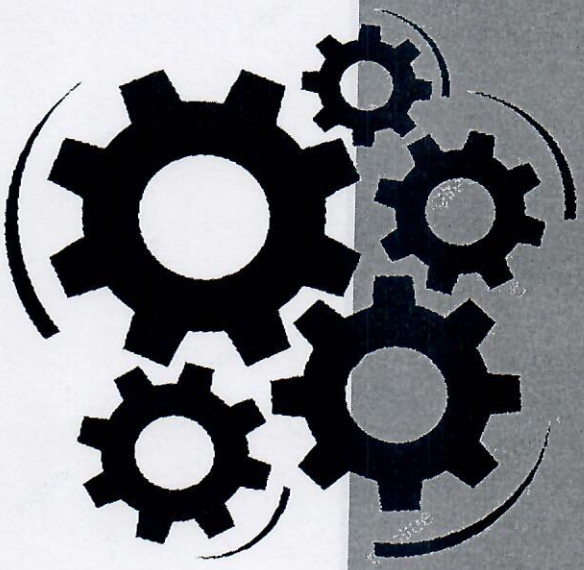
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ ของกองโรคติดต่อทั่วไป



กลุ่มยุทธศาสตร์และพัฒนาองค์กร
กองโรคติดต่อทั่วไป กรมควบคุมโรค

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกองโรคติดต่อทั่วไป

๑.การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

ที่	ระเบียบปฏิบัติ
๑	จัดวางเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงไว้ในบริเวณที่มีความปลอดภัย ระมัดระวังการจัดตั้งอุปกรณ์ให้อยู่ในสภาพที่มั่นคงและไม่ล้มหรือโอนเอียงได้โดยง่าย
๒	ผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นในกรณีที่ทำเครื่องชำรุดหรือสูญหายไปโดยประมาทหรือเลินเล่อ
๓	ระมัดระวังการใช้งาน และดูแลรักษาความสะอาดของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอย่างสม่ำเสมอ
๔	ไม่เข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้ - การพนัน - การวิพากษ์ วิจารณ์ ที่เกี่ยวข้องกับ ชาติ ศาสนา และพระมหากษัตริย์ - สิ่งลามก อนาจาร - สิ่งผิดกฎหมาย ผิดศีลธรรม หรือผิดจริยธรรม - ห้ามเล่นเกมส์ ดูภาพยนต์ หรือฟังเพลง ผ่านระบบเครือข่ายในเวลาราชการ
๕	ห้ามใช้ระบบเครือข่ายเพื่อส่ง กระจาย หรือแจกจ่ายข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต รวมทั้ง ข้อมูลที่เป็นความลับของกอง ไปยังบุคคลที่ไม่ได้รับอนุญาต
๖	ห้ามใช้ระบบเครือข่ายเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงของกอง
๗	ตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอ หากไม่ใช้งานเกินกว่า ๑๕ นาที
๘	ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๓ ชั่วโมง
๙	ห้ามเจ้าหน้าที่ทั่วไปติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในระบบเครือข่ายของกอง เพื่อให้บุคคลอื่นสามารถเข้าถึงหรือเชื่อมต่อเพื่อเข้าสู่ระบบเครือข่าย
๑๐	ให้ออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ
๑๑	ต้องขออนุมัติจากผู้มีอำนาจ ในกรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกกอง
๑๒	ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัปเดต (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดสิทธิ์
๑๓	ในการใช้งานระบบเครือข่ายอินเทอร์เน็ตไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน
๑๔	หลังจากสิ้นสุดการใช้งานระบบอินเทอร์เน็ต (Internet) ให้ทำการออกจากระบบ (logout) Authentication และปิดเว็บบราวเซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๒. ระเบียบปฏิบัติสำหรับการบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับฐานข้อมูลและสารสนเทศ

ผู้รับผิดชอบ : คณะทำงานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กองโรคติดต่อทั่วไป

