แจ้งความวิทยาการ

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

เลขที่ ๒ /๖๕

เรื่อง แนวทางการปฏิบัติเพื่อรองรับประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.๒๕๖๓

๑. ความมุ่งหมาย เพื่อให้ นขต.ทอ.ที่มีการจัดเก็บข้อมูลส่วนบุคคลได้มีแนวทางการปฏิบัติในการดำเนินการรักษาความปลอดภัยของข้อมูลฯ ให้เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.๒๕๖๓

๒. ความเป็นมา พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ มีผลบังคับใช้เมื่อ ๑ มิ.ย.๖๕ และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ออกประกาศกระทรวงฯ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.๒๕๖๓ ดังนั้น ทสส.ทอ. จึงได้จัดทำแจ้งความวิทยาการ “แนวทางการปฏิบัติเพื่อรองรับประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.๒๕๖๓” โดยอ้างอิงกับระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓

๓. ผู้ปฏิบัติ นขต.ทอ.ที่มีการจัดเก็บข้อมูลส่วนบุคคลในระบบสารสนเทศ หรือในรูปแบบฐานข้อมูลอิเล็กทรอนิกส์

๔. ปฏิบัติเมื่อ ได้รับแจ้งความวิทยาการฯ ฉบับนี้

๕. การปฏิบัติ นขต.ทอ.ที่มีการจัดเก็บข้อมูลส่วนบุคคล ดำเนินการ ดังนี้

๕.๑ การป้องกันทางกายภาพ (Physical Safeguard) ให้ดำเนินการตาม ผนวก ก

๕.๒ การป้องกันด้านเทคนิค (Technical Safeguard) ให้ดำเนินการตาม ผนวก ข

๕.๓ การป้องกันด้านการบริหารจัดการ (Administrative Safeguard) และการกำหนดมาตรการให้ดำเนินการตาม ผนวก ค

๖. สิ่งที่ส่งมาด้วย ผนวก ก มาตรการป้องกันทางกายภาพ (Physical Safeguard)
ผนวก ข มาตรการป้องกันด้านเทคนิค (Technical Safeguard)
ผนวก ค มาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard)

๗. อื่น ๆ -

พล.อ.ท.
จก.ทสส.ทอ.
๑ ส.ค.๖๕

ผนวก ก

มาตรการป้องกันทางกายภาพ (Physical Safeguard)

วัตถุประสงค์

เพื่อป้องกันไม่ให้มีการเข้าถึงอาคาร สถานที่ ซึ่งเป็นที่ตั้งของระบบสารสนเทศ และพื้นที่ใช้งานระบบสารสนเทศโดยไม่ได้รับอนุญาต ซึ่งจะก่อให้เกิดความเสียหาย การแทรกแซงต่อสารสนเทศ โครงสร้างพื้นฐานและอุปกรณ์ประมวลผลสารสนเทศ

๑. เครื่องคอมพิวเตอร์หรือระบบที่ใช้งาน ต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออกของบุคคลเป็นจำนวนมาก ไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกชัดเจนถึงการมีระบบงานอยู่ภายในสถานที่ดังกล่าว ประตูและหน้าต่างของสำนักงานหรือห้องต้องใส่กุญแจเสมอเมื่อไม่มีคนอยู่

๒. ผู้ปฏิบัติงานต้องตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานเป็นประจำทุกวันหลังเลิกงานเพื่อให้มั่นใจว่า ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปิดล็อคอย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๓. ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลฯ ต้องไม่ถูกทิ้งไว้บนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจโดยไม่มีผู้เฝ้าดูแล

๔. ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลฯ ต้องไม่ถูกทิ้งในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม

๕. เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของหน่วยงานเท่านั้น

๖. ต้องมีการควบคุมการปฏิบัติงานในบริเวณพื้นที่ควบคุม โดยต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” และ “ห้ามถ่ายภาพหรือวิดีโอ” บริเวณภายในพื้นที่ที่มีการจัดเก็บและประมวลผลข้อมูลฯ

๗. อาคารและสถานที่ ซึ่งมีเครื่องคอมพิวเตอร์ที่ใช้สำหรับจัดเก็บและประมวลผลข้อมูลฯ ต้องจัดให้มีเวรยามรักษาการณ์

ผนวก ข

มาตรการป้องกันด้านเทคนิค (Technical Safeguard)

