ภาคผนวก ๑

รายละเอียดคุณลักษณะเฉพาะ

ภาคผนวก ๑
รายละเอียดคุณลักษณะเฉพาะสำหรับ
โครงการพัฒนาและปรับปรุงระบบความมั่นคงปลอดภัย
ระบบเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงการคลัง

ระบบคอมพิวเตอร์สำหรับ โครงการพัฒนาและปรับปรุงระบบความมั่นคงปลอดภัย ระบบเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงการคลัง ที่จะจัดซื้อครั้งนี้ จะต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ อยู่ในสภาพที่ใช้งานได้ทันที และมีคุณลักษณะเฉพาะตรงตามที่กำหนดไว้ ดังมีรายละเอียดต่อไปนี้

๑. ระบบบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารแบบรวมศูนย์ ๑ ระบบ ประกอบไปด้วย

๑.๑ ระบบบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารแบบรวมศูนย์ จำนวน ๑ ระบบ มีคุณลักษณะอย่างน้อย ดังนี้

๑.๑.๑ เป็นอุปกรณ์ Appliance ที่ออกแบบมาเพื่อใช้งานในลักษณะ SIEM (Security Incident and Event Management) โดยเฉพาะ

๑.๑.๒ สามารถวิเคราะห์หาความสัมพันธ์ (Correlation) ของข้อมูล Log หรือ Event เพื่อการเฝ้าระวังและเตือนภัยเหตุการณ์ภัยคุกคามได้ในแบบ Real Time

๑.๑.๓ สามารถรับเหตุการณ์ที่เกิดขึ้นอย่างต่อเนื่องได้ไม่น้อยกว่า ๖๐,๐๐๐ เหตุการณ์ต่อวินาที (Event Per Second : EPS)

๑.๑.๔ มีส่วนที่ทำหน้าที่รับ Log จากอุปกรณ์ต้นทาง โดยสามารถรับ Log จากอุปกรณ์ต่าง ๆ และแปลงให้อยู่ในรูปแบบที่เหมาะสมเพื่อใช้วิเคราะห์หาความสัมพันธ์ ได้ไม่น้อยกว่า ๒๔,๐๐๐ เหตุการณ์ต่อวินาที (Event Per Second: EPS) หรือเสนออุปกรณ์ภายนอกมาเชื่อมต่อซึ่งสามารถทำหน้าที่ดังกล่าวทดแทนได้ โดยมีประสิทธิภาพไม่น้อยกว่าคุณลักษณะข้างต้น และมีหน่วยความจำหรือพื้นที่จัดเก็บข้อมูลที่สามารถจัดเก็บ Log ที่ถูกแปลงแล้ว ได้ในตัวเอง เพื่อป้องกันการสูญหายของข้อมูล ในกรณีที่เกิดปัญหาการเชื่อมต่อ

๑.๑.๕ สามารถรับ Log หรือ Event และแปลงให้อยู่ในรูปแบบที่เหมาะสมในการวิเคราะห์หาความสัมพันธ์ ได้ไม่น้อยกว่า ๑๕๐ ผลิตภัณฑ์

๑.๑.๖ สามารถวิเคราะห์ข้อมูล Log หรือ Event จากอุปกรณ์และระบบต่าง ๆ ได้แก่ Firewall, IDS/IPS, Switch, Router, Anti-Virus, Web Server ได้แก่ Apache, IIS ระบบปฏิบัติการ ได้แก่ UNIX, Windows ระบบฐานข้อมูล ได้แก่ Oracle, MySQL, MSSQL, DB๒ ได้เป็นอย่างน้อย

๑.๑.๗ สามารถวิเคราะห์หาความสัมพันธ์ของข้อมูล Log หรือ Event ระหว่างอุปกรณ์ได้

๑.๑.๘ สามารถลดความซ้ำซ้อนของ Log หรือ Event ที่เกิดขึ้นได้ (Log Aggregation)

๑.๑.๙ สามารถแสดงรายงานในลักษณะ Dashboard และสามารถเพิ่มและปรับแต่งได้

๑.๑.๑๐ สามารถจัดทำรายงานในรูปแบบตาราง และ Graphic ได้ในรูปแบบ Line Chart, Bar Chart, Pie Chart ได้เป็นอย่างน้อย

๑.๑.๑๑ สามารถส่งออก (Export) รายงาน ในรูปแบบ Excel (CSV) และ Pdf ได้เป็นอย่างน้อย

๑.๑.๑๒ สามารถกำหนดเงื่อนไขในการเรียกดูข้อมูลได้ เช่น ตามวันเวลา ตามชื่ออุปกรณ์

๑.๑.๑๓ สามารถกำหนดสิทธิผู้ใช้งานในการเข้าถึงข้อมูลในระดับต่าง ๆ ได้ตามลักษณะหน้าที่ของผู้ใช้ (Role Base Access Control) และสามารถ Integrate กับ LDAP ได้เป็นอย่างน้อย

๑.๑.๑๔ มีหน้าจอบริหารจัดการระบบได้ในรูปแบบ GUI (Graphical User Interface)

๑.๑.๑๕ สามารถแจ้งเตือน (Alert) เมื่อตรวจพบเหตุการณ์ภัยคุกคาม ไปยังผู้ดูแลระบบได้โดยผ่านช่องทาง E-mail, SMS, SNMP และ Syslog ได้เป็นอย่างน้อย

๑.๑.๑๖ สามารถแจ้งเตือนเมื่อตรวจพบเหตุการณ์ภัยคุกคาม ในลักษณะ Case Management ซึ่งสามารถกำหนดขั้นตอนการทำงานในลักษณะ Workflow ได้เป็นอย่างน้อย

๑.๑.๑๗ มี Report และ Dashboard ที่ใช้งานตามมาตรฐาน ISO๒๗๐๐๑ หรือ ISO๒๗๐๐๒ เป็นอย่างน้อย

๑.๑.๑๘ สามารถจัดเก็บคำสั่งหรือรูปแบบการทำรายงานที่สร้างขึ้นเองเพื่อนำมาใช้งานครั้งต่อไปได้โดยไม่ต้องสร้างรายงานขึ้นใหม่

๑.๑.๑๙ สามารถสร้างกลุ่มของ IP Address หรือ Username เพื่อใช้ติดตามภัยคุกคามสารสนเทศของกลุ่มดังกล่าวได้

๑.๑.๒๐ มี Correlation Rule สำเร็จรูปพร้อมใช้งาน ไม่น้อยกว่า ๑๕๐ Rules

๑.๑.๒๑ สามารถทำการสำรองข้อมูล Configuration ต่าง ๆ ไปยัง External Storage ได้

๑.๒ การพัฒนาระบบบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารแบบรวมศูนย์ มีรายละเอียดอย่างน้อย ดังนี้

๑.๒.๑ ดำเนินการสำรวจ วิเคราะห์ รวบรวม ข้อมูล Log หรือ Event ของอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย และอุปกรณ์ด้านความปลอดภัย ของกระทรวงการคลัง ที่มีความสำคัญจำเป็น และเหมาะสม สำหรับการเฝ้าระวังและเตือนภัยเหตุการณ์ภัยคุกคาม

๑.๒.๒ ดำเนินการตรวจสอบช่องโหว่ด้วยการทำ Vulnerability Assessment จำนวนไม่น้อยกว่า ๑๐ อุปกรณ์ หรือ IP Address โดยมีรายละเอียดดังนี้

