

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

โรงพยาบาลโนนไทย

เพื่อให้โรงพยาบาลโนนไทยสามารถปฏิบัติงานได้ตามแนวทางปฏิบัติ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ได้อย่างมีประสิทธิภาพและมีมาตรฐานในระดับเดียวกัน งานสารสนเทศจึงได้วางแนวทางให้เจ้าหน้าที่ของโรงพยาบาลโนนไทยใช้ในการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ สำหรับนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศฉบับนี้ประกอบไปด้วย

ส่วนที่ 1 นโยบายควบคุมการเข้าถึงและการทำงานของระบบสารสนเทศ

1. การควบคุมการเข้าถึงและใช้งานสารสนเทศ (access control)
2. การบริหารจัดการเข้าถึงของผู้ใช้งาน (user access management)
3. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)
4. การควบคุมการเข้าถึงเครือข่าย (network access control)
5. การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)
6. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (application and information access control)
7. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (wireless access control)
8. การรักษาความมั่นคงปลอดภัยทางด้านการภาพและสิ่งแวดล้อม (physical and environmental security)
9. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
10. การใช้งานคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา
11. การบริหารจัดการการเข้าถึงข้อมูลตามลำดับชั้นความลับ
12. การใช้งานระบบอินเทอร์เน็ต (internet)
13. การใช้งานเครือข่ายสังคมออนไลน์ (social network)
14. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (log)

ส่วนที่ 2 นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

ส่วนที่ 3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ 4 นโยบายสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

ส่วนที่ 1

นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

1. เพื่อให้มีแนวทางปฏิบัติในการรักษาความปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน
2. เพื่อให้ผู้รับผิดชอบผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดได้อย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความปลอดภัย

ผู้รับผิดชอบ

1. ศูนย์สารสนเทศ

แนวปฏิบัติ

1. การควบคุมการเข้าถึงและใช้งานสารสนเทศ (access control)

- 1.1 จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน
- 1.2 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้
 - (1) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น
 - อ่านอย่างเดียว
 - สร้างข้อมูล
 - ป้อนข้อมูล
 - แก้ไข
 - อนุมัติ
 - ไม่มีสิทธิ
 - (2) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของ ผู้ใช้งาน (user access management) ที่ได้กำหนดไว้
 - (3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับ มอบหมาย
- 1.3 ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล
 - (1) จัดแบ่งประเภทของข้อมูล ออกเป็น
 - ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
 - ข้อมูลสารสนเทศของผู้รับบริการ เช่น ข้อมูลประวัติการรักษา ต่าง ๆ เป็นต้น

- (2) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น 3 ระดับ คือ
 - ข้อมูลที่มีระดับความสำคัญมากที่สุด
 - ข้อมูลที่มีระดับความสำคัญปานกลาง
 - ข้อมูลที่มีระดับความสำคัญน้อย
- (3) จัดแบ่งลำดับชั้นความลับของข้อมูล
 - ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย อย่างร้ายแรงที่สุด
 - ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย อย่างร้ายแรง
 - ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
 - ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้
- (4) จัดแบ่งระดับชั้นการเข้าถึง
 - ระดับชั้นสำหรับผู้บริหาร
 - ระดับชั้นสำหรับผู้ใช้งานทั่วไป
 - ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย
- (5) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

1.4 มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วน คือ

- (1) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบ สารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ
- (2) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความ มั่นคงปลอดภัย

2. การบริหารจัดการเข้าถึงของผู้ใช้งาน (user access management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการ สร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อ ป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

- 2.1 มีการกำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัย สารสนเทศ (information security awareness training)
- 2.2 ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและ ผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มี มาตรการเชิงป้องกันตามความเหมาะสม
- 2.3 มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (user registration) ครอบคลุมในเรื่องต่อไปนี้
 - (1) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน
 - (2) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน
 - (3) มีการกำหนดชื่อผู้ใช้งาน (username) ที่ไม่ซ้ำกันกับผู้ใช้งานคนอื่น ๆ

