มหาวิทยาลัยราชภัฏสงขลา
แผนงาน.....
งาน.....

ผู้กำหนดคุณลักษณะ.....
(นายกฤษณ์วรา รัตนโอภาส)
ผู้ตรวจคุณลักษณะ.....
(ผศ.ดร.อำนาจ ทองขาว)

ลำดับที่	รายการ	งบประมาณที่ได้รับ		รายละเอียด
		จำนวน (หน่วย)	จำนวนเงิน (บาท)	
1.	โปรแกรมป้องกันไวรัส	1 โปรแกรม	240,000 บาท	**คุณลักษณะโปรแกรมป้องกันไวรัส** เป็นโปรแกรมป้องกันและตรวจสอบไวรัสแบบบริหารจัดการบน Cloud จำนวน 200 ชุด 1 ปี และแบบอิสระ จำนวน 20 ชุด เป็นระยะเวลา 1 ปี ประกอบด้วย 1. Management Console (ระบบบริหารจากส่วนกลางของโปรแกรมป้องกันไวรัส) 1.1 ผลิตภัณฑ์ป้องกันไวรัสต้องสามารถควบคุมและบริหารจัดการจากส่วนกลางซึ่งเป็นการทำงานภายใต้สถาปัตยกรรมแบบ Cloud และบริหารจัดการผ่าน Web service ได้ 1.2 จำนวนสิทธิของผู้ใช้งานที่ควบคุมผ่านระบบการควบคุมจากส่วนกลางภายใต้สถาปัตยกรรมแบบ Cloud ต้องมีจำนวนไม่น้อยกว่า 250 Users 1.3 ระบบบริหารจัดการจากส่วนกลางสามารถสามารถควบคุม เครื่องลูกข่ายที่เป็นแบบ Physical, Laptop, Server, Virtualization ในรูปแบบ Guest install และสามารถที่จะบริหารจัดการภายใต้ Management เดียวกันได้ 1.4 ระบบจะต้องสามารถสร้างผู้ดูแลระบบได้มากกว่า 1 ชื่อบัญชีและมีประวัติการเข้าใช้งาน ของแต่ละชื่อบัญชี และสามารถกำหนดสิทธิได้ว่าผู้ดูแลระบบสมารถบริหารจัดการเฉพาะกลุ่มที่ให้สิทธิได้ 1.5 ระบบจะต้องสามารถแจ้งเตือนไปยังผู้ดูแลระบบโดยผ่านช่องทางอีเมล

				มากกว่า 1 อีเมล ตามข้อมูลดังต่อไปนี้ ได้เป็นอย่างน้อย - Malware outbreak - Update Available - License Expires - Antimalware Event 1.6 บริหารจัดการได้ผ่านทางเว็บบราวเซอร์ ในรูปแบบ Https โปรโตคอล รองรับการทำงานกับ Browser ดังต่อไปนี้ Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+ 1.7 ระบบต้องสามารถส่งรูปแบบรายงานได้โดยอัตโนมัติตามช่วงเวลาที่กำหนดไว้ และรายงานดังกล่าวจะต้องถูกส่งมาในรูปแบบของการบีบอัดแบบ Zip ไฟล์ซึ่งมีไฟล์ PDF และ CSV ถูกบีบอัดอยู่ใน Zip ดังกล่าว 2. Security for Endpoint (ระบบป้องกันไวรัสสำหรับเครื่องแม่ข่าย) 2.1 สามารถติดตั้งร่วมกับระบบปฏิบัติการ - Server operating systems: Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server - Red Hat Enterprise Linux / CentOS 5.6 or higher Ubuntu 10.04 LTS or higher SUSE Linux Enterprise Server 11 or higher OpenSUSE 11 or higher Fedora 15 or higher Debian 5.0 or higher