(๑) ดำเนินการตรวจสอบช่องโหว่ด้วยการทำ Vulnerability Assessment จำนวนอย่างน้อย ๑ ครั้ง และดำเนินการเพิ่มเติม จำนวนไม่น้อยกว่า ๗ ครั้ง ภายในระยะเวลา ๒ ปี หลังการตรวจรับงวดสุดท้ายเสร็จสมบูรณ์ โดยมีรายละเอียดดำเนินการอย่างน้อยดังนี้

(๑.๑) ออกแบบแผน และดำเนินการตรวจสอบช่องโหว่ด้วยการทำ Vulnerability Assessment

(๑.๒) หลังจากการตรวจสอบหาช่องโหว่ในครั้งแรก ต้องทำการตรวจสอบอีกครั้ง เพื่อตรวจสอบว่าช่องโหว่ที่สำคัญได้รับการแก้ไขอย่างเหมาะสม

(๑.๓) ส่งรายงานผล สรุปช่องโหว่ พร้อมข้อแนะนำในการแก้ไขอย่างละเอียดในการตรวจสอบช่องโหว่แต่ละครั้ง

(๒) ดำเนินการเจาะระบบ (Penetration Testing) จำนวนอย่างน้อย ๑ ครั้ง และดำเนินการเพิ่มเติม จำนวนไม่น้อยกว่า ๓ ครั้ง ภายในระยะเวลา ๒ ปี หลังการตรวจรับงวดสุดท้ายเสร็จสมบูรณ์ โดยมีรายละเอียดดำเนินการอย่างน้อยดังนี้

(๒.๑) ออกแบบแผน และดำเนินการเจาะระบบ (Penetration Testing) ในรูปแบบ Black-box penetration testing โดยผู้ให้บริการไม่มีข้อมูลเกี่ยวกับองค์กร ทำการจำลองสถานการณ์การทดสอบจากภายนอก

ระบบ หรือดำเนินการในรูปแบบอื่น ๆ ตามที่คณะกรรมการตรวจรับ หรือผู้ที่ได้รับมอบหมายจากคณะกรรมการตรวจรับ หรือผู้ที่ได้รับมอบหมายจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำหนด

(๒.๒) หลังจากการทดสอบเจาะระบบครั้งแรก ต้องทำการทดสอบเจาะระบบอีกครั้ง เพื่อตรวจสอบว่าช่องโหว่ที่สำคัญได้รับการแก้ไขอย่างเหมาะสม

(๒.๓) ส่งรายงานผล สรุปช่องโหว่ตามลำดับความสำคัญ วิธีการในการแก้ไขอย่างละเอียด ในการเจาะระบบแต่ละครั้ง

(๒.๔) ใช้บุคลากรจำนวนไม่น้อยกว่า ๒ คนขึ้นไป โดยสมาชิกในทีมต้องมีใบรับรอง (Certificate) รวมแล้ว อย่างน้อยดังต่อไปนี้ CISSP, CEH, OSCP, SSCP และ ISO/IEC ๒๗๐๐๑ Lead Auditor

(๒.๕) การเจาะระบบต้องไม่สร้างความเสียหายใด ๆ ต่อระบบอันจะทำให้ระบบไม่สามารถให้บริการต่อไปได้ และต้องแจ้งเจ้าหน้าที่ให้ทราบทุกครั้งก่อนเข้าดำเนินงานในแต่ละขั้นตอน

(๓) ส่งมอบซอฟต์แวร์ ที่ใช้ดำเนินการทำ Vulnerability Assessment ที่มีลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย พร้อมปรับปรุงข้อมูลช่องโหว่ (Updates) เป็นระยะเวลาไม่น้อยกว่า ๒ ปี ในรูปแบบ Virtual Machine (VM)/Virtual Appliance ที่ติดตั้งและทำการ Hardening โดยตรงจากเจ้าของผลิตภัณฑ์

(๔) ซอฟต์แวร์ ที่ใช้ดำเนินการทำ Vulnerability Assessment ในรูปแบบ Virtual Machine (VM)/Virtual Appliance ที่ติดตั้งและทำการ Hardening โดยตรงจากเจ้าของผลิตภัณฑ์ มีคุณลักษณะอย่างน้อยดังนี้

(๔.๑) สามารถตรวจสอบช่องโหว่ครอบคลุมในระดับของ Network, Operating System และ Web Application เป็นอย่างน้อย

(๔.๒) สามารถตรวจสอบช่องโหว่ได้ไม่น้อยกว่า ๑๐ เครื่องพร้อม ๆ กัน

(๔.๓) สามารถตรวจสอบช่องโหว่ของ Web Application ได้ตาม OWASP Top ๑๐ ของปีล่าสุดที่เผยแพร่ ได้เป็นอย่างน้อย

(๔.๔) สามารถตรวจสอบช่องโหว่ในกรณีที่มีการยืนยันตัวตนด้วยบัญชีผู้ใช้ได้

(๔.๕) สามารถตั้งเวลาล่วงหน้าที่จะดำเนินการตรวจสอบช่องโหว่ได้

(๔.๖) สามารถสแกนหาเครื่องคอมพิวเตอร์ต่าง ๆ ภายในระบบเครือข่ายได้แบบอัตโนมัติ พร้อมสร้างแผนผังโครงสร้างระบบเครือข่ายให้สามารถเห็นภาพรวมของระบบ ได้

(๔.๗) สามารถตั้งชื่อและลำดับความสำคัญของเครื่องต่างๆที่จะสแกนได้

(๔.๘) มีหน้าจอรายงานในลักษณะ Dashboard แสดงผลรวมของการตรวจสอบช่องโหว่ และสามารถปรับแต่งได้

(๔.๙) มีการเข้ารหัสแบบ end-to-end ในการส่งข้อมูลระหว่างการตรวจสอบช่องโหว่ เพื่อป้องกันข้อมูลรั่วไหล

(๔.๑๐) สามารถปรับปรุงข้อมูลช่องโหว่ (Updates) ได้แบบอัตโนมัติ

(๔.๑๑) สามารถ Import ผลจากการทดสอบเจาะระบบจากเครื่องมืออื่น ๆ ได้

(๔.๑๒) มี Application Programming Interface (API) เพื่อเชื่อมต่อการทำงานกับระบบอื่น ๆ ได้

(๔.๑๓) สามารถสร้างบัญชีผู้ใช้งานเพื่อเข้าสู่ระบบได้หลายระดับ และจำกัดสิทธิ์ในการดูข้อมูลที่แตกต่างกันได้

๑.๒.๓ ออกแบบและพัฒนาระบบติดตาม เฝ้าระวังเหตุการณ์ผิดปกติ/ภัยคุกคาม อันประกอบด้วยด้วยรายละเอียดอย่างน้อยดังนี้

(๑) วิเคราะห์และออกแบบ ระบบบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารแบบรวมศูนย์

(๒) ออกแบบและจัดทำ Use-Case

(๓) สำรวจ วิเคราะห์ รวบรวม ข้อมูล Log หรือ Event ของอุปกรณ์ ตาม Use-Case

(๔) จัดทำหน้าจอตาม Use-Case เพื่อใช้ติดตาม เฝ้าระวังเหตุการณ์ผิดปกติ/ภัยคุกคาม

(๕) ประเมินความเสี่ยงด้านสารสนเทศของสำนักงานปลัดกระทรวงการคลัง เพื่อใช้ในการจัดทำร่างนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ สำนักงานปลัดกระทรวงการคลัง โดยผู้ประเมินจะต้องมีใบรับรอง (Certificate) ISMS Lead auditor เป็นอย่างน้อย