- (4) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น
 - (5) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
 - (6) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย
 - (7) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ
 - (8) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจาก ผู้อำนวยการ ศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย
 - (9) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออก จากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น
- 2.4 มีการบริหารจัดการสิทธิของผู้ใช้งาน (user management) โดยแสดงรายละเอียดที่เกี่ยวกับการ ควบคุมและ จำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึง สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้
- (1) แสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน
 - (2) มีการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความ รับผิดชอบ และตาม ความจำเป็นในการใช้งาน
 - (3) การมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง
 - (4) มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน
- 2.5 มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) โดยจัดทำ กระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้
- (1) มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
 - (2) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน
 - (3) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราวและควรเปลี่ยนให้รหัสผ่านยากต่อการเดา
 - (4) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว
 - (5) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน
- 2.6 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องมีกระบวนการ ทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมี การเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

3. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูล สารสนเทศ มีข้อปฏิบัติอย่างน้อย ดังนี้

- 3.1 มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password use) สำหรับผู้ใช้งาน เพื่อให้สามารถ กำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้
- (1) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก
 - (2) ควรตั้งรหัสผ่านที่ยากต่อการคาดเดา
 - (3) ควรกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสม กันระหว่าง ตัวอักษรที่เป็นตัว พิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน
 - (4) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

- (5) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
 - (6) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
 - (7) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
 - (8) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือ เก็บไว้ในระบบคอมพิวเตอร์
 - (9) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)
 - (10) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น
 - (11) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที
 - (12) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อ ทราบวาร์รหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้
 - (13) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน
- 3.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกัน ไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้
- (1) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต
 - (2) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว
 - (3) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน
 - (4) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน
 - (5) ตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา 30 นาที และต้องใส่ รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้
- 3.3 การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะ เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้น จากการใช้งาน ดังนี้
- (1) มีการกำหนดมาตรการป้องกันทรัพย์สินขององค์กร และควบคุมไม่ให้มีการทิ้งหรือปล่อย ทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่าง ๆ เช่น
 - การจัดการบริเวณล้อมรอบ
 - การควบคุมการเข้า-ออก
 - การจัดบริเวณการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก
 - การวางอุปกรณ์
 - ระบบและอุปกรณ์สนับสนุนการทำงาน
 - (2) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้
 - แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
 - กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ
 - วัฒนธรรมองค์กร
 - (3) มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

- (4) มีการกำหนดขอบเขตของการป้องกัน ดังนี้
- ทุกคนต้องตระหนักและปฏิบัติตามใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
 - ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
 - จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
 - ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิทัล เครื่อง สำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น

4. การควบคุมการเข้าถึงเครือข่าย (network access control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ให้ดำเนินการอย่างน้อยดังนี้

- 4.1 การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- (1) มีการกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการ ที่อนุญาตให้มีการใช้งานได้
 - (2) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับ อนุญาตให้เข้าถึงเท่านั้น
 - (3) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (application) ระบบเครือข่ายไร้สาย (wireless LAN) ระบบอินเทอร์เน็ต (internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และ ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ ดังกล่าวอย่างน้อยปีละ 1 ครั้ง
- 4.2 การยืนยันตัวตนบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงานจะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวตนก่อนที่จะอนุญาตให้ผู้ใช้งาน ที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้
- (1) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (identification) ด้วยชื่อผู้ใช้งาน (username) ทุกครั้ง
 - (2) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมี วิธีการยืนยันตัวตนบุคคล (authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้ รหัสผ่าน (password) หรือการใช้ สมาร์ทการ์ด เป็นต้น
 - (3) จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของ หน่วยงาน อย่างน้อย 1 วิธี
 - (4) การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต ให้มีการตรวจสอบผู้ใช้งานด้วย
- 4.3 การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการหรือ กระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้ในการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการ เข้าถึง ดังนี้
- (1) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์
 - (2) มีการควบคุมการใช้งานอย่างเหมาะสม
 - (3) จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
- 4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการ เข้าถึงทางกายภาพ และทางเครือข่าย

