โครงการพัฒนาระบบเครือข่ายเพื่อสนับสนุนการเรียนการสอน
คุณสมบัติของระบบแยกตามรายการ ดังนี้

1 ระบบป้องกันและตรวจจับการบุกรุกเครือข่าย (Firewall) จำนวน 1 ระบบ

คุณลักษณะเฉพาะระบบป้องกันและตรวจจับการบุกรุกเครือข่ายดังต่อไปนี้

1) เป็นอุปกรณ์ Appliance ที่มีหน่วยประมวลผลเป็นแบบ ASIC ซึ่งได้รับการออกแบบมาเพื่อทำหน้าที่รักษาความปลอดภัยของเครือข่ายโดยเฉพาะ
2) มี Network Interface แบบ 10GE SFP+ อย่างน้อย 2 ports และ แบบ Gigabit (RJ45) ไม่น้อยกว่า 14 ports
3) มีความเร็วในการทำงานของ Firewall ได้ไม่น้อยกว่า 20/20/20Gbpsโดยที่ package UDP (1518/512/64 byte UDP) ตามลำดับ และได้รับการรองรับตามมาตรฐานของ ICSA ด้าน Firewall
4) สามารถรองรับการเชื่อมต่อพร้อมๆกัน (concurrent Sessions) ได้ไม่น้อยกว่า 7,000,000 การเชื่อมต่อ และ รองรับการเชื่อมต่อใหม่ (New Sessions/Second) ได้ด้วยความเร็วไม่น้อยกว่า 190,000 การเชื่อมต่อ (sessions) ต่อวินาที
5) มีความสามารถในการตรวจจับและป้องกันไวรัสคอมพิวเตอร์ในโปรโตคอล FTP, HTTP, IMAP, IMAPS, POP3, POP3S, SMTP และ SMTPS โดยได้รับการรองรับตามมาตรฐานของ ICSA ด้าน Antivirus และต้องสามารถ update ฐานข้อมูลไวรัสฯ (virus signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติตลอด ระยะของการรับประกันอุปกรณ์
6) มีความสามารถในการป้องกันการบุกรุก (Intrusion Prevention) โดยสามารถ update ฐานข้อมูลการบุกรุก (attack signature) ผ่านเครือข่าย Internet ได้เองโดยอัตโนมัติตลอดระยะของการรับประกัน และได้รับการ รับรองมาตรฐานจาก ICSA ด้าน Intrusion Prevention
7) สามารถเข้ารหัสเพื่อการส่งข้อมูลด้วยวิธีการ VPN โดยมีใช้วิธีการเข้ารหัสแบบ 3DES/AES IPSecและ SSL-VPN เพื่อความปลอดภัยในการติดต่อจากระยะไกลได้ และได้รับการรับรองตามมาตรฐานของ ICSA ด้าน IPSecและ SSL-VPN
8) มีความเร็วในการทำงาน IPSec VPN ได้ไม่น้อยกว่า 8Gbps
9) รองรับการเชื่อมโยงด้วย SSL VPN พร้อมๆ กันได้ไม่น้อยกว่า 10,000 users
10) สามารถทำงานในลักษณะ Content Filtering ได้ โดยสามารถกำหนดให้อุปกรณ์ป้องกันการเข้าถึง URL หรือ Web site ที่ต้องห้ามได้ (URL blocking)
11) สามารถป้องกันการเข้าถึง Web site โดยกำหนดแยกตามประเภทของ Web site (Web Categories) ได้ โดยมี สิทธิในการเข้าตรวจสอบฐานข้อมูลประเภทของ Web site ได้ตลอดระยะของการรับประกัน
12) รองรับการตรวจสอบผู้ใช้ (User Authentication) กับฐานข้อมูลผู้ใช้ภายในตัวอุปกรณ์, ผู้ใช้ใน RADIUS, ใน LDAP และ Windows Active Directory ได้เป็นอย่างน้อย

13) สามารถระบุชนิดและควบคุมการใช้งาน Application ต่างๆ ได้ไม่น้อยกว่า 3,000 Applications โดยต้องมี Application ตามรายการต่อไปนี้ด้วย
    - Application Peer-to-Peer ได้แก่ Bit Torrent, eDonkey, Gnutella, Kazaaและ and WinNY
    - Instant Messaging ได้แก่ MSN, Yahoo IM, AOL-IM, ICQ ,Facebook, Youtubeและ MySpace
14) สามารถกำหนดนโยบายรักษาความปลอดภัยที่แตกต่างกัน ตามรายละเอียดเฉพาะของเครื่องใช้งาน ดังต่อไปนี้ ได้เป็นอย่างน้อย
    - แยกตามระบบปฏิบัติการเครื่องคอมพิวเตอร์ที่ใช้งาน อันได้แก่ Mac OS, Windows และ Linux
    - แยกตามชนิดของ Smart Phone ที่ใช้งาน อันได้แก่ iPhone, Android, Windows และ BlackBerry
    - แยกตามชนิดของ Tablet ที่ใช้งาน อันได้แก่ iPad, Android, Windows และ BlackBerry Playbook
15) มี Hard Disk ความจุไม่น้อยกว่า 128 GB และมี Power Supply เป็นแบบ Redundant

2. ระบบป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) จำนวน 1 ระบบ

คุณลักษณะเฉพาะระบบป้องกันการบุกรุกเว็บไซต์ ดังต่อไปนี้

1) เป็นอุปกรณ์ทำหน้าที่ในการป้องกันด้าน Web Application หรือ Web Service โดยเฉพาะ
2) มีจุดเชื่อมต่อ Network แบบ 10/100/1000 Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 4 Ports
3) รองรับการส่งผ่านข้อมูลได้อย่างน้อย 100 Mbps
4) อุปกรณ์ที่นำเสนอต้องมีขนาดพื้นที่จัดเก็บข้อมูล(Disk Storage) ไม่น้อยกว่า 1 TB เป็นอย่างน้อย
5) อุปกรณ์ที่นำเสนอต้องไม่มีกำหนด Application licenses (unlimited licenses)
6) สามารถบริหารจัดการอุปกรณ์ผ่านทาง Web Base หรือ CLI ได้เป็นอย่างน้อย
7) สามารถตรวจจับพฤติกรรมการใช้งาน Web Application ของผู้ที่เข้ามาใช้บริการ Web Application บนเครื่องคอมพิวเตอร์แม่ข่ายต่างๆ ได้
8) อุปกรณ์ที่นำเสนอจะต้องสามารถทำงานแบบ Transparent Inspection และTrue Transparent Proxy และ Reverse Proxy และ Offline Sniffing สำหรับตรวจสอบพฤติกรรมได้เป็นอย่างน้อย
9) มีความสามารถในการทำงานและปกป้อง Web Application ต่างๆได้โดยรองรับ HTTP และ HTTPS ได้เป็นอย่างน้อย
10) สามารถส่งข้อมูล Log File แบบ Syslog ได้เป็นอย่างน้อย
11) สามารถปรับเทียบเวลา (Sync) กับอุปกรณ์ภายนอกได้
12) สามารถทำ Authentication Offload แบบ Local, LDAP, NTLM และ Radius ได้เป็นอย่างน้อย

13) สามารถรองรับการทำงาน High Availability แบบ Active / Passive ได้

14) รองรับการทำงาน แบบ SSL offload ได้เป็นอย่างน้อย

15) สามารถทำงาน Vulnerability Scanner PCI DSS 6.6

16) รองรับการป้องกันการถูกโจมตีด้วยวิธีต่างๆ ได้อย่างน้อยดังนี้

- Cross-site Scripting
- Cookie Poisoning
- Session Hijacking
- Command injection
- Outbound Data Leakage
- Brute Force Login
- Access Rate Control
- Remote File Inclusion
- Search Engine Hacking
- Buffer Overflow
- SQL injection

17) สามารถทำรายงานการถูกโจมตีได้ในรูปแบบ HTML หรือ PDF หรือ XLS หรือดีกว่า

18) สามารถใช้งานตามมาตรฐาน IPv6 ได้

19) อุปกรณ์ที่นำเสนอต้องได้รับ Certified ICSA WAF เป็นอย่างน้อย

20) อุปกรณ์ที่นำเสนอต้องได้รับมาตรฐาน FCC Part 15 Class A , CE ,UL,CB,VCCI เป็นอย่างน้อย

3. ระบบกระจายสัญญาณหลัก (Core Switch)

คุณลักษณะเฉพาะระบบกระจายสัญญาณหลัก ดังต่อไปนี้

1) โครงสร้างเป็นลักษณะ (Modular Chassis) สามารถรองรับ Switching Bandwidth ที่มีความเร็วไม่น้อยกว่า 920Gbpsและมีความสามารถในการรับส่งข้อมูลไม่น้อยกว่า 250Mppsสำหรับ IPv4 และ 125Mppsสำหรับ IPv6
2) รองรับการเพิ่มหน่วยประมวลผล Processor Engine และ Switching Fabric สำรองที่สามารถทำงานทดแทน กันได้ทันทีในลักษณะ N+1 Redundancy โดยขนาดของ Switching Fabric ต้องไม่น้อยกว่า 920 Gbpsใน กรณีที่ Processor Engine หรือ Switching Fabric หลักหยุดทำงาน
3) มีซอฟต์แวร์ปฏิบัติการ (OS) แบบ Modular เพื่อสนับสนุนการให้บริการแบบ Non-Stop โดยทำ Multitasking Process และ Protect Memory ของแต่ละ Process ได้

4) รองรับการทำ ISSU (In-Service Software Upgrade) และ Hitless Failover หรือ Stateful Switch Over ในกรณีที่ Processor Engine หลักเสียหรือหยุดทำงาน โดยฟังก์ชั่น STP, LACP, 802.1x authentication, VRRP ต้องสามารถทำงานต่อเนื่องได้โดยไม่หยุดชะงัก
5) สนับสนุนการทำ Non-Stop Routing และ Non-Stop Forwarding ได้
6) มีระบบจ่ายไฟสำรอง N+1 Redundancy Power Supply
7) มีพอร์ต Gigabit Ethernet แบบ 10/100/1000BaseTไม่น้อยกว่า 48 พอร์ต
8) พอร์ต 10 Gigabit Ethernet แบบ SFP อย่างน้อย 8 พอร์ต
9) SFP Module แบบ Single Mode หัวต่อแบบ LC สามารถทำงานร่วมกับ Switch Cisco ได้ จำนวนไม่น้อยกว่า 5 ตัว
10) สามารถเพิ่มโมดูล เพื่อเชื่อมต่อกับอุปกรณ์ CWDM (Coarse Wavelength-Division Multiplexing) และ DWDM (Dense Wavelength-Division Multiplexing) ได้
11) รองรับ Power over Ethernet ตามมาตรฐาน IEEE 802.3afและ IEEE 802.3at ได้ไม่น้อยกว่า 60 watts ต่อพอร์ต
12) รองรับการทำ hop-by-hop encryption ตามมาตรฐาน IEEE 802.1AE และ Security Group Tags (hardware-ready) ได้เป็นอย่างน้อย
13) สามารถสนับสนุนจำนวน MAC Addresses ไม่น้อยกว่า 55,000 addresses
14) สามารถทำงานตามมาตรฐาน IEEE802.1D, IEEE802.1w, IEEE802.1s, IEEE802.1p และ IEEE802.1q และสามารถติดตั้ง VLAN id. ได้ไม่น้อยกว่า 4,094 Active VLAN และสามารถที่จะแลกเปลี่ยนข้อมูล ระหว่างอุปกรณ์ LAN Switch ที่เสนอมาทั้งหมดได้
15) เมื่อมีอุปกรณ์ใหม่ (IP Devices) เข้ามาต่อเชื่อมในระบบเครือข่าย อุปกรณ์สามารถแจ้งเตือนผู้ดูแลระบบ ผ่านทาง SNMP Trap และแลกเปลี่ยนข้อมูลระหว่างกันตามมาตรฐาน IEEE 802.1ab Link Layer Discovery Protocol (LLDP) เพื่อที่จะแก้ไขค่าติดตั้ง (configuration) ของพอร์ตนั้น ให้มีเงื่อนไขที่ได้กำหนดไว้ ได้แก่ QoS, port security, PACL, PoE class ได้โดยอัตโนมัติ
16) สนับสนุน Uni-Directional Link Detection (UDLD) สำหรับตรวจสอบความผิดพลาดของการเชื่อมต่อสายสัญญาณได้
17) สนับสนุนการทำ Port Mirror ได้ไม่น้อยกว่า 8 กลุ่มพร้อมๆ กันทั้งขาเข้าและออกจากพอร์ตและ VLAN ที่อยู่ต่างโมดูลกันได้
18) สนับสนุนการทำ Bandwidth Aggregation ตามมาตรฐาน IEEE 802.3ad LACP แบบ Layer 2 (bridge interface) และ Layer 3 (routed interface) aggregation group ได้ไม่น้อยกว่า 8 พอร์ตต่อ 1 กลุ่ม

