ Data Center โดยมีคุณสมบัติดังต่อไปนี้เป็นอย่างน้อย

6.9.15.1 สามารถสร้าง Data Center Topology Map หรือ Logical network โดยกำหนดภาพการต่อเชื่อม Data Center ในแต่ละ Site ได้

6.9.15.2 สามารถแสดงการเชื่อมต่อ virtual switch หรือ ชื่อของระบบเครื่องแม่ข่ายเสมือน (Virtual Machine) เช่น VMware หรือ XEN หรือ Microsoft Hyper-V ได้

6.9.15.3 สนับสนุนการทำ Virtual Network Management หรือ Virtual Network Interface Management ได้

6.9.16 สามารถกำหนดการแสดงสถานะของอุปกรณ์เป็นกลุ่มๆ (Monitor Index) ได้ โดยมีค่าต่างๆ ของสถานะของอุปกรณ์ดังต่อไปนี้

6.9.16.1 Percentage of CPU Usage

6.9.16.2 Percentage of Memory Usage

6.9.16.3 Response Time of Device (ms) หรือ Performances of Device หรือ TOP N port utilization หรือ Device throughput

6.9.16.4 Percentage of Device Unreachability Proportion หรือ Status up/down of devices

6.9.17 สนับสนุนการค้นหาตำแหน่ง หมายเลข IP address หรือ MAC Address ในระบบเครือข่ายได้

6.9.18 มี Application Programming Interface (API)

6.9.19 สามารถตรวจสอบประสิทธิภาพการทำงานของอุปกรณ์เครือข่าย

6.9.20 สามารถแสดงแผนภูมิปริมาณข้อมูลในระบบโดยการรับค่าร่วมกับโปรโตคอล SFlow, Netflow หรือ NetStream หรือ CoreFlow2 ได้

6.9.21 สามารถออกรายงาน (Report) หรือ Export ในรูปแบบของ Topology Report, Performance Report และ Inventory Report ได้

6.9.22 สามารถกำหนดรูปแบบของรายงาน (Customized Reporting) หรือ สามารถกำหนดช่วงเวลาในการส่งรายงานไปยังผู้รับได้โดยอัตโนมัติ โดยสามารถส่งออก (Export) รายงานได้ เช่น PDF หรือ XML หรือ CSV เป็นอย่างน้อย

6.10 อุปกรณ์ SSL-VPN

6.10.1 ต้องมีระบบปฏิบัติการที่ออกแบบเฉพาะ SSL VPN Appliance

6.10.2 ต้องทำงานได้ทั้งแบบไม่ต้องติดตั้ง Client program (client less, Web-based client) และในแบบที่ต้องติดตั้ง Client program เพื่อใช้งานร่วมกับ Application อื่นๆ ได้ โดย Client ต้องสามารถติดตั้งใช้งานร่วมกับอุปกรณ์ดังต่อไปนี้ได้

6.10.2.1 Windows-bases PC (ใช้ได้กับ Window 7 และ Version ที่สูงขึ้นไป

6.10.2.2 MacOSX-bases PC

6.10.2.3 Linux-based PC

6.10.2.4 IOS Mobile Device (version 7 ขึ้นไป)

6.10.2.5 Android Mobile Device (version 4 ขึ้นไป)

6.10.3 Concurrent User ไม่น้อยกว่า 100 User

6.10.4 การทำงานแบบ Client less ต้องควบคุมจำกัดเครื่องคอมพิวเตอร์ปลายทาง (Client) โดยวิธีการดังต่อไปนี้

6.10.4.1 Anti-virus detection

6.10.4.2 Personal Firewall detection

6.10.4.3 Browser Cache Control หรือ Browser and Version

6.10.5 ต้องควบคุมการเข้าถึงเครื่องแม่ข่าย และ ทรัพยากรต่างๆ โดยใช้วิธีดังต่อไปนี้ได้

6.10.5.1 Access Control List (Source/ Destination IP Network) หรือ Network Access Control (IP and MAC Address, Browser Type and Version)

