แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ Digital Health Platform กระทรวงสาธารณสุข (แพลตฟอร์มหมอพร้อม) พ.ศ. ๒๕๖๗

หมวดที่ ๑
การเข้าถึงและควบคุมการใช้งานระบบหมอพร้อม (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบหมอพร้อม (Business Requirement For Access Control)

วัตถุประสงค์

เพื่อให้บุคลากรสำนักสุขภาพดิจิทัล รวมทั้งบุคคลภายนอก ให้มีความรู้ ความเข้าใจและสามารถปฏิบัติตามแนวทางปฏิบัติในการเข้าถึงและควบคุมการใช้งานระบบหมอพร้อม (Access Control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบหมอพร้อม (Business Requirement For Access Control) พร้อมทั้งตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และระบบหมอพร้อม

นโยบาย

บุคลากรสำนักสุขภาพดิจิทัล รวมทั้งบุคคลภายนอกต้องให้ความสำคัญและสนับสนุน การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยเฉพาะการเข้าถึงและการควบคุมการใช้งานสารสนเทศหมอพร้อม และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศหมอพร้อม

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลสารสนเทศและอุปกรณ์ในการประมวลผล ให้คำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้

๑.๑ การเข้าถึงและควบคุมการใช้งานระบบหมอพร้อม และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบหมอพร้อม ต้องสอดคล้อง และเป็นไปตามคำสั่งมอบหมายให้ปฏิบัติราชการและคำสั่งมอบอำนาจ

๑.๒ เจ้าของระบบมีหน้าที่ในการอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์ และระบบหมอพร้อมให้กับผู้ใช้งาน

๑.๓ ผู้ดูแลระบบมีหน้าที่กำหนดสิทธิให้แก่ผู้ใช้งานตามที่เจ้าของระบบอนุมัติ

๑.๔ ผู้ดูแลระบบมีหน้าที่ในการสร้างบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน สำหรับเข้าระบบหมอพร้อม ตลอดจนควบคุม การใช้งานและดูแลรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และระบบหมอพร้อม

๑.๕ ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อมตามสิทธิที่ได้รับเท่านั้น

๑.๖ เมื่อมีความจำเป็นต้องให้บุคคลภายนอกเข้าถึงระบบคอมพิวเตอร์ ระบบหมอพร้อม ต้องแจ้งเหตุผลและความจำเป็นเพื่อขออนุมัติสำหรับการปฏิบัติงานตามภารกิจจากเจ้าของระบบ และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหาย บุคคลภายนอกต้องรับผิดชอบผลที่เกิดจากการกระทำของตน

๒. การควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม 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 สิทธิของผู้ดูแลระบบ (Administrator) กำหนดสิทธิ ตรวจสอบสิทธิ ทบทวนสิทธิ และบริหารจัดการระบบคอมพิวเตอร์และระบบหมอพร้อม

๓. การกำหนดประเภทของข้อมูล ลำดับความสำคัญ ลำดับชั้นความลับ รวมถึงระดับชั้น การเข้าถึง เวลาที่เข้าถึง และช่องทางการเข้าถึง ดังนี้

๓.๑ ประเภทของข้อมูล แบ่งเป็น ๓ ประเภท ดังนี้

๓.๑.๑ ข้อมูลสารสนเทศสำหรับการบริหาร ได้แก่ รายงานการฉีดวัคซีน

๓.๑.๒ ข้อมูลสารสนเทศสำหรับสนับสนุนการปฏิบัติงาน ได้แก่ ข้อมูลการรับบริการการฉีดวัคซีน,ข้อมูลการตรวจหาเชื้อโควิด 19 ,ข้อมูลประวัติการรักษา เป็นต้น

๓.๑.๓ ข้อมูลสารสนเทศสำหรับการเผยแพร่แก่ประชาชนทั่วไป ได้แก่ ประวัติการได้รับวัคซีนป้องกันการติดเชื้อโควิด 19 ผลการตรวจหาเชื้อโควิด 19 ด้วยวิธี RT-PCR และ ATK เอกสารรับรองการได้รับวัคซีน, ประวัติการรักษา, แบบประเมินอาการหลังฉีดวัคซีน เป็นต้น

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 ซึ่งถ้าหากความลับดังกล่าว ทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้รับทราบจะทำให้เกิดความเสียหาย หรือเป็นภยันตรายต่อความมั่นคง ความปลอดภัย หรือความสงบเรียบร้อยของประเทศชาติหรือพันธมิตร หรือการดำเนินงานของหน่วยงานที่เกี่ยวข้องอย่างร้ายแรงที่สุด

๓.๓.๒ ลับมาก - ความลับที่มีความสำคัญมาก เกี่ยวกับข่าวสาร วัตถุหรือบุคคล ซึ่งถ้าหากความลับดังกล่าว ทั้งหมดหรือเพียงบางส่วนราวไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหาย หรือเป็นภยันตรายต่อความมั่นคงปลอดภัยของประเทศชาติหรือพันธมิตร หรือความสงบเรียบร้อยภายในราชอาณาจักร หรือการดำเนินงานของขององค์กรหรือหน่วยงานที่เกี่ยวข้องได้อย่างร้ายแรง

๓.๓.๓ ลับ - ความลับที่มีความสำคัญเกี่ยวกับ ข่าวสาร วัตถุหรือบุคคล ซึ่งถ้าหากความลับดังกล่าว ทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคล ผู้ไม่มีหน้าที่ได้ทราบจะทำให้เกิดความเสียหายหรือเป็นภยันตรายต่อราชการ หรือการดำเนินงานขององค์กรหรือหน่วยงานที่เกี่ยวข้องได้

๓.๓.๔ ปกปิด -ความลับซึ่งไม่เปิดเผยให้ผู้ไม่มีหน้าที่ได้ทราบ โดยสงวนไว้ให้ทราบเฉพาะบุคคลที่มีหน้าที่ต้องทราบเพื่อประโยชน์ในการปฏิบัติภารกิจองค์กรเท่านั้น

๓.๔ ระดับชั้นการเข้าถึง แบ่งเป็น ๔ ระดับ ดังนี้

๓.๔.๑ กลุ่มผู้บริหาร

๓.๔.๒ กลุ่มผู้ปฏิบัติ

๓.๔.๓ กลุ่มผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๓.๔.๔ กลุ่มประชาชนทั่วไป

๓.๕ เวลาที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศหมอพร้อม สามารถเข้าถึงได้ตลอด ๒๔ ชม. x ๗ วัน

๓.๖ ช่องทางการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม ได้ ๒ ช่องทาง

๓.๖.๑ ระบบเครือข่ายภายนอก (Internet)

๓.๖.๒ ระบบแอปพลิเคชัน (Application)

๔. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม (Business Requirement For Access Control) ดังนี้

๔.๑ เจ้าของระบบอนุมัติสิทธิให้ผู้ใช้งาน ตามภารกิจเพื่อให้สามารถเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม เฉพาะในส่วนที่ได้รับมอบหมาย ตามความจำเป็นในการใช้งาน

๔.๒ ผู้ดูแลระบบกำหนดสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศให้กับผู้ใช้งานตามที่เจ้าของระบบอนุมัติ

หมวดที่ ๒
การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Management)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อมเฉพาะผู้ใช้งานที่ได้รับอนุญาตแล้ว และสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตะหนักถึงเรื่องความมั่นคงปลอดภัยสารสนเทศหมอพร้อมและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดให้มีกระบวนการสำหรับการลงทะเบียนสำหรับผู้ใช้งานใหม่ (User Registration) เพื่อรับสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อมตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

๒. กำหนดกระบวนการสำหรับการยกเลิกสิทธิการใช้งานเมื่อไม่ได้ปฏิบัติงานที่กลุ่มงานดิจิทัลสุขภาพ

๓. กำหนดให้มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) อย่างรัดกุมโดยให้มีการควบคุม จำกัด และเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์ระบบหมอพร้อมตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การลงทะเบียนผู้ใช้งาน ให้ดำเนินการ ดังนี้

๑.๑ ผู้รับผิดชอบด้านสารสนเทศของหน่วยงานต้องกำหนดแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม อย่างน้อยประกอบด้วย ชื่อ นามสกุล ตำแหน่ง สังกัด และหมายเลขโทรศัพท์

๑.๒ การขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม ให้ดำเนินการ ดังนี้

๑.๒.๑ กรณีบุคลากรสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

(๑) ให้บุคลากรกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม

(๒) ให้หน่วยงานส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อมให้เจ้าของระบบที่ขอใช้งาน

(๓) ให้เจ้าของระบบอนุมัติสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศหมอพร้อม

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิ ตามที่เจ้าของระบบอนุมัติ

๑.๒.๒ กรณีบุคคลภายสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

(๑) ให้บุคคลภายนอกกรอกข้อมูลลงในฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม พร้อมระบุเหตุผลในการเข้าใช้งานหรือหนังสือขอเข้าใช้งานจากบริษัท/หน่วยงานต้นสังกัด

(๒) ให้หน่วยงานพิจารณาเหตุผล และดำเนินการส่งแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม ให้เจ้าของระบบที่ขอใช้งาน

(๓) ให้เจ้าของระบบอนุมัติสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม

(๔) ให้ผู้ดูแลระบบกำหนดสิทธิตามที่เจ้าของระบบ อนุมัติพร้อมทั้งแจ้งให้หน่วยงานเจ้าของบุคลากรรับทราบ

๑.๓ การสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่าน (Password) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๑.๓.๑ การสร้างบัญชีผู้ใช้งาน (Username) ให้เจ้าของระบบ กำหนด เช่น ชื่อภาษาอังกฤษหรือบัตรประจำตัวประชาชน