19) สนับสนุนความสามารถด้านการตรวจสอบและยืนยันตัวตนผู้ใช้งาน (Authentication) ดังต่อไปนี้
    - IEEE 802.1x และ User/Device MAC-Authentication และ Microsoft windows machine authentication
    - สามารถกำหนดรูปแบบการ Authentication ได้แก่ IEEE802.1x, MAC Authentication และ Web Authentication ในแต่ละพอร์ต ตามลำดับก่อนหลัง (Order) ได้
    - สามารถเลือกให้ เปิดใช้งานพอร์ตแบบ Unrestricted Access หรือระบุ ACL ไม่ว่าผู้ใช้/เครื่องจะทำการ Authentication ผ่านหรือไม่ก็ตาม เพื่อให้ง่ายในการเริ่มติดตั้ง และตรวจสอบความพร้อมของผู้ใช้โดย กระทบต่อการทำงานน้อยที่สุด
20) สามารถติดตั้ง Routed Interface ได้ไม่น้อยกว่า 4,000 interfaces เพื่อทำ IP routing protocol ได้แก่ Static Route, RIPv1/2, OSPF, OSPFv3 และ RIPngได้เป็นอย่างน้อย
21) รองรับการทำ IP Multicast routing protocol ได้แก่ PIM Dense Mode, PIM Sparse Mode และ PIM Source Specific Mode ได้ และ IP Multicast membership ได้แก่ IGMPv3 Snooping, MLD และ IGMP filtering ได้เป็นอย่างน้อย
22) รองรับการอัพเกรดซอฟต์แวร์เพื่อทำ Routing protocol ได้แก่ BGP, Virtual Route Forwarding และ Policy based routing ได้ไม่น้อยกว่า 256,000 routes สำหรับ IPv4 และ 128,000 routes สำหรับ IPv6
23) สามารถอัพเกรดซอฟต์แวร์เพื่อทำ fallback bridging (VLAN bridging) เพื่อส่งผ่านข้อมูลที่ไม่ใช่ IP packet (forward non-IP packets) ข้าม VLAN ได้
24) สามารถกำหนดคุณภาพการให้บริการ Quality of Service (QoS) ได้เป็นอย่างน้อย
25) สามารถให้บริการ DHCP server และ DHCP relay ได้
26) มีฟังก์ชั่นที่สามารถป้องกันการโจมตีหน่วยประมวลผลกลาง (CPU DoS Attack) ด้วยการทำ Traffic Rate-Limiting ที่ CPU Input Queue ได้โดยอัตโนมัติ
27) สามารถกำหนดการป้องกันการส่งผ่านข้อมูลด้วย Access Control List (ACL) Layer 2-4 ได้ โดยใช้ Hardware ในระดับ Routed Interface และ Intra VLAN ได้
28) มีฟังก์ชั่นที่สามารถป้องกันการโจมตี หรือบุกรุก ด้วย BPDU Guard, Spanning Tree Root Guard, Port Security, Manual IP and MAC Address Binding, Private VLAN, DHCP Snooping, Dynamic ARP Inspection, Unicast Reverse Path Forwarding (URPF) และ IP Source Guard ได้
29) สนับสนุนการตรวจสอบประสิทธิภาพของโครงข่าย ร่วมกับอุปกรณ์สลับสัญญาณที่นำเสนอในโครงการได้ โดยสามารถตรวจสอบค่า ได้แก่ Delay, Jitter, Packet loss, Packet sequencing, Path, Connectivity, HTTP, FTP, DNS และ DHCP ได้เป็นอย่างน้อย