6.10.5.2 Service / Port

6.10.5.3 Destination URL

6.10.5.4 Encryption key ไม่น้อยกว่า 128 bit

6.10.5.5 Timebase (Scheduling)

6.10.5.6 User Group Policy

6.10.6 ต้องสามารถเข้ารหัสลับตามขั้นตอนวิธี (algorithm) แบบ AES เป็นอย่างน้อยได้

6.10.7 ต้องสามารถแฮชชิง (Hashing) ดังขั้นตอนวิธีต่อไปนี้ได้

6.10.7.1 SHA-1

6.10.7.2 MD5

6.10.8 ต้องสามารถพิสูจน์ตัวตน (Authentication) ร่วมกับระบบภายนอก ไม่น้อยกว่าวิธีการดังนี้

6.10.8.1 LDAP authentication

6.10.8.2 RADIUS authentication

6.10.8.3 Active Directory authentication

6.10.8.4 Single Sign-on

6.10.9 การทำงานในแบบ Clientless จะต้องทำงานดังต่อไปนี้ได้ทันที

6.10.9.1 File Sharing (CIFS)

6.10.9.2 SSH/ Telnet client

6.10.9.3 Remote Desktop Client

6.10.10 การทำงานในแบบ Client Install จะต้องสามารถทำงานดังต่อไปนี้ได้ทันที

6.10.10.1 การควบคุม version ของ client program หรือ ควบคุมโดยให้ใช้ client installer จากระบบเท่านั้น

6.10.10.2 ใช้งานร่วมกัน Application ต่างๆ ดังต่อไปนี้ได้เป็นอย่างน้อย

(1) Microsoft Outlook with Microsoft Exchange 2003 Server ขึ้นไป

(2) SAP

6.10.11 การ Configuration SSL VPN Server จะต้องสามารถทำได้โดยผ่าน Web-bases Management

6.10.12 ต้องรองรับการทำงาน High Availability ในรูปแบบ Active/Active หรือ Active/Passive ได้ทันที โดยไม่มีค่าใช้จ่ายเพิ่มเติม

6.10.13 สามารถลบข้อมูล cache, cookies, history ต่างๆที่เกิดขึ้นได้หมด หลังจาก ผู้ใช้งานออกจากระบบ หรือ ปิดบราวเซอร์บนระบบปฏิบัติการ Windows ได้เป็นอย่างน้อย

6.10.14 สามารถแยกกลุ่มผู้ใช้งาน โดยกำหนด policy และ resource ในการเข้าถึงได้

6.10.15 ต้องควบคุมจำนวนการใช้งาน Maximum Concurrent Session หรือ Multiple Session ของ User ได้

6.11 ระบบควบคุมการเข้าใช้งานเครือข่าย

6.11.1 ต้องสามารถตรวจสอบการใช้งาน ของผู้ใช้งานแต่ละคนได้

6.11.2 การบริหารจัดการต้องทำผ่านช่องทางสื่อสารที่มีการเข้ารหัสลับ เช่น HTTPS และต้องรองรับการบริหารจัดการด้วย SNMP และสามารถส่ง Log ไปยัง Syslog Server ได้

6.11.3 ต้องรองรับการใช้งานของเครื่อง Client อย่างน้อย เช่น

6.11.3.1 Windows-based PC (ใช้ได้กับ Windows 7 และ Version ที่สูงขึ้นไป

6.11.3.2 MacOSX-based PC

6.11.3.3 Linux-based PC

6.11.3.4 อุปกรณ์อื่น ๆ ที่ใช้ MAC Address

6.11.4 สามารถกำหนดนโยบาย Access Control รวมในองค์กรแบบ Centralized Security Policy เช่น ไม่อนุญาตให้เข้าใช้งาน กรณีไม่ติดตั้ง หรือไม่เปิดใช้งาน Anti-virus (เฉพาะ Window-based)

6.11.5 ต้องตรวจสอบสถานภาพของ Windows based client ว่าใช้ระบบปฏิบัติการรุ่นใด และ/หรือ สถานภาพโปรแกรม Antivirus (ติดตั้ง ใช้งาน ความทันสมัย) และ/หรือ สถานภาพโปรแกรม (ติดตั้งใช้งาน) Personal Firewall และ/หรือ ระบบอื่น ๆ ที่จำเป็น ก่อนการเข้าถึงเครือข่าย

6.11.6 สามารถ Monitor ผู้ใช้ หรือ endpoints ที่อยู่ภายในเครือข่าย ได้แบบ Real time และผู้ให้บริการมีหน้าที่ปรับปรุง Script หรือ Critiria หรือ Policy ตามที่ สทอภ. แจ้งตลอดระยะเวลาโครงการ

6.11.7 สามารถกำหนดสิทธิของผู้ดูแลระบบได้หลายระดับ เช่น No Access หรือ Deny, Read, Write และแบบกำหนดเอง (Custom) หรือเทียบเท่า

6.12 ข้อกำหนดในการบริการ (Service Level Agreement : SLA)

6.12.1 ระบบเครือข่ายต้องให้บริการได้ตลอด 24 ชม. ทุกวันไม่เว้นวันหยุด โดยต้องมีความพร้อมใช้ (Availabilty) เฉลี่ยทั้งระบบไม่น้อยกว่า 99.7% และต่อชิ้นไม่น้อยกว่า 99.5% ต่อไตรมาส

6.12.2 เวลาทำการ หมายถึง วันจันทร์-วันศุกร์ เวลา 08:30 น. - 17:30 น. เว้นวันหยุดของ สทอภ.

6.12.3 ในระหว่างระยะเวลาการรับประกันผลิตภัณฑ์และการบำรุงรักษา ผู้ให้บริการจะต้องทำการประกันผลิตภัณฑ์และการบำรุงรักษาแบบ Onsite Service โดยมีรายละเอียดดังนี้

6.12.3.1 จัดเจ้าหน้าที่ที่มีความรู้ความสามารถในการดูแลและบริหารจัดการระบบ เข้ามาดำเนินการตรวจสอบ และบำรุงรักษาระบบ เป็นประจำทุก 6 เดือน พร้อมจัดทำเอกสารรายงานสถานะและผลทดสอบการทำงานของอุปกรณ์ (ตามเอกสารแนบท้าย)

6.12.3.2 บำรุงรักษาและตรวจสภาพการทำงานของอุปกรณ์ทั้งหมด ให้มีสภาพความพร้อมในการทำงานได้ตามปกติ

6.12.3.3 ทำการสำรองข้อมูลค่า Parameter และ Configuration ของอุปกรณ์ เพื่อใช้สำหรับการ Recovery เมื่อมีปัญหาเกิดขึ้นกับอุปกรณ์

6.12.3.4 บำรุงรักษา ทำความสะอาด ขจัดฝุ่นละอองของอุปกรณ์พร้อมทั้งตรวจสอบภาพแวดล้อมการทำงาน เช่น อุณหภูมิ, ความชื้น, ระบบไฟฟ้า และสถานที่ตั้งอุปกรณ์ เพื่อป้องกันปัญหาด้านกายภาพ และเพื่อให้ระบบ ทำงานได้อย่างมีประสิทธิภาพ ทั้งนี้ในการบำรุงรักษาจะต้องไม่มีผลกระทบต่อการรับประกัน และก่อให้เกิดผลเสียต่อการปฏิบัติงานของระบบเครือข่าย

6.12.3.5 จัดทำแผนสำรองข้อมูลและกู้คืน พร้อมสำรองข้อมูล (Backup) ค่า Configuration และค่าพารามิเตอร์ต่างๆ ที่อยู่ในอุปกรณ์เครือข่าย

6.12.3.6 จัดทำการทดสอบการสำรองข้อมูลและกู้คืนระบบที่นำเสนอ อย่างน้อยปีละ 1 ครั้ง ตลอดระยะเวลาการรับประกัน

