ร่าง

ขอบเขตของงาน (Terms of Reference: TOR)

โครงการค่าลิขสิทธิ์ซอฟแวร์และระบบปฏิบัติการ

อุปกรณ์เครือข่ายเทคโนโลยีสารสนเทศมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

---

1. ความเป็นมา/หลักการและเหตุผล

บนพื้นฐานการเรียนรู้แบบไร้ขีดจำกัดเพื่อที่จะก้าวตามทันเทคโนโลยีกับโลกของการศึกษา ในแบบการเรียนรู้ด้วยตนเองผ่านสื่อในรูปแบบต่างๆที่ต้องการในยุคของการสื่อสารแบบไร้พรมแดนซึ่งรูปแบบในการเรียนรู้อย่างกว้างขวางและเป็นไปได้จริง ณ ปัจจุบันนั้นคือการเรียนรู้ผ่านระบบอิเล็กทรอนิกส์ หรือการเรียนรู้ผ่านเครือข่ายคอมพิวเตอร์ การเรียนรู้ผ่านระบบคอมพิวเตอร์นั้นสิ่งที่จะตามมาและเราไม่อาจจะปฏิเสธได้เลย คือคำว่า "ลิขสิทธิ์" ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ได้ให้ความหมายของคำว่า "ลิขสิทธิ์" ว่าหมายถึง สิทธิแต่เพียงผู้เดียวที่จะทำการใดๆ ตามพระราชบัญญัตินี้เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น นั่นก็หมายความว่า เจ้าของลิขสิทธิ์เพียงผู้เดียวเท่านั้นที่มีสิทธิ จะทำอย่างไรก็ได้กับงานอันมีลิขสิทธิ์ของตนเองงานที่ได้รับความคุ้มครองตามพระราชบัญญัติลิขสิทธิ์พ.ศ. 2537 ประกอบด้วย

1.งานวรรณกรรม

2.งานนาฏกรรม

3.งานศิลปกรรม

4.งานดนตรีกรรม

5.โสตทัศนวัสดุ

6.ภาพยนตร์

7.สิ่งบันทึกเสียง

8.งานแพร่เสียงแพร่ภาพ

9.งานอื่นใดในแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะของผู้สร้างสรรค์

โปรแกรมคอมพิวเตอร์ คือ คำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่นำไปใช้กับเครื่องคอมพิวเตอร์เพื่อให้เครื่องคอมพิวเตอร์ทำงาน หรือเพื่อให้ได้รับผลอย่างหนึ่งอย่างใด ทั้งนี้ไม่ว่าจะเป็นภาษาโปรแกรมคอมพิวเตอร์ในลักษณะใด เช่น ภาษาซี ภาษาโคบอลล์ ภาษาเบสิค โปรแกรม Windows โปรแกรม Adobe Photoshop รวม ทั้ง เกมคอมพิวเตอร์ประเภทต่างๆ ด้วย อาทิเช่น Play Station ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 โปรแกรมคอมพิวเตอร์ถูกจัดให้เป็นงานวรรณกรรม ประเภทหนึ่ง ดังนั้น โปรแกรมคอมพิวเตอร์จึงเป็นงานที่มีลิขสิทธิ์ และได้รับความคุ้มครองตามกฎหมาย

2. วัตถุประสงค์

เจ้าของลิขสิทธิ์โปรแกรมคอมพิวเตอร์ จะอนุญาตให้ผู้ใช้โปรแกรมคอมพิวเตอร์สามารถใช้โปรแกรมคอมพิวเตอร์ได้ในขอบเขตที่ตนกำหนดขึ้น ซึ่งเจ้าของลิขสิทธิ์ จะกำหนดขอบเขตการใช้สิทธิไว้ในสัญญาอนุญาตให้ใช้สิทธิโปรแกรม คอมพิวเตอร์ (Software License Agreement) ซึ่งอาจอยู่ในรูปแบบเอกสารหรือปรากฏอยู่ในตัวโปรแกรม ซึ่งผู้ใช้จะต้องอ่านและยอมรับ (Accept) ข้อกำหนด และเงื่อนไขการใช้ดังกล่าวเสียก่อนจึงจะสามารถใช้โปรแกรมดังกล่าวได้ เนื่องจากการใช้โปรแกรมไม่ถูกต้อง ตามเงื่อนไขการใช้สิทธิถือเป็นการละเมิดลิขสิทธิ์ต่อเจ้าของลิขสิทธิ์