30) สามารถจัดเก็บข้อมูลสถิติการใช้งานเครือข่าย (IPv4 และ IPv6 Flow Usage Statistic) ตามมาตรฐาน Netflow v9 หรือ sFlow v9 ได้ไม่น้อยกว่า 128,000IPv4 Flows และสามารถสุ่มการจัดเก็บข้อมูล Sampling Flow และทำ Flexible flow เพื่อเลือกประเภทหรือกลุ่มของข้อมูลและส่งไปยัง collector ที่แตกต่างกันได้ มากกว่า 3 เครื่องพร้อมๆ กัน
31) สนับสนุนการป้องกัน Anomaly traffic และ malware โดยการกำหนดนโยบายผ่านทาง Flexible NetFlowหรือ sFlowได้
32) มีระบบจ่ายไฟขนาดไม่น้อยกว่า 1000 Watt และรองรับการทำ Redundant Power Supply ได้
33) มีพอร์ต Out-of-band management แบบ RS-232, USB และ 10/100/1000Base TXอย่างละ 1 พอร์ต เพื่อต่อ Terminal กำหนดค่าการทำงานของอุปกรณ์ และสำหรับตรวจสอบระบบได้ โดยในระหว่างการแก้ไข Configuration ต้องสามารถทำ Rollback ได้
34) สามารถทำ Layer 2 trace route ได้ เพื่อช่วยในการแก้ปัญหาและตรวจสอบหา physical path โดยดูจาก source และ/หรือ destination ของ MAC ได้
35) สามารถเข้าไปบริหารและจัดการอุปกรณ์ด้วย CLI, Telnet, debug, SSHv2, NTPv3, Syslog, และ SNMPv3 ได้

