**ประกาศสำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่**

**เรื่อง การกำหนดหัวข้อร่างขอบเขตของงาน (Term of Reference: TOR)**

**โครงการจัดซื้ออุปกรณ์ป้องกันภัยระบบเครือข่ายคอมพิวเตอร์(IPS: Intrusion Prevention System)**

## 1. ความเป็นมา

ตามที่สำนักบริการเทคโนโลยีสารสนเทศ เป็นหน่วยงานกลางในการสนับสนุนการทำงานด้านเทคโนโลยีให้กับมหาวิทยาลัย ประกอบกับเป็นหน่วยงานที่ให้บริการทางด้านการจัดเก็บข้อมูล (Data Center) ของมหาวิทยาลัย ประกอบกับปัจจุบันในระบบเครือข่ายอินเทอร์เน็ตนั้นมีภัยคุกคามต่างๆ มากมายในหลากหลายรูปแบบและนับวันยิ่งมีมากขึ้นและมีความรุนแรงสูงขึ้น ซึ่งมหาวิทยาลัยฯ ก็เป็นหน่วยงานที่มีการเชื่อมต่อเข้าสู่ระบบอินเทอร์เน็ตเพื่อใช้ประโยชน์ในด้านการเรียนการสอน การวิจัย และการบริหารงาน ทำให้ต้องมีการตระหนักถึงภัยคุกคามต่างๆ ที่อาจเข้าสู่ระบบเครือข่ายหลักของมหาวิทยาลัยฯ ทั้งนี้เพื่อประโยชน์ของผู้ใช้งานภายในมหาวิทยาลัยฯ เองที่จะได้ใช้งานระบบเครือข่ายที่มีความปลอดภัยจากภัยคุกคามในรูปแบบต่างๆ จึงเห็นว่ามีความจำเป็นอย่างยิ่งที่จะต้องมีระบบที่ช่วยในการกรองข้อมูลต่างๆ ที่เชื่อมต่อเข้าสู่ระบบอินเทอร์เน็ตให้มีความปลอดภัยนั่นคือระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ (Intrusion Prevention System) ซึ่งจะเป็นระบบที่ช่วยในการเฝ้าระวังภัยคุกคามต่างๆ ผ่านระบบเครือข่ายฯ อีกทั้งเมื่อสามารถตรวจจับภัยคุกคามต่างๆ ได้แล้วก็จะทำหน้าที่ป้องกันไม่ให้ภัยคุกคามเหล่านั้นเข้าสู่ระบบเครือข่ายหลักของมหาวิทยาลัยได้อีกด้วย

จากเหตุผลดังกล่าวข้างต้น จึงจำเป็นต้องมีการจัดหาระบบป้องกันภัยเครือข่ายคอมพิวเตอร์ดังกล่าวมาทำการติดตั้งภายในระบบเครือข่ายของมหาวิทยาลัย

## 2. วัตถุประสงค์

2.1 เพื่อควบคุมและเพิ่มประสิทธิภาพทางด้านระบบรักษาความปลอดภัยให้กับระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่ายของมหาวิทยาลัยในภาพรวม

2.2 เพื่อป้องกันการถูกโจมตีจากภายในและภายนอกจนทำให้ระบบเครือข่ายหลักและระบบอินเทอร์เน็ตหยุดทำงาน

2.3 ช่วยป้องกันการเจาะระบบและการโจรกรรมข้อมูลที่สำคัญของมหาวิทยาลัย

**3. ผู้มีสิทธิ์เสนอราคาจะต้องมีคุณสมบัติ ดังต่อไปนี้**

3.1 เป็นผู้มีอาชีพขายพัสดุดังกล่าว มีความสามารถตามกฎหมายไม่เป็นบุคคลล้มละลาย และไม่อยู่ระหว่างเลิกกิจการ

3.2 เป็นนิติบุคคลที่จดทะเบียนในประเทศไทยและประกอบธุรกิจขายสินค้าและบริการที่สำนักบริการเทคโนโลยีสารสนเทศ ต้องการจะซื้อ และดำเนินธุรกิจมาแล้วไม่น้อยกว่า 2 ปี ณ วันที่ยื่นซอง มีเงินทุนจดทะเบียนไม่น้อยกว่า 1 ล้านบาท

3.3 ไม่มีชื่ออยู่ในหนังสือแจ้งเวียนทิ้งงานของทางราชการ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มครอง ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

