กรมสนับสนุนบริการสุขภาพ
DEPARTMENT OF HEALTH SERVICE SUPPORT

แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

สารบัญ หน้า

๑. แนวปฏิบัติการควบคุมการเข้าถึงและควบคุมการใช้อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย และระบบ สารสนเทศ ๒

๑.๑ การควบคุมการเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ ๒

๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน ๓

๑.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน ๕

๑.๔ การควบคุมการเข้าถึงเครือข่าย ๗

๑.๕ การควบคุมการเข้าถึงระบบปฏิบัติการ ๙

๑.๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ ๑๐

๑.๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย ๑๒

๑.๘ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม ๑๓

๑.๙ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ๑๕

๑.๑๐ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ ๑๖

๑.๑๑ การใช้งานระบบอินเทอร์เน็ต ๑๖

๑.๑๒ การใช้งานอุปกรณ์ป้องกันการบุกรุก ๑๗

๑.๑๓ การใช้งานเครือข่ายสังคมออนไลน์ ๑๗

๑.๑๔ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ๑๘

๒. แนวปฏิบัติระบบสารองของสารสนเทศ และแผนเตรียมความพร้อมกรณีฉุกเฉิน ๑๘

๓. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ๒๐

๑. แนวปฏิบัติการควบคุมการเข้าถึงและควบคุมการใช้อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ

เพื่อกำหนดเป็นมาตรการ มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้อง เข้าถึงและใช้อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ โดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิ ในการเข้าถึง เพื่อให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลได้ โดยมอบหมายให้กลุ่มบริหารทั่วไปและแผนงาน และผู้ดูแลระบบที่ได้รับมอบหมายเป็นผู้รับผิดชอบ โดยมีแนวทางการปฏิบัติ ดังนี้

๑.๑ การควบคุมการเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ

๑.๑.๑ จัดทำบัญชีสินทรัพย์หรือทะเบียนสินทรัพย์ การจำแนกกลุ่มทรัพยากรของระบบหรือ การทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึง และควบคุมการใช้งานระบบสารสนเทศ โดยกำหนดให้มีการอนุญาต การกำหนดสิทธิ หรือการมอบอานาจ ดังนี้

- กำหนดสิทธิของผู้ใช้งานในแต่ละกลุ่มงานเป็นผู้รับผิดชอบ และมอบหมายผู้ที่เกี่ยวข้อง

๑.๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูล ไว้ในแต่ละกลุ่มงาน ได้แก่

-ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี

-ข้อมูลสารสนเทศด้านวิชาการที่ให้บริการ ได้แก่ ข้อมูลการออบแบบด้านวิศวกรรม

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ ได้แก่

-ข้อมูลสารสนเทศที่มีระดับความสำคัญมากที่สุด

-ข้อมูลสารสนเทศที่มีระดับความสำคัญปานกลาง

-ข้อมูลสารสนเทศที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล ได้แก่

-ลับที่สุด (Top Secret) หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญมากที่สุดต่อการดำเนินงานของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ และกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือใช้สารสนเทศดังกล่าวได้ การเปิดเผยทั้งหมดหรือบางส่วน หรือการเข้าถึงสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาต จะเกิดความเสียหายแก่ประโยชน์แห่งรัฐหรือศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ อย่างร้ายแรงที่สุด

-ลับมาก (Secret) หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญปานกลางต่อการดำเนินงานของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ และกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น ที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ การเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาต จะเกิดความเสียหายแก่ประโยชน์แห่งรัฐ หรือ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ อย่างร้ายแรง

-ลับ (Confidential) หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญปานกลางต่อการดำเนินงาน ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ และกำหนดให้บุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึง หรือใช้ข้อมูลสารสนเทศดังกล่าวได้ การเปิดเผยหรือการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาต จะเกิดความเสียหายแก่ประโยชน์แห่งรัฐหรือ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

-ใช้ภายใน (Internal Use) หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญต่ำต่อการดำเนินงาน ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ สารสนเทศ ลำดับชั้นใช้ภายในนี้ จะอนุญาตให้ใช้ภายในหน่วยงานที่กำหนดเท่านั้น การเปิดเผยหรือการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้ โดยไม่ได้รับอนุญาตอาจก่อให้เกิดผลกระทบต่อการปฏิบัติงานประจำวัน ของหน่วยงานดังกล่าว หรือเกิดความเสียหายแก่ประโยชน์แห่งรัฐ หรือศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

-ทั่วไป (Public) หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญต่ำต่อ การดำเนินงานของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ สารสนเทศลำดับชั้นทั่วไปนี้ เป็นข้อมูลสารสนเทศที่ผู้บริหารอนุมัติให้เปิดเผยต่อสาธารณะได้ อย่างไรก็ดี ข้อมูลสารสนเทศในระดับชั้นนี้ต้องได้รับการป้องกัน หรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน (Integrity) เพื่อสร้างความเชื่อมั่นให้แก่ผู้ใช้งานสารสนเทศรวมทั้งรักษาภาพลักษณ์และชื่อเสียงของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

(๔) จัดแบ่งระดับชั้นการเข้าถึง ได้แก่

-ระดับชั้นสำหรับผู้บริหาร คือ ผู้อำนวยศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ หรือผู้ที่ได้รับมอบหมาย

-ระดับชั้นสำหรับผู้ใช้งานทั่วไป คือ เจ้าหน้าที่ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ที่มีหน้าที่เกี่ยวข้องและต้องได้รับอนุญาตจากผู้บังคับบัญชา

-ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย คือ เจ้าหน้าที่ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ที่มีหน้าที่เกี่ยวข้องและต้องได้รับอนุญาตจากศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

