# ขอบเขตของงาน (Terms of Reference: TOR)
# โครงการจัดซื้อระบบบริหารการติดต่อสื่อสารและพัฒนาการเรียนรู้ พร้อมป้องกันการบุกรุกไซเบอร์จากภายนอก มหาวิทยาลัยราชภัฏสวนสุนันทา

## 1. หลักการและเหตุผล

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสวนสุนันทา มีวัตถุประสงค์ในการให้บริการคอมพิวเตอร์ บริการสารสนเทศ บริการเครือข่าย บริการอินทราเน็ต และอินเตอร์เน็ต มีการควบคุมดูแล และพัฒนาระบบคอมพิวเตอร์ระบบงานแม่ข่าย และระบบเครือข่ายคอมพิวเตอร์ให้สามารถใช้งานได้ตลอดเวลา โดยมหาวิทยาลัยราชภัฏสวนสุนันทา มุ่งเน้นการพัฒนากำลังคนในด้านวิทยาศาสตร์และเทคโนโลยีให้มีทักษะความชำนาญในวิชาชีพเพื่อเสริมสร้างทุนมนุษย์ที่มีมูลค่าเพิ่มให้กับประเทศไทย เป็นมหาวิทยาลัยแห่งเทคโนโลยีที่จัดการศึกษาวิชาชีพบนพื้นฐานด้านวิทยาศาสตร์และเทคโนโลยีที่มีคุณภาพเพื่อส่งเสริมวิชาการและวิชาชีพชั้นสูงที่เน้นการปฏิบัติ ทำการสอน ทำการวิจัย การผลิตครูวิชาชีพ ทะนุบำรุงศิลปและวัฒนธรรม และด้านวิชาชีพเฉพาะทางระดับปริญญาเป็นหลัก ดังนั้นสำนักวิทยบริการและเทคโนโลยีสารสนเทศ จึงเล็งเห็นถึงความจำเป็นในการนำเทคโนโลยีดิจิตอลมาให้บริการในทุกด้าน โดยพิจารณาถึงปัจจัยสภาพแวดล้อมในด้านต่าง ๆ เป็นสำคัญ ทั้งในด้านความมั่นคงปลอดภัยของระบบสารสนเทศ การเข้าใช้งานค้นคว้าฐานข้อมูลการวิจัย การใช้งานโปรแกรมประยุกต์ อีกทั้งเพื่อป้องกันภัยคุกคามทางด้านเทคโนโลยีสารสนเทศรวมถึงการขโมยข้อมูล หรือความลับทางราชการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศจึงมีความประสงค์ที่จัดซื้อระบบบริหารการติดต่อสื่อสารและพัฒนาการเรียนรู้พร้อมป้องกันการบุกรุกไซเบอร์จากภายนอกเพื่อสนับสนุนการปฏิบัติงานของเจ้าหน้าที่ อาจารย์ นักศึกษา งานวิจัยต่าง ๆ ได้อย่างมีประสิทธิภาพ

## 2. วัตถุประสงค์

2.1 เพื่อเพิ่มประสิทธิภาพการติดต่อสื่อสารและพัฒนาการเรียนรู้เชื่อมต่อการเข้าถึงจากระยะไกลจากภายนอกมหาวิทยาลัย

2.2 เพื่อป้องกันการบุกรุก และภัยคุกคามไซเบอร์จากภายนอกมหาวิทยาลัยให้มีความมั่นคงปลอดภัย

2.3 เพื่อทดแทนของเดิมให้ใช้งานได้อย่างมีประสิทธิภาพ

## 3. คุณสมบัติของผู้เสนอราคา

3.1 ผู้เสนอราคาต้องเป็นผู้มีอาชีพขายพัสดุที่ประกวดราคาดังกล่าว

3.2 ผู้เสนอราคาต้องไม่เป็นผู้ที่ถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานของทางราชการ และได้แจ้งเวียนชื่อไว้แล้วหรือไม่เป็นผู้ที่ได้รับผลของการสั่งให้นิติบุคคลหรือบุคคลอื่นเป็นผู้ทิ้งงานตามระเบียบของทางราชการ

3.3 ผู้เสนอราคาต้องไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้เสนอราคาได้มีคำสั่งให้สละสิทธิ์ความคุ้มกันเช่นว่านั้น

3.4 ผู้เสนอราคาต้องไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้เสนอราคารายอื่นที่เข้าเสนอราคาให้แก่มหาวิทยาลัยราชภัฏสวนสุนันทา ณ วันประกาศประกวดราคาหรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรมในการเสนอราคาครั้งนี้

3.5 ผู้เสนอราคาจะต้องเป็นนิติบุคคลจดทะเบียนในประเทศไทย

3.6 ผู้เสนอราคาต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่าย หรือแสดงบัญชีรายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญ

3.7 ผู้เสนอราคาที่จะเข้าเสนอราคาต้องลงทะเบียนในระบบอิเล็กทรนิกส์ของกรมบัญชีกลางที่เว็บไซต์ศูนย์ข้อมูลจัดซื้อจัดจ้างภาครัฐ

3.8 คู่สัญญาต้องรับจ่ายเงินผ่านบัญชีฝากกระแสรายวัน เว้นแต่การรับจ่ายเงินแต่ล่ะครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจรับจ่ายเป็นเงินสดก็ได้

**4. แบบรูปรายการและคุณลักษณะ**

ตามเอกสารแนบ

**5. ระยะเวลาดำเนินการ**

120 วัน

**6. วงเงินในการจัดหา**

ราคากลาง 15,000,000 บาท (สิบห้าล้านบาทถ้วน)

# ขอบเขตของงาน (Terms of Reference: TOR)
# โครงการจัดซื้อระบบบริหารการติดต่อสื่อสารและพัฒนาการเรียนรู้ พร้อมป้องกันการบุกรุกไซเบอร์จากภายนอก มหาวิทยาลัยราชภัฏสวนสุนันทา