ที่	ระเบียบปฏิบัติ
๑	จัดทำ/ทบทวน และปรับปรุงนโยบายความมั่นคงปลอดภัยฯ อย่างสม่ำเสมอ ปีละ ๑ ครั้ง
๒	สื่อสารให้บุคลากรทราบและตระหนักถึงความสำคัญของการปฏิบัติตามนโยบายความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศของกอง อย่างเคร่งครัดและสม่ำเสมอ
๓	จัดประชุมเกี่ยวกับการบริหารจัดการด้านความมั่นคงปลอดภัยฯ อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง โดยกำหนดวาระการประชุมที่ต้องหารือกัน ดังนี้ การตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยฯ และผลการตรวจสอบ แผนการดำเนินการเชิงป้องกัน/แก้ไข จากผลการตรวจสอบดังกล่าว การปรับปรุงนโยบายความมั่นคงปลอดภัยสำหรับปีถัดไป การประเมินความเสี่ยงและแผนลดความเสี่ยง การจัดทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบให้เพียงพอต่อการจัดการดังกล่าว
๔	ตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยฯ ปีละ ๑ ครั้ง และจัดทำแผนเพื่อปรับปรุง หรือแก้ไขปัญหาที่พบ
๕	แจ้งเวียนให้บุคลากรระมัดระวัง และดูแลทรัพย์สินของกอง ที่ตนเองใช้ในการปฏิบัติงาน เพื่อป้องกันการสูญหาย ปีละ ๑ ครั้ง
๖	กำหนดแนวทางการใช้งานระบบเครือข่าย โดยห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้ ๖.๑ การพนัน ๖.๒ การวิพากษ์ วิจารณ์ ที่เกี่ยวข้องกับ ชาติ ศาสนา และพระมหากษัตริย์ ๖.๓ สิ่งลามก อนาจาร ๖.๔ สิ่งผิดกฎหมาย ผิดศีลธรรม หรือผิดจริยธรรม ๖.๕ ห้ามเล่นเกมส์ ดูภาพยนต์ หรือฟังเพลง ผ่านระบบเครือข่ายในเวลาราชการ

๓. ระเบียบปฏิบัติสำหรับการจัดการกับเอกสารที่เกี่ยวข้องกับระบบ

ผู้รับผิดชอบ : งานพัฒนาเทคโนโลยีสารสนเทศ

ที่	ระเบียบปฏิบัติ
๑	จัดทำและปรับปรุงคู่มือการปฏิบัติงานให้มีความทันสมัย และจัดเก็บไว้ในสถานที่ปลอดภัย มีเนื้อหาครอบคลุมระบบงาน เครื่อง server และอุปกรณ์ที่มีความสำคัญ เช่น คู่มือระบบงานต่างๆ ทั้งในส่วนของผู้ใช้งานและผู้ดูแลระบบ คู่มือการตรวจสอบสถานะของ server และระบบเครือข่าย คู่มือการตรวจสอบระบบและอุปกรณ์ต่างๆ ในห้องเครื่อง คู่มือการสำรองข้อมูล คู่มือการตรวจสอบทรัพยากรของระบบ เป็นต้น
๒	จำกัดการเข้าถึงคู่มือการปฏิบัติงานเฉพาะทีมงานที่มีความเกี่ยวข้องเท่านั้น
๓	หากจัดเก็บคู่มือการปฏิบัติงานไว้บนระบบเครือข่าย ต้องป้องกันการเข้าถึงข้อมูล โดยกำหนดรหัสผ่านให้เข้าถึงได้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น

๔. ระเบียบปฏิบัติสำหรับการจัดการระบบเครือข่าย

ผู้รับผิดชอบ : งานพัฒนาเทคโนโลยีและสารสนเทศ

ที่	ระเบียบปฏิบัติ
๑	ปรับปรุงผังระบบเครือข่ายให้มีความทันสมัย อย่างน้อยปีละ ๑ ครั้ง
๒	จัดแบ่ง และปรับปรุงระบบเครือข่ายออกเป็นกลุ่มๆ ตามลักษณะการใช้งาน และ ระบบงานที่มีความสำคัญ
๓	จำกัดการเชื่อมต่อไปยังเครื่อง server ระบบงาน หรืออุปกรณ์ที่มีความสำคัญ โดยกำหนดให้เครื่องคอมพิวเตอร์ที่สามารถเชื่อมต่อได้จะต้องเป็นเครื่องที่มาจากเครื่องของผู้ดูแลระบบเท่านั้น
๔	ปิดบริการบนเครื่อง server ที่ไม่มีความจำเป็นในการใช้งาน
๕	ติดตั้ง Patch แบบอัตโนมัติ บนเครื่องคอมพิวเตอร์ส่วนบุคคลของผู้ใช้งานทั้งหมดของกอง