(๕) การกำหนดเวลาจำนวนช่องทางที่สามารถเข้าถึง

-ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)

-โทรศัพท์หรือโทรสาร (เข้าถึงได้ในเวลาราชการ)

-หนังสือหรือบันทึกข้อความ (เข้าถึงได้ในเวลาราชการ)

-ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

-ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

-ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

-เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา)

-การประชุมทางไกล (เข้าถึงได้ในเวลาราชการ และในช่วงเวลาพิเศษเป็นรายครั้ง)

๑.๑.๔ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงระบบสารสนเทศ โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑) มีการควบคุมการเข้าถึงระบบสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนด ด้านความมั่นคงปลอดภัย

๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน

เพื่อควบคุมการเข้าถึงระบบสารสนเทศให้สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตแล้ว และสร้างความรู้ความเข้าใจให้กับผู้ใช้งานด้านการจัดการโดยการจัดฝึกอบรมหลักสูตรการสร้างความตระหนัก เรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ให้ปฏิบัติ ดังนี้

๑.๒.๑ มีการกำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๑.๒.๒ ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๑.๒.๓ การลงทะเบียนและการระงับสิทธิผู้ใช้งาน

(๑) การลงทะเบียนผู้ใช้งานในระบบสารสนเทศ ให้ผู้ร้องขอ กรอกแบบฟอร์มการลงทะเบียนผู้ใช้งาน ให้ผู้อนุมัติพิจารณาความเหมาะสมของระดับสิทธิที่ร้องขอ เจ้าหน้าที่ผู้ดูแลระบบกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) จัดส่งให้กับผู้ร้องขอ

(๒) การแก้ไขเปลี่ยนแปลงสิทธิผู้ใช้งานในระบบสารสนเทศ ให้ผู้ร้องขอ กรอกแบบฟอร์ม การลงทะเบียนผู้ใช้งานให้ผู้อนุมัติพิจารณาความเหมาะสมของการแก้ไขเปลี่ยนแปลงสิทธิ จากนั้นให้เจ้าหน้าที่ผู้ดูแลระบบดำเนินการแก้ไขเปลี่ยนแปลงสิทธิผู้ใช้งาน

(๓) การระงับสิทธิผู้ใช้งานในระบบสารสนเทศ ให้ผู้ร้องขอ กรอกแบบฟอร์มการลงทะเบียนผู้ใช้งานให้ผู้อนุมัติพิจารณาการระงับสิทธิ จากนั้นให้เจ้าหน้าที่ผู้ดูแลระบบดำเนินการระงับสิทธิผู้ใช้งาน

(๔) ต้องกำหนดให้มีการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งานในการเข้าถึงข้อมูลหรือระบบสารสนเทศตามหน้าที่ความรับผิดชอบ

(๕) ต้องจัดทำเอกสารการมอบหมายสิทธิการเข้าถึงข้อมูลหรือระบบสารสนเทศ และจัดเก็บไว้เป็นหลักฐานในการดำเนินงาน

๑.๒.๔ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

(๒) การกำหนดชื่อผู้ใช้งาน (User Name) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำ ให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานอื่น

(๓) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

(๔) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ โดยให้ผู้ร้องขอ กรอกแบบฟอร์มการลงทะเบียนผู้ใช้งานให้ผู้อนุมัติพิจารณาความเหมาะสมในการขอใช้งานสิทธิผู้ดูแลระบบระดับสูงสุด จากนั้นให้เจ้าหน้าที่ผู้ดูแลระบบ จัดส่งชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ให้กับผู้ร้องขอ เมื่อใช้งานเสร็จสิ้น ให้ดำเนินการส่งคืนรหัสผ่านให้กับผู้ดูแลระบบ จากนั้นผู้ดูแลระบบต้องดำเนินการเปลี่ยนรหัสผ่านใหม่และจัดเก็บซองรหัสผ่านในตู้ที่มีการปิดล็อกอย่างมั่นคงปลอดภัย

๑.๒.๕ การบริหารจัดการรหัสผ่านสาหรับผู้ใช้งาน (User Password Management) ให้ผู้ดูแลระบบจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) คารต้องมีการเปลี่ยนรหัสผ่านทุก ๆ ๖ เดือน หรือทันทีที่ได้รับสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหล

(๒) จำนวนตัวอักษรมากกว่าหรือเท่ากับ 6 ตัวอักษร

(๓) ต้องมีการผสมกันระหว่างตัวอักษรอักขระอย่างน้อย 2 ประเภท ดังนี้

-ตัวเลข (Numerical Character)

-ตัวอักษร (Alphabet)

-ตัวอักขระพิเศษ (Special Character)

(๔) ไม่ตั้งรหัสผ่านด้วย ชื่อ วันเดือนปีเกิด หรือข้อความใดที่ง่ายต่อการล่วงรู้หรือง่ายต่อการคาดเดา

(๕) กำหนดให้ระบบปฏิบัติการ Microsoft Windows และ อุปกรณ์เครือข่าย ไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย ๕ รหัสผ่านที่เคยใช้งานล่าสุด

(๖) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ห้ามใช้บุคคลอื่นในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(๗) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน และผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

(๘) เปลี่ยนรหัสผ่านตั้งต้นของระบบสารสนเทศทันทีหลังจากติดตั้งระบบสารสนเทศใหม่

(๙) การเปลี่ยนรหัสผ่าน ต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๑๐) จำกัดเวลาการเชื่อมต่อสาหรับระบบสารสนเทศที่มีความเสี่ยงสูง หรือระบบสารสนเทศที่มีความสำคัญ เพื่อลดโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต

๑.๒.๖ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น เพื่อให้มั่นใจว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม โดยผู้ดูแลระบบ ดำเนินการรวบรวมรายการสิทธิ ของผู้ใช้งานในระบบต่าง ๆ และบันทึกลงในแบบฟอร์มการดำเนินการทบทวนสิทธิ เพื่อส่งให้ผู้ใช้งาน หรือหน่วยงานต้นสังกัดของผู้ใช้งาน พิจารณาทบทวนความเหมาะสมของสิทธิการเข้าถึงระบบสารสนเทศ ในปัจจุบัน โดยหากต้องการปรับปรุงแก้ไขสิทธิ ให้แจ้งผู้ดูแลระบบเพื่อดำเนินการปรับปรุงแก้ไขสิทธิ ตามผลการทบทวน

๑.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ ให้ปฏิบัติดังนี้

๑.๓.๑ การกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

(๑) ผู้ดูแลระบบต้องมีการบริหารจัดการรหัสผ่าน และส่งให้ผู้ใช้บริการ

(๒) ควรตั้งรหัสผ่านที่ยากต่อการคาดเดา และให้มีตัวอักษรจานวนมากกว่าหรือเท่ากับ ๖ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๓) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๔) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๕) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๖) เก็บรักษารหัสผ่านไว้เป็นความลับ

(๗) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๘) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(๙) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๐) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๑) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๒) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบสารสนเทศต่าง ๆ ที่ตนใช้งาน

(๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๔) ผู้ดูแลระบบต้องเปลี่ยนรหัสถี่กว่าผู้ใช้งานทั่วไป

๑.๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ สามารถเข้าถึงอุปกรณ์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๒) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๑.๓.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(๑) ผู้ดูแลระบบ ต้องกำหนดมาตรการป้องกันสินทรัพย์ขององค์กรให้ครอบคลุมเรื่องต่าง ๆ โดยควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น การจัดการบริเวณล้อมรอบ การควบคุมการเข้า-ออก การจัดบริเวณการเข้าถึง การส่งผลิตภัณฑ์ โดยบุคคลภายนอก การวางอุปกรณ์ ระบบและอุปกรณ์สนับสนุนการทำงาน เป็นต้น

(๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่าง ๆ ดังนี้

-แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ

-กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ

-วัฒนธรรมองค์กร

(๓) ผู้ดูแลระบบ ต้องกำหนดให้มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน และต้องกำหนดให้ผู้ใช้งาน ออกจากระบบโดยทันทีเมื่อเสร็จสิ้นงาน

(๔) มีการกำหนดขอบเขตของการป้องกัน ดังนี้

-ผู้ใช้งานต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันสินทรัพย์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

-ผู้ใช้งานต้องลงชื่อออกจากระบบทันที เมื่อไม่ได้ใช้งาน หรือจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

-จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

-ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

-นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

(๕) มีมาตรการทำลายสื่อบันทึกข้อมูล และข้อมูลอิเล็กทรอนิกส์ ดังนี้

-ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรืออุปกรณ์บันทึกข้อมูลอื่นโดยการฟอร์แมตอุปกรณ์ดังกล่าวให้ไม่สามารถเรียกข้อมูลกลับมาได้ ก่อนทำการเปลี่ยน ทดแทน ทำลาย หรือจำหน่าย

-ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติในการทำลายอุปกรณ์บันทึกข้อมูลหรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

๑.๓.๔ การจัดหาและการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงจากระบบที่มีอยู่เดิม ต้องมีการวิเคราะห์และระบุข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศไว้ด้วย โดยนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

(๑) ต้องมีระบบล็อกอินเข้าใช้งานระบบสารสนเทศ และต้องมีการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ

(๒) ต้องมีระบบป้องกันการรักษาความปลอดภัย ของข้อมูลสารสนเทศให้กับระบบสารสนเทศที่เป็นแบบเว็บแอพพลิเคชั่นโดยใช้การเข้ารหัสข้อมูลผ่านโปรโตคอล

๑.๔ การควบคุมการเข้าถึงเครือข่าย

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ให้ผู้ดูแลระบบปฏิบัติ ดังนี้

๑.๔.๑ การใช้บริการเครือข่าย ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของ การให้บริการ ได้แก่ โซนภายใน (Internal Zone) และ โซนภายนอก (External Zone) เพื่อควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ และต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) ผู้ดูแลระบบต้องกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้มีการใช้งานได้

(๒) มีข้อปฏิบัติสำหรับผู้ใช้งาน ให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น พร้อมทั้งจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้ากลุ่มบริหารงานทั่วไปและแผนงาน หรือผู้ดูแลระบบที่ได้รับมอบหมาย ก่อนที่จะใช้งานในทุกกรณี

(๓) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยผู้ดูแลระบบต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๑.๔.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

(๑) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน จะต้องได้รับการอนุมัติจากหัวหน้ากลุ่มบริหารงานทั่วไปและแผนงานก่อนทุกครั้ง และมีการควบคุมอย่างเข้มงวด โดยผู้ใช้งานจะต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการขออนุญาต อย่างเพียงพอ

(๒) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (User Name) ทุกครั้ง และผู้ดูแลระบบจะต้องตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ อย่างน้อย ๑ วิธี เช่น มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม เป็นต้น

(๓) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

(๔) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตที่ใช้ไว้ตลอดเวลาโดยไม่จำเป็น ควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๑.๔.๓ การระบุอุปกรณ์บนเครือข่าย ผู้ดูและระบบต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๑) การควบคุมการใช้งานอย่างเหมาะสม และจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้ โดยผู้ขอใช้บริการ จะต้องได้รับการอนุญาตจากหัวหน้ากลุ่มบริหารงานทั่วไปและแผนงานก่อนทุกครั้ง