6.12.3.7 เมื่อเกิดความผิดปกติขึ้นกับระบบ จากการตรวจสอบทาง System Log หรือตรวจพบโดยทางอื่น หรือได้รับแจ้งจาก สทอภ. จะทำการจัดเจ้าหน้าที่ที่มีความรู้ความชำนาญเข้าไปดำเนินการตรวจสอบปัญหาที่เกิดขึ้นภายใน 2 ชั่วโมง (การให้บริการถึงที่ตั้งให้พิจารณาตามความเหมาะสม) และจัดการซ่อมแซมให้อยู่ในสภาพใช้งานได้ตามปกติภายในเวลา 6 ชั่วโมง หากการดำเนินการแก้ไขไม่สามารถดำเนินการแก้ไขหรือซ่อมแซมให้แล้วเสร็จภายในเวลาที่กำหนด จะจัดหาอะไหล่ หรืออุปกรณ์ที่มีความสามารถใช้งานเทียบเท่า มาเปลี่ยนแทนเพื่อให้ระบบ สามารถใช้งานได้ก่อนในช่วงเวลาที่นำอุปกรณ์ที่เสียไปซ่อม

6.12.3.8 ดำเนินการปรับปรุงเวอร์ชั่นของ Software และ Firmware ของอุปกรณ์ให้ทันสมัย เพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพ โดยจะดำเนินการทดสอบให้เรียบร้อยก่อนดำเนินการลงโปรแกรมว่าไม่มีผลกระทบต่อการทำงานของระบบเครือข่าย ของ สทอภ. แต่หากพิจารณาแล้วเห็นว่าไม่สมควรดำเนินการอันเนื่องมาจากสาเหตุใดๆ ก็ตาม จะทำหนังสือเป็นลายลักษณ์อักษร ถึงข้อดีข้อเสียดังกล่าว เพื่อให้ สทอภ. ได้พิจารณา

6.12.4 ผู้ให้บริการจะต้องแสดงรายชื่อเจ้าหน้าที่ผู้เชี่ยวชาญ ที่จะให้บริการบำรุงรักษาและซ่อมแซมแก้ไขอุปกรณ์เครือข่ายคอมพิวเตอร์ อย่างน้อย 3 คน ที่เป็นพนักงานประจำ เสนอต่อ สทอภ. พร้อมประวัติการศึกษาและประสบการณ์ พร้อมทั้งลงนามกำกับ มาพร้อมกับการยื่นซองเอกสารทางเทคนิคและในกรณีที่มีการเปลี่ยนบุคคลภายหลัง ให้แจ้งการเปลี่ยนแปลงให้ สทอภ. ทราบด้วย

6.12.5 การตรวจสอบบำรุงรักษาอุปกรณ์เครือข่ายคอมพิวเตอร์ ผู้ให้บริการมีหน้าที่บำรุงรักษาอุปกรณ์เครือข่ายคอมพิวเตอร์ให้อยู่ในสภาพใช้งานได้ดีอยู่เสมอด้วยค่าใช้จ่ายของผู้ให้บริการ โดยต้องจัดหาช่างผู้มีความรู้ความชำนาญและมีฝีมือดีมาตรวจสอบบำรุงรักษาและซ่อมแซมแก้ไขตลอดระยะเวลาการรับประกัน อย่างน้อย 6 ครั้ง โดยให้มีระยะเวลาทุกๆ 6 เดือน พร้อมทั้ง Upgrade Firmware และหรือ Software ให้เป็นเวอร์ชั่นล่าสุด

6.12.6 ในกรณีที่อุปกรณ์เครือข่ายคอมพิวเตอร์ โปรแกรม และอุปกรณ์ต่างๆ เสียหาย ไม่สามารถใช้งานได้ อันเนื่องมาจากการบำรุงรักษาของผู้ให้บริการนั้น ผู้ให้บริการจะต้องรับผิดชอบในการซ่อมแซมหรือจัดหาอุปกรณ์เครือข่ายคอมพิวเตอร์โปรแกรม และอุปกรณ์ต่างๆ ใหม่ ที่มีคุณสมบัติเท่าเทียมหรือดีกว่า มาใช้ทดแทนให้ระบบสามารถทำงานได้ปกติดังเดิม โดยผู้ให้บริการต้องรับผิดชอบค่าใช้จ่ายทั้งหมด

6.12.7 ผู้ให้บริการต้องจัดทำแผนผัง(ขนาดไม่ต่ำกว่า A3) โครงสร้างระบบเครือข่าย (Network Diagram) ภาพรวมทั้งหมด ของ สทอภ.

