แนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยสารสนเทศ ปีงบประมาณ ๒๕๖๖
ของกองสถานพยาบาลและการประกอบโรคศิลปะ กรมสนับสนุนบริการสุขภาพ

ตามนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ กำหนดให้ทุกหน่วยงานในสังกัดกรมสนับสนุนบริการสุขภาพ ต้องปฏิบัติตามนโยบายดังกล่าว ดังนั้น เพื่อให้บุคลากรของกองสถานพยาบาลและการประกอบโรคศิลปะ สามารถปฏิบัติตามนโยบายฯได้อย่างมีประสิทธิภาพ กองสถานพยาบาลและการประกอบโรคศิลปะจึงได้จัดทำแนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยสารสนเทศ ของกองสถานพยาบาลและการประกอบโรคศิลปะ กรมสนับสนุนบริการสุขภาพ โดยให้ถือปฏิบัติในทิศทางเดียวกัน

แนวทางปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ของกองสถานพยาบาลและการประกอบโรคศิลปะ กรมสนับสนุนบริการสุขภาพ ประกอบด้วย ๔ หัวข้อหลักดังนี้

๑.การเข้าถึงหรือควบคุมการใช้สารสนเทศ

๒.การจัดให้มีการสำรองข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีเหตุฉุกเฉิน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓.จัดการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศปีละครั้ง

๔.การปฏิบัติตามข้อกฎหมายที่เกี่ยวข้อง

แนวปฏิบัติ/มาตรการในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ของกองสถานพยาบาลและการประกอบโรคศิลปะ กรมสนับสนุนบริการสุขภาพ มีดังต่อไปนี้

๑.การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

ข้อ ๑.๑ การควบคุมการเข้าถึงสารสนเทศ (Access control policy) ให้ปฏิบัติดังต่อไปนี้

(๑) กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้อง

(๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๑.๒ การลงทะเบียนผู้ใช้งานของระบบสารสนเทศใดของกองสถานพยาบาลและการประกอบโรคศิลปะ เช่น ระบบเว็บไซต์ของกองสถานพยาบาลและการประกอบโรคศิลปะ,ระบบคุ้มครองผู้บริโภคด้านบริการสุขภาพ เป็นต้น ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายปฏิบัติ เมื่อมีการลาออกหรือโยกย้ายแผนกหรือหน่วยงานที่ได้รับแจ้งจากหน่วยงานต้นสังกัดให้ดำเนินการปรับปรุงหรือถอดถอนสิทธิภายใน ๓ วันนับจากวันที่ได้รับแจ้ง

ข้อ ๑.๓ การบริหารจัดการสิทธิการใช้งานระบบ ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

(๑) กำหนดบัญชีรายชื่อและรายละเอียดการใช้งานสารสนเทศของกองสถานพยาบาลและการประกอบโรคศิลปะ

(๒) กำหนดสิทธิการใช้งานระบบงานตามหน้าที่ความรับผิดชอบของผู้ใช้งานตามความจำเป็นของผู้ใช้งาน

(๓)จัดให้มีการสร้างบัญชีรายชื่อผู้ใช้งานแยกเป็นรายบุคคล

ข้อ ๑.๔ การบริหารจัดการรหัสผ่านผู้ใช้งาน(User Password Management) ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

- จัดให้มีการส่งบัญชีผู้ใช้งานและรหัสผ่าน โดยใส่ซองปิดผนึกและประทับตรา “ลับ” และส่งไปยังผู้ใช้งาน และแนบระเบียบอื่นๆที่เกี่ยวข้องกับการปฏิบัติงานของผู้ใช้งาน รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามเอกสารแนบดังกล่าวโดยเคร่งครัด

ข้อ ๑.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review Of User Access Right) ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

- จัดให้มีการทบทวนบัญชีผู้ใช้งานและสิทธิผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑.๖ การใช้งานรหัสผ่าน ให้ผู้ใช้งานปฏิบัติดังนี้

(๑) ให้กำหนดรหัสผ่านส่วนบุคคลประกอบไปด้วยชุดตัวอักษรภาษาอังกฤษ ตัวเลขและอักขระพิเศษอย่างน้อย ๘ ตัวขึ้นไป และยากต่อการคาดเดา