๑.๓.๒ การกำหนดรหัสผ่าน (Password) ชุดของตัวอักษรภาษาอังกฤษตัวพิมพ์ใหญ่และตัวพิมพ์เล็กหรืออักขระพิเศษ อย่างน้อย ๘ ตัวขึ้นไป ที่ยากต่อการคาดเดา

๑.๓.๓ ให้ผู้ดูแลระบบ แจ้งบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้ผู้ใช้งานทราบโดยตรง

๑.๓.๔ เมื่อผู้ใช้งาน มีการเปลี่ยนแปลงข้อมูลให้แจ้งเจ้าของระบบ เพื่อปรับปรุงข้อมูลผู้ใช้งาน

๒. การยกเลิกสิทธิการใช้งาน ให้ดำเนินการดังนี้

๒.๑ ให้หน่วยงานแจ้งเจ้าของระบบ เพื่อขอยกเลิกสิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม เมื่อมีการลาออก ให้โอน หรือสิ้นสุดการจ้าง

๒.๒ ผู้ดูแลระบบ จะดำเนินการปิดบัญชีผู้ใช้งาน (Username) และแจ้งกลับไปยังหน่วยงานรับทราบ

๓. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ในการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อมของผู้ใช้งาน ให้ดำเนินการดังนี้

๓.๑ ในกรณีที่มีการเปลี่ยนแปลงตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย ให้หน่วยงานแจ้งเจ้าของระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม

๓.๒ ในกรณีที่ผู้ใช้งาน ต้องการสิทธิเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศหมอพร้อมที่สูงกว่าระดับสิทธิที่ได้รับ ขอให้แจ้งความประสงค์พร้อมเหตุผลต่อเจ้าของระบบ เพื่อให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม

๔. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ดำเนินการตามหลักเกณฑ์ ดังนี้

๔.๑ ในกรณีที่ผู้ใช้งาน ลืมรหัสผ่าน (Password) ให้ขอรับรหัสผ่านใหม่ตามวิธีการของเจ้าของระบบคอมพิวเตอร์และระบบหมอพร้อมกำหนด เช่น โทรศัพท์ หรือออนไลน์

๔.๒ ผู้ใช้งาน ต้องเปลี่ยนรหัสผ่าน (Password) ใหม่ทุก ๑ ปี และรหัสผ่าน (Password) ใหม่ต้องไม่ซ้ำกับรหัสผ่าน (Password) เดิม

๕. ผู้ดูแลระบบ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง เพื่อกำหนดสิทธิให้สอดคล้องตามภารกิจที่เปลี่ยนไป

หมวดที่ ๓
การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
(User Responsibilities)

วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศหมอพร้อมและการลักขโมยอุปกรณ์ในการประมวลผลข้อมูล (Process Device)

นโยบาย

๑. กำหนดแนวปฏิบัติในงานใช้งานรหัสผ่าน (Password) และการเปลี่ยนรหัสผ่าน (Password)

๒. กำหนดแนวทางปฏิบัติในการป้องกันระบบคอมพิวเตอร์และระบบหมอพร้อมในขณะที่ไม่มีผู้ใช้งาน (User) เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศหมอพร้อมในขณะที่ไม่มีผู้ใช้งาน (User) ดูแล

๓. กำหนดแนวทางปฏิบัติในการควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศหมอพร้อม (Clear Desk and Clear Screen Policy) ได้แก่ เอกสาร สื่อบันทึกข้อมูล และข้อมูลสารสนเทศหมอพร้อม เพื่อไม่ให้สินทรัพย์ (Asset) อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งาน (User) ออกจากระบบคอมพิวเตอร์และระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๔. กำหนดให้ผู้ใช้งาน (User) อาจนำเข้ารหัสข้อมูล (Encryption) มาใช้กับการส่งข้อมูลที่สำคัญหรือข้อมูลที่เป็นความลับของสำนักสุขภาพดิจิทัล โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

แนวปฏิบัติ

๑. การใช้งานรหัสผ่าน (Password) ให้ดำเนินการ ดังนี้

๑.๑ ผู้ใช้งานต้องกำหนดรหัสผ่าน (Password) ตามหมวดที่ ๒ ข้อ ๑.๓ และต้องเปลี่ยนรหัสผ่านตามข้อ ๔.๒

๑.๒ ผู้ใช้งานต้องไม่ใช้รหัสผ่าน (Password) ร่วมกับบุคคลอื่น และไม่ควรให้ระบบคอมพิวเตอร์หรือระบบหมอพร้อมจำรหัสผ่าน (Password) ในการเข้าใช้งานอัตโนมัติ