6.12.8 ผู้ให้บริการต้องจัดทำคู่มือการติดตั้งและแผนภาพการเชื่อมต่อของระบบที่เสนอ (System Configuration) ภาพรวมทั้งหมด ของ สทอภ.

6.12.9 เจ้าหน้าที่สนับสนุน/Network Engineer ต้องส่งมอบรายงานผลการดำเนินงานรายเดือนทุกสิ้นเดือน พร้อมการวิเคราะห์ โดยรายงานประกอบด้วย

6.12.9.1 รายงานข้อขัดข้องในการใช้งานระบบเครือข่าย และสาเหตุพร้อมทั้งการแก้ไข

6.12.9.2 รายละเอียดการรับแจ้ง/แก้ไขปัญหา ในเดือน พร้อมเปรียบเทียบกับข้อกำหนดในการบริการ

6.12.9.3 รายงานสภาพความพร้อมใช้ของระบบเครือข่าย (Availability ของอุปกรณ์ทุกชิ้น) ในรอบเดือน

6.12.9.4 รายงานการโจมตีระบบเครือข่าย (ถ้ามี)

6.12.9.5รายงานการวิเคราะห์และข้อแนะนำในการปรับปรุงระบบเครือข่าย (หาก สทอภ. ร้องขอ)

6.12.9.6รายงานการปรับปรุงด้านความปลอดภัย/นโยบายความปลอดภัยของระบบเครือข่าย (ถ้ามี)

6.12.9.7 รายงานการบริการอื่นๆ ดังนี้ TOP Application, TOP port of switch utilization และ TOP user/IP utilization เป็นอย่างน้อย

6.12.10 กรณีที่ผู้ให้บริการมีความประสงค์จะเปลี่ยน เจ้าหน้าที่สนับสนุน/Network Engineer ผู้ให้บริการต้องส่ง เจ้าหน้าที่สนับสนุน/Network Engineer ที่จะเข้ามาประจำการที่ สทอภ. เป็นเวลาอย่างน้อย 2 สัปดาห์เพื่อการเรียนรู้งาน โดย เจ้าหน้าที่สนับสนุน/Network Engineer เดิมยังคงทำงานต่อไปตามปกติ เว้นแต่เป็นการเปลี่ยนโดยเร่งด่วน สามารถดำเนินการได้ทันที

6.12.11 สทอภ. อาจร้องขอให้เปลี่ยน เจ้าหน้าที่สนับสนุน/Network Engineer ในกรณีที่มีพฤติกรรมไม่เหมาะสม เช่น ขาดจริยธรรมในการบริการ ,มีปัญหาด้านกริยามารยาท, ขาดความรู้ความสามารถในการแก้ไขปัญหาบ่อยครั้ง เป็นต้น โดยการเปลี่ยน เจ้าหน้าที่สนับสนุน/Network Engineer ดังกล่าว ให้ถือเป็นการเปลี่ยน โดยเร่งด่วนและให้กระทำให้แล้วเสร็จภายใน 5 วันทำการ

6.12.12 ในกรณีที่ผู้ให้บริการ ปฏิบัติงานผิดพลาด บกพร่อง รวมถึงมีการโจมตี และโจรกรรมข้อมูลผ่านระบบเครือข่าย จนเป็นเหตุให้เกิดข้อพิพาท หรือ มีความเสียหายเกิดขึ้นกับ สทอภ. ผู้ให้บริการจะต้องเป็นผู้รับผิดชอบความเสียหายที่เกิดขึ้นและจัดการกรณีพิพาทนั้นให้เสร็จสิ้นโดยเร็ว

