นโยบายความมั่นคงปลอดภัย

ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ICT Security Policy

ฉบับ ปี พ.ศ.2564

โรงพยาบาลชุมแสง

หมวดที่ ๑

การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และ การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

(Business Requirements For Access Control)

วัตถุประสงค์

เพื่อให้บุคลากรโรงพยาบาลชุมแสง และบุคคลภายนอก ให้มีความรู้ ความเข้าใจและสามารถปฏิบัติตามแนวทางปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements For Access Control) พร้อมทั้งตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศ

นโยบาย

บุคลากรโรงพยาบาลชุมแสง และบุคคลภายนอกต้องให้ความสำคัญและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยเฉพาะการเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูล ให้คำนึงถึงการใช้งาน และความมั่นคงปลอดภัย ดังนี้

๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ และการใช้งานตามภารกิจเพื่อควบคุมการ เข้าถึงสารสนเทศ ต้องสอดคล้อง และเป็นไปตามคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ

๑.๒ เจ้าของระบบมีหน้าที่ในการอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศให้กับผู้ใช้งาน

๑.๓ ผู้ดูแลระบบมีหน้าที่กำหนดสิทธิให้แก่ผู้ใช้งานตามที่เจ้าของระบบอนุมัติ

๑.๔ ผู้ดูแลระบบมีหน้าที่ในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน สำหรับการเข้าระบบคอมพิวเตอร์และระบบสารสนเทศ ตลอดจนควบคุม การใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบสารสนเทศ

๑.๕ ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามสิทธิที่ได้รับเท่านั้น

๑.๖ เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบสารสนเทศ ต้องแจ้งเหตุผลความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจจากเจ้าของระบบ และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหาย บุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

๑.๗ การเข้าถึงห้องศูนย์ข้อมูล (Data Center) ให้ดำเนินการ ดังนี้

๑.๗.๑ กลุ่มเทคโนโลยีสารสนเทศต้องกำหนดข้อปฏิบัติสำหรับการปฏิบัติงานในห้องศูนย์ข้อมูล (Data Center)

๑.๗.๒ การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใด ๆ ออกจากห้องศูนย์ข้อมูล (Data Center) ต้องได้รับอนุมัติจากผู้อำนวยการโรงพยาบาลชุมแสง

๑.๗.๓ ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์ข้อมูล (Data Center) เว้นแต่ได้รับ อนุญาตจากผู้ได้รับมอบหมายดูแลห้องศูนย์ข้อมูล (Data Center)

๑.๗.๔ ห้ามนำอาหาร เครื่องดื่ม เข้ามาในห้องศูนย์ข้อมูล (Data Center)

๑.๗.๕ ห้ามถ่ายรูป อุปกรณ์ภายในห้องศูนย์ข้อมูล (Data Center) ก่อนได้รับอนุญาต จากผู้ได้รับมอบหมายดูแลห้องศูนย์ข้อมูล (Data Center)

๒. การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ กำหนด ดังนี้

๒.๑ สิทธิของผู้ใช้งาน (User) ประกอบด้วย

๒.๑.๑ อ่านอย่างเดียว

๒.๑.๒ สร้างข้อมูล

๒.๑.๓ แก้ไขข้อมูล

๒.๑.๔ ลบข้อมูล

๒.๒ สิทธิผู้ดูแลระบบ (Administrator) กำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และบริหารจัดการระบบคอมพิวเตอร์และระบบสารสนเทศ

๓. การกำหนดประเภทของข้อมูล ลำดับความสำคัญ ลำดับชั้นความลับ รวมถึงระดับชั้น การเข้าถึง เวลาที่เข้าถึง และช่องทางการเข้าถึง ดังนี้

๓.๑ ประเภทของข้อมูล แบ่งเป็น ๓ ประเภท ดังนี้

๓.๑.๑ ข้อมูลสารสนเทศสำหรับการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร และข้อมูลงบประมาณรายจ่าย (SMART)

๓.๑.๒ ข้อมูลสารสนเทศสำหรับการสนับสนุนการปฏิบัติงาน ได้แก่ ข้อมูลระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ (GFMIS)

๓.๑.๓ ข้อมูลสารสนเทศสำหรับการเผยแพร่แก่ประชาชนทั่วไปและผู้ที่สนใจ ได้แก่ ข้อมูลในเว็บไซต์ของกรมสนับสนุนบริการสุขภาพ

๓.๒ ลำดับความสำคัญของข้อมูล แบ่งเป็น ๓ ระดับ ดังนี้

๓.๒.๑ สำคัญมากที่สุด

๓.๒.๒ สำคัญมาก

๓.๒.๓ ปกติ

๓.๓ ลำดับชั้นความลับของข้อมูล แบ่งเป็น ๔ ระดับ ดังนี้

๓.๓.๑ ลับที่สุด – ความลับที่มีความสำคัญที่สุด เกี่ยวกับข่าวสาร วัตถุหรือบุคคล ซึ่งถ้า หากความลับดังกล่าว ทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหาย หรือเป็นภยันตรายต่อความมั่นคงความปลอดภัย หรือความสงบเรียบร้อยของประเทศชาติ หรือพันธมิตร หรือการ ดำเนินงานของหน่วยงานที่เกี่ยวข้องอย่างร้ายแรงที่สุด

๓.๓.๒ ลับมาก - ความลับที่มีความสำคัญมาก เกี่ยวกับข่าวสาร วัตถุหรือบุคคล ซึ่งถ้าหาก ความลับดังกล่าว ทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล Pผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหาย หรือ เป็นภยันตรายต่อความมั่นคงความปลอดภัยของประเทศชาติหรือพันธมิตร หรือความสงบเรียบร้อยภายใน ราชอาณาจักร หรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้องได้อย่างร้ายแรง

๓.๓.๓ ลับ - ความลับที่มีความสำคัญเกี่ยวกับ ข่าวสาร วัตถุหรือบุคคล ซึ่งถ้าหาก ความลับดังกล่าว ทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหาย หรือเป็นภยันตรายต่อราชการ หรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้องได้