๕. ระเบียบปฏิบัติสำหรับการจัดการการลาออกหรือย้ายหน่วยงานของบุคลากร

ผู้รับผิดชอบ : งานพัฒนาเทคโนโลยีสารสนเทศ

ที่	ระเบียบปฏิบัติ
๑	ถอดถอนสิทธิของผู้ที่ลาออกหรือย้ายหน่วยงานออกจากระบบต่างๆทั้งหมด โดยทันทีที่ได้รับแจ้งจากงานการเจ้าหน้าที่ กลุ่มบริหารทั่วไป

๖. ระเบียบปฏิบัติสำหรับการจัดการไวรัส

ผู้รับผิดชอบ : งานพัฒนาเทคโนโลยีสารสนเทศ

ที่	ระเบียบปฏิบัติ
๑	ตรวจสอบการทำงานของโปรแกรม Anti-virus และการปรับปรุงฐานข้อมูลไวรัส (Virus signature) อย่างสม่ำเสมอ หากพบว่าทำงานผิดปกติ ให้รีบดำเนินการแก้ไข
๒	ติดตั้งโปรแกรมป้องกันไวรัสให้กับผู้ใช้งานเพื่อให้ทำงานในลักษณะทันทีทันใด (Realtime Scan) เมื่อมีการเปิดไฟล์ขึ้นมาใช้งาน
๓	ติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยกับเครื่องคอมพิวเตอร์ทุกเครื่อง

๗. ระเบียบปฏิบัติสำหรับการสำรองข้อมูล

ผู้รับผิดชอบ : ผู้ที่ได้รับมอบหมายจากกลุ่มงาน/สำนักงาน (งานพัฒนาเทคโนโลยีสารสนเทศ)

ที่	ระเบียบปฏิบัติ
๑	กำหนดชนิดของข้อมูลบนระบบงานที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้
๒	กำหนดความถี่ในการสำรองข้อมูลของระบบงานดังกล่าว
๓	สำรองข้อมูลตามความถี่ที่กำหนดไว้ และควรนำข้อมูลที่สำรองไว้นั้น ไปเก็บนอกสถานที่ อย่างน้อย ๑ ชุด
๔	บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา/ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
๕	จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
๖	จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๘. ระเบียบปฏิบัติในการลงทะเบียนและควบคุมการเข้าถึงระบบ

ผู้รับผิดชอบ : งานพัฒนาเทคโนโลยีสารสนเทศ

ที่	ระเบียบปฏิบัติ
๑	ลงทะเบียนผู้ใช้งานใหม่ และกำหนดสิทธิของผู้ใช้งานควรให้สิทธิการใช้งานตามความจำเป็น
๒	ทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง ทำบันทึกการทบทวนและ จัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง
๓	ทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งาน (สำหรับหน่วยงานภายนอก) อย่างน้อยปีละ ๑ ครั้ง ทำบันทึกการทบทวนและจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง
๔	จัดส่งบัญชีผู้ใช้งานและรหัสผ่าน โดยใส่ซองปิดผนึก และประทับตรา “ลับ” และส่งให้ผู้ใช้งาน พร้อมแนบเอกสาร “ระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์ และ ระบบเครือข่าย” รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด

๙. ระเบียบปฏิบัติในการพัฒนาระบบงาน

ผู้รับผิดชอบ : คณะทำงานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กองโรคติดต่อทั่วไป

ที่	ระเบียบปฏิบัติ
๑	ทดสอบระบบงานใหม่โดยผู้ใช้งานที่เกี่ยวข้องให้ครอบคลุมตามข้อกำหนดที่ระบุไว้ใน TOR เมื่อตรวจรับแล้วจึงจะเปิดให้บริการระบบงานนั้นได้
๒	กำหนดมาตรฐานการเข้ารหัสข้อมูลของระบบงานสำคัญที่มีการรับส่งระหว่างเครื่องลูกข่ายกับเครื่อง server และกำหนดให้พัฒนาระบบตามมาตรฐานนี้
๓	รวบรวมและจัดเก็บ source code ของระบบงานทั้งหมดไว้ในสถานที่เดียวกันที่มีความปลอดภัย และควบคุมให้มี version ของ source code อย่างน้อย ๒ versions ล่าสุดและกำหนดให้ผู้ที่เกี่ยวข้องเท่านั้นที่สามารถเข้าถึงได้
๔	จัดการอบรมสำหรับระบบงานใหม่ให้แก่ผู้ใช้งานทั้งหมดที่เกี่ยวข้อง
๕	จัดทำคู่มือการใช้งานสำหรับระบบงานใหม่อย่างน้อยสำหรับผู้ใช้งานและผู้ดูแลระบบ

