

อ้างอิงถึงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	หน้าเอกสารอ้างอิง
2. ระบบรักษาความปลอดภัยเครือข่ายศูนย์ข้อมูล (Security System) จำนวน 1 ระบบ มีรายละเอียดดังต่อไปนี้			
2.1	อุปกรณ์ป้องกันการโจมตีเครือข่ายคอมพิวเตอร์ (Network Firewall) จำนวน 1 ระบบ มีคุณสมบัติอย่างน้อยดังต่อไปนี้		
2.1.1	เป็นอุปกรณ์ที่ได้รับการออกแบบสำหรับติดตั้งกับตู้ อุปกรณ์สื่อสารมาตรฐาน 19 นิ้ว (19" Rack) โดยเฉพาะ พร้อมอุปกรณ์ประกอบยึดเพื่อติดตั้ง		
2.1.2	เป็นอุปกรณ์ที่ได้รับการออกแบบการทำงานขึ้นมาเพื่อการป้องกันการโจมตีเครือข่ายคอมพิวเตอร์ (Network Firewall) โดยเฉพาะ		
2.1.3	ต้องทำงานในลักษณะ High Availability (HA) แบบ Active/Passive หรือ Active/Active ได้		
2.1.4	เป็นอุปกรณ์เครือข่ายแบบ Appliance ที่มีประสิทธิภาพการทำงานด้าน Firewall ไม่น้อยกว่า 36 Gbps และมีประสิทธิภาพการทำงานไม่น้อยกว่า 16 Gbps เมื่อเปิดใช้งาน IPS		
2.1.5	เป็นอุปกรณ์ที่ออกแบบให้มีช่องเชื่อมต่อเครือข่ายเป็นแบบ Modular เพื่อสามารถเปลี่ยนแปลงและเพิ่มขยายชนิดของ Interface ใช้งานได้		

อ้างอิงถึงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	หน้าเอกสารอ้างอิง
2.1.6	อุปกรณ์มีช่องเชื่อมต่อ 2.5 Gigabit Ethernet จำนวนอย่างน้อย 8 พอร์ต และมีพอร์ตแบบ 10 Gigabit ชนิด Fiber อย่างน้อย 2 พอร์ต และต้องมี Module เพิ่มขยายพอร์ตแบบ 10 Gigabit ได้อีกอย่างน้อย 4 พอร์ต พร้อม Transceiver SFP+ MM 8 units		
2.1.7	มีหน่วยเก็บข้อมูลขนาดความจุไม่น้อยกว่า 200 GB		
2.1.8	มี power supply จำนวน 2 หน่วย ทำงานแบบ Redundant		
2.1.9	สามารถรองรับจำนวนการเชื่อมต่อพร้อมกัน (Concurrent Connection) ได้อย่างน้อย 1,500,000 Connections		
2.1.10	สามารถรองรับจำนวนการเชื่อมต่อใหม่ต่อวินาที (New Connection) ได้อย่างน้อย 80,000 New Connection ต่อวินาที		
2.1.11	สามารถทำงาน IPSec VPN ได้ โดยมีประสิทธิภาพการทำงานไม่น้อยกว่า 6 Gbps และรองรับการเข้ารหัสได้สูงสุด 8,192 bit		
2.1.12	รองรับการทำ IPSec VPN ได้ไม่น้อยกว่า 2,000 Tunnel		

อ้างอิงถึงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	หน้าเอกสารอ้างอิง
2.1.13	รองรับการเข้าถึงเครือข่ายจากระยะไกลแบบ SSL VPN ได้ไม่น้อยกว่า 500 clients		
2.1.14	สามารถทำ Firewall Rule หรือ Filter ตรวจสอบและควบคุมการสื่อสารข้อมูล (Traffic) โดยจำแนกตามประเภทของ แอปพลิเคชัน (Application) ได้ และสามารถอำนวยความสะดวกในการทำ Firewall Rule/Filter ด้วยการทำ Drag and Drop ได้		
2.1.15	ต้องกำหนดนโยบายการใช้งานแบบ User-Based Policy ได้		
2.1.16	ต้องสามารถทำนโยบาย Host Reputation เพื่อกำหนด score ความปลอดภัยได้		
2.1.17	ต้องทำ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้		
2.1.18	ต้องใช้งานหรือกำหนด Routing แบบ Static, Policy Based Routing และ Dynamic Routing แบบ RIP, OSPF, และ BGP ได้		
2.1.19	ต้องทำงานในแบบ Transparent Mode, Routed Mode, และ Hybrid Mode ได้		
2.1.20	ต้องทำ WAN Link Redundancy ได้		