วัตถุประสงค์

เพื่อเป็นการป้องกันไม่ให้มีการใช้ประโยชน์จากช่องโหว่ของซอฟต์แวร์ในระบบสารสนเทศในการโจมตีทางไซเบอร์ และเพื่อกำหนดให้มีการเก็บหลักฐานหรือบันทึกเหตุการณ์ที่เกิดขึ้นกับระบบสารสนเทศและมีความพร้อมรองรับกระบวนการตรวจพิสูจน์หลักฐานดิจิทัลจากหน่วยงานที่เกี่ยวข้อง

๑. การใช้เครือข่ายไร้สายต้องมีการป้องกันทั้งการพิสูจน์ทราบตัวตนผู้ใช้งาน และการเข้ารหัสที่มีความปลอดภัย ตลอดจนต้องมีการขึ้นทะเบียนอุปกรณ์เชื่อมต่อแบบไร้สาย (Wireless Access Point)

๒. จัดให้มีระบบกระแสไฟฟ้าสำรอง เช่น ใช้ Uninterruptible Power Supply (UPS) เป็นต้น และต้องมีการตรวจสอบระบบไฟฟ้าสำรอง อย่างน้อยปีละ ๒ ครั้ง

๓. เครื่องคอมพิวเตอร์ที่ใช้สำหรับจัดเก็บและประมวลผลข้อมูลฯ และเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ต้องได้รับการติดตั้งและเปิดใช้งานซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย และต้องมีการปรับปรุงข้อมูลล่าสุด (Update Malware Definition) อยู่เสมอ

๔. ห้ามใช้คอมพิวเตอร์ที่ใช้สำหรับจัดเก็บและประมวลผลข้อมูลฯ เชื่อมต่ออินเทอร์เน็ตหรือระบบอื่น ๆ ของหน่วยงานภายนอก ทอ.

๕. เครื่องคอมพิวเตอร์แม่ข่ายต้องปิดฟังก์ชันการทำงานเชื่อมต่อกับอินเทอร์เน็ต ยกเว้นในกรณีที่จำเป็นต้องใช้เป็นครั้งคราวเท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมประสงค์ร้าย มีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่าย

๖. หากผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller : DC) มีความจำเป็นต้องอนุญาตให้ผู้ปฏิบัติงานสามารถเข้าถึงระบบงานได้จากเครือข่ายภายนอก ทอ. ต้องมีการยืนยันตัวตนผู้ใช้งานแบบ ๒ วิธีเป็นอย่างน้อยก่อนเข้าสู่ระบบงาน

๗. ต้องมีการบันทึกกิจกรรมการใช้งานระบบจัดเก็บและประมวลผลข้อมูลฯ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ

๘. ข้อมูลเหตุการณ์ของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ ต้องมีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้อง

๙. ต้องมีการป้องกันข้อมูลการบันทึกกิจกรรมหรือเหตุการณ์ ที่เกี่ยวข้องกับการใช้งานสารสนเทศเพื่อป้องกันการเปลี่ยนแปลง หรือการแก้ไขโดยไม่ได้รับอนุญาต

๑๐. ต้องตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่ใช้ในระบบงานให้ตรงกัน (Clock Synchronization) เพื่อความถูกต้องของข้อมูลเหตุการณ์ ในกรณีที่ต้องมีการตรวจสอบ

๑๑. หากมีความ...

๑๑. หากมีความจำเป็นต้องนำอุปกรณ์คอมพิวเตอร์แบบพกพา เช่น คอมพิวเตอร์แบบโน้ตบุ๊ก แท็ปเล็ต Smart Phone และอุปกรณ์สื่อสารเคลื่อนที่อื่น ๆ เป็นต้น มาใช้งานในการจัดเก็บและประมวลผลข้อมูลฯ ต้องมีการลงทะเบียนขออนุญาตใช้งาน

๑๒. ก่อนนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้อง ไปซ่อมบำรุงหรือจำหน่ายขายซาก หรือนำไปใช้ในภารกิจอื่น ๆ ต้องทำลายข้อมูลฯ ไม่ให้สามารถกู้คืนข้อมูลฯ กลับมาใช้ได้อีก

๑๓. ห้ามมีการใช้งานสื่อบันทึกข้อมูลที่ถอดย้ายได้ (Removable Storage Devices) กับเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเก็บและการประมวลผลข้อมูลฯ

๑๔. ต้องมีการ Log in ก่อนใช้งานระบบ และเมื่อมีการพิมพ์รหัสผ่านผิดพลาดเกิน ๓ ครั้ง ให้ปฏิเสธการใช้งาน และให้มีการเปลี่ยนรหัสผ่านในการ Log in ทุก ๆ ๑๘๐ วัน