1. ระบบป้องกันการบุกรุกไซเบอร์จากภายนอก
   1.1 เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance ที่ออกแบบมาโดยเฉพาะ มีคุณลักษณะดังนี้
      1.1.1 อุปกรณ์ต้องมีการออกแบบ Platform Architecture ให้มีการแยกการทำงานของหน่วยประมวลผลสำหรับการบริหารจัดการ (Control Plane) และหน่วยประมวลผลสำหรับการจัดการข้อมูล (Data Plane) แยกออกจากกัน
      1.1.2 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1G/2.5G/5G/10G Base-T หรือดีกว่าจำนวนไม่น้อยกว่า 8 ช่อง และมี Interface 1G/10G แบบ SFP/SFP+ จำนวนไม่น้อยกว่า 12 ช่อง และมี Interface 40G/100G จำนวนไม่น้อยกว่า 4 ช่อง และมี Interface แบบ 1Gbps สำหรับบริการจัดการ (Out of Band Management) ไม่น้อยกว่า 1 พอร์ท และ Interface แบบ Micro-USB Console ไม่น้อยกว่า 1 พอร์ท
      1.1.3 อุปกรณ์จะต้องมี Firewall Throughput หรือ Application Firewall Throughput ไม่น้อยกว่า 46.2 Gbps
      1.1.4 อุปกรณ์จะต้องมี Threat Prevention Throughput ไม่น้อยกว่า 22.5 Gbps ในการทดสอบด้วยรูปแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix
      1.1.5 อุปกรณ์ต้องรองรับ Max Sessions ไม่น้อยกว่า 3,600,000 sessions และ New Sessions ไม่น้อยกว่า 295,000 ต่อ วินาที
      1.1.6 มีระบบตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ อย่างน้อย ดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment เป็นต้นได้
      1.1.7 สามารถใช้งานตามมาตรฐาน IPv6 ได้
      1.1.8 อุปกรณ์จะต้องมี Storage แบบ SSD สำหรับจัดเก็บข้อมูลของระบบขนาดไม่ต่ำกว่า 480 GB
      1.1.9 สามารถติดตั้งในรูปแบบ Transparent Inline, Non-Inline Monitoring (Tap), L2 และ L3 หรือเทียบเท่าได้ และ สามารถทำงานได้พร้อมกันโดยไม่ต้องแบ่ง Virtual System หรือ Virtual Domain
      1.1.10 สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้

1.1.11 สามารถ Routing แบบ Static, Dynamic Routing และ Policy Based Forwarding หรือ Policy based Routing ได้

1.1.12 สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน ( Authentication Systems ) ได้แก่ Active Directory, LDAP, Radius ได้

1.1.13 สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้อุปกรณ์สามารถรับ Syslog ที่มีข้อมูลของ IP Address และ User จากระบบอื่น เพื่อมาใช้ในการยืนยันตัวตน ของ User ที่เข้ามาใช้งานระบบ โดยรองรับทั้ง User Log-in และ User Log-out หรือ สามารถเสนออุปกรณ์ที่สามารถทำงานแทนได้

1.1.14 สามารถควบคุมประเภทของไฟล์ที่อนุญาตให้ download และ upload บนแต่ละ Application ได้ รวมทั้งสามารถป้องกันการรั่วไหลของข้อมูล ( Data Filtering ) ออกจากระบบเครือข่าย เช่น File Type .pdf เป็นต้น

1.1.15 สามารถป้องกันภัยคุกคามประเภท Vulnerability และ Spyware ได้โดยสามารถมีการอัพเดท Signature ใหม่แบบอัตโนมัติได้

1.1.16 สามารถทำการคัดกรอง log ( log filtering ) และส่ง log ผ่าน HTTP-based API ไปยังอุปกรณ์ 3rd Party ต่าง ๆ ได้ หรือสามารถเสนออุปกรณ์ที่รับ Syslog เข้าไป Process แล้วส่งค่า HTTP-based API ออกมาให้ อุปกรณ์ 3rd Party ต่าง ๆ ได้

1.1.17 สามารถเรียกดูสรุปข้อมูลของ Traffic Log ชนิดต่างๆ ผ่านทาง WebGUI ของอุปกรณ์เองได้

1.1.18 สามารถทำรายงานต่างๆ ได้อย่างน้อยดังนี้ หรือ เสนออุปกรณ์ทำรายงานที่มีความสามารถเทียบเท่า หรือ มากกว่า

- Top Application, Application Category
- Top Source, User, Destination
- User activity report
- สามารถทำรายงานรวมถึงปรับแต่งรายงานตามความต้องการ ในรูปแบบ PDF ได้เป็นอย่างน้อย
- สามารถตั้งเวลาส่งรายงานผ่านทาง Email แบบอัตโนมัติได้

กรณีอุปกรณ์ไม่สามารถทำ Report ขั้นต้นเหล่านี้ได้ สามารถเสนออุปกรณ์ในการทำ Report ที่รองรับการทำ Report ขั้นต้นนี้ได้

1.1.19 รองรับการติดตั้งเพื่อทำ High Availability แบบ Active-Active หรือ Active-Passive ได้เป็นอย่างน้อย

1.1.20 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย

1.1.21 มี Power Supply แบบ Redundant

1.1.22 อุปกรณ์ที่นำเสนอจะต้องอยู่ใน Gartner Magic Quadrant Enterprise Network Firewalls ระดับ Leader เป็นอย่างน้อย

1.1.23 ต้องรับประกันอุปกรณ์เป็นเวลาอย่างน้อย 3 ปี

1.1.24 มีโปรแกรมสำหรับจัดเก็บข้อมูลอุปกรณ์ป้องกันเครือข่าย ทำงานอย่างน้อยดังนี้

1.1.24.1 เป็นโปรแกรม สำหรับติดตั้งซอฟต์แวร์เพื่อใช้ในการจัดเก็บข้อมูลอุปกรณ์ป้องกันระบบเครือข่าย (Firewall) สำหรับติดตั้งลงบนเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (Virtual Machine) โดยสามารถเก็บรวบรวมเหตุการณ์ (logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่นำเสนอมาในโครงการ

1.1.24.2 สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH ได้

1.1.24.3 มีระบบการพิสูจน์ตัวตนของผู้ดูแลระบบ (Administrator) โดยใช้ฐานข้อมูลจาก Local Database และ RADIUS ได้เป็นอย่างน้อย

1.1.24.4 ระบบสามารถบริหารจัดการและปรับเปลี่ยนค่าต่างๆจากส่วนกลาง เช่น นโยบายรักษาความปลอดภัย (Policies), อ็อบเจ็กต์ (Object) แล้วทำการส่งผ่านการตั้งค่าไปยังอุปกรณ์รักษาความปลอดภัย บนเครือข่ายคอมพิวเตอร์ลูกข่ายที่นำเสนอได้

1.1.24.5 สามารถเรียกดูสรุปข้อมูลของ Applications, URL Categories, Threats, System health และ Data ในรูปแบบของกราฟฟิคได้

1.1.24.6 สามารถทำรายงาน รวมถึงปรับแต่งรายงานตามความต้องการ ในรูปแบบ CSV และ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลาส่งรายงานผ่านทาง Email แบบอัตโนมัติได้

1.1.24.7 สามารถบริหารจัดการและควบคุมอุปกรณ์ป้องกันเครือข่าย (Firewall) ที่ใช้ในโครงการนี้ได้จากส่วนกลาง

1.1.24.8 รองรับการใช้งานและให้การสนับสนุนไม่น้อยกว่า 3 ปี

**1.2 อุปกรณ์ตรวจจับข้อมูลจราจรทางเครือข่าย มีคุณลักษณะเฉพาะอย่างน้อย ดังนี้**

1.2.1 ระบบตรวจจับข้อมูลจราจรทางเครือข่าย Sensor หรือ Network Traffic Analysis หรือ Event Receiver หรือ Event/Flow Collector หรือเทียบเท่าสำหรับวิเคราะห์ Logs หรือ Network Traffic จากตัวอุปกรณ์ต้นทาง และไม่ใช่อุปกรณ์ Firewall

1.2.2 มีเนื้อที่จัดเก็บข้อมูลหรือ Hard Disk ขนาด 1 TB (ก่อนทำการ Format) หรือดีกว่า

1.2.3 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) อย่างน้อยดังนี้

1.2.3.1 แบบ 10/100/1000 Base-T จำนวนไม่น้อยกว่า 6 ช่อง

1.2.3.2 แบบ 10G SFP+ จำนวนไม่น้อยกว่า 2 ช่อง

1.2.4 มี Power Supplies แบบ Redundant จำนวนไม่น้อยกว่า 2 หน่วย

1.2.5 มีความสามารถในการทำงานในสภาวะปกติ Peak Sustained Throughput ได้ไม่น้อยกว่า 2 Gbps

1.2.6 สามารถวิเคราะห์และประมวลผล Logs หรือ Traffic จากระบบและอุปกรณ์ต่าง ๆ ได้แก่ Network Switch, Firewall และ Endpoint Protection แบบ Traffic Mirror (SPAN) หรือแบบ API ได้

1.2.7 สามารถทำการวิเคราะห์ข้อมูลในเครือข่ายจาก Network Traffic หรือการทำ Security Analytic เพื่อทำการตรวจจับ Malware และ Threat ต่าง ๆ ประกอบด้วย Web Attack, Vulnerability Exploit Detection, Brute-Force Attack, Malware, APT Detection และ Abnormal Traffic ได้

1.2.8 สามารถตรวจจับประเภทข้อมูลจราจรทางคอมพิวเตอร์ได้อย่างน้อยดังนี้ DNS Flow, HTTP Flow, SMB Flow และ Mail Flow

1.2.9 สามารถส่ง Security Events และ Abnormal Behavior ไปยังอุปกรณ์วิเคราะห์สำหรับตรวจจับภัยคุกคามอัจฉริยะและแพลตฟอร์มการตอบสนองในโครงการนี้ได้

1.2.10 สามารถตรวจจับวิธีการบุกรุกเว็บไซต์ (Web Attack) ได้อย่างน้อย ดังนี้ SQL Injection, XSS Attack, Trojan, Website Scan, Webshell, Cross-site Request Forgery, OS Command Injection, File Inclusion, Path Traversal และ Information Disclosure

1.2.11 สามารถตรวจจับ Password Protection ได้อย่างน้อย ดังนี้ FTP weak password, Web-access weak password และ Web-access cleartext

1.2.12 สามารถตรวจจับวิธีการบุกรุกทางเครือข่ายขั้นสูง (APT) ได้อย่างน้อย ดังนี้ IP Scanning, Port Scanning, DGA Domain, DDoS, Reverse Connection, IRC Communication, Bitcoin mining, HFS File transfer และ Web Reputation

1.2.13 สามารถตรวจจับวิธีการโจมตีผ่านช่องโหว่ (Vulnerability) ได้อย่างน้อย ดังนี้ Database, DNS, FTP, Mail, Network Devices, Shellcode, System, Telnet, Web, Application, Web ActiveX, Backdoor, Spyware, Trojan และ Worm Vulnerability ได้

1.2.14 สามารถใช้งานตามมาตรฐาน IPv6 ได้

1.2.15 สามารถตรวจจับการบุกรุกจาก Real Time Streaming Protocol (RTSP) ได้

1.2.16 ต้องรับประกันอุปกรณ์เป็นเวลาอย่างน้อย 3 ปี

**1.3 อุปกรณ์วิเคราะห์สำหรับตรวจจับภัยคุกคามอัจฉริยะและแพลตฟอร์มการตอบสนอง จำนวน 1 ชุด มีรายละเอียดคุณลักษณะเฉพาะอย่างน้อย ดังนี้**

1.3.1 เป็นอุปกรณ์สำหรับตรวจจับภัยคุกคามอัจฉริยะและแพลตฟอร์มการตอบสนองในรูปแบบ Appliance หรือ Virtual Appliance โดยหากเสนอในรูปแบบ Virtual Appliance ต้องมีเครื่องคอมพิวเตอร์แม่ข่ายเพื่อใช้ติดตั้ง Virtual Appliance ที่เสนอ

1.3.2 Appliance หรือ เครื่องคอมพิวเตอร์แม่ข่ายเพื่อใช้ติดตั้ง Virtual Appliance ต้องมีคุณลักษณะเฉพาะอย่างน้อย ดังนี้

1.3.2.1 มีหน่วยประมวลผลกลาง CPU โดยมีจำนวนแกนประมวลผล (Core) ไม่น้อยกว่า 16 แกนหลัก (16 Cores)

1.3.2.2 มีหน่วยความจำ (Memory) ไม่น้อยกว่า 128 GB

1.3.2.3 มีเนื้อที่จัดเก็บข้อมูลหรือ Hard Disk ขนาด 32 TB (ก่อนทำการ Format)

1.3.2.4 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) อย่างน้อยดังนี้

1.3.2.4.1 แบบ 10/100/1000 Base-T จำนวนไม่น้อยกว่า 6 ช่อง

1.3.2.4.2 แบบ 10G SFP+ จำนวนไม่น้อยกว่า 2 ช่อง

1.3.2.5 มี Power Supplies แบบ Redundant จำนวนไม่น้อยกว่า 2 หน่วย

1.3.2.6 ในกรณีเสนอในรูปแบบ Virtual Appliance ต้องสามารถติดตั้งใช้งาน Virtual Appliance ที่เสนอ บนเครื่องคอมพิวเตอร์แม่ข่ายได้

1.3.3 สามารถบริหารจัดการผ่าน Web Interface หรือ GUI ได้เป็นอย่างน้อย

1.3.4 ระบบสามารถบันทึกและดึงข้อมูล Log ประเภทต่าง ๆ ได้ เช่น DNS, Traffic, Web Attack, Vulnerability Exploit, Botnet และ Admin logs ได้

1.3.5 สามารถค้นหาและดึงข้อมูล Logs ได้โดยการกำหนด Combination Key ต่าง ๆ อย่างน้อยดังนี้ Log types, IP Address, Port, Data Source และ Attack Type เพื่อช่วยในการค้นหา

1.3.6 มีรูปแบบความสัมพันธ์ (Correlation Rules) สำหรับใช้วิเคราะห์ข้อมูลภัยคุกคามหรือ Security Event ได้ โดยไม่ต้องข้อมูลที่ต้องสงสัยไปวิเคราะห์ยังภายนอก

1.3.7 มีคุณลักษณะการวิเคราะห์เหตุการณ์โดยใช้เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence หรือ Machine Learning)

1.3.8 สามารถตรวจสอบปัญหาและ Drill down ลงไปถึงข้อมูลในเครือข่ายระดับ Flow หรือ Logs ของ Transaction ที่เกิดปัญหาได้

1.3.9 สามารถวิเคราะห์ผลกระทบจากภัยคุกคามได้ (Threat Impact Analysis) แหล่งที่มาของการโจมตี เช่น Entry Point และ Traceback Asset Relation ได้

1.3.10 สามารถบริหารจัดการรายละเอียดอุปกรณ์ Asset Management โดยสามารถตรวจพบอุปกรณ์ต้นทางได้โดยอัตโนมัติ (Auto-discovered) และสามารถกำหนด IP Address, Group, Hostname, Owner, OS, Service(Port) ได้เป็นอย่างน้อย

1.3.11 ระบบมีความสามารถวิเคราะห์ไฟล์ (File Threat Analysis) ได้โดยมีสามารถวิเคราะห์แบบ Static Engine และ AI Engine

1.3.12 มี Responses Policy หรือ Playbook พร้อมใช้มาให้กับระบบ (Build-in) และสามารถสร้างเพิ่มเติม แก้ไข ปรับเปลี่ยนตามต้องการ (Customize) ได้

1.3.13 สามารถกำหนดให้ Responses Policy หรือ Playbook ทำงานได้ตามเงื่อนไขหรือเหตุการณ์ที่กำหนดได้

1.3.14 สามารถกำหนดให้ Responses Policy หรือ Playbook ทำงานตามช่วงเวลาที่กำหนดหรือ Task ที่กำหนดได้

1.3.15 เป็นผลิตภัณฑ์ที่มีเครื่องหมายการค้าเดียวกันกับระบบตรวจจับข้อมูลจราจรทางเครือข่าย

1.3.16 สามารถแจ้งเตือนผ่าน Email หรือ SMS ได้

1.3.17 สามารถออกรายงานในรูปแบบ PDF หรือ DOC ได้

1.3.18 สามารถทำงานร่วมกับอุปกรณ์ป้องกันเครือข่ายในโครงการนี้ได้แบบอัตโนมัติ โดยส่งคำสั่ง Correlated Block และ Access Control ได้เป็นอย่างน้อย

1.3.19 ต้องรับประกันอุปกรณ์เป็นเวลาอย่างน้อย 3 ปี

**1.4 โปรแกรมตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยและภัยคุกคามพร้อมทำการตอบสนอง (Extended Detection and Response) สำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) จำนวนไม่น้อยกว่า 20 การใช้งาน มีคุณสมบัติอย่างน้อย ดังนี้**

1.4.1 เป็นระบบป้องกันไวรัสลิขสิทธิ์แบบ Cloud-based โดยสามารถบริหารจัดการได้ผ่าน Web Interface ของระบบ Cloud ของผู้ให้บริการ

1.4.2 สามารถรองรับการติดตั้งและใช้งานได้บนระบบปฏิบัติการดังต่อไปนี้ ระบบปฏิบัติการ Windows Server 2008 R2, SBS 2011, 2012, 2012 R2, 2016, 2019 และ Linux ได้เป็นอย่างน้อย

1.4.3 เป็นโปรแกรมป้องกันไวรัสสามารถป้องกันภัยคุกคามจาก Viruses, Worms, Trojans, Spyware และ Malware ได้เป็นอย่างน้อย