(๖) จัดทำแผนการจัดการความเสี่ยง (Risk Treatment Plan)

(๗) จัดทำร่างนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ สำนักงานปลัดกระทรวงการคลัง ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(๘) จัดทำร่างนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงการคลัง

(๙) จัดทำสื่อประชาสัมพันธ์แบบวิดีทัศน์ในรูปแบบเอนิเมชั่น แสดงเนื้อหาที่เกี่ยวเนื่องกับภัยคุกคามสารสนเทศ หรือ การเผยแพร่นโยบายและแนวปฏิบัติของกระทรวงการคลัง จำนวนไม่น้อยกว่า ๖ ชิ้นงาน

(๑๐) จัดทำโปสเตอร์ประชาสัมพันธ์ขนาดไม่น้อยกว่า A๓ ที่แสดงเนื้อหาที่เกี่ยวเนื่องกับภัยคุกคามสารสนเทศ หรือ การเผยแพร่นโยบายและแนวปฏิบัติของกระทรวงการคลัง จำนวนไม่น้อยกว่า ๘ รูปแบบ รูปแบบละไม่น้อยกว่า ๒๐ ชิ้น

(๑๑) จัดกิจกรรมประชาสัมพันธ์เพื่อเผยแพร่เนื้อหาที่เกี่ยวเนื่องกับภัยคุกคามสารสนเทศ หรือ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ภายในกระทรวงการคลัง จำนวนไม่น้อยกว่า ๑ ครั้ง

๑.๒.๔ ออกแบบและพัฒนาระบบการแจ้งเตือนกรณีตรวจพบเหตุการณ์ผิดปกติ/ภัยคุกคาม

๑.๒.๕ ออกแบบและพัฒนากระบวนการปฏิบัติงาน กระบวนการตอบสนองต่อเหตุการณ์ผิดปกติ/ภัยคุกคาม

๑.๒.๖ จัดทำคู่มือการตรวจสอบความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย (System and Network Security Checklist) เพื่อให้ผู้ดูแลระบบสามารถใช้เป็นแนวทางเพื่อปฏิบัติตามเพื่อมาตรฐานการรักษาความปลอดภัยของระบบเครือข่ายอย่างต่อเนื่อง

๑.๒.๗ ออกแบบและจัดทำ Use-Case จำนวนไม่น้อยกว่า ๑๐ Use-Case และดำเนินการเพิ่มเติมจำนวนไม่น้อยกว่า ๓ Use-Case ภายในระยะเวลา ๑ ปี หลังการตรวจรับงวดสุดท้ายเสร็จสมบูรณ์ ในหัวข้อเรื่อง เช่น

(๑) การตรวจสอบการเปลี่ยนแปลงหน้าเว็บไซต์จากผู้ไม่ประสงค์ดี พร้อมแจ้งเตือนให้แก่ผู้ดูแลระบบ หรือผู้รับผิดชอบ

(๒) การตรวจสอบการเชื่อมต่อของ Client หรือ Server ในกระทรวงการคลังที่มีปริมาณการเชื่อมต่อในปริมาณมากเกินกว่าปกติ เพื่อตรวจจับ Botnet หรือการแพร่กระจายของ Worm

(๓) การตรวจสอบเหตุการณ์ Link Down ของ Switch ที่มีความสำคัญต่อการเชื่อมต่อระบบสารสนเทศของกระทรวงการคลัง พร้อมแจ้งเตือนให้แก่ผู้ดูแลระบบ หรือผู้รับผิดชอบ

ทั้งนี้ หัวข้อเรื่องสามารถเปลี่ยนแปลงได้ตามที่คณะกรรมการตรวจรับ หรือผู้ที่ได้รับมอบหมายจากคณะกรรมการตรวจรับ หรือผู้ที่ได้รับมอบหมายจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำหนด

๑.๒.๘ จัดหาเจ้าหน้าที่สำหรับติดตามเฝ้าระวังภัยคุกคาม ที่มีความรู้ความสามารถในการใช้งานระบบบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารแบบรวมศูนย์ ประจำที่กระทรวงการคลัง จำนวนไม่น้อยกว่า ๑ คน เป็นระยะเวลา ๑ ปี หลังการตรวจรับงวดสุดท้ายเสร็จสมบูรณ์ โดยมีรายละเอียดคุณสมบัติ และหน้าที่ความรับผิดชอบ อย่างน้อยดังนี้

(๑) มีประสบการณ์ในการติดตามเฝ้าระวังภัยคุกคามสารสนเทศ ไม่น้อยกว่า ๒ ปี

(๒) มีใบรับรอง (Certificate) ด้านความปลอดภัยสารสนเทศ อย่างน้อย ๑ ใบรับรอง จาก CompTIA Security+ หรือ EC-Council CEH (Certified Ethical Hacker) หรือ ISC๒ SSCP (Systems Security Certified Practitioner) หรือดีกว่า

(๓) มีใบรับรองการอบรม การใช้งานระบบ SIEM ที่จัดซื้อในโครงการนี้ สำหรับผู้ดูแลระบบหรือเทียบเท่า หรือดีกว่า จากเจ้าของผลิตภัณฑ์ หรือตัวแทนจำหน่ายผลิตภัณฑ์

(๔) ติดตามเฝ้าระวังภัยคุกคามสารสนเทศ ตามวันและเวลาราชการ เป็นอย่างน้อย หรือตามที่คณะกรรมการตรวจรับ หรือผู้ที่ได้รับมอบหมายจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำหนด

(๕) ติดตามเฝ้าระวังภัยคุกคามสารสนเทศ และหากมีเหตุการณ์ภัยคุกคามสารสนเทศเกิดขึ้น ให้ดำเนินการให้ดำเนินการวิเคราะห์ ตรวจสอบ หาสาเหตุ แก้ไข ให้คำแนะนำเพื่อให้อุปกรณ์หรือระบบงานใช้งานได้ปกติดังเดิม

(๖) จัดทำรายงานสรุปเหตุการณ์ผิดปกติ/ภัยคุกคาม รายวัน รายสัปดาห์ รายเดือน เป็นอย่างน้อย

(๗) ให้คำปรึกษาแนะนำด้านการรักษาความปลอดภัยสารสนเทศแก่เจ้าหน้าที่กระทรวงการคลังที่เกี่ยวข้อง

๑.๒.๙ ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายที่จัดซื้อในโครงการนี้

๑.๒.๑๐ ติดตั้งอุปกรณ์ Firewall ที่จัดซื้อในโครงการนี้

๑.๒.๑๑ ติดตั้งอุปกรณ์ Intrusion Prevention System ที่จัดซื้อในโครงการนี้

๑.๒.๑๒ ติดตั้งอุปกรณ์ Web Application Firewall ที่จัดซื้อในโครงการนี้ โดยติดตั้งใช้งานในลักษณะ High Availability แบบ Active-Stand by เป็นอย่างน้อย หรือตามที่คณะกรรมการตรวจรับ หรือผู้ที่ได้รับมอบหมายจากคณะกรรมการตรวจรับกำหนด สำหรับ

การติดตั้งในลักษณะ High Availability แบบ Active-Stand by ต้องมีอุปกรณ์สำหรับควบคุมการบริหารจัดการแยกต่างหาก โดยต้องเสนออุปกรณ์ Appliance ที่มีคุณลักษณะอย่างน้อยดังนี้