(๒) ให้เปลี่ยนรหัสผ่านส่วนบุคคล อย่างน้อยทุก ๖ เดือน

(๓)ในกรณีที่จำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเพื่อทดสอบหรือแก้ไขการใช้งานระบบให้ดำเนินการเปลี่ยนรหัสผ่านทันทีเมื่อการทดสอบหรือแก้ไขการใช้งานเสร็จสิ้นลงแล้ว

ข้อ ๑.๗ นโยบายการใช้งานอินเทอร์เน็ต ให้ผู้ใช้งานปฏิบัติดังนี้

(๑) ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

- การพนัน,ลามก,อนาจาร
-อื่นๆที่เกี่ยวกับสิ่งผิดกฎหมาย ผิดศีลธรรมหรือผิดจริยธรรม

ข้อ๑.๘ นโยบายการใช้บริการระบบ Web Mail ให้ผู้ใช้งานปฏิบัติดังนี้

(๑)ห้ามส่งอีเมลที่มีลักษณะเป็นจดหมายลูกโซ่

(๒)ห้ามส่งอีเมลที่มีลักษณะเป็นการละเมิดกฎหมายหรือสิทธิของผู้อื่น

(๓)ให้ทำการสำรองข้อมูลอีเมลตามความจำเป็นอย่างสม่ำเสมอ

(๔)ห้ามเปิดอีเมลที่ไม่รู้จัก เพื่อป้องกันไวรัสคอมพิวเตอร์แพร่กระจายมายังองค์กร

ข้อ๑.๙ นโยบายการใช้งานเครื่องคอมพิวเตอร์ของกองสถานพยาบาลและการประกอบโรคศิลปะ กรมสนับสนุนบริการสุขภาพ

(๑) กลุ่มแผนงานและประเมินผล มีหน้าที่บริหารจัดการเครื่องคอมพิวเตอร์ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

(๒) ผู้ใช้งานเครื่องคอมพิวเตอร์มีหน้าที่ บำรุงรักษาเครื่อง จัดพื้นที่ให้มีความโปร่ง อากาศถ่ายเทได้สะดวก จัดเก็บสายไฟให้เป็นระเบียบ ทำการจัดเรียงข้อมูลเครื่อง(Defragment) เครื่องเป็นประจำ มีการทำความสะอาดข้อมูลระบบปฏิบัติการและข้อมูลที่จัดเก็บในเครื่อง(Cleansing) สแกนแอนติไวรัส เพื่อให้เครื่องใช้งานได้อย่างมีประสิทธิภาพ

(๓) ถ้าเจ้าของผู้ใช้งานยินยอมให้ผู้อื่นเข้าใช้งานเครื่องคอมพิวเตอร์ของตนเองแล้วเกิดความเสียหาย เจ้าของผู้ใช้งานต้องรบผิดชอบต่อความเสียหายที่เกิดขึ้น

(๔) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลของตนเองที่จัดเก็บในเครื่องคอมพิวเตอร์ เพื่อใช้กู้คืนข้อมูล ในกรณีเครื่องคอมพิวเตอร์ได้รับความเสียหาย

ข้อ๑.๑๐ ผู้ใช้งานคอมพิวเตอร์ notebook ห้องประชุมจะต้องดำเนินการสแกนไวรัสจากอุปกรณ์จัดเก็บข้อมูล เช่น Flashdrive ,External Hardisk,โทรศัพท์มือถือ หรืออุปกรณ์อื่นๆที่ใช้เชื่อมต่อกับคอมพิวเตอร์ notebook ทุกครั้ง และเมื่อใช้งาน คอมพิวเตอร์ notebook ห้องประชุมเสร็จแล้วขอให้ลบไฟล์หรือโอนย้ายไฟล์ที่บันทึกไว้ออกจากคอมพิวเตอร์ notebook ห้องประชุมทันที

๒. การจัดให้มีการสำรองข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน เพื่อให้สามารถใช้งานสารสนเทศได้ปกติอย่างต่อเนื่อง

ข้อ ๒.๑ กำหนดหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับการจัดทำแผนเตรียมความพร้อมฯ ให้ผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

- กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ที่เกี่ยวข้องกับการจัดทำแผนเตรียมความพร้อมของระบบต่างๆที่ต้องมีการกู้คืน

ข้อ ๒.๒ การจัดทำแผนเตรียมความพร้อมฯ ให้ผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

