ระเบียบปฏิบัติด้านความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ

สำนักงานปลัดกระทรวงสาธารณสุข

ระเบียบปฏิบัติสำหรับการบริหารจัดการ ด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ

ระเบียบปฏิบัติสำหรับการบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
ผู้รับผิดชอบ : คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์

ที่	ระเบียบปฏิบัติ
1.	จัดให้มีการทำ และปรับปรุงนโยบายด้านความมั่นคงปลอดภัยอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
2.	แสดงเจตนารมณ์ หรือสื่อสารให้เจ้าหน้าที่ทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยขององค์กรโดยเคร่งครัด อย่างสม่ำเสมอ
3.	จัดให้มีการประชุมเกี่ยวกับการบริหารจัดการด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง โดยกำหนดให้มีวาระการประชุมที่ต้องหารือกันอย่างน้อยดังนี้ - การตรวจสอบการปฏิบัติตามนโยบายความมั่นคงฯ และผลการตรวจสอบ - แผนการดำเนินการเชิงป้องกัน/แก้ไข จากผลการตรวจสอบดังกล่าว - การปรับปรุงนโยบายความมั่นคงปลอดภัยสำหรับปีถัดไป - การประเมินความเสี่ยงและแผนลดความเสี่ยง รวมทั้งจัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่เพียงพอต่อการจัดการดังกล่าว
4.	จัดให้มีการสร้างความตระหนักทางด้านความมั่นคงปลอดภัยเพื่อให้เจ้าหน้าที่ขององค์กร มีความรู้ความเข้าใจ และสามารถป้องกันตนเองได้ในเบื้องต้น อย่างน้อยปีละ 1 ครั้ง
5.	จัดให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศ ปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อลดความเสี่ยง หรือปัญหาที่พบ
6.	จัดให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัย โดยผู้ตรวจสอบภายในด้านสารสนเทศ ปีละ 1 ครั้ง และจัดให้มีการทำแผนเพื่อปรับปรุง หรือแก้ไขปัญหาที่พบ
7.	จัดให้มีการแจ้งเวียนให้เจ้าหน้าที่ทั้งหมดได้ระมัดระวัง และดูแลทรัพย์สินขององค์กรที่ตนเองใช้งาน เพื่อป้องกันการสูญหาย อย่างน้อยปีละ 1 ครั้ง
8.	กำหนดนโยบายการใช้งานระบบเครือข่ายอย่างชัดเจนว่า บริการใดที่อนุญาตให้ใช้งาน และบริการใดไม่อนุญาตให้ใช้งาน เช่น การใช้งาน MSN ดูหนังฟังเพลงผ่านทางอินเตอร์เน็ต เป็นต้น รวมทั้งปรับปรุงนโยบายตามความจำเป็น **นโยบายการใช้งานระบบเครือข่าย** ขณะนี้ประกอบด้วย ▪ ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้ - การพนัน - วิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และ พระมหากษัตริย์ - ลามก อนาจาร - อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ผิดศีลธรรม หรือผิดจริยธรรม ▪ ห้ามเล่นเกมส์ ดูภาพยนต์ หรือฟังเพลง ผ่านทางอินเทอร์เน็ตในเวลาทำงาน

ระเบียบปฏิบัติสำหรับการบริหารจัดการคอมพิวเตอร์และระบบเครือข่าย

ระเบียบปฏิบัติสำหรับการจัดการกับเอกสารที่เกี่ยวข้องกับระบบ

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย และ/หรือ ผู้พัฒนาระบบ

ที่	ระเบียบปฏิบัติ
1	จัดทำ และ ปรับปรุงคู่มือการปฏิบัติงานให้มีความทันสมัย รวมทั้งให้จัดเก็บไว้ในสถานที่ที่มีความปลอดภัยอย่างน้อยให้ครอบคลุมระบบงาน เครื่องเซิร์ฟเวอร์ และอุปกรณ์ที่มีความสำคัญ ดังนี้ o คู่มือระบบงานต่างๆ ทั้งในส่วนของผู้ใช้งาน และผู้ดูแลระบบ o คู่มือการตรวจสอบสถานะของเซิร์ฟเวอร์ และระบบเครือข่าย o คู่มือการตรวจสอบระบบและอุปกรณ์ต่างๆ ในห้องเครื่อง o คู่มือการสำรองข้อมูล o คู่มือการตรวจสอบทรัพยากรของระบบ
2	ให้จำกัดการเข้าถึงคู่มือการปฏิบัติงานเฉพาะทีมงานที่มีความเกี่ยวข้องเท่านั้น
3	หากมีการจัดเก็บคู่มือการปฏิบัติงานไว้บนระบบเครือข่าย จัดให้มีการป้องกันการเข้าถึงเพื่อให้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น