				Amazon Linux AMI 2.2 รองรับการติดตั้งโปรแกรมผ่านโปรแกรมบริหารจัดการจากส่วนกลาง (Network Discovery) หรือแบบ ส่งเป็น e-mail หรือ ติดตั้งเอง โดยใช้ไฟล์ติดตั้งด้วยไฟล์เดียวได้ 2.3 สามารถทำการตรวจจับ Malware ประเภทดังต่อไปนี้ได้ ไวรัส, โทรจัน, worm, rootkit , phishing , Adware, Key logger เป็นอย่างน้อย 2.4 สามารถกำหนดนโยบายการรักษาความปลอดภัย เพื่อนำไปใช้โดยผู้ใช้ปลายทางไม่สามารถยกเลิกหรือแก้ไขนโยบายได้เอง 2.5 สามารถสั่งสแกน/อัพเดททันทีหรือกำหนดช่วงเวลาการ สแกน/อัพเดท ได้จาก Management Console 2.6 มีฟังก์ชันในการเฝ้าระวังการทำงานของ Ransomware เพื่อป้องกันไม่ให้สร้างความเสียหายกับเครื่องได้ (Ransomware Vaccine) 2.7 ผู้ดูแลระบบ สามารถเลือกที่จะทำการลบไฟล์ (Delete) ที่ต้องสงสัยว่าเป็นไวรัส หรือ สามารถกักกันไฟล์ (Quarantine)ที่ต้องสงสัยได้ 2.8 ต้องสามารถกำหนดพาสเวิร์ดในการป้องกันการถอนการติดตั้งโปรแกรมได 2.9 สามารถอัพเดทฐานข้อมูลแอนตี้ไวรัสผ่านทาง web Management console ได้หรือ อัพเดทผ่านทางเครื่องที่อยู่ในระบบเครือข่ายเดียวกันได้ โดยสามารถเลือกกำหนด ได้เพียงช่องทางเดียวหรือได้ทั้งสองช่องทาง 2.10 เมื่อตรวจพบเจอไวรัสสามารถทำการแจ้งเตือนไปยังผู้ดูแลระบบผ่านทางอีเมล์ได้ โดยอัตโนมัติ โดยสามารถกำหนดให้ส่งได้มากกว่า 1 email 2.11 สามารถทำการกู้คืนไฟล์ (Restore) ไฟล์ที่ถูกกักกัน (Quarantine) กลับไป

				ยังตำแหน่งเดิมได้โดยผ่านทาง management console หรือผ่านทางเครื่องลูกข่าย 2.12 สามารถกำหนดการอัพเดท ได้ตามช่วงเวลาโดยแบ่งตามกลุ่ม เพื่อสามารถจัดสรรการอัพเดทได 3. GravityZone Security for Endpoint (ระบบป้องกันไวรัส สำหรับเครื่องลูกข่าย) 3.1 สามารถติดตั้งร่วมกับระบบปฏิบัติการ - Workstation operating systems: Windows 10 TH2 ,Windows 10 (1) Windows 8.1, Windows 8, Windows 7, Windows Vista with Service Pack 1, Windows XP with Service Pack 3, - Mac OS X El Capitan (10.11.x) , Mac OS X Yosemite (10.10.5) , Mac OS X Mavericks(10.9.5) Mac OS X Mountain Lion (10.8.5) 3.2 รองรับการติดตั้งโปรแกรมผ่านโปรแกรมบริหารจัดการจากส่วนกลาง (Network Discovery) หรือแบบส่งเป็น email หรือติดตั้งเอง โดยใช้ไฟล์ติดตั้งด้วยไฟล์เดียวได้ 3.3 สามารถทำการตรวจจับ Malware ประเภทดังต่อไปนี้ได้ ไวรัส, โทรจัน, worm, rootkit, phishing, Adware, Keylogger เป็นอย่างน้อย 3.4 มีฟังก์ชันในการเฝ้าระวังการทำงานของ Ransomware เพื่อป้องกันไม่ให้สร้างความเสียหายกับเครื่องได้ (Ransomware Vaccine) 3.5 สามารถกำหนดนโยบายการรักษาความปลอดภัย เพื่อนำไปใช้โดยผู้ใช้ปลายทางไม่สามารถยกเลิกหรือแก้ไขนโยบายได้เอง 3.6 สามารถสั่งสแกน/อัพเดททันทีหรือกำหนดช่วงเวลาการ สแกน/อัพเดท ได้จาก Management Console พร้อม