7. การส่งมอบและติดตั้ง

7.1 ส่งมอบระบบอุปกรณ์และดำเนินการติดตั้ง (Hardware/SoftwareDelivery) ณ สถานที่ติดตั้ง พร้อมทั้งทดสอบระบบอุปกรณ์ทั้งหมดให้สามารถใช้งานได้สมบูรณ์ตามข้อกำหนดและเงื่อนไขสัญญาภายในระยะเวลา 120 วัน นับถัดจากวันลงนามในสัญญา ประกอบด้วย

7.1.1 การส่งมอบรายงานการออกแบบระบบ (System Design) จำนวน 5 ชุด ทั้งในรูปแบบของเอกสารพิมพ์ (Hard Copy) และในรูปสื่ออิเล็กทรอนิกส์ (Digital File) ภายใน 30 วัน ประกอบด้วย

7.1.1.1 ผลการสำรวจพื้นที่ให้บริการของระบบเครือข่ายหลัก สถานที่ติดตั้งระบบอุปกรณ์ฯ

7.1.1.2 แผนการดำเนินงาน (Implementation Plan)

7.1.1.3 รายละเอียดและรายการอุปกรณ์ที่จะส่งมอบ เช่น ยี่ห้อ รุ่น จำนวน เป็นต้น

7.1.1.4 แผนและขั้นตอนการทดสอบ ตรวจงานที่ส่งมอบ

7.1.2 ติดตั้งระบบอุปกรณ์ (Hardware/SoftwareDelivery) ให้แล้วเสร็จภายใน 90 วัน

7.1.3 ดำเนินการฝึกอบรม (ครั้งแรก) ให้แล้วเสร็จภายใน 120 วัน และส่งมอบเอกสาร ในรูปแบบของเอกสารพิมพ์ (Hard Copy) และในรูปสื่ออิเล็กทรอนิกส์ (Digital File) ประกอบด้วย

7.1.3.1 รายงานผลดำเนินการติดตั้ง และการทดสอบระบบ

7.1.3.2 เอกสารลิขสิทธิ์ซอฟต์แวร์ (Certificate License)

7.1.3.3 เอกสารคู่มือการปฏิบัติงาน (Operation Manual) และการบำรุงรักษาระบบ (Maintenance Manual) ระบบอุปกรณ์ที่ส่งมอบ

7.1.3.4 คู่มือการติดตั้งและแผนภาพการเชื่อมต่อของระบบที่เสนอ (System Configuration) ภาพรวมทั้งหมด ของ สทอภ.

7.2 ผู้ให้บริการจะต้องดำเนินการฝึกอบรมทบทวนให้เจ้าหน้าที่ของ สทอภ. อย่างน้อยอีก 4 ครั้ง (ทุกๆ 12 เดือน) และนำปัญหาที่พบในช่วงที่ผ่านมาเป็นกรณีศึกษา โดยจัดส่งเอกสารและผลการฝึกอบรมพร้อมรายงานสรุปผลการให้บริการรายเดือน

8. ระยะเวลาการให้บริการเช่าระบบเครือข่ายคอมพิวเตอร์หลัก ของ สทอภ.

ระยะเวลาเช่า 1800 วัน นับตั้งแต่ส่งมอบและติดตั้งระบบตามข้อ 7.1 และคณะกรรมการได้ตรวจรับงานเรียบร้อยแล้ว

9. สถานที่ส่งมอบงาน

ผู้ให้บริการจะต้องดำเนินการติดตั้งทดสอบ และส่งมอบระบบ อุปกรณ์ และซอฟต์แวร์ ณ สถานที่ปฏิบัติงานของสำนักงานฯ ดังนี้

9.1 สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ สำนักงานใหญ่ (ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550) ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 เลขที่ 120 หมู่ 3 อาคารรวมหน่วยราชการ (อาคารรัฐประศาสนภักดี) ชั้น 6 และชั้น 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

