แบบความรู้และแนวปฏิบัติที่ดี

การใช้งาน VPN RUTS เพื่อการเข้าถึงข้อมูลภายในมหาวิทยาลัยฯ
จากการใช้งานอินเทอร์เน็ตภายนอกเครือข่ายมหาวิทยาลัยฯ

VPN RUTS หรือ เครือข่ายส่วนตัวเสมือน ใช้เทคนิคการทำ tunneling วิ่งบนเครือข่ายอินเทอร์เน็ต ทำให้ไม่ว่าจะอยู่ที่ไหน ก็เสมือนว่ายังใช้งานระบบเครือข่ายของมหาวิทยาลัยฯ หลังจากเชื่อมต่อ VPN RUTS แล้ว ข้อมูลจราจรทั้งหมดจะวิ่งมายัง tunneling ระบบเครือข่ายภายในมหาวิทยาลัยฯ ก่อนออกสู่อินเทอร์เน็ต VPN RUTS แบบ L2TP IPsec เสมือนว่าผู้ใช้เข้ามาใช้งานภายในระบบเครือข่ายของมหาวิทยาลัยฯ จึงทำให้เข้าถึงทรัพยากรต่าง ๆ ที่ถูกจำกัดให้ใช้งานได้เฉพาะภายในมหาวิทยาลัยเท่านั้น เช่น E-Database ฐานข้อมูลอิเล็กทรอนิกส์ อื่น ๆ VPN RUTS สามารถใช้ได้หลายระบบปฏิบัติการได้แก่ Windows 10 , Windows 7 Android , IOS IPhone และ Mac OSX

การใช้งาน VPN RUTS อาจจะมีความเร็วต่ำกว่าการใช้งานอินเทอร์เน็ตโดยตรง ควรเชื่อมต่อ VPN RUTS เมื่อต้องการใช้ทรัพยากรภายในของมหาวิทยาลัยฯ เท่านั้น ไม่ควรใช้ VPN RUTS ในการใช้งานอินเทอร์เน็ตปกติ และให้ตัดการเชื่อมต่อ VPN RUTS ทุกครั้งเมื่อไม่ต้องการใช้งานทรัพยากรภายในมหาวิทยาลัยฯ

ข้อกำหนดและแนวปฏิบัติที่ดีในการใช้งาน VPN RUTS

1. การเข้าใช้งานระบบเครือข่ายส่วนตัวเสมือน VPN RUTS เพื่อค้นคว้าฐานข้อมูลงานวิจัย ฐานข้อมูลต่าง ๆ สงวนสิทธิ์สำหรับนักศึกษาและบุคลากรของมหาวิทยาลัยฯ ที่มีบัญชีผู้ใช้งานอินเทอร์เน็ต (e-Passport) เท่านั้น
2. ทำการตั้งค่าอุปกรณ์เพื่อให้รองรับการใช้งาน VPN RUTS โดยระบบปฏิบัติการที่รองรับการใช้งาน VPN RUTS ได้แก่ Windows 10 , Windows 7 Android , IOS IPhone และ Mac OSX
3. ทำการเปิดใช้งาน VPN RUTS โดยการกรอกรหัสผู้ใช้งานอินเทอร์เน็ต (e-Passport) เมื่อต้องการเข้าถึงข้อมูลภายในมหาวิทยาลัยฯ จากการใช้งานอินเทอร์เน็ตภายนอกเครือข่ายมหาวิทยาลัยฯ
4. การใช้งาน VPN RUTS นั้นจะต้องใช้งานเมื่อต้องการใช้ทรัพยากรภายในของมหาวิทยาลัยฯ เท่านั้น ไม่ควรใช้ VPN RUTS ในการใช้งานอินเทอร์เน็ตปกติ
5. ตัดการเชื่อมต่อ VPN RUTS ทุกครั้งหลังจากใช้งาน