นโยบายความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ สำนักโรคติดต่อทั่วไป

ระบบฐานข้อมูลและสารสนเทศ มีความสำคัญยิ่งต่อการดำเนินงานตามภารกิจและการสื่อสารของส่วนราชการ ดังนั้น เพื่อให้ระบบฐานข้อมูลและสารสนเทศของสำนักโรคติดต่อทั่วไปมีความมั่นคง ปลอดภัย มีประสิทธิภาพ สามารถนำไปใช้สนับสนุนการปฏิบัติงานให้บรรลุเป้าหมายตามวัตถุประสงค์ และสนับสนุนการบริหารส่วนราชการได้อย่างมีประสิทธิภาพและประสิทธิผล รวมทั้งเพื่อให้สอดคล้องกับประกาศกระทรวงสาธารณสุข ประกาศ ณ วันที่ ๒๘ กรกฎาคม พ.ศ. ๒๕๕๓ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงสาธารณสุข สำนักโรคติดต่อทั่วไปจึงจัดทำนโยบายความมั่นคง ปลอดภัยของระบบฐานข้อมูลและสารสนเทศของสำนักโรคติดต่อทั่วไป

วัตถุประสงค์และขอบเขต

๑. เพื่อดูแลรักษาความปลอดภัยของฐานข้อมูลต่างๆ ของสำนักโรคติดต่อทั่วไป ป้องกันการบุกรุกข้อมูล (hack) ป้องกันข้อมูลสูญหายเนื่องจากการใช้งานในลักษณะที่ไม่ถูกต้อง จากสถานการณ์ความไม่แน่นอน หรือจากภัยพิบัติ

๒. เพื่อให้บุคลากรของสำนักโรคติดต่อทั่วไป รวมทั้งบุคลากรของหน่วยงานที่เกี่ยวข้อง ผู้มีส่วนได้ส่วนเสียและประชาชน มีความเชื่อมั่นในความปลอดภัยของระบบฐานข้อมูลและสารสนเทศของสำนักฯ รวมทั้งมีความเชื่อมั่นในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

๓. เพื่อเผยแพร่ให้บุคลากรทุกระดับของสำนักโรคติดต่อทั่วไปรับทราบ และตระหนักถึงความสำคัญของนโยบายความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ ซึ่งบุคลากรทุกคนต้องรับทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

องค์ประกอบของนโยบาย

๑. นโยบายความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

ผู้รับผิดชอบจัดให้มีระบบสำรองไฟฟ้าหรือเครื่องสำรองไฟฟ้า (UPS) สำหรับเครื่องคอมพิวเตอร์ทุกเครื่อง มีเครื่องสำหรับสำรองฐานข้อมูล (Backup Hard Disk) ขนาดใหญ่ ที่มีความจุตั้งแต่ ๕๐๐ GB ขึ้นไป เพื่อให้ กลุ่ม/ด่าน/ที่ทำการแพทย์ ใช้สำรองข้อมูลตามความเหมาะสมและตามความจำเป็น ขึ้นอยู่กับขนาดหรือปริมาณฐานข้อมูลในความรับผิดชอบของหน่วยงานนั้นๆ และมีสื่อสำรองข้อมูลชนิดพกพาเพื่อความสะดวกในการเก็บรักษาและเคลื่อนย้าย มีการกำหนดระเบียบปฏิบัติในการจัดวางเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง การใช้งาน และการบำรุงรักษา รวมทั้งอุปกรณ์ทั้งหมดที่เกี่ยวข้องกับระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ จัดให้มีทำเนียบรายชื่อพร้อมข้อมูลสำหรับติดต่อ (เช่น หมายเลขโทรศัพท์/โทรสาร/E-mail) ของผู้รับผิดชอบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่ใช้ปฏิบัติงานประจำ ผู้รับผิดชอบอุปกรณ์อื่นๆ ที่ใช้สนับสนุนการทำงานของระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ ตลอดจนรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ ที่เกี่ยวข้องกรณีเกิดสถานการณ์ความไม่แน่นอนหรือภัยพิบัติร้ายแรงที่สำนักฯ ไม่สามารถแก้ไขปัญหาได้ สำหรับการนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงออกไปนอกสำนักงาน ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการสำนักฯ หรือหัวหน้ากลุ่ม / หัวหน้าด่าน / หัวหน้าที่ทำการแพทย์

