ส่วนที่ 1: ข้อมูลหน่วยงานและผู้ขอใช้

ชื่อ-นามสกุลผู้ขอใช้ _____ ตำแหน่ง _____

หน่วยงาน _____ กลุ่มงาน/ภาควิชา _____

พื้นที่การศึกษา _____ อยู่ที่ อาคาร _____ ชั้น _____ ห้อง _____

เบอร์โทรศัพท์ติดต่อ (ภายใน)_____ เบอร์โทรศัพท์มือถือ _____

อีเมล (อีเมลมหาวิทยาลัยเท่านั้น) _____

ส่วนที่ 2: ขอใช้ Public IP Address

มีความประสงค์ขอใช้ Public IP Address จำนวน _____ เลขหมาย Domain _____

วัตถุประสงค์ในการใช้งาน _____

_____

_____

_____

ชนิด/แบบ ☐ Server ☐ PC ☐ อื่นๆ โปรดระบุ _____

ชื่ออุปกรณ์ / เซิร์ฟเวอร์ : _____

ยี่ห้อ _____ รุ่น _____ ระบบปฏิบัติการ _____

หมายเลข Hardware Address/Mac Address _____

บริการที่ต้องการเปิดใช้งาน (Service/Application):

1. _____
2. _____
3. _____

พอร์ตที่ต้องการเปิด (Port / Protocol):

Port _____ / TCP

Port _____ / UDP

Port _____ / TCP/UDP

ขอบเขตการอนุญาตเข้าถึง:

☐ Allow from Internet (0.0.0.0/0)

☐ Allow from Specific IP / Subnet: _____

☐ อื่น ๆ: _____

ต้องการ NAT แบบ:

☐ Full NAT

☐ ไม่ต้องการ NAT (ใช้ Public IP บน Interface/Server/PC โดยตรง)

ผู้ดูแล / ควบคุมเครื่อง นาย/นาง/นางสาว_____

เบอร์โทรศัพท์ติดต่อ (ภายใน)_____ เบอร์โทรศัพท์มือถือ _____

ระเบียบการใช้บริการระบบเครือข่ายมหาวิทยาลัย
(ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560)

1. ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ (มาตรา 10)
2. ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ
   2.1 โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา
   2.2 นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน
   2.3 นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา
   2.4 นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้
   2.5 เผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ตามข้อ 2.1 – 2.4 โดยรู้อยู่แล้วว่าเป็นข้อมูลดังกล่าว (มาตรา 14)
3. ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท (มาตรา 16)
4. การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ (Computer Log) ตามกฎหมาย
   เพื่อให้การใช้งาน Public IP Address ของมหาวิทยาลัยเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ พ.ศ. 2563 สำนักคอมพิวเตอร์จะดำเนินการเก็บข้อมูลจราจรคอมพิวเตอร์ (Computer Log) ดังต่อไปนี้
   4.1 สำนักคอมพิวเตอร์จะจัดเก็บข้อมูลจราจรคอมพิวเตอร์ที่สามารถระบุความเชื่อมโยงระหว่างผู้ใช้ อุปกรณ์ และ Public IP Address ได้อย่างชัดเจนดังข้อด้านล่างดังนี้
      4.1.1 หมายเลข IP Address (Private และ Public)
      4.1.2 หมายเลข MAC Address
      4.1.3 วัน เวลาเริ่มต้นและสิ้นสุดการใช้งาน
      4.1.4 ข้อมูลการพิสูจน์ตัวตน (Authentication)
      4.1.5 ข้อมูลการเชื่อมต่อที่จำเป็นเพื่อการตรวจสอบเหตุการณ์ด้านความปลอดภัย
   4.2 ข้อมูลจราจรคอมพิวเตอร์จะถูกเก็บรักษาเป็นระยะเวลา ไม่น้อยกว่า 90 วัน นับจากวันที่ข้อมูลนั้นถูกสร้างขึ้น ตามที่กฎหมายกำหนด
   4.3 ในกรณีที่พนักงานเจ้าหน้าที่ตามกฎหมายร้องขอเป็นลายลักษณ์อักษร สำนักคอมพิวเตอร์มีหน้าที่ต้องขยายระยะเวลาเก็บข้อมูลจราจรคอมพิวเตอร์ออกไปได้ สูงสุดไม่เกิน 1 ปี เพื่อประโยชน์ในการสืบสวนหรือสอบสวน
   4.4 สำนักคอมพิวเตอร์จะรักษาความปลอดภัยของข้อมูลจราจรคอมพิวเตอร์ตามหลักเกณฑ์ที่เหมาะสม และจะเปิดเผยข้อมูลดังกล่าวเฉพาะเมื่อมีคำสั่งหรืออำนาจตามกฎหมายเท่านั้น
5. ไม่อนุญาตให้ใช้อุปกรณ์ประเภท NAS เชื่อมต่อด้วย Public IP
   ไม่อนุญาตให้นำอุปกรณ์ประเภท Network Attached Storage (NAS) มาใช้งานร่วมกับหมายเลข Public IP ของมหาวิทยาลัย ไม่ว่าด้วยวัตถุประสงค์ใด ๆ เนื่องจากอุปกรณ์ NAS มักถูกโจมตีจากอินเทอร์เน็ตสาธารณะอย่างแพร่หลาย และมีความเสี่ยงสูงต่อการถูกบุกรุกทางไซเบอร์ทั้งจากช่องโหว่ซอฟต์แวร์ การตั้งค่าที่ไม่ปลอดภัย หรือการเข้ารหัสข้อมูลเรียกค่าไถ่ (Ransomware) เพื่อความปลอดภัยของโครงสร้างพื้นฐาน

