นโยบายการเข้าร่วม eduroam ประเทศไทย

1. เกี่ยวกับเอกสารฉบับนี้
    1) เอกสารฉบับนี้ใช้เพื่อเป็นแนวทางในการใช้งาน และให้บริการการเชื่อมต่อเครือข่าย eduroam เพื่อวัตถุประสงค์ทางการศึกษา
    2) eduroam ย่อมาจาก “educational roaming” เป็นเครื่องหมายที่จดทะเบียนโดย TERENA ที่ก่อกำเนิดจากเครือข่ายการศึกษาและวิจัยของยุโรป (NRENs) เพื่อการใช้งานเครือข่ายที่เรียบง่าย ปลอดภัย และรองรับผู้ใช้งานที่ขยายตัวเพิ่มมากขึ้นได้
    3) นิยาม
        3.1) สำนักงานฯ หมายถึง สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet) สังกัดสำนักงานคณะกรรมการการอุดมศึกษา
        3.2) NRO หรือ National Roaming Operator for Thailand หมายถึง ผู้ดำเนินการหลักของ eduroam ของประเทศไทย โดยผู้รับผิดชอบหลักของโครงการนี้ คือ สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet)
        3.3) IdP หรือ Identity Provider หมายถึง สถาบันต้นสังกัด หรือสถาบันการศึกษาที่เป็นผู้กำหนดและตรวจสอบการยืนยันตัวตนการเข้าใช้งานของคณาจารย์ เจ้าหน้าที่ และนิสิตนักศึกษาของสถาบันของตน
        3.4) SP หรือ Service Provider หมายถึง สถาบันที่ให้บริการการเชื่อมต่อ หรือสถาบันการศึกษาที่ให้บริการเครือข่ายแก่ผู้มาเยือนให้เชื่อมต่อเข้าเครือข่าย eduroam ได้ โดยจะอนุญาตการเข้าใช้งานเมื่อสถาบันต้นสังกัดของผู้ใช้ที่มาเยือน ตอบยืนยันตัวตน

2. บทบาทและความรับผิดชอบ
    1) สำนักงานฯ เป็นผู้รับผิดชอบโครงการนี้ โดยทำหน้าที่เป็นผู้ดำเนินการหลักของประเทศไทย (National Roaming Operator for Thailand) เรียกโดยย่อว่า NRO
    2) สถาบันการศึกษาที่เข้าร่วมโครงการ ทำหน้าที่เป็นผู้ตรวจสอบสิทธิการใช้งาน เรียกว่า สถาบันต้นสังกัด (Identity Provider) เรียกโดยย่อว่า IdP
    3) สถาบันการศึกษาที่เข้าร่วมโครงการ ทำหน้าที่ให้บริการเครือข่าย เพื่อให้ผู้มาเยือนเชื่อมต่อเข้าเครือข่ายได้ เรียกว่าสถาบันที่ให้บริการการเชื่อมต่อ (Service Provider) เรียกโดยย่อว่า SP
    4) สถาบันการศึกษาที่เข้าร่วมโครงการจะต้องรับหน้าที่ทั้ง IdP และ SP

3. ผู้ดำเนินการหลักของประเทศไทย (NRO)
    1) สำนักงานฯ เป็นผู้รับผิดชอบการให้บริการ eduroam สำหรับประเทศไทย โดยทำหน้าที่เป็นผู้กำหนดนโยบายการใช้งานระดับประเทศ
    2) บทบาทหลักของ สำนักงานฯ คือ
        (1) ประสานงาน ช่วยเหลือ และสนับสนุนการให้บริการ eduroam โดยกำหนดให้มีรายชื่อผู้ประสานงานอย่างชัดเจน
        (2) รักษาสภาพการเชื่อมต่อกับ eduroam ทั้งในประเทศและต่างประเทศ
        (3) จัดเตรียมหน้าเว็บเพจ eduroam เพื่อให้ข้อมูลที่เกี่ยวข้อง