๒. นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ

ผู้รับผิดชอบจัดให้มีขั้นตอนการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ จัดให้มีการระบุและพิสูจน์ตัวตนของผู้ใช้งาน มีการกำหนดรหัสผ่าน จำกัดและควบคุมการใช้งานโปรแกรมประเภท Utilities เพื่อป้องกันการละเมิดหรือการหลีกเลี่ยงมาตรการรักษาความมั่นคงปลอดภัยฯ มีการกำหนดให้ระบบตัดการใช้งานของผู้ใช้ หากผู้ใช้หยุดการใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้ และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

๓. นโยบายการควบคุมการเข้าถึงระบบฐานข้อมูลและสารสนเทศ

ผู้รับผิดชอบจัดให้มีการลงทะเบียนผู้ใช้งานและกำหนดรหัสผ่าน มีการกำหนดหลักเกณฑ์ผู้ใช้ที่มีสิทธิ์เข้าถึงระบบฐานข้อมูลให้เหมาะสมตามระดับความจำเป็นในการใช้งาน มีการทบทวนสิทธิ์การใช้งานตามระยะเวลาที่กำหนด และตรวจสอบการละเมิดความปลอดภัย มีการกำหนดเส้นทางการเชื่อมต่อของระบบเทคโนโลยีสารสนเทศ โดยต้องผ่านระบบรักษาความปลอดภัย เช่น Firewall และการตรวจสอบไวรัสคอมพิวเตอร์ เป็นต้น อาจออกแบบระบบเครือข่ายโดยการแบ่งเขตการใช้งาน (Zone) เพื่อสามารถควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ สำหรับข้อมูลที่เป็นความลับ เช่น ข้อมูลยืนยันตัวตน ฯลฯ ต้องกำหนดการเข้ารหัสข้อมูล มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล ควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศจากภายนอก โดยการกำหนดสิทธิ์ควบคุม Port ที่ใช้เข้าสู่ระบบให้รัดกุม รวมทั้งกำหนดให้แสดงตัวตนของผู้ใช้งาน (Identification) และการพิสูจน์ยืนยันตัวตน (Authentication)

๔. นโยบายการเฝ้าระวังเพื่อความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ

ผู้รับผิดชอบต้องตั้งเวลาในเครื่องคอมพิวเตอร์ทุกเครื่องของสำนักฯ ให้ตรงกัน (Clock Synchronization) โดยอ้างอิงจากแหล่งเทียบเวลาที่เป็นมาตรฐาน มีการบันทึกเหตุการณ์เกี่ยวกับการใช้งานสารสนเทศ (Audit Logging) อย่างสม่ำเสมอตามระยะเวลาที่กำหนด มีมาตรการในการป้องกันการเปลี่ยนแปลงหรือการแก้ไขข้อมูลบันทึกเหตุการณ์โดยไม่ได้รับอนุญาต (Protection of Log Information) มีการกำหนดขั้นตอนเพื่อตรวจสอบการใช้งานระบบและอุปกรณ์ รวมทั้งสิ่งผิดปกติที่เกิดขึ้น มีการบันทึกสิ่งผิดปกติหรือเหตุการณ์ที่เป็นข้อผิดพลาดที่เกิดขึ้นจากการใช้งานสารสนเทศ (Fault Logging) วิเคราะห์สิ่งผิดปกติหรือข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามความเหมาะสม มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้อง (Administrator and Operator Logs)