				ทั้งสามารถสั่งปิดเครื่องภายหลังจากการสแกนได้ 3.7 ผู้ดูแลระบบ สามารถเลือกที่จะทำการลบไฟล์(Delete) ที่ต้องสงสัยว่าเป็นไวรัส หรือ สามารถกักกันไฟล์(Quarantine)ที่ต้องสงสัยได้ 3.8 ต้องสามารถกำหนดพาสเวิร์ดในการป้องกันการถอนการติดตั้งโปรแกรมได้ 3.9 สามารถอัพเดทฐานข้อมูลแอนตี้ไวรัสผ่านทาง web Management console ได้หรือ อัพเดทผ่านทางเครื่องที่อยู่ในระบบเครือข่ายเดียวกันได้ โดยสามารถเลือกกำหนด ได้เพียงช่องทางเดียวหรือได้ทั้งสองช่องทาง 3.10 สามารถกำหนดให้เครื่องลูกข่ายทำหน้าที่รับข้อมูลการอัพเดทจากทาง management console และเครื่องดังกล่าว สามารถกระจายข้อมูลการ update ต่อไปยังเครื่องลูกข่ายอื่นๆได้ 3.11 เมื่อตรวจพบเจอไวรัส สามารถทำการแจ้งเตือนไปยังผู้ดูแลระบบผ่านทางอีเมล์ได้ โดยอัตโนมัติ โดยสามารถกำหนดให้ส่งได้มากกว่า 1 email 3.12 สามารถทำการคืนไฟล์ (Restore) ไฟล์ที่ถูกกักกัน (Quarantine) กลับไปยังตำแหน่งเดิมได้โดยผ่านทาง management console หรือผ่านทางเครื่องลูกข่าย หรือกำหนดโฟลเดอร์ปลายทางที่ต้องการใหม่ได้ 3.13 สามารถกำหนดการอัพเดท ได้ตามช่วงเวลาโดยแบ่งตามกลุ่ม เพื่อสามารถจัดสรรการอัพเดทได้ 3.14 สามารถกำหนดการเข้าถึงเว็บไซต์/โปรแกรม ว่าอนุญาต/ไม่อนุญาต ให้เข้าใช้งานได้ 3.15 สามารถบล๊อกเว็บหลอกลวงหรือเว็บที่อาจเป็นอันตรายได้ (Anti-Phishing) 3.16 มีไฟล์วอลที่สามารถป้องกันภัยคุกคามที่เข้ามาโจมตีทั้งขาเข้าและขาออกได้

				พร้อมทั้งแจ้งเตือนหากมีโปรแกรมหรือโปรเซสใดพยายามจะเชื่อมต่อมาใช้งานกับ Port ภายในเครื่องได้ 3.17 สามารถตั้งค่าให้เครื่องคอมพิวเตอร์ มีการเปลี่ยนใช้ policy อื่นโดยอัตโนมัติตามเงื่อนไขที่กำหนดไว้ได้อย่างน้อย ดังต่อไปนี้ - IP address ของเครื่องลูกข่ายมีการเปลี่ยนแปลง - Gateway address ของเครื่องลูกข่ายมีการเปลี่ยนแปลง - DNS server ของเครื่องลูกข่ายมีการเปลี่ยนแปลง - รูปแบบการเชื่อมต่อระบบเครือข่ายมีการเปลี่ยนแปลง เช่น เปลี่ยนจาก LAN ไปใช้งาน Wireless LAN เป็นต้น 3.18 สามารถตรวจจับแอนตี้ไวรัสที่ใช้งานอยู่ก่อนการติดตั้งใหม่ ได้ไม่น้อยกว่า 10 ชนิด เพื่อการถอดถอนแอนตี้ไวรัส ก่อนการติดตั้ง 3.19 สามารถทำการสแกนอุปกรณ์ต่อพ่วง (Removable device) และ network drive ได้ 3.20 มีเทคโนโลยีการสแกนอย่างน้อย ดังต่อไปนี้ - Local scan: การสแกนโดยใช้ทรัพยากรที่มีอยู่ในเครื่องคอมพิวเตอร์เท่านั้น - Hybrid scan: การสแกนโดยอาศัยทรัพยากรเพียงส่วนนึงในเครื่องและใช้ cloud security ในการช่วยสแกน - มีเทคโนโลยี Fingerprinting ไฟล์เพื่อไม่ทำการสแกนซ้ำไฟล์เดิม แต่จะทำการสแกนไฟล์ที่เป็นไฟล์ใหม่และไฟล์ที่มีการอัพเดตหรือไฟล์ติดไวรัส 3.21 สามารถอนุญาตให้ใช้งานหรือไม่ให้ใช้งานอุปกรณ์ต่อพ่วงจำพวก External storage, Internal storage, Bluetooth, Network adaptor,