9.2 สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ สำนักงานสาขาบางเขน เลขที่ 196 ถนนพหลโยธิน แขวงลาดยาว เขตจตุจักร กรุงเทพฯ 10900

9.3 สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ (องค์การมหาชน) สำนักงานสาขาอุทยานรังสรรค์นวัตกรรมอวกาศ 88 หมู่ 9 ตำบลทุ่งสุขลา อำเภอศรีราชา ชลบุรี

10. กำหนดยืนราคา

กำหนดยืนราคาไม่น้อยกว่า 60 วัน นับแต่วันยืนยันราคาสุดท้าย

11. วงเงินงบประมาณ

ภายในวงเงิน 26,750,000.- บาท (ยี่สิบหกล้านเจ็ดแสนห้าหมื่นบาทถ้วน)

12. เงื่อนไขการชำระเงิน

สำนักงานฯ จะชำระเงินค่าจ้างเหมาบริการ (ค่าใช้บริการ) เป็นรายงวด งวดละเท่าๆ กันเป็นจำนวน 60 งวด ทุกๆ 30 วัน นับตั้งแต่วันที่ส่งมอบระบบและติดตั้งแล้วเสร็จตามข้อ 7 เมื่อผู้ให้บริการได้ส่งมอบรายงานและคณะกรรมการได้ตรวจรับรายงานเรียบร้อยแล้ว ดังนี้

- รายงานการเข้าปฏิบัติงานของเจ้าหน้าที่สนับสนุน/Network Engineer ในรอบเดือน
- รายงานภาพรวมการให้บริการของระบบเครือข่าย

- รายงานข้อขัดข้องในการใช้งานระบบเครือข่าย และสาเหตุพร้อมทั้งการแก้ไข
- รายละเอียดการรับแจ้ง/แก้ไขปัญหา ในเดือน พร้อมเปรียบเทียบกับข้อกำหนดในการบริการ
- รายงานสภาพความพร้อมใช้ของระบบเครือข่าย (Availability ของอุปกรณ์ทุกชิ้น) ในรอบเดือน
- รายงานการโจมตีระบบเครือข่าย (ถ้ามี)
- รายงานการวิเคราะห์และข้อแนะนำในการปรับปรุงระบบเครือข่าย (หาก สทอภ. ร้องขอ)
- รายงานการปรับปรุงด้านความปลอดภัย/นโยบายความปลอดภัยของระบบเครือข่าย (ถ้ามี)
- รายงานการบริการอื่นๆ ดังนี้ TOP Application, TOP port of switch utilization และ TOP user/IP utilization เป็นอย่างน้อย

13. การขอเช่าเพิ่มโดยใช้ราคาเดิม (Repeat order)

สำนักงานฯ อาจขอเช่าเพิ่มอุปกรณ์โดยเป็นยี่ห้อและรุ่นเดียวกันกับที่ส่งมอบและใช้อัตราค่าเช่าราคาเดียวกันกับสัญญาเช่าของโครงการนี้ ทั้งนี้ สำนักงานฯ จะแจ้งให้ทราบภายใน 90 วันนับตั้งแต่การส่งมอบครบถ้วน และไม่จำกัดจำนวนครั้งในการแจ้ง โดยคิดมูลค่ารวมของอุปกรณ์ที่เช่าเพิ่มเติม ไม่เกินร้อยละ 10 ของมูลค่าตามสัญญาเช่าของโครงการนี้

14. ค่าปรับ

14.1 ในกรณีที่ผู้ให้บริการไม่สามารถส่งมอบและติดตั้งได้ตามข้อ 7.1 ผู้ให้บริการจะต้องเสียค่าปรับให้แก่ สทอภ. ในอัตราร้อยละ 0.1 ของมูลค่าสัญญาทั้งหมดต่อวัน จนกว่าอุปกรณ์จะสามารถทำงานได้ตามปกติ โดยเศษของวันจะถือเป็นหนึ่งวันเต็ม