ระเบียบปฏิบัติสำหรับการจัดการระบบเครือข่าย

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ
1	ปรับปรุงผังเครือข่ายให้มีความทันสมัย อย่างน้อยปีละ 1 ครั้ง
2	จัดแบ่ง และปรับปรุงระบบเครือข่ายออกเป็นกลุ่ม ๆ ตามลักษณะการใช้งาน เช่น แบ่งตามกลุ่มเครื่องเซิร์ฟเวอร์ เครื่องลูกข่าย และ ระบบงานที่มีความสำคัญ
3	จำกัดการเชื่อมต่อไปยังเครื่องเซิร์ฟเวอร์ ระบบงาน หรืออุปกรณ์ที่มีความสำคัญ โดยจะต้องกำหนดให้เครื่องคอมพิวเตอร์ที่สามารถเชื่อมต่อได้จะต้องเป็นเครื่องที่มาจากเครื่องของผู้ดูแลระบบเท่านั้น
4	ปิดบริการบนเครื่องเซิร์ฟเวอร์ที่ไม่มีความจำเป็นในการใช้งาน
5	กำหนดให้ใช้โปรแกรมมาตรฐานที่มีการเข้ารหัสข้อมูลที่ใช้สำหรับการเชื่อมต่อจากภายในเครือข่ายเพื่อเข้าสู่เครื่องเซิร์ฟเวอร์ หรืออุปกรณ์เครือข่าย (กรมต้องกำหนดโปรแกรมนี้ขึ้นมา และ ใช้เป็นมาตรฐานเดียวกันในการเชื่อมต่อไปยังเครื่องเซิร์ฟเวอร์ หรืออุปกรณ์เครือข่าย)
6	กำหนดให้ใช้โปรแกรมมาตรฐานที่มีการเข้ารหัสข้อมูลที่ใช้สำหรับการเชื่อมต่อจากระยะไกลภายนอกองค์กรเข้ามาสู่เครือข่ายภายในองค์กร (สำนักงานปลัดกระทรวงสาธารณสุขต้องกำหนดโปรแกรมนี้ขึ้นมาและใช้เป็นมาตรฐานเดียวกันในการเชื่อมต่อจากภายนอกเข้ามา)
7	ติดตั้ง Patch แบบอัตโนมัติ บนเครื่องคอมพิวเตอร์ส่วนบุคคลของผู้ใช้งานทั้งหมดขององค์กร
8	ปรับแต่งไฟร์วอลล์เพื่อให้เป็นไปตาม**นโยบายการใช้งานระบบเครือข่าย**ที่ผู้บริหารได้กำหนดไว้

ระเบียบปฏิบัติสำหรับการจัดการการลาออกหรือย้ายหน่วยงานของเจ้าหน้าที่

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ
1	ถอดถอนสิทธิของผู้ที่ลาออกหรือย้ายหน่วยงานออกจากระบบต่างๆ ทั้งหมดโดยทันทีที่ได้รับแจ้งจากกองการเจ้าหน้าที่

ระเบียบปฏิบัติสำหรับการใช้งานห้องเครื่อง

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ
1	ห้ามนำบุคคลภายนอกเข้าไปในห้องเครื่องโดยไม่มีกิจที่จำเป็น
2	ห้ามใส่รองเท้าเข้าห้องเครื่อง
3	ห้ามนำอาหารและเครื่องดื่มเข้าไปในบริเวณห้องเครื่อง
4	ตรวจสอบประตูทางเข้า-ออก และหน้าต่างของห้องเครื่องให้ปิดล็อคอยู่เสมอ
5	ตรวจสอบสภาพการทำงานของอุปกรณ์สนับสนุนการทำงานของระบบคอมพิวเตอร์ ได้แก่ ▪ ระบบกระแสไฟฟ้า ▪ ระบบการควบคุมความชื้น ▪ ระบบการระบายอากาศ ▪ ระบบการปรับอุณหภูมิ ▪ ระบบกระแสไฟฟ้าสำรอง ▪ ระบบ UPS ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ อย่างน้อยวันละ 1 ครั้ง ยกเว้นการตรวจสอบระบบกระแสไฟฟ้าสำรอง ให้ตรวจสอบเดือนละ 1 ครั้ง
6	จัดวางเครื่องคอมพิวเตอร์ อุปกรณ์สื่อสาร หรือทรัพย์สินอื่นๆ ไว้ในบริเวณที่มีความปลอดภัย ระมัดระวังการจัดตั้งอุปกรณ์ให้อยู่ในสภาพที่มั่นคงและไม่ล้มหรือโอนเอียงได้โดยง่าย