1.4.4 มีเทคโนโลยีในการตรวจสอบไวรัสหรือมัลแวร์ที่ใช้เทคนิค Deep Learning AI, Signature-based Malware detection, Anti-exploit techniques เพื่อป้องกันเครื่องคอมพิวเตอร์แม่ข่ายจาก Malware, File-less attacks และ Zero-day exploits ได้เป็นอย่างน้อย

1.4.5 สามารถยกเว้นการสแกนโดยกำหนดในรูปแบบ File, Folder, Process, Website, AMSI, IPS และ Exploits ได้เป็นอย่างน้อย

1.4.6 สามารถป้องกันมัลแวร์ชนิดแรนซั่มแวร์ (Ransomware) จากการเข้ารหัสไฟล์ และสามารถเรียกคืนไฟล์ (Rolls Back Files) ที่ถูกเข้ารหัสจากมัลแวร์คอมพิวเตอร์ชนิดแรนซั่มแวร์ (Ransomware) ได้

1.4.7 สามารถป้องกันมัลแวร์ชนิดแรนซั่มแวร์ (Ransomware) จากการเข้ารหัสที่ Master boot record ได้

1.4.8 สามารถป้องกันการโอนย้ายข้อมูลออกจากเครื่องคอมพิวเตอร์ (Data Loss Prevention – DLP) โดยสามารถระบุเงื่อนไขได้ดังนี้ ชื่อไฟล์และนามสกุลไฟล์ (File Name) ประเภทของไฟล์ (File Type) และ เนื้อหาที่อยู่ในไฟล์เอกสาร (Content Rule) โดยไม่ต้องซื้อ Subscription เพิ่มเติม

1.4.9 มีความสามารถในการควบคุมพอร์ตการเชื่อมต่อบนเครื่องแม่ข่ายโดยสามารถกำหนดสิทธิ์การใช้งาน เช่น Allow, Read Only และ Block ให้กับอุปกรณ์ประเภท Removable storage ได้

1.4.10 สามารถควบคุมการเข้าถึงเว็บไซต์ (Web Control) ที่ไม่พึงประสงค์ตามโดยสามารถเลือก Allow, Warn และ Block ได้

1.4.11 สามารถเปลี่ยนแปลง Website category และสร้าง Website Tag เพื่อควบคุมการใช้งาน Website ของเครื่องแม่ข่ายได้

1.4.12 สามารถป้องกันการรันซอฟท์แวร์ที่ไม่ได้รับอนุญาตบนเครื่องคอมพิวเตอร์แม่ข่ายได้ (Server Lockdown)

1.4.13 สามารถทำ File Integrity Monitoring เพื่อให้สอดคล้องตาม PCI DSS โดยสามารถ Monitor การเปลี่ยนแปลงของ Files, Folders, Registry keys และ registry values ได้เป็นอย่างน้อย

1.4.14 สามารถทำการแจ้งเตือนการพบไวรัสคอมพิวเตอร์ผ่านทาง Desktop messaging, Email alert และ Event logging ได้เป็นอย่างน้อย

1.4.15 สามารถเรียกดูจุดกำเนิดของการโจมตีได้ โดยแสดงผลให้เห็นทั้ง Process ต้นกำเนิด (Root Cause) การเรียกใช้งานของ Process การเปิด Connection ไปยัง IP ต่าง ๆ การโจมตีช่องโหว่ (Exploit) ของ Application บนเครื่องแม่ข่าย

1.4.16 สามารถป้องกันการปรับเปลี่ยนการตั้งค่า และป้องกันการถอนการติดตั้งโปรแกรมป้องกันไวรัสโดยใช้รหัสผ่านได้ (Tamper Protection)

1.4.17 รองรับการสื่อสารกันระหว่าง Endpoint กับอุปกรณ์ป้องกันการบุกรุก เช่น Firewall,IPS เพื่อจำกัดการเข้าใช้งานของ Endpoint ที่ไม่ปลอดภัยในเครือข่าย (Security Heartbeat

1.4.18 สามารถตัดการเชื่อมต่อ (Containment/Isolation) เครื่องแม่ข่ายออกจากระบบเครือข่ายผ่านทางระบบบริหารจัดการได้ โดยสามารถเลือก Isolate ได้แม้ไม่มีสถานะติดไวรัส โดยอนุญาติให้เชื่อมต่อได้เพียงระบบบริหารจัดการ เช่น DNS, DHCP, PING, Local port, Remote port, และ Remote address ที่ระบุไว้เท่านั้น

1.4.19 สามารถทำการดึงข้อมูลที่ต้องการจากเครื่องแม่ข่าย เพื่อใช้ในการตรวจสอบและวิเคราะห์ถึงการโจมตีที่เกิดขึ้นได้ (forensic snapshot)

1.4.20 รองรับการค้นหาข้อมูลข้ามฐานข้อมูลผลิตภัณฑ์อื่นได้ในอนาคต เช่น Firewall และ E-mail ได้เป็นอย่างน้อย

1.4.21 ผลิตภัณฑ์ที่นำเสนอต้องมีชื่อใน Gartner Magic Quadrant ในส่วนของ Magic Quadrant for Endpoint Protection Platforms เป็นอย่างน้อย

**2. ระบบบริหารการติดต่อสื่อสารและพัฒนาการเรียนรู้จัดการการเข้าถึงจากระยะไกล จำนวน 1 ระบบ ต้องมีคุณลักษณะดังนี้**

**2.1 เป็นอุปกรณ์ SSLVPN แบบ Appliance ที่ออกแบบมาเพื่อใช้เป็น SSLVPN โดยเฉพาะ ไม่ใช่อุปกรณ์แบบ UTM (Unified Threat Management)**

2.1.1 สามารถใช้งานพร้อมกันจำนวนไม่น้อยกว่า 300 Concurrent Connections หรือ Concurrent sessions/Users พร้อมลิขสิทธิ์การใช้งาน