๑.๓ ผู้ใช้งานต้องไม่เปิดเผยรหัสผ่าน (Password) สำหรับการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อมให้ผู้อื่นรับรู้ โดยเก็บเป็นความลับเสมือนว่าเป็นสมบัติส่วนตัว ห้ามจดหรือเขียนรหัสผ่าน (Password) ที่ใช้งานไว้ในที่เปิดเผย

๑.๔ หากมีความจำเป็นต้องบอกรหัสผ่าน (Password) แก่บุคคลอื่นเนื่องจากความจำเป็นในการเข้าถึงหลังดำเนินการเสร็จสิ้นแล้วให้เปลี่ยนรหัสผ่าน (Password) ใหม่ทันที

๑.๕ หากมีการกระทำความผิดเกิดขึ้นจากบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของบุคคลใด บุคคลนั้นต้องมีส่วนร่วมในการรับผิดชอบต่อการกระทำความผิดนั้น เว้นแต่เจ้าของบัญชีผู้ใช้งาน (Username) ได้กระทำการป้องกันตามแนวปฏิบัติที่กำหนดแล้ว

๒. ผู้ใช้งานต้องออกจากระบบ (Log Out) ทันทีเมื่อเลิกใช้งานจากระบบคอมพิวเตอร์และระบบหมอพร้อม

๓. การควบคุมสินทรัพย์ (Asset) และการเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อม (Clear Desk and Clear Screen Policy) ให้ดำเนินการตามหลักเกณฑ์ดังนี้

๓.๑ ระบบคอมพิวเตอร์และระบบสารสนเทศหมอพร้อม รวมถึงอุปกรณ์ในการประมวลผล (Process Device) มีวัตถุประสงค์เพื่อใช้ในการปฏิบัติงานของสำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข เท่านั้น

๓.๒ ผู้ใช้งานต้องรับผิดชอบต่อสินทรัพย์ (Asset) ของสำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข และให้ใช้งานด้วยความระมัดระวังเสมือนเป็นทรัพย์สินส่วนตน

๓.๓ ผู้ใช้งานต้องไปดัดแปลงหรือไม่ติดตั้งอุปกรณ์หรือซอฟต์แวร์ใดๆ ที่เครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์พกพา หรือระบบคอมพิวเตอร์และระบบหมอพร้อม ในกรณีที่มีความจำเป็นในการใช้งานเพิ่มเติมให้แจ้งความประสงค์พร้อมเหตุผลต่อผู้ดูแลระบบสารสนเทศหมอพร้อม

๓.๔ ผู้ใช้งานต้องใช้ความระมัดระวังในการบันทึกข้อมูลสารสนเทศไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพา หรือการ์ดความจำในโทรศัพท์มือถือ เพื่อป้องกันการรั่วไหลของข้อมูล

๓.๕ บุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานด้านระบบหมอพร้อม ต้องขออนุมัติเป็นลายลักษณ์อักษรก่อนเข้าปฏิบัติงาน

๓.๖ การทำลายอุปกรณ์บันทึกข้อมูลหรือนำอุปกรณ์บันทึกข้อมูลกลับมาใช้งานใหม่ให้ดำเนินการดังนี้

๓.๖.๑ การทำลายอุปกรณ์บันทึกข้อมูล เช่น Flash Drive CD/DVD ฮาร์ดดิสก์ เทป เป็นต้น ให้ใช้วิธีทุบ หรือบดให้เสียหาย หรือเผาทำลายด้วยวิธีการทำลายตามมาตรฐานสากล หรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

๓.๖.๒ การนำอุปกรณ์บันทึกข้อมูลไปใช้งานใหม่ ให้ฟอร์แมต (Format) อุปกรณ์บันทึกข้อมูลนั้นโดยใช้วิธีการ ฟอร์แมต (Format) ตามมาตรฐานสากล หรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนด

หมวดที่ ๔
การควบคุมการเข้าถึงเครือข่าย
(Network Access control)

วัตถุประสงค์

เพื่อให้มีการควบคุมและป้องกันการเข้าถึงเครือข่ายให้มีความมั่นคง

นโยบาย

๑. กำหนดแนวปฏิบัติในการเข้าถึงเครือข่ายของผู้ใช้งาน (User) เฉพาะที่ได้รับอนุญาตให้เข้าถึง

๒. กำหนดแนวปฏิบัติในการยืนยันตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร (User Authentication for External Connections) โดยต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาต ให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถใช้งานเครือข่าย ระบบคอมพิวเตอร์และระบบสารสนเทศหมอพร้อมของสำนักสุขภาพดิจิทัลได้

๓. กำหนดแนวปฏิบัติในการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) โดยต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และต้องใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

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

๕. กำหนดแนวปฏิบัติในการควบคุมเชื่อมต่อทางเครือข่าย (Network Connection Control) โดยต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน

๖. กำหนดแนวปฏิบัติในการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศหมอพร้อมและการส่งข้อมูลสารสนเทศหมอพร้อมสอดคล้องกับแนวปฏิบัติการเข้าถึงและการควบคุมการใช้งานสารสนเทศหมอพร้อม (Access control) และการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศหมอพร้อม (Business Requirements for Access Control)