ที่	ระเบียบปฏิบัติ
7	ติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) เพิ่มเติมตามความจำเป็น เช่น ในกรณีที่เป็นมุมอับ รวมทั้งตรวจสอบการทำงานของกล้องให้มีการทำงานอย่างถูกต้อง ต่อเนื่องและให้สามารถเก็บภาพได้ในมุมกว้าง และไม่มีสิ่งกีดขวาง โดยบันทึกภาพล่าสุดไว้อย่างน้อย 1 เดือน
8	ตรวจสอบการทำงานของอุปกรณ์ดับเพลิงอย่างน้อยปีละ 1 ครั้ง ว่ายังใช้งานได้เป็นปกติหรือไม่
9	ให้ดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของห้องเครื่องอย่างสม่ำเสมอ ต้องไม่เก็บกล่องกระดาษหรือสิ่งที่จะเป็นเชื้อเพลิงไว้ในห้องเครื่อง
10	ตรวจสอบและจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย
11	ตรวจสอบห้องสายสัญญาณสื่อสารให้มีการปิดล็อกอยู่เสมอ
12	จัดทำหรือต่อสัญญาการบำรุงรักษาระบบงานสำคัญ ไฟร์วอลล์ เราท์เตอร์ อุปกรณ์ UPS สำหรับระบบงานสำคัญ และเครื่องปรับอากาศในห้องเครื่อง ให้ครบถ้วน
13	จัดให้ระบบงานสำคัญ เครื่องเซิร์ฟเวอร์ และอุปกรณ์ที่มีความสำคัญต้องมีอุปกรณ์ UPS และระบบกระแสไฟฟ้าสำรอง (electricity power generator) เพื่อสนับสนุนการทำงานอย่างครบถ้วน

ระเบียบปฏิบัติสำหรับการจัดการทรัพยากรของเครื่องเซิร์ฟเวอร์
ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ
1.	ดำเนินการตรวจสอบทรัพยากรของเซิร์ฟเวอร์สำหรับระบบงานสำคัญอย่างน้อยสัปดาห์ละ 1 ครั้ง สิ่งที่ควรตรวจสอบ ประกอบด้วย ปริมาณการใช้ CPU ปริมาณการใช้ฮาร์ดดิสก์ ปริมาณการใช้หน่วยความจำ และปริมาณการใช้เครือข่าย รวมทั้งควรมีการตรวจสอบการใช้งานเครือข่ายโดยภาพรวม (เช่น โดยการใช้โปรแกรม MRTG)
2.	บันทึกข้อมูลการใช้ทรัพยากรดังกล่าวไว้ด้วย (เพื่อใช้ในการตรวจสอบแนวโน้มการใช้ทรัพยากร รวมทั้งวางแผนจัดซื้อเพิ่มเติมตามความจำเป็นในอนาคต)
3.	ตั้งและหมั่นตรวจสอบสัญญาณนาฬิกาของเครื่องเซิร์ฟเวอร์ตามที่ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ระบุไว้ และของระบบงานสำคัญให้มีความถูกต้องอยู่เสมอ (โดยสามารถอ้างอิงเวลาได้จาก "clock.thaicert.org")

ระเบียบปฏิบัติสำหรับการจัดการไวรัส
ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ
1.	ตรวจสอบว่าเครื่องเซิร์ฟเวอร์ป้องกันไวรัสยังทำงานตามปกติ และมีการปรับปรุงฐานข้อมูลไวรัส (Virus signature) หรือไม่ ต้องทำการตรวจสอบอย่างน้อยวันละ 1 ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบดำเนินการแก้ไข (ข้อนี้จะใช้ได้กับองค์กรที่มีการใช้งานโปรแกรมป้องกันไวรัสแบบ Client/Server เท่านั้น)
2.	ทำการติดตั้งโปรแกรมป้องกันไวรัสให้กับผู้ใช้งานเพื่อให้ทำงานในลักษณะทันทีทันใด (Real-time Scan) เมื่อมีการเปิดไฟล์ขึ้นมาใช้งาน
3.	ทำการติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัย กับเครื่องลูกข่ายทั้งหมด เครื่องเซิร์ฟเวอร์สำหรับระบบงานสำคัญ และเครื่องเมล์เซิร์ฟเวอร์