4. สถาบันต้นสังกัด (IdP)
    1) ทำหน้าที่เป็นผู้กำหนดและตรวจสอบการยืนยันตัวตนการเข้าใช้งานแก่คณาจารย์ เจ้าหน้าที่ และนิสิตนักศึกษาของสถาบันต้นสังกัด
    2) ทำหน้าที่เป็นผู้ให้คำแนะนำ ให้ความรู้ และความช่วยเหลือแก่ผู้ใช้งานของสถาบัน เมื่อเข้าใช้งานที่สถาบันที่ให้บริการการเชื่อมต่อในที่ต่างๆ และแจ้งให้ผู้ใช้งานทราบว่าการใช้งานเครือข่ายอาจจะมีการเก็บบันทึกข้อมูลการจราจร
    3) ทำหน้าที่บันทึกข้อมูลการตรวจสอบการยืนยันตัวตนและการอนุมัติการเข้าใช้งาน และให้ข้อมูลที่จำเป็นแก่ NRO เพื่อแก้ปัญหา
    4) จัดเตรียมบัญชีผู้ใช้งานทดสอบ (test account) เพื่อให้ NRO ใช้ในการทดสอบเท่านั้น และไม่สามารถนำบัญชีนี้ไปใช้งานเครือข่ายตามปกติได้
    5) เป็นผู้รับภาระดำเนินการต่อพฤติกรรมการใช้งานที่ผิดประเภทหรือขัดต่อกฎหมายของผู้ใช้งานในสังกัด
    6) ต้องมีการกำหนดเจ้าหน้าที่เพื่อทำหน้าที่แก้ไขปัญหาให้กับผู้ใช้งานและเป็นผู้ประสานงานกับทาง NRO อย่างชัดเจน
    7) ทำหน้าที่ประสานงานกับทาง NRO เพื่อแก้ปัญหาเรื่องความปลอดภัย และตอบสนองต่อการร้องขอของ NRO ในช่วงเวลาที่เหมาะสม

5. สถาบันที่ให้บริการการเชื่อมต่อ (SP)
    1) เป็นผู้ให้บริการการเชื่อมต่อ โดยจะอนุญาตการเข้าใช้งานเมื่อสถาบันต้นสังกัดของผู้ใช้ที่มาเยือน (IdP) ตอบยืนยันตัวตน
    2) แจ้งให้ผู้ใช้งานที่มาเยือนทราบถึงลักษณะการบันทึกข้อมูลการใช้งานเครือข่ายอย่างชัดเจน

3) ทำหน้าที่ให้บริการผ่านเครือข่ายไร้สายตามมาตรฐาน IEEE 802.11 g หรือดีกว่า โดยประกาศชื่อ SSID เป็น “eduroam” (ตัวพิมพ์เล็กทั้งหมด) โดย SP จะต้องไม่ใช้การล็อกอินผ่านเว็บ (Web Login) กับผู้ใช้งานที่มาเยือน
4) ทำหน้าที่ตั้งค่าระบบความปลอดภัยคือ การยืนยันตัวตนแบบ IEEE 802.1X (EAP) หรือดีกว่า โดยไม่รวมถึง EAP-MD5 และมีการใช้งาน WPA/TKIP หรือดีกว่า (แนะนำให้ใช้ WPA2)
5) อนุญาตให้ผู้ใช้งานที่มาเยือนสามารถใช้โปรโตคอล VPN, OpenVPN, http, https, pop, pop3s, imap, imaps และ ssh เป็นอย่างน้อย
6) ควรกำหนดให้ eduroam ใช้งานผ่าน VLAN ที่แยกออกจากการใช้งานเครือข่ายอื่น
7) ควรกำหนดให้ eduroam จ่าย IP จริง (Public IP address) โดยเป็น IPv4 หรือ IPv6
8) ต้องไม่เก็บค่าบริการใช้งาน eduroam

6. ผู้ใช้งานที่มาเยือน (User)
    1) ต้องปฏิบัติตามนโยบายการใช้งานทั้งของสถาบันต้นสังกัด (IdP) และสถาบันที่ให้บริการการเชื่อมต่อ (SP) รวมถึงปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550
    2) เป็นผู้รับชอบในการเชื่อมต่อกับ eduroam ซึ่งเป็นตัวจริง (genuine) ของแต่ละ SP ตามคำแนะนำของ IdP ก่อนที่จะกรอกชื่อบัญชีและรหัสผู้ใช้เพื่อเข้าใช้งาน
    3) ต้องเป็นผู้รับผิดชอบต่อบัญชีและรหัสผ่านของตนเอง ถ้าสงสัยว่าบัญชีที่ใช้งานไม่ปลอดภัย ต้องรีบติดต่อกลับไปยัง IdP ทันที
    4) เป็นผู้ที่แจ้งเหตุผิดปกติของ eduroam ต่อ IdP และ SP (ถ้าเป็นไปได้)

7. การบันทึกข้อมูล (Logging)
    1) IdP และ SP ต้องบันทึกทั้งการยืนยันตัวตนและการร้องขอ (authentication and accounting requests) อย่างน้อยดังนี้
        (1) วัน เวลา ที่ได้รับการร้องขอ
        (2) อัตตลักษณ์ของผู้ร้องขอ (RADIUS request’s identifier)
        (3) ผลการร้องขอการยืนยันตัวตน พร้อมเหตุผลหากถูกปฏิเสธ
        (4) ค่าสถานะ accounting
    2) SP ต้องบันทึกการเชื่อมต่อ DHCP ดังต่อไปนี้
        (1) วัน เวลา ที่อนุญาตรวมถึงระยะเวลาที่อนุญาต
        (2) MAC address ของผู้ใช้ที่มาเยือน
        (3) IP address ของผู้ใช้ที่มาเยือน