(๒) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์ โดยผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย เช่น รายชื่อผู้ขอใช้บริการ IP Address Mac Address และผังเครือข่าย เป็นต้น

(๓) อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของต้นทางและปลายทางได้

๑.๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่ง ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

(๑) ผู้ดูแลระบบ ต้องกำหนดการเปิด -ปิด พอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุม การเข้าถึงของอุปกรณ์เครือข่ายต่างๆ และปิดพอร์ตที่เสี่ยงต่อการก่อให้เกิดความเสียหายต่อระบบเครือข่ายและอุปกรณ์ที่ไม่มีความจำเป็นในการใช้งาน

(๒) บุคคลภายนอกที่เข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายต้องได้รับการอนุญาตจากผู้ดูแลระบบ

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบ ให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๑.๔.๕ การแบ่งแยกเครือข่าย ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายภายในหน่วยงาน และเครือข่ายภายนอกหน่วยงาน

๑.๔.๖ การควบคุมการเชื่อมต่อเครือข่าย ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ดังนี้

(๑) ผู้ดูแลระบบต้องมีการตรวจสอบการเชื่อมต่อเครือข่าย

(๒) จำกัดสิทธิของผู้ใช้ในการเชื่อมต่อเครือข่าย

(๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(๔) ผู้ดูแลระบบต้องมีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ผู้ดูแลระบบต้องควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๑.๔.๗ การควบคุมการจัดเส้นทางบนเครือข่าย ผู้ดูแลระบบ ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลสารสนเทศ ดังนี้

(๑) ควบคุมไม่ให้มีการเปิดเผยการใช้หมายเลขเครือข่าย (IP Address)

(๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมต่อเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๑.๔.๘ การควบคุมการเข้าใช้งานระบบจากระยะไกล (Remote Access)

(๑) ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) ต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

(๓) ผู้ใช้งานต้องแสดงหลักฐานและเหตุผลความจำเป็น และต้องได้รับอนุมัติจากหัวหน้ากลุ่มบริหารงานทั่วไปและแผนงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๔) มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม ต้องดูแลและจัดการโดยผู้ดูแลระบบ และต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๑.๕ การควบคุมการเข้าถึงระบบปฏิบัติการ

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาตให้ปฏิบัติ ดังนี้

๑.๕.๑ ผู้ดูแลระบบ (System Administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ และกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของ เครื่องคอมพิวเตอร์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

๑.๕.๒ การเข้าใช้งานและการเข้าถึงระบบปฏิบัติการ

(๑) ผู้ดูแลระบบ ต้องจัดไม่ให้ระบบปฏิบัติการแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบปฏิบัติการก่อนที่การเข้าสู่ระบบปฏิบัติการจะเสร็จสมบูรณ์

(๒) ระบบปฏิบัติการต้องสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๑.๕.๓ การระบุและยืนยันตัวตนของผู้ใช้งาน ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง ดังนี้

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ให้เป็นไปตามการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน ใน ข้อที่ ๑.๓.๑

(๒) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น Smart Card เป็นต้น

๑.๕.๔ การใช้งานโปรแกรมอรรถประโยชน์ ผู้ดูแลระบบต้องจำกัด และควบคุมการใช้งานโปรแกรมอรรถประโยชน์สาหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิด สามารถทาให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ หรือที่มี อยู่แล้ว โดยให้ผู้ดูแลระบบดำเนินการ ดังนี้

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ ห้ามลงโปรแกรมที่ละเมิดลิขสิทธิ์ และลงโปรแกรมได้ไม่เกิน 10 โปรแกรมเท่านั้น

(๒) ให้ผู้ดูแลระบบตรวจสอบโปรแกรมอรรถประโยชน์ และต้องได้รับการอนุญาต จากผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพหรือผู้ดูแลระบบที่ได้รับมอบหมาย ก่อนการใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๑.๕.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง ให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out) เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๑) กรณีระบบสารสนเทศทั่วไป ให้ยุติการใช้งานเมื่อว่างเว้นจากการใช้งานเป็นเวลา ๑๕ นาที

๑.๕.๖ การจากัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ ต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางและต้องจำกัดระยะเวลาในการเชื่อมต่อ เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น โดยกำหนดให้ใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง หรือกำหนดให้ ใช้งานได้เฉพาะในช่วงเวลาการทำงานของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ตามปกติ เป็นต้น

๑.๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

ผู้ดูแลระบบต้องมีการควบคุม อย่างน้อยดังนี้

๑.๖.๑ การจำกัดการเข้าถึงระบบสารสนเทศ ผู้ดูแลระบบต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงระบบสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยเป็นไปตามหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึง หรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงระบบสารสนเทศที่ได้กำหนดไว้

๑.๖.๒ ระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ผู้ดูแลระบบต้องมีการควบคุมและให้ดำเนินการ ดังนี้

(๑) แยกระบบสารสนเทศซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ได้แก่

-ระบบงานสารบรรณ

-ระบบงานพัสดุ

-ระบบงานวิชาการ

-ระบบงานฐานข้อมูลอ้างอิงกลาง

(๒) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวใน โดยเฉพาะ

(๓) มีการควบคุมอุปกรณ์คอมพิวเตอร์ ระบบสื่อสารและการปฏิบัติงานจากภายนอกหน่วยงาน ที่เกี่ยวข้องกับระบบดังกล่าว