3.4 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่นที่เข้าเสนอราคาให้แก่มหาวิทยาลัยเชียงใหม่ ณ วันประกาศจัดซื้อ หรือเป็นผู้กระทำการอันใดเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการคัดเลือกในครั้งนี้

3.5 เป็นผู้ปฏิบัติตามประกาศคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ เรื่องหลักเกณฑ์และวิธีการจัดทำ และแสดงบัญชีรายการรับจ่ายของโครงการที่บุคคลหรือนิติบุคคลเป็นคู่สัญญากับหน่วยงานของรัฐ พ.ศ. 2554 ดังนี้

3.6 บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญา ต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่ายหรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ

3.7 บุคคลหรือนิติบุคคลที่จะเข้าเป็นคู่สัญญากับหน่วยงานของรัฐ ซึ่งได้ดำเนินการจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์(e-Government Procurement : e-GP) ต้องลงทะเบียนในระบบอิเล็กทรอนิกส์ของกรมบัญชีกลางที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐ

**4. การพิจารณาทางเทคนิค (คุณสมบัติและข้อกำหนดทางเทคนิค)**

**อุปกรณ์ตรวจจับและป้องกัน การบุกรุกบนระบบเครือข่าย (Intrusion Prevention System)**

4.1 เป็นอุปกรณ์แบบ Hardware Appliance ที่ออกแบบมาเพื่อทำหน้าที่ป้องกันการบุกรุกระบบเครือข่ายโดยเฉพาะ (Next Generation Intrusion Prevention System) โดยเฉพาะ โดยไม่ใช่อุปกรณ์แบบ UTM หรืออุปกรณ์ Firewall ที่ทำงานแบบ IPS

4.2 มีความสามารถในการตรวจจับ (IPS Throughput) ไม่น้อยกว่า 15 Gbps และอุปกรณ์สามารถรองรับ Concurrent Connections ไม่น้อยกว่า 17,000,000 Concurrent Connections

4.3 ระบบจะต้องถูกออกแบบมาเพื่อทำงานร่วมกับเครือข่ายโดยไม่เกิดผลกระทบ โดยจะต้องมีค่า Latency Time ไม่เกิน 150 microseconds

4.4 มีพอร์ต Network Interface Fiber 10 Gbps SR ไม่น้อยกว่า 4 พอร์ตหรือ 2 Segments

4.5 มีพอร์ตสำหรับบริหารจัดการอุปกรณ์แบบ 10/100/1000 Ethernet หรือดีกว่า อย่างน้อย 2 พอร์ต และ Serial Port อย่างน้อย 1 port (Out of band management)

4.6 อุปกรณ์ต้องสามารถทำ Hardware Bypass ในกรณี Hardware/Software เกิดปัญหา รวมถึงกรณีไฟฟ้าดับ โดยสามารถเลือก Fail-open หรือ Fail-Close ในแต่ละ segment ได้

4.7 สามารถตรวจจับวิธีการบุกรุกและป้องกันเครือข่ายได้อย่างน้อยดังนี้ Signature matching, Protocol/Packet Anomalies, Statistical anomalies หรือ Application anomalies, Overflow, Worm, Virus, Backdoor Program, Trojan horse, Port Scanning, Spy ware, Dos หรือ DDoS ได้

4.8 สามารถตรวจสอบป้องกันเทคนิคการหลบซ่อนการโจมตีแบบ IP Defragmentation, TCP Segmentation ได้

4.9 สามารถตรวจสอบและป้องกันการโจมตีที่มีการเข้ารหัสด้วย SSL Encryption ได้

4.10 อุปกรณ์ที่เสนอต้องมีระบบ Redundant Power Supply หรือ Hot Swap จำนวน 2 หน่วย เพื่อรองรับในกรณีที่ Power Supply ตัวใดตัวหนึ่งไม่สามารถทำงานได้

4.11 สามารถบริหารจัดการอุปกรณ์ได้ผ่าน Command–line หรือ GUI โดยผ่านเว็บแบบ HTTPS

4.12 ระบบจะต้องสามารถให้คำแนะนำและปรับแต่งนโยบายเรื่องความปลอดภัยและประเมินความเสี่ยงของระบบจากการถูกโจมตีได้อย่างอัตโนมัติโดยอาศัยข้อมูลได้ทั้งจากการทำ Passive Scan หรือ Active Scan (Vulnerability Management) และต้องเป็นผลิตภัณฑ์ที่มีเครื่องหมายทางทางการค้ายี่ห้อเดียวกับอุปกรณ์ NGIPS ที่นำเสนอเท่านั้น