(๑) สามารถใช้บริหารจัดการอุปกรณ์ Web Application Firewall ทั้ง ๒ ตัวที่จัดซื้อในโครงการนี้ แบบศูนย์กลาง ในการทำ High Availability แบบ Active-Stand by ได้

(๒) มี Hard Drive อย่างน้อย ๕๐๐ GB

(๓) มี Memory อย่างน้อย ๘ GB

(๔) มีพอร์ต Gigabit Ethernet จำนวนไม่น้อยกว่า ๒ พอร์ต

๑.๒.๑๓ ติดตั้งระบบแสดงผลเพื่อการติดตามเฝ้าระวังเหตุการณ์ผิดปกติ/ภัยคุกคาม ที่จัดซื้อในโครงการนี้

๑.๒.๑๔ จัดหา ติดตั้ง เครื่องคอมพิวเตอร์ตั้งโต๊ะ จำนวนไม่น้อยกว่า ๔ ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อยดังนี้

(๑) มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า ๔ แกนหลัก (๔ Core) หรือ ๘ แกนเสมือน (๘ Thread) โดยมีความเร็วสัญญาณนาฬิกาไม่น้อยกว่า ๓.๐ GHz และมีหน่วยความจำแบบ L๓ Cache Memory ไม่น้อยกว่า ๖ MB จำนวน ๑ หน่วย

(๒) มีหน่วยความจำหลัก (RAM) ชนิด DDR๓ หรือดีกว่า ขนาดไม่น้อยกว่า ๔ GB

(๓) มีหน่วยจัดเก็บข้อมูล (Hard Disk) ชนิด SATA หรือดีกว่า ขนาดความจุไม่น้อยกว่า ๑ TB

(๔) มี DVD-RW หรือดีกว่า จำนวนไม่น้อยกว่า ๑ หน่วย

(๕) มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๑ ช่อง

(๖) มีระบบเสียงสนับสนุนการทำงานตามมาตรฐาน High Definltion Audio (HD Audio) หรือดีกว่า และลำโพง จำนวนไม่น้อยกว่า ๑ หน่วย

(๗) มีจอภาพแบบ LCD หรือดีกว่า ที่มีขนาดไม่น้อยกว่า ๒๐ นิ้ว มี Contrast Ratio ไม่น้อยกว่า ๖๐๐:๑ และมีเครื่องหมายการค้าเดียวกันกับเครื่องคอมพิวเตอร์ตั้งโต๊ะที่เสนอ จำนวนไม่น้อยกว่า ๓ จอภาพ

(๘) มีการ์ดแสดงผลที่สามารถเชื่อมต่อและแสดงผลกับจอภาพที่เสนอในข้อ ๑.๒.๑๔ (๗) ได้ โดยสามารถแสดงผลภาพในรูปแบบ Extend บนจอทั้งหมด หรือแสดงผลภาพได้อิสระในแต่ละจอ ได้เป็นอย่างน้อย

(๙) มีพอร์ต USB จำนวนไม่น้อยกว่า ๔ พอร์ต

(๑๐) มีเมาส์แบบ Wheel Optical หรือดีกว่า ที่มีการเชื่อมต่อแบบ USB และมีเครื่องหมายการค้าเดียวกันกับเครื่องคอมพิวเตอร์ตั้งโต๊ะที่เสนอ จำนวนไม่น้อยกว่า ๑ หน่วย

(๑๑) มีแป้นพิมพ์ (Keyboard) ที่มีการเชื่อมต่อแบบ USB มีตัวอักษรภาษาไทยและภาษาอังกฤษอยู่บนแป้นอย่างถาวร และมีเครื่องหมายการค้าเดียวกันกับเครื่องคอมพิวเตอร์ตั้งโต๊ะที่เสนอ จำนวนไม่น้อยกว่า ๑ หน่วย

(๑๒) มีระบบปฏิบัติการ Windows ๘ หรือเวอร์ชั่นล่าสุด หรือดีกว่า ที่มีลิขสิทธิ์ที่ถูกต้องตามกฎหมาย

(๑๓)มีชุดโปรแกรม Microsoft Office ซึ่งประกอบด้วย Word, Excel และ PowerPoint เวอร์ชั่นล่าสุด ที่มีลิขสิทธิ์ที่ถูกต้องตามกฎหมาย

๑.๒.๑๕ จัดหา ติดตั้ง โต๊ะ สำหรับวางชุดเครื่องคอมพิวเตอร์ตั้งโต๊ะ (ข้อ ๑.๒.๑๔) จำนวนไม่น้อยกว่า ๔ ตัว และเก้าอี้แบบล้อเลื่อน ที่มีพนักพิง ที่เท้าแขน และปรับระดับความสูงได้ จำนวนไม่น้อยกว่า ๔ ตัว

๑.๒.๑๖ ในการติดตั้ง ระบบแสดงผลเพื่อการติดตามเฝ้าระวังเหตุการณ์ผิดปกติ/ภัยคุกคาม เครื่องคอมพิวเตอร์ตั้งโต๊ะ โต๊ะและเก้าอี้ ที่จัดซื้อในโครงการนี้ หากสถานที่ติดตั้งยังไม่พร้อมหรือไม่อำนวยต่อการติดตั้ง สามารถดำเนินการติดตั้งภายหลังการตรวจรับงวดสุดท้ายได้ โดยต้องได้รับการเห็นชอบจากคณะกรรมการตรวจรับเสียก่อน แต่ต้องดำเนินการติดตั้งให้แล้วเสร็จภายในระยะเวลา ๑ ปี หลังการตรวจรับงวดสุดท้ายเสร็จสมบูรณ์

๑.๒.๑๗ จัดหา ติดตั้ง เครื่องสำรองไฟฟ้าแบบตั้งโต๊ะ จำนวน ๑ ชุด โดยมีขนาดกำลังจ่ายไฟไม่น้อยกว่า ๑๙๘๐ วัตต์ หรือ ๒๒๐๐ VA เป็นประเภท Sine Wave Line Interactive หรือดีกว่า สามารถสำรองไฟฟ้าที่ Full load ได้ไม่น้อยกว่า ๗ นาที และได้รับมาตรฐาน CE, EN ๕๐๐๙๑-๑, EN ๕๐๐๙๑-๒, VDE และ RoHS เป็นอย่างน้อย

๑.๒.๑๘ จัดหา ติดตั้ง อุปกรณ์ส่งสัญญาณ Streaming จำนวน ๑ ชุด ซึ่งสามารถสตรีมมิ่งวีดีโอได้โดยไม่ต้องใช้งานกับคอมพิวเตอร์ สามารถแปลงสัญญาณวีดีโอ H.๒๖๔ Video Encoder ได้ รองรับสัญญาณเข้าไม่น้อยกว่า ๑๐๘๐p มีพอร์ต HDMI In และ HDMI Out สามารถใช้งานบนร่วมกับ Wowza Media Server และซอฟต์แวร์สำหรับ Streaming Server ที่จะซื้อในโครงการนี้ได้เป็นอย่างน้อย

๑.๒.๑๙ จัดหา ติดตั้ง ซอฟต์แวร์สำหรับ Streaming Server จำนวน ๑ ชุด พร้อมลิขสิทธิ์ที่ถูกต้องตามกฎหมาย ซึ่งสามารถใช้งานสามารถใช้งานโปรโตคอล RTMP, RTSP และ MPEG-TS และสนับสนุน Video On-Demand ในฟอร์แมท FLV, MP๔ และ MP๓ ได้เป็นอย่างน้อย

๒. เครื่องคอมพิวเตอร์แม่ข่าย จำนวน ๒ ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อย ดังนี้

