แนวทางปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ และระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมที่ดิน

การควบคุมการเข้าถึงระบบเครือข่ายสื่อสาร

เป็นการควบคุมบุคคลที่เข้าสู่ระบบเครือข่ายสื่อสารของกรมที่ดิน เพื่อความปลอดภัยของข้อมูลและทรัพยากรของกรมที่ดิน จึงต้องมีการกำหนดมาตรการรักษาความปลอดภัย

๑. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่าย จะต้องขอใช้งานกับผู้ดูแลระบบ โดยกรอกข้อมูลลงใน “แบบฟอร์มคำขออนุญาตเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร” และต้องได้รับพิจารณาอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษร

๒. ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายสื่อสารให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๓. ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายสื่อสารลงในแบบฟอร์ม

๔. มีการจัดทำผังการเชื่อมโยงเครือข่าย และมีการปรับปรุงให้เป็นปัจจุบันเสมอ

๕. การจัดการเครือข่าย

๕.๑ มีการแบ่งแยกเครือข่ายเป็นเครือข่ายภายใน เครือข่ายภายนอก และเครือข่ายไร้สาย

๕.๒ มีการจัดแบ่งแยกส่วนเครือข่าย/กลุ่ม เพื่อป้องกันและควบคุมการเข้าถึง ได้แก่ ส่วนที่เป็นสาธารณะ ส่วนที่เชื่อมต่อภายใน ส่วนที่เกี่ยวข้องกับสินทรัพย์สำคัญหรือที่เป็นอันตราย กลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๕.๓ มีการใช้ VLAN ในแต่ละส่วนเครือข่าย/กลุ่ม เช่นกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๕.๔ มีการติดตั้งอุปกรณ์ Gateway กั้นไว้ระหว่างเครือข่ายเพื่อเป็นตัวควบคุมข้อมูลที่สื่อสารกันระหว่างเครือข่าย

๕.๕ อุปกรณ์ในเครือข่ายมีการปรับแต่งให้สามารถควบคุมหรือกรองข้อมูลที่สื่อสารกันระหว่างเครือข่าย

๖. มีการควบคุมและป้องกันให้ปลอดภัย เช่น การใช้การตรวจสอบตัวตน การเข้ารหัสผ่าน การเลือกกำหนดความถี่ช่องสัญญาณเอง เป็นต้น

๗. มีการจัดเก็บข้อมูลจารจรทางเครือข่ายตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๘. มีการตรวจสอบการทำงานของระบบเครือข่ายและอุปกรณ์เครือข่าย อย่างสม่ำเสมอ

๙. มีการตั้งค่าและการปรับแต่งค่า (Configuration) ที่ถูกต้องเหมาะสมและเป็นปัจจุบัน

๑๐. มีการเฝ้าระวังระบบเครือข่าย

๑๑. มีการสำรองข้อมูลการตั้งค่าของอุปกรณ์เครือข่าย

๑๒. มีการ Update patch หรือ release ของซอฟต์แวร์ระบบหรือ firmware

๑๓. มีการตรวจสอบช่องโหว่ของอุปกรณ์และเครื่องแม่ข่ายที่ให้บริการในระบบเครือข่ายของกรมที่ดิน

๑๔. มีการทดสอบการบุกรุกเครือข่าย

การควบคุมการเข้าถึงระบบเครือข่ายสื่อสารจากภายใน

๑. การควบคุมการเชื่อมต่อทางเครือข่าย

๑.๑ การขอติดตั้งจุดเพื่อเชื่อมต่อเข้าเครือข่ายของศูนย์สารสนเทศที่ดิน ต้องทำเป็นหนังสือและได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ได้รับมอบหมาย

๑.๒ ดูแลและปรับปรุงสิทธิการเข้าถึงและใช้งานเครือข่ายของผู้ใช้งานอยู่เสมอ

๑.๓ มีอุปกรณ์ในการกรองการรับส่งข้อมูล เช่น อีเมล์ การรับส่งแฟ้มข้อมูล การเข้าถึงแบบโต้ตอบหรือการแช็ท การเข้าถึงโปรแกรมประยุกต์