แนวปฏิบัติ

๑. การเข้าถึงเครือข่ายของผู้ใช้งาน

๑.๑ การใช้งานระบบเครือข่ายภายนอก (Internet) ให้ดำเนินการดังนี้

๑.๑.๑ กำหนดให้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองสำหรับเข้าใช้งานระบบเครือข่ายนอก (Internet)

๑.๑.๒ ห้ามเปิดเผยข้อมูลสำคัญหรือข้อมูลที่เป็นความลับของระบบหมอพร้อมเว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๑.๓ ต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ โดยเคร่งครัด

๑.๑.๔ ต้องระมัดระวังการดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมต่างๆ เพราะอาจเป็นการละเมิดทรัพย์สินทางปัญญา หรืออาจทำให้มีไวรัสคอมพิวเตอร์บุกรุก โจมตีระบบคอมพิวเตอร์และระบบสารสนเทศหมอพร้อม โดยแจ้งให้ผู้ดูแลระบบสารสนเทศหมอพร้อมของหน่วยงานค้นสังกัดทราบก่อนติดตั้งการใช้งาน

๑.๒ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ให้ดำเนินการ ดังนี้

๑.๒.๑ การนำเสนอเนื้อหาข้อมูลผ่านเครือข่ายสังคมออนไลน์ (Social Network) ภายใต้ระบบหมอพร้อม ควรนำเสนอเกี่ยวกับภารกิจงานของระบบ เช่น ผลการงานและข่าวสาร โดยการนำเข้าข้อมูลต้องเป็นผู้ที่ได้รับมอบหมายจากระบบหมอพร้อม และต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และที่แก้ไขเพิ่มเติม

๑.๒.๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับของระบบหมอพร้อม ผ่านเครือข่ายสังคมออนไลน์ (Social Network) เว้นแต่ได้รับอนุญาตจากเจ้าของข้อมูล

๑.๒.๓ กรณีประชาชนหรือหน่วยงานอื่นมีความคิดเห็นแตกต่าง ต้องชี้แจงด้วยเหตุผล งดเว้นการโต้ตอบด้วยความรุนแรง และควรพิจารณานำความคิดเห็นดังกล่าวมาใช้ในการพัฒนาปรับปรุงต่อไป

๑.๒.๔ ห้ามแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความคิดเห็นจากระบบหมอพร้อม และต้องแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความคิดเห็นส่วนตัว

๑.๒.๕ หากเกิดความผิดพลาดจากการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) ผู้ใช้งาน ต้องรับผิดชอบความเสียหายที่เกิดขึ้นและดำเนินการแก้ไขทันที

๒. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ให้ดำเนินการ ดังนี้

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

๒.๒ การนำเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ มาใช้งานบนเครือข่ายต้องได้รับอนุญาตจากผู้รับผิดชอบด้านระบบหมอพร้อม

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

๓.๑ ดูแล/ตรวจสอบ พอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งแบบ (Remote Diagnosis and Configuration Port Protection) รวมทั้งการควบคุมการเข้าพอร์ตทางกายภาพและเครือข่าย

๓.๒ เปิดใช้งานเฉพาะพอร์ตที่จำเป็นสำหรับการใช้งานเท่านั้นและต้องตรวจสอบพอร์ตที่เปิดให้บริการ อย่างน้อยปีละ ๑ ครั้ง

๔. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ให้ดำเนินการ ดังนี้

๔.๑ กลุ่มเทคโนโลยีสารสนเทศต้องติดตั้งระบบป้องกันการบุกรุกโจมตีทางเครือข่าย (Firewall) เพื่อใช้เป็นจุดควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

๔.๒ ผู้ดูแลระบบต้องไม่เปิดเผยข้อมูลการเชื่อมต่อทางเครือข่าย ก่อนได้รับอนุญาตสำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข

๔.๓ ผู้ดูแลระบบมีหน้าที่ในการควบคุมการเชื่อมต่อสัญญาณหรือยกเลิก การเชื่อมต่อสัญญาณตามที่ได้รับอนุญาตจากสำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข ทั้งนี้ หากพบข้อผิดพลาดหรือเห็นว่าหมดความจำเป็นในการเชื่อมต่อสัญญาณให้รายงานสำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข ทันที

๔.๔ การเชื่อมต่อเครือข่ายสารสนเทศระหว่างระบบหมอพร้อม กับหน่วยงานภายนอก ต้องได้รับอนุญาตจากสำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข และเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ของผู้ให้บริการที่มีความน่าเชื่อถือ