๑๕. ข้อมูลที่มีการกำหนดชั้นความลับ ให้มีการเข้ารหัสข้อมูลฯ ก่อนการจัดเก็บในระบบงาน

ผนวก ค

มาตรการป้องกันด้านการบริหารจัดการ (Administrative Safeguard)

วัตถุประสงค์

เพื่อเป็นการจำกัดการเข้าถึงข้อมูลฯ และใช้เป็นแนวทางในการดำเนินการที่จะทำให้ข้อมูลฯ มีความปลอดภัยจากการรั่วไหล

๑. กำหนดกลุ่มและจัดทำบัญชีรายชื่อของผู้ใช้งานระบบสารสนเทศ และต้องกำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน และลบ เป็นต้น ตลอดจนต้องกำหนดสิทธิ์เข้าถึงได้เฉพาะข้อมูลที่จำเป็นต่อการใช้งานเท่านั้น และให้ปรับปรุงบัญชีรายชื่อให้ทันสมัยอยู่เสมอ

๒. จัดทำบัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator เป็นต้น โดยต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงาน

๓. เครื่องคอมพิวเตอร์ที่ใช้สำหรับจัดเก็บและประมวลผลข้อมูลฯ ต้องมีการจำกัดและควบคุมการใช้โปรแกรมประยุกต์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยระบบสารสนเทศอย่างใกล้ชิด

๔. กำหนดให้ อาคาร สถานที่ซึ่งเป็นที่ตั้งของระบบสารสนเทศ และพื้นที่ใช้งานระบบสารสนเทศที่ใช้สำหรับจัดเก็บและประมวลผลข้อมูลฯ เป็นพื้นที่หวงห้าม โดยกำหนดให้พื้นที่ที่มีเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเก็บข้อมูลฯ และพื้นที่ที่มีเครื่องคอมพิวเตอร์แม่ข่าย เป็น “เขตหวงห้ามเด็ดขาด” และพื้นที่ที่มีเครื่องคอมพิวเตอร์ที่ใช้ในการประมวลผลข้อมูลฯ เป็น “เขตหวงห้ามเฉพาะ” พร้อมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานสารสนเทศ

๕. พื้นที่ใช้งานระบบสารสนเทศในส่วนที่เป็นหน่วยแสดงผล ต้องปลอดภัยจากการได้ยินและการมองเห็นของผู้ไม่มีอำนาจหน้าที่ที่จะเข้าถึง รวมถึงการบันทึกภาพจากกล้องวงจรปิดโดยให้กำหนดมาตรการควบคุมบุคคลก่อนจะเข้าพื้นที่หวงห้ามอีกชั้นหนึ่ง

๖. กำหนดมาตรการป้องกันเพิ่มเติมให้เหมาะสม เช่น ห้ามนำอุปกรณ์สื่อสาร ถ่ายภาพ หรือสื่อบันทึกข้อมูลที่ถอดย้ายได้ (Removable Storage Device) เข้าไปภายใน “เขตหวงห้ามเด็ดขาด” หรือ “เขตหวงห้ามเฉพาะ” เป็นต้น

๗. ต้องกำหนดบุคคลที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ผ่านเข้า-ออกในแต่ละพื้นที่อย่างชัดเจน

๘. บุคคลจะได้รับสิทธิ์ให้เข้า-ออกสถานที่ได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๙. หากมีข้าราชการ ทอ.ที่ไม่ใช่ผู้มีหน้าที่ปฏิบัติงานหรือผู้ที่มาติดต่อเรื่องข้อมูลฯ หน่วยต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้จะต้องแสดงบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกข้อมูลของบุคคลและการขอเข้า-ออกไว้เป็นหลักฐาน พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย ๑ ปี

๑๐. ผู้ปฏิบัติงาน...

๑๐. ผู้ปฏิบัติงานของหน่วยและบุคคลภายนอกต้องติดบัตรแสดงตนตลอดเวลาขณะอยู่ในพื้นที่ใช้งานสารสนเทศ

๑๑. ผู้ปฏิบัติงานของหน่วยต้องไม่เปิดประตูเข้าพื้นที่ทิ้งไว้ หรือยินยอมให้บุคคลอื่นที่ไม่ได้รับอนุญาตเข้าภายในพื้นที่ควบคุม “เขตหวงห้ามเด็ดขาด” และ/หรือ “เขตหวงห้ามเฉพาะ”

๑๒. ผู้ปฏิบัติงานต้องแจ้งเจ้าหน้าที่รักษาความปลอดภัยทันที เมื่อพบเห็นบุคคลแปลกหน้าหรือบุคคลที่ไม่ติดบัตรเจ้าหน้าที่หรือบัตรผู้มาติดต่อ