๓.๓.๔ ปกปิด – ความลับซึ่งไม่พึ่งเปิดเผยให้ผู้ไม่มีหน้าที่ได้ทราบ โดยสงวนไว้ให้ทราบ เฉพาะบุคคลที่มีหน้าที่ต้องทราบเพื่อประโยชน์ในการปฏิบัติภารกิจองค์กรเท่านั้น

๓.๔ ระดับชั้นการเข้าถึง แบ่งเป็น ๓ ระดับ ดังนี้

๓.๔.๑ กลุ่มผู้บริหาร

๓.๔.๒ กลุ่มผู้ปฏิบัติงาน

๓.๔.๓ กลุ่มประชาชนทั่วไปและผู้ที่สนใจ

๓.๕ เวลาที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ สามารถเข้าถึงได้ตลอด ๒๔ X ๗ วัน

๓.๖ ช่องทางการเข้าถึงสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ได้ ๒ ช่องทาง ดังนี้

๓.๖.๑ ระบบเครือข่ายภายใน (Intranet)

๓.๖.๒ ระบบเครือข่ายภายนอก (Internet)

๔. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Business Requirements For Access Control) ดังนี้

๔.๑ เจ้าของระบบอนุมัติสิทธิให้ผู้ใช้งาน ตามภารกิจเพื่อให้สามารถเข้าถึงระบบคอมพิวเตอร์และ ระบบสารสนเทศ เฉพาะในส่วนที่ได้รับมอบหมาย ตามความเป็นจำในการใช้งาน

๔.๒ ผู้ดูแลระบบกำหนดสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งาน ตามที่เจ้าของระบบอนุมัติ

หมวดที่ ๒
การบริหารจัดการเข้าถึงของผู้ใช้งาน
(User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศเฉพาะผู้ใช้งานที่ได้รับอนุญาตแล้ว และ สร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศและ ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดให้มีกระบวนการสำหรับการลงทะเบียนบุคลากรใหม่ (User Registration) เพื่อรับสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

๒. กำหนดกระบวนการสำหรับการยกเลิกสิทธิการใช้งานเมื่อไม่ได้ปฏิบัติงานที่กรมสนับสนุนบริการสุขภาพ

๓. กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุมโดยให้มีการควบคุม จำกัด และเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์ระบบสารสนเทศตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การลงทะเบียนผู้ใช้งาน ให้ดำเนินการ ดังนี้

๑.๑ ผู้รับผิดชอบด้านสารสนเทศของหน่วยงานต้องกำหนดแบบฟอร์มการขออนุญาตเข้าถึง ระบบคอมพิวเตอร์และระบบสารสนเทศ อย่างน้อยประกอบด้วยชื่อ นามสกุล ตำแหน่ง สังกัด และหมายเลข โทรศัพท์

๑.๒ การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้ดำเนินการ ดังนี้

๑.๒.๑ กรณีบุคลากรกรมสนับสนุนบริการสุขภาพ

(๑) ให้บุคลากรกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๒) ให้หน่วยงานส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้เจ้าของระบบที่ขอใช้งาน

(๓) ให้เจ้าของระบบอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิ ตามที่เจ้าของระบบอนุมัติ พร้อมทั้งแจ้งให้หน่วยงานเจ้าของบุคลากรรับทราบ

๑.๒.๒ กรณีบุคคลภายนอก

(๑) ให้บุคคลภายนอกกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ พร้อมระบุเหตุผลในการเข้าใช้งาน หรือหนังสือขอเข้าใช้งานจากบริษัท/หน่วยงานต้นสังกัด

(๒) ให้หน่วยงานพิจารณาเหตุผล และดำเนินการส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้เจ้าของระบบที่ขอใช้งาน

(๓) ให้เจ้าของระบบอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิตามที่เจ้าของระบบ อนุมัติพร้อมทั้งแจ้งให้หน่วยงานเจ้าของบุคลากรรับทราบ

๑.๓ การสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๑.๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้เจ้าของระบบ กำหนด เช่น ชื่อภาษาอังกฤษ หรือบัตรประจำตัวประชาชนตามด้วยเครื่องหมาย “ ” หรือ “ ” ตามด้วยอักษรนามสกุลตัวแรก หรือลักษณะอื่นใด ตามที่เจ้าของระบบ ที่มีการตกลงร่วมกัน

๑.๓.๒ การกำหนดรหัสผ่าน (Password) ชุดของตัวอักษรภาษาอังกฤษ ตัวเลข และอักขระพิเศษ อย่างน้อย 4 ตัวขึ้นไป และยากต่อการคาดเดา

๑.๓.๓ ให้ผู้ดูแลระบบ แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ผู้ใช้งาน ทราบโดยตรง

๑.๓.๔ เมื่อผู้ใช้งาน มีการเปลี่ยนข้อมูลให้แจ้งเจ้าของระบบ เพื่อปรับปรุงข้อมูลผู้ใช้งาน

๒. การยกเลิกสิทธิการใช้งานของบุคลากร หรือบุคคลภายนอกให้ดำเนินการ ดังนี้

๒.๑ ให้หน่วยงานแจ้งเจ้าของระบบ เพื่อขอยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของบุคลากร เมื่อมีการลาออก ให้โอน หรือสิ้นสุด การจ้าง

๒.๒ ผู้ดูแลระบบ จะดำเนินการปิดบัญชีผู้ใช้งาน (Username) และแจ้งกลับไปยังหน่วยงานรับทราบ

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้ใช้งาน ให้ดำเนินการ ดังนี้

๓.๑ ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้หน่วยงานแจ้งเจ้าของระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๓.๒ ในกรณีที่ผู้ใช้งาน ต้องการสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ที่สูง กว่าระดับสิทธิที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่อเจ้าของระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลง สิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ดำเนินการ ตามหลักเกณฑ์ ดังนี้

๔.๑ ในกรณีที่ผู้ใช้งาน ลืมรหัสผ่าน (Password) ให้ขอรับรหัสผ่านใหม่ วิธีการของเจ้าของระบบคอมพิวเตอร์และระบบสารสนเทศ กำหนด เช่น โทรศัพท์ หรือ ออนไลน์

๔.๒ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๑ ปี และรหัสผ่าน (Password) ใหม่ ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม

๕. ผู้ดูแลระบบ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสุดสิ้นการจ้าง เพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป และการรักษา ความมั่นคงปลอดภัย ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

หมวดที่ ๓
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดขอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงระบบ คอมพิวเตอร์และระบบสารสนเทศ โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลับลอบทำสำเนาข้อมูล สารสนเทศและการลักขโมยอุปกรณ์ในการประมวลผลข้อมูล (Process Device)

นโยบาย

๑. กำหนดแนวปฏิบัติในการใช้งานรหัสผ่าน (Password) และการเปลี่ยนรหัสผ่าน (Password)

๒. กำหนดแนวปฏิบัติในการป้องกันระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศในขณะที่ไม่มีผู้ใช้งาน (User) ดูแล

๓. กำหนดแนวปฏิบัติในการควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ได้แก่ เอกสาร สื่อบันทึกข้อมูล และข้อมูลสารสนเทศ เพื่อไม่ให้สินทรัพย์ (Asset) อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งาน (User) ออกจากระบบคอมพิวเตอร์และระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔. กำหนดให้ผู้ใช้งาน (User) อาจนำการเข้ารหัสข้อมูล (Encryption) มาใช้กับการรับส่งข้อมูล ที่สำคัญหรือข้อมูลที่เป็นความลับของกรมสนับสนุนบริการสุขภาพ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษา ความลับทางราชการ พ.ศ. ๒๕๕๔

แนวปฏิบัติ

๑. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้

๑.๑ ผู้ใช้งานต้องกำหนดรหัสผ่าน (Password) ตามหมวดที่ ๒ ข้อ ๑.๓ และต้องเปลี่ยนรหัสผ่าน ตาม ข้อ ๔.๒

๑.๒ ผู้ใช้งานต้องไม่ใช้รหัสผ่าน (Password) ร่วมกับบุคคลอื่น และไม่ควรให้ระบบคอมพิวเตอร์ หรือระบบสารสนเทศจำรหัสผ่าน (Password) ในการเข้าใช้งานโดยอัตโนมัติ

๑.๓ ผู้ใช้งานต้องไม่เปิดเผยรหัสผ่าน (Password) สำหรับการเข้าถึงระบบคอมพิวเตอร์ และ ระบบสารสนเทศให้บุคคลอื่นรับรู้ โดยเก็บเป็นความลับเสมือนเป็นสมบัติส่วนตัว ห้ามจดหรือเขียนรหัสผ่าน (Password) ที่ใช้งานไว้ในที่เปิดเผย

๑.๔ หากมีความจำเป็นต้องบอกรหัสผ่าน (Password) แก่บุคคลอื่นเนื่องจากความจำเป็นในการเข้าถึงหลังจากดำเนินการเสร็จสิ้นแล้วให้เปลี่ยนรหัสผ่าน (Password) ใหม่ทันที

๑.๕ หากมีการกระทำความผิดเกิดขึ้นจากบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องมีส่วนร่วมในการรับผิดชอบต่อการกระทำความผิดนั้น เว้นแต่เจ้าของ บัญชีผู้ใช้งาน (Username) ได้กระทำการป้องกันตามแนวปฏิบัติที่กำหนดแล้ว

๒. ผู้ใช้งานต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศ

๓. การควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ (Clear Desk and Clear Screen Policy) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๓.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงอุปกรณ์ในการประมวลผลข้อมูล (Process Device) มีวัตถุประสงค์เพื่อใช้ในการปฏิบัติงานของกรมสนับสนุนบริการสุขภาพเท่านั้น

๓.๒ ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ (Asset) ของกรมสนับสนุนบริการสุขภาพ และให้ใช้ งานด้วยความระมัดระวังเสมือนเป็นทรัพย์สินส่วนตน

๓.๓ ผู้ใช้งานต้องไม่ดัดแปลงหรือไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ใด ๆ ที่เครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์พกพา หรือระบบคอมพิวเตอร์และระบบสารสนเทศ ในกรณีที่มีความจำเป็นในการใช้งาน เพิ่มเติม ให้แจ้งความประสงค์พร้อมเหตุผลต่อผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัด

๓.๔ ผู้ใช้งานต้องใช้ความระมัดระวังในการบันทึกข้อมูลสารสนเทศไว้ในอุปกรณ์บันทึกข้อมูล แบบพกพา หรือการ์ดความจำในโทรศัพท์มือถือ เพื่อป้องกันการรั่วไหลของข้อมูล

๓.๕ บุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานด้านสารสนเทศ ต้องขออนุมัติเป็นลายลักษณ์อักษรก่อนเข้าปฏิบัติงาน

๓.๖ การทำลายอุปกรณ์บันทึกข้อมูลหรือการนำอุปกรณ์บันทึกข้อมูลกลับมาใช้งานใหม่ให้ดำเนินการ ดังนี้

๓.๖.๑ การทำลายอุปกรณ์บันทึกข้อมูล เช่น Flash Drive CD/DVD ฮาร์ดดิสก์ เทป เป็นต้น ให้ใช้วิธีการทุบ หรือบดให้เสียหาย หรือเผาทำลายด้วยวิธีการทำลายตามมาตรฐานสากล หรือตามที่ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

๓.๖.๒ การนำอุปกรณ์บันทึกข้อมูลไปใช้งานใหม่ ให้ฟอร์แมต (Format) อุปกรณ์บันทึกข้อมูลนั้นโดยใช้วิธีการฟอร์แมต (Format) ตามมาตรฐานสากล หรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

หมวดที่ ๔
การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายให้มีความมั่นคงปลอดภัย นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงเครือข่ายของผู้ใช้งาน (User) เฉพาะที่ได้รับอนุญาตให้เข้าถึง

๒. กำหนดแนวปฏิบัติในการยืนยันตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections) โดยต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาต ให้ผู้ใช้งานที่อยู่ภายนอกองค์กร สามารถใช้งานเครือข่าย ระบบคอมพิวเตอร์และระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพได้

๓. กำหนดแนวปฏิบัติในการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) โดย ต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และต้องใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๔. กำหนดแนวปฏิบัติในการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) โดยต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕. กำหนดแนวปฏิบัติในการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) โดยต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน

5. กำหนดแนวปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศและการส่งข้อมูล สารสนเทศสอดคล้องกับแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) และการ ใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

แนวปฏิบัติ

๑ การเข้าถึงเครือข่ายของผู้ใช้งาน

๑.๑ การใช้งานระบบเครือข่ายภายนอก (Internet) ให้ดำเนินการ ดังนี้

๑.๑.๑ กำหนดให้ใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง สำหรับเข้าใช้งานระบบเครือข่ายภายนอก (Internet)

๑.๑.๒ ห้ามใช้งานระบบเครือข่ายภายนอก (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) สูงที่ไม่เกี่ยวข้องกับการปฏิบัติหน้าที่ราชการ ได้แก่ รายการบันเทิงต่าง ๆ ในเวลาราชการ

๑.๑.๓ ห้ามเข้าชมเว็บไซต์ที่ไม่เหมาะสม ได้แก่ เว็บไซต์ที่ขัดศีลธรรม ลามกอนาจาร เว็บไซต์ที่มีเนื้อหาที่ทำให้สถาบันชาติ ศาสนา และพระมหากษัตริย์เสื่อมเสีย

๑.๑.๔ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของกรมสนับสนุนบริการสุขภาพ เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๑.๕ ต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พระราชบัญญัติการ รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยเคร่งครัด

๑.๑.๖ ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่างๆ เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบคอมพิวเตอร์และระบบสารสนเทศ โดยแจ้งให้ผู้ดูแลระบบสารสนเทศของหน่วยงานต้นสังกัดทราบก่อนติดตั้งใช้งาน

๑.๒ การใช้งานจดหมายอิเล็กทรอนิกส์ (E – Mail) โดเมนเนม (Domain Name) ของกรมสนับสนุนบริการสุขภาพ (@hss.mail.go.th) ให้ดำเนินการ ดังนี้

๑.๒.๑ ห้ามใช้งานจดหมายอิเล็กทรอนิกส์ (E - Mail) ในทางที่ไม่ถูกต้อง ผิดกฎหมาย ละเมิดศีลธรรม

๑.๒.๒ ต้องไม่แสวงหาผลประโยชน์หรือให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจด้วยการ ใช้งานจดหมายอิเล็กทรอนิกส์ (E – Mail) ที่ส่งโดยโดเมนเนม (Domain Name) ของกรมสนับสนุนบริการสุขภาพ

๑.๒.๓ ต้องตรวจสอบชื่อผู้ส่งจดหมายอิเล็กทรอนิกส์ (Sender) ก่อนเปิดจดหมายอิเล็กทรอนิกส์ (E - Mail) เพื่อป้องกันการเปิดไฟล์อันตรายที่อาจมีไวรัสคอมพิวเตอร์ โดยเฉพาะ Executable File ได้แก่ ไฟล์ที่มีนามสกุล .exe, .Com, bat และ inf ที่อาจนำเข้าสู่ระบบเครือข่ายกรมสนับสนุนบริการสุขภาพ

๑.๒.๔ หลักจากการใช้งานจดหมายอิเล็กทรอนิกส์ (E – Mail) ต้องออกจากระบบ (LogOut) ทันที ๑.๓ การใช้งานเครือข่ายไร้สาย (WiFi) ให้ดำเนินการ ดังนี้

๑.๓.๑ ผู้ดูแลระบบต้องทำการเปลี่ยนค่า Service Set Identifier (SSID) ที่ถูกกำหนดเป็นค่ามาตรฐานมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณแบบไร้สาย (Access Point) มาติดตั้งเพื่อใช้งาน

๑.๓.๒ ผู้ใช้งานต้องใช้ชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ที่เป็น ของตนเองในการพิสูจน์ตัวตน (Authentication) เพื่อเข้าใช้งานเครือข่ายไร้สาย (WiFi)

๑.๓.๓ ผู้ใช้งานต้องไม่นำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ ที่เป็น ทรัพย์สินของกรมสนับสนุนบริการสุขภาพไปใช้งานเครือข่ายไร้สาย (WiFi) ที่ไม่น่าเชื่อถือ

๑.๓.๔ ผู้ใช้งานไม่ควรทำธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ระหว่างการใช้งานเครือข่ายไร้สาย (WiFi) เนื่องจากอาจเกิดความไม่ปลอดภัยและอาจขาดการเชื่อมต่อของสัญญาณ

๑.๓.๕ ห้ามผู้ใช้งานติดตั้งและเปิดการทำงานโปรแกรมดักจับข้อมูล (Network Snifer) เพราะอาจเกิดความเสียหายต่อระบบเครือข่ายไร้สายของกรมสนับสนุนบริการสุขภาพ และมี

ความผิด ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑.๔ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้

๑.๔.๑ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ภายใต้ หน่วยงานของกรมสนับสนุนบริการสุขภาพ ควรนำเสนอเกี่ยวกับภารกิจงานของหน่วยงาน เช่น ผลการดำเนินงาน และข่าวสาร โดยการนำเข้าข้อมูลต้องเป็นผู้ที่ได้รับมอบหมายจากหน่วยงาน และต้องตามพระราชบัญญัติว่าด้วยการ กระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑.๔.๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับของกรมสนับสนุนบริการสุขภาพผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๔.๓ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงต่อไป

๑.๔.๔ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากกรมสนับสนุน บริการสุขภาพ และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๑.๔.๕ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งาน ต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที

๒. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ให้ดำเนินการ ดังนี้

๒.๑ ผู้รับผิดชอบด้านสารสนเทศของหน่วยงานต้องจัดทำผังระบบเครือข่าย (Network Diagram) พร้อมรายละเอียดอุปกรณ์บนเครือข่ายที่เห็นว่าจำเป็นต่อการใช้งาน ได้แก่ กลุ่มอุปกรณ์ เลขที่อยู่ไอพี (IP Address) และหมายเลขเฉพาะอุปกรณ์ (MAC Address) โดยให้ปรับปรุงทุก ๒ ปี หรือตามความเหมาะสม