๕. นโยบายการสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

ผู้รับผิดชอบกำหนดขั้นตอนการปฏิบัติเพื่อควบคุมการติดตั้ง Software ต่างๆ ลงไปยังระบบที่ให้บริการเพื่อลดความเสี่ยงที่จะทำให้ระบบให้บริการเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้ หลีกเลี่ยงการใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการสำหรับทำการทดสอบระบบ จำกัดการเข้าถึง Source Code สำหรับระบบที่ให้บริการ เพื่อป้องกันการเปลี่ยนแปลงที่อาจเกิดขึ้นโดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนา

๖. นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer หรือ PC) และเครื่องคอมพิวเตอร์พกพา (Notebook)

เครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของส่วนราชการ โปรแกรมใช้งานต่างๆ ควรมีลิขสิทธิ์ถูกต้องตามกฎหมาย ไม่ติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับงานที่ปฏิบัติ กำหนดให้ใช้ Username และ Password ก่อนใช้งาน รวมทั้งการ lock หน้าจอ และใช้โปรแกรม Screen Saver เมื่อพักการใช้งานชั่วคราว ผู้ใช้ (User) ต้องทำการ

สำรองข้อมูล (Backup) โดยใช้สื่อบันทึกข้อมูลที่มีความเหมาะสมและต้องเก็บรักษาไว้ในที่ปลอดภัย และควรทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๗. นโยบายการใช้งานเครือข่ายคอมพิวเตอร์สากล (Internet) และ จดหมายอิเล็กทรอนิกส์ (E-mail)

ผู้รับผิดชอบกำหนดผู้ใช้ที่มีสิทธิ์เชื่อมต่อระบบเพื่อใช้งานเครือข่ายคอมพิวเตอร์สากล (Internet) และจดหมายอิเล็กทรอนิกส์ (E-mail) กำหนดแนวทางการใช้งานเครือข่ายคอมพิวเตอร์สากล (Internet) และจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ถูกต้อง โดยไม่ละเมิดสิทธิ์หรือสร้างปัญหาให้แก่ระบบหรือผู้ใช้อื่น มีระบบรักษาความปลอดภัย เพื่อตรวจสอบการใช้งานและภัยคุกคาม มีการเก็บข้อมูลการเข้าถึงระบบและข้อมูลจราจรทางคอมพิวเตอร์

๘. นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless)

ผู้รับผิดชอบ กำหนดสิทธิ์ผู้ใช้งานและกำหนดรหัสผ่านในการเข้าถึงระบบเครือข่ายไร้สาย (Wireless) ลงทะเบียนอุปกรณ์ไร้สายทุกเครื่อง จัดวางอุปกรณ์ Access Point ในตำแหน่งที่สามารถป้องกันบุคคลภายนอกหรือผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้งานได้

๙. นโยบายการป้องกันโปรแกรมไม่ประสงค์ดี

ผู้รับผิดชอบติดตั้งโปรแกรมป้องกันไวรัสในเครื่องคอมพิวเตอร์ทุกเครื่อง ผู้ใช้ต้องตรวจสอบไวรัสคอมพิวเตอร์จากสื่อบันทึกข้อมูลทุกประเภทก่อนนำมาใช้งานร่วมกับคอมพิวเตอร์

นโยบายความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศของสำนักโรคติดต่อทั่วไปนี้ เป็นมาตรการและแนวทางด้านการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและฐานข้อมูลต่างๆ ของสำนักฯ เพื่อให้บุคลากรสามารถใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในระดับที่ปลอดภัย ช่วยลดความเสียหายที่อาจจะเกิดกับข้อมูล เครื่องคอมพิวเตอร์ และอุปกรณ์ที่เกี่ยวข้อง บุคลากรของสำนักฯ จะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ เดือนพฤศจิกายน พ.ศ. ๒๕๕๙

ลงชื่อ ร.ต.อ.
(รุ่งเรือง กิจผาติ)
ผู้อำนวยการสำนักโรคติดต่อทั่วไป