(4) ระยะเวลาการเก็บบันทึกข้อมูลของ DHCP อย่างน้อย 3 เดือน หรือตามกฎหมายกำหนด

8. การให้ความช่วยเหลือ
    1) IdP ควรจัดเตรียมการช่วยเหลือแก่ผู้ใช้งานของตนในการเข้าใช้งานที่สถาบัน SP ต่างๆ
    2) SP ควรจัดเตรียมความช่วยเหลือแก่ผู้ใช้งานที่มาเยือน
    3) SP ควรจัดเตรียมข้อมูลพื้นฐานเกี่ยวกับการใช้งาน eduroam บนหน้าเวพเพจของทางสถาบันให้ชัดเจนซึ่งประกอบด้วยข้อมูลดังนี้
        (1) ข้อความที่ยืนยันถึงเอกสารฉบับนี้ที่ประกาศใช้อย่างชัดเจนที่เว็บเพจของ NRO หน้าที่เกี่ยวกับ eduroam
        (2) มี URL เชื่อมไปยังหน้านโยบายการใช้งานของ SP
        (3) รายการ หรือแผนที่ ที่กำหนดตำแหน่งที่ให้บริการ eduroam
        (4) รายละเอียดที่มีการประกาศ SSID “eduroam” แบบ broadcast หรือ ไม่ broadcast
        (5) รายละเอียดขั้นตอนการยืนยันตัวตน และบริการที่มีให้
        (6) รายละเอียดเกี่ยวกับการใช้งาน non-transparent application proxy รวมถึงการตั้งค่า (ถ้ามี)
        (7) มี URL เชื่อม ไปยังหน้าเวพของ NRO พร้อมทั้ง logo และ trademark ของ eduroam
        (8) มีรายละเอียดแจ้งให้ชัดเจนถึงนโยบาย ลักษณะการจัดเก็บข้อมูลการใช้งาน สิ่งที่เก็บ และระยะเวลาที่เก็บ

9. การติดต่อสื่อสารระหว่างสถาบัน
    1) สถาบันที่เข้าร่วม eduroam ต้องเตรียมรายชื่อผู้ประสานงานและแก้ปัญหาร่วมกันกับทาง NRO โดยมีผู้ประสานงานหลัก 1 คน และผู้ประสานงานรองอีก 1 คน พร้อมรายละเอียดการติดต่อ และต้องแจ้งกับทาง NRO ถ้ามีการเปลี่ยนแปลงรายชื่อตามเวลาที่เหมาะสม
    2) สถาบันที่เข้าร่วม eduroam ต้องแจ้งมายัง NRO เมื่อพบเหตุทางด้านความปลอดภัย การใช้งานผิดประเภท การขัดข้องของการใช้งาน และการเปลี่ยนแปลงนโยบายการเข้าใช้งาน

10. การบังคับใช้ และการระงับการใช้งาน
    1) สิทธิในการบังคับใช้งานและการเปลี่ยนแปลงของเอกสารฉบับนี้เป็นของ NRO
    2) การเปลี่ยนแปลงใดๆ ของเอกสารฉบับนี้จะเป็นไปตามความเห็นชอบของหน่วยงานที่เข้าร่วมและ NRO

3) สถาบันที่เชื่อมต่อเข้ากับ eduroam ของประเทศไทย ถือว่ายอมรับในนโยบายการใช้งานที่กำหนดขึ้นโดยเอกสารฉบับนี้
4) ในกรณีที่เกิดความจำเป็น NRO มีสิทธิในการหยุดให้บริการ eduroam หรือให้บริการแบบมีข้อจำกัด ทั้งนี้ NRO จะต้องแจ้งถึงเหตุและความจำเป็นดังกล่าวแก่สถาบันที่เข้าร่วมรับทราบ
5) NRO จะติดต่อหรือส่ง email เหตุต่างๆ ไปยังผู้ประสานงาน โดยอาจต้องการความร่วมมือในการแก้ปัญหาจากสถาบันที่เข้าร่วม ถ้าไม่มีการติดกลับหรือการให้ความร่วมมือ ทาง NRO ขอสงวนสิทธิในการปิดการเชื่อมต่อ eduroam ของสถาบันนั้นๆ
6) SP สามารถตั้งค่าเครือข่ายของตน เพื่อไม่ให้บริการแก่ผู้ใช้บางคน หรือทุกคนจากบางสถาบันได้
7) IdP อาจถอนหรือไม่อนุญาตให้ผู้ใช้บางคนของตน เข้าใช้งาน eduroam ได้โดยการถอนบัญชีผู้ใช้จากฐานข้อมูลที่ใช้ในการยืนยันตัวตน
8) IdP ต้องให้ความมั่นใจว่า ผู้ใช้งานของตนที่ทำผิดจะได้รับบทลงโทษตามนโยบายของสถาบันต้นสังกัด โดยไม่ขึ้นกับเวลาและพื้นที่ที่ประกอบความผิด