๒.๒ การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ มาใช้งานบนเครือข่ายต้องได้รับ อนุญาตจากผู้รับผิดชอบด้านสารสนเทศของหน่วยงาน

๓. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) ให้ดำเนินการ ดังนี้

๓.๑ กลุ่มเทคโนโลยีสารสนเทศมีดูแล/ตรวจสอบ พอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnostic and Configuration Port Protection) รวมทั้งการควบคุมการเข้าถึงพอร์ตทางกายภาพและเครือข่าย

๓.๒ กลุ่มเทคโนโลยีสารสนเทศต้องเปิดใช้งานเฉพาะพอร์ตที่จำเป็นสำหรับการใช้งานเท่านั้น และต้องตรวจสอบพอร์ตที่เปิดให้บริการ อย่างน้อยปีละ ๑ ครั้ง

๔. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ให้ดำเนินการ ดังนี้

๔.๑ กลุ่มเทคโนโลยีสารสนเทศต้องติดตั้งระบบป้องกันการบุกรุกโจมตีทางเครือข่าย (Firewall) เพื่อใช้เป็นจุดควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

๔.๒ ผู้ดูแลระบบต้องไม่เปิดเผยข้อมูลการเชื่อมต่อทางเครือข่าย ก่อนได้รับอนุญาตจากกลุ่ม เทคโนโลยีสารสนเทศ

๔.๓ ผู้ดูแลระบบมีหน้าที่ในการควบคุมการเชื่อมต่อสัญญาณหรือยกเลิก การเชื่อมต่อสัญญาณ ตามที่ได้รับอนุญาตจากกลุ่มเทคโนโลยีสารสนเทศ ทั้งนี้ หากพบข้อผิดพลาดหรือเห็นว่า หมดความจำเป็นในการ เชื่อมต่อสัญญาณให้รายงานกลุ่มเทคโนโลยีสารสนเทศทันที

๔.๔ การเชื่อมต่อเครือข่ายสารสนเทศระหว่างกรมสนับสนุนบริการสุขภาพ กับหน่วยงานภายนอก ต้องได้รับอนุญาตจากอธิบดีและเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ของผู้ให้บริการที่มีความน่าเชื่อถือ

๕. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ให้ดำเนินการ ดังนี้

๕.๑ ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อระบบคอมพิวเตอร์และระบบสารสนเทศเป็นไปอย่างมีประสิทธิภาพ และการรับ – ส่ง หรือ การไหลเวียนของข้อมูลหรือสารสนเทศเป็นไปอย่างรวดเร็ว

๕.๒ ผู้ดูแลระบบต้องเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ของผู้ใช้งานเป็นระยะเวลาไม่ น้อยกว่า ๙๐ วัน ความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

หมวดที่ ๕

การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกัน การเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงระบบปฏิบัติการโดยต้องมีการควบคุมการเข้าถึงด้วยวิธีการยืนยัน ตัวตนที่ปลอดภัย

๒. กำหนดแนวปฏิบัติใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) โดยควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการ ความมั่นคงปลอดภัยที่ได้กำหนดไว้

แนวปฏิบัติ

๑. ผู้ใช้งานต้องใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง สำหรับเข้าถึงระบบปฏิบัติการ

๒. ผู้ใช้งานไม่มีสิทธิ์เปลี่ยนแปลงแก้ไขค่าต่าง ๆ ของระบบปฏิบัติการ เช่น

๒.๑ Product Key หรือ License ของระบบปฏิบัติการ

๒.๒ ค่าคอนฟิกกูเรชั่น (Configuration) ต่าง ๆ เช่น Computer Name, IP Address เป็นต้น ๓. การจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) กำหนด ดังนี้

๓.๑ ผู้ใช้งานต้องไม่ดัดแปลงหรือติดตั้งโปรแกรมอรรถประโยชน์ใด ๆ บนระบบปฏิบัติการ ทั้งนี้ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติม ให้แจ้งความประสงค์ต่อผู้รับผิดชอบด้านสารสนเทศของหน่วยงาน

๓.๒ การใช้งานโปรแกรมอรรถประโยชน์อื่น ๆ นอกเหนือจากที่ติดตั้งมากับระบบปฏิบัติการ เช่น โปรแกรมดักจับข้อมูล (Network Sniffer) โปรแกรมประเภทดักจับรหัสผ่าน (Password Sniffer) และ โปรแกรม Formatter กำหนดให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่มีสิทธิใช้งาน

หมวดที่ 6

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

(Application and Information Access Control)

วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application Information Access Control) โดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติสำหรับระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อกรมสนับสนุนบริการสุขภาพ โดยต้องได้รับการแยกออกจากระบบอื่นๆ และ มีการควบคุมสภาพแวดล้อมโดยเฉพาะ พร้อมทั้งให้มีการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสาร เคลื่อนที่ ที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking)

๒. กำหนดแนวปฏิบัติในการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยต้องกำหนด ข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศ จากความเสี่ยงของการใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๓. กำหนดแนวปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) โดยต้องกำหนด ข้อปฏิบัติแผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกสำนักงาน

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการดังนี้

๑.๑ ผู้ดูแลระบบ (Administrator) ต้องกำหนดให้ผู้ใช้งานที่เข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศผ่านเครือข่ายภายนอก ให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN)

๑.๒ การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) รายละเอียดปรากฏตามภาคผนวก

๒. ระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมสนับสนุนบริการสุขภาพให้ดำเนินการ ดังนี้

๒.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศ ซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ดังนี้

๒.๑.๑ ระบบการบริหารจัดการความมั่นคงปลอดภัยและเครือข่าย ได้แก่ ระบบ Antivirus ,ระบบ Backup System,ระบบ Domain Name Server,ระบบ Dynamic Host Configuration Protocol,ระบบ Network Management,ระบบ Network Monitoring และระบบจัดเก็บข้อมูลกลาง

๒.๑.๒ ระบบการบริหารการเงินการคลังภาครัฐสู่ระบบอิเล็กทรอนิกส์ (GFMIS)

๒.๒ ระบบคอมพิวเตอร์และระบบสารสนเทศ ซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อกรมสนับสนุนบริการสุขภาพ ต้องได้รับการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกออกจาก ระบบอื่นๆ

๒.๓ ผู้ดูแลระบบต้องแบ่งพื้นที่สำหรับการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายตามระดับความสำคัญและความปลอดภัยของระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อกรมสนับสนุนบริการสุขภาพ เพื่อควบคุมสภาพแวดล้อมโดยเฉพาะ

๒.๔. การใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing And Teleworking) เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศซึ่งไวต่อการ รบกวนมีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องเข้าถึงในสถานที่ที่มีความปลอดภัยและต้องได้รับอนุญาตจากกลุ่มเทคโนโลยีสารสนเทศ

๓. การควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ให้ดำเนินการ ดังนี้

๓.๑.๑ อุปกรณ์สื่อสารเคลื่อนที่ ได้แก่ Smart Phone และ Tablet ต้องได้รับการยืนยันตัว ตัน โดยใช้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของผู้ใช้งานสำหรับการเข้าใช้งาน

๔.การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) กำหนด ดังนี้

๔.๑ ผู้ใช้งานต้องปฏิบัติตามหมวด 5 แนวปฏิบัติ ข้อ ๑ การควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction)

๔.๒ เมื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศแล้ว ผู้ใช้งานต้องระมัดระวังไม่ให้ผู้ไม่มี ส่วนเกี่ยวข้องเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศจากเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ ได้และต้องออกจากระบบ (Log Out) ทันทีเมื่อปฏิบัติเลิกใช้งาน

หมวดที่ ๗

การจัดทำระบบสำรองของระบบสารสนเทศ

(Disaster Recovery Site)

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลสารสนเทศและการกู้คืนข้อมูลสารสนเทศและการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ ซึ่งได้รวมการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความ พร้อมฉุกเฉิน และการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ และการสำรองข้อมูลและกู้คืน ข้อมูลสารสนเทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่องแม่ในสภาวะวิกฤต หรือ เหตุการณ์ฉุกเฉินต่างๆ และสามารถกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสมและสามารถใช้งาน สารสนเทศได้อย่างต่อเนื่อง

นโยบาย

๑. พิจารณาคัดเลือกระบบสารสนเทศที่เหมาะสมในการจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน

๒. จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ เพื่อให้สามารถเข้าถึงสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้ อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ

แนวปฏิบัติ

๑. ผู้ดูแลระบบจะต้องจัดทำการสำรองของระบบสารสนเทศโดยมีขั้นตอน ดังนี้

๑.๑ ผู้ดูแลระบบจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูล และการกู้คืนข้อมูลสารสนเทศ

๑.๒ กำหนดรูปการสำรองข้อมูลระบบสารสนเทศ ดังนี้

๑.๒.๑ คัดเลือกระบบสารสนเทศในการสำรองข้อมูล

๑.๒.๒ กำหนดรูปแบบการสำรองข้อมูล เช่น เฉพาะส่วนที่มีการเพิ่มขึ้นมา (Incremental Backup) แบบสมบูรณ์ (Full Backup)

๑.๒.๓ กำหนดความถี่ในการสำรองข้อมูลตามความเหมาะสมของระบบสารสนเทศ

๑.๓ ผู้ดูแลระบบดำเนินการสำรองของระบบสารสนเทศ ตามข้อที่ ๑.๒

๒. ผู้ดูแลระบบต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศที่สำรองไว้ อย่างน้อย ๑ ระบบ โดยอย่างน้อยปีละ ๑ ครั้ง

๓. กลุ่มเทคโนโลยีสารสนเทศดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยกำหนดให้ปรับปรุงแผนดังกล่าวทุก ๑ ปี

๔. มีการทบทวนระบบสารสนเทศในการระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ 8

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(Risk Assessment and Risk Management)

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยด้านสารสนเทศ ทำให้มั่นใจว่านโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่กำหนด มีความมั่นคงปลอดภัย และ หน่วยงานสามารถปฏิบัติตามได้อย่างมีประสิทธิภาพ

นโยบาย

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒.การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสียงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

แนวปฏิบัติ

๑. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒. กำหนดให้มีผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๒.๑ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศประจำปีงบประมาณ ให้ดำเนินการ โดยกลุ่มตรวจสอบภายใน (Internal Auditor)

๒.๒ หากมีความประสงค์ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศเชิงเทคนิค ให้ดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

3. กำหนดแนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๓.๑ ผู้ตรวจสอบต้องจัดการทำรายงานพร้อมข้อเสนอแนะในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๒ กลุ่มเทคโนโลยีสารสนเทศต้องอำนวยความสะดวกแก่ผู้ตรวจสอบในการตรวจสอบข้อมูลที่สำคัญ

๓.๓ ในกรณีที่ผู้ตรวจสอบจำเป็นต้องเข้าถึงข้อมูลสำคัญให้กลุ่มเทคโนโลยีสารสนเทศ สร้างสำเนาสำหรับข้อมูลนั้น โดยให้ผู้ตรวจสอบใช้งานและทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือหากประสงค์จัดเก็บข้อมูลนั้นเป็นหลักฐานให้แจ้งกลุ่มเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๓.๔ ในกรณีการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบประเมินความเสี่ยงระบบคอมพิวเตอร์และระบบสารสนเทศ ให้แยกการติดตั้งเครื่องมือออกจากระบบที่ให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว (Read Only)

๓.๕ ผู้ตรวจสอบต้องแจ้งความเสี่ยงและระบุความรุนแรงของเครื่องมือที่ใช้ในการตรวจสอบและประเมินความเสี่ยง