4. ระบบบริหารจัดการ DNS, DHCP

คุณลักษณะเฉพาะระบบบริหารจัดการ DNS, DHCP ดังต่อไปนี้

1) อุปกรณ์ออกแบบมาสำหรับใช้ในการบริหารจัดการระบบ DNS และ DHCP โดยเฉพาะ
2) มีความสามารถในการจัดการ/ให้บริการ DNS, DNSSEC, DHCP, NTP, TFTP และ IP Address Management ได้ภายในอุปกรณ์ตัวเดียวกัน
3) มีจุดเชื่อมต่อชนิด 10/100/1000 Base-T Ethernet จำนวนไม่น้อยกว่า 2 พอร์ต และมีจุดเชื่อมต่อสำหรับ HA แยกโดยอิสระชนิด 10/100/1000 Base-T Ethernet จำนวนไม่น้อยกว่า 1 พอร์ต
4) มีจุดเชื่อมต่อสำหรับบริหารจัดการอุปกรณ์ (Management interface) ชนิด 10/100/1000 Base-T Ethernet จำนวนไม่น้อยกว่า 1 พอร์ต
5) มี LCD Panel สำหรับตรวจดูสถานะของอุปกรณ์คร่าวๆ ได้ เช่น network setting, software version, serial number เป็นต้น
6) รองรับ DNS Query ได้ไม่น้อยกว่า 15,000 queries per sec และ DHCP Lease per sec ไม่น้อยกว่า 105 Leases per sec โดยสามารถอ้างอิงได้จาก web site หรือ เอกสารจากเจ้าของผลิตภัณฑ์
7) ระบบบริหารจัดการอุปกรณ์จะต้องเป็นแบบ GUI หรือ Web base ได้
8) มีความสามารถในการทำ HA, MAC Address filtering ได้

9) รองรับการทำ centralized management แบบ Grid ได้ในอนาคต โดยไม่จำเป็นต้องเปลี่ยนอุปกรณ์
10) รองรับการบริหารจัดการ Microsoft DNS, DHCP ได้ในอนาคต โดยไม่จำเป็นต้องเปลี่ยนอุปกรณ์
11) สามารถทำ TSIG (Secret key transaction authentication), DNSSEC หรือ ระบบ Secure Transfer อื่นๆ ที่ดีกว่า
12) สามารถกำหนดระดับของ Admin ให้มีสิทธิในการจัดการแยกแต่ละ Network หรือ ระบบ หรือ Device ได้ (Granular, Role-Base Administration)
13) ได้รับมาตรฐานความปลอดภัยดังต่อไปนี้ เป็นอย่างน้อย UL, FCC, CE และ RoHS
14) สามารถทำ Real-Time update (ในส่วนของ DNS) เช่น Dynamic DNS ได้เป็นอย่างน้อย
15) มีระบบ Time Synchronize service โดยผ่านทาง NTP protocol
16) รองรับ Remote Management แบบ Light Out Management, IPMI 2.0

5. ข้อกำหนดเพิ่มเติม

1) อุปกรณ์ที่ติดตั้งในระบบป้องกันและตรวจจับการบุกรุกเครือข่าย ต้องสามารถกำหนดการพิสูจน์ตัวตนเพื่อใช้งานทรัพยากรที่อยู่ภายในระบบโดยทำการพิสูจน์ตัวตนเพียงครั้งเดียว (RADIUS Single Sign On) และสามารถใช้ร่วมกับ อุปกรณ์ตัวอื่นได้
2) อุปกรณ์ที่ติดตั้งในระบบต้องสามารถรองรับการทำงานร่วมกับระบบ EDU Roam ได้
3) การกำหนดนโยบายระบบป้องกันและตรวจจับการบุกรุกเครือข่ายและระบบป้องกันการบุกรุก ต้องถูกกำหนดโดยวิศวกรจากบริษัทที่มีผู้เชี่ยวชาญร่วมกับผู้ดูแลระบบของทางมหาวิทยาลัย
4) การกำหนดรูปแบบการทำงานของระบบกระจายสัญญาณหลัก (Core Switch) ต้องถูกกำหนดโดยวิศวกรจากบริษัทที่มีผู้เชี่ยวชาญร่วมกับผู้ดูแลระบบของทางมหาวิทยาลัย
5) การกำหนดรูปแบบการทำงานของ DNS และ DHCPต้องถูกกำหนดโดยวิศวกรจากบริษัทที่มีผู้เชี่ยวชาญร่วมกับผู้ดูแลระบบของทางมหาวิทยาลัย
6) อุปกรณ์ที่ติดตั้งภายในระบบต้องนำมาให้คณะกรรมการตรวจรับ ตรวจสอบก่อนที่จะดำเนินการติดตั้ง
7) อุปกรณ์ที่ติดตั้งภายในระบบ ต้องสามารถติดตั้งในตู้เก็บอุปกรณ์มาตรฐานขนาด 19 นิ้วได้
8) ผู้รับจ้างต้องติดตั้งและทดสอบการทำงานของระบบจนสามารถใช้งานได้สมบูรณ์ ก่อนส่งมอบระบบ
9) ระหว่างการติดตั้ง หากทำงานนอกเวลาราชการ ผู้รับจ้างฯจะต้องเป็นผู้รับภาระในการจ่ายค่าล่วงเวลาให้กับเจ้าหน้าที่ของผู้ว่าจ้าง
10) สามารถทำงานกับระบบไฟฟ้าในประเทศไทยแบบ 220-240 VAC, 50Hz ได้
11) ผู้รับจ้าง ต้องรับประกันคุณภาพการทำงานภาพรวมของระบบ จากการติดตั้งอุปกรณ์เป็นระยะเวลาอย่างน้อย 1 ปี โดยอุปกรณ์ที่ติดตั้งในระบบต้องสามารถเชื่อมต่อใช้งานร่วมกับระบบเดิมของมหาวิทยาลัยที่มีการใช้งานอยู่ในปัจจุบันได้เป็นอย่างดี