๑๓. ผู้ปฏิบัติงานในระบบงานต้องรับผิดชอบ และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ในพื้นที่ใช้งานสารสนเทศ

๑๔. ต้องกำหนดให้มีวิธีการในการตรวจสอบอุปกรณ์ซึ่งมีข้อมูลสำคัญเก็บไว้เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าวก่อนนำอุปกรณ์ไปแจกจ่ายหรือการนำกลับมาใช้งานใหม่

๑๕. ต้องมีการแยกเครื่องมือในการประมวลผลสารสนเทศ การพัฒนาและทดสอบระบบ รวมทั้งควรแยกระบบเครือข่ายของการพัฒนาออกจากระบบที่ใช้งานจริง ทั้งนี้เพื่อป้องกันปัญหาจากการแก้ไขระบบโดยผู้ที่ไม่ได้รับอนุญาตหรือเกิดจากความผิดพลาดในระหว่างการพัฒนาระบบ

๑๖. ห้ามผู้ใช้งานใช้เครื่องคอมพิวเตอร์ที่ใช้สำหรับการจัดเก็บและประมวลผลข้อมูลฯ ทำการดาวน์โหลดแชร์แวร์ หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ต โดยปราศจากการตรวจสอบผ่านศูนย์ไซเบอร์กองทัพอากาศ หลังจากผ่านการตรวจสอบแล้ว ผู้ใช้งานต้องทำการสแกนด้วยซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย ก่อนการใช้งาน

๑๗. หากมีการใช้เครื่องคอมพิวเตอร์ที่ใช้สำหรับการจัดเก็บและประมวลผลข้อมูลฯ ดาวน์โหลดไฟล์แนบของอีเมล สำเนาจากแผ่นดิสก์ หรือไฟล์แชร์ต่าง ๆ ต้องทำการสแกนหาโปรแกรมประสงค์ร้ายก่อนเปิดใช้งาน

๑๘. ห้ามผู้ใช้งานเครื่องคอมพิวเตอร์ที่ใช้สำหรับการจัดเก็บและประมวลผลข้อมูลฯ ขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย

๑๙. ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้น ที่ได้รับอนุญาตให้สามารถรับ-ส่งผ่านเครือข่ายสารสนเทศของหน่วยงาน ทั้งนี้ผู้ใช้งานควรรับไฟล์จากบุคคลที่ตนรู้จัก นอกจากนี้ผู้ใช้งานต้องทำการสแกนโปรแกรมประสงค์ร้ายในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย ก่อนเปิดใช้งานเสมอ

๒๐. ผู้ปฏิบัติงานในระบบการจัดเก็บและการประมวลผลข้อมูลฯ ให้ลงชื่อในใบบันทึกรับรองการรักษาความลับ เมื่อเข้ารับตำแหน่งหรือหน้าที่ (รปภ.๑๗)

๒๑. ผู้ปฏิบัติงานในระบบการจัดเก็บและการประมวลผลข้อมูลฯ ต้องได้รับการอนุญาตจากผู้ควบคุมข้อมูลส่วนบุคคล (DC) ของหน่วยงาน

๒๒. เมื่อผู้ปฏิบัติงานฯ พ้นจากการปฏิบัติหน้าที่ ให้ตัดชื่อออกจากทะเบียนความไว้วางใจของบุคคลพร้อมทั้งจัดทำรายชื่อบุคคลดังกล่าวไว้เป็นหลักฐานเพื่อการตรวจสอบ และให้ลงชื่อในใบรับรองการรักษาความลับเมื่อพ้นตำแหน่งหรือหน้าที่ (รปภ.๑๘)

๒๓. ต้องจัดทำ...

๒๓. ต้องจัดทำบันทึกรายละเอียด การเข้าถึง การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ ของผู้ปฏิบัติงานฯ

๒๔. เก็บรักษาชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้เป็นความลับ

๒๕. ห้ามเปิดจอคอมพิวเตอร์ที่ใช้ในการจัดเก็บและประมวลผลข้อมูลฯ ทิ้งไว้ เมื่อไม่มีผู้นั่งปฏิบัติงานประจำที่นั่ง และให้ควบคุมหน้าจอคอมพิวเตอร์ ไม่ให้มีข้อมูลสำคัญปรากฏขณะไม่ได้ใช้งาน

๒๖. พิจารณาใช้วิธีการกำหนดชั้นความลับให้กับข้อมูลฯ ที่จัดเก็บ