๒.๑ มีหน่วยประมวลผลกลาง (CPU) เป็นแบบ Intel Xeon Processor E๗ Family หรือดีกว่า จำนวนไม่น้อยกว่า ๒ หน่วย แต่ละหน่วยมีจำนวน Core ไม่น้อยกว่า ๑๒ Cores และมีความเร็วสัญญาณนาฬิกาแต่ละ CPU ไม่น้อยกว่า ๒.๖ GHz

๒.๒ มี Cache ไม่น้อยกว่า ๓๐ MB ต่อ Processor

๒.๓ มีหน่วยความจำแบบ DDR๓ หรือดีกว่า ขนาดไม่น้อยกว่า ๖๔ GB

๒.๔ Hard Disk จะต้องเป็นแบบ SSD หรือ Hot Plug SFF SAS ความเร็วอย่างน้อย ๑๕K rpm หรือดีกว่า ขนาดความจุไม่น้อยกว่า ๔๕๐ GB จำนวนอย่างน้อย ๖ หน่วย

๒.๕ มี DVD-ROM หรือดีกว่า แบบติดตั้งภายใน (Internal) หรือภายนอก (External) จำนวนไม่น้อยกว่า ๑ หน่วย

๒.๖ มี Network Interface Card แบบ Ethernet ความเร็ว ๑/๑๐ Gbps หรือดีกว่า จำนวนไม่น้อยกว่า ๒ พอร์ตพร้อมสายเชื่อมต่อ

๒.๗ มีอุปกรณ์ FC Host Bus Adapter ความเร็วไม่น้อยกว่า ๘Gb หรือดีกว่า จำนวนไม่น้อยกว่า ๒ พอร์ตพร้อมสายเชื่อมต่อ

๒.๘ มี RAID Controller หรืออุปกรณ์ในการจัดการ RAID สามารถรองรับการทำงานแบบ RAID ไม่น้อยกว่า RAID ๐, ๑, ๕

๒.๙ มี Power Supply แบบ Redundant Hot Swappable จำนวนไม่น้อยกว่า ๒ หน่วย

๒.๑๐ มีระบบปฏิบัติการ หรือ ซอฟต์แวร์ Virtual Machine (VM) พร้อมลิขสิทธิ์เท่ากับจำนวน CPU ที่ถูกต้องตามกฎหมาย ที่สามารถใช้ติดตั้งระบบบริหารจัดการข้อมูลและเหตุการณ์ด้านความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารแบบรวมศูนย์ในส่วนซอฟต์แวร์ที่ใช้ดำเนินการทำ Vulnerability Assessment ได้

๓. อุปกรณ์ Firewall สำหรับ Intranet/DMZ Zone จำนวน ๒ ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อย ดังนี้

๓.๑ เป็นอุปกรณ์ Appliance ที่ออกแบบมาเพื่อใช้งานในลักษณะ Next Generation Firewall โดยเฉพาะ โดยทำงานแบบ Stateful Inspection Firewall และสามารถวิเคราะห์ข้อมูลได้ถึงระดับ Application Layer

๓.๒ มีประสิทธิภาพในการทำงาน Firewall (Firewall Throughput) ความเร็วไม่น้อยกว่า ๙๐ Gbps ในสภาวะการใช้งานกับ Packet ขนาด ๑๕๑๘ bytes หรือ ความเร็วไม่น้อยกว่า ๑๔ Gbps ในสภาวะการใช้งานกับ Packet ในระดับ Application Protocol หรือในสภาวะการใช้งานจริง (Production)

๓.๓ สามารถทำงานที่ Concurrent Session/Connection ได้ไม่น้อยกว่า ๕,๐๐๐,๐๐๐ sessions/connections ในสภาวะการใช้งานทดสอบตามมาตรฐาน RFC ๒๕๔๔ และ ๓๕๑๑ หรือ Concurrent Session/Connection ได้ไม่น้อยกว่า ๔,๐๐๐,๐๐๐ sessions/connections ในสภาวะการทดสอบโดยเจ้าของผลิตภัณฑ์

๓.๔ สามารถรับการเชื่อมต่อได้ไม่น้อยกว่า ๑๓๐,๐๐๐ Sessions/Connections Per Second ในสภาวะการใช้งานทดสอบตามมาตรฐาน RFC ๒๕๔๔ และ ๓๕๑๑ หรือ สามารถรับการเชื่อมต่อได้ไม่น้อยกว่า ๑๒๐,๐๐๐ Sessions/Connections Per Second ในสภาวะการทดสอบโดยเจ้าของผลิตภัณฑ์

๓.๕ สามารถทำงานร่วมกับ Active Directory เพื่อเชื่อมโยงข้อมูลผู้ใช้งานบนเครือข่ายได้

๓.๖ มีพอร์ต Ethernet สำหรับเชื่อมต่อที่ความเร็ว ๑๐ Gbps (๑๐GBase-F SFP+) พร้อมโมดูล จำนวนไม่น้อยกว่า ๔ พอร์ต

๓.๗ มีพอร์ต Ethernet สำหรับเชื่อมต่อที่ความเร็ว ๑ Gbps แบบ RJ-๔๕ หรือดีกว่า จำนวนไม่น้อยกว่า ๔ พอร์ต

๓.๘ มีช่องเชื่อมต่อสำหรับบริหารอุปกรณ์ Management Port ความเร็ว ๑๐/๑๐๐/๑๐๐๐ Mbps จำนวนไม่น้อยกว่า ๑ Port

๓.๙ มีช่องเชื่อมต่อสำหรับบริหารอุปกรณ์ Console Port แบบ RJ45 จำนวนไม่น้อยกว่า ๑ Port

๓.๑๐ สามารถบริหารจัดการอุปกรณ์ด้วย Command Line Interface (CLI) และ Graphic User Interface (GUI) ได้เป็นอย่างน้อย

๓.๑๑ มี Power Supply แบบ Dual Redundant Hot Swappable Power Supplies

๓.๑๒ รู้จักแอพพลิเคชั่นได้ไม่น้อยกว่า ๑,๙๐๐ แอพพลิเคชั่น

๓.๑๓ สามารถติดตั้งในตู้ Rack มาตรฐานขนาด ๑๙ นิ้วได้

๓.๑๔ สามารถใช้งานในเครือข่าย IPv๔ และ IPv๖ ได้

๓.๑๕ ผลิตภัณฑ์ที่นำเสนอต้องอยู่ใน Gartner’s Leaders Quadrant ในเรื่องของ Enterprise Network Firewalls ปี ๒๐๑๓ หรือใหม่กว่า เป็นอย่างน้อย

๓.๑๖ มีการปรับปรุงข้อมูลรูปแบบการบุกรุก (Signature) เป็นระยะเวลาไม่น้อยกว่า ๒ ปี

๔. อุปกรณ์ Intrusion Prevention System จำนวน ๑ ชุด มีคุณลักษณะอย่างน้อย ดังนี้

๔.๑ เป็นอุปกรณ์ Appliance ที่ออกแบบมาเพื่อใช้งานในลักษณะ Next Generation Intrusion Prevention System โดยเฉพาะ

๔.๒ มีประสิทธิภาพในการทำงาน IPS (IPS Throughput) ความเร็วไม่น้อยกว่า ๔ Gbps

๔.๓ สามารถรับการเชื่อมต่อได้พร้อมกันสูงสุด (Maximum Concurrent Connections) ได้ไม่น้อยกว่า ๒,๐๐๐,๐๐๐ การเชื่อมต่อ