แนวทางปฏิบัติสำหรับการสำรองข้อมูล

ผู้รับผิดชอบ : ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ผู้พัฒนาระบบและผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ
1	กำหนดรายชื่อของระบบงานสำคัญทั้งหมด และเมล์เซิร์ฟเวอร์
2	กำหนดรายชื่อของเซิร์ฟเวอร์ตามที่ พ.ร.บ.ฯ ได้กำหนดไว้ เช่น เว็บเซิร์ฟเวอร์ เป็นต้น
3	กำหนดผู้รับผิดชอบในการสำรองข้อมูล
4	กำหนดชนิดของข้อมูลบนระบบงานหรือบนเซิร์ฟเวอร์ดังกล่าวที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ อย่างน้อยต้องประกอบด้วย ▪ ข้อมูลในฐานข้อมูลของระบบงาน ▪ ข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการและซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง เป็นต้น ▪ ข้อมูลอีเมล์
5	กำหนดความถี่ในการสำรองข้อมูลของระบบงานหรือเซิร์ฟเวอร์ดังกล่าว
6	ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย 1 ชุด

ระเบียบปฏิบัติในการจัดเก็บข้อมูลล็อกตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ
1	จัดเก็บข้อมูลล็อกดังต่อไปนี้ เครื่องเซิร์ฟเวอร์ FTP (FTP.log), Mail (SMTP.log), Firewall/Proxy/Gateway (เช่น FW.log), Web (Access.log), RADIUS (RADIUS.log) หรือ TACACS+ (TACACS.log) อย่างน้อยเป็นระยะเวลา 90 วัน
2	จำกัดการเข้าถึงข้อมูลล็อกดังกล่าวโดยกำหนดให้เฉพาะผู้ดูแลระบบเครือข่ายเท่านั้นที่สามารถเข้าถึงได้

ระเบียบปฏิบัติในการลงทะเบียนและควบคุมการเข้าถึงระบบ

ผู้รับผิดชอบ : ผู้ดูแลระบบเครือข่าย และ ผู้พัฒนาระบบงาน

ที่	ระเบียบปฏิบัติ
1	กำหนดให้มีการลงทะเบียนสำหรับผู้ใช้งานใหม่ตาม "**แบบฟอร์มสำหรับลงทะเบียนผู้ใช้งาน**" และกำหนดสิทธิของผู้ใช้งานตามที่ระบุไว้ในแบบฟอร์มฯ แต่ควรให้สิทธิความจำเป็นในการใช้งานเท่านั้น
2	ให้ทำการทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งาน สำหรับเจ้าหน้าที่ของสำนักงานปลัดกระทรวงสาธารณสุข อย่างน้อยปีละ 1 ครั้ง และให้ทำบันทึกการทบทวนดังกล่าว และจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง
3	ให้ทำการทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งาน สำหรับหน่วยงานภายนอก อย่างน้อยปีละ 1 ครั้ง และให้ทำบันทึกการทบทวนดังกล่าว และจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง
4	ให้ทำการจัดส่งบัญชีผู้ใช้งานและรหัสผ่าน โดยใส่ซองปิดผนึก และประทับตรา "ลับ" และส่งไปยังผู้ใช้งาน และแนบเอกสาร "**ระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์ และระบบเครือข่าย**" รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด

ระเบียบปฏิบัติในการพัฒนาระบบงาน

ผู้รับผิดชอบ : ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และ/หรือ ผู้พัฒนาระบบงาน และ/หรือ ผู้ดูแลระบบเครือข่าย

ที่	ระเบียบปฏิบัติ
1	จัดให้มีการตรวจรับและทดสอบระบบงานใหม่โดยผู้ใช้งานที่เกี่ยวข้องให้ครอบคลุมตามข้อกำหนดที่ระบุไว้ใน TOR จนกระทั่งการตรวจรับเสร็จสิ้น จึงจะเปิดให้บริการระบบงานนั้นได้
2	สำหรับระบบงานสำคัญ ให้กำหนดมาตรฐานการเข้ารหัสข้อมูลที่มีการรับ-ส่งระหว่างเครื่องลูกข่ายกับเครื่องเซิร์ฟเวอร์ และกำหนดให้พัฒนาระบบตามมาตรฐานนี้
3	แสดงข้อความเตือนที่หน้าจอภายหลังจากการล็อกอินเสร็จสิ้น ข้อความเตือนดังกล่าว ได้แก่ *"ระบบนี้เป็นระบบที่เป็นทรัพย์สินของสำนักงานปลัดกระทรวงสาธารณสุข การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้นจึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงานหากมีการตรวจพบอาจมีการลงโทษทางวินัย หรือดำเนินการทางกฎหมายตามความเหมาะสม นอกจากนั้นแล้วสำนักงานปลัดกระทรวงสาธารณสุขมีสิทธิในการตรวจสอบพฤติกรรมการใช้งานในระหว่างที่ผู้ใช้ใช้ระบบงานนี้"*
4	พัฒนาระบบงานตาม**แนวทางในการตรวจสอบข้อมูลนำเข้า (Guideline for Input Validation)**
5	ทำการทดสอบระบบงาน และบันทึกผลการทดสอบเก็บไว้เป็นลายลักษณ์อักษรตาม**แนวทางในการตรวจสอบข้อมูลนำเข้า (Input Validation Guideline)**
6	พัฒนาระบบงานเพื่อให้สามารถกำหนดรหัสผ่านที่มีความเข้มแข็งตาม**ระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน**
7	รวบรวมและจัดเก็บซอร์สโค้ดของระบบงานทั้งหมดไว้ในสถานที่เดียวกันที่มีความปลอดภัย และควบคุมให้มีเวอร์ชันของซอร์สโค้ด อย่างน้อย 2 เวอร์ชันล่าสุดและกำหนดให้ผู้ที่เกี่ยวข้องเท่านั้นจึงจะสามารถเข้าถึงได้
8	จัดให้มีการอบรมสำหรับระบบงานใหม่ให้แก่ผู้ใช้งานทั้งหมดที่เกี่ยวข้อง
9	จัดทำคู่มือการใช้งานสำหรับระบบงานใหม่อย่างน้อยสำหรับผู้ใช้งาน และผู้ดูแลระบบ

แนวทางในการตรวจสอบข้อมูลนำเข้า (Guideline for input validation)

ผู้รับผิดชอบ : ผู้พัฒนาระบบ

ที่	ระเบียบปฏิบัติ
1	ปฏิบัติตามแนวทางในการตรวจสอบข้อมูลนำเข้าดังนี้ เพื่อป้องกันข้อมูลนำเข้ามีความผิดพลาด o ตรวจสอบข้อมูลนำเข้าให้ตรงกับชนิดของข้อมูลของตัวแปรของโปรแกรม o ตรวจสอบข้อมูลนำเข้าให้อยู่ภายในช่วงของค่าของตัวแปรของโปรแกรม o ตรวจสอบข้อมูลนำเข้าให้อยู่ภายในค่าขอบเขตบนและล่างของตัวแปรของโปรแกรม o ตรวจสอบข้อมูลนำเข้าเพื่อป้องกันไม่ให้อยู่นอกช่วงของค่าที่กำหนดไว้ o ตรวจสอบข้อมูลนำเข้าเพื่อป้องกันข้อมูลขาดหายหรือไม่ครบถ้วน o ตรวจสอบข้อมูลนำเข้าเพื่อป้องกันการใส่ตัวอักษรไม่ถูกต้อง o ตรวจสอบข้อมูลนำเข้าเพื่อป้องกันการลืมใส่ค่าคีย์หรือไม่ให้คีย์มีความซ้ำซ้อนกัน o ตรวจสอบข้อมูลนำเข้าเพื่อป้องกันการใส่ตัวอักษรพิเศษต่างๆ

ระเบียบปฏิบัติสำหรับการใช้งานคอมพิวเตอร์และระบบเครือข่าย

ระเบียบปฏิบัติสำหรับการใช้งานเครื่องคอมพิวเตอร์และเครือข่ายอย่างเหมาะสม
ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข

ที่	ระเบียบปฏิบัติ
1	ให้ผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นในกรณีที่ทำเครื่องให้ชำรุดหรือสูญหายไปโดยประมาทหรือเลินเล่อ
2	ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 3 ชั่วโมง
3	ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า 15 นาที
4	ระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคล และระบบเครือข่ายเหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งานทรัพย์สินของตนเอง
5	ห้ามเจ้าหน้าที่ทั่วไปติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย
6	ห้ามเจ้าหน้าที่ทั่วไปติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในระบบเครือข่ายขององค์กร เพื่อให้บุคคลอื่นสามารถเข้าถึงหรือเชื่อมต่อเพื่อเข้าสู่ระบบเครือข่ายขององค์กร
7	ต้องขออนุมัติจากทางฝ่ายอาคารหรือผู้มีอำนาจ ในกรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกสำนักงาน
8	ให้ออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

ระเบียบปฏิบัติสำหรับการป้องกันไวรัส
ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข

ที่	ระเบียบปฏิบัติ
1.	ตรวจสอบว่าโปรแกรมป้องกันไวรัสยังทำงานตามปกติและมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ ต้องทำการตรวจสอบอย่างน้อยวันละ 1 ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบแจ้งเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศเพื่อดำเนินการแก้ไขโดยทันที
2.	หากเครื่องของผู้ใช้งานยังไม่มีโปรแกรมตรวจสอบไวรัสให้ดาวน์โหลดโปรแกรมTrendMicro OfficeScan และคู่มือการติดตั้งที่ http://www.moph.go.th/download/
3.	Scan Virus ที่ Removable Drive ทุกครั้งที่มีการเชื่อมต่อ
4.	กรณีพบ Virus แต่โปรแกรม Anti Virus ไม่สามารถกำจัดได้ ให้รีบแจ้งคณะทำงานของหน่วยงานดำเนินการทันที หากยังไม่สามารถกำจัดได้ ให้คณะทำงานของหน่วยงานแจ้งศูนย์เทคโนโลยีสารสนเทศ ฯ โดยใช้แบบแจ้งซ่อมครุภัณฑ์คอมพิวเตอร์ เพื่อดำเนินการแก้ไขต่อไป

ระเบียบปฏิบัติสำหรับการป้องกันการละเมิดลิขสิทธิ์และสิทธิทางปัญญา
ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข

ที่	ระเบียบปฏิบัติ
1.	ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น
2.	ระมัดระวังการใช้งานเอกสารหรือข้อมูลต่างๆ ซึ่งอยู่ในรูปแบบใดก็ตาม และได้มีการกำหนดเงื่อนไขการใช้งานเอาไว้ ต้องปฏิบัติตามเงื่อนไขดังกล่าวอย่างเคร่งครัด เพื่อไม่ให้เป็นการละเมิดทรัพย์สินทางปัญญาของบุคคลอื่น

ระเบียบปฏิบัติสำหรับการใช้งานอินเทอร์เน็ต

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข

ที่	ระเบียบปฏิบัติ
1.	ห้ามทำการดาวน์โหลด หรือส่งไฟล์ประเภทสื่อลามก อนาจาร
2.	ห้ามเล่นเกมส์ ดูภาพยนต์ หรือฟังเพลง ผ่านทางอินเทอร์เน็ตในเวลาทำงาน
3.	ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้ -การพนัน -วิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และ พระมหากษัตริย์ -ลามก อนาจาร -อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ผิดศีลธรรม หรือผิดจริยธรรม
4.	ห้ามใช้งานข้อมูลที่ได้รับโดยผ่านทางอินเทอร์เน็ตที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของข้อมูลนั้น
5.	ห้ามใช้อินเทอร์เน็ตเพื่อส่ง กระจาย หรือแจกจ่าย ดังต่อไปนี้ -ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต -ข้อมูลที่เป็นความลับขององค์กรไปยังบุคคลที่ไม่ได้รับอนุญาต
6.	ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงขององค์กร

ระเบียบปฏิบัติสำหรับการใช้งานอีเมล์

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข

ที่	ระเบียบปฏิบัติ
1	ห้ามมิให้เข้าถึงข้อมูลอีเมล์ของบุคคลอื่นโดยไม่ได้รับอนุญาต
2	ห้ามลงทะเบียนด้วย E-mail Address ที่องค์กรมอบให้ไว้ตามที่อยู่เว็บไซต์ต่างๆ ที่ไม่เกี่ยวข้องกับงานขององค์กร
3	ห้ามทำการส่งอีเมล์ที่เกี่ยวข้องกับงานขององค์กรด้วย E-mail Address อื่นที่นอกเหนือจากที่องค์กรจัดให้
4	ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)
5	ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)
6	ห้ามส่งอีเมล์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น
7	ห้ามส่งอีเมล์ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา
8	ห้ามปลอมแปลงอีเมล์ของบุคคลอื่น
9	ห้ามรับ หรือส่งอีเมล์แทนบุคคลอื่นโดยไม่ได้รับอนุญาต
10	ห้ามส่งอีเมล์ที่มีขนาดใหญ่เกินกว่า 8 เมกกะไบต์ หรือตามที่องค์กรระบุไว้
11	ห้ามส่งอีเมล์ที่เป็นความลับขององค์กร เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลอีเมล์ที่องค์กรกำหนดไว้
12	ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่อีเมล์ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ
13	ให้ใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับอีเมล์เท่าที่มีความจำเป็นต้องรับรู้รับทราบในข้อมูลที่ส่งไป
14	ให้ใช้คำที่สุภาพในการส่งอีเมล์
15	ให้ระบุชื่อของผู้ส่งในอีเมล์ทุกฉบับที่ส่งไป
16	ให้ทำการสำรองข้อมูลอีเมล์ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าองค์กรจะทำการสำรองข้อมูลอีเมล์ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้นอีเมล์ที่เก่ามากๆ และจำเป็นต้องใช้งานจึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