				Imaging device ได้ 4. คุณสมบัติของโปรแกรมป้องกันไวรัสบนเครื่องลูกข่ายแบบอิสระ (Stand Alone) 4.1 เป็นโปรแกรมป้องกันไวรัสที่สนับสนุนการทำงานบนระบบปฏิบัติการดังต่อไปนี้ Microsoft WindowsXP/Vista/7/8/8.1/10 ได้เป็นอย่างน้อย 4.2 สามารถป้องกัน Malware ต่างๆ ได้แบบ Proactive ซึ่ง ได้แก่ Viruses, Spyware, Trojans, Worms, Adware และ Root kits โดยไม่ทำให้เครื่องคอมพิวเตอร์ช้าลง หรือก่อความรำคาญขณะใช้งานคอมพิวเตอร์ 4.3 สามารถป้องกันและกำจัด Malware ต่างๆ ได้ทั้งแบบ Real-time file system protection และแบบ OnDemand Scanning 4.4 ใช้วิธีการตรวจสอบ Malware โดยวิธีดังนี้ - ตรวจสอบโดยอาศัยการอ้างอิงจากฐานข้อมูลแบบ Definition หรือ Signatures - ตรวจสอบโดยอาศัยการวิเคราะห์พฤติกรรมแบบ Heuristics และ Advanced Heuristics 4.5 สามารถตรวจจับ Potentially Unwanted Applications และ Potentially Unsafe Applications ได้ 4.6 สามารถตรวจสอบภัยคุกคามจากทางอินเตอร์เน็ตและอีเมล์ผ่านทาง Protocol HTTP, HTTPS, POP3, POP3S, IMAP และ IMAPS 4.7 สามารถตรวจจับภัยคุกคามผ่าน Media ดังนี้ Local Drives, Removable Media, Networks Drives 4.8 สามารถตรวจสอบไฟล์ที่สร้างขึ้นใหม่จำพวกไฟล์บีบอัดได้ ซึ่งได้แก่ Self-

				extracting files และ Runtime packers 4.9 มีระบบปิดกั้นการโจมตีโดยใช้ช่องโหว่ของโปรแกรมประยุกต์ (Exploit Blocker) 4.10 สามารถป้องกัน Phishing ได้ 4.11 มีระบบสแกนหน่วยความจำขั้นสูง เพื่อตรวจจับมัลแวร์ที่ใช้เทคนิคการโจมตีที่ซับซ้อน (Advanced Memory Scanner) 4.12 มีโมดูลในการสแกนอีเมล์ไวรัสที่สามารถรวมเข้ากับ Microsoft Outlook, Outlook Express และ Windows Mail ได้ที่ตัวเครื่องลูกข่ายโดยตรง 4.13 มีระบบ Host Intrusion Prevention System และระบบ Self-defense เพื่อป้องกันภัยคุกคามโจมตีระบบได้ 4.14 มีโมดูล Document Protection เพื่อป้องกันไวรัสติดไฟล์เอกสาร Microsoft Office 4.15 มีเครื่องมือในการสร้างแผ่น Boot CD เพื่อสแกนและกำจัดไวรัสนอกระบบปฏิบัติการได้ 4.16 มีเทคโนโลยีในการตรวจสอบ Process ที่รันอยู่ในระบบว่ามีความเสี่ยงในระบบความรักษาความปลอดภัยในระดับใด โดยตรวจสอบจากฐานข้อมูลของผู้ผลิตโปรแกรมป้องกันไวรัส (Cloud-powered scanning) 4.17 สามารถทำ Web Filtering ได้โดยสามารถกำหนด URL ที่ต้องการ Block ไม่ต้องการให้ผู้ใช้งานเข้าถึงได้ และสามารถ Exclude URL ที่ไม่ต้องการให้โปรแกรมป้องกันไวรัสสแกนได้ 4.18 สามารถตั้งค่ารหัสผ่านในการล็อคการตั้งค่าโปรแกรมได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปลี่ยนแปลงการตั้งค่าโปรแกรม

				4.19 สามารถอัพเดทฐานข้อมูลไวรัสของโปรแกรมได้โดยอัตโนมัติ และสามารถอัพเดทส่วนประกอบต่างๆ ของโปรแกรมได้ 4.20 สามารถทำการสแกนไฟล์ที่กักไว้ใน Quarantine หลังจากอัพเดท เพื่อตรวจสอบไฟล์ที่กักเก็บไว้อีกครั้ง 4.21 สามารถกำหนดการใช้งาน Removable Media ได้ โดยสามารถระบุ Device ID ของ Removable Media และทำการ Blocked, Read-only และ Read-write ได้ 4.22 สามารถทำการ Rollback ฐานข้อมูลไวรัสได้ในกรณีที่เกิดปัญหาเกี่ยวกับฐานข้อมูลไวรัส 4.23 มีฟังก์ชั่น Presentation mode เพื่อปิดการทำงานของหน้าต่างป๊อบ-อัพ เมื่อใช้งานแอพพลิเคชั่นแบบเต็มจอ 4.24 มีเครื่องมือในการตรวจสอบข้อมูลของเครื่องคอมพิวเตอร์ในโปรแกรมป้องกันไวรัสเอง เพื่อการวิเคราะห์ข้อมูลได้ (Diagnostic tool) 4.25 สามารถสนับสนุนการทำงานร่วมกับ Microsoft NAP ได้ 4.26 มีความสามารถในการตรวจสอบ Patch ของ Windows ที่ยังไม่ได้ติดตั้งอัพเดท และแจ้งเตือน Patch ที่ในโปรแกรมป้องกันไวรัสได้ 4.27 โปรแกรมต้องสามารถสร้าง Application memory dump เพื่อใช้ในการตรวจสอบปัญหาได้ 4.28 สามารถทำ Update Server เพื่อให้บริการการอัพเดทผ่าน HTTP/HTTPS และสามารถทำ Authentication เครื่องที่จะเข้ามาอัพเดทได้ 4.29 ต้องผ่านการรับรองและมีใบรับรองจาก ICSA Lab และ West Coast Lab 4.30 เป็นผลิตภัณฑ์ได้รับรางวัล VB100

				มากกว่า 80 ครั้ง 5. คุณสมบัติของเครื่องมือบริหารจัดการโปรแกรมป้องกันไวรัสบนเครื่องลูกข่ายแบบอิสระ (Stand Alone) 5.1 สามารถติดตั้งทำงานบนระบบปฏิบัติการดังต่อไปนี้ Microsoft Windows Server 2003/Server 2008/Server 2012 และ Microsoft Windows Small Business Server 2003/2008/2011 ได้เป็นอย่างน้อย 5.2 สามารถบริการจัดการได้ผ่านเว็บบราวเซอร์ (Web Console) 5.3 สามารถตรวจสอบ Inventory ของเครื่องลูกข่ายได้ดังนี้ Computer Name, IP Address ,MAC Address และ Operating System ได้เป็นอย่างน้อย 5.4 สามารถมอนิเตอร์ เพื่อดูแลการทำงานของเครื่องลูกข่ายแบบ Real Time ได้ดังนี้ เวอร์ชั่นของฐานข้อมูลไวรัส, ระยะเวลาที่เครื่องลูกข่ายเข้ามาเชื่อมต่อครั้งสุดท้าย, ชื่อและเวอร์ชั่นของโปรแกรมป้องกันไวรัสที่ติดตั้งอยู่ที่เครื่องลูกข่ายและปัญหาที่เกิดขึ้นกับเครื่องลูกข่ายได้เป็นอย่างน้อย 5.5 สามารถเรียกดูและปรับแต่งการตั้งค่าโปรแกรมของเครื่องลูกข่ายได้ 5.6 สามารถกำหนดนโยบายของเครื่องลูกข่ายตาม Group ได้ 5.7 สามารถสั่งงานในการอัพเดทฐานข้อมูลไวรัสและสั่งงาน On-Demand Scan ไปยังเครื่องลูกข่ายได้ 5.8 สามารถส่งข้อมูลไปเก็บไว้บนฐานข้อมูล MSSQL และ MYSQL ได้ 5.9 สามารถกำหนดสิทธิในการเข้าถึงได้หลายระดับ เช่น แบบผู้ดูแลระบบ และแบบอ่านได้อย่างเดียว 5.10 สามารถแจ้งเตือนเมื่อเกิดเหตุการณ์ต่างๆ ไปยังผู้ดูแลระบบได้ ผ่านทาง

