



แนวทางปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๑. ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยกรอกข้อมูลลงใน “แบบขออนุญาตเข้าใช้ระบบสารสนเทศและการสื่อสาร” และต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร
๒. ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน
๓. ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย ลงในแบบฟอร์ม
๔. ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
๕. ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น
๖. ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (default) มาจากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน
๗. ผู้ดูแลระบบควรเปลี่ยนค่าชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย
๘. ผู้ดูแลระบบต้องกำหนดค่า WEB (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ Access Point เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น
๙. ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิ์ในการใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ชื่อผู้ใช้ และรหัสผ่านตามที่กำหนดไว้เท่านั้น ให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง
๑๐. ผู้ดูแลระบบควรจะมีการติดตั้งไฟร์วอลล์ (Fire wall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร
๑๑. ผู้ดูแลระบบควรกำหนดให้ผู้ใช้งานระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี
๑๒. ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย