(สำเนา)

บันทึกข้อความ

หน่วยรับ

ส่วนราชการ ทสส.ทอ.(สนผ.โทร.๒-๘๓๔๑)

ที่ กห ๐๖๐๙.๓/๑๒๓๓ **วันที่** ๒๑ ก.ย.๖๖

เรื่อง ขออนุมัติมาตรการรักษาความปลอดภัยข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

เรียน ผบ.ทอ.

๑. ตามระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัย พ.ศ.๒๕๖๕ ข้อ ๑๒ ให้ ทสส.ทอ. มีหน้าที่กำหนดแนวทางและมาตรการรักษาความปลอดภัยข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ พร้อมทั้งอำนวยการ ประสานงาน กำกับดูแล การปฏิบัติตามมาตรการรักษาความปลอดภัยของ ทอ. ให้เป็นไปตามระเบียบ ฯ รวมถึงระเบียบ คำสั่ง ทอ.ที่เกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศ และให้คำแนะนำและข้อเสนอแนะในการปรับปรุงมาตรการรักษาความปลอดภัยข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ของ นขต.ทอ.ให้มีประสิทธิภาพ รัดกุม และทันสมัยอยู่เสมอ นั้น

๒. ทสส.ทอ.ดำเนินการแล้ว ดังนี้

๒.๑ จัดประชุมหารือร่วมกับผู้แทน ขว.ทอ. เพื่อรับทราบแนวทางการจัดทำคู่มือ หรือมาตรการรักษาความปลอดภัยด้านต่าง ๆ รองรับ ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัย พ.ศ.๒๕๖๕ เมื่อ ๑๗ ก.พ.๖๖ โดยมี ผอ.สบค.ทสส.ทอ.เป็นประธาน

๒.๒ จัดทำมาตรการรักษาความปลอดภัยข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ รายละเอียดสรุปได้ ดังนี้

๒.๒.๑ ด้านการบริหารจัดการข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๒.๒.๑.๑ การบริหารจัดการด้านบุคลากร

๒.๒.๑.๒ การบริหารจัดการด้านเครื่องมือหรืออุปกรณ์อิเล็กทรอนิกส์

๒.๒.๑.๓ การบริหารจัดการด้านระบบสารสนเทศและระบบเครือข่าย

๒.๒.๑.๔ การบริหารจัดการด้านกระบวนการและพื้นที่ใช้งานสารสนเทศฯ

๒.๒.๒ ด้านเทคนิคที่เกี่ยวข้องกับข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๒.๒.๒.๑ เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ประเภทอื่น ๆ

๒.๒.๒.๒ ระบบสารสนเทศและระบบเครือข่าย

๒.๒.๒.๓ การปฏิบัติที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์และระบบอิเล็กทรอนิกส์

๒.๒.๓ ด้านกระบวนการที่เกี่ยวข้องกับข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๒.๒.๓.๑ การจัดทำข้อมูลข่าวสารลับในรูปแบบข้อมูลอิเล็กทรอนิกส์

๒.๒.๓.๒ การสำเนาแฟ้มข้อมูลข่าวสารลับด้วยกระบวนการทางอิเล็กทรอนิกส์

๒.๒.๓.๓ การส่งข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๒.๒.๓.๔ การรับข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๒.๒.๓.๕ การเก็บรักษาข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๒.๒.๓.๖ การทำลายข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๒.๒.๓.๗ การปฏิบัติ...

๒.๒.๓.๗ การปฏิบัติในการใช้ระบบไปรษณีย์อิเล็กทรอนิกส์ ทอ. ในการรับ-ส่งข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๒.๒.๓.๘ การปฏิบัติในส่วนอื่น ๆ ที่เกี่ยวข้องกับข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๓. ทสส.ทอ.พิจารณาแล้ว เพื่อให้การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ เป็นไปด้วยความเรียบร้อย สอดคล้องกับระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัย พ.ศ.๒๕๖๕ จึงเห็นสมควรอนุมัติมาตรการรักษาความปลอดภัยข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ (ตามแนบ) และให้ดำเนินการดังนี้

๓.๑ ทสส.ทอ.กำกับดูแลการปฏิบัติเกี่ยวกับการรักษาความปลอดภัยข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ ให้เป็นไปตามระเบียบ คำสั่ง ที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศและปรับปรุงแก้ไขมาตรการฯ ให้มีความทันสมัยอย่างต่อเนื่อง

๓.๒ นขต.ทอ.ดำเนินการเกี่ยวกับการรักษาความปลอดภัยข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ ตามมาตรการฯ อย่างเคร่งครัด

จึงเรียนมาเพื่อพิจารณาอนุมัติตามข้อ ๓

(ลงชื่อ) พล.อ.ท.วิเชียร เรืองพระยา
จก.ทสส.ทอ.

อนุมัติตามข้อ ๓

(ลงชื่อ) พล.อ.อ.พันธ์ภักดี พัฒนกุล
ผบ.ทอ.
๑๒ ต.ค.๖๖

การแจกจ่าย
- นขต.ทอ.

สำเนาถูกต้อง
น.อ.
(นราธิป พุทธสีมา)
ผอ.กนผ.สนผ.ทสส.ทอ.
๑๓ ต.ค.๖๖

ร.ต.เกรียงไกร ฯ พิมพ์/ทาน
น.อ. ตรวจ

มาตรการรักษาความปลอดภัยข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

เพื่อให้การดำเนินการที่เกี่ยวข้องกับข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ สามารถนำไปใช้ประโยชน์ หรือนำเข้าสู่ระบบสารสนเทศ ทอ. และส่งผ่านระบบไปรษณีย์อิเล็กทรอนิกส์ ทอ.ได้อย่างถูกต้อง เหมาะสม และปลอดภัย ไม่ก่อให้เกิดการรั่วไหลของข้อมูล จึงให้ นขต.ทอ.ดำเนินการ ดังนี้

๑. ด้านการบริหารจัดการข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๑.๑ การบริหารจัดการด้านบุคลากร

๑.๑.๑ กำหนดกลุ่มและจัดทำบัญชีรายชื่อของผู้ใช้งานระบบสารสนเทศที่เกี่ยวข้องและต้องกำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน และลบ เป็นต้น ตลอดจนต้องกำหนดสิทธิ์เข้าถึงได้เฉพาะข้อมูลที่จำเป็นต่อการใช้งานเท่านั้น และให้ปรับปรุงบัญชีรายชื่อให้ทันสมัยอยู่เสมอ

๑.๑.๒ จัดทำบัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator โดยต้องได้รับการพิจารณามอบหมายให้ผู้ใช้งานตามความจำเป็น และมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงาน

๑.๑.๓ ต้องจัดทำบันทึกรายละเอียดการเข้าถึง การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ ของผู้ปฏิบัติงาน

๑.๑.๔ ต้องเก็บรักษาชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้เป็นความลับ

๑.๑.๕ ต้องกำหนดบุคคลที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้า-ออกในแต่ละพื้นที่ที่ใช้งานระบบสารสนเทศอย่างชัดเจน

๑.๑.๖ บุคคลจะได้รับสิทธิ์ให้เข้า-ออกสถานที่ได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๑.๑.๗ หากมีข้าราชการ ทอ.ที่ไม่ใช่ผู้มีหน้าที่ปฏิบัติงาน หรือผู้ที่มาติดต่อเรื่องข้อมูลฯ หน่วยต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาตให้บุคคลเข้าพื้นที่ใช้งานระบบสารสนเทศเป็นการชั่วคราว ทั้งนี้จะต้องแสดงบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ทางราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ใช้งานระบบสารสนเทศ ต้องจดบันทึกข้อมูลของบุคคล และการขอเข้า-ออกไว้เป็นหลักฐาน พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย ๑ ปี

๑.๑.๘ ผู้ปฏิบัติงานของหน่วยและบุคคลภายนอกต้องติดบัตรแสดงตนขณะอยู่ในพื้นที่ใช้งานระบบสารสนเทศอยู่ตลอดเวลา

๑.๑.๙ ผู้ปฏิบัติงานของหน่วยต้องไม่เปิดประตูเข้าพื้นที่ทิ้งไว้ หรือยินยอมให้บุคคลอื่นที่ไม่ได้รับอนุญาตติดตามเข้ามาภายในพื้นที่ควบคุม “เขตหวงห้ามเด็ดขาด” และ/หรือ “เขตหวงห้ามเฉพาะ”

๑.๑.๑๐ ผู้ปฏิบัติงานต้องแจ้งเจ้าหน้าที่รักษาความปลอดภัยทันที เมื่อพบเห็นบุคคลแปลกหน้า หรือบุคคลที่ไม่ติดบัตรเจ้าหน้าที่ หรือบัตรผู้มาติดต่อ

๑.๑.๑๑ ผู้ปฏิบัติงานในระบบงานต้องรับผิดชอบ และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ในพื้นที่ใช้งานระบบสารสนเทศ

๑.๑.๑๒ ผู้ปฏิบัติงานในระบบการจัดเก็บและการประมวลผลข้อมูลสารสนเทศให้ลงนามในบันทึกรับรองการรักษาความลับ เมื่อเข้ารับตำแหน่ง หรือหน้าที่ (รปภ.๓)

๑.๑.๑๓ ผู้ปฏิบัติงานในระบบการจัดเก็บและการประมวลผลข้อมูลสารสนเทศต้องได้รับการอนุญาตจากผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ของหน่วยงาน

๑.๑.๑๔ เมื่อผู้...

๑.๑.๑๔ เมื่อผู้ปฏิบัติงานในระบบการจัดเก็บและการประมวลผลข้อมูลสารสนเทศพ้นจากการปฏิบัติหน้าที่ ให้ตัดชื่อออกจากทะเบียนความไว้วางใจของบุคคล พร้อมทั้งจัดทำรายชื่อบุคคลดังกล่าวไว้เป็นหลักฐานเพื่อการตรวจสอบ และให้ลงชื่อในบันทึกรับรองการรักษาความลับเมื่อพ้นตำแหน่งหรือหน้าที่ (รปภ.๖)

๑.๒ การบริหารจัดการด้านเครื่องมือหรืออุปกรณ์อิเล็กทรอนิกส์

๑.๒.๑ เครื่องคอมพิวเตอร์ที่ใช้สำหรับจัดเก็บและประมวลผลข้อมูลสารสนเทศต้องมีการจำกัด และควบคุมการใช้โปรแกรมประยุกต์ที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

๑.๒.๒ กำหนดมาตรการป้องกันเพิ่มเติมให้เหมาะสม เช่น ห้ามนำอุปกรณ์สื่อสาร กล้องถ่ายภาพ หรือสื่อบันทึกข้อมูลที่ถอดย้ายได้ (Removable Storage Device) เข้าไปภายใน “เขตหวงห้ามเด็ดขาด” หรือ “เขตหวงห้ามเฉพาะ” เป็นต้น

๑.๒.๓ ต้องกำหนดให้มีวิธีการในการตรวจสอบอุปกรณ์ซึ่งมีข้อมูลสำคัญเก็บไว้เพื่อป้องกันการรั่วไหล หรือการเปิดเผยข้อมูลดังกล่าวก่อนนำอุปกรณ์ไปแจกจ่าย หรือการนำกลับมาใช้งานใหม่

๑.๒.๔ ต้องมีการแยกเครื่องมือในการประมวลผลข้อมูลสารสนเทศ ในการพัฒนาและทดสอบระบบ รวมทั้งควรแยกระบบเครือข่ายของการพัฒนาออกจากระบบที่ใช้งานจริง ทั้งนี้ เพื่อป้องกันปัญหาจากการแก้ไขระบบโดยผู้ที่ไม่ได้รับอนุญาต หรือเกิดจากความผิดพลาดในระหว่างการพัฒนาระบบ

๑.๒.๕ ห้ามผู้ใช้งานใช้เครื่องคอมพิวเตอร์ที่ใช้สำหรับการจัดเก็บและประมวลผลข้อมูลสารสนเทศ ทำการดาวน์โหลด แชร์แวร์ หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ต ซึ่งปราศจากการตรวจสอบจาก ศชบ.ทอ.และเมื่อผ่านการตรวจสอบแล้ว ให้ผู้ใช้งานทำการสแกนด้วยซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้ายก่อนการใช้งานอีกครั้ง

๑.๒.๖ หากมีการใช้เครื่องคอมพิวเตอร์ที่ใช้สำหรับการจัดเก็บและประมวลผลข้อมูลสารสนเทศ ดาวน์โหลดไฟล์แนบของอีเมล สำเนาจากแผ่นดิสก์ หรือไฟล์แชร์ต่าง ๆ ต้องทำการสแกนหาโปรแกรมประสงค์ร้ายก่อนเปิดใช้งานไฟล์เหล่านั้น

๑.๒.๗ ห้ามผู้ใช้งานเครื่องคอมพิวเตอร์ที่ใช้สำหรับการจัดเก็บและประมวลผลข้อมูลสารสนเทศ ขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย

๑.๒.๘ ห้ามเปิดจอคอมพิวเตอร์ที่ใช้ในการจัดเก็บและประมวลผลข้อมูลสารสนเทศทิ้งไว้ เมื่อไม่มีผู้นั่งปฏิบัติงานประจำที่นั่ง และให้ควบคุมหน้าจอคอมพิวเตอร์ ไม่ให้มีข้อมูลสำคัญปรากฏขณะไม่ได้ใช้งาน

๑.๓ การบริหารจัดการด้านการส่งข้อมูลผ่านระบบสารสนเทศและระบบเครือข่าย

๑.๓.๑ ห้ามผู้ใช้งานส่งไฟล์ที่ไม่เกี่ยวข้องกับการทำงานผ่านระบบสารสนเทศและระบบเครือข่ายของหน่วยงาน

๑.๓.๒ ผู้ใช้งานควรรับไฟล์จากบุคคลที่ตนรู้จักเท่านั้น และต้องทำการสแกนไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้ายก่อนเปิดใช้งานเสมอ

๑.๔ การบริหารจัดการด้านกระบวนการและพื้นที่ใช้งานระบบสารสนเทศ

๑.๔.๑ พิจารณาใช้วิธีการกำหนดชั้นความลับให้กับข้อมูลสารสนเทศ ที่จัดเก็บ

๑.๔.๒ มีการกำหนดให้ อาคาร สถานที่ซึ่งเป็นที่ตั้งของระบบสารสนเทศ และพื้นที่ใช้งานระบบสารสนเทศที่ใช้สำหรับจัดเก็บและประมวลผลข้อมูลสารสนเทศ เป็นพื้นที่หวงห้าม โดยกำหนดให้พื้นที่ที่มี

เครื่องคอมพิวเตอร์ที่ใช้ในการจัดเก็บข้อมูลสารสนเทศ และพื้นที่ที่มีเครื่องคอมพิวเตอร์แม่ข่าย เป็น “เขตหวงห้ามเด็ดขาด” และพื้นที่ที่มีเครื่องคอมพิวเตอร์ที่ใช้ในการประมวลผลข้อมูลสารสนเทศ เป็น “เขตหวงห้ามเฉพาะ” พร้อมทั้งจัดทำแผนผังแสดงตำแหน่งและชนิดของพื้นที่ใช้งานระบบสารสนเทศ

๑.๔.๓ พื้นที่ใช้งานระบบสารสนเทศในส่วนที่เป็นหน่วยแสดงผล ต้องปลอดภัยจากการได้ยิน และการมองเห็นของผู้ไม่มีอำนาจหน้าที่ที่จะเข้าถึง รวมถึงการบันทึกภาพจากกล้องโทรทัศน์วงจรปิด โดยให้กำหนดมาตรการควบคุมบุคคลก่อนจะเข้าพื้นที่หวงห้ามอีกชั้นหนึ่งด้วย

๒. ด้านเทคนิคที่เกี่ยวข้องกับข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๒.๑ เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ประเภทอื่น ๆ

๒.๑.๑ เครื่องคอมพิวเตอร์ที่ใช้สำหรับจัดเก็บและประมวลผลข้อมูลข่าวสารลับฯ ต้องได้รับการติดตั้งซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย โดยต้องเปิดใช้งานซอฟต์แวร์ป้องกันฯ ตลอดเวลาที่ใช้งาน และต้องมีการปรับปรุงข้อมูลล่าสุด (Update Malware Definition) อยู่เสมอ และต้องกำหนดให้มีการลงชื่อเข้าใช้งานเครื่องคอมพิวเตอร์ ควบคู่กับการตั้งเวลาการพักหน้าจอคอมพิวเตอร์

๒.๑.๒ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ต้องได้รับการติดตั้งและเปิดใช้งานซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย และต้องมีการปรับปรุงข้อมูลล่าสุด (Update Malware Definition) อยู่เสมอ

๒.๑.๓ เครื่องคอมพิวเตอร์แม่ข่ายต้องปิดฟังก์ชันการทำงานเชื่อมต่อกับอินเทอร์เน็ต ยกเว้นในกรณีที่จำเป็นต้องใช้เป็นครั้งคราวเท่านั้น เพื่อเป็นการป้องกันและลดโอกาสไม่ให้โปรแกรมประสงค์ร้าย มีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่าย

๒.๑.๔ ต้องตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ที่ใช้ในระบบงานให้ตรงกัน (Clock Synchronization) เพื่อความถูกต้องของข้อมูลเหตุการณ์ในกรณีที่ต้องมีการตรวจสอบ

๒.๑.๕ หากมีความจำเป็นต้องนำอุปกรณ์คอมพิวเตอร์แบบพกพา เช่น เครื่องคอมพิวเตอร์โน้ตบุ๊ก คอมพิวเตอร์แท็บเล็ต สมาร์ทโฟน และอุปกรณ์สื่อสารเคลื่อนที่อื่น ๆ มาใช้งานในการจัดเก็บและประมวลผลข้อมูลข่าวสารลับฯ ต้องมีการลงทะเบียนขออนุญาตใช้งาน

๒.๑.๖ ก่อนนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้อง ไปซ่อมบำรุงหรือจำหน่ายขายซาก หรือนำไปใช้ในภารกิจอื่น ต้องทำลายข้อมูลข่าวสารลับฯ ไม่ให้สามารถกู้คืนข้อมูลข่าวสารลับฯ กลับมาใช้ได้อีก

๒.๑.๗ การใช้งานสื่อบันทึกข้อมูล เช่น ซีดีรอมและอื่น ๆ เป็นต้น ที่เป็นสื่อในลักษณะ ถอดแยก และเคลื่อนย้ายได้ โดยมีการกำหนดชั้นความลับบันทึกไว้ในสื่อดังกล่าว ต้องแสดงชั้นความลับไว้บนสื่อบันทึกข้อมูลนั้น และให้พิทักษ์รักษาตามชั้นความลับนั้น และให้เก็บในกล่อง หรือหีบห่อ ซึ่งมีเครื่องหมายแสดงชั้นความลับนั้น ๆ

๒.๑.๘ หากมีการเข้าถึง เปิด หรือนำข้อมูลข่าวสารลับไปใช้งาน จำเป็นต้องมีการคัดลอกข้อมูลข่าวสารลับฯ ลงบนเครื่องคอมพิวเตอร์ เพื่อทำการถอดรหัสก่อนนำข้อมูลข่าวสารลับฯ ไปใช้งาน หลังการใช้งาน ให้ทำการกำจัดสื่อบันทึกข้อมูลด้วยการทำลายทิ้ง ในกรณีที่เป็นสื่อบันทึกข้อมูลแบบนำกลับมาใช้ซ้ำไม่ได้ หรือทำการลบแล้วล้างข้อมูลทั้งหมดจากสื่อบันทึกข้อมูล ภายใต้สิ่งแวดล้อมที่ได้มีการควบคุมไม่ให้สามารถกู้คืนกลับมาได้ ในกรณีที่เป็นสื่อบันทึกข้อมูลที่สามารถนำกลับมาใช้ซ้ำได้

๒.๑.๙ เมื่อหมดความต้องการในการใช้งานข้อมูลข่าวสารลับดังกล่าวแล้ว ให้ทำการลบข้อมูลดังกล่าวออกจากเครื่องคอมพิวเตอร์ และต้องตรวจสอบว่าข้อมูลดังกล่าวได้ถูกลบออกจากถังขยะในเครื่องคอมพิวเตอร์

๒.๑.๑๐ ห้ามใช้...

๒.๑.๑๐ ห้ามใช้งานเครื่องคอมพิวเตอร์ที่ไม่ปลอดภัย เช่น ไม่มีการกำหนดให้มีการลงชื่อเข้าใช้งานเครื่องคอมพิวเตอร์ และไม่มีการตั้งเวลาการพักหน้าจอคอมพิวเตอร์ ในการเข้าถึง เปิด หรือนำข้อมูลข่าวสารลับไปใช้งาน

๒.๑.๑๑ หากมีความจำเป็นต้องใช้งานข้อมูลข่าวสารลับในการทำงานอย่างไม่ต่อเนื่อง ให้ทำลายข้อมูลข่าวสารลับที่ถูกถอดรหัส ภายใต้สิ่งแวดล้อมที่ได้มีการควบคุมไม่ให้สามารถกู้คืนกลับมาได้ คงเหลือไว้แต่ข้อมูลข่าวสารลับที่ถูกเข้ารหัส เก็บไว้ในเครื่องคอมพิวเตอร์ที่มีความปลอดภัย หรือสื่อบันทึกข้อมูลที่มีเครื่องหมายที่แสดงชั้นความลับนั้น ๆ

๒.๒ ระบบสารสนเทศและระบบเครือข่าย

๒.๒.๑ การใช้เครือข่ายไร้สายต้องมีการป้องกันทั้งการพิสูจน์ทราบตัวตนผู้ใช้งานและการเข้ารหัสที่มีความปลอดภัย (ควรกำหนดมาตรฐานความปลอดภัยด้วย เช่น ไม่น้อยกว่า WPA2 เป็นต้น) ตลอดจน ต้องมีการขึ้นทะเบียนอุปกรณ์เชื่อมต่อแบบไร้สาย (Wireless Access Point)

๒.๒.๒ ต้องมีการป้องกันข้อมูลการบันทึกกิจกรรมหรือเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลง หรือการแก้ไขโดยไม่ได้รับอนุญาต

๒.๒.๓ ต้องมีการลงชื่อเข้าใช้ (Log in) ก่อนใช้งานระบบทุกครั้ง และเมื่อมีการป้อนรหัสผ่านผิดพลาดเกิน ๓ ครั้ง ให้ปฏิเสธการใช้งาน และให้มีการเปลี่ยนรหัสผ่านในการลงชื่อเข้าใช้ (Log in) ทุก ๆ ๑๘๐ วัน

๒.๓ การปฏิบัติที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์และระบบอิเล็กทรอนิกส์

๒.๓.๑ ระบบจัดเก็บและประมวลผลข้อมูลข่าวสารลับที่สามารถใช้ในการแลกเปลี่ยนข้อมูลข่าวสารลับ ได้แก่ ระบบงานสารบรรณอิเล็กทรอนิกส์ (e-admin) และระบบไปรษณีย์อิเล็กทรอนิกส์ ทอ. (RTAF Mail) โดยเครื่องคอมพิวเตอร์ที่จะเข้าถึง เปิด หรือนำข้อมูลข่าวสารลับไปใช้งานผ่านระบบจัดเก็บและประมวลผลข้อมูลข่าวสารลับ จะต้องติดตั้งโปรแกรมเข้ารหัสข้อมูล ทอ. (RTAF Encryption)

๒.๓.๒ ต้องมีการบันทึกกิจกรรมการใช้งานระบบจัดเก็บและประมวลผลข้อมูลข่าวสารลับฯ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอ

๒.๓.๓ ข้อมูลเหตุการณ์ของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ ต้องมีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้อง

๒.๓.๔ ข้อมูลที่มีการกำหนดชั้นความลับ ให้มีการเข้ารหัสข้อมูลข่าวสารลับฯ ก่อนการจัดเก็บในระบบงาน

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

๓. ด้านกระบวนการที่เกี่ยวข้องกับข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๓.๑ การจัดทำข้อมูลข่าวสารลับในรูปแบบข้อมูลอิเล็กทรอนิกส์

๓.๑.๑ การจัดทำข้อมูลข่าวสารลับในรูปแบบข้อมูลอิเล็กทรอนิกส์ตามส่วนนี้ คือ การแปลงสภาพข้อมูลข่าวสารลับจากต้นฉบับให้อยู่ในรูปแบบแฟ้มข้อมูล เพื่อนำไปใช้ประโยชน์ หรือนำเข้าสู่ระบบสารสนเทศของ ทอ. หรือระบบไปรษณีย์อิเล็กทรอนิกส์ ทอ.

๓.๑.๒ การแปลง...

๓.๑.๒ การแปลงสภาพข้อมูลข่าวสารลับให้อยู่ในรูปแบบอิเล็กทรอนิกส์ ก่อนนำเข้าระบบสารสนเทศของ ทอ. ระบบไปรษณีย์อิเล็กทรอนิกส์ ทอ. หรือส่งผ่านสื่อกลางบันทึกข้อมูลต้องดำเนินการเข้ารหัสสารสนเทศตามระเบียบหรือคำสั่งของ ทอ.ที่เกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศ และระเบียบปฏิบัติประจำที่เกี่ยวข้อง

๓.๑.๓ เมื่อแฟ้มข้อมูลข่าวสารลับได้รับการเข้ารหัสแล้ว จะต้องลบ หรือทำลายแฟ้มข้อมูลต้นฉบับที่ไม่ถูกเข้ารหัสเมื่อหมดความจำเป็นทันที

๓.๑.๔ ข้อมูลข่าวสารลับที่เป็นต้นฉบับที่ไม่ได้นำไปใช้งานต่อ จะต้องจัดเก็บไว้ในที่ปลอดภัยตามคำแนะนำของมาตรการนี้

๓.๒ การสำเนาแฟ้มข้อมูลข่าวสารลับด้วยกระบวนการทางอิเล็กทรอนิกส์

๓.๒.๑ นายทะเบียนข้อมูลข่าวสารลับของหน่วยงานสังกัด ทอ. บันทึกการแจกจ่ายสำเนาลงในทะเบียนส่ง และทะเบียนควบคุมข้อมูลข่าวสารลับ โดยระบุคำว่า “อิเล็กทรอนิกส์” ในรายการแจกจ่ายที่เป็นสำเนาในรูปแบบอิเล็กทรอนิกส์

๓.๒.๒ แฟ้มข้อมูลที่สำเนาแจกจ่ายแต่ละชุด ให้มีการบันทึกชื่อหน่วยงานหรือหน่วยงานย่อยที่ได้รับสำเนา วันที่แจกจ่าย ในรูปแบบลายน้ำ ณ บริเวณที่เห็นได้ชัดเจน แต่ไม่ควรทับซ้อนกับการแสดงเครื่องหมายหรือข้อความอื่นของข้อมูลข่าวสารลับต้นฉบับ แล้วแต่กรณี

๓.๓ การส่งข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๓.๓.๑ การส่งข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์เป็นการนำส่งสำเนาข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ ด้วยกระบวนการทางอิเล็กทรอนิกส์ไปให้หน่วยงานไปจนถึงบุคคลผู้ที่เกี่ยวข้องกับข้อมูลข่าวสารลับดังกล่าวทางอิเล็กทรอนิกส์ตามสายการบังคับบัญชา

๓.๓.๒ นายทะเบียนข้อมูลข่าวสารลับส่งข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ผ่านระบบสารบรรณอิเล็กทรอนิกส์ ทอ.เป็นหลัก หรือเลือกวิธีการส่งที่เหมาะสมตามคำแนะนำที่ ทสส.ทอ. กำหนด โดยให้ดำเนินการด้านงานทะเบียน เช่นเดียวกับการรับ-ส่งข้อมูลข่าวสารลับ (ในส่วนที่ ๒ ของระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัย พ.ศ.๒๕๖๕)

๓.๓.๓ บุคคลที่ถือครองข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ สามารถส่งข้อมูลข่าวสารลับให้กับกำลังพล ทอ.ที่มีสิทธิ์เข้าถึงข้อมูลข่าวสารลับนั้น ทั้งนี้ เพื่อใช้ในการปฏิบัติงานเท่านั้น โดยต้องแจ้งต่อนายทะเบียนข้อมูลข่าวสารลับของหน่วยงานต้นสังกัดทราบ และลงชื่อในทะเบียนส่ง และทะเบียนควบคุมข้อมูลข่าวสารลับ

๓.๓.๔ การตอบรับข้อมูลข่าวสารลับด้วยระบบไปรษณีย์อิเล็กทรอนิกส์ ทอ. ให้ปฏิบัติตามข้อ ๓.๗ การปฏิบัติในการใช้ระบบไปรษณีย์อิเล็กทรอนิกส์ ทอ. ในการรับ-ส่งข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๓.๓.๕ นายทะเบียนข้อมูลข่าวสารลับลงทะเบียนส่ง และทะเบียนควบคุมข้อมูลข่าวสารลับ โดยให้ระบุรายละเอียดว่าเป็นข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ และระบุวิธีการส่งไว้ในทะเบียนดังกล่าวด้วย

๓.๔ การรับข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๓.๔.๑ การรับ เป็นขั้นตอนที่หน่วยงานหรือกำลังพล ทอ.ผู้เกี่ยวข้องและมีสิทธิ์เข้าถึงข้อมูลข่าวสารลับ นำข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ไปปฏิบัติงานต่อ

๓.๔.๒ นายทะเบียน...