อ้างอิงถึงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	หน้าเอกสารอ้างอิง
2.1.21	ต้องป้องกันการโจมตีเครือข่ายคอมพิวเตอร์จากภายนอกในรูปแบบดังนี้ ได้เป็นอย่างดีน้อย เช่น TCP Syn Flood, UDP Flood, ICMP Flood, IP Address Spoof, Port Scan, DoS/DDoS, Buffer Overflow, Cross Site Scripting, SQL Injection, Malicious Web 2.0 code, Data evasion, Trojan, Virus, Botnet และ Spyware		
2.1.22	สามารถสร้างรายงานได้บนตัวอุปกรณ์ (Embedded Reporting) สำหรับการตรวจสอบได้ดังต่อไปนี้ Top Host, Top Protocol, Top Website และส่งออกในรูปแบบไฟล์ PDF ได้		
2.1.23	สามารถบริหารจัดการอุปกรณ์ผ่านทาง Web Browser และทำงานแบบ Privacy mode ตามมาตรฐาน GDPR ได้		
2.1.24	มีความสามารถในการทำ Private data management โดยสามารถออก Ticket ชั่วคราวสำหรับผู้บริหารจัดการที่ต้องการเข้าถึง Log หรือ ข้อมูลที่เป็น Private data ได้		

อ้างอิงถึงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	หน้าเอกสารอ้างอิง
2.1.25	สามารถทำงาน Authentication แบบ Multi Domain และมี Internal LDAP เพื่อใช้เก็บชื่อและรหัสผู้ใช้งาน บนตัวอุปกรณ์เอง		
2.1.26	ต้องแจ้งเตือนในกรณีที่เกิดเหตุการณ์ต่างๆ ผ่านทาง SMTP และ SNMP ได้		
2.1.27	ต้องสามารถส่งออกข้อมูลจากการบันทึก (Log) ผ่านทาง Syslog โดยรองรับรูปแบบ UDP, TCP และ TLS ได้เป็นอย่างน้อย		
2.1.28	รองรับการบริหารจัดการช่องโหว่ (Vulnerability Management) โดยใช้เทคนิคการวิเคราะห์แบบ Passive Scanner ที่ตรวจจับช่องโหว่ได้ในทันที ขณะนั้น (real-time) โดยสามารถตรวจจับชนิดของ Operating System, Application และ Host ของ อุปกรณ์ภายในเครือข่าย รวมทั้งแสดงข้อมูลรายละเอียด ระดับความรุนแรงของช่องโหว่ที่ตรวจพบ (Criticality) และวิธีการแก้ไข (Remediation) ให้ผู้ปฏิบัติงานทราบ ได้		
2.1.29	ต้องเป็นอุปกรณ์ที่ได้รับการรับรองตามมาตรฐานความปลอดภัย CE, CB และ FCC		

อ้างอิงถึงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	หน้าเอกสารอ้างอิง
2.1.30	ต้องเป็นอุปกรณ์ที่ใช้งานตามมาตรฐาน IPv4 และ IPv6 ได้		
2.1.31	อุปกรณ์ต้องมีการรับประกันสินค้าจากผู้ผลิตโดยตรง หรือผู้แทนจำหน่ายที่ได้รับการแต่งตั้งอย่างเป็นทางการ ประจำสาขาในประเทศไทยเป็นระยะเวลาไม่น้อยกว่า 2 ปี โดยแสดงหนังสือเอกสารยืนยันว่าจะรับประกันมา พร้อมกับการเสนอราคา		
2.1.32	ผู้เสนอราคาต้องจัดหาอุปกรณ์จากบริษัทผู้ผลิตหรือจากตัวแทนจำหน่ายที่ได้รับการแต่งตั้งอย่างเป็นทางการ ประจำสาขาในประเทศไทย โดยต้องแสดงหนังสือหรือเอกสารหลักฐานการเป็นตัวแทนจำหน่ายประจำสาขา ประเทศไทยมาพร้อมการยื่นข้อเสนอประกวดราคา		
2.1.33	ผู้เสนอราคาจำเป็นต้องกรอกตารางรายละเอียดคุณลักษณะเปรียบเทียบโดยแจ้งถ้อยคำที่ปรากฏตามรายละเอียดคุณลักษณะอย่างเป็นจริงเพื่อแสดงคุณสมบัติครุภัณฑ์ที่ผู้เสนอราคาต้องการที่จะนำเสนอ ในช่องว่างด้านคุณลักษณะเฉพาะที่เสนอเพื่อทำการเปรียบเทียบรายละเอียดในแต่ละรายการทุกรายการ โดยครบถ้วนและไม่บิดเบือนจากรายละเอียด คุณลักษณะของกรมฝนหลวงและการบินเกษตร		

อ้างอิงถึงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	หน้าเอกสารอ้างอิง
2.1.34	ผู้เสนอราคายอมรับที่จะกรอกข้อความโดยครบถ้วน และจะไม่ปิดเป็นรายละเอียดคุณลักษณะของกรมฝนหลวงและการบินเกษตรและยอมรับผลการพิจารณา โดยยึดจากรายละเอียดคุณลักษณะที่กำหนดของกรม ฝนหลวงและการบินเกษตร		