๑๐. ระเบียบปฏิบัติสำหรับการป้องกันไวรัส

ผู้รับผิดชอบ : บุคลากรกองโรคติดต่อทั่วไปทุกระดับที่ครอบครอง/ใช้งานเครื่องคอมพิวเตอร์ของกอง

ที่	ระเบียบปฏิบัติ
๑	ตรวจสอบว่าโปรแกรมป้องกันไวรัสยังทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ต้องทำการตรวจสอบอย่างน้อยวันละ ๑ ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบแจ้งงานพัฒนาเทคโนโลยีสารสนเทศ เพื่อดำเนินการแก้ไขโดยทันที
๒	Scan Virus ที่ Removable Drive ทุกครั้งที่มีการเชื่อมต่อ
๓	กรณีพบ Virus แต่โปรแกรม Anti Virus ไม่สามารถกำจัดได้ ให้รีบแจ้งงานพัฒนาเทคโนโลยีสารสนเทศดำเนินการทันที หากยังไม่สามารถกำจัดได้ให้งานพัฒนาเทคโนโลยีสารสนเทศ ประสาน/แจ้งกองดิจิทัลเพื่อการควบคุมโรค ดำเนินการแก้ไขต่อไป

๑๑. การควบคุมการใช้จดหมายอิเล็กทรอนกส์ (E-mail)

ผู้รับผิดชอบ : บุคลากรกองโรคติดต่อทั่วไปทุกระดับที่ครอบครอง/ใช้งานเครื่องคอมพิวเตอร์ของกอง

ที่	ระเบียบปฏิบัติ
๑	ห้ามมิให้เข้าถึงข้อมูล E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต
๒	ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)
๓	ห้ามส่ง E-mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)
๔	ห้ามส่ง E-mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น
๕	ห้ามส่ง E-mail ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา
๖	ห้ามปลอมแปลง E-mail ของบุคคลอื่น
๗	ห้ามส่ง E-mail ที่เป็นความลับของกอง เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูล E-mail ที่กองกำหนดไว้
๘	ให้ระบุชื่อของผู้ส่งใน E-mail ทุกฉบับที่ส่งไป
๙	ให้ทำการสำรองข้อมูล E-mail ตามความจำเป็นอย่างสม่ำเสมอ
๑๐	ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่าน หรือรับ หรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-mail) ของตน
๑๑	หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง
๑๒	ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนการเปิดเพื่อตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น
๑๓	ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
๑๔	ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุดและควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์
๑๕	ข้อควรระวังผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือ จดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

๑๒. การใช้งานเครื่องคอมพิวเตอร์ชนิดพกพา (Notebook)

ผู้รับผิดชอบ : บุคลากรกองโรคติดต่อทั่วไปทุกระดับ และงานพัฒนาเทคโนโลยีสารสนเทศ

ที่	ระเบียบปฏิบัติ
๑	เครื่องคอมพิวเตอร์ชนิดพกพา (Notebook) ที่ใช้ร่วมกัน ให้ทำการกรอกแบบฟอร์มยืม/คืน เพื่อขออนุมัติการนำไปใช้งาน และป้องกันการสูญหาย
๒	ตรวจสอบอย่างสม่ำเสมอว่าโปรแกรมป้องกันไวรัสที่ใช้งานอยู่ได้รับการปรับปรุงฐานข้อมูลและรูปแบบไวรัสอย่างสม่ำเสมอ
๓	ระมัดระวังและรักษาเครื่องคอมพิวเตอรชนิดพกพา (Notebook) เมื่อมีการนำไปใช้งานนอกสถานที่ เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
๔	เมื่ออยู่ในที่สาธารณะหรือในห้องประชุม ห้ามทิ้งเครื่องไว้โดยไม่มีผู้ดูแล
๕	ตั้งค่า Screen Saver เพื่อล็อกหน้าจออัตโนมัติ หากไม่ใช้งานเกินกว่า ๑๕ นาที
๖	เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานราชการ
๗	ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ
๘	ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม
๙	ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับ เครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น
๑๐	หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้
๑๑	ไม่วางของทับบนหน้าจอและแป้นพิมพ์
๑๒	การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้
๑๓	การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
๑๔	ผู้ใช้งานต้องไม่ใช้ข้อความที่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมหรือข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์ การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
๑๕	ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย
๑๖	ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