12) ผู้รับจ้างต้องติดตั้งระบบและเดินสายเชื่อมต่ออุปกรณ์ให้เป็นระเบียบโดยใช้อุปกรณ์ช่วยในการจัดเก็บสายทั้งระบบ
13) อุปกรณ์ที่ติดตั้งในระบบ ต้องเชื่อมต่อกับระบบสำรองไฟฟ้าเดิมภายในห้องที่กำหนดให้
14) อุปกรณ์ที่ติดตั้งในระบบ สามารถ Upgrade firmware ได้ตลอดอายุการใช้งาน
15) ผู้รับจ้างต้องดำเนินการอบรมการใช้งานของทุกอุปกรณ์
16) ผู้รับจ้างฯ จะต้องรับประกันคุณภาพการทำงานของระบบ รวมถึงอุปกรณ์ที่ติดตั้งในระบบแบบOn-site serviceโดยเมื่อกรณีที่ระบบมีปัญหาที่ไม่เกี่ยวกับความเสียหายของอุปกรณ์ ผู้รับจ้างฯ ต้องแก้ไขให้ระบบสามารถกลับมาใช้งานได้ภายใน 12 ชั่วโมง และเมื่อกรณีที่ระบบมีปัญหาเนื่องจากความเสียหายของอุปกรณ์ผู้รับจ้างฯ ต้องเปลี่ยนอุปกรณ์ที่สามารถทดแทนให้สามารถใช้งานได้ปกติภายใน 48 ชั่วโมง ให้เริ่มนับตั้งแต่วันตรวจรับ โดยการให้บริการ ผู้รับจ้างฯ จะต้องทำการซ่อมแซม หรือเปลี่ยนใหม่โดยให้ยึดเวลาที่แจ้งซ่อมหรือขอรับบริการเป็นสำคัญ โดยที่ผู้ว่าจ้าง ไม่ต้องรับผิดชอบค่าใช้จ่ายใด ๆ ทั้งสิ้น นอกเสียจากความเสียหายนั้นเกิดจากภัยธรรมชาติ หรือมีข้อพิสูจน์ว่าความเสียหายที่เกิดขึ้น ไม่ได้เกิดจากคุณภาพของอุปกรณ์
ผู้รับจ้างฯ จะต้องมีแผนการบำรุงรักษาระบบ และดำเนินการตรวจเช็คตามแผน อย่างน้อยปีละ 1 ครั้ง
17) อุปกรณ์ทีเสนอทุกรายการ ต้องรับประกันตัวสินค้าอย่างน้อย 1 ปี โดยมีหนังสือรับรองการรับประกันจากผู้ผลิต

******มหาวิทยาลัยราชภัฏเพชรบูรณ์******