ระเบียบปฏิบัติสำหรับการป้องกันการใช้ทรัพยากรผิดวัตถุประสงค์

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข

ที่	ระเบียบปฏิบัติ
เจ้าหน้าที่จะต้องไม่ใช้ระบบเครือข่าย โดยมีวัตถุประสงค์ดังต่อไปนี้	
1	เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
2	เพื่อการกระทำที่ขัดต่อ พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
3	เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
4	เพื่อการค้าขาย หรือผลประโยชน์ส่วนตัว หรือผลประโยชน์ทางการเมือง
5	เพื่อการเข้าถึง แสดง จัดเก็บ แจกจ่าย แก้ไข จัดทำ หรือบันทึกข้อมูลที่มีเนื้อหาไม่เหมาะสม เช่น ข้อมูลอันเป็นเท็จ ข้อมูลที่มีผลต่อความมั่นคงของสถาบันชาติ ศาสนาและพระมหากษัตริย์ ภาพลามกอนาจาร ภาพตัดต่อของบุคคลอื่น หรือข้อมูลที่ก่อให้เกิดความเสื่อมเสียอับอายแก่องค์กรหรือบุคคลอื่น เป็นต้น
6	เพื่อทำการเผยแพร่ข้อมูล หรืออนุญาตให้ผู้อื่นเผยแพร่ข้อมูลเพื่อการกล่าวร้าย หมิ่นประมาท หรือพาดพิง บุคคลอื่น จนทำให้องค์กรถูกฟ้องร้องหรือก่อให้เกิดความเสียหายแก่องค์กร
7	เพื่อการเปิดเผยข้อมูลลับซึ่งได้มาจากการปฏิบัติงานให้แก่องค์กร ไม่ว่าจะเป็นข้อมูลขององค์กรหรือบุคคลภายนอก ก็ตาม
8	เพื่อขัดขวางหรือโจมตี การใช้งานระบบเครือข่ายขององค์กร หรือของหน่วยงานภายนอกอื่น
9	เพื่อแพร่กระจายไวรัส หนอน ม้าโทรจัน สปายแวร์ สแปมเมล์ หรือโปรแกรมไม่ประสงค์ดีอื่นๆ
10	เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กรไปยังที่อยู่เว็บ หรือห้องสนทนาใดๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง
11	เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายต่อองค์กร

ระเบียบปฏิบัติสำหรับการใช้งานเครื่องคอมพิวเตอร์โน้ตบุ๊ก

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข

ที่	ระเบียบปฏิบัติ
1	ในกรณีที่เป็นเครื่องโน้ตบุ๊คที่ใช้ร่วมกันให้ทำการกรอก**แบบฟอร์มยืม-คืนสำหรับเครื่องคอมพิวเตอร์โน้ตบุ๊ค**นั้น เพื่อขออนุมัติการนำไปใช้งาน และป้องกันการสูญหาย
2	ตรวจสอบอย่างสม่ำเสมอว่าโปรแกรมป้องกันไวรัสที่ใช้งานอยู่ได้รับการปรับปรุงฐานข้อมูลรูปแบบไวรัสอย่างสม่ำเสมอ
3	ให้ระมัดระวังและรักษาเครื่องคอมพิวเตอร์โน้ตบุ๊คเมื่อมีการนำไปใช้งานนอกสถานที่ เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
4	เมื่ออยู่ในที่สาธารณะหรือในห้องประชุม ห้ามปล่อยเครื่องทิ้งไว้โดยไม่มีผู้ดูแล
5	ตรวจสอบว่าได้มีการตั้งค่า Screen Saver เพื่อให้ทำการล็อกหน้าจอโดยอัตโนมัติหลังจากที่ไม่ได้ใช้งานเกินกว่า 15 นาที

ระเบียบปฏิบัติสำหรับการกำหนดและป้องกันรหัสผ่าน

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข

ที่	ระเบียบปฏิบัติ
1	เก็บรักษารหัสผ่านของตนเองไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น
2	กำหนดรหัสผ่านให้มีคุณสมบัติ ตาม**ระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน**
3	กำหนดรหัสผ่านสำหรับการใช้ไฟล์ข้อมูลร่วมกันบนเครือข่าย
4	ห้ามบันทึกรหัสผ่านไว้ในโปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำรหัสผ่านของตน (เช่น ในโปรแกรมเว็บบราวเซอร์จะสามารถเลือกให้โปรแกรมช่วยจำรหัสผ่านไว้ให้)
5	ต้องไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น
6	ในกรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเพื่อให้สามารถปฏิบัติงานแทนตนเองได้ หลังจากที่ทำงานนั้นเสร็จเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

ระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข

ที่	ระเบียบปฏิบัติ
	กำหนดรหัสผ่านให้มีคุณสมบัติ ดังต่อไปนี้
1	มีความยาวไม่น้อยกว่า 6 ตัวอักษร ยกเว้นระบบเก่าๆ ที่ไม่สามารถดำเนินการได้
2	มีการผสมผสานกันระหว่างตัวอักษรที่เป็นตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน
3	ไม่กำหนดรหัสผ่านจากคำศัพท์ที่ปรากฏในพจนานุกรม
4	เปลี่ยนรหัสผ่านทุกๆ 6 เดือนสำหรับเจ้าหน้าที่ทั่วไปและทุกๆ 3 เดือนสำหรับเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ

ระเบียบปฏิบัติสำหรับการใช้งานห้องเครื่อง

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข

ที่	ระเบียบปฏิบัติ
1	ห้ามเจ้าหน้าที่เข้าไปในบริเวณห้องเครื่องโดยไม่มีกิจที่เกี่ยวข้อง
2	ห้ามใส่รองเท้าเข้าห้องเครื่อง
3	หากพบเห็นความผิดปกติในห้องเครื่อง เช่น มีทรัพย์สินหาย มีร่องรอยการบุกรุก เป็นต้น ให้รีบแจ้งเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ
4	ให้ปฏิบัติตามคำแนะนำของเจ้าหน้าที่ที่ดูแลห้องเครื่องอย่างเคร่งครัด

ระเบียบปฏิบัติสำหรับการลงทะเบียนเข้าใช้ระบบงาน

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข

ที่	ระเบียบปฏิบัติ
1	เมื่อเจ้าหน้าที่ใหม่เข้ามาปฏิบัติหน้าที่ ให้กรอกแบบฟอร์มเพื่อขออนุมัติใช้งานระบบงาน ตามแบบฟอร์มลงทะเบียนผู้ใช้งาน และนำเสนอต่อผู้บังคับบัญชาเพื่อขอการอนุมัติ
2	ห้ามเจ้าหน้าที่ใหม่ใช้ระบบงานขององค์กรจนกว่าจะได้รับการอนุมัติให้ใช้งานโดยผ่านการลงทะเบียนก่อน

ระเบียบปฏิบัติสำหรับการจัดซื้อจัดจ้างทางด้าน ICT

ผู้รับผิดชอบ : เจ้าหน้าที่ทั้งหมดของสำนักงานปลัดกระทรวงสาธารณสุข

ที่	ระเบียบปฏิบัติ
1	ในการจัดซื้อจัดจ้างที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ให้ทำเรื่องผ่านทางศูนย์เทคโนโลยีสารสนเทศเพื่อดูความเข้ากันได้กับโครงสร้างพื้นฐานสารสนเทศขององค์กร และความเหมาะสมในการใช้งาน ก่อนการจัดซื้อจัดจ้าง

ระเบียบปฏิบัติสำหรับการนำข้อมูลเผยแพร่สู่สาธารณะ

ระเบียบปฏิบัติสำหรับการนำข้อมูลเผยแพร่สู่สาธารณะ
ผู้รับผิดชอบ : ผู้รับผิดชอบข้อมูลที่ต้องนำเผยแพร่สู่สาธารณะ

ที่	ระเบียบปฏิบัติ
1.	ให้ผู้ที่เป็นเจ้าของข้อมูลที่ต้องการนำข้อมูลนั้นขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ของสำนักงานปลัดกระทรวงสาธารณสุข จะต้องทำการตรวจสอบความถูกต้องของข้อมูลก่อน หากมีความผิดพลาดเกิดขึ้นกับเนื้อหาจะต้องรับผิดชอบต่อความผิดพลาดนั้น
2.	ให้ผู้ที่มีหน้าที่รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ของสำนักงานปลัดกระทรวงสาธารณสุขจะต้องดำเนินการด้วยตนเอง โดยห้ามมิให้ผู้อื่นดำเนินการแทน

ผู้ทบทวน : .....

นายสินชัย ต่อวัฒนกิจกุล

(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)

ผู้อนุมัติ : .....

นายศิริวัฒน์ ทิพย์ธราดล
(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กระทรวงสาธารณสุข)
4 ก.ย. 52