๕. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ให้ดำเนินการ ดังนี้

๕.๑ ผู้ดูแลระบบต้องควบคุมการจัดการเส้นทางบนเครือข่าย (Network Routing Control) เพื่อให้การเชื่อมต่อระบบคอมพิวเตอร์และระบบหมอพร้อมเป็นไปอย่างมีประสิทธิภาพ และการรับ-ส่ง หรือการไหลเวียนของข้อมูลเป็นไปอย่างรวดเร็ว

๕.๒ ผู้ดูแลระบบต้องเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ของผู้ใช้งานเป็นระยะเวลาไม่น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และแก้ไขเพิ่มเติม

หมวดที่ ๕
การควบคุมการเข้าถึงระบบหมอพร้อม
(Mohprompt System Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบหมอพร้อม (Mohprompt System Access Control) เพื่อป้องกันการเข้าถึงระบบหมอพร้อมโดยไม่ได้รับอนุญาต

นโยบาย

๑. กำหนดแนวปฏิบัติแนวปฏิบัติสำหรับระบบคอมพิวเตอร์และระบบสารสนเทศหมอพร้อมซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อสำนักสุขภาพดิจิทัล โดยต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ พร้อมทั้งให้มีการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ที่ปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking)

๒. กำหนดแนวปฏิบัติในการควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องระบบคอมพิวเตอร์และระบบสารสนเทศหมอพร้อม และข้อมูลสารสนเทศหมอพร้อมจากความเสี่ยงของการใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๓. กำหนดแนวปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) โดยต้องกำหนดข้อปฏิบัติแผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติจากภายนอกสำนักงาน

แนวปฏิบัติ

๑. ควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการดังนี้

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

๑.๒ การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource)

๒. ระบบคอมพิวเตอร์และระบบหมอพร้อม ซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ดังนี้

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

๒.๒ ระบบคอมพิวเตอร์และระบบหมอพร้อมซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อองค์กร ต้องได้รับการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายแยกออกจากระบบอื่นๆ

๒.๓ ผู้ดูแลระบบต้องแบ่งพื้นที่สำหรับการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายตามระดับความสำคัญและความปลอดภัยของระบบคอมพิวเตอร์และระบบหมอพร้อมซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร เพื่อควบคุมสภาพแวดล้อมโดยเฉพาะ

๒.๔ การใช้เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ปฏิบัติจากภายนอกองค์กร (Mobile Computing And Teleworking) เพื่อเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อมซึ่งไวต่อการรบกวนมีผลกระทบมีความสำคัญสูงต่อองค์กร ต้องเข้าถึงในสถานที่ที่มีความปลอดภัยและต้องได้รับอนุญาตจากสำนักสุขภาพดิจิทัล

๓. การควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ให้ดำเนินการดังนี้

๓.๑. อุปกรณ์สื่อสารเคลื่อนที่ได้แก่ Smart Phone และ Tablet ต้องได้รับการยืนยันตัวตนโดยบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของผู้ใช้งานสำหรับการเข้าใช้งาน

๔. การปฏิบัติงานจากหน่วยงานภายนอกหน่วยงาน (Teleworking) กำหนด ดังนี้

๔.๑ ผู้ใช้งานต้องปฏิบัติตามหมวด ๖ แนวปฏิบัติ ข้อ ๑ การควบคุมการเข้าถึงระบบหมอพร้อม (Information Access Restriction)

๔.๒ เมื่อเข้าระบบคอมพิวเตอร์และระบบหมอพร้อมแล้ว ผู้ใช้งานต้องระมัดระวังไม่ให้ผู้ไม่มีส่วนเกี่ยวข้องเข้าถึงระบบคอมพิวเตอร์และระบบหมอพร้อมจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ สื่อสารเคลื่อนที่ได้และต้องออกจากระบบ (Logout) ทันที เมื่อเลิกปฏิบัติหน้าที่

หมวด ๖
การจัดทำระบบสำรองของระบบหมอพร้อม
(Disaster Recovery Site)

วัตถุประสงค์

เพื่อจัดทำระบบสำรองของระบบหมอพร้อมให้อยู่ในสภาพพร้อมใช้งาน โดยการสำรองข้อมูลหมอพร้อมและการกู้คืนข้อมูลระบบหมอพร้อม และการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ ซึ่งได้รวบรวมความเสี่ยงของระบบหมอพร้อม การเตรียมความพร้อมฉุกเฉิน และการบริหารความต่อเนื่องในสภาวะวิกฤตของระบบหมอพร้อม และการสำรองข้อมูลและการกู้คืนข้อมูลสารสนเทศไว้ด้วยแล้ว เพื่อให้สามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่องแม้ในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่างๆ และสามารถกู้คืนระบบหมอพร้อมได้ภายในระยะเวลาที่เหมาะสมและสามารถใช้งานได้อย่างต่อเนื่อง

นโยบาย

๑. พิจารณาคัดเลือกระบบสารสนเทศที่เหมาะสมในการจัดการทำระบบสำรองข้อมูลให้อยู่ในสภาพพร้อมใช้งาน