๑.๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่ ผู้ดูแลระบบต้องมีการกำหนด แนวปฏิบัติและมาตรการที่เหมาะสมในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่ เพื่อปกป้องข้อมูลสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่ และต้องไม่ให้บุคคลภายนอกคัดลอกข้อมูลสารสนเทศจากอุปกรณ์คอมพิวเตอร์ที่นำไปใช้ได้ มีการเก็บข้อมูลเกี่ยวกับอุปกรณ์คอมพิวเตอร์เคลื่อนที่ ชื่อผู้ใช้งาน ซึ่งหากปรากฏความเสียหายร้ายแรง ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น นอกจากนี้ ผู้ใช้งาน ต้องปฏิบัติ ดังนี้

(๑) เครื่องคอมพิวเตอร์ที่ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ มอบให้ผู้ใช้งาน เป็นทรัพย์สินของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ดังนั้น ผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ เท่านั้น

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ต้องเป็นโปรแกรมที่ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือนำไปให้ผู้อื่นใช้งาน

(๓) ผู้ใช้งาน มีหน้าที่ดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ และต้องรับผิดชอบ ต่อความเสียหายที่อาจเกิดขึ้นนั้นด้วย

(๔) ปิดเครื่องคอมพิวเตอร์เมื่อไม่ใช้งานหรือเสร็จสิ้นการใช้งานแล้วในทันที

(๕) ทำการล็อคหน้าจอเครื่องคอมพิวเตอร์หลังจากที่ไม่ได้ใช้งานเป็นเวลา ๕ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

(๖) การนำเครื่องคอมพิวเตอร์มาใช้กับระบบเครือข่ายของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ต้องพิสูจน์ตัวตนผ่านระบบพิสูจน์ตัวตนก่อนเข้าใช้งานทุกครั้ง

(๗) ไม่อนุญาตให้เข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม

(๘) ห้ามผู้ใช้งานใช้อุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่กระทาความผิด ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๑.๖.๔ การปฏิบัติงานจากภายนอกหน่วยงาน ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน ผู้ดูแลระบบต้องกำหนดขั้นตอนการขออนุมัติการปฏิบัติงานจากภายนอกหน่วยงาน กำหนดสิทธิหรือระงับสิทธิ การเข้าถึงระบบสารสนเทศ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งในการปฏิบัติงานจากภายนอกหน่วยงาน หากปรากฏความเสียหายร้ายแรง ผู้ปฏิบัติงานจากภายนอกหน่วยงานต้องรับผิดชอบต่อความเสียหาย ที่เกิดขึ้น นอกจากนี้ ผู้ใช้งาน ต้องปฏิบัติ ดังนี้

(๑) กรอกแบบฟอร์มการขอใช้งานจากภายนอก

(๒) ชี้แจงแผนงานและขั้นตอนปฏิบัติ เพื่อเสนอการขออนุมัติการขอใช้งานจากภายนอก

(๓) ตรวจสอบการทางานอย่างเคร่งครัด

๑.๖.๕ ในกรณีที่ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ได้มีการว่าจ้างกับบริษัทต่าง ๆ เพื่อดำเนินโครงการของการพัฒนาระบบสารสนเทศ ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ และต้องลงนามในสัญญาการว่าจ้างกับบริษัทต่าง ๆ ให้มีการจัดทำเอกสารแนบท้ายสัญญาว่าด้วยการรักษาข้อมูลที่เป็นความลับด้านระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลสารสนเทศ ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ กับบริษัทคู่สัญญา โดยมีการกำหนดมาตรการ ดังนี้

(๑) ผู้รับจ้างมีหน้าที่ในการคัดสรรพนักงานที่เข้ามาดำเนินโครงการของการพัฒนาระบบสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ จะต้องไม่เคยเป็นผู้มีความผิดเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ ระหว่างการจ้างผู้รับจ้างมีหน้าที่และความรับผิดชอบในการควบคุมดูแลพนักงานของผู้รับจ้างให้รักษาข้อมูลที่เป็นความลับเช่นเดียวกับที่ผู้รับจ้างต้องปฏิบัติ ผู้รับจ้างจะต้องใช้ความระมัดระวังอย่างที่สุดตามที่ผู้ประกอบวิชาชีพจะพึงมีในการรักษาข้อมูลที่เป็นความลับอย่างเคร่งครัด โดยไม่บอกหรือเปิดเผยข้อมูลที่เป็นความลับแก่บุคคลภายนอกรู้ ไม่ว่ากรณีใด ๆ ทั้งสิ้น เว้นแต่เพื่อความจำเป็นในการปฏิบัติงานตามหน้าที่ของผู้รับจ้างตามสัญญาหลักเท่านั้น ต้องเสริมสร้างความเข้าใจอันดีต่อพนักงานทุกคน เพื่อให้การปฏิบัติ และการบริหารงานด้านการรักษาข้อมูลบังเกิดผลมากที่สุด

(๒) เมื่อสิ้นสุดการปฏิบัติงานตามสัญญาหลักหรือสัญญาหลักสิ้นสุดลงไม่ว่าด้วยเหตุใด ๆ ผู้รับจ้างต้องคืนเอกสาร แบบแปลน พิมพ์เขียว หรือคู่มือปฏิบัติงานเกี่ยวกับงานที่ว่าจ้างที่ได้รับไป จากผู้ว่าจ้างทันที และมิให้ทำสำเนาไว้ไม่ว่าในรูปของเอกสารหรือข้อมูลอิเล็กทรอนิกส์อื่นใดทั้งสิ้น

๑.๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑.๗.๑ ผู้ดูแลระบบ ต้องดำเนินการดังต่อไปนี้