๔.๔ สามารถรับการเชื่อมต่อด้วยอัตราสูงสุด (Connections Per Second) ได้ไม่น้อยกว่า ๖๐,๐๐๐ Connections/sec

๔.๕ มีค่า Latency ไม่เกิน ๑๕๐ milliseconds

๔.๖ สามารถป้องกันผู้บุกรุกหรือโจมตีแบบต่าง ๆ เหล่านี้ ได้เป็นอย่างน้อย

- Worms
- Viruses
- Trojans
- Blended Threats
- Buffer Overflows
- Malform Traffic หรือ Exploit
- P๒P Attacks หรือ Protocol Discovery
- Spyware
- Statistical Anomalies หรือ DoS
- Rate-based Threats หรือ DDoS
- Port Scans
- Zero-day Threats
- VoIP Attacks หรือ Evasion Attempt
- IPv๖ Attacks
- Application Anomalies
- TCP Segmentations หรือ Statistical Deviation
- IP Fragmentation

๔.๗ สามารถควบคุมและจำกัดการใช้งานแอพพลิเคชั่น (Applications) บนเครือข่ายได้

๔.๘ สามารถแสดงระดับความรุนแรง หรือ ระดับผลกระทบของเหตุการณ์ภัยคุกคามได้

๔.๙ มี Application Programming Interface (API) เพื่อรองรับการเชื่อมต่อ (Integration) กับระบบอื่น ๆ ได้

๔.๑๐ สามารถสำรวจและเก็บข้อมูล อุปกรณ์คอมพิวเตอร์ และแอพพลิเคชั่นบนเครือข่ายได้ หรือสามารถทำงานร่วมกับซอฟต์แวร์ที่ใช้ดำเนินการทำ Vulnerability Assessment ที่จัดซื้อในโครงการนี้ได้

๔.๑๑ สามารถทำงานร่วมกับ LDAP เพื่อเชื่อมโยงข้อมูลผู้ใช้งานบนเครือข่ายได้

๔.๑๒ สามารถสร้างและปรับแต่ง IPS rules หรือ Signatures ได้ตามความต้องการของผู้ใช้ (Custom IPS rules หรือ User-defined signatures)

๔.๑๓ สามารถกำหนด IPS rules ตามช่องโหว่ (Vulnerability) ได้

๔.๑๔ สามารถตรวจจับข้อมูลจราจรบนเครือข่ายที่มีพฤติกรรมผิดปกติได้ (Anomaly-based Detection)

๔.๑๕ สามารถบริหารจัดการสิทธิของผู้ใช้งานตามหน้าที่ที่รับผิดชอบได้ (Role-based)

๔.๑๖ มีพอร์ต Ethernet สำหรับเชื่อมต่อที่ความเร็ว ๑๐ Gbps (SR) จำนวนไม่น้อยกว่า ๔ พอร์ต และทำงานในโหมด Fail-Open ได้

๔.๑๗ มีพอร์ต Ethernet สำหรับเชื่อมต่อที่ความเร็ว ๑ Gbps (Copper) จำนวนไม่น้อยกว่า ๔ พอร์ต และทำงานในลักษณะ Fail-Open ได้

๔.๑๘ มีช่องเชื่อมต่อสำหรับบริหารอุปกรณ์ Management Port ความเร็วไม่น้อยกว่า ๑Gbps จำนวนไม่น้อยกว่า ๑ Port

๔.๑๙ สามารถบริหารจัดการอุปกรณ์ผ่านทาง Command Line Interface (CLI) และ Graphic User Interface (GUI) ได้เป็นอย่างน้อย

๔.๒๐ มี Power Supply แบบ Dual Redundant Hot Swappable Power Supplies

๔.๒๑ สามารถติดตั้งในตู้ Rack มาตรฐานขนาด ๑๙ นิ้วได้

๔.๒๒ สามารถใช้งานในเครือข่าย IPv๔ และ IPv๖ ได้

๔.๒๓ ผลิตภัณฑ์ที่นำเสนอต้องอยู่ใน Gartner's Leaders Quadrant ในเรื่องของ Intrusion Prevention Systems ปี ๒๐๑๓ หรือใหม่กว่า เป็นอย่างน้อย

๔.๒๔ มีการปรับปรุงข้อมูลรูปแบบการบุกรุก (Signature) เป็นระยะเวลาไม่น้อยกว่า ๒ ปี

๕. อุปกรณ์ Web Application Firewall จำนวน ๒ ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อย ดังนี้

๕.๑ เป็นอุปกรณ์ Appliance ที่ออกแบบมาเพื่อใช้งานในลักษณะ Web Application Firewall โดยเฉพาะ และได้รับการรับรองมาตรฐานจาก ICSA เป็นอย่างน้อย

๕.๒ สามารถใช้ป้องกันระบบ Web Application และ Web Service ที่สามารถติดต่อสื่อสารถึงกันโดย XML ผ่าน SOAP อินเตอร์เฟซ ได้เป็นอย่างน้อย

๕.๓ มีประสิทธิภาพในการทำงาน (Throughput) ความเร็วไม่น้อยกว่า ๕๐๐ Mbps

๕.๔ รองรับการส่งผ่านข้อมูลประเภท HTTP ได้ไม่น้อยกว่า ๒๒,๐๐๐ transactions ต่อวินาที

๕.๕ สามารถป้องกันการโจมตีระบบ Application ในแบบ Brute Force Login, Buffer Overflow, Cross Site Request Forgery (CSRF), Cross Site Scripting (XSS), Session Hijacking, Site Reconnaissance, SQL Injection ได้เป็นอย่างน้อย

๕.๖ สามารถแจ้งเตือนในกรณีที่เกิดเหตุการณ์ต่างๆ ผ่านทางอีเมล์ ได้เป็นอย่างน้อย

๕.๗ สามารถเรียนรู้การใช้งานปกติของ Web Application เพื่อใช้ป้องกันการใช้งานที่ผิดปกติจากเดิมได้

๕.๘ มีหน้าจอบริหารจัดการระบบได้ในรูปแบบ GUI (Graphical User Interface) ในลักษณะ Web-based โดยสามารถกำหนดสิทธิ และระดับการเข้าถึงอุปกรณ์ ให้กับผู้ดูแลแต่ละคนได้

๕.๙ สามารถอัพเดท Signature ที่ใช้ในการป้องกันภัยคุกคามอย่างสม่ำเสมอ ได้ทั้งแบบ ด้วยมือ (Manual) และแบบอัตโนมัติ (Automatic) ซึ่งสามารถอัพเดทได้ทันที หากตรวจพบภัยคุกคามใหม่ และแบบตั้งเวลาให้ Check update automatic เป็นอย่างน้อย โดยการอัพเดท Signature ต้องแยกต่างหากจากการอัพเดท Firmware และ OS

๕.๑๐ สามารถแสดงรายงานในลักษณะ Real-time Dashboard

๕.๑๑ สามารถทำงานร่วมกับ NTP หรือ SNTP เพื่อปรับเวลาให้ถูกต้องแม่นยำจาก Time Server ได้

๕.๑๒ สามารถออกรายงานในรูปแบบ PDF หรือ Html ได้ โดยประกอบด้วยรายงานอย่างน้อย ดังนี้ Daily Report, Weekly Report, Monthly report และ Top ๑๐ Violation

๕.๑๓ สามารถใช้งานในรูปแบบดังนี้ ได้เป็นอย่างน้อย

- Reverse Proxy
- In-Line (Bridge หรือ Transparent Proxy)
- Non-inline (Span หรือ Offline หรือ Sniffer) หรือ Learning หรือ Staging