เครือข่ายของมหาวิทยาลัย สำนักคอมพิวเตอร์จะไม่อนุญาตให้มีการเปิดบริการ NAS ต่ออินเทอร์เน็ตโดยตรง และหากตรวจพบการใช้งานที่เข้าข่ายดังกล่าว สำนักคอมพิวเตอร์มีสิทธิ์ ระงับการใช้งาน Public IP นั้นทันที โดยไม่แจ้งให้ทราบล่วงหน้า

6. อำนาจการตรวจสอบและระงับการใช้งาน Public IP ของมหาวิทยาลัย

สำนักคอมพิวเตอร์มีสิทธิ์ตรวจสอบคอมพิวเตอร์หรืออุปกรณ์ที่ได้รับการจัดสรร Public IP Address ของมหาวิทยาลัย เพื่อยืนยันว่าเป็นอุปกรณ์ที่ถูกต้องตามกฎหมาย และปลอดภัยต่อระบบเครือข่าย

หากพบพฤติการณ์หรือพฤติกรรมที่อาจเข้าข่ายดังต่อไปนี้ ทางสำนักคอมพิวเตอร์จะระงับการใช้ Public IP ดังกล่าวทันทีโดยไม่แจ้งให้ทราบล่วงหน้า เพื่อความปลอดภัยของระบบเครือข่ายภายในและภายนอกของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

6.1 อุปกรณ์ดังกล่าวอาจเป็นซอฟต์แวร์หรือฮาร์ดแวร์ที่ไม่มีลิขสิทธิ์หรือผิดกฎหมาย

6.2 อุปกรณ์ต้องสงสัยว่าเป็นต้นทางการโจมตี (source of attack)

6.3 อุปกรณ์อาจเป็นเป้าหมายถูกโจมตี (target of attack) และก่อให้เกิดความเสี่ยงต่อระบบเครือข่าย

6.4 ตรวจพบทราฟฟิกผิดปกติ พฤติกรรมที่เข้าข่ายเป็นการโจมตี หรือกิจกรรมที่เสี่ยงต่อความมั่นคงปลอดภัยของระบบ

การดำเนินการดังกล่าวเป็นไปเพื่อป้องกันความเสียหายต่อระบบเครือข่ายของมหาวิทยาลัยและการให้บริการอินเทอร์เน็ตโดยรวม

ข้าพเจ้าขอสมัครเป็นผู้ใช้งานระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี และขอรับรองว่าจะปฏิบัติตามระเบียบ แนวปฏิบัติ และข้อบังคับการใช้บริการเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ทั้งที่มีอยู่แล้วและที่จะมีประกาศเพิ่มเติมในอนาคตโดยเคร่งครัดทุกประการ

ข้าพเจ้ายินยอมรับผิดชอบต่อการใช้งานระบบเครือข่ายของตนเอง และยอมรับผิดตามกฎหมายหากพบว่าการใช้งานของข้าพเจ้าเป็นการฝ่าฝืนระเบียบ หรือส่งผลกระทบต่อระบบเครือข่ายของมหาวิทยาลัยหรือหน่วยงานภายนอก

ส่วนที่ 3: หลักฐานการรับทราบ

ลงชื่อ_____ลายเซ็นผู้ขอใช้

(_____)

ลงชื่อ_____ลายเซ็นหัวหน้าหน่วยงาน/ผู้บังคับบัญชา

(_____)

วันที่ _____ เดือน _____ พ.ศ. _____

ขั้นตอนการส่งแบบฟอร์ม:

1. กรอกข้อมูลให้ครบถ้วน
2. สแกน (Scan) แบบฟอร์มที่ลงนามแล้ว
3. ส่งเป็นไฟล์ PDF มาที่ **ccsupport@kmutt.ac.th**
4. ใช้หัวข้ออีเมล: **"แบบฟอร์มขอใช้บริการหมายเลข Public IP Address - [ชื่อหน่วยงาน]"**

หากมีข้อสงสัยสามารถติดต่อสอบถามได้ที่ Call Center สำนักคอมพิวเตอร์ โทร. 9444 หรือ 111