- (1) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและ ปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย
 - (2) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย
 - (3) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัด ระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็น ลายลักษณ์อักษร
- 4.5 การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่ม ผู้ใช้งาน โดย แบ่งออกเป็น 2 เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก
- 4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึง หรือใช้งาน เครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดัง
- (1) มีการตรวจสอบการเชื่อมต่อเครือข่าย
 - (2) จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย
- 4.7 การควบคุมการเข้าใช้งานระบบจากภายนอก
- (1) การเข้าสู่ระบบจากระยะไกล (remote access) ผู้ระบบสารสนเทศและเครือข่ายของ หน่วยงาน ต้องมี การกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน
 - (2) การเข้าสู่ระบบจากระยะไกล (remote access) ต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของ ผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น
 - (3) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกลต้องได้รับ การอนุมัติจาก ผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมายก่อน และมีการควบคุม อย่างเข้มงวดก่อนนำมาใช้และ ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบ สารสนเทศอย่างเคร่งครัด
 - (4) ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผล หรือความ จำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอและต้องได้รับอนุมัติจาก ผู้อำนวยการศูนย์หรือผู้ดูแล ระบบที่ได้รับมอบหมายอย่างเป็นทางการ
 - (5) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรมีเปิด port และ modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัด การเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

- 5.1 กำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของ เครื่องคอมพิวเตอร์ของหน่วยงาน
- 5.2 กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้อง ควบคุมโดยแสดง วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย
- 5.3 ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ ผู้ใช้งานมี ข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตน ที่ เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

 - (1) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบ สารสนเทศของ หน่วยงาน
 - (2) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็น

ทางด้านกระบวนการทำงานขององค์กรนั้น ๆ

(3) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น Smart Card

5.4 การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งาน โปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บาง ชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

(1) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรม อรรถประโยชน์

(2) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(3) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

5.5 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้อง จำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

(1) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบ สารสนเทศหรือ แอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ 1 ชม. ต่อการ เชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น

(2) กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานใน สถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) เป็นต้น มีการจำกัดช่วงระยะเวลา การเชื่อมต่อ

6. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

6.1 การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการ เข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการ เข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

6.2 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่ เหมาะสมในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ เพื่อปกป้องสารสนเทศจากความเสี่ยง ของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

6.3 การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและ ขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

7. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

7.1 ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน จะต้องทำการลงทะเบียนกับผู้ดูแล ระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับ มอบหมาย

7.2 ผู้ดูแลระบบ (system administrator) ต้องดำเนินการดังต่อไปนี้

(1) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับ หน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการ ทบทวนสิทธิการเข้าถึงอย่าง

สม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตาม ความจำเป็นในการใช้งาน

- (2) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนเครือข่ายไร้สาย
- (3) ควรทำการเปลี่ยนค่า SSID (service set identifier) ที่ถูกกำหนดเป็นค่า Default มาจาก ผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (access point) มาใช้งาน
- (4) ควรเปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้อุปกรณ์หรือเจาะรหัสได้โดยง่าย
- (5) ต้องกำหนดค่าใช้ WEP (wired equivalent privacy) หรือ WPA (Wi-Fi protected access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN client และอุปกรณ์กระจาย สัญญาณ (access point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น
- (6) ควรจะมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับ เครือข่ายภายในหน่วยงาน
- (7) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย อย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบ เครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ รายงานต่อผู้ดูแลระบบโดยทันที

8. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (physical and environmental security)

8.1 ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (data center)

- (1) ให้ศูนย์เป็นผู้กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำ แผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือ ระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น
- (2) ให้ศูนย์เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศ
- (3) ให้ศูนย์กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศ
- (4) หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบ เครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่อง คอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม
- (5) มีระบบสนับสนุนการท างานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการ ใช้งานโดยให้มีระบบดังนี้ เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบน้ำและเครื่องดับเพลิง ระบบปรับอากาศและควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุน เหล่านี้กันอย่างสม่ำเสมอให้มั่นใจได้ว่า ระบบทำงานตามปกติ และลดความเสี่ยงจากการ ล้มเหลวในการทำงานของระบบ
- (6) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่อง ทำงานผิดปกติหรือหยุดการทำงาน

8.2 การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (cabling security)

- (1) ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณ เพื่อทำให้เกิดความเสียหาย
- (2) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวน ของสัญญาณ
- (3) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

