แนวทางปฏิบัติ/ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ของกองกฎหมาย กรมสนับสนุนบริการสุขภาพ

ตามนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ กำหนดให้ทุกหน่วยงานในสังกัดกรมสนับสนุนบริการสุขภาพ ต้องปฏิบัติตามนโยบายดังกล่าว ดังนั้น เพื่อให้บุคลากรของกองกฎหมาย สามารถปฏิบัติตามนโยบายฯได้อย่างมีประสิทธิภาพ กองกฎหมาย จึงได้จัดทำแนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ของกองกฎหมาย กรมสนับสนุนบริการสุขภาพ ขึ้น โดยให้ถือปฏิบัติในทิศทางเดียวกัน

แนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ของกองกฎหมาย กรมสนับสนุนบริการสุขภาพ ประกอบด้วย ๓ หัวข้อหลัก ดังนี้

๑.การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๒.การจัดให้มีการสำรองข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพพร้อมใช้งาน

๓.การปฏิบัติตามข้อกฎหมายที่เกี่ยวข้อง

<u>แนวปฏิบัติ</u>

แนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ของกองกฎหมาย กรมสนับสนุนบริการสุขภาพ ที่กำหนดไว้ มีดังต่อไปนี้

๑.การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

ข้อ ๑.๑ นโยบายการควบคุมการเข้าถึงสารสนเทศ(Access control policy) ให้ผู้บริหารหรือผู้ที่ได้รับมอบหมายปฏิบัติดังต่อไปนี้

-จัดทำข้อปฏิบัติการควบคุมการเข้าถึงสารสนเทศอย่างเป็นลายลักษณ์อักษร

ข้อ ๑.๒ การลงทะเบียนผู้ใช้งานของระบบสารสนเทศใดของกองกฎหมาย เช่น ระบบเว็บไซต์กองกฎหมาย,ระบบควบคุมการเบิกจ่ายและรายงานผลการดำเนินงาน(SMART) เป็นต้น ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายปฏิบัติ เมื่อมีการลาออกหรือโยกย้ายแผนกหรือหน่วยงานหรือได้รับแจ้งจากหน่วยงานต้นสังกัดให้ดำเนินการปรับปรุงหรือถอดถอนสิทธิภายใน ๕ วัน นับจากวันที่ได้รับแจ้ง

ข้อ ๑.๓ การบริหารจัดการสิทธิการใช้งานระบบ ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

(๑) กำหนดบัญชีรายชื่อและรายละเอียดการใช้งานสารสนเทศของกองกฎหมาย

(๒) กำหนดสิทธิการใช้งานระบบงานตามหน้าที่ความรับผิดชอบของผู้ใช้งานตามความจำเป็นของผู้ใช้งาน

(๓) จัดให้มีการสร้างบัญชีรายชื่อผู้ใช้งานแยกเป็นรายบุคคล

ข้อ ๑.๔ การบริหารจัดการรหัสผ่านผู้ใช้งาน(User password management) ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

-จัดทำระเบียบหรือแนวทางที่เกี่ยวข้องกับการปฏิบัติงานของผู้ใช้งาน รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามเอกสารแนบดังกล่าวโดยเคร่งครัด

ข้อ ๑.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน(Review of user access rights) ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

-จัดให้มีการทบทวนบัญชีผู้ใช้งานและสิทธิผู้ใช้งาน อย่างน้อยปีละ ๒ ครั้ง

ข้อ ๑.๖ การใช้งานรหัสผ่าน ให้ผู้ใช้งานปฏิบัติดังนี้

(๑) ให้กำหนดรหัสผ่านส่วนบุคคลที่มีความยาว ๖-๘ ตัวอักษร และมีอักขระปน

(๒) เก็บรักษารหัสผ่านของตนเองไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น

(๓) ในกรณีที่จำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น เพื่อให้สามารถปฏิบัติงานแทนตนเองได้ หลังจากที่ทำงานเสร็จเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

ข้อ ๑.๗ นโยบายการใช้งานบริการอินเทอร์เน็ต ให้ผู้ใช้งานปฏิบัติดังนี้

(๑) ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

- การพนัน ,ลามก อนาจาร
- อื่นๆที่เกี่ยวกับสิ่งผิดกฎหมาย ผิดศีลธรรมหรือผิดจริยธรรม

ข้อ ๑.๘ นโยบายการใช้บริการระบบ web mail ให้ผู้ใช้งานปฏิบัติดังนี้

(๑) ใช้ระบบ web mail ของหน่วยงานราชการ ในกรณีที่ติดต่อสื่อสารในเรื่องเกี่ยวกับการปฏิบัติงานเท่านั้น

(๒) ห้ามส่งเมล์ที่มีลักษณะเป็นจดหมายลูกโซ่

(๓) ห้ามส่งเมล์ที่มีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของผู้อื่น