				อีเมล และSNMP Trap 5.11 สามารถเชื่อมต่อกับ Active Directory โดยใช้โปรโตคอล LDAP ได้ 5.12 มี Dashboard เพื่อมอนิเตอร์สถานะต่างๆได้ 5.13 สามารถทำการบริหารจัดการ Quarantine ของเครื่องลูกข่ายทั้งหมดได้ 5.14 สามารถออกรายงานอันดับไวรัส หรือเครื่องที่ติดไวรัสมากที่สุด เป็นต้น ได้ 5.15 สามารถตั้ง Schedule ในการออกรายงานและส่งอีเมล์ไปยังผู้ดูแลระบบได้ 5.16 การจัดทำรายงาน สามารถนำเอาข้อมูลออกมาได้ในรูปแบบของ CSV Format, PDF Format และ PS Format 5.17 สามารถตั้งค่า SMTP เพื่อใช้ในการส่งอีเมล์ไปยังผู้ดูแลระบบ 5.18 สามารถทำการติดตั้งและถอดถอนโปรแกรม antivirus สำหรับเครื่องลูกข่ายแบบรีโมทจากศูนย์กลางได้ **รายละเอียดทั่วไป** ผู้เสนอราคาจะต้องเป็นผู้แทนจำหน่าย หรือเป็นผู้จัดจำหน่ายที่ได้รับการแต่งตั้งให้มีสิทธิในการจำหน่าย และบริการหลังการขายจากตัวแทนจำหน่าย หรือผู้ผลิต สาขาประจำประเทศไทย เท่านั้น โดยต้องมีหนังสือแต่งตั้งมาแสดงในวันที่เสนอราคาด้วย

มหาวิทยาลัยราชภัฏสงขลา ผู้กำหนดคุณลักษณะ.....
แผนงาน..... (นายกฤษณวรา รัตนโอภาส)
งาน..... ผู้ตรวจคุณลักษณะ.....
(ผศ.ดร.อำนาจ ทองขาว)

ลำดับที่	รายการ	งบประมาณที่ได้รับ		รายละเอียด
		จำนวน (หน่วย)	จำนวนเงิน (บาท)	
2.	โปรแกรม Campus Agreement	1 โปรแกรม	260,000 บาท	**คุณลักษณะโปรแกรม Campus Agreement** 1. ผู้เสนอราคาจะต้องเป็นผู้แทนจำหน่าย หรือเป็นผู้จัดจำหน่ายที่ได้รับการแต่งตั้งให้มีสิทธิ์ในการจำหน่ายลิขสิทธิ์ประเภทสถานศึกษา Authorized Education Reseller จากตัวแทนจำหน่าย หรือผู้ผลิต สาขาประจำประเทศไทย เท่านั้น โดยต้องมีหนังสือแต่งตั้งมาแสดงในวันที่ เสนอราคาด้วย 2. โปรแกรม Campus Agreement จะต้องครอบคลุมสิทธิ์การใช้งานในโปรแกรมอย่างน้อย ดังต่อไปนี้ ภายในระยะเวลา 1 ปี ในจำนวนไม่ต่ำกว่า 80 Users **Core CAL Suite and Enterprise CAL Suite** **The Core CAL Suite is equivalent to the following licenses:** - Windows Server CAL - Microsoft SharePoint Server Standard CAL - Microsoft Exchange Server Standard CAL - Microsoft System Center Configuration Manager Client Management License - System Center Endpoint Protection (antivirus client and subscription service) - Microsoft Lync Server Standard CAL **The Enterprise CAL Suite is equivalent to the following licenses:** - All of the components of the Core

				CAL Suite (listed above) - Exchange Server Enterprise CAL with Services* - Exchange Online with Archiving for Exchange Server - SharePoint Server Enterprise CAL - Lync Server Enterprise CAL - Windows Server Active Directory Rights Management Services CAL - System Center Client Management Suite - System Center Operations Manager Client Management License - System Center Service Manager Client Management License - System Center Data Protection Manager Client Management License - System Center Orchestrator (formerly Opalis) Client Management License 3. ต้องสามารถใช้ในการ Upgrade windows ที่ถูกต้องตามลิขสิทธิ์ใน Version เก่ากว่าปัจจุบันได้ ตามจำนวนสิทธิ์ที่ได้ 4. ต้องสามารถใช้สิทธิ์ในการติดตั้ง Office Professional Plus ได้ตามจำนวนสิทธิ์ที่ได้