๓.๔.๒ นายทะเบียนข้อมูลข่าวสารลับของหน่วยงานผู้รับข้อมูลข่าวสารลับผ่านระบบสารบรรณอิเล็กทรอนิกส์ ทอ. ดำเนินการลงทะเบียนรับ และตอบรับข้อมูลข่าวสารลับ เช่นเดียวกับการรับ-ส่งข้อมูลข่าวสารลับตามปกติ

๓.๔.๓ กำลังพล ทอ.ที่เกี่ยวข้องกับข้อมูลข่าวสารลับซึ่งเป็นผู้รับทราบข้อมูลข่าวสารลับจากระบบไปรษณีย์อิเล็กทรอนิกส์ ทอ. ให้ใช้งานกับเครื่องคอมพิวเตอร์ของส่วนงานราชการที่มีความปลอดภัยเท่านั้น

๓.๔.๔ กำลังพล ทอ.ที่เกี่ยวข้องกับข้อมูลข่าวสารลับที่ผ่านการเข้ารหัสด้วยโปรแกรมเข้ารหัส ทอ. ต้องประสานกับนายทะเบียนข้อมูลข่าวสารลับของ นขต.ทอ. เพื่อลงทะเบียนขอรับโปรแกรมเข้ารหัส ทอ.มาติดตั้งยังเครื่องคอมพิวเตอร์ ตามระเบียบปฏิบัติประจำการใช้งานโปรแกรมเข้ารหัส ทอ. ของ นขต.ทอ.

๓.๕ การเก็บรักษาข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๓.๕.๑ การเก็บรักษาข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์บนสื่อกลางบันทึกข้อมูล มีจุดมุ่งหมายเพื่อมิให้เกิดการรั่วไหลของข้อมูลข่าวสารที่มีชั้นความลับ อันอาจส่งผลกระทบต่อความมั่นคง ภาพลักษณ์ และความน่าเชื่อถือของหน่วยงาน หากมีความจำเป็นต้องเก็บรักษาไว้เพื่อใช้ในการปฏิบัติงาน จะต้องอยู่ในรูปแบบที่มีการเข้ารหัสอยู่เสมอ และให้ลบหรือทำลายแฟ้มข้อมูลต้นฉบับและแฟ้มข้อมูลที่ถูกถอดรหัสเมื่อไม่มีความจำเป็นในการใช้งานโดยทันที

๓.๕.๒ นายทะเบียนข้อมูลข่าวสารลับของหน่วยงานในสังกัด ทอ.ที่ได้รับข้อมูลข่าวสารลับที่เป็นแฟ้มข้อมูลจากระบบสารบรรณอิเล็กทรอนิกส์ ทอ. หรือระบบไปรษณีย์อิเล็กทรอนิกส์ ทอ. สามารถบันทึกแฟ้มข้อมูลลงเครื่องคอมพิวเตอร์สำนักงานที่มีความปลอดภัยเพื่อดำเนินการด้านงานสารบรรณ และทำการลบหรือทำลายแฟ้มข้อมูลข่าวสารลับทันที เมื่อปฏิบัติงานเสร็จสิ้น

๓.๕.๓ กำลังพล ทอ.ที่เกี่ยวข้องกับข้อมูลข่าวสารลับ เมื่อได้รับข้อมูลข่าวสารลับในรูปแบบแฟ้มข้อมูล ให้ทำการบันทึกลงในสื่อกลางบันทึกข้อมูลประเภทหน่วยความจำภายนอก แบบถอดแยกและเคลื่อนย้ายได้ โดยสื่อกลางบันทึกข้อมูลดังกล่าวต้องแสดงชั้นความลับไว้บนสื่อกลางบันทึกข้อมูล หรือแสดงชั้นความลับไว้ที่ชื่อของแฟ้มงานที่รวบรวมข้อมูลข่าวสารลับนั้น และให้ทำการเข้ารหัสสื่อกลางบันทึกข้อมูลหรือที่แฟ้มงาน แล้วแต่กรณี

๓.๖ การทำลายข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๓.๖.๑ ข้อมูลข่าวสารลับที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์บนระบบสารบรรณอิเล็กทรอนิกส์ ทอ. ให้สามารถเก็บรักษาอยู่ในระบบสารสนเทศนั้นต่อไป ทั้งนี้ ให้ยึดถือการปฏิบัติตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ.๒๕๒๖ และระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ ๒) พ.ศ.๒๕๔๘