3. ขอบเขตของงาน

ผู้เสนอราคาจะต้องรับผิดชอบในการดำเนินงานตามขั้นตอนดังนี้

1) ปรับปรุงอุปกรณ์ป้องกันไวรัสจากจดหมายอิเล็กทรอนิกส์ (MFE Email Gateway S120)
2) ปรับรุ่นระบบปฏิบัติการอุปกรณ์ป้องกันระบบเครือข่าย (ISG-1000)
3) ปรับรุ่นระบบปฏิบัติการอุปกรณ์ป้องกันระบบเครือข่าย (SSG-550)
4) บำรุงรักษาอุปกรณ์เก็บเหตุการณ์ระบบเครือข่าย (L3000)
5) ซอฟต์แวร์ไมโครซอฟท์สำหรับสถานศึกษา 1 ปี

4. คุณสมบัติของผู้เสนอราคา

1) ผู้เสนอราคาต้องเป็นผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์
2) ผู้เสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการและได้แจ้งเวียนชื่อแล้ว หรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ
3) ผู้เสนอราคาต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่น และ/หรือต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันระหว่างผู้เสนอราคากับผู้ให้บริการตลาดกลางอิเล็กทรอนิกส์ ณ วันประกาศประกวดราคาซื้อด้วยวิธีการทางอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการประกวดซื้อด้วยระบบอิเล็กทรอนิกส์ครั้งนี้
4) ผู้เสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์และความคุ้มกันเช่นว่านั้น
5) ผู้เสนอราคาต้องผ่านการคัดเลือกผู้มีคุณสมบัติเบื้องต้นในการซื้อของมหาวิทยาลัยฯ
6) ผู้เสนอราคาต้องเป็นนิติบุคคลตามกฎหมายที่จดทะเบียนในประเทศไทยเป็นเวลาไม่น้อยกว่า 3 ปี นับถึงวันยื่นซอง ซึ่งประกอบธุรกิจเกี่ยวกับการขาย และ/หรือให้เช่า และ/หรือให้เช่าซื้อ และ/หรือ

การรับจ้างพัฒนาหรือปรับแต่งระบบงานคอมพิวเตอร์ และ/หรือการบริการเกี่ยวกับระบบคอมพิวเตอร์โดยตรง

5. คุณลักษณะเฉพาะ

ปรากฏตามเอกสารแนบมาพร้อม TOR ดังรายละเอียดคุณลักษณะโครงการค่าลิขสิทธิ์ซอฟแวร์และระบบปฏิบัติการอุปกรณ์เครือข่ายเทคโนโลยีสารสนเทศมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

6. ระยะเวลาการดำเนินงาน

พฤศจิกายน พ.ศ. 2553 – มกราคม2554

7. ระยะเวลาในการส่งมอบ

ผู้เสนอยื่นซองประกวดราคาต้องสามารถส่งของและติดตั้งระบบให้ใช้งานได้ภายใน 60วันนับจากวันที่ได้รับการสั่งซื้อหรือวันที่ทำสัญญากับทางมหาวิทยาลัย

8. วงเงินในการจัดหา

งบประมาณในการดำเนินโครงการนี้ จำนวน 3,010,000 บาท(สามล้านหนึ่งหมื่นบาทถ้วน)

รายละเอียดโครงการค่าลิขสิทธิ์ซอฟแวร์และระบบปฏิบัติการอุปกรณ์เครือข่ายเทคโนโลยีสารสนเทศ มหาวิทยาลัย

.....

โครงการค่าลิขสิทธิ์ซอฟแวร์และระบบปฏิบัติการอุปกรณ์เครือข่ายเทคโนโลยีสารสนเทศ มหาวิทยาลัย

รายละเอียด ประกอบด้วย

1. ปรับปรุงอุปกรณ์ป้องกันไวรัสจากจดหมายอิเล็กทรอนิกส์ (MFE Email Gateway S120)
2. ปรับรุ่นระบบปฏิบัติการอุปกรณ์ป้องกันระบบเครือข่าย (ISG-1000)
3. ปรับรุ่นระบบปฏิบัติการอุปกรณ์ป้องกันระบบเครือข่าย (SSG-550)
4. บำรุงรักษาอุปกรณ์เก็บเหตุการณ์ระบบเครือข่าย (L3000)
5. ซอฟต์แวร์ไมโครซอฟท์สำหรับสถานศึกษา 1 ปี

คุณลักษณะของแต่ละระบบมีรายละเอียดดังต่อไปนี้

1 ปรับปรุงอุปกรณ์ป้องกันไวรัสจากจดหมายอิเล็กทรอนิกส์ (MFE Email Gateway S120) จำนวน 1 ชุด มีรายละเอียดดังนี้

1.1 ปรับปรุงอุปกรณ์รักษาความปลอดภัยสำหรับ Email Gateway แบบ Appliance ที่ออกแบบเฉพาะสำหรับทำหน้าที่ป้องกัน Spam, Image-Spam, Phishing, Zombie และ Virus

1.2 อุปกรณ์มีระบบปฏิบัติการเฉพาะที่มีการ Hardening เพื่อให้มีความปลอดภัยในการทำงานเป็น Email Gateway

1.3 มีประสิทธิภาพในการตรวจจับสแปมได้ไม่น้อยกว่า 35,000 Messages/Hour

1.4 ระบบต้องมี license เพื่อการตรวจจับอีเมล์ Spam,Virus และทำ Image Analysis ได้ไม่น้อยกว่า 100 users

1.5 สามารถทำงานแบบ Domain Key โดย Stamp รหัสกับ Email ทุกฉบับเพื่อระบุว่าอีเมล์ได้ผ่านการส่งจากระบบที่ถูกอ้างถึงได้อย่างถูกต้องรวมทั้งทำให้ผู้รับได้รับความมั่นใจว่าได้รับ Email จากผู้ส่งที่แท้จริงเพื่อป้องกันเรื่อง Email Faking

1.6 มีระบบควบคุมและป้องกันข้อมูลรั่วไหล (DataLoss Prevention) โดยสามารถกำหนดการป้องกันข้อมูลตามเงื่อนไขของข้อกำหนดสากลต่างๆ เช่น PCI, SOX,HIPAA,GLBA เป็นต้น รวมทั้งสามารถกำหนดเงื่อนไขในลักษณะของการให้น้ำหนักของข้อความต่างๆ (Weighted Dictionary) ตามความต้องการได้

1.7 สามารถเข้ารหัสอีเมล์โดยใช้โปรโตคอล TLS, S/MIME และ OpenPGP ได้เป็นอย่างน้อย

1.8 คุณสมบัติด้านการป้องกันและตรวจจับการบุกรุก (Intrusion Prevention) ดังต่อไปนี้

1.8.1 Denial-of-Service (DoS)

1.8.2 Directory Harvest Attack (DHA)

1.8.3 Buffer Overflow

1.8.4 Unauthorized access

1.9 มีคุณสมบัติด้านการตรวจจับ Spam, Image Spam, Phishing, Zombie ดังนี้

1.9.1 การตรวจจับสแปมต้องรองรับการตรวจจับด้วยวิธีดังต่อไปนี้เป็นอย่างน้อย

1.9.1.1 Reverse DNSlookup

1.9.1.2 Behavior analysis

1.9.1.3 Real-time Black List (RBL)

1.9.1.4 URL Filtering and Decoding

1.9.1.5 Bayesian Filtering

1.9.1.6 Body hash และ Fuzzy hash

1.9.1.7 Whitelist และ Blacklist

1.9.1.8 Email Header Analysis

1.9.1.9 Sender ID (SID)

1.9.1.10 Anomaly Detection Engine (ADE)

1.9.2 สามารถตรวจจับ Spam ที่มากับอีเมล์ได้ทั้งขาเข้าและขาออกพร้อมกัน

1.9.3 มีฐานข้อมูลสำหรับตรวจจับแหล่งที่มาของ Spammer, มีฐานข้อมูลด้านการแพร่กระจายของ Zombie และมีฐานข้อมูลในการตรวจจับ Phishing โดยอุปกรณ์สามารถใช้ฐานข้อมูลเหล่านี้ในการตรวจสอบอีเมล์ได้แบบ Real-time

1.9.4 เมื่อตรวจพบสแปมสามารถเลือกจัดการกับอีเมล์ได้อย่างน้อยดังต่อไปนี้

1.9.4.1 เพิ่มข้อความที่ Subject ของอีเมล์ก่อนจะส่งต่อไปยังผู้รับ (users)

1.9.4.2 เพิ่ม Field ลงใน Header ของอีเมล์ก่อนจะส่งต่อไปยังผู้รับ (users)

1.9.4.3 ลบอีเมล์

1.9.4.4 กักเก็บอีเมล์ (Quarantine)

1.9.4.5 ส่งต่ออีเมล์ (Forward) ไปยังผู้ที่เกี่ยวข้อง

1.9.4.6 แจ้งเตือน (Notify) ทางอีเมล์ไปยังผู้ดูแลระบบ

1.9.5 มีคุณสมบัติในการทำ Email Connection Control เพื่อควบคุมปริมาณของconnection จากแหล่งที่มีประวัติการส่งสแปมเมล์เข้ามาในระบบในปริมาณสูงผิดปรกติ

1.9.6 มีคุณสมบัติในการตรวจจับ Email Traffic ที่มีลักษณะผิดปกติ (Email Anomaly Detection) โดยการติดตาม (monitor) ผู้ส่ง, จำนวน Email ที่ส่ง, ไฟล์ Attachment และค่าทางสถิติอื่นๆ ที่มีพฤติกรรมต้องสงสัยโดยสามารถกับเก็บ Email เหล่านี้ไว้บนตัวอุปกรณ์เพื่อนำมาตรวจสอบในภายหลัง

1.9.7 สามารถการตรวจจับสแปมได้แบบอัตโนมัติโดยไม่จำเป็นต้องปรับแต่ง Spam Engine บนตัวอุปกรณ์ และรองรับในกรณีที่ผู้ใช้ต้องการปรับแต่งค่า Spam Engine เองแบบ Manual

1.9.8 มีคุณสมบัติในการสรุปรายการของอีเมล์ที่เก็บอยู่ใน Quarantine ของผู้ใช้แต่ละคน โดยส่งอีเมลสรุปไปให้ผู้ใช้ตามเวลาที่กำหนด เช่น ทุกๆ 4 ชั่วโมง หรือทุกวัน ได้โดยไม่ต้องใช้ Software และ Hardware เพิ่มเติมเพื่อให้ผู้ใช้สามารถบริหารจัดการอีเมล์ที่ถูกเก็บไว้ใน Quarantine ของตัวเองได้

1.9.9 คุณสมบัติการสรุปรายการของอีเมล์ที่เก็บอยู่ใน Quarantine ของผู้ใช้สามารถกำหนดให้เปิดการใช้งานเฉพาะผู้ใช้บางคน หรือบางกลุ่มได้

1.9.10 มีคุณสมบัติในการตรวจจับ Image Spam ได้

1.9.11 สามารถแสดงค่าคะแนน (Score) สำหรับตรวจจับสแปมในแต่ละอัลกอริทึมที่ใช้ในการตรวจสอบของอีเมล์แต่ละฉบับผ่านทาง GUI ได้

1.9.12 สามารถตรวจจับภาพที่ไม่เหมาะสม เช่น ภาพโป๊ (Pornographic image, Sexually offensive images) ที่อยู่ในอีเมล์ หรืออยู่ในไฟล์แนบของอีเมล์ได้

1.10 คุณสมบัติด้านการตรวจจับไวรัส

1.10.1 มีคุณสมบัติในการทำ Virus Outbreak Defender เพื่อป้องกันองค์กรจากการแพร่ระบาดของไวรัสใหม่ๆ ที่ยังไม่มี signature ในการตรวจจับ โดยทำการกับเก็บอีเมล์แบบ Dynamic (Dynamic Quarantine) โดยอีเมล์ต้องสงสัยว่าจะมีไวรัสรูปแบบใหม่จะถูกกับเก็บไว้ในตัวอุปกรณ์โดยอัตโนมัติจนกว่าจะมี Signature สำหรับตรวจจับไวรัสเหล่านี้