๑.๔ จำกัดช่วงวันหรือช่วงเวลาในการอนุญาตให้เชื่อมต่อตามความจำเป็น

๑.๕ จำกัดระยะเวลาการใช้งานเครือข่ายที่เชื่อมต่อ เช่น ตัดการเชื่อมต่อเมื่อใช้งานได้ระยะหนึ่งซึ่งได้กำหนดไว้ล่วงหน้า จำกัดการเชื่อมต่อเครือข่ายให้เป็นเฉพาะภายในระยะเวลาทำการ ให้ตรวจสอบยืนยันตัวตนใหม่ทุกช่วงเวลาที่กำหนด

๑.๖ กำหนดการหมดเวลาการใช้งานระบบเทคโนโลยีสารสนเทศ โดยมีกลไกในการยกเลิกเมื่อไม่ได้ใช้งานตามระยะเวลาที่กำหนด

๒. การควบคุมการกำหนดเส้นทางบนเครือข่าย

๒.๑ มีการควบคุมการกำหนดเส้นทางบนเครือข่ายบนอุปกรณ์เครือข่าย ได้แก่ Firewall, Core switch, Edge Switch, Router เป็นต้น

๒.๒ มีอุปกรณ์ Gateway ในการตรวจสอบต้นทางและปลายทาง ณ จุดควบคุมที่อยู่ระหว่างเครือข่ายภายใน โดยการใช้ Proxy หรือ NAT

๒.๓ มีการกำหนดโปรโตคอล สิทธิ IP Address ในการเชื่อมโยงเครือข่ายของอุปกรณ์และผู้ใช้งานเครือข่ายให้เหมาะสม

๒.๔ มีการกำหนดโปรโตคอล และพอร์ตการใช้งานของแต่ละกลุ่มผู้ใช้ เช่น HTTP, FTP, SMTP, TELNET

๒.๕ มีการกำหนด VLAN เพื่อควบคุมและกำหนดสิทธิการใช้งาน

๓. การระบุและพิสูจน์ตัวตนของผู้ใช้งาน

๓.๑ มีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน โดยต้องแสดงตัวตนด้วยชื่อผู้ใช้ พิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน ในการเข้าสู่เครือข่าย

๓.๒ มีการยืนยันตัวตนอย่างเข้มข้นแทนการใช้รหัสผ่าน เช่นวิธีการใช้ การเข้ารหัสเพื่อรักษาความลับ Smart Card, Token หรือ วิธีการทาง Bio Metric

การควบคุมการเข้าถึงระบบเครือข่ายจากภายนอก

๑. การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐาน ของความจำเป็นเท่านั้นและไม่เปิดพอร์ตและโมเด็มที่ใช้ทิ้งไว้โดยไม่จำเป็น ช่องทางการเข้าสู่ระบบ จากภายนอกมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอเท่าที่จำเป็น

๒. วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๓. ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการปฏิบัติงาน และต้องได้รับอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย

๔. ในการเข้าถึงระบบเครือข่ายจากภายนอก ด้วยเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา อุปกรณ์คอมพิวเตอร์พกพา รวมถึงอุปกรณ์สื่อสารเคลื่อนที่ ต้องมีการควบคุมพอร์ตที่ใช้ในการเข้าสู่ระบบอย่างรัดกุมและมีการแบ่งช่องสัญญาณอย่างชัดเจน

๕. มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก โดยต้องแสดงตัวตนด้วยชื่อผู้ใช้ พิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน และการเข้าสู่ระบบเทคโนโลยีสารสนเทศจากอินเทอร์เน็ตนั้นจะมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานด้วย

๖. มีการใช้อุปกรณ์พิเศษเพื่อยืนยันตัวตนอย่างเข้มข้นในการเข้าระบบแทนการใช้รหัสผ่าน เมื่อต้องปฏิบัติงานภายนอกองค์กร เช่นการใช้อุปกรณ์ Token

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑. ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณ ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๒. ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและทำการสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่

๓. ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ชื่อผู้ใช้งาน และรหัสผ่านที่ถูกกำหนดเป็นค่าตั้งต้นจากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน

๔. ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ (WPA Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่างอุปกรณ์รับ และอุปกรณ์กระจายสัญญาณเพื่อให้ยากต่อการดักจับและปลอดภัย

๕. ผู้ดูแลระบบต้องเลือกใช้วิธีการควบคุม MAC address และชื่อผู้ใช้ รหัสผ่านของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address และชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

๖. ผู้ดูแลระบบต้องมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร

๗. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

๘. ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบการทำงานของเครื่อง/อุปกรณ์ที่เชื่อมต่อในระบบเครือข่ายไร้สาย เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย