# นโยบายและแนวทางปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ
# งานประกัน ยุทธศาสตร์ เทคโนโลยีสารสนเทศ โรงพยาบาลเวียงแก่น
# ปีงบประมาณ 2566

**1. หลักการและเหตุผล**

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่างๆในระบบสารสนเทศ มีความมั่นคงปลอดภัย เชื่อถือได้ ทางโรงพยาบาลเวียงแก่นจึงได้กำหนดแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลเวียงแก่นเป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่อง และป้องกันภัยคุกคามต่างๆ และการปฏิบัติตามเจตนารมณ์ของพระราชกฤษฎีกา ดังกล่าวได้อย่างถูกต้องและเหมาะสม รวมถึงยังได้เตรียมความพร้อมตามกฎหมายและประกาศด้านเทคโนโลยีสารสนเทศอื่นๆ ที่เกี่ยวข้อง และการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่าง ๆ อีกด้วย

**2. วัตถุประสงค์**

โรงพยาบาลเวียงแก่น ได้กำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีวัตถุประสงค์ ดังต่อไปนี้

2.1 เพื่อกำหนดมาตรฐานแนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบ เทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลเวียงแก่นให้เป็นไปตามกฎหมายและระเบียบ ปฏิบัติที่เกี่ยวข้อง

2.2 เพื่อให้เกิดความเชื่อมั่นด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลเวียงแก่น และทำให้ดำเนินงานต่าง ๆ เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

2.3 เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหาร เจ้าหน้าที่ทุกระดับ เจ้าหน้าที่ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร มีความรู้ความเข้าใจ และตระหนักถึงความสำคัญและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2.4 เพื่อให้มีระบบตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของเทคโนโลยีและสารสนเทศ อย่างสม่ำเสมอ

## 3. เป้าหมาย

เป้าหมายในการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ โรงพยาบาลเวียงแก่น มีรายละเอียดดังต่อไปนี้

3.1 ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อ นโยบายของโรงพยาบาลเวียงแก่น

3.2 เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

3.3 เผยแพร่ความรู้ และข่าวสารเพื่อสร้างความตระหนักให้บุคลากรและผู้เกี่ยวข้องทุกระดับทั้งของโรงพยาบาลเวียงแก่น และหน่วยงานที่เกี่ยวข้อง

3.4 ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

## 4. องค์ประกอบของนโยบาย

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลเวียงแก่น จัดทำขึ้นเพื่อกำหนด แนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องและเป็นไปตามนโยบายที่ กำหนดไว้ โดยมีรายละเอียดดังต่อไปนี้

**ส่วนที่ 1 นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ**

1. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล (Information Access Control)
2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
3. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
4. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)
5. การใช้งานอินเทอร์เน็ต (Use of the Internet)
6. การบริหารจัดการคอมพิวเตอร์แม่ข่าย
7. การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์
8. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
9. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
10. การเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ใช้งานร่วมกัน
11. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ (Application and Information Access Control)
12. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Traffic Log Management)
13. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator)

14. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)
15. การรักษา ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

**ส่วนที่ 2 นโยบายการจัดทำระบบสำรองข้อทูลสารสนเทศ**

**ส่วนที่ 3 นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ**

**ส่วนที่ 4 นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศ (Information Security Awareness Policy)**

## ส่วนที่ 1 นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

**วัตถุประสงค์**

1. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการใช้ งานระบบสารสนเทศของโรงพยาบาล

2. เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องทุกฝ่าย ได้รับรู้ เข้าใจขั้นตอนและปฏิบัติตามแนวทางบริหารจัดการ บัญชีผู้ใช้สารสนเทศของโรงพยาบาลโดยเคร่งครัด

**ผู้รับผิดชอบ**

1. ฝ่ายงานสารสนเทศทางการแพทย์

2. เจ้าหน้าที่ที่ได้รับมอบหมาย อ้างอิงมาตรฐาน มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

**แนวปฏิบัติ**

**<u>1. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล (Information Access Control)</u>**

1.1 จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน

จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน เพื่อจำแนกกลุ่มทรัพยากรของระบบ เทคโนโลยีและสารสนเทศ

1.2 กำหนดสิทธิ์การเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล ดังนี้

1) ไม่มีสิทธิ์
2) อ่านได้อย่างเดียว
3) สร้างข้อมูล
4) ป้อนข้อมูล
5) แก้ไขข้อมูล
6) ลบข้อมูล
7) อนุมัติการใช้ข้อมูล

1.3 กำหนดประเภทข้อมูลของโรงพยาบาลเป็น 5 ประเภทหลักๆ ดังนี้

1) ข้อมูลทางระบบ
2) ข้อมูลบุคลากรทางการแพทย์
3) ข้อมูลการเงินและบัญชี
4) ข้อมูลการให้บริการผู้ป่วย
5) ข้อมูลการจราจรทางคอมพิวเตอร์และระบบอินเตอร์เน็ต

1.4 กำหนดระดับชั้นความลับของข้อมูลและสารสนเทศของโรงพยาบาลเป็น 4 ระดับดังนี้

1) ลับ รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง

2) ส่วนบุคคล ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือหน่วยงานที่ดูแลข้อมูลนั้น

3) ประเภทใช้ภายในเท่านั้น เป็นข้อมูลที่ใช้ในกลุ่มย่อยหรือระหว่างหน่วยงานภายในโรงพยาบาล และองค์กรที่เกี่ยวข้อง

4) เปิดเผยได้ เป็นข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกโรงพยาบาล

1.5 เกณฑ์ในการกำหนดชั้นความลับของข้อมูล

**ประเภทลับ** หมายถึง ข้อมูลที่รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง

**ประเภทส่วนบุคคล** หมายถึง ข้อมูลที่ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือหน่วยงานที่ ดูแล ข้อมูลนั้น

**ประเภทใช้ภายในเท่านั้น** หมายถึง ข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างฝ่าย/ หน่วยงาน หรือข้อมูลที่เผยแพร่เฉพาะภายในโรงพยาบาล และองค์กรที่เกี่ยวข้อง

**ประเภทเปิดเผยได้** หมายถึง ข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกโรงพยาบาล

1.6 กำหนดระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาลดังนี้

1) การเข้าถึงสำหรับผู้บริหาร

2) การเข้าถึงสำหรับผู้ปฏิบัติงานตามภาระหน้าที่

3) การเข้าถึงสำหรับผู้ดูแลระบบ นโยบายและแนวทางปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศโรงพยาบาลเวียงแก่น

4) การเข้าถึงระดับผู้ใช้งานทั่วไป

1.7 เกณฑ์การแบ่งระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล

ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น ผู้ปฏิบัติงาน เข้าถึงได้ตามอำนาจหน้าที่ที่ได้รับมอบหมาย

1.7.1.1 ผู้ดูแลระบบ มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตาม อำนาจหน้าที่

1.7.1.2 บุคคล เข้าถึงได้เฉพาะข้อมูลส่วนบุคคลของตนเองและข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้

1.7.1.3 ผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น

1.7.1.4 การกำหนดสิทธิ์พิเศษสามารถดำเนินการได้เมื่อได้รับอนุมัติจากผู้มีอำนาจหรือเจ้าของข้อมูล เท่านั้น

1.7.1.5 การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้เมื่อได้รับความยินยอมจากเจ้าของสิทธิ์ หรือหน่วยงานหลักเท่านั้น

1.8 กำหนดให้มีหน่วยงานหลักในการอนุญาตการเข้าถึงข้อมูลและสารสนเทศ ของโรงพยาบาลในแต่ละประเภทดังนี้

1.8.1 ข้อมูลทั่วไปและข้อมูลบุลากร หน่วยงานหลักคือ งานบริหาร

1.8.2 ข้อมูลเผยแพร่บนเว็บไซต์ หน่วยงานหลักคือ งานสารสนเทศ

1.8.3 ข้อมูลการเงินและบัญชี หน่วยงานหลักคือ งานการเงิน และบัญชี

1.8.4 ข้อมูลทางการรักษา ขึ้นอยู่กับงานเวชระเบียนและแพทย์

1.8.5 ข้อมูลทางการบริหาร ขึ้นอยู่กับหน่วยงานที่โรงพยาบาล มอบหมายเป็นหน่วยงานหลัก

1.8.6 ข้อมูลการจราจรทางคอมพิวเตอร์ศูนย์คอมพิวเตอร์และหน่วยงานที่ให้บริการระบบสารสนเทศ

1.8.7 การกำหนดกฏเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับ การอนุญาต การกำหนดสิทธิ์ ของโรงพยาบาลเวียงแก่น

1.9 การควบคุมการเปลี่ยนแปลง

1.9.1 การเปลี่ยนแปลงใดๆ ที่อาจส่งผลกระทบต่อข้อมูลและสารสนเทศที่ใช้งานอยู่ให้ดำเนินการ ดังนี้

(1) พิจารณาวางแผนดำเนินการเปลี่ยนแปลง รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในการเปลี่ยนแปลง

(2) แจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบเกี่ยวกับการเปลี่ยนแปลงนั้นๆ เพื่อให้บุคคล เหล่านั้นมีเวลาเพียงพอในการเตรียมความพร้อมก่อนที่จะดำเนินการเปลี่ยนแปลงนโยบายและแนวทางปฏิบัติ ในการรักษาความปลอดภัยด้านสารสนเทศโรงพยาบาลเวียงแก่น

(3) ต้องตรวจสอบความสมบูรณ์ของข้อมูลและสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลง

1.9.2 ต้องจัดเก็บซอร์สโค้ดและไลบรารี่ของระบบสารสนเทศทั้งเวอร์ชั่นปัจจุบันและเวอร์ชั่นเก่าไว้ ในสถานที่ที่มีความมั่นคงปลอดภัย เพื่อให้สามารถนำกลับมาใช้ได้เมื่อจำเป็น

1.10 การกำหนดการใช้งานตามภารกิจ

1.10.1 การควบคุมการเข้าถึงระบบสารสนเทศ

(1) นักศึกษาฝึกงาน จะให้สิทธิ์ทันทีที่มีสภาพเป็นนักศึกษาฝึกงานและหมดสิทธิ์เมื่อพ้นระยะการฝึกงานไปแล้ว 10 วัน

(2) บุคลากร จะให้สิทธิ์เข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้น สภาพการเป็นบุคลากร

(3) ผู้บริหาร จะให้สิทธิ์เข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้น สภาพการเป็นผู้บริหาร

(4) บุคคลภายนอก ได้รับอนุญาตเฉพาะระบบและช่วงเวลาที่กำหนด

1.10.2 ข้อจำกัดในการเข้าถึง

(1) นักศึกษาฝึกงาน เข้าถึงได้เฉพาะระบบที่ได้รับอนุญาต

(2) บุคลากร เข้าถึงได้ตามสิทธิ์เบื้องต้นและภารกิจที่ได้รับมอบหมาย

(3) ผู้บริหาร เข้าถึงตามสิทธิ์และภารกิจที่ได้รับมอบหมาย

(4) บุคคลภายนอก เข้าถึงได้ตามที่ได้รับอนุญาต

1.11 ระยะเวลาการใช้งาน

1.11.1. ระยะเวลาการเข้าถึงและการใช้งา นข้อมูลและสารสนเทศและระบบ สารสนเทศ ผู้ใช้งาน จะเข้าถึงและใช้งานได้ ดังนี้

(1) การเข้าถึงในเวลาราชการ 08.30-16.30 น.

(2) การเข้าถึงนอกเวลาราชการ หลัง 16.30 น. เป็นต้นไป

(3) การเข้าถึงในช่วงวันหยุดราชการและวันหยุดนขัตฤกษ์

1.11.2. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ

(1) กำหนดให้ระบบสารสนเทศที่มีความเสี่ยงสูงหรือระบบที่มีข้อมูลสำคัญ ต้องตัดและ หมดเวลาการใช้งานที่สั้นขึ้นเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (2) ต้องจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับระบบสารสนเทศความเสี่ยงสูง หรือระบบที่มีข้อมูลสำคัญ

1.12. การหมดสิทธิ์การเข้าถึงและใช้งานข้อมูลสารสนเทศและระบบสารสนเทศ 1.12.1. บัญชีผู้ใช้หมดอายุ

1.12.2. เมื่อมีการเปลี่ยนแปลงสิทธิ์การเข้าถึง

1.12.3. ถูกระงับสิทธิ์

1.13. การทบทวนและตรวจสอบสิทธิ์การเข้าถึงและการใช้งานข้อมูล สารสนเทศ และระบบสารสนเทศ

1.13.1. ทบทวนและตรวจสอบสิทธิ์การเข้าถึงและใช้งานระบบสารสนเทศ ปีละ 1 ครั้ง โดย ผู้ดูแลระบบพิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงานที่ขอสิทธิ์ จัดส่ง รายชื่อนั้นให้กับหน่วยงานที่ขอสิทธิ์เพื่อดำเนินการทบทวนว่า มีรายชื่อที่ลาออกหรือไม่ หรือมีการเปลี่ยนแปลง แต่ยังไม่ได้แก้ไขสิทธิ์การเข้าถึงให้ถูกต้องหรือไม่

1.13.2. หน่วยงานผู้ขอสิทธิ์แจ้งกลับผู้ดูแลระบบเพื่อดำเนินการแก้ไขให้ถูกต้อง

1.13.3. หน่วยงานที่เป็นเจ้าของระบบสารสนเทศต้องตรวจสอบคุณสมบัติและสิทธิ์ของผู้ใช้อย่าง สม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องดำเนินการเปลี่ยนแปลงสิทธิ์ให้สอดคล้องกับระดับชั้นการเข้าถึงและการใช้งานระบบทันที

1.14. ช่องทางการเข้าถึง

1.14.1. เครือข่ายภายในโรงพยาบาล

1.14.2. เครือข่ายภายนอกโรงพยาบาล

1.14.3. เข้าถึงโดยผ่านระบบที่จัดไว้ให้

**2. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)**

2.1. การสร้างความรู้ความเข้าใจให้แก่ผู้ใช้งาน

2.1.1. ต้องจัดทำหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัย ด้านสารสนเทศ

2.1.2. อบรมผู้ใช้งาน เพื่อให้สามารถใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศได้อย่าง ถูกต้อง รวมถึงให้ตระหนักและเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานข้อมูลและสารสนเทศ และระบบสารสนเทศโดยไม่ระมัดระวัง

2.1.3. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควร ระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

2.2. การแบ่งกลุ่มบัญชีผู้ใช้ บัญชีผู้ใช้ระบบสารสนเทศของโรงพยาบาลจัดทำขึ้นเพื่อควบคุมการเข้าถึงและใช้งาน สารสนเทศและระบบสารสนเทศของโรงพยาบาล ต้องระบุชื่อบัญชีผู้ใช้แยกเป็นรายบุคคลที่ไม่ซ้ำซ้อน กัน โดยแบ่งกลุ่มผู้ใช้งานออกเป็น 4 กลุ่มคือ

2.2.1. นักศึกษาฝึกงาน

2.2.2. บุคลากรของโรงพยาบาล

2.2.3. หัวหน้ากลุ่มงาน

2.2.4. ผู้ดูแลระบบ

2.2.5. ผู้รับบริการ

2.3. การลงทะเบียนผู้ใช้งาน

2.3.1. นักศึกษาฝึกงานทุกคน ได้รับบัญชีผู้ใช้โดยอัตโนมัติ ทันทีที่ป้อนข้อมูลเข้าสู่ระบบสารสนเทศ

2.3.2. บุคลากร ผู้บริหาร ของโรงพยาบาล และผู้เยี่ยมชมของหน่วยงาน งานสารสนเทศจะสร้างบัญชีบุคลากรใหม่โดยอัตโนมัติทันทีที่เจ้าหน้าที่
ป้อนข้อมูลบุคลากรเข้าระบบสารสนเทศ บุคลากร

2.3.3. ผู้รับบริการ ได้รับบัญชีผู้ใช้โดยอัตโนมัติ ทันทีที่ป้อนข้อมูลเข้าสู่ระบบสารสนเทศ โดยการ Scan QR-Code

2.4. การจัดการบัญชีผู้ใช้

2.4.1. การบริหารจัดการบัญชีผู้ใช้สำหรับบุคลากร ดำเนินการโดยผ่านผู้แทนของหน่วยงาน โดยผู้บริหารของหน่วยงานแจ้งชื่อผู้แทนที่จะรับผิดชอบในการดูแลบัญชีผู้ใช้ของบุคลากร ในสังกัด เป็นลายลักษณ์อักษรถึงผู้อำนวยการ โดยมีรายละเอียด ดังนี้

(1) ชื่อหน่วยงาน

(2) ชื่อ-สกุล

(3) ชื่อบัญชีผู้ใช้

(4) อีเมล

(5) หมายเลขโทรศัพท์

2.4.2. การเปลี่ยนแปลงของหน่วยงาน ให้แจ้งเป็นลายลักษณ์อักษร ลงนามโดยผู้บริหารของหน่วยงาน ระบุผู้รับผิดชอบเดิม และชื่อผู้รับผิดชอบใหม่ พร้อมอีเมล และหมายเลขโทรศัพท์ที่ติดต่อได้ของผู้รับผิดชอบใหม่

2.5. การจัดการสิทธิ์ของผู้ใช้งาน

2.5.1. เมื่อเจ้าหน้าที่ของหน่วยงาน ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอ บในระบบที่เคย ขอสิทธิ์การใช้งานไว้ ต้องรีบแจ้งเพื่อเปลี่ยนสิทธิ์หรือถอดถอนสิทธิ์ออกจากระบบทันที

2.5.2. การแจ้งขอใช้สิทธิ์/เปลี่ยนแปลงสิทธิ์ในการเข้าถึงและใช้งานข้อมูลและสารสนเทศและระบบ สารสนเทศจะต้องจัดทำเป็นลายลักษณ์อักษร ระบุเหตุผล และความจำเป็น

(1) ลงชื่อโดยผู้บริหารของหน่วยงานที่ขอใช้

(2) ส่งถึงผู้บริหารของหน่วยงานหลัก

(3) เก็บเอกสารไว้เป็นหลักฐานอ้างอิงทั้งฝ่ายผู้ขอและผู้อนุญาต

(4) หน่วยงานหลักสำเนาเอกสารการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ

2.5.3. ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ์ ในกรณีตรวจพบว่ามีการกระทำความผิดตาม นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

2.5.4. กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน ต้องพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์ พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา โดยต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการ

(1) ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ต้องควบคุมการใช้งานเฉพาะ กรณีจำเป็นเท่านั้น

(2) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลา ดังกล่าว

(3) ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้ งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

2.6. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

2.6.1. ผู้ดูแลระบบต้องก าหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคง ปลอดภัย

2.6.2. ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดย ผู้อื่นและกำหนดรหัสผ่านที่แตกต่างกัน

2.6.3. ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่ง

2.6.4. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านที่มีความยากต่อการคาดเดา

2.6.5. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเป็นระยะหรือทุกครั้งที่มีการแจ้งเตือนหรือบังคับให้เปลี่ยน รหัสผ่านจากผู้ดูแลระบบ

2.6.6. ผู้ใช้งานต้องลงบันทึกการออกจากระบบทันทีเมื่อเลิกใช้งานระบบหรือไม่อยู่หน้าจอเป็น เวลานาน

2.6.7. กรณีผู้ดูแลระบบตรวจพบว่ารหัสผ่านของผู้ใช้งานไม่มีความปลอดภัย หรือตรวจสอบได้ว่าถูก นำไปใช้โดยผู้อื่น ผู้ใช้งานรายนั้นจะถูกตัดสิทธิ์การใช้งานชั่วคราวจนกว่าจะดำเนินการเปลี่ยน รหัสผ่านเป็นที่เรียบร้อย

2.7. การทบทวนสิทธิ์การเข้าถึง

2.7.1. ต้องมีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชี ผู้ใช้อย่างน้อยปีละ 1 ครั้ง

2.7.2. บัญชีผู้ใช้จะหมดอายุ ดังนี้

(1) กรณีบุคลากร หมดอายุเมื่อพ้นสภาพการเป็นบุคลากร ยกเว้น ผู้เกษียณอายุราชการซึ่งสามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับเข้าอินเทอร์เน็ต เท่านั้น

(2) กรณีนักศึกษาฝึกงาน หมดอายุหลังพ้นสภาพการเป็นนักศึกษาฝึกงาน 10 วัน ซึ่งสามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับเข้าอินเทอร์เน็ตเท่านั้น

(3) กรณีที่ไม่ใช่บุคลากร หมดอายุตามวันที่ระบุในเอกสารขอเปิดบัญชี

**3. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)**

3.1. การใช้งานบัญชีผู้ใช้และรหัสผ่าน

3.1.1. ผู้ใช้งานต้องทำการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้และรหัสผ่าน โดยผู้ใช้งานแต่ละคน ต้องมีบัญชีชื่อผู้ใช้ของตนเอง และห้ามทำการเผยแพร่แจกจ่ายหรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน

3.1.2. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีเมื่อสงสัยว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

3.2. การใช้งานรหัสผ่าน

3.2.1. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนด

3.2.2. ไม่กำหนดรหัสผ่านที่มีส่วนหนึ่งมาจากสิ่งที่สื่อถึงตัวผู้ใช้งาน เช่น ชื่อ นามสกุล ชื่อเล่น ชื่อ บิดา ชื่อมารดา ชื่อหน่วยงาน หรือคำศัพท์ที่มีใช้ในพจนานุกรม เป็นต้น ต้องประกอบด้วย ตัวอักษรไม่น้อยกว่า 8 ตัว

โดยต้องผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และ ตัวอักขระพิเศษเข้าด้วยกัน

3.2.3. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

3.2.4. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

3.2.5. หลีกเลี่ยงการใช้รหัสผ่านเดียวกับระบบงานต่าง ๆ ที่มีสิทธิ์ใช้งาน

3.2.6. เก็บบัญชีและรหัสผ่านของตนเองไว้เป็นความลับ

3.3. การป้องกันอุปกรณ์ขณะไม่มีผู้ใช้งาน

3.3.1. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อก หน้าจอภาพเมื่อไม่มีการใช้งาน

หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน 3.3.2. ผู้ใช้งานต้องล็อกอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแล

3.3.3. ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้ผู้ใช้งานเข้าใจมาตรการป้องกันที่กำหนดไว้

3.4. การจัดวางและการป้องกันอุปกรณ์

3.4.1. จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการสูญหายหรือใช้งานโดยไม่ได้ รับอนุญาต

3.4.2. อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย

3.4.3. ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบ

เทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ว่าอยู่ในระดับปกติหรือไม่

3.5. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

3.5.1. จัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศไว้ในสถานที่มั่นคง ปลอดภัย

3.5.2. ต้องควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศ โดยผู้เป็น เจ้าของหรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษรเท่านั้น

3.5.3. มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญ ในอุปกรณ์ที่ใช้ ในการบันทึกข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นน
าอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้ เข้าถึงข้อมูลสำคัญได้

3.5.4. สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม เพื่อ ป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

3.5.5. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษา ความลับทางราชการ พ.ศ. 2544

3.5.6 จัดทำแนวทางสำหรับจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูล หรือ เอกสารตอบโต้ และแนวทางต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่ต้องปฏิบัติตาม

3.5.7. โปรแกรมต่างๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ เป็นโปรแกรมที่ ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรม และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานเพราะเป็น การกระทำที่ผิดกฎหมาย

3.5.8 ไม่เก็บข้อมูลสำคัญของโรงพยาบาลไว้บนเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลที่เป็น สมบัติส่วนบุคคล

3.5.9. ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำการเปลี่ยน หรือทดแทนอุปกรณ์

3.5.10. ต้องลบหรือฟอร์แมต (Format) ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อน ทำลายหรือเปลี่ยนทดแทนหรือจำหน่ายอุปกรณ์

3.5.11. ต้องลบข้อมูลที่ไม่มีการใช้งานตั้งแต่ 5 ปีขึ้นไปออกจากฐานข้อมูล และสำรองข้อมูลลง ฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และจัดเก็บ ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล ทั้งนี้ การลบหรือทำลาย ข้อมูลอิเล็กทรอนิกส์ดังกล่าว ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติให้ทำลายสื่อ บันทึกข้อมูล หรือ ลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูลทุกครั้ง

3.6. การป้องกันโปรแกรมไม่ประสงค์ดี

3.6.1. ผู้ใช้งานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมไม่ประสงค์ดีรวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

3.6.2. ต้องทำการปรับปรุงระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ นโยบายและแนวทางปฏิบัติใน การรักษาความปลอดภัยด้านสารสนเทศโรงพยาบาลเวียงแก่น

3.6.3. ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศ ผ่านทางระบบเครือข่าย และผ่านทาง สื่อ บันทึกข้อมูลทุกชนิด ผู้ใช้งานต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมไม่ ประสงค์ดี ก่อนการรับส่งทุกครั้ง

3.6.4. ผู้ใช้งานต้องตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันโปรแกรมไม่ประสงค์ดี ก่อนการเปิดใช้ ไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่นไฟล์ที่มีนามสกุล .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe เป็นต้น

## 4. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

4.1. การเข้าใช้งานระบบเครือข่าย

4.1.1. การเข้าถึงระบบเครือข่ายจะต้องพิสูจน์ตัวตนผู้ใช้งานด้วยบัญชีผู้ใช้

4.1.2. ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงระบบเครือข่าย สามารถเข้าใช้ได้เฉพาะบริการในระบบ  เครือข่ายตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

4.1.3. การเข้าถึงระบบเครือข่ายจากภายนอกต้องอยู่บนพื้นฐานของความจำเป็น เท่านั้น และต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นเป็นพิเศษจากมาตรฐานการ เข้าถึงระบบเครือข่ายจากภายใน

4.1.4. เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องที่ต้องการให้เข้าถึงได้จากอินเทอร์เน็ตจะต้องลงทะเบียน กับงานสารสนเทศ

4.1.5. จำกัดการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน รวมทั้งตรวจสอบเปิดปิดพอร์ตอุปกรณ์เครือข่าย ตามความจำเป็น

4.1.6. การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแล ระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

4.1.7. การเข้าใช้เครือข่ายของบุคคลที่ไม่มีบัญชีผู้ใช้ของมหาวิทยาลัย ต้องขออนุญาตใช้บัญชี ชั่วคราวจากมหาวิทยาลัย ซึ่งจะเข้าถึงได้ตามสิทธิ์ที่ได้รับอนุญาตและจะต้องพิสูจน์ตัวตน ด้วยบัญชีชั่วคราวนั้น

4.2. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

4.2.1. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในจะต้องทำการลงทะเบียน กับผู้ดูแลระบบ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการ หรือ ผู้บริหารหน่วยงานที่เป็นเจ้าของระบบเครือข่ายไร้สายนั้น

4.2.2. ผู้ดูแลระบบเครือข่ายไร้สายต้องดำเนินการดังต่อไปนี้

(1) ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานระบบเครือข่ายไร้สายให้เหมาะสมกับ หน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ (2) ต้องลงทะเบียนอุปกรณ์กระจายสัญญาณ (access point) ทุกตัวที่นำมาใช้ใน ระบบเครือข่ายไร้สาย

(3) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณเพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์ รั่วไหลออกนอกพื้นที่ใช้งาน และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอก อาคารหรือบริเวณขอบเขตที่ควบคุมได้

(4) ต้องทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าปริยายมาจากผู้ผลิตทันทีที่นำ อุปกรณ์กระจายสัญญาณมาใช้งาน

(5) ต้องเปลี่ยนค่าชื่อบัญชีผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการ ทำงานของอุปกรณ์กระจายสัญญาณ และต้องเลือกใช้บัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสผ่านได้โดยง่าย

(6) ต้องเข้ารหัสข้อมูลระหว่าง wireless LAN client และอุปกรณ์กระจายสัญญาณ ด้วยวิธี ที่มีความประสิทธิภาพไม่ด้อยกว่าวิธี WPA2 (Wi-Fi Protected Access) เพื่อให้ยากต่อ การ ดักจับข้อมูล และทำให้ปลอดภัยมากขึ้น

(7) ต้องติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับ เครือข่ายภายใน

(8) ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบ เครือข่ายไร้สาย อย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบ เครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ รายงานต่องานสารสนเทศทราบโดยทันที

4.3. การระบุอุปกรณ์ที่นำมาเชื่อมต่อบนเครือข่าย

4.3.1. อุปกรณ์ที่นำมาเชื่อมต่อได้รับหมายเลขไอพีแอดเดรสตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย

4.3.2. เก็บข้อมูลการใช้ MAC Address จากเครื่องบริการกำหนดค่าหมายเลขไอพีแอดเดรส (DHCP Server) หรือจาก ARP Table บนสวิทช์ L3

4.4. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

4.4.1. ต้องควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม

4.4.2. ต้องกำหนดรหัสผ่านสำหรับตรวจสอบและปรับแต่งอุปกรณ์เครือข่าย เมื่อใช้การเชื่อมต่อ โดยตรงบนตัวอุปกรณ์

4.4.3. ไม่อนุญาตให้เชื่อมต่อพอร์ตโดยตรงจากเครือข่ายภายนอก แต่ให้เชื่อมต่อผ่านช่องทางที่ปลอดภัยที่กำหนด เช่น VPN เป็นต้น

4.4.4. อุปกรณ์เครือข่ายคอมพิวเตอร์ที่สำคัญต้องจัดเก็บในห้องอุปกรณ์เครือข่ายที่ควบคุมความ ปลอดภัย

4.4.5. ต้องปิดพอร์ตหรือปิดบริการ บนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

4.4.6. ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่าง สม่ำเสมออย่างน้อยสัปดาห์ละ 1 ครั้ง

4.5. การแบ่งแยกเครือข่าย (segregation in networks)

4.5.1. ต้องจัดท าแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่าย ภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ
พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ 4.5.2. แบ่งแยกเครือข่ายตามกลุ่มของบริการ กลุ่มผู้ใช้และระบบงานต่าง ๆ

4.5.3. ต้องใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย ๆ

4.5.4. ต้องใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอก
หน่วยงาน ซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของ หน่วยงาน

4.6. การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control)

4.6.1. อนุญาตการเชื่อมต่อเฉพาะหมายเลขไอพีแอดเดรสที่กำหนดให้เท่านั้น

4.6.2. ระบบเครือข่ายที่เชื่อมต่อไปยังเครือข่ายอื่น ๆ ภายนอก ต้องติดตั้งระบบ
ตรวจจับการบุกรุก และต้องมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี

4.7. การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control)

4.7.1. อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลขไอพีแอดเดรสที่กำหนด

4.7.2. มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย

4.7.3. ต้องตรวจสอบหมายเลขไอพีแอดเดรสของต้นทางและปลายทาง

4.7.4. ต้องควบคุมการไหลของข้อมูลผ่านเครือข่าย

4.7.5. ต้องกำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและ การใช้งานบริการเครือข่าย

4.7.6. ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่อง
คอมพิวเตอร์แม่ข่าย เพื่อระงับการใช้จากเส้นทางอื่น

4.8. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอก (User Authentication for External Connections)

4.8.1. ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตนด้วยชื่อผู้ใช้งานทุกครั้ง

4.8.2. ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน ต้องเป็นผู้ที่ได้รับสิทธิ์ในการเข้าใช้บริการแล้วเท่านั้น

4.8.3. ต้องมีระบบตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศ โดยจะต้องมีวิธีการยืนยันตัวตนด้วยการป้อนชื่อผู้ใช้งานและรหัสผ่าน เพื่อ แสดงว่าเป็นผู้ใช้งานตัวจริง

**5. การใช้งานอินเทอร์เน็ต (use of the Internet)**

5.1. ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่จัดสรรไว้ตามสิทธิ์ที่ได้รับ

5.2. ห้ามใช้อินเทอร์เน็ตของโรงพยาบาลเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล

5.3. ผู้ใช้งานต้องไม่เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจ กระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อ สังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย เป็นต้น

5.4. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการ ปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

5.5. ไม่ควรใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมากหรือเป็นเวลานาน

**6. การบริหารจัดการคอมพิวเตอร์แม่ข่าย**

6.1. กำหนดผู้ดูแลระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องอย่างเป็นลายลักษณ์อักษร

6.2. มีขั้นตอน/กระบวนการในการตรวจสอบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือ เปลี่ยนแปลงค่าที่ผิดปกติ จะต้องดำเนินการแก้ไขและบันทึกรายงานการแก้ไขโดยทันที

6.3. ตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง และอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิดให้ตรง กับเวลาอ้างอิงมาตรฐาน

6.4. เปิดใช้บริการเท่าที่จำเป็นเท่านั้น โดยต้องมีมาตรการป้องกันเพิ่มเติมสำหรับบริการที่มีความเสี่ยงต่อ ระบบรักษาความปลอดภัยด้วย

6.5. ต้องปรับปรุงระบบซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ เพื่ออุดช่องโหว่ต่างๆ

6.6. ต้องทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อน ติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

6.7. การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบของหน่วยงาน

**7. การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์**

7.1. บุคลากร นำบัญชีผู้ใช้ของโรงพยาบาลไปลงทะเบียนเพื่อใช้บริการระบบจดหมายอิเล็กทรอนิกส์ โดยรหัสผ่านของบัญชีผู้ใช้ กับรหัสผ่านของบัญชีผู้ใช้ จดหมายอิเล็กทรอนิกส์จะแยกกัน

7.2. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่านหรือรับ-ส่งข้อความ

7.3. กรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงบนหัวข้อ จดหมายอิเล็กทรอนิกส์

7.4. ผู้ใช้งานมีหน้าที่จะต้องรักษาบัญชีผู้ใช้ และรหัสผ่านเป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง เพื่อป้องกันการใช้งานโดยผู้ไม่ประสงค์ดี

7.5. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องบันทึกการออกทุก ครั้ง เพื่อ ป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ของตน

7.6. ในการตรวจสอบความผิดปกติของการใช้งานจดหมายอิเล็กทรอนิกส์ หากพบว่าผู้ใช้งานรายใดส่ง จดหมายอิเล็กทรอนิกส์มากกว่าจำนวนที่ควรจะเป็น ระบบจะทำการเปลี่ยนรหัสผ่านอัตโนมัติ เพื่อ ป้องกันความเสียหายที่จะเกิดกับระบบ

7.7. ก่อนส่งต่อ เปิดไฟล์ หรือคลิกลิ้งค์ที่แนบมา ต้องตรวจสอบให้แน่ใจก่อนว่าไม่ใช่จดหมายหลอกลวง

7.8. ต้องไม่ส่งข้อมูลส่วนบุคคลที่สำคัญ เช่น รหัสผ่าน บัญชีผู้ใช้ หมายเลขบัตรประชาชน หมายเลขบัตร เครดิต ฯลฯ ผ่านจดหมายอิเล็กทรอนิกส์

**8. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System access control)**

8.1. ผู้ดูแลระบบ (System Administrator)

8.1.1. ต้องกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

8.2. กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

8.2.1. ต้องไม่ให้ระบบแสดงรายละเอียดสำคัญของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

8.2.2. ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่าน จากเครื่องปลายทาง

8.2.3. จำกัดระยะเวลาสำหรับใช้ในการป้องกันรหัสผ่าน

8.2.4. จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

8.3. ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

8.3.1. ผู้ใช้งานต้องมีบัญชีผู้ใช้ และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศ

8.3.2. สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม โดยใช้สมาร์ทการ์ด RFID หรือเครื่องอ่านลายพิมพ์นิ้วมือ หรือวิธีการอื่นที่มีความปลอดภัย

8.4. การบริหารจัดการรหัสผ่าน (Password Management System)

8.4.1. ต้องจำกัดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนครั้ง ที่กำหนด ระบบจะทำการล็อกสิทธิ์การเข้าถึงของผู้ใช้งาน ทำให้ไม่สามารถใช้งานได้จนกว่าผู้ดูแล ระบบจะปลดล็อกให้

8.4.2. ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีความพยายามในการเดา รหัสผ่านจากเครื่องปลายทาง

8.4.3. มีระบบให้ผู้ใช้งานสามารถเปลี่ยนและยืนยันรหัสผ่านได้ด้วยตนเอง

8.4.4. ต้องจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของระบบงาน

8.4.5. ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของ ตนเอง แต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

8.4.6. เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้ที่ ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

8.5. การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

8.5.1. จำกัดสิทธิ์การเข้าถึง และกำหนดสิทธิ์อย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

8.5.2. จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

8.5.3. ต้องจัดเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

8.5.4. ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

8.5.5. โปรแกรมที่ติดตั้ง ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย

8.5.6. ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ แล้วนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

8.6. การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-Out)

8.6.1. ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลา ไม่เกิน 30 นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน 15 นาที ตามความเหมาะสม  เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

8.6.2. ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ ระบบโดยอัตโนมัติ

8.6.3. เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องกำหนดระยะเวลาให้ทำการปิดเครื่อง โดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

8.7. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

8.7.1. กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบ สารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง
เพื่อให้ผู้ใช้งานสามารถใช้งานได้ นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น
กำหนดให้ใช้งานได้ 3 ชั่วโมง ตอ่ การเชื่อมต่อหนึ่งครั้ง เป็นต้น
และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติเท่านั้น

8.7.2. การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณา ถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

8.7.3. กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง และ/หรือระบบงานที่มีการใช้ งานในสถานที่ที่มีความเสี่ยงในที่สาธารณะ หรือพื้นที่ภายนอกสำนักงาน มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

**9. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย**

9.1. หัวหน้าหน่วยงานที่เป็นเจ้าของเครื่องคอมพิวเตอร์แม่ข่าย ต้องแต่งตั้งผู้มีสิทธิ์ และกำหนดจำนวนผู้มี สิทธิ์ในการเข้าถึงระบบปฏิบัติการ

9.2. ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของตัวเอง

9.3. ต้องไม่แสดงรายละเอียดสำคัญของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

9.4. ต้องตั้งค่าระบบให้สามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดา รหัสผ่านจากเครื่องปลายทาง

9.5. ผู้ดูแลระบบต้องยุติการให้บริการทันที ในกรณีตรวจพบว่ามีการใช้งานที่ผิดปกติ หรือไม่ปลอดภัย

9.6. ห้ามการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่ โรงพยาบาลไม่อนุญาต

9.7. ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานต้องตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญ อย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

9.8. ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่ประสงค์ดีบนเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง

9.9. กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ สำหรับการจัดการกับโปรแกรมไม่ ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืน ระบบจากความเสียหายที่พบ เป็นต้น

9.10. ต้องติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ 9.11. ต้องสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้ผู้ดูแลระบบและผู้ใช้งานมี ความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ ประสงค์ดี ว่าต้องดำเนินการอย่างไร

**10. การเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ใช้งาน**ร่วมกัน

10.1. ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของ ตัวเอง

10.2. ระบบต้องไม่แสดงรายละเอียดสำคัญก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

10.3. ต้องตั้งค่าระบบให้สามารถยุติการเชื่อมต่อเมื่อพบว่ามีความพยายามคาดเดารหัสผ่าน

10.4. ระบบจะต้องจำกัดสิทธิ์ผู้ใช้งานในการติดตั้ง เปลี่ยนแปลง หรือลบโปรแกรมหรือข้อมูลบนเครื่อง

**11. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ (application and information access control)**

11.1. การจำกัดการเข้าถึงสารสนเทศ

11.1.1. การจำกัดการเข้าถึงของผู้ใช้งาน

(1) เข้าได้ตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

(2) กำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล

(3) ต้องบันทึกการออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

11.1.2. แบ่งกลุ่มบุคลากรที่ปฏิบัติงานด้านสารสนเทศ ออกเป็น 3 กลุ่ม คือ ผู้ดูแลระบบ ผู้พัฒนาระบบงาน และผู้ใช้งานระบบ โดยกำหนดหน้าที่รับผิดชอบอย่างชัดเจนเป็นลายลักษณ์อักษร

11.1.3. การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ต้องบันทึกข้อมูลพฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศที่สำคัญ ดังนี้

(1) ชื่อบัญชีผู้ใช้

(2) วันเวลาที่เข้าถึงระบบ

(3) วันเวลาที่ออกจากระบบ

(4) เหตุการณ์สำคัญที่เกิดขึ้น

(5) บันทึกการเข้าใช้ทั้งที่สำเร็จและไม่สำเร็จ

(6) ความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(7) แสดงการใช้สิทธิ์ เช่น สิทธิ์ของผู้ดูแลระบบ

(8) แสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์เป็นต้น

(9) หมายเลขไอพีแอดเดรสที่เข้าถึง

(10) แสดงการหยุดการทำงานของระบบป้องกันการบุกรุก

(11) แสดงการหยุดการทำงานของระบบงานที่สำคัญๆ

11.1.4. การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ที่เป็น มาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

11.1.5. การควบคุมผู้รับเหมาช่วง (outsource) กรณีมีการจ้างเหมาบำรุงรักษา ดูแล และ พัฒนาระบบสารสนเทศ