1.10.2 สามารถตรวจจับไวรัสที่มากับอีเมล์ได้ทั้งขาเข้าและขาออกเพร้อมกัน

1.10.3 รองรับการใช้งานระบบตรวจสอบไวรัส (Anti-Virus Engine) ได้อีก 1 ระบบได้ในอนาคต เพื่อเพิ่มความสามารถในการตรวจจับอีเมล์ไวรัส

1.10.4 เมื่อตรวจพบไวรัส สามารถเลือกจัดการกับอีเมล์ได้อย่างน้อยดังต่อไปนี้

- Clean virus
- ลบอีเมล์
- กักเก็บอีเมล์ (Quarantine)
- ส่งต่ออีเมล์ (Forward) ไปยังผู้ที่เกี่ยวข้อง
- แจ้งเตือน (Notify) ทางอีเมล์ไปยังผู้ดูแลระบบ

1.10.5 สามารถทำการดาวน์โหลด Signature ได้โดยอัตโนมัติ

1.11 คุณสมบัติด้านการควบคุมลักษณะของอีเมล์ที่รับส่ง

1.11.1 สามารถจำกัดชนิดของไฟล์ที่สามารถรับส่ง (File Type), จำกัดขนาดของอีเมล์ (Limit Email Size), ดักจับข้อความที่ไม่เหมาะสมหรือไม่สอดคล้องกับนโยบายขององค์กรที่อยู่ในอีเมล์โดยตรวจจับได้ทั้งขาเข้าและขาออกเพร้อมกัน

1.11.2 รองรับการใช้งานร่วมกับ LDAP และ Active Directory เพื่อตรวจสอบอีเมล์ผู้รับว่ามีอยู่จริงหรือไม่และสามารถนำ Group จาก LDAP และ Active Directory มาใช้ในการสร้าง Policy ในการตรวจจับ

1.12 คุณสมบัติด้านการบริหารจัดการ

1.12.1 รองรับการส่ง Syslog ไปยังระบบ Syslog Server หรือระบบ Centralized Log Management และสามารถส่ง E-mail แจ้งเตือนได้

1.12.2 สามารถบริหารจัดการอุปกรณ์ผ่าน WEB based Management(HTTPS) และ Command Line(Console, SSH)ได้

1.12.3 มีระบบ Dashboard ที่แสดงข้อมูลแบบ Real-time โดยสามารถแสดงปริมาณสแปมเมล์, ปริมาณไวรัสเมล์, ปริมาณอีเมล์ที่ถูกเก็บ (Quarantine), ปริมาณการใช้ CPU, Memory, Disk และสถานะของ Service ได้เป็นอย่างน้อย

1.12.4 มีระบบสร้างรายงาน (Report) บนตัวอุปกรณ์เอง และสามารถสร้างรายงานแบบอัตโนมัติทุกวัน และสามารถส่งไปยังผู้ดูแลระบบได้ โดยสามารถแสดงรายงานได้ดังต่อไปนี้ได้เป็นอย่างน้อย

1.12.4.1 จำนวนสแปม และไวรัส

1.12.4.2 ปริมาณอีเมล์ขาเข้าและปริมาณอีเมล์ขาออก

1.12.4.3 Top Spam Sender, Top Spam Receiver และ Top Virus Signature

1.12.4.4 สามารถแสดงข้อมูลแบบรายวัน, รายสัปดาห์, รายเดือน และรายปีได้

1.12.5 สามารถตรวจสอบสถานะของอีเมล์ว่ามีการส่งออกจากตัวอุปกรณ์แล้ว หรือถูกกักเก็บไว้บนตัวอุปกรณ์

1.13 มีคุณสมบัติในการทำหน้าที่เป็น Webmail Protection เช่น Microsoft Outlook Web Access, iNotesได้

1.14 ระบบที่นำเสนอจะต้องอยู่ในระดับ Quadrant Leader ใน Secure E-Mail Gateways Gartner ปี 2010 เป็นอย่างน้อย