2.1.2 มี SSL VPN Throughput ในรูปแบบ Max Tunnel Throughput SSL mode ไม่น้อยกว่า 2.5Gbps หรือ Max Throughput ESP mode ไม่น้อยกว่า 3.5 Gbps

2.1.3 มี Interface แบบ 1/10GbE จำนวนไม่น้อยกว่า 2 พอร์ต และมี Interface แบบ 1GbE ที่ใช้ในการบริหารจัดการจำนวนไม่น้อยกว่า 1 พอร์ต

2

2.1.4 สามารถใช้งานแบบ Clientless โดยไม่ต้องติดตั้งโปรแกรมเพิ่มเติมที่เครื่อง Client โดยรองรับ Application และ Protocol ดังนี้

2.1.4.1 Web-based Application

2.1.4.2 Remote Desktop Protocol (RDP)

2.1.4.3 SharePoint

2.1.4.4 HTML5 browsers

2.1.5 มี Memory (RAM) ไม่น้อยกว่า 16 GB และ Storage ไม่น้อยกว่า 480 GB SSD

2.1.6 อุปกรณ์ที่เสนอต้องมี Form Factor แบบ Rack Mountable

2.1.7 สามารถทำ Split Tunneling ได้

2.1.8 มี Software Agent ภายใต้ผลิตภัณฑ์เดียวกันกับอุปกรณ์

2.1.9 สามารถทำการตรวจสอบสิทธิการใช้งาน (Authentication) โดยใช้ Authentication Server ดังต่อไปนี้

2.1.9.1 Local Authentication Server

2.1.9.2 LDAP Server

2.1.9.3 RADIUS Server

2.1.9.4 AD Server

2.1.9.5 Certification Server

2.1.9.6 SAML Server

2.1.10 สามารถตรวจสอบคุณสมบัติของเครื่อง Client (Host Checker) ก่อนการอนุญาตให้ Login หรือ ก่อนได้รับสิทธิ์ โดยต้องสามารถกำหนดการตรวจสอบได้อย่างน้อยดังนี้

2.1.10.1 การตรวจสอบสำหรับ Windows

2.1.10.1.1 Antivirus

2.1.10.1.2 Firewall

2.1.10.1.3 Operating System

2.1.10.1.4 Ports

2.1.10.1.5 Registry

2.1.10.1.6 MAC Address

2.1.10.1.7 File

2.1.10.1.8 Process

2.1.10.1.9 Machine Certificate

2.1.10.2 การตรวจสอบสำหรับ Mac

2.1.10.2.1 Antivirus

2.1.10.2.2 Firewall

2.1.10.2.3 Ports

2.1.10.2.4 Process

2.1.10.2.5 File

2.1.11 สามารถลบข้อมูลที่เกิดขึ้นระหว่างการเชื่อมต่อ หลังจากที่ผู้ใช้งานออกจากระบบ เช่น Browser Cache, Session, Cookies และ Passwords ได้เป็นอย่างน้อย

2.1.12 รองรับการทำงานของ SSL , TLS v.1.0,TLS v1.1 และ TLS v1.2 ได้

2.1.13 สามารถรองรับการใช้งานจาก Web browser เช่น Google Chrome, Internet Explorer, Firefox ได้เป็นอย่างน้อย

2.1.14 สามารถใช้งานจาก Operating System ในเครื่อง Client ได้หลากหลาย อย่างน้อย ดังต่อไปนี้

2.1.14.1 Windows

2.1.14.2 Mac OSX

2.1.14.3 Linux

2.1.14.4 iOS Mobile Device

2.1.14.5 Android Mobile Device

2.1.15 ผู้ดูแลระบบต้องสามารถ Monitor ผ่าน Web เพื่อตรวจสอบ User Session ที่ใช้งานขณะนั้น รวมถึงสามารถ Delete Session (Disconnect) ของ User แต่ละคนได้

2.1.16 สามารถทำ Single Sign-ON (SSO) แบบ NTLMV2, Kerberos, Basic Authentication, forms-based, header variable-based, และ SAML-based ได้

2.1.17 สามารถกำหนดช่วงเวลา Idle timeout และ Session timeout ของ User แต่ละกลุ่ม (Role) ได้ และกำหนดให้มีการแจ้งเตือนก่อน timeout ได้

2.1.18 สามารถกำหนดให้ผู้ใช้งานสามารถเข้าใช้งานได้หลาย sessions พร้อมกัน (Multiple session per user)

2.1.19 สามารถส่ง Log ไปยัง Syslog Server ภายนอกได้

2.1.20 สามารถรองรับการทำ Simple Network Management Protocol (SNMP) ได้

2.1.21 อุปกรณ์ที่เสนอต้องได้รับมาตรฐานความปลอดภัย TuV SUD หรือ TuV GS, IEC หรือ CE เป็นอย่างน้อย

2.1.22 ผลิตภัณฑ์ต้องได้รับการรับรองตามมาตรฐาน ICSA Lab Certified SSL-TLS หรือ FIPS 140-2

2.1.23 รองรับการทำงานร่วมกับระบบพิสูจน์ตัวตนแบบหลายปัจจัย (Multi Factor Authentication: MFA) ร่วมกับ Google Authenticator, RSA, one-time passwords(OTP) และ Certificate Authentication ได้เป็นอย่างน้อย

2.1.24 รองรับการทำงานร่วมกันระหว่าง Virtual Desktop Infrastructure (VDI)ได้

**2.2 ระบบบริหารจัดการพิสูจน์ตัวตน จำนวน 1 ระบบ**

2.2.1 ตั้งและปรับปรุง Configuration พื้นฐานให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพ โดยใช้ Software Open Source บนระบบปฏิบัติการตระกูล Linux, FreeBSD, NetBSD ในการพัฒนา

2.2.2 สามารถเชื่อกับฐานข้อมูลผู้ใช้ระบบงาน SSRU ของระบบงานเดิมกับการใช้งานได้

2.2.3 รองรับการเชื่อมต่อกับฐานข้อมูลของผู้ใช้งานภายนอก (External User Databases) ดังต่อไปนี้ LDAP, MySQL, PostgreSQL, Oracle , MsSQL ได้เป็นอย่างน้อย

2.2.4 สามารถสนับสนุนการทำ Authentication, Authorization และ Accounting ได้

2.2.5 สนับสนุนมาตรฐาน Authentication แบบ PAP ,CHAP ,MS-Chap และ MS-CHAP-V2 เป็นอย่างน้อย

2.2.6 สามารถบริหารจัดการ Account ผ่านทาง Web Browser ได้ โดยมีรายละเอียดดังต่อไปนี้

2.2.6.1 ส่วนของผู้ใช้ทั่วไป

2.2.6.1.1 ทำการเชื่อมต่อข้อมูลชื่อผู้ใช้และรหัสผ่านจากในฐานข้อมูลของระบบพิสูจน์ตัวตนเดิมของมหาวิทยาลัยฯ ที่ใช้อยู่ในปัจจุบัน

2.2.6.1.2 ระบบสามารถแสดงสถานะการใช้งานของผู้ใช้นั้นๆ ได้ ในรูปแบบรายงาน

2.2.6.1.3 ผู้ใช้สามารถตรวจสอบการใช้งานของตนเองที่ได้ลงทะเบียนไว้ได้สูงสุด 90 วัน โดยสามารถค้นหาย้อนหลังได้จาก วันที่ถึงวันที่

2.2.6.2 ส่วนของผู้ดูแลระบบ

2.2.6.2.1 สามารถค้นหารายการผู้ใช้ ที่ต้องการได้

2.2.6.2.2 แสดงรายงานผู้ใช้ ทั้งหมดหรือแสดงแบบเงื่อนไขตามที่ผู้ดูระบบต้องการได้ ดังต่อไปนี้

- ชื่อผู้ใช้
- ชื่อ-สกุล
- ชื่ออีเมล์
- ประเภทบุคคล ได้แก่ นักศึกษา เจ้าหน้าที่ อาจารย์(กลุ่ม)
- คณะวิชา

2.2.6.2.3 สรุปผลรายการผู้ใช้ แบบมีเงื่อนไขตามที่ผู้ดูแลระบบต้องการและแสดงในรูปแบบของไฟล์ Excel ได้

2.2.6.2.4 สามารถตรวจสอบการใช้งานย้อนหลังในแต่ละหมายเลข MAC Addressทั้งหมดได้สูงสุด 90 วัน

2.2.6.2.5 สามารถลบ แก้ไข ข้อมูลผู้ใช้ ตามคำร้องจากผู้ใช้งานได้

2.2.6.2.6 สามารถกำหนดจำนวนการใช้งานพร้อมกัน ต่อ 1 username ได้

2.2.6.2.7 สามารถกำหนดจำนวนการ ดาวน์โหลด สูงสุดได้ โดยกำหนดเป็น

- ต่อวัน
- ต่อสัปดาห์
- ต่อเดือน

2.2.6.2.8 สามารถกำหนดจำนวนเวลาการใช้งาน สูงสุดได้ โดยกำหนดเป็น
- ต่อวัน
- ต่อสัปดาห์
- ต่อเดือน

2.2.6.2.9 สามารถกำหนดวันหมดอายุได้

2.2.6.2.10 สามารถกำหนด ช่วงเวลาการใช้งานได้ เช่น วันจันทร์ ใช้งานได้ 8:00-13:00 วันอังคาร ใช้งานได้ 9:00-15:00

2.2.6.2.11 ส่วนของผู้ดูแลระบบระดับสูงสุด สามารถกระทำทุกอย่างเหมือนกับผู้ดูแลระบบแต่มีความสามารถกระทำได้เพิ่มเติมดังนี้

2.2.6.2.11.1 สามารถเพิ่ม ลบ แก้ไขผู้ดูแลระบบได้

2.2.6.2.11.2 สามารถกำหนดสิทธิ์การใช้งานของผู้ดูแลระบบในแต่ละเมนูได้ โดยแบ่งสิทธิ์เป็น ไม่เห็นเมนู, ดูได้อย่างเดียว, จัดการทุกอย่างได้ เป็นอย่างน้อย

2.2.6.2.11.3 สามารถตรวจสอบเหตุการณ์การทำงานของผู้ใช้โดยมีการตรวจสอบเหตุการณ์ย้อนหลังว่าที่ผ่านมามีการเปลี่ยนแปลงข้อมูลอะไรบ้าง (User log)

2.2.6.2.11.4 สามารถตรวจสอบการทำงานของผู้ดูแลระบบ โดยมีการตรวจสอบเหตุการณ์ย้อนหลังว่าที่ผ่านมาว่า ได้ทำการ เพิ่มลบแก้ไข ข้อมูลอะไรบ้าง (Admin log)

2.2.6.2.12 รับประกันเป็นเวลา 1 ปี ในกรณีที่เกิดปัญหาจะมีการติดต่อเข้ามาทำการแก้ไขโดยวิธีการรีโมทเพื่อทำให้การแก้ไขเป็นไปอย่างรวดเร็ว และหากกรณียังแก้ไขไม่ได้ต้องส่งเจ้าหน้าที่เข้า On-Site Service หลังจากที่ได้รับแจ้ง

**ข้อกำหนดทั่วไป**

1. ผู้เสนอราคาจะต้องประกอบธุรกิจเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์ และมีประสบการณ์การติดตั้งอุปกรณ์เครือข่ายอย่างน้อย 1 โครงการมูลค่าไม่ต่ำกว่า 5,000,000 บาท โดยให้ทำเอกสารแนบมาในวันยื่นซองด้วย
2. ผู้เสนอราคาต้องจัดทำเอกสารเปรียบเทียบรายละเอียดข้อเสนอกับข้อกำหนดรายละเอียด (Specification) ของ มหาวิทยาลัย เป็นรายข้อทุกข้อ (Statement of compliance) โดยใช้เปรียบเทียบแบบตาราง ในการเปรียบเทียบรายการดังกล่าว หากมีกรณีที่ต้องมีการอ้างอิงข้อความหรือเอกสารในส่วนอื่น ที่จัดทำเสนอมาผู้เสนอ ราคาจะต้องระบุให้เป็นไปอย่างชัดเจน สามารถตรวจสอบได้ง่ายไว้ในเอกสาร เปรียบเทียบด้วยว่า สิ่งที่ต้องการอ้างอิงถึงให้หมายเหตุหรือขีดเส้นใต้หรือระบายสีพร้อมเขียนหัวข้อกำกับไว้ เพื่อให้สามารถไปตรวจสอบกับ เอกสารเปรียบเทียบได้ง่าย และตรงกันด้วย “หากผู้เสนอราคาไม่ดำเนินการตามข้อนี้คณะกรรมการพิจารณาผลการประกวดราคาขอสงวนสิทธิในการไม่พิจารณาข้อเสนอของผู้เสนอราคา”
3. ผู้เสนอราคาจะต้องทำความเข้าใจในเอกสารทุกฉบับให้เป็นที่เข้าใจโดยชัดแจ้งและไม่ว่ากรณีใดๆ ผู้เสนอราคาจะ ยกขึ้นเป็นข้ออ้าง โดยอาศัยเหตุผลจากการที่ละเลยไม่ทำความเข้าใจในข้อความดังกล่าวหรือละเลยไม่ปฏิบัติตามข้อความนั้น หรือโดยการอ้างความสำคัญผิดในความหมายของข้อความในใบแจ้งความเสนอนั้นไม่ได้
4. ผู้เสนอราคาต้องทำการเสนอแผนดำเนินการติดตั้งให้กับมหาวิทยาลัยมาใน วันยื่นซองเอกสารด้วย
5. ในกรณีที่มีความจำเป็นต้องตีความข้อความใดในเอกสารประกวดราคา หรือเอกสารเสนอราคา หรือเอกสารอื่นใดก็ตาม ซึ่งมีความจำเป็นต้องวินิจฉัยตัดสินในการประกวดราคา เพื่อให้การประกวดราคาเป็นไป ด้วยความเรียบร้อยและบรรลุวัตถุประสงค์ มหาวิทยาลัย สงวนสิทธิ์ที่จะเป็นผู้ตีความและวินิจฉัยข้อขัดแย้ง ซึ่งให้ถือเป็นอันเด็ดขาดและถึงที่สุด
6. ผู้เสนอราคาต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศโดยให้ยื่นขณะเข้าเสนอราคาของอุปกรณ์ที่เสนอ
7. ผู้เสนอราคาต้องมีผู้เชี่ยวชาญที่ได้รับประกาศนียบัตร (Certified Professional) สำหรับระบบเครือข่าย CCNP หรือ Palo Networks Accredited System Engineer (PSE) อย่างน้อย 2 คน โดยให้ยื่นขณะเข้าเสนอราคา
8. ผู้เสนอราคาต้องทำการเซ็นบันทึกข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement)กับสำนักวิทยบริการและเทคโนโลยีสารสนเทศในวันทำสัญญาและให้ถือว่าเอกสารฉบับนี้เป็นส่วนหนึ่งของคู่สัญญาด้วย
9. ผู้เสนอราคาต้องส่งสินค้า ภายใน 120 วันนับจากวันทำสัญญา

**การรับประกันและบริการ** หลังจากการติดตั้งเสร็จเรียบร้อยแล้ว ผู้เสนอราคาจะต้อง

1. รับประกันเครื่องอุปกรณ์และการติดตั้ง และให้ใช้งานได้กับระบบเดิม ถ้าหากเกิดการขัดข้อง ชำรุด เสียหายเนื่องจากเครื่องและชิ้นส่วนไม่ถูกต้อง สาเหตุที่เป็นไปตามสัญญาที่ทำกับผู้ซื้อ นับตั้งแต่วันตรวจรับมอบในระยะเวลาดังกล่าวนี้ ผู้เสนอราคาจะต้องทำการซ่อมแซมเปลี่ยนใหม่โดยไม่คิดมูลค่า
2. การติดตั้งระบบฯ ต้องไม่กระทบต่อการทำงานของระบบเดิม หรือก่อให้เกิดความเสียหายแก่ทางมหาวิทยาลัย ทั้งนี้หากมีความเสียหายเกิดขึ้นจากการติดตั้งระบบฯ หรืออุปกรณ์ที่เสนอไม่สามารถรองรับปริมาณการใช้งานได้ ผู้เสนอราคาต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้น และต้องดำเนินการให้สามารถใช้งานได้ตามปกติ
3. หาก Firmware ของอุปกรณ์หรือ Software ใด ๆ ของระบบที่เสนอในโครงการนี้มีเวอร์ชั่นที่ได้รับการปรับปรุงและสอดคล้องกับการใช้งานของมหาวิทยาลัย ให้ทำการปรับปรุงให้เป็นเวอร์ชั่นปัจจุบันด้วยเมื่อเกิดปัญหา โดยผู้เสนอราคาไม่คิดค่าใช้จ่าย ใด ๆ จากทางมหาวิทยาลัย
4. กรณีเครื่องอุปกรณ์การติดตั้งมีปัญหา ต้องดำเนินการซ่อมและบริการให้ใช้งานได้ภายใน 1 วัน หากไม่สามารถซ่อมได้ให้นำอุปกรณ์มาให้ใช้งานทดแทนจนกว่าจะทำการซ่อมเสร็จ
5. จัดทำแผนการดูแล ตรวจเช็คระบบเครื่องและอุปกรณ์ เดือนละ 2 ครั้ง เป็น onsite หรือ online Support ได้แล้วแต่สถาณการณ์ไม่ปกติเช่น การเกิดจราจล การแพร่ระบาดของไวรัส Covid-19
6. ผู้เสนอราคาต้องจัดอบรมผลิตภัณฑ์ที่เสนอให้กับผู้ดูแลระบบไม่น้อยกว่า 1 หลักสูตร
7. รับประกันเครื่องอุปกรณ์ไม่น้อยกว่า 3 ปี