- จัดทำแผนกู้คืนงานระบบงานที่สำคัญ

ข้อ ๒.๓ การทดสอบและปรับปรุงแผนเตรียมความพร้อมฯ ให้ผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

(๑) กำหนดให้มีการจัดทำแผนการทดสอบการกู้คืนระบบงานที่สำคัญและการทดสอบแผนดังกล่าว อย่างน้อยปีละ ๑ ครั้ง

(๒) ปรับปรุงแผนกู้คืนระบบงานที่สำคัญให้ทันสมัยอย่างสม่ำเสมอ

ข้อ ๒.๔ การสำรองและทดสอบข้อมูลของระบบงานที่สำคัญตามระยะเวลาที่เหมาะสม ให้ผู้ดูแลปฏิบัติดังนี้

(๑) จัดทำแผนสำรองข้อมูลสำหรับระบบงานที่สำคัญ

(๒) ตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วนหรือไม่ หากไม่สำเร็จให้หาสาเหตุดำเนินการแก้ไขและดำเนินการใหม่อีกครั้งหนึ่ง

(๓) ทดสอบกู้คืนข้อมูลที่สำรองไว้เป็นระยะ เช่นปีละ ๑ ครั้ง เพื่อดูว่าข้อมูลยังคงสามารถใช้งานได้เป็นปกติหรือไม่

๓. การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของกองสถานพยาบาลและการประกอบโรคศิลปะกรมสนับสนุนบริการสุขภาพ กำหนดให้ผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

ข้อ ๓.๑ จัดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของกองสถานพยาบาลและการประกอบโรคศิลปะ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๓.๒ จัดให้มีการจัดเรียงลำดับความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและนำความเสี่ยงที่อยู่ในระดับสูงถึงระดับสูงมาก มาจัดทำแผนควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ข้อ ๓.๓ นำแผนควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศไปสู่การปฏิบัติ

ข้อ ๓.๔ ติดตามประเมินผลแผนควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๔.การปฏิบัติตามกฎหมายที่เกี่ยวข้อง

ข้อ ๔.๑ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ พ.ศ.๒๕๕๓

ข้อ ๔.๑.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม กำหนดให้ผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

- จัดอบรมบุคลากรให้ความรู้ ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดขึ้นจากการใช้ระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔.๑.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล กำหนดให้ผู้ที่ได้รับมอบหมาย ปฏิบัติดังนี้

- จัดให้มีการเข้ารหัสก่อนเข้าเครื่องคอมพิวเตอร์ของหน่วยงาน หรือกำหนดให้มีการเข้ารหัสก่อนเข้าสู่ระบบสารสนเทศของหน่วยงาน

ข้อ ๔.๑.๓ การใช้งานโปรแกรมอรรถประโยชน์ (Use Of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว กำหนดให้ผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

- กำหนดให้มีการควบคุมการใช้งานโปรแกรมอรรถประโยชน์ โดยผ่านการพิจารณาจากคณะกรรมการพัฒนาดิจิทัลเพื่อการคุ้มครองผู้บริโภคด้านบริการสุขภาพ กองสถานพยาบาลและการประกอบโรคศิลปะ

- กำหนดห้ามมิให้ผู้ปฏิบัติงาน/บุคลากรของกองสถานพยาบาลและการประกอบโรคศิลปะ ดาวน์โหลดโปรแกรมอรรถประโยชน์ ที่ไม่ได้รับอนุญาตมาติดตั้งและใช้งานเครื่องคอมพิวเตอร์ของหน่วยงาน

ข้อ ๔.๒ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ.๒๕๕๕

ข้อ ๔.๒.๑ การบริหารจัดการทรัพย์สินสารสนเทศมีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อใช้งานในภายหลัง กำหนดให้ผู้ที่ได้รับมอบหมายปฏิบัติดังนี้

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

(๒) ขึ้นทะเบียนทรัพย์สินที่ได้รับจัดสรรใหม่ทุกครั้ง

(๓) มีการตรวจสอบ ปรับปรุง ทบทวน ทะเบียนบัญชีทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง

(๔) หน่วยงานต้องระบุรายชื่อผู้ที่ใช้อุปกรณ์คอมพิวเตอร์-เครือข่าย และ Software

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๗ กุมภาพันธ์ พ.ศ.๒๕๖๖

(นางนลินา ตันตินิรามัย)
ผู้อำนวยการกองสถานพยาบาลและการประกอบโรคศิลปะ