1.15 ผู้เสนอราคาต้องได้รับการแต่งตั้งอย่างเป็นทางการจากบริษัทผู้ผลิตอุปกรณ์หรือเจ้าของผลิตภัณฑ์โดยตรงเท่านั้น

2 ปรับรุ่นระบบปฏิบัติการอุปกรณ์ป้องกันระบบเครือข่าย (ISG-1000) จำนวน 1 ชุด

2.1 Upgrade Firmware อุปกรณ์ Fire Wall จำนวน 1หน่วย (ISG-1000)

2.2 ผู้เสนอราคาต้องได้รับการรับรองจากบริษัทผู้ผลิตให้เป็นผู้ดำเนินการปรับปรุง Firmware ให้มหาวิทยาลัย โดยผู้เสนอราคาต้องนำเอกสารรับรองจากผู้ผลิตมายื่นให้คณะกรรมการพิจารณาในวันยื่นซอง

3 ปรับรุ่นระบบปฏิบัติการอุปกรณ์ป้องกันระบบเครือข่าย (SSG-550) จำนวน 2 ชุด

3.1 Upgrade Firmware อุปกรณ์ Fire Wall จำนวน 1หน่วย (SSG-550)

3.2 ผู้เสนอราคาต้องได้รับการรับรองจากบริษัทผู้ผลิตให้เป็นผู้ดำเนินการปรับปรุง Firmware ให้มหาวิทยาลัย โดยผู้เสนอราคาต้องนำเอกสารรับรองจากผู้ผลิตมายื่นให้คณะกรรมการพิจารณาในวันยื่นซอง

4 บำรุงรักษาอุปกรณ์เก็บเหตุการณ์ระบบเครือข่าย (L3000)จำนวน 1 ชุด

4.1 ตรวจเช็คอุปกรณ์ Logger จำนวน 1 หน่วย (L3000)

4.2 ปรับ Configure File ให้รับ Log ของ อุปกรณ์ Juniper NAC

4.3 ผู้เสนอราคาต้องได้รับการรับรองจากบริษัทผู้ผลิตให้เป็นผู้ดำเนินการบำรุงรักษาอุปกรณ์เก็บเหตุการณ์ระบบเครือข่าย (L3000)ให้มหาวิทยาลัย โดยผู้เสนอราคาต้องนำเอกสารรับรองจากผู้ผลิตมายื่นให้คณะกรรมการพิจารณาในวันยื่นซอง

5 ซอฟต์แวร์ไมโครซอฟท์สำหรับสถานศึกษา 1 ปี รายละเอียดประกอบด้วย

5.1 มีโปรแกรมระบบปฏิบัติการแบบ Microsoft Windows Upgrade ซึ่งสามารถปรับปรุงรุ่นที่ใช้งาน (Upgrade) ได้เป็นรุ่นล่าสุดโดยครอบคลุมการ Upgrade ใช้ งานได้ไม่น้อยกว่า 1 ปี

5.2 มีโปรแกรมระบบงานสำนักงานแบบ Microsoft Windows Office ซึ่งสามารถปรับปรุงรุ่นที่ใช้งาน (Upgrade) ได้เป็นรุ่นล่าสุดโดยครอบคลุมการ Upgrade ใช้งานได้ไม่น้อยกว่า 1 ปี

5.3 มีลิขสิทธิ์การใช้จากเครื่องลูกข่าย (Client Access License) สำหรับ Exchange Server, Share Point Server, SMS Server และ Windows Server โดยครอบคลุมการ Upgrade ใช้งานได้ไม่น้อยกว่า 1 ปี

5.4 มีจำนวนลิขสิทธิ์ที่เสนอจะต้องครอบคลุมไม่น้อยกว่า 350 ผู้ใช้งาน

ผู้เสนอราคาต้องได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายอย่างเป็นทางการจากผู้ผลิตโปรแกรมหรือตัวแทนจำหน่าย ภาคการศึกษา โดยให้ผู้เสนอราคานำเอกสารการแต่งตั้งมาให้คณะกรรมการพิจารณาในวันยื่นซอง