๒. จัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของสำนักสุขภาพดิจิทัล เพื่อให้สามารถเข้าถึงระบบสารสนเทศได้อย่างปกติต่อเนื่อง และต้องปรับปรุงแผนดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

แผนปฏิบัติ

๑. ผู้ดูแลระบบจะต้องจัดการทำการสำรองระบบหมอพร้อมโดยมีขั้นตอน ดังนี้

๑.๑ ผู้ดูแลระบบจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการสำรองข้อมูล และการกู้คืนข้อมูลระบบหมอพร้อม

๑.๒ กำหนดรูปแบบการสำรองข้อมูลระบบหมอพร้อม ดังนี้

๑.๒.๑ คัดเลือกระบบสารสนเทศในการสำรองข้อมูล

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

๑.๒.๓ กำหนดความถี่ในการสำรองข้อมูลตามความเหมาะสมของระบบหมอพร้อม

๑.๓ ผู้ดูแลระบบดำเนินการสำรองของระบบหมอพร้อม ตามข้อ ๑.๒

๒. ผู้ดูแลระบบต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศที่สำรองไว้ อย่างน้อย ๑ ระบบ โดยอย่างน้อยปีละ ๑ ครั้ง

๓. สำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข ดำเนินการจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตของระบบหมอพร้อม เพื่อให้สามารถใช้งานได้ตามปกติอย่างต่อเนื่อง

๔. มีการทบทวนระบบหมอพร้อมในการสำรอง อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๗
การตรวจสอบและประเมินความเสี่ยงของหมอพร้อม
(Risk Assessment and Risk Management)

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติการตรวจสอบและประเมินความเสี่ยงของหมอพร้อมทำให้มั่นใจว่าแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบหมอพร้อมที่กำหนดมีความมั่นคงปลอดภัยและหน่วยงานสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ

นโยบาย

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

๒. การตรวจสอบและการประเมินความเสี่ยงด้านสารสนเทศจะต้องดำเนินการโดยผู้ตรวจสอบภายในหน่วยงานรัฐ (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยของสารสนเทศหมอพร้อม

แนวปฏิบัติ

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

๒. กำหนดให้มีผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของระบบหมอพร้อม ดังนี้

๒.๑ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศประจำปีงบประมาณให้ดำเนินการโดยกลุ่มตรวจสอบภายใน (Internal Auditor)

๒.๒ หากมีความประสงค์ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของระบบหมอพร้อมเชิงเทคนิค ให้ดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

๓. กำหนดแนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของระบบหมอพร้อม ดังนี้

๓.๑ ผู้ตรวจสอบต้องจัดทำรายงานพร้อมข้อเสนอแนะในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของระบบหมอพร้อม

๓.๒ สำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข ต้องอำนวยความสะดวกแก่ผู้ตรวจสอบภายในการตรวจสอบข้อมูลที่สำคัญ

๓.๓ ในกรณีที่ผู้ตรวจสอบจำเป็นต้องเข้าถึงข้อมูลสำคัญ ให้สำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข สร้างสำเนาสำหรับข้อมูลนั้น โดยให้ผู้ตรวจสอบใช้งานและทำลาย หรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือหากประสงค์ จัดเก็บข้อมูลนั้นเป็นหลักฐานให้แจ้งสำนักสุขภาพดิจิทัล สำนักงานปลัดกระทรวงสาธารณสุข เป็นลายลักษณ์อักษร

๓.๔ ในกรณีติดตั้งเครื่องมือที่ใช้ในการตรวจสอบประเมินความเสี่ยงระบบคอมพิวเตอร์และระบบหมอพร้อม ให้แยกการติดตั้งเครื่องมือออกจากระบบที่ใช้บริการจริง หรือระบบที่ใช้ในการพัฒนาและกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว (Read Only)

๓.๕ ผู้ตรวจสอบต้องแจ้งความเสี่ยงและระบุความรุนแรงของเครื่องมือที่ใช้ในการตรวจสอบและประเมินความเสี่ยง

หมวดที่ ๘
การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบหมอพร้อม
(Information Security Incident Management)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบหมอพร้อมได้รับการดำเนินการอย่างถูกต้อง มีประสิทธิภาพในช่วงระยะเวลาที่เหมาะสม

แนวปฏิบัติ

๑. จัดให้มีขั้นตอนหรือกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบหมอพร้อมที่สำคัญ รวมทั้งกำหนดผู้มีหน้าที่รับผิดชอบซึ่งมีความรู้ความสามารถและประสบการณ์ โดยมีขั้นตอนและกระบวนการดังต่อไปนี้

๑.๑ การกำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์อย่างเป็นลายลักษณ์อักษร

๑.๒ การประเมินเหตุการณ์และจุดอ่อนของมาตรการรักษาความมั่นคงปลอดภัยของระบบหมอพร้อม และพิจารณาว่าควรจัดเป็นเหตุการณ์และมีระดับความรุนแรงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศหมอพร้อม