(๑) ทำการลงทะเบียนผู้ใช้งานระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนอนุญาตให้เข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

(๒) ทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้เชื่อมต่อกับระบบเครือข่ายไร้สาย

(๓) ควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๔) ทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(๕) เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงาน ของอุปกรณ์ไร้สายและควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

(๗) เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (User Name) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้ (User Name) รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้

(๘) มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

(๙) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่๑๑ ทราบโดยทันที

๑.๗.๒ ผู้ใช้งานที่จะใช้งานระบบเครือข่ายไร้สายของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจาก ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่๑๑ หรือผู้ดูแลระบบที่ได้รับมอบหมาย ระมัดระวังความปลอดภัยในการใช้งานเครือข่ายไร้สาย และต้องใช้งานผ่านบัญชีผู้ใช้ของตนเอง

๑.๗.๓ ผู้ใช้งาน ต้องไม่ดำเนินการดังต่อไปนี้

(๑) นำอุปกรณ์ไร้สาย มาติดตั้งหรือเปิดใช้งานเองในศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ไม่ว่าจะเป็น Access Point, Wireless Routers, Wireless USB Client หรือ Wireless Card

(๒) เปิดระบบเครือข่ายไร้สายแบบจุดต่อจุด (Ad-Hoc) หรือ Peer-to-Peer Network

(๓) นำรหัสผ่านที่ได้รับอนุญาตไปทำการเปิดเผยต่อผู้อื่นหรือสาธารณะ

(๔) โอน จำหน่าย หรือจ่ายแจกสิทธิที่ผู้ใช้งานได้รับ ให้กับผู้อื่น

(๕) ให้ผู้อื่นใช้งานผ่านบัญชีผู้ใช้ของตน หากเกิดปัญหาใด ๆ เจ้าของบัญชีจะต้องเป็นผู้รับผิดชอบทุกกรณี

๑.๘ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑.๘.๑ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อบนสายสัญญาณและอุปกรณ์

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ต้องป้องกันการเข้าถึงของบุคคลภายนอก

(๗) สำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๑.๘.๒ การบำรุงรักษาอุปกรณ์

(๑) ให้มีการบำรุงรักษาอุปกรณ์ ได้แก่ อุปกรณ์เครือข่าย อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สนับสนุน ตามรอบระยะเวลา และปฏิบัติตามคำแนะนำของผู้ผลิต

(๒) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์ทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๓) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่ตรวจสอบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว จากนั้นดำเนินการรายงานสรุปผลการเฝ้าระวังเหตุการณ์ให้ผู้บังคับบัญชาและผู้ที่เกี่ยวข้องทราบเป็นประจำทุกเดือน

(๔)ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

(๕) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑.๘.๓ การนำสินทรัพย์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ออกนอกหน่วยงาน

(๑) ต้องขออนุญาตก่อนนำอุปกรณ์หรือสินทรัพย์นั้นออกไปใช้งาน

(๒) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งาน

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ต้องตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ออกไปใช้งาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๑.๘.๔ การป้องกันอุปกรณ์ที่นำไปใช้นอกศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือสินทรัพย์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์ เป็นต้น

(๒) ให้เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์เสมือนเป็นสินทรัพย์ของตนเอง

๑.๘.๕ การกำจัดอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว โดยเมื่อต้องการทำลายสื่อบันทึกข้อมูล หรือถึงรอบการทำลายสื่อบันทึกข้อมูลตามแบบฟอร์มบันทึกรายการสินทรัพย์ผู้ร้องขอต้องกรอกแบบฟอร์มขอทำลายสื่อบันทึกข้อมูล และส่งต่อให้แก่ผู้เชี่ยวชาญด้านพัฒนาความมั่นคงปลอดภัยสารสนเทศหรือเจ้าหน้าที่ส่วนบริหารคอมพิวเตอร์และเครือข่ายที่ได้รับมอบหมาย เพื่อขออนุมัติการทำลายสื่อบันทึกข้อมูล

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๑.๘.๖ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารที่เกี่ยวข้องกับระบบสารสนเทศ

(๑) จัดเก็บเอกสารไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ให้เจ้าของระบบสารสนเทศมีหน้าที่ควบคุมการเข้าถึงและการทำลายเอกสาร

(๓) ให้มีการควบคุมการเข้าถึงเอกสารที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ

(๔) การขอขึ้นทะเบียนเอกสาร ให้กรอกแบบฟอร์มคำร้องขอดำเนินการเกี่ยวกับเอกสาร เพื่อขึ้นทะเบียนเอกสาร โดยให้ผู้บังคับบัญชาพิจารณาอนุมัติการขึ้นทะเบียนเอกสาร จากนั้นนายทะเบียนเอกสารดำเนินการประกาศให้ผู้ที่เกี่ยวข้องรับทราบ

(๕) การทบทวนเอกสาร ผู้ได้รับมอบหมายให้เป็นผู้ควบคุมทะเบียนเอกสาร แจ้งเจ้าของเอกสารเมื่อถึงรอบการทบทวนเอกสารรับทราบ ผู้จัดทำเอกสารดำเนินการทบทวนเอกสารตามรอบการทบทวน และประกาศผลการทบทวนเอกสาร

๑.๙ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

๑.๙.๑ การใช้งานทั่วไป ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) เครื่องคอมพิวเตอร์ที่ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ อนุญาตให้ผู้ใช้งาน เป็นสินทรัพย์ของ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ต้องเป็นโปรแกรมที่ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ เท่านั้น

(๕) ก่อนการใช้งานกับสื่อบันทึกข้อมูลแบบพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสคอมพิวเตอร์โดยโปรแกรมป้องกันไวรัสคอมพิวเตอร์