4.13 ระบบจะต้องสามารถจัดการควบคุม Applications (Application Control) ต่างๆ ได้ไม่น้อยกว่า 2,000 applications

4.14 ระบบสามารถระบุพฤติกรรมที่น่าสงสัย ของเครื่องที่อาจจะมีภัยคุกคาม หรือ ถูกติดตั้งมัลแวร์ (Indications of Compromise) ได้

4.15 ระบบสามารถตรวจสอบและระบุได้ถึงความน่าเชื่อถือของโดเมนและไอพี (Domain and IP Reputation) ได้อย่างน้อยดังนี้ Attackers, Bots, CnC, Malware, Phishing, Spam และ Tor exit node ได้

4.16 ระบบจะต้องสามารถตรวจสอบไฟล์ พร้อมทั้งบอกชนิดของไฟล์ตามหมวดหมู่อย่างน้อยดังนี้ System files, Graphics, Encoded, PDF files, Executables, Multimedia, Archive และ Office Documents ได้

4.17 สามารถรองรับการตรวจสอบมัลแมร์ชั้นสูง (Advance Malware) ผ่านโปรโตคอล HTTP, POP3, SMTP, FTP, SMB และ IMAP โดยอาศัยการวิเคราะห์ไฟล์ unknown malware และใช้เทคนิคการส่งไฟล์ที่มีคุณสมบัติตามที่กำหนดไปที่ cloud ของผู้ผลิตที่เสนอได้

4.18 สามารถใช้งานมาตรฐาน IPv6 ทั้งการจัดการ IPS และการตรวจสอบข้อมูลการโจมตี โดยผ่านการ ทดสอบจากหน่วยงานที่น่าเชื่อถือเช่น ICSA หรือ USGv6

4.19 ได้รับการรองรับมาตรฐาน FCC, UL หรือ CE เป็นอย่างน้อย

4.20 ได้รับการรับรองมาตรฐานจาก ICSA หรือ NSS Labs หรือ Common Criteria เป็นอย่างน้อย

4.21 ผลิตภัณฑ์ที่นำเสนอต้องอยู่ใน Gartner Magic Quadrant (Leader) ในเรื่องของ Intrusion Prevention System ปี 2016 เป็นอย่างน้อย

4.22 อุปกรณ์ที่เสนอต้องสามารถทำงานร่วมกับระบบบริหารจัดการของ Intrusion Prevention System เดิมของมหาวิทยาลัยได้

## 5. ข้อกำหนดการติดตั้ง

5.1 ผู้เสนอราคาจะต้องมีหนังสือรับรองการรับประกัน และการให้บริการ ณ สถานที่ติดตั้ง โดยบริษัทผู้ผลิต หรือบริษัทประจำประเทศไทยของผู้ผลิต เป็นระยะเวลา 3 ปี และจะต้องยื่นเอกสารนี้พร้อมเอกสารเสนอราคา

5.2 ผู้ชนะการประกวดราคาต้องส่งมอบ อุปกรณ์ป้องกันภัยระบบเครือข่ายคอมพิวเตอร์ (IPS: Intrusion Prevention System) ภายใน 60 วัน นับจากวันลงนามในสัญญา ซึ่งหากเกินกว่าระยะเวลาดังกล่าว ผู้ชนะการประกวดราคาต้องถูกปรับในอัตราวันละ 0.1 เปอร์เซ็น ของราคาทั้งหมด

5.3 ผู้ชนะการประกวดราคาต้องเสนอแผนการติดตั้งของระบบทั้งหมดอย่างละเอียด ซึ่งประกอบด้วยรายชื่อผู้รับผิดชอบโครงการ สถานที่ติดต่อ หมายเลขโทรศัพท์ ขั้นตอนการติดตั้งอุปกรณ์ในระบบต่างๆ และระยะเวลาในการดำเนินการแต่ละขั้นตอนที่แน่นอนให้กับมหาวิทยาลัยพิจารณาเห็นชอบภายใน 20 วัน นับจากวันลงนามในสัญญาจ้าง