๕.๑๔ สามารถทำการ Bypass traffic (Fail Open) ในกรณีที่อุปกรณ์มีปัญหาได้ หรือเสนออุปกรณ์ภายนอกที่มีเครื่องหมายการค้าเดียวกันหรือต่างกันกับอุปกรณ์ มาเชื่อมต่อ ซึ่งสามารถทำหน้าที่ดังกล่าวได้ และไม่ทำให้ประสิทธิภาพของอุปกรณ์ลดลง

๕.๑๕ มีพอร์ต Ethernet ความเร็ว ๑๐/๑๐๐/๑๐๐๐ จำนวนไม่น้อยกว่า ๔ พอร์ต และรองรับการเพิ่มพอร์ต ๑๐G Fiber SR/LR จำนวนไม่น้อยกว่า ๒ พอร์ต ได้ในอนาคต

๕.๑๖ มี Power Supply แบบ Dual Redundant Hot Swappable Power Supplies

๕.๑๗ มี Hard drive ชนิด Hot-swap หรือดีกว่า ขนาดรวมไม่น้อยกว่า ๕๐๐ GB

๕.๑๘ สามารถติดตั้งในตู้ Rack มาตรฐานขนาด ๑๙ นิ้วได้

๕.๑๙ ได้รับการรับรองมาตรฐานด้าน Web Application Firewall จาก ICSA เป็นอย่างน้อย

๕.๒๐ สามารถใช้งานในเครือข่าย IPv๔ และ IPv๖ ได้

๕.๒๑ มีการปรับปรุงข้อมูลรูปแบบการบุกรุก (Signature) เป็นระยะเวลาไม่น้อยกว่า ๒ ปี

๕.๒๒ สามารถทำงานร่วมกับซอฟต์แวร์ที่ใช้ดำเนินการทำ Vulnerability Assessment ที่จัดซื้อในโครงการนี้ได้

๖. ระบบแสดงผลเพื่อการติดตามเฝ้าระวังเหตุการณ์ผิดปกติ/ภัยคุกคาม ๑ ระบบ ประกอบไปด้วย

๖.๑ จอภาพแสดงผล จำนวน ๔ ชุด โดยแต่ละชุดมีคุณลักษณะอย่างน้อย ดังนี้

๖.๑.๑ เป็นจอภาพชนิดแอลซีดี หรือดีกว่า ขนาดไม่น้อยกว่า ๕๕ นิ้ว

๖.๑.๒ หน้าจอแสดงผลใช้เทคโนโลยีแบบ IPS (In-plane switching) หรือดีกว่า

๖.๑.๓ สามารถแสดงผลความละเอียดแบบ Full HD (๑๙๒๐x๑๐๘๐) หรือดีกว่า

๖.๑.๔ มีค่า Aspect Ratio ที่ ๑๖:๙

๖.๑.๕ มีค่าความสว่างไม่น้อยกว่า ๕๐๐ cd/m๒

๖.๑.๖ มีค่าความหนาแน่นของจุดภาพ (Pixel Density) ไม่น้อยกว่า ๔๐ dpi

๖.๑.๗ มีค่าความลึกของเม็ดสี (Color Depth) ไม่น้อยกว่า ๑๐ bits

๖.๑.๘ มีอัตราส่วนความแตกต่างระหว่างภาพสีขาวและสีดำ (Contrast Ratio) ไม่น้อยกว่า ๑,๔๐๐:๑

๖.๑.๙ แหล่งกำเนิดแสงของจอแสดงผล (Backlight) เป็นแบบ Direct LED หรือดีกว่า และมีอายุการใช้งานไม่น้อยกว่า ๖๐,๐๐๐ ชั่วโมง

๖.๑.๑๐ มีมุมมองภาพไม่น้อยกว่า ๑๗๘ องศา ทั้งในแนบราบ (Horizontal) และแนวดิ่ง (Vertical)

๖.๑.๑๑ มีพัดลมระบายความร้อน ชนิด Low noise fan หรือดีกว่า

๖.๑.๑๒ มีช่องรับสัญญาณเข้า ประกอบไปด้วย

(๑) ช่องต่อสัญญาณ DSub หรือช่องต่อสัญญาณ HDMI จำนวนไม่น้อยกว่า ๑ ช่อง

(๒) ช่องต่อสัญญาณ DVI จำนวนไม่น้อยกว่า ๑ ช่อง

๖.๑.๑๓ มีช่องสัญญาณออกแบบ Display Port จำนวนไม่น้อยกว่า ๑ ช่อง

๖.๑.๑๔ มีช่องเชื่อมต่อระบบเครือข่าย (Ethernet) จำนวนอย่างน้อย ๒ ports

๖.๑.๑๕ เมื่อนำจอภาพมาต่อกันในลักษณะ Video Wall ๒x๒ ต้องมีขนาดรอยต่อระหว่างจอภาพ ไม่เกิน ๓.๖ มิลลิเมตร และมีซอฟต์แวร์ติดตั้งภายนอก สำหรับควบคุมและตรวจสอบสถานะการทำงานของจอแสดงภาพโดยรวม ซึ่งสามารถสั่งเปิด-ปิด, ตั้งค่าต่างๆ, เลือกแหล่งสัญญาณเข้า, ระบบปรับสีและความสว่างระหว่างจอให้เท่ากันแบบอัตโนมัติ และกำหนดระดับของผู้ใช้งานได้เป็นอย่างน้อย

๖.๑.๑๖ ได้จากการรับรองมาตรฐานจาก CE หรือ FCC หรือ CCC หรือดีกว่า

๖.๒ อุปกรณ์ควบคุมการแสดงผลในรูปแบบ Video Wall จำนวน ๑ ชุด มีคุณลักษณะอย่างน้อยดังนี้

๖.๒.๑ มีช่องรับสัญญาณเข้า แบบ DVI Universal อย่างน้อย ๔ ช่องสัญญาณ แต่ละช่องสัญญาณสามารถเลือกต่อกับสัญญาณภาพแบบ DVI, RGB (VGA), Component หรือ HDMI โดยสามารถตรวจสอบรูปแบบของสัญญาณเข้าโดยอัตโนมัติได้ และรองรับสัญญาณเข้าได้สูงสุดไม่ต่ำกว่า ๑๙๒๐x๑๒๐๐ pixels ต่อช่องสัญญาณ

๖.๒.๒ มีช่องจ่ายสัญญาณออก แบบ DVI จำนวนไม่น้อยกว่า ๔ ช่อง แต่ละช่องสัญญาณสามารถจ่ายสัญญาณภาพออกได้สูงสุดไม่ต่ำกว่า ๑๙๒๐x๑๒๐๐ pixels หรือไม่ต่ำกว่าค่าความละเอียดสูงสุดของ จอภาพแสดงผล (ข้อ ๖.๑) ต่อช่องสัญญาณ

๖.๒.๓ มีอุปกรณ์แบบขาตั้งพื้นสำหรับติดตั้ง จอภาพแสดงผล (ข้อ ๖.๑) ที่จัดซื้อในโครงการนี้ ในรูปแบบ Video Wall ๒x๒ ได้ และมีเครื่องหมายการค้าเดียวกับจอภาพแสดงผล (ข้อ ๖.๑)

๖.๒.๔ สามารถเชื่อมต่อกับ จอภาพแสดงผล ที่จัดซื้อในโครงการนี้ได้ และมีเครื่องหมายการค้าเดียวกับจอภาพแสดงผล (ข้อ ๖.๑)