๑๓. ระเบียบปฏิบัติสำหรับการนำข้อมูลเผยแพร่สู่สาธารณะ

ผู้รับผิดชอบ : กลุ่มงาน/สำนักงาน เจ้าของข้อมูลที่เผยแพร่

ที่	ระเบียบปฏิบัติ
๑	กลุ่มงาน/สำนักงาน ที่เป็นเจ้าของข้อมูลที่ต้องการเผยแพร่สู่สาธารณะผ่านเว็บไซต์ของกอง ต้องทำการตรวจสอบความถูกต้องของข้อมูลก่อน หากมีความผิดพลาดเกิดขึ้นกับเนื้อหาจะต้องรับผิดชอบต่อความผิดพลาดนั้น
๒	ให้ผู้ที่ได้รับมอบหมายในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะผ่านเว็บไซต์ของกองจะต้องดำเนินการด้วยตนเอง ห้ามมิให้ผู้อื่นดำเนินการแทน

ผู้เสนอแผน

(นางวิรงรอง แก้วสมบูรณ์)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
หัวหน้ากลุ่มยุทธศาสตร์และพัฒนาองค์กร
วันที่ ๒๓ มีนาคม พ.ศ. ๒๕๖๖

ผู้อนุมัติ

(นายวิชาญ บุญกิติกร)
ผู้อำนวยการกองโรคติดต่อทั่วไป
วันที่ ๒๔ มีนาคม พ.ศ. ๒๕๖๖

ประกาศกรมควบคุมโรค

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมควบคุมโรค เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กรมควบคุมโรค และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น

ฉะนั้นอาศัยอำนาจตามความในมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ อธิบดีกรมควบคุมโรค จึงออกประกาศไว้ ดังนี้

๑. ประกาศนี้เรียกว่า "ประกาศกรมควบคุมโรค เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ"

๒. บรรดาประกาศและคำสั่งอื่นใดในส่วนที่กำหนดไว้แล้ว ซึ่งขัด หรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

๓. ประกาศนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ ลูกจ้างประจำ พนักงานราชการ และลูกจ้างชั่วคราว สังกัดกรมควบคุมโรค ที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศของกรมควบคุมโรค และบุคคลภายนอกที่เข้ามาใช้บริการระบบสารสนเทศของกรมควบคุมโรค รวมถึงหน่วยงานภายนอก ที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศของกรมควบคุมโรค

๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมควบคุมโรค มีวัตถุประสงค์ ดังต่อไปนี้

๔.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานสารสนเทศของกรมควบคุมโรค ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานของกรมควบคุมโรค ได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๔.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมควบคุมโรคตระหนักถึงความสำคัญของการรักษาความมั่นคงสารสนเทศในการใช้งานด้านสารสนเทศของกรมควบคุมโรค เพื่อปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละ ๑ ครั้ง

๕. นโยบาย...

๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมควบคุมโรค กำหนดประเด็นสำคัญดังต่อไปนี้

๕.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๕.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๕.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๕.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่กระทรวงสาธารณสุขจัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งโซน (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๕.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

๕.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๕.๒ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่องและมีเสถียรภาพ ต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญเรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๕.๓ ต้องตรวจสอบ...

๕.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้ผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๒ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๖. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูงจะกำหนดบทลงโทษแก่บุคลากรผู้ปฏิบัติงานนั้น โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๗. ให้ใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมควบคุมโรค ตามแนบท้ายประกาศนี้

๘. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๓๑ มกราคม พ.ศ. ๒๕๖๖

(นายธเรศ กรัษนัยรวิวงค์)
อธิบดีกรมควบคุมโรค