5.4 ก่อนที่ผู้ชนะการประกวดราคาจะเข้าดำเนินการใดๆ ผู้ชนะการประกวดราคาจะต้องทำจดหมายแจ้งให้กับมหาวิทยาลัยรับทราบก่อนจะเข้าดำเนินการจริงอย่างน้อย 5 วันทำการ และจะต้องรอให้ได้รับการอนุมัติจากมหาวิทยาลัยก่อน จึงจะสามารถดำเนินการใดๆ ได้ ซึ่งหากผู้ชนะการประกวดราคาเข้าทำการติดตั้งระบบใดๆ โดยไม่ได้รับการอนุมัติจากมหาวิทยาลัย มหาวิทยาลัยมีสิทธิที่จะให้บริษัทดำเนินการรื้อถอนระบบๆ ต่างที่ได้ติดตั้งไปแล้ว โดยให้ถือเป็นความผิดและความรับผิดชอบของผู้ชนะการประกวดราคา

5.5 ผู้ชนะการประกวดราคาต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น เนื่องจากการติดตั้งอุปกรณ์หรือความเสียหายใดที่เกิดขึ้นเนื่องจากการปฏิบัติงานของผู้ชนะการประกวดราคา ผู้ชนะการประกวดราคาจะต้องดำเนินการซ่อมแซมแก้ไขให้อยู่ในสภาพเดิมโดยเร็วและยินยอมชดใช้ค่าเสียหายที่เกิดขึ้นให้กับมหาวิทยาลัย

5.6 การติดตั้งอุปกรณ์และระบบที่ผู้ชนะการประกวดราคาได้เสนอ หรือติดตั้งอุปกรณ์และระบบอื่นใดเพิ่มเติม ซึ่งหากไม่ได้ระบุไว้ในข้อกำหนดของมหาวิทยาลัย ให้อยู่ในดุลยพินิจของมหาวิทยาลัยที่จะเป็นผู้กำหนดลักษณะและรูปแบบของการติดตั้ง โดยขึ้นอยู่กับความจำเป็นและสภาพการใช้งานจริงเพื่อให้ระบบสามารถใช้งานได้อย่างมีประสิทธิภาพเป็นสำคัญ

## 6. การรับประกันและการอบรมภายหลังการติดตั้ง

การรับประกัน หลังจากการติดตั้งเสร็จเรียบร้อยแล้ว ผู้ขายจะต้องรับประกันการติดตั้ง ถ้าหากเกิดการขัดข้องเสียหาย ไม่ว่าจะเนื่องจากการติดตั้งไม่ถูกต้อง การเกิดปัญหาของระบบรักษาความปลอดภัยฯ หรือด้วยเหตุประการใดก็ตามจากการใช้งานปกติ เป็นเวลาไม่น้อยกว่า 3 ปี นับตั้งแต่วันตรวจรับมอบ ในระยะเวลาดังกล่าวนี้ ผู้เสนอราคาจะต้องทำการซ่อมแซม แก้ไข ตรวจสอบให้โดยไม่คิดมูลค่า

## 7. ข้อกำหนดอื่นๆ

ในกรณีจำเป็นมหาวิทยาลัยสามารถขอเพิ่ม ลด หรือเปลี่ยนแปลงอุปกรณ์ต่างๆ ให้แตกต่างจากที่ระบุไว้ในเอกสารนี้ได้ เพื่อให้อุปกรณ์และระบบต่างๆ ที่เสนอสามารถทำงานร่วมกับระบบเครือข่ายและระบบคอมพิวเตอร์ทั้งหมดของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ โดยผู้ชนะการประกวดราคาจะต้องปฏิบัติตามที่มหาวิทยาลัยกำหนด และจะต้องเสนอมูลค่าของปริมาณงานที่เพิ่มขึ้น หรือลดลงให้มหาวิทยาลัยพิจารณาก่อนที่ผู้ชนะประกวดราคาจะดำเนินการ ซึ่งมหาวิทยาลัยจะชำระหรือขอคืนเงินดังกล่าวให้กับผู้ชนะการประกวดราคาเมื่อมหาวิทยาลัยได้ทำการตรวจรับและเบิกจ่ายต่อไป ทั้งนี้มหาวิทยาลัยขอสงวนสิทธิ์ที่จะพิจารณาจัดหาผู้ดำเนินการรายอื่นแทนผู้ชนะประกวดราคาได้ หากพบว่ามูลค่าของปริมาณงานที่เพิ่มขึ้นหรือลดลงนั้น เป็นราคาที่ไม่เป็นธรรมต่อทางราชการและอาจก่อให้เกิดความเสียหายต่อทางราชการได้