๑.๓ จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่แจ้งเหตุการณ์ และรายงานเหตุการณ์ให้ผู้เกี่ยวข้องทราบ และดำเนินการต่อไป

๑.๔ การดำเนินการเพื่อตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างมีประสิทธิภาพ เพื่อทำให้เหตุการณ์คลี่คลายหรือกลับสู่สภาวะปกติ

๑.๕ วิเคราะห์ รวบรวม และรายงานเหตุกาณ์ต่อผู้บังคับบัญชาทราบ ทั้งนี้เพื่อระบุถึงสาเหตุและเพื่อใช้ประโยชน์จากผลการวิเคราะห์มนการเตรียมความพร้อมรองรับเหตุการณ์ที่อาจเกิดขึ้นได้ในอนาคต

๒. ต้องจัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ ผ่านบุคคลหรือหน่วยงานที่ทำหน้าที่รับแจ้งเหตุการณ์ (Point of Contact) โดยให้ดำเนินการดังนี้

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

๒.๒ รายงานผู้บังคับบัญชาเมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย เช่น

- การบุกรุกทางกายภาพ
- การปฏิบัติงานที่ไม่เป็นตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศหมอพร้อม
- การเปลี่ยนแปลง การเข้าถึงโดยไม่ได้รับอนุญาต
- การทำงานผิดของระบบและอุปกรณ์ หรือการปฏิบัติงานจัดให้มีบุคคลหรือหน่วยงาน (Point of Contact) เพื่อทำหน้าที่รายงานเหตุการณ์ที่เกิดขึ้นต่อผู้บังคับบัญชา โดยให้รายงานดังต่อไปนี้

รายงานทันทีเมื่อเกิดเหตุ	ระหว่างดำเนินการแก้ไข	แก้ปัญหาได้ และเหตุยุติ
๑.วันเวลาที่เกิดเหตุการณ์ ๒.ระบบที่เกิดเหตุรายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น ๓.ผลกระทบที่คาดว่าจะเกิดขึ้น ๔.ชื่อผู้ติดต่อ/ประสานงาน เพื่อให้ข้อมูล	๑.วันเวลาที่เกิดเหตุการณ์ ๒.ระบบที่เกิดเหตุรายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น ๓.ผลกระทบที่คาดว่าจะเกิดขึ้น ๔.ดำเนินการแก้ไขปัญหาและระยะเวลาในการแก้ไข ๕.ความคืบหน้าในการแก้ไขปัญหา	๑.วันเวลาที่เกิดเหตุการณ์ ๒.ระบบที่เกิดเหตุรายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น ๓.ผลกระทบที่คาดว่าจะเกิดขึ้น ๔.ดำเนินการแก้ไขปัญหา ๕.ผลการแก้ไขปัญหา และระยะเวลาในการแก้ไข ๖.แนวทางป้องกันในอนาคตและการเก็บรวบรวมหลักฐาน หรือระบุสาเหตุและแนวทางแก้ไขต่อไป

รายงานทันทีเมื่อเกิดเหตุ	ระหว่างดำเนินการแก้ไข	แก้ปัญหาได้ และเหตุยุติ
รายงานโดยไม่ชักช้า อาจแจ้งด้วยวาจาหรือช่องทางใดช่องทางหนึ่งที่รวดเร็วและทันต่อเหตุการณ์ และตรวจสอบในเบื้องต้นแล้ว ตามหนังสือสั่งการ ของสำนักงานปลัดกระทรวงสาธารณสุข ที่ สธ ๐๒๑๒/ว ๘๘๐๗ ลงวัน ๒๒ เมษายน ๒๕๖๕ เรื่อง ให้หน่วยงานปฏิบัติงานให้มีความมั่นคงปลอดภัยไซเบอร์ ข้อที่ ๖ กรณีพบภัยคุกคามทางไซเบอร์ ให้ประสานศูนย์ประสานการรักษาความมั่นคงปปลอดภัยไซเบอร์สาธารณสุข (Health CIRT) ทันที	รายงานโดยไม่ชักช้า อาจแจ้งด้วยวาจาหรือช่องทางใดช่องทางหนึ่งที่รวดเร็วและทันต่อเหตุการณ์เมื่อทราบเหตุการณ์และตรวจสอบในเบื้องต้นแล้ว ตามหนังสือสั่งการของสำนักงานปลัดกระทรวงสาธารณสุข ที่ สธ ๐๒๑๒/ว ๘๘๐๗ ลงวัน ๒๒ เมษายน ๒๕๖๕ เรื่อง ให้หน่วยงานปฏิบัติงานให้มีความมั่นคงปลอดภัยไซเบอร์	รายงานเป็นลายลักษณ์อักษรโดยมีเนื้อหาจากข้อมูลข้างต้น