14.2 ในกรณีที่ผู้ให้บริการไม่สามารถให้ให้บริการได้ตามเงื่อนไขที่กำหนดข้างต้น ผู้ให้บริการจะต้องเสียค่าปรับให้แก่ สทอภ. ในอัตราร้อยละ 0.1 ของมูลค่าสัญญาทั้งหมดต่อวัน จนกว่าอุปกรณ์จะสามารถทำงานได้ตามปกติ โดยเศษของวันจะถือเป็นหนึ่งวันเต็ม

15. ข้อสงวนสิทธิ์

สำนักงานฯ จะประเมินผลการใช้บริการระบบเครือข่ายหลัก ในรอบปี (ทุก 12 เดือน) หากผลการประเมินไม่ผ่านตามข้อกำหนด หรือผู้ให้บริการไม่สามารถให้บริการได้ตามข้อกำหนด สำนักงานฯ ขอสงวนสิทธิ์ยกเลิกการใช้บริการ และผู้ให้บริการต้องให้สำนักงานใช้งานระบบดังกล่าวต่อไปอีกเป็นเวลา ไม่น้อยกว่า 12 เดือน หรือจนกว่าจะหมดระยะเวลาตามสัญญา (กรณีระยะเวลาของสัญญาเหลือน้อยกว่า 12 เดือน)

16. เงื่อนไขอื่น ๆ

ในกรณีที่ผู้ให้บริการ ปฏิบัติงานผิดพลาด บกพร่อง รวมถึงมีการโจมตี และโจรกรรมข้อมูลผ่านระบบเครือข่ายหลัก จนเป็นเหตุให้เกิดข้อพิพาท หรือ มีความเสียหายเกิดขึ้นกับ สทอภ. ผู้ให้บริการจะต้องเป็นผู้รับผิดชอบความเสียหายที่เกิดขึ้นและจัดการกรณีพิพาทนั้นให้เสร็จสิ้นโดยเร็ว

17. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

17.1 คณะกรรมการดำเนินการจ้างฯ จะพิจารณาคัดเลือกข้อเสนอ ดังนี้

17.1.1 พิจารณาจากข้อกำหนดทางเทคนิคโดยมีน้ำหนักคะแนน 60 คะแนน มีรายการพิจารณา ดังนี้

17.1.1.1 การออกแบบระบบและการนำเสนอ 15 คะแนน

(1) รายงานการออกแบบระบบ (10 คะแนน)

(2) เอกสารและการนำเสนอ (5 คะแนน)

17.1.1.2 ประสิทธิภาพของอุปกรณ์ที่เสนอ 30 คะแนน

(1) Core Switch, Access Switch ตามข้อ 5.1.1, 5.1.2 (10 คะแนน)

(2) อุปกรณ์ป้องกันเครือข่าย (Firewall) ตามข้อ 5.1.3 (10 คะแนน)

(3) ซอฟต์แวร์ (Software) บริหารจัดการเครือข่าย ตามข้อ 5.1.6 (5 คะแนน)

(4) อุปกรณ์อื่นๆ (5 คะแนน)

17.1.1.3 ข้อเสนอด้านบุคลากรของโครงการ 5 คะแนน

17.1.1.4 ข้อเสนอในการบริการ (Service Level Agreement : SLA) 5 คะแนน

17.1.1.5 ข้อเสนอการฝึกอบรม 5 คะแนน

17.1.2 พิจารณาจากราคา โดยมีน้ำหนักคะแนน 40 คะแนน

เอกสารแนบท้าย 2: แบบฟอร์มรายงานสถานะและผลทดสอบการทำงานของอุปกรณ์

Project Name :					
Location :					
Contract No.:					
Product Information					
Model :		**Part Number :**		**Serial Number :**	

Check list

1. System Information Check

Boot time	
Firmware Version	

2. Module Check

Module Name/ Slot no	Module Status	Post Status	Remark

3. Management Check

Item	Yes	No	Remark
Serial console Port			
Telnet			
Web			
SNMP			

4. Comfiguration Check

Item	Yes	No	Remark
Backup Config			
Modified Config			
System Log			

5. Special Comment