**8. ระยะเวลาดำเนินการ 60 วัน นับจากวันลงนามในสัญญา**

ผู้ชนะการประกวดราคาจะต้องดำเนินการส่งมอบครุภัณฑ์ระบบเครือข่ายคอมพิวเตอร์ ติดตั้งและดำเนินการตาม TOR ที่กำหนด ทุกรายการจะต้องส่งมอบ พร้อมติดตั้งเพื่อให้ใช้งานได้เป็นอย่างดี ภายใน 60 วัน นับจากวันลงนามในสัญญา หากส่งมอบล่าช้าไม่เป็นไปตามกำหนดเวลาผู้ชนะการประกวดราคาจะถูกปรับเป็นรายวัน วันละ 0.1 %

**9. วงเงินในการจัดซื้อ 6,000,000 บาท (หกล้านบาทถ้วน)**

ในการประกวดราคาจัดซื้อจัดจ้างด้วยระบบอิเล็กทรอนิกส์ผู้เสนอราคาจะต้องเสนอราคาลดขั้นต่ำ (Minimum Bid) ไม่น้อยกว่าครั้งละ 10,000 บาท จากราคาสูงสุดในการประกวดราคาและการเสนอราคาครั้งถัดไปต้องเสนอราคาครั้งละไม่น้อยกว่า 10,000 บาท จากราคาครั้งสุดท้ายที่เสนอลดแล้ว

**10. สถานที่ติดต่อเพื่อขอทราบข้อมูลเพิ่มเติมหรือเสนอแนะวิจารณ์หรือแสดงความคิดเห็นโดยเปิดเผยตัว**

งานการเงินการคลังและพัสดุ
สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
เลขที่ 239 ถนนห้วยแก้ว ตำบลสุเทพ อำเภอเมือง จังหวัดเชียงใหม่ 50200
โทรศัพท์ 053-94-3807
โทรสาร 053-94-3825
**E-mail : benjaporn.pong@cmu.ac.th** / opas.m@cmu.ac.th

ขอรับรองว่าการกำหนดคุณลักษณะของพัสดุ ข้างต้นเป็นไปตามข้อกำหนด ในมติคณะรัฐมนตรีตามหนังสือที่ นร 0203/ว157 ลงวันที่ 27 ธันวาคม 2519

ประกาศ ณ วันที่ 5 พฤษภาคม 2560

(ลงนาม) ถนอมพร เลาหจรัสแสง
(รองศาสตราจารย์ ดร.ถนอมพร เลาหจรัสแสง)
รักษาการแทนผู้อำนวยการสำนักบริการเทคโนโลยีสารสนเทศ

# ตารางแสดงการบันทึกรายละเอียดประกาศร่าง TOR

| **รายการข้อมูล** | **คำอธิบาย** |
|---|---|
| 1. ชื่อหน่วยงาน | สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ |
| 2. ชื่อเรื่องร่าง TOR | โครงการจัดซื้ออุปกรณ์ป้องกันภัยระบบเครือข่ายคอมพิวเตอร์ |
| 3. วงเงินงบประมาณ (บาท) | 6,000,000 บาท (หกล้านบาทถ้วน) |
| 4. ราคากลาง (บาท) | 6,000,000 บาท (หกล้านบาทถ้วน) |
| 5. ราคาสูงสุดที่พึงรับได้ (บาท) | 6,000,000 บาท (หกล้านบาทถ้วน) |
| 6. วันที่ประกาศ | 5 พฤษภาคม 2560 |
| 7. จำนวนวันที่สิ้นสุดรับฟังข้อวิจารณ์ | 11 พฤษภาคม 2560 |
| 8. อีเมล์แอดเดรส | benjaporn.pong@cmu.ac.th, opas.m@cmu.ac.th |
| 9. ที่อยู่โครงการ | สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่<br>เลขที่ 239 ถ.ห้วยแก้ว ต.สุเทพ อ.เมือง จ.เชียงใหม่ |
| 10. จังหวัด | เชียงใหม่ |