(๖) ไม่เก็บข้อมูลสำคัญของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่

(๗) ไม่นำอาหาร เครื่องดื่ม หรือสิ่งที่เป็นของเหลว มาวางใกล้บริเวณเครื่องคอมพิวเตอร์

(๘) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

(๙) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับ เครื่องคอมพิวเตอร์แบบพกพาเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากที่สูง เป็นต้น

(๑๐) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๑๑) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๑๒) ไม่วางของทับบนเครื่องคอมพิวเตอร์ หรือแป้นพิมพ์

(๑๓) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย

(๑๔) ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อยที่ติดตั้งอยู่ภายในเครื่องคอมพิวเตอร์รวมถึงแบตเตอรี่

๑.๙.๒ การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD DVD หรือ External Hard Disk เป็นต้น

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เนื่องจากหากมีความเสียหายเกิดขึ้นต่อ Hard Disk อาจก่อให้เกิดผลกระทบต่อการดำเนินการของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ได้

๑.๑๐ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๑.๑๐.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๑.๑๐.๒ เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๑.๑๐.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

๑.๑๐.๔ ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ใน สื่อบันทึกข้อมูลก่อน เป็นต้น

๑.๑๑ การใช้งานระบบอินเทอร์เน็ต

๑.๑๑.๑ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ จัดสรรไว้เท่านั้น เช่น Proxy Firewall เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เว้นแต่มีเหตุผลความจำเป็นและได้รับอนุมัติจากหัวหน้ากลุ่มบริหารทั่วไปและแผนงานหรือผู้ดูแลระบบ ที่ได้รับมอบหมายแล้วเท่านั้น

๑.๑๑.๒ จะต้องมีการตั้งค่าเครื่องคอมพิวเตอร์ เพื่อทำการอุดช่องโหว่ ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ต

๑.๑๑.๓ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ และต้องไม่ใช้ระบบอินเทอร์เน็ต ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงแห่งชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อ ความเสียหายให้กับศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ เป็นต้น

๑.๑๑.๔ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๑.๑๑.๕ ห้ามดาวน์โหลดโปรแกรมใช้งาน จากระบบอินเทอร์เน็ตที่เป็นการละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๑.๑๑.๖ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ไม่เสนอความคิดเห็น ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสีย ต่อชื่อเสียงของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ หรือทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๑.๑๑.๗ ผู้ใช้งานต้องทำการปิดเว็บบราวเซอร์เมื่อสิ้นสุดการใช้งาน เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๑.๑๒ การใช้งานอุปกรณ์ป้องกันการบุกรุก (Firewall)

๑.๑๒.๑ ต้องกำหนดเงื่อนไขของการเชื่อมต่อหรือการให้บริการที่ได้รับอนุญาตเท่านั้น โดยกำหนดเงื่อนไขเป็น Deny All Allow Some คือ ห้ามทุกการเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก เว้นแต่จะได้รับการอนุญาต

๑.๑๒.๒ เงื่อนไขการเชื่อมต่อหรือการให้บริการที่กำหนดว่าได้รับอนุญาตให้ผ่านอุปกรณ์ป้องกันการบุกรุกได้ จะต้องบันทึกเป็นเอกสาร และสำเนาให้กับผู้ดูแลระบบรับทราบ โดยเงื่อนไขของการอนุญาตจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบและรายงานให้ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ทราบ

๑.๑๒.๓ เส้นทางการสื่อสารคอมพิวเตอร์ที่เข้าออกจากศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ จะต้องได้รับการติดตั้งอุปกรณ์ป้องกันการบุกรุกในทุกเส้นทาง

๑.๑๒.๔ ต้องไม่อนุญาตให้การสื่อสารจากภายนอกองค์กร ผ่านเข้าไปในองค์กรได้ โดยจะยอมให้เข้ามาในส่วน ที่ได้รับอนุญาตเท่านั้น

๑.๑๒.๕ หากมีการเพิ่มเติมหรือเปลี่ยนแปลงเส้นทางการสื่อสารคอมพิวเตอร์ จะต้องได้รับ การอนุญาตจากผู้ดูแลระบบก่อน และต้องมีการตรวจสอบผลกระทบกับอุปกรณ์ป้องกันการบุกรุก และเงื่อนไขที่ตั้งให้กับอุปกรณ์ป้องกันการบุกรุก

๑.๑๒.๖ อุปกรณ์ป้องกันการบุกรุกที่นำมาใช้งาน จะต้องทำหน้าที่ป้องกันการบุกรุกเพียงอย่างเดียวโดยไม่ทำหน้าที่อื่น ๆ เช่น AntiVirus Gateway เป็นต้น

๑.๑๒.๗ ผู้ดูแลระบบจะต้องตรวจสอบการทำงานของอุปกรณ์ป้องกันการบุกรุก จากบันทึก การทำงาน (Log File) อย่างสม่ำเสมอ อย่างน้อยทุกสัปดาห์ และรายงานให้ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ทราบเป็นรายเดือน

๑.๑๒.๘ การเปลี่ยนแปลงใด ๆ ที่เกี่ยวกับอุปกรณ์ป้องกันการบุกรุกจะต้องได้รับการบันทึก อย่างน้อยต้องประกอบด้วยการตั้งค่าการเชื่อมต่อ หรือบริการที่ได้รับอนุญาต

๑.๑๒.๙ อุปกรณ์ป้องกันการบุกรุกจะต้องได้รับการป้องกันจากการเข้าถึงทางกายภาพ โดยจะต้องติดตั้งในห้องที่มีการรักษาความปลอดภัย มีการล็อก โดยอนุญาตให้ผู้ดูแลระบบเท่านั้นที่สามารถเข้าถึงได้