๖.๒.๕ มีสายสัญญาณเชื่อมต่อดังต่อไปนี้

(๑) สายสัญญาณเชื่อมต่อระหว่าง อุปกรณ์ควบคุมการแสดงผลในรูปแบบ Video Wall กับจอภาพแสดงผล ความยาวไม่น้อยกว่า ๒๐ เมตร จำนวนไม่น้อยกว่า ๔ เส้น

(๒) สายเชื่อมต่อสัญญาณเข้าอุปกรณ์ควบคุมการแสดงผลในรูปแบบ Video Wall ซึ่งสามารถแสดงภาพออกบนหน้าจอแสดงผลได้อย่างคมชัดและไม่มีสัญญาณรบกวน จำนวนไม่น้อยกว่า ๔ เส้น

๖.๒.๖ มีหน่วยประมวลผลกลาง (CPU) ไม่น้อยกว่า ๔ แกนหลัก (๔ Core) หรือ ๘ แกนเสมือน (๘ Thread) โดยมีความเร็วสัญญาณนาฬิกาไม่น้อยกว่า ๓.๖ GHz

๖.๒.๗ มีหน่วยความจำหลักอย่างไม่น้อยกว่า ๓๒ GB

๖.๒.๘ มี Hard Disk แบบ SATA หรือดีกว่า ขนาดความจุไม่น้อยกว่า ๓๒๐ GB จำนวนอย่างน้อย ๒ หน่วย ซึ่งแต่ละหน่วยสามารถถอดเปลี่ยนได้โดยไม่ต้องปิดเครื่อง และสามารถทำงานได้แบบ Redundant RAID-๑ ได้เป็นอย่างน้อย

๖.๒.๙ มี Power Supply จำนวนอย่างน้อย ๒ หน่วย ซึ่งแต่ละหน่วยสามารถถอดเปลี่ยนได้โดยไม่ต้องปิดเครื่อง และสามารถทำงานได้แบบ Redundant ได้เป็นอย่างน้อย

๖.๒.๑๐ มีช่องเชื่อมต่อระบบเครือข่าย (Ethernet) แบบ Gigabit จำนวนอย่างน้อย ๒ ports

๖.๒.๑๑ สามารถแสดงภาพจากแหล่งสัญญาณภาพแบบ Streaming Video ได้พร้อมกันไม่น้อยกว่า ๒๔ ภาพ

๖.๒.๑๒ มีระบบปฏิบัติการแบบ Windows ๗ หรือดีกว่า ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

๖.๒.๑๓ เป็นอุปกรณ์ที่สามารถติดตั้งแบบ Rack Mount

๖.๒.๑๔ ได้จากการรับรองมาตรฐานจาก CE หรือ FCC Class A หรือดีกว่า

๖.๓ ซอฟต์แวร์ควบคุมการแสดงผลในรูปแบบ Video Wall จำนวน ๑ ชุด มีคุณลักษณะอย่างน้อยดังนี้

๖.๓.๑ มีหน้าจอควบคุมแบบ GUI (Graphical User Interface) เพื่อใช้ควบคุมการแสดงผลในรูปแบบ Video Wall

๖.๓.๒ สามารถกำหนดหน้าจอการแสดงภาพแบบเป็นตาราง (Grid) ได้

๖.๓.๓ สามารถจัดวางตำแหน่งแต่ละภาพอย่างอิสระบนจอแสดงผล โดยสามารถแสดงภาพจากแหล่งสัญญาณภาพต่างๆ ได้พร้อมกันได้ไม่น้อยกว่า ๓๖ ภาพ

๖.๓.๔ สามารถสร้าง, แก้ไข, บันทึก และ Load/Unload รูปแบบการแสดงภาพต่างๆ มาใช้ภายหลังได้เป็นอย่างน้อย

๖.๓.๕ มี Application Programming Interface (API) เพื่อรองรับการเชื่อมต่อ (Integration) กับระบบอื่น ในการสั่งการการแสดงภาพ

๖.๓.๖ สามารถติดตั้งใช้งานได้บนระบบปฏิบัติการ Windows ๗ หรือสูงกว่า ได้เป็นอย่างน้อย

๖.๓.๗ สามารถกำหนดสิทธิ์ของผู้ใช้งานในระดับต่างๆ (Roles & Permission)

๖.๓.๘ สามารถติดตั้งใช้งานพร้อมกันได้ไม่น้อยกว่า ๕ เครื่อง

๖.๓.๙ สามารถเรียกรูปแบบการแสดงภาพแบบต่างๆที่กำหนดไว้ ผ่านทางอุปกรณ์ Tablet ที่มีระบบปฏิบัติการแบบ iOS ได้เป็นอย่างน้อย

๖.๓.๑๐ มีระบบสำรองข้อมูลระบบและกู้คืนข้อมูลภายหลัง (Backup และ Restore Configuration)

๖.๓.๑๑ สามารถกำหนดขนาดและตำแหน่ง Windows การแสดงผลได้อิสระทุกขนาด และทุกตำแหน่ง ได้แก่ แสดงภาพเต็ม ๑ จอ, แสดงภาพคร่อมระหว่างหลายจอ, แสดงภาพใหญ่เต็มจอ Video Wall ได้เป็นอย่างน้อย

๖.๓.๑๒ สามารถแสดงภาพและจัดวางตำแหน่งแต่ละภาพอย่างอิสระบนจอแสดงผล จากแหล่งสัญญาณภาพที่เป็น Website หรือ Web Application ได้พร้อมๆ กัน

๖.๓.๑๓ สามารถแสดงภาพและจัดวางตำแหน่งแต่ละภาพอย่างอิสระบนจอแสดงผล จากแหล่งสัญญาณภาพที่เป็น ภาพจากหน้าจอ Desktop ของเครื่องคอมพิวเตอร์ ได้หลายเครื่องพร้อม ๆ กัน และสามารถใช้คีย์บอร์ดและเมาส์จากอุปกรณ์ควบคุมการแสดงผลในรูปแบบ Video Wall (ข้อ ๖.๒) สั่งการเครื่องคอมพิวเตอร์เหล่านั้นได้

๖.๓.๑๔ สามารถแสดงภาพและจัดวางตำแหน่งแต่ละภาพอย่างอิสระบนจอแสดงผล จากแหล่งสัญญาณภาพที่เป็น ภาพจาก Local file หรือ Local application ที่อยู่บน อุปกรณ์ควบคุมการแสดงผลในรูปแบบ Video Wall (ข้อ ๖.๒) ได้พร้อม ๆ กัน

๖.๓.๑๕ สามารถใช้คีย์บอร์ดและเมาส์จากเครื่องคอมพิวเตอร์บนเครือข่าย สั่งการอุปกรณ์ควบคุมการแสดงผลในรูปแบบ Video Wall (ข้อ ๖.๒) และสามารถใช้คีย์บอร์ดและเมาส์

จากอุปกรณ์ควบคุมการแสดงผลในรูปแบบ Video Wall (ข้อ ๖.๒) สั่งการเครื่องคอมพิวเตอร์บนเครือข่ายได้

๖.๓.๑๖ มีลิขสิทธิ์การใช้งานที่ถูกต้องตามกฎหมาย

๖.๓.๑๗ สามารถใช้งานกับ จอภาพแสดงผล และ อุปกรณ์ควบคุมการแสดงผลในรูปแบบ Video Wall ที่จัดซื้อในโครงการนี้ได้