- (4) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของ บุคคลภายนอก
- 8.3 การบำรุงรักษาอุปกรณ์ (equipment maintenance)
- (1) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต
 - (2) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามผู้ผลิตแนะนำ
 - (3) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการ ตรวจสอบหรือ ประเมินในภายหลัง
 - (4) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุง อุปกรณ์ดังกล่าว
 - (5) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการ บำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- 8.4 การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ
- (1) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย
 - (2) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น
 - (3) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บน เครือข่ายสาธารณะ เช่น อินเทอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

9. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

- 9.1 ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ
- (1) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น
 - (2) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน
 - (3) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ
- 9.2 ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ
- (1) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลง ระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะ ดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ
 - (2) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้ง วางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ ระบบปฏิบัติการใหม่
- 9.3 มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)
- (1) ผู้ให้บริการที่ต้องการสิทธิในการเข้าถึงระบบสารสนเทศของหน่วยงานจะต้องทำเรื่องขอ อนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้อำนวยการศูนย์
 - (2) ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบงานของผู้ให้บริการที่สิ้นสุดการว่าจ้าง หรือเปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้
 - (3) กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (production environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่าง เข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้
 - (4) การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็น เท่านั้นและไม่เปิด

ช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกล (Modem) ที่ใช้ทิ้ง เอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

9.4 มาตรการควบคุมช่องโหว่ทางเทคนิค

- (1) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการ ช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังต่อไปนี้
 - ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
 - สถานที่ที่ติดตั้ง
 - เครื่องที่ติดตั้ง
 - ผู้ผลิตซอฟต์แวร์
 - ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้นๆ
- (2) กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที
- (3) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบการดำเนินการ ดังนี้
 - มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
 - ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน
 - กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น
- (4) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้ งานได้อย่างจำกัด ระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็น ลายลักษณ์อักษร

9.5 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (audit logging) มีการบันทึก พฤติกรรมการใช้งาน (log) การเข้าถึงระบบสารสนเทศ ดังนี้

- (1) ข้อมูลชื่อบัญชีผู้ใช้งาน
- (2) ข้อมูลวันเวลาที่เข้าถึงระบบ
- (3) ข้อมูลวันเวลาที่ออกจากระบบ
- (4) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
- (5) ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ
- (6) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
- (7) ข้อมูลการเปลี่ยนการตั้งค่าของระบบ
- (8) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น
- (9) ข้อมูลไอพีแอดเดรสที่เข้าถึง
- (10) ข้อมูลโปรโตคอลเครือข่ายที่ใช้
- (11) ข้อมูลแสดงการหยุดการท างานของระบบป้องกันไวรัสคอมพิวเตอร์
- (12) ข้อมูลแสดงการส ารองข้อมูลไม่สำเร็จ

10. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

10.1 การใช้งานทั่วไป

- (1) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ผู้ใช้ งาน ใช้งานเป็นทรัพย์สินของหน่วยงาน ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน
- (2) ไม่อนุญาตให้ผู้ใช้ งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ ของหน่วยงาน

- (3) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของ ศูนย์หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับ หน่วยงานเท่านั้น
- (4) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรม ป้องกันไวรัส
- (5) การใช้เครื่องคอมพิวเตอร์เป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักกระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
- (6) ไม่วางของทับบนหน้าจอและแป้นพิมพ์
- (7) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

10.2 การสำรองข้อมูลและการกู้คืน

- (1) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น
- (2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลสำรองไว้อย่างสม่ำเสมอ
- (3) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญ เกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

11. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

- 11.1 ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการ ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ
- 11.2 เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน เหล่านี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- 11.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการ เข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล
- 11.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (encryption) ที่เป็น มาตรฐานสากล เช่น SSL, VPN หรือ XMLEncryption เป็นต้น
- 11.5 ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอก พื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

12. การใช้งานระบบอินเทอร์เน็ต (internet)

- 12.1 กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อ ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น เช่น Proxy , firewall เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-Up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและได้รับ การอนุมัติจากผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมายแล้วเท่านั้น
- 12.2 การใช้งานเครื่องคอมพิวเตอร์ จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ของระบบปฏิบัติการ
- 12.3 ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของ ระบบ

เครือข่ายและความปลอดภัยทางข้อมูลของหน่วยงาน และต้องไม่ใช้ระบบอินเทอร์เน็ตของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสมเช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงแห่งชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับหน่วยงาน เป็นต้น

- 12.4 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงานที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านระบบอินเทอร์เน็ต
- 12.5 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการ ดาวน์โหลดการปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
- 12.6 หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการ เข้าใช้งานโดยบุคคลอื่นๆ

13. การใช้งานเครือข่ายสังคมออนไลน์ (social network)

- 13.1 อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น
- 13.2 ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบต่อหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์
- 13.3 หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบต่อหน่วยงาน ผู้ใช้งาน ต้องแจ้งต่อศูนย์โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

14. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (log)

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ให้ปฏิบัติ ดังต่อไปนี้

- 14.1 จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง
- 14.2 ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT auditor) หรือบุคคลที่หน่วยงานมอบหมาย
- 14.3 กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบ บันทึกการพยายามเข้า สู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้งานสิ้นสุดลง
- 14.5 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ 2

นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

1. เพื่อให้ระบบสารสนเทศของหน่วยงาน ให้บริการได้อย่างต่อเนื่อง
2. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับ หน่วยงาน เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

1. ศูนย์สารสนเทศ

แนวปฏิบัติ

1. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อม ใช้งานตามแนวทางต่อไปนี้
 - 1.1 มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบ สารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง
 - 1.2 กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรอง ข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการ สำรองข้อมูล ดังนี้
 - กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
 - กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรอง ข้อมูลแบบเต็ม (full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (incremental backup)
 - บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อ ข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
 - ตรวจสอบข้อมูลทั้งหมดของระบบว่ามี การสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลการตั้งค่า ข้อมูลในฐานข้อมูล เป็นต้น
 - จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้ สามารถแสดงถึงระบบ ซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการ สำรองข้อมูลไว้อย่างชัดเจน
 - จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับ หน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้เกิดผลกระทบต่อข้อมูลที่จัดเก็บไว้ที่นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น
 - ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
 - ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
 - จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่สำรองเก็บไว้
 - ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูล อย่างสม่ำเสมอ
 - กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้
2. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อม กรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทาง ต่อไปนี้

- 2.1 มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้
- (1) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
 - (2) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อ ลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลาานาน ไฟไหม้ แผ่นดินไหว การชุมนุม ประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น
 - (3) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
 - (4) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
 - (5) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ
 - (6) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น
- 2.2 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้ อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง
3. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบ สำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
 4. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อม กรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง
 5. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อ สภาพ ความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 3

นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

1. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ
2. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

1. ศูนย์สารสนเทศ
2. ผู้ตรวจสอบภายใน (internal auditor) หรือผู้ตรวจสอบจากภายนอก (external auditor)

แนวปฏิบัติ

1. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อยดังนี้
 - 1.1 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ 1 ครั้ง
 - 1.2 ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ
2. มีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้
 - 2.1 มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง
 - 2.2 มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง
 - 2.3 มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
 - 2.4 มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้
 - (1) ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
 - (2) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้ โดยมีการป้องกันเป็นอย่างดี
 - (3) ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหาร จัดการความมั่นคงปลอดภัย
 - (4) ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลล็อก แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ
 - (5) ในกรณีที่มือเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการ ติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการ พัฒนา และมีการจัดเก็บป้องกันเครื่องมือเหล่านั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ 4

นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

1. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของ หน่วยงาน
2. เพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน
3. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

1. ศูนย์สารสนเทศ

แนวปฏิบัติ

1. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน อย่างน้อยปีละ 1 ครั้ง หรือ ทุกครั้งที่มี การปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ
2. จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน
3. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหา แนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน
4. จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้าง ความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า 1 ครั้ง โดย อาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดให้ความรู้
5. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะกระดานความรู้ หรือข้อระวังในรูปแบบที่ สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ
6. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ เป็นต้นไป

ประกาศ ณ วันที่

(.....)

โรงพยาบาลนนไทย