๑.๑๒.๑๐ ข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่เข้า-ออกอุปกรณ์ป้องกันการบุกรุก จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูล โดยจะต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไม่น้อยกว่า ๙๐ วัน

๑.๑๒.๑๑ ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ มีสิทธิที่จะระงับการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่า จะได้รับการแก้ไข

๑.๑๒.๑๒ ผู้ละเมิดนโยบายด้านความปลอดภัยของอุปกรณ์ป้องกันการบุกรุก จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

๑.๑๓ การใช้งานเครือข่ายสังคมออนไลน์

๑.๑๓.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ได้กำหนดไว้เท่านั้น

๑.๑๓.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัย อยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ จากการใช้งานเครือข่ายสังคมออนไลน์

๑.๑๓.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ผู้ใช้งานต้องแจ้งต่อ ประธาน หรือคณะกรรมการรักษาความมั่งคงปลอดภัยระบบสารสนเทศของหน่วยงานให้เร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑.๑๔ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์

๑.๑๔.๑ ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษา ความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ กำหนดชั้นความลับในการเข้าถึง

๑.๑๔.๒ ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้

๑.๑๔.๓ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

๑.๑๔.๔ ต้องมีวิธีป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ได้แก่ ผู้ตรวจสอบระบบสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ (IT Auditor) หรือบุคคลที่ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ มอบหมาย

๒. แนวปฏิบัติระบบสำรองของสารสนเทศ และแผนเตรียมความพร้อมกรณีฉุกเฉิน

เพื่อให้ระบบสารสนเทศของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ สามารถให้บริการได้อย่างต่อเนื่อง จึงกำหนดแนวปฏิบัติระบบสำรองของระบบสารสนเทศ เป็นผู้รับผิดชอบ ดังนี้

๒.๑ ผู้ดูแลระบบต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสม ให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๒.๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

-กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

-กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทาการสำรองเช่น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

-บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรองสำเร็จ/ไม่สำเร็จเป็นต้น

-ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลการคอนฟิกกูเรชั่น ข้อมูลในฐานข้อมูล เป็นต้น

-จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

-จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับศูนย์สนับสนุนบริการสุขภาพที่๑๑ ควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับศูนย์สนับสนุนบริการสุขภาพที่๑๑ เช่น ไฟไหม้ เป็นต้น

-ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

-ทดสอบบันทึกข้อมูลที่สำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

-จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

-ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๒.๒ ให้ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุง แผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

๒.๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๒.๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๒.๓ หัวหน้ากลุ่มบริหารทั่วไปและแผนงาน ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองและการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณี ที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๒.๔ ผู้ดูแลระบบต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๕ ผู้ดูแลระบบมีการทบทวนระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ของศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ อย่างน้อยปีละ ๑ ครั้ง

๒.๖ ผู้ดูแลระบบต้องกำหนดชนิดของข้อมูลและระยะเวลาที่ต้องการจะสำรองข้อมูล ว่าข้อมูล ที่ต้องการสำรองเป็นข้อมูลชนิดใด และต้องใช้พื้นที่สำหรับการสำรองข้อมูลเท่าใด

๒.๗ ผู้ดูแลระบบต้องจัดทำการสำรองข้อมูลแบบบางส่วน (Incremental Backup) อย่างน้อยสัปดาห์ละ ๑ ครั้ง

๒.๘ ผู้ดูแลระบบต้องจัดทำการทดสอบการกู้กลับคืนของข้อมูล (Restore) ทุก ๖ เดือน

๒.๙ ผู้ดูแลระบบต้องจัดให้มีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๒.๑๐ ข้อมูลที่สำรองและถูกจัดลำดับความสำคัญมากที่สุด ต้องมีการสำรองข้อมูลมากกว่า ๑ ชุด และต้องทำการสำรองข้อมูลไปยังสถานที่อื่นเพื่อความปลอดภัย

๓. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ และเพื่อเป็นการป้องกันและ ลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ จึงกำหนดแนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมอบหมายให้หัวหน้ากลุ่มบริหารทั่วไปและแผนงาน และผู้ตรวจสอบภายใน (Internal Auditor) แต่งตั้งโดยศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ ดังนี้

๓.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) โดยผู้ตรวจสอบภายใน (Internal Auditor) แต่งตั้งโดย ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้ศูนย์สนับสนุนบริการสุขภาพที่ ๑๑ ได้ทราบถึงระดับความเสี่ยงและระดับ ความมั่นคงปลอดภัยสารสนเทศ

๓.๒ แนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง มีดังนี้

๓.๒.๑ ต้องมีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๒ ต้องมีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๓ ต้องมีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๓.๒.๔ ต้องมีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ต้องแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ลงชื่อ ..... ประธานคณะกรรมการรักษาความมั่นคงฯ

(นายวันชัย มั่นสัมฤทธิ์)

ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๑๑

ลงชื่อ ..... คณะทำงาน

(นายสุเทพ พ่วงแม่กลอง)

รองวิชาการ

ลงชื่อ ..... คณะทำงาน

(นายประโชติ สุวรรณรัตน์)

รองบริหาร

ลงชื่อ ..... คณะทำงาน

(นายธีรเดช ภัทรวโรดม)

หัวหน้ากลุ่มบริหารงานทั่วไปและแผนงาน

ลงชื่อ ..... คณะทำงาน/เลขานุการ

(นายชาญศิลป์ แสงอรุณ)

ช่างฝีมือโรงงาน ช๔