หมวดที่ ๙

การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

(Information Security Incident Management)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการดำเนินการ อย่างถูกต้อง มีประสิทธิภาพในช่วงระยะเวลาที่เหมาะสม

แนวทางปฏิบัติ

๑. จัดให้มีขั้นตอนหรือกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศที่สำคัญ รวมทั้งกำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถ และประสบการณ์ โดยขั้นมีการกำหนดขั้นตอนและกระบวนการดังต่อไปนี้

๑.๑ การกำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร

๑.๒ การประเมินเหตุการณ์หรือจุดอ่อนของมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และพิจารณาว่าควรจัดเป็นเหตุการณ์และมีระดับความรุนแรงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ

๑.๓ จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ และรายงานเหตุการณ์ ผู้ที่เกี่ยวข้อง ให้ทราบและดำเนินการต่อไป

๑.๔ การดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ เพื่อทำให้เหตุการณ์ คลี่คลายหรือกลับสู่ภาวะปกติ

๑.๕ วิเคราะห์ รวบรวมและรายงานเหตุการณ์ต่อผู้บังคับบัญชาทราบ ทั้งนี้ เพื่อระบุถึงสาเหตุการณ์ และเพื่อใช้ประโยชน์จากผลการวิเคราะห์ในการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้อีกในอนาคต

๒. ต้องจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ ผ่านบุคคล หรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์ (point of contact) โดยให้ดำเนินการดังนี้

๒.๑ แจ้งผู้บังคับบัญชา โดยช่องทางใดช่องทางหนึ่งที่รวดเร็วและทันต่อเหตุการณ์ เช่น Social Network, E-mail เป็นต้น ทั้งนี้ เนื้อหาขั้นต่ำ ต้องประกอบด้วย วันเวลา เหตุการณ์ ผลกระทบที่คาดว่าจะเกิดขึ้น

๒.๒ รายงานผู้บังคับบัญชาเมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย เช่น - การบุกรุกด้านกายภาพ - การปฏิบัติงานที่ไม่เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ - การเปลี่ยนแปลง การเข้าถึงโดยไม่ได้รับอนุญาต - การทำงานผิดของโปรแกรมและอุปกรณ์คอมพิวเตอร์ หรือการปฏิบัติงาน

จัดให้มีบุคคลหรือหน่วยงานงาน (point of contact) เพื่อทำหน้าที่รายงานเหตุการณ์ที่เกิดขึ้นต่อผู้บังคับบัญชา โดยให้รายงานดังต่อไปนี้

รายงานทันทีเมื่อเกิดเหตุ	ระหว่างดำเนินการแก้ไข	แก้ไขปัญหาได้ และเหตุยุติ
1.วันเวลาที่เกิดเหตุการณ์ 2. ระบบที่เกิดเหตุรายละเอียดและ สาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้น 4. ชื่อผู้ติดต่อ/ประสานงานของบริษัทเพื่อให้ข้อมูล	1. วันเวลาที่เกิดเหตุการณ์ 2. ระบบที่เกิดเหตุรายละเอียดและ สาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้น 4. ดำเนินการแก้ไขปัญหาและระยะเวลาในการแก้ไข 5. ความคืบหน้าในการแก้ไขปัญหา	1. วันเวลาที่เกิดเหตุการณ์ 2. ระบบที่เกิดเหตุรายละเอียดและ สาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้นโดย ประเมินมูลค่าความเสียหาย 4. ดำเนินการแก้ไขปัญหา 5. ผลการแก้ไขปัญหา และระยะเวลาในการแก้ไข 6. แนวทางป้องกันในอนาคตและการเก็บรวบรวมหลักฐานเพื่อระบุสาเหตุและแนวทางแก้ไขต่อไป

รายงานทันทีเมื่อเกิดเหตุ	ระหว่างดำเนินการแก้ไข	แก้ไขปัญหาได้ และเหตุยุติ
รายงานโดยไม่ชักช้า อาจแจ้งด้วยวาจาหรือช่องทางใดช่องทางหนึ่งที่รวดเร็วและทันต่อเหตุการณ์ เมื่อทราบเหตุการณ์และตรวจสอบในเบื้องต้นแล้ว	รายงานโดยไม่ชักช้า อาจแจ้งด้วยวาจาหรือช่องทางใดช่องทางหนึ่งที่รวดเร็วและทันต่อเหตุการณ์ เมื่อทราบเหตุการณ์และตรวจสอบในเบื้องต้นแล้ว	รายงานเป็นลายลักษณ์อักษรโดยมีเนื้อหาจากข้อมูลข้างต้น

ภาคผนวก

การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศของผู้รับจ้าง (Outsource)

เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศ ข้อมูลสารสนเทศ ศูนย์ข้อมูลและสารสนเทศ และพื้นที่ปฏิบัติงานทั่วไป ซึ่งเป็นทรัพย์สินที่มีค่าของกรมสนับสนุนบริการสุขภาพมีความปลอดภัยต่อการถูกบุกรุก โจมตีและลดความเสี่ยงต่อลักลอบเปิดเผยข้อมูลสารสนเทศ จึงกำหนดแนวปฏิบัติการควบคุมการเข้าถึง ระบบ คอมพิวเตอร์และระบบสารสนเทศของผู้รับจ้าง (Outsource) ดังนี้

๑. ก่อนปฏิบัติงาน

๑.๑ ผู้รับจ้าง (Outsource) ต้องขออนุญาตหัวหน้าส่วนราชการนั้น ๆ เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับบุคคลภายนอก ตามหมวดที่ ๒ ข้อปฏิบัติที่ ๑

๑.๒ หัวหน้าส่วนราชการหรือผู้ที่ได้รับมอบหมายพิจารณาเหตุผลการขออนุญาตดังกล่าวและต้องอนุมัติเป็นลายลักษณ์อักษร

๒. ระหว่างปฏิบัติงาน

๒.๑ ผู้รับจ้าง (Outsource) ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน

๒.๒ ผู้รับผิดชอบด้านสารสนเทศหรือผู้ที่ได้รับมอบหมายจากหัวหน้าส่วนราชการต้องกำกับดูแลการ ปฏิบัติงานของผู้รับจ้าง โดยเฉพาะการติดตั้ง ซ่อมแซม หรือการเปลี่ยนอุปกรณ์ประมวลผลข้อมูลภายในห้อง ศูนย์ข้อมูล (Data Center) ต้องกำกับดูแลโดยเคร่งครัด

๒.๓ ผู้รับจ้างต้องปฏิบัติตามหน้าที่ที่ได้รับมอบหมายเท่านั้นและต้องคำนึงถึงการรักษาความลับข้อมูล ของทางราชการเป็นสำคัญ หากเกิดปัญหาระหว่างการปฏิบัติงานให้แจ้งผู้รับผิดชอบด้านสารสนเทศหรือผู้ที่ ได้รับมอบหมายที่กำกับดูแลการปฏิบัติงานทันที

๓. หลังปฏิบัติงาน

๓.๑ ให้ผู้รับจ้างแจ้งความประสงค์ต่อผู้รับผิดชอบด้านสารสนเทศเพื่อยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศทันทีเมื่อปฏิบัติงานแล้วเสร็จ

๓.๒ ผู้ดูแลระบบ จะยกเลิกสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ และลบข้อมูลสารสนเทศของผู้รับจ้างเป็นการถาวรทันทีเมื่อสิ้นสุดการจ้างงานหรือข้อตกลงร่วมกัน

๔. การรักษาความลับ

ผู้รับจ้างต้องลงนามในสัญญาหรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลง ดังกล่าว ต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

ข้อปฏิบัติการเข้าใช้งานห้องศูนย์ข้อมูล (Data Center)

เพื่อให้การเข้าออกห้องศูนย์ข้อมูล (Data Center) เป็นไปด้วยความสะดวก เรียบร้อย มีความปลอดภัย จึงได้มีการกำหนดข้อปฏิบัติ ดังนี้

๑. บุคคลผู้มีสิทธิเข้าใช้งานห้องศูนย์ข้อมูล (Data Center) ประกอบด้วย

๑.๑ ผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) หมายถึง เจ้าหน้าที่ของกลุ่มเทคโนโลยีสารสนเทศที่ได้รับมอบหมายจากผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม ให้รับผิดชอบดูแลห้องศูนย์ข้อมูล (Data Center)

๑.๒ เจ้าหน้าที่ผู้รับผิดชอบห้องศูนย์ข้อมูล (Data Center) จากบริษัท หมายถึง เจ้าหน้าที่ของ บริษัท ที่ได้รับการผู้รับจ้างในการบำรุงรักษาเครือข่าย ห้องศูนย์ข้อมูล (Data Center) กรมสนับสนุนบริการสุขภาพ

๑.๓ บุคคลภายนอก หมายถึง ผู้ที่เข้ามาปฏิบัติงานตามภารกิจ โดยต้องการรับการอนุมัติจาก ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขานุการกรม

๒. การเข้าใช้งานห้องศูนย์ข้อมูล (Data Center) มีขั้นตอนดังนี้

๒.๑ ผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) เข้าใช้งานโดยการสแกนลายนิ้วมือ หรือรหัส การใช้งานของอุปกรณ์เปิด – ปิด ประตู หน้าห้องศูนย์ข้อมูล (Data Center)

๒.๒ เจ้าหน้าที่ผู้รับผิดชอบห้องศูนย์ข้อมูล (Data Center) จากบริษัท เข้าใช้งานโดยการสแกน ลายนิ้วมือ หรือรหัส การใช้งานของอุปกรณ์เปิด - ปิด ประตู หน้าห้องศูนย์ข้อมูล (Data Center) โดยได้รับ การอนุมัติการนำเข้าลายนิ้วมือจากได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center)

๒.๓ บุคคลภายนอกจะต้องทำเป็นหนังสือขอเข้าพื้นที่เป็นลายลักษณ์อักษรเท่านั้น โดยให้หนังสือจะต้องระบุ วัน เวลา ที่ชัดเจน จำนวน หรือรายชื่อบุคลากร พร้อมด้วยเหตุผลความจำเป็นโดยมีผู้ได้รับ มอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) เป็นผู้นำพาเข้าและควบคุมตลอดเวลา

๒.๔ บุคคลภายนอก ต้องลงทะเบียนเซ็นชื่อการเข้าในสมุดหน้าห้องทุกครั้ง และเมื่อเสร็จภารกิจต้องเซ็นชื่อออก ทุกครั้งเช่นกัน

๓. ระยะเวลาการเข้าใช้งานห้องศูนย์ข้อมูล (Data Center) มีรายละเอียด ดังนี้

๓.๑ วันและเวลาราชการ ๘.๓๐ - ๑๖.๓๐ น.

๓.๒ กรณีที่มีเหตุฉุกเฉิน หรือนอกวันและเวลาราชการ ที่มีความจำเป็นต้องเข้าห้องศูนย์ข้อมูล (Data Center) ให้แจ้งได้รับมอบหมายให้ผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center) ทราบ ถึงเหตุผลและความจำเป็นในการเข้าไปใช้งาน

๔. ห้ามนำอาหาร เครื่องดื่ม เข้ามาในห้องศูนย์ข้อมูล (Data Center)

๕. ห้ามถ่ายรูป อุปกรณ์ภายในห้องศูนย์ข้อมูล (Data Center) ก่อนได้รับอนุญาตจากผู้ได้รับมอบหมายดูแลห้องศูนย์ข้อมูล (Data Center)

๖. เมื่อเสร็จภารกิจให้ตรวจสอบความเรียบร้อยก่อนออกจากศูนย์ข้อมูล (Data Center) เช่น ไฟ ประตู

เจ้าหน้าที่ผู้ได้รับมอบหมายให้ดูแลห้องศูนย์ข้อมูล (Data Center)

อาคารโรงพยาบาลชุมแสง

ได้แก่

นายอารยะ เลขวัฒนะ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	เบอร์ 08 1628 0988
นางสาวนวนันท์ สัมพันธ์มิตร	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	เบอร์ 08 5381 2799