

แนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของกรมที่ดิน

เพื่อให้ระบบสารสนเทศและการสื่อสารของกรมที่ดิน มีความมั่นคงปลอดภัยจากภัยคุกคาม และการโจมตีระบบจากผู้ไม่ประสงค์ดี กรมที่ดินเห็นควรให้เจ้าหน้าที่ของส่วนราชการในสังกัด ตระหนักรู้ และให้ความสำคัญในการนำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมที่ดิน ซึ่งได้ประกาศใช้เมื่อวันที่ ๙ มกราคม ๒๕๕๖ ไปใช้ในการปฏิบัติงานและถือปฏิบัติอย่างเคร่งครัด และให้ความร่วมมือในการใช้ระบบสารสนเทศและเครือข่ายสื่อสารของกรมที่ดินภายใต้กฎหมาย เทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อประสิทธิภาพการใช้งานและความมั่นคงปลอดภัยโดยรวม ตามแนวทาง ดำเนินงานในส่วนของผู้ใช้งาน สรุปได้ดังนี้

๑. นำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมที่ดิน ประจำปี งบประมาณ พ.ศ. ๒๕๕๖ ไปใช้ในการปฏิบัติงานและถือปฏิบัติอย่างเคร่งครัด

๒. ติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ของกรมที่ดินที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย ในเครื่องคอมพิวเตอร์ของทางราชการทุกเครื่อง พร้อมปรับปรุงฐานข้อมูลไวรัสคอมพิวเตอร์ล่าสุด และให้สแกน (Scan) ไวรัสคอมพิวเตอร์บนอุปกรณ์พกพาต่าง ๆ เช่น Flash Drive, Thumb Drive, Handy Drive หรือ External Hard disk เป็นต้น ก่อนนำมาพ่วงต่อกับเครื่องคอมพิวเตอร์ และเปิดไฟล์ใช้งาน

๓. ในกรณี ผู้ใช้งานได้รับอนุญาตจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษรให้นำ เครื่องคอมพิวเตอร์ส่วนตัว หรือเครื่องคอมพิวเตอร์ที่รับบริจาคมาใช้ในการปฏิบัติงานราชการ ผู้ใช้งานต้อง ตรวจสอบการติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตฐานข้อมูลไวรัสคอมพิวเตอร์ล่าสุด ก่อนนำเครื่องคอมพิวเตอร์ส่วนตัวหรือเครื่องคอมพิวเตอร์ที่รับบริจาค หรืออุปกรณ์พกพาอื่นใดมาเชื่อมต่อกับเครือข่าย สื่อสารของกรมที่ดิน

๔. สำรวจข้อมูลครุภัณฑ์คอมพิวเตอร์ทุกรายการและกรอกข้อมูลในแบบคำขอขึ้นทะเบียนครุภัณฑ์คอมพิวเตอร์และเครือข่ายสื่อสาร ตามแนวปฏิบัติ ข้อ ๕.๑.๗ การควบคุมการเข้าถึงระบบเครือข่ายสื่อสาร (๔) จัดเก็บไว้ที่สำนักงานที่ดิน และทำการบันทึก/ปรับปรุงรายการครุภัณฑ์ฯ ในระบบสำรวจครุภัณฑ์คอมพิวเตอร์และ รั้ววัด(ที่อยู่เว็บไซต์คือ <http://miscat.dol.go.th/survey>) ซึ่งสำนักเทคโนโลยีสารสนเทศจะเปิดระบบฯ และแจ้งหน่วยงานให้ปรับปรุงข้อมูลประจำปีในลำดับต่อไป



๕. สำรองข้อมูลสำคัญที่ใช้งานอย่างสม่ำเสมอ และหากเป็นไปได้ให้เก็บข้อมูลที่ทำการสำรองไว้ใน อุปกรณ์ที่ไม่มีการเชื่อมต่อกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายอื่น ๆ

๖. ไม่ควรคลิกลิงก์หรือเปิดไฟล์ที่แนบมากับอีเมลที่น่าสงสัย หากไม่มั่นใจว่าเป็นอีเมลที่น่าเชื่อถือ หรือไม่รู้จักผู้ส่งอีเมล ให้ลบอีเมลนั้นทิ้งไป และควรดาวน์โหลดซอฟต์แวร์จากแหล่งที่น่าเชื่อถือเท่านั้น

๗. ติดตามข่าวสารด้านความมั่นคงปลอดภัยระบบสารสนเทศ และ Update แนวความคิดของผู้ไม่ประสงค์ดี ซึ่งในปัจจุบันจะใช้ความรู้ขั้นสูงในการโจมตีและโจรกรรมข้อมูลสำคัญ เพื่อรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร และสามารถดาวน์โหลดไฟล์เอกสารที่เกี่ยวข้องได้จาก เว็บไซต์มาตรการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศกรมที่ดิน ที่อยู่เว็บไซต์ (URL) <http://nam.dol.go.th/dolsecure>

๘. สำหรับผู้ใช้งานที่สงสัยว่าอาจตกเป็นเหยื่อของไวรัสคอมพิวเตอร์ ให้ตัดการเชื่อมต่อระหว่าง เครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อกับระบบเครือข่ายสื่อสารของกรมที่ดินและเครือข่ายอินเทอร์เน็ตในพื้นที่

๙. กรณีเครื่องคอมพิวเตอร์ติดไวรัสฯ สามารถประสานงานขอคำแนะนำ หรือความช่วยเหลือจาก สำนักเทคโนโลยีสารสนเทศ ทางโทรศัพท์หมายเลข ๐ - ๒๕๐๓-๒๑๑๐ - ๙ ต่อ ๔๐๕, ๔๐๖ หรือ ๐ - ๒๕๐๓ - ๓๓๖๙ หรือ ๐ - ๒๙๘๔ - ๐๘๖๐ หรือโทรศัพท์ผ่านระบบอินเทอร์เน็ต (VoIP): ๐๐๐๐๐๑ - ๓ หรือ ๐๐๐๐๑๐ - ๑๑