(๔) ห้ามเปิดเมล์ที่ไม่รู้จัก เพื่อป้องกันไวรัสคอมพิวเตอร์แพร่กระจายมายังองค์กร

ข้อ ๑.๙ นโยบายการใช้งานเครื่องคอมพิวเตอร์ กองกฎหมาย กรมสนับสนุนบริการสุขภาพ

(๑) กลุ่มบริหารงานทั่วไปและแผนงานมีหน้าที่บริหารจัดการและบำรุงรักษาเครื่องคอมพิวเตอร์ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

(๒) ผู้ใช้งานเครื่องคอมพิวเตอร์จะต้องกำหนดรหัสผ่านส่วนบุคคลสำหรับเปิดใช้งานเครื่องคอมพิวเตอร์ทุกครั้งที่เปิดเครื่อง

(๓) ถ้าเจ้าของผู้ใช้งานยินยอมให้ผู้อื่นเข้าใช้งานเครื่องคอมพิวเตอร์ของตนเองแล้วเกิดความเสียหาย เจ้าของผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

(๔) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลของตนเองที่จัดเก็บในเครื่องคอมพิวเตอร์ เพื่อใช้กู้คืนข้อมูล ในกรณีเครื่องคอมพิวเตอร์ได้รับความเสียหาย

๒.การจัดให้มีการสำรองข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพพร้อมใช้งาน

ข้อ ๒.๑ การสำรองและทดสอบข้อมูลของระบบงานที่สำคัญตามระยะเวลาที่เหมาะสม ให้ผู้ดูแลระบบปฏิบัติดังนี้

(๑) จัดทำแผนสำรองข้อมูลสำหรับระบบงานที่สำคัญ

(๒) ตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วนหรือไม่ หากไม่สำเร็จให้หาสาเหตุดำเนินการแก้ไขและดำเนินการใหม่อีกครั้งหนึ่ง

(๓) ทดสอบกู้คืนข้อมูลที่สำรองไว้เป็นระยะ เช่น ปีละ ๑ ครั้ง เพื่อดูว่าข้อมูลยังคงสามารถใช้งานได้เป็นปกติหรือไม่

๓.การปฏิบัติตามข้อกฎหมายที่เกี่ยวข้อง

๓.๑ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓

ข้อ ๓.๑.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม กำหนดให้ผู้ที่ได้รับมอบหมาย ปฏิบัติดังนี้

-จัดอบรมรหรือส่งเสริมบุคลากรให้มีความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๓.๑.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล กำหนดให้ผู้ที่ได้รับมอบหมาย ปฏิบัติดังนี้

-จัดให้มีการเข้ารหัสก่อนเข้าเครื่องคอมพิวเตอร์ของหน่วยงาน หรือกำหนดให้มีการเข้ารหัสก่อนเข้าสู่ระบบสารสนเทศของหน่วยงาน

ข้อ ๓.๑.๓ การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุม การใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว กำหนดให้ผู้ที่ได้รับมอบหมาย ปฏิบัติดังนี้

-กำหนดให้มีการควบคุมการใช้งานโปแกรมอรรถประโยชน์ โดยผ่านการพิจารณาจากคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกลุ่มตรวจสอบภายใน

-กำหนดห้ามมิให้ผู้ปฏิบัติงาน/บุคลากรของกลุ่มตรวจสอบภายใน ดาวน์โหลดโปรแกรมอรรถประโยชน์ ที่ไม่ได้รับอนุญาตมาติดตั้งและใช้งานในเครื่องคอมพิวเตอร์ของหน่วยงาน

๓.๒ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

ข้อ ๓.๒.๑ การบริหารจัดการทรัพย์สินสารสนเทศมีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง กำหนดให้ผู้ที่ได้รับมอบหมาย ปฏิบัติดังนี้

(๑) จัดทำทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศ โดยอย่างน้อยมีรายละเอียดเกี่ยวกับชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบและรายละเอียดเกี่ยวกับคุณลักษณะของทรัพย์สิน เช่น CPU RAM Hard Disk เป็นต้น

(๒) ขึ้นทะเบียนทรัพย์สินที่ได้รับจัดสรรใหม่ทุกครั้ง

(๓) มีการตรวจสอบ ปรับปรุง ทบทวน ทะเบียนบัญชีทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง

(๔) หน่วยงานต้องระบุรายชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์-เครือข่ายและ software

(๕) กำหนดข้อปฏิบัติในการคืนทรัพย์สินภายใน ๗ วัน ตามกำหนดเวลา และกรณีการใช้งานประจำทุกวัน ต้องคืนทรัพย์เมื่อสิ้นสุดการจ้าง/หมดสัญญา/มีการโอน-ย้าย-ลาออกหรือเกษียณอายุ ภายใน ๑ วัน

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๙ พฤศจิกายน พ.ศ. ๒๕๖๔

(นางจันฑนา จินดาถาวรกิจ)
ผู้อำนวยการกองกฎหมาย