๓.๖.๒ ข้อมูลข่าวสารลับที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์บนระบบไปรษณีย์อิเล็กทรอนิกส์ ทอ. ให้ลบออกจากกล่องจดหมายขาเข้า กล่องจดหมายขาออก และติดตามลบข้อมูลข่าวสารลับที่กล่องจดหมายที่ถูกลบภายใน ๑ ปี นับตั้งแต่วันที่มีการรับ-ส่งข้อมูลข่าวสารลับ

๓.๖.๓ ข้อมูลข่าวสารลับที่อยู่ในรูปแบบแฟ้มข้อมูล ให้ลบหรือทำลายตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ทอ. จนไม่สามารถกู้คืน หรือสามารถนำข้อมูลส่วนใดส่วนหนึ่งมาประกอบกันเป็นข้อมูลที่มีความอ่อนไหวได้

๓.๗ การปฏิบัติ...

๓.๗ การปฏิบัติในการใช้ระบบไปรษณีย์อิเล็กทรอนิกส์ ทอ. ในการรับ-ส่งข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์

๓.๗.๑ ให้ใช้งานกับเครื่องคอมพิวเตอร์ของส่วนงานราชการที่มีความปลอดภัยเท่านั้น

๓.๗.๒ นายทะเบียนข้อมูลข่าวสารลับหรือกำลังพล ทอ.ที่ถือครองข้อมูลข่าวสารลับซึ่งเป็นผู้สร้างไปรษณีย์อิเล็กทรอนิกส์ใหม่เพื่อส่งข้อมูลข่าวสารลับ ต้องตรวจสอบให้มีความสมบูรณ์ถูกต้องของข้อความ โดยมีขั้นตอนการดำเนินการที่สำคัญ ได้แก่ ตรวจสอบรายชื่อผู้รับว่าเป็นผู้มีสิทธิเข้าถึงข้อมูลข่าวสารลับนั้น กำหนดตัวเลือก การแสดงตัวเลือกของข้อความให้เป็น “ลับเฉพาะ” และ “ร้องขอการแจ้งเมื่อผู้รับเปิดอ่าน” ระบุข้อความจำกัดความรับผิดในส่วนท้ายของไปรษณีย์อิเล็กทรอนิกส์ ทอ. ว่า “ไปรษณีย์อิเล็กทรอนิกส์ฉบับนี้เป็นข้อมูลที่เป็นความลับ และอาจเป็นข้อมูลที่เป็นเอกสิทธิ์เฉพาะบุคคล การนำข้อมูลดังกล่าวไปใช้หรือเปิดเผยให้บุคคลอื่นใดล่วงรู้ เป็นการกระทำที่ไม่ได้รับอนุญาต” และกำหนดให้ผู้ส่งลงชื่อในทะเบียนส่ง

๓.๗.๓ เมื่อผู้ส่งได้รับการตอบรับจากผู้รับข้อมูลข่าวสารลับ ให้แจ้งต่อนายทะเบียนข้อมูลข่าวสารลับทราบ เพื่อบันทึกลงในทะเบียนควบคุมข้อมูลข่าวสารลับ

๓.๗.๔ บุคคลผู้ได้รับข้อมูลข่าวสารลับเพื่อนำไปปฏิบัติงาน ทำการตอบรับที่ตัวเลือกการตอบรับที่ปรากฏอยู่ภายในไปรษณีย์อิเล็กทรอนิกส์ฉบับนั้น หรือดำเนินการตอบรับด้วยวิธีการใด ๆ ที่เหมาะสมตามลำดับความเร่งด่วน และวัตถุประสงค์ในการรักษาความลับของทางราชการ

๓.๗.๕ แจ้งนายทะเบียนข้อมูลข่าวสารลับของหน่วยงานต้นสังกัด ลงทะเบียนรับ

๓.๗.๖ ในกรณีตรวจสอบพบไปรษณีย์อิเล็กทรอนิกส์ที่เป็นข้อมูลข่าวสารลับในกล่องจดหมายอื่นที่ไม่ใช่กล่องจดหมายขาเข้า ให้ทำการตรวจสอบว่าข้อมูลข่าวสารลับนั้นมีความถูกต้อง ให้ดำเนินการย้ายไปรษณีย์อิเล็กทรอนิกส์นั้นไปยังกล่องจดหมายขาเข้า แล้วปฏิบัติตามข้อ ๓.๓.๑ ต่อไป

๓.๘ การปฏิบัติในส่วนอื่น ๆ ที่เกี่ยวข้องกับข้อมูลข่าวสารลับในรูปแบบอิเล็กทรอนิกส์ที่ไม่ได้กำหนดไว้เป็นการเฉพาะในมาตรการฯ นี้ ให้ดำเนินการตามระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นที่เกี่ยวข้องของทางราชการได้โดยอนุโลม