บันทึกข้อความ

ส่วนราชการ คณะทำงานเทคโนโลยีสารสนเทศ กองแบบแผน

ที่ สธ ๐๗๐๓.๐๐๗/ ๕ วันที่ ๑ เมษายน ๒๕๖๔

เรื่อง แนวทางการปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

เรียน ผู้อำนวยการกองแบบแผน

ตามที่ งานเทคโนโลยีสารสนเทศ กลุ่มบริหารทั่วไปและแผนงาน กองแบบแผน ได้จัดทำประกาศ เรื่อง แนวทางการปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อเป็นแนวทางในการปฏิบัติให้กับเจ้าหน้าที่กองแบบแผน ด้านความมั่นคงปลอดภัยระบบสารสนเทศ ตามนโยบายกรมสนับสนุนบริการสุขภาพ แล้วนั้น

ในการนี้ งานเทคโนโลยีสารสนเทศ กลุ่มบริหารทั่วไปและแผนงาน กองแบบแผน ขอส่งประกาศ เรื่อง แนวทางการปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณาลงนามต่อไปด้วยจะเป็นพระคุณ

(นายพรกฤษณ์ แทนแก้ว)
ประธานคณะทำงานฯ

(นายถาวร ขาวแสง)
ผู้อำนวยการกองแบบแผน

ประกาศ กองแบบแผนกรมสนับสนุนบริการสุขภาพ
เรื่อง แนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

ตามนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ กำหนดให้ทุกหน่วยงานในสังกัดกรมสนับสนุนบริการสุขภาพ ต้องปฏิบัติตามนโยบายดังกล่าว ดังนั้นเพื่อให้บุคลากรของกองแบบแผน สามารถปฏิบัติตามนโยบายความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ กองแบบแผนจึงจัดทำแนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองแบบแผน กรมสนับสนุนบริการสุขภาพขึ้น เพื่อให้ถือปฏิบัติตามแนวทางการเดียวกัน

แนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองแบบแผน กรมสนับสนุนบริการสุขภาพ ประกอบด้วย ๔ ข้อ ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำ แผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) จัดการประเมินความเสี่ยงด้านสารสนเทศ ปีละ ๑ ครั้ง

(๔) การปฏิบัติตามข้อกฎหมายที่เกี่ยวข้อง

<u>แนวปฏิบัติ</u>

แนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองแบบแผน กรมสนับสนุนบริการสุขภาพ กำหนดไว้ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๑.๑ นโยบายการควบคุมการเข้าถึงสารสนเทศ ให้ผู้บริหารหรือผู้ที่ได้รับมอบหมาย จัดทำนโยบายการควบคุมการเข้าถึงสารสนเทศเป็นลายลักษณ์อักษร พร้อมทั้งประกาศนโยบายและข้อปฏิบัติให้เจ้าหน้าที่ภายในหน่วยงานทราบและถือปฏิบัติ

๑.๒ การลงทะเบียนผู้ใช้งานของระบบสารสนเทศใดของกองแบบแผน อาทิเช่น ระบบ Website ของกองแบบแผน ระบบติดตามประเมินผลแผนงานโครงการของกองแบบแผน (SMART) เป็นต้น ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ปฏิบัติดังนี้ เมื่อมีการเกษียณอายุราชการ ลาออก โอน ย้าย หรือได้รับแจ้งจากหน่วยงานต้นสังกัดให้ดำเนินการปรับปรุงหรือถอดถอนสิทธิภายใน ๓ วันนับจากวันที่ได้รับแจ้ง

๑.๓ การบริหารจัดการสิทธิการใช้งานระบบฐานข้อมูล ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

- กำหนดบัญชีรายชื่อและรายละเอียดการใช้งานสารสนเทศของกองแบบแผน
- กำหนดสิทธิการใช้งานระบบงานตามหน้าที่ความรับผิดชอบของผู้ใช้งานตามความจำเป็น
- จัดให้มีการสร้างบัญชีรายชื่อผู้ใช้งานแยกเป็นรายบุคคล

๑.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย ส่งบัญชีผู้ใช้งานและรหัสผ่าน โดยใส่ซองปิดผนึกและประทับตรา "ลับ" และส่งไปยังผู้ใช้งาน และแนบระเบียบอื่น ๆ ที่เกี่ยวข้องกับการปฏิบัติงานของผู้ใช้งาน รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามเอกสารแนบดังกล่าวโดยเคร่งครัด

๑.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายจัดให้มีการทบทวนบัญชีผู้ใช้งานและสิทธิผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง

๑.๖ การใช้งานรหัสผ่าน (Password Use) ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

- กำหนดรหัสผ่านส่วนบุคคลที่มีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยให้มีทั้งตัวอักษรเล็ก ใหญ่ ผสมตัวเลข
- ควรเก็บรักษารหัสผ่านของตนเองไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น
- กรณีที่จำเป็นต้องให้รหัสผ่านแก่ผู้อื่น หลังจากดำเนินงานเสร็จสิ้นให้ทำการเปลี่ยนรหัสผ่านทันที

๑.๗ นโยบายการใช้งานบริการอินเทอร์เน็ต ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

- ห้ามเข้า Website ที่อยู่ในประเภท การพนัน ลามก อนาจาร สิ่งผิดกฎหมาย ผิดศีลธรรม ผิดจริยธรรม หรือเว็บไซต์ที่เสี่ยงหรือขัดต่อข้อกฎหมาย เป็นต้น

๑.๘ นโยบายการใช้บริการระบบ Web Mail ให้ผู้ใช้งานปฏิบัติดังต่อไปนี้

- ใช้ระบบ Web Mail ของหน่วยงานราชการ ในกรณีที่ติดต่อสื่อสารในเรื่องที่เกี่ยวกับการปฏิบัติงานเท่านั้น
- ห้ามส่งเมล์ที่มีลักษณะเป็นจดหมายลูกโซ่
- ห้ามส่งเมล์ที่มีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของผู้อื่น
- สำรองข้อมูลอีเมล์ตามความจำเป็นอย่างสม่ำเสมอ
- ห้ามเปิดเมล์ที่ไม่รู้จัก เพื่อป้องกันไวรัสคอมพิวเตอร์แพร่กระจายภายในองค์กร

๑.๙ นโยบายการใช้งานคอมพิวเตอร์ ของกองแบบแผน กรมสนับสนุนบริการสุขภาพ

- งานเทคโนโลยีสารสนเทศ กลุ่มบริหารทั่วไปและแผนงาน มีหน้าที่บริหารจัดการและบำรุงรักษาเครื่องคอมพิวเตอร์ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ
- ผู้ใช้งานจะต้องกำหนดรหัสผ่านส่วนบุคคลสำหรับเปิดใช้งานเครื่องคอมพิวเตอร์
- หากเกิดความเสียหายต่อเครื่องคอมพิวเตอร์เมื่อมีผู้อื่นมาใช้งานเจ้าของผู้ใช้งานจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น
- ผู้ใช้งานจะต้องสำรองข้อมูลของตนเอง เพื่อใช้กู้คืนข้อมูล ในกรณีเครื่องคอมพิวเตอร์ได้รับความเสียหาย

(๒) การจัดให้มีการสำรองข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

- จัดทำแผนเตรียมความพร้อมของระบบต่าง ๆ ที่ต้องมีการกู้คืน
- งานเทคโนโลยีสารสนเทศ จัดทำแผนกู้คืนระบบงานที่สำคัญ

๒.๑ การทดสอบและปรับปรุงแผนเตรียมความพร้อมฯ ให้ผู้ที่ได้รับมอบหมายปฏิบัติดังต่อไปนี้

- กำหนดให้มีการจัดทำแผนการทดสอบการกู้คืนระบบงานที่สำคัญและการทดสอบแผนอย่างน้อยปีละ ๑ ครั้ง
- ปรับปรุงแผนกู้คืนระบบงานที่สำคัญให้ทันสมัยอยู่เสมอ

๒.๒ การสำรองและทดสอบข้อมูลของระบบงานที่สำคัญตามระยะเวลาที่เหมาะสม ให้ผู้ดูแลระบบปฏิบัติดังต่อไปนี้

- ดำเนินการสำรองข้อมูลให้อยู่ในสภาพพร้อมใช้งานอย่างสม่ำเสมอ
- จัดทำแผนสำรองข้อมูลสำหรับระบบงานที่สำคัญ
- ดำเนินการตรวจสอบการสำรองข้อมูลว่าสำเร็จครบถ้วนหรือไม่ หากไม่สำเร็จให้หาสาเหตุเพื่อแก้ไขและดำเนินการตรวจสอบใหม่ จนกว่าการสำรองข้อมูลจะครบถ้วน
- ดำเนินการทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างน้อยปีละ ๒ ครั้ง และตรวจสอบว่าข้อมูลยังคงสามารถใช้งานได้เป็นปกติ

(๓) การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของกองแบบแผน กรมสนับสนุนบริการสุขภาพ กำหนดให้ผู้ที่ได้รับมอบหมายปฏิบัติดังต่อไปนี้

- ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของกองแบบแผน กรมสนับสนุนบริการสุขภาพ อย่างน้อยปีละ ๑ ครั้ง
- จัดเรียงลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและนำความเสี่ยงที่อยู่ในระดับสูงถึงระดับสูงมาก มาจัดทำแผนควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- นำแผนควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศไปสู่การปฏิบัติ
- ติดตามประเมินผลแผนควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- จัดทำแผนรับรองสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ

(๔) การปฏิบัติตามข้อกฎหมายที่เกี่ยวข้อง กำหนดให้ปฏิบัติดังต่อไปนี้

๔.๑ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

- สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อตระหนักถึงภัยหรือผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ กำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม กำหนดให้ผู้ที่ได้รับมอบหมายโครงการจัดอบรมบุคลากรภายในหน่วยงานให้มีความรู้ความเข้าใจ ตระหนักถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง
- การป้องกันอุปกรณ์ขณะที่ไม่มีผู้ใช้งาน ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันผู้ไม่มีสิทธิใช้งานเข้าถึงอุปกรณ์ของหน่วยงาน ให้ผู้ที่ได้รับมอบหมาย กำหนดให้มีการเข้ารหัสก่อนเปิดใช้งานคอมพิวเตอร์ของหน่วยงาน หรือกำหนดให้มีการเข้ารหัสก่อนเข้าสู่ระบบสารสนเทศของหน่วยงาน
- การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว กำหนดให้ผู้ที่ได้รับมอบหมาย ปฏิบัติดังต่อไปนี้
- กำหนดให้มีการควบคุมการใช้งานโปรแกรมอรรถประโยชน์ โดยผ่านการพิจารณาจากคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองแบบแผน

- กำหนดห้ามมิให้ผู้ปฏิบัติงาน บุคลากรภายในหน่วยงานกองแบบแผน ดาวน์โหลดโปรแกรมอรรถประโยชน์ ที่ไม่ได้รับอนุญาตมาติดตั้งและใช้งานในเครื่องคอมพิวเตอร์ของหน่วยงาน หากเกิดความเสียหายกับเครื่องคอมพิวเตอร์ผู้ละเมิดต้องเป็นผู้รับผิดชอบ

- หากมีความจำเป็นต้องติดตั้งโปรแกรมอรรถประโยชน์ข้างต้น ให้ทำบันทึกขออนุญาติต่อผู้อำนวยการกองแบบแผน และให้เจ้าหน้าที่งานเทคโนโลยีสารสนเทศ กองแบบแผน เป็นผู้ดำเนินการติดตั้ง

๔.๒ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ การบริหารจัดการทรัพย์สินสารสนเทศมีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศโดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง กำหนดให้ผู้ที่ได้รับมอบหมาย ปฏิบัติดังต่อไปนี้

- จัดทำทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยอย่างน้อยควรมีรายละเอียดเกี่ยวกับชื่ออุปกรณ์ หมายเลขครุภัณฑ์ หมายเลขสินทรัพย์ วันเดือนปีที่ได้รับ ชื่อผู้ใช้งาน สถานที่ใช้งาน รายละเอียดเกี่ยวกับคุณลักษณะของทรัพย์สิน เช่น CPU RAM Harddisk เป็นต้น
- ขึ้นทะเบียนทรัพย์สินที่ได้รับการจัดสรรทุกครั้ง
- ตรวจสอบ ปรับปรุง ทบทวน ทะเบียนบัญชีทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง
- หน่วยงานต้องระบุรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง เครือข่ายและ Software

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑๑ เมษายน พ.ศ. ๒๕๖๔

(นายถาวร ขาวแสง)
ผู้อำนวยการกองแบบแผน