(1) มีกระบวนการคัดเลือกผู้รับเหมาช่วงโดยเฉพาะ และต้องกำหนดคุณสมบัติของผู้รับเหมาช่วงที่ชัดเจน เช่น ต้องมีประสบการณ์ มีลูกค้าอ้างอิงน่าเชื่อถือ หรือใบรับรองทางด้าน ทักษะวิชาชีพตามมาตรฐานสากล มีความพร้อมด้านเทคโนโลยีของการรับเหมาช่วงทั้งในส่วนของ ฮาร์ดแวร์และซอฟท์แวร์ รวมถึงระบบสนับสนุน อื่นๆ เพื่อให้ได้ผู้รับเหมาช่วงที่มีคุณสมบัติตรงตาม มาตรฐานที่หน่วยงานต้องการ

(2) มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับเหมาช่วง และต้องกำหนดขอบเขตและระดับการรับเหมาช่วงอย่างชัดเจน และผู้รับเหมาช่วงต้องนำเสนอรายละเอียดงาน ขอบเขตงานอย่างครบถ้วน

(3) หน่วยงานต้องเข้าไปตรวจสอบรายละเอียดของการปฏิบัติงานของผู้รับเหมาช่วงได้ เช่น ร่วมกำหนดวิธีการทำงาน การตรวจติดตามคุณภาพของผู้รับเหมาช่วงเป็นระยะ ๆ ตามที่กำหนดไว้ หรือการสุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ เพื่อพิจารณากระบวนการที่ ผู้รับเหมาช่วงใช้ในการปฏิบัติงาน และเพื่อประเมินความสม่ำเสมอของผู้รับเหมาช่วงในการกระทำ ตามข้อกำหนดของหน่วยงาน

(4) ต้องควบคุมการเข้าถึงของข้อมูลที่ชัดเจน มีระบบบันทึกการเข้าถึงข้อมูล และการสำรองข้อมูลทุกขั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญหรือให้ใช้ข้อมูลจากชุดจำลองแทนข้อมูล จริง

(5) มีหลักเกณฑ์และกระบวนการในการตรวจรับงานที่ส่งมอบโดยผู้รับเหมาช่วงที่ ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

11.2. ระบบซึ่งไวต่อการรบกวน มีผลกระทบต่อคนกลุ่มใหญ่ หรือระบบที่มีความสำคัญต่อหน่วยงาน จะต้องดำเนินการดังนี้

11.2.1. ระบบซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูง ได้แก่ ระบบสารสนเทศบุคลากร และระบบสารสนเทศทางการเงิน ต้องแยกออกจาก ระบบอื่น และแสดงให้เห็น ถึงผลกระทบและระดับความสำคัญ

11.2.2. ต้องควบคุมสภาพแวดล้อมของระบบซึ่งไวต่อการรบกวนโดยเฉพาะ

(1) มีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่มีหน้าที่ที่ได้รับมอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

(2) ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่น

(3) ทำการป้องกันการมีทรัพยากรไม่เพียงพอ

(4) มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต

11.2.3. ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอก องค์กร

11.3. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

11.3.1. แนวปฏิบัติสำหรับการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ทั้งของส่วนตัวและ อุปกรณ์ของทางราชการ

(1) ต้องล็อกหรือยึดเครื่องให้อยู่กับที่กรณีที่นำเครื่องไปใช้ในที่สาธารณะ หรือในบริเวณ ที่มีความเสี่ยงต่อการสูญหาย

(2) ต้องเปิดใช้ระบบล็อกหน้าจออัตโนมัติหรือปิดเครื่องอัตโนมัติเมื่อไม่ได้ใช้งานและใน กรณีที่ไม่ได้ใช้งานเป็นการชั่วคราวต้องล็อกหน้าจอทุกครั้ง

(3) ผู้ใช้ต้องตั้งรหัสผ่านเพื่อเข้าใช้งานคอมพิวเตอร์แบบพกพา

(4) ไม่ใช้อุปกรณ์คอมพิวเตอร์แบบพกพาร่วมกับบุคคลอื่น

(5) ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส ก่อนการใช้งานสื่อบันทึกข้อมูลพกพาต่าง ๆ

(6) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ที่ใช้งานอยู่ หากจำเป็นต้องจัดเก็บข้อมูลบนอุปกรณ์ดังกล่าวจะต้องเข้ารหัสข้อมูลทุกครั้ง

(7) ห้ามใช้อุปกรณ์คอมพิวเตอร์และสื่อสารพกพา เป็นอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายภายในโรงพยาบาล

(8) ต้องจัดการกับโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาเช่น ติดตั้งโปรแกรมป้องกันมัลแวร์ ปรับปรุงระบบปฏิบัติการให้ทันสมัย ไม่ติดตั้งซอฟต์แวร์ผิด กฎหมาย ไม่ติดตั้งซอฟต์แวร์ที่ไม่รู้จัก ฯลฯ

(9)มีกระบวนการจัดการกรณีที่อุปกรณ์คอมพิวเตอร์พกพาเกิดการสูญหายหรือถูกขโมย เช่น เปิดระบบล็อกไบออส เข้ารหัสไฟล์ข้อมูล เข้ารหัสฮาร์ดดิสก์ ติดตั้งโปรแกรมติดตามเครื่อง ฯลฯ

11.3.2. การสำรองข้อมูลและการกู้คืน

(1) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึก ข้อมูลสำรอง (backup media) เช่น ซีดี ดีวีดี ฮาร์ดดิสก์ภายนอก (External hard disks) เป็นต้น

(2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อบันทึกข้อมูลสำรองไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อ การรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

11.4. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

11.4.1. ผู้ใช้งานงานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

11.4.2. ต้องรักษาความปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงาน จากระยะไกลและระบบงานต่าง ๆ ภายในองค์กร

11.4.3. มีมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงาน ของผู้ใช้งานจากระยะไกล เพื่อป้องกันการขโมยอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

11.4.4. ผู้ใช้งานต้องไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศ ขององค์กรในสถานที่ดังกล่าว

11.4.5. ต้องตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบสารสนเทศขององค์กร จากระยะไกลมีระบบป้องกันไวรัสและการใช้งานไฟร์วอลล์อย่างเหมาะสม 11.4.6. ต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้เข้าถึงสำหรับการปฏิบัติงาน จาก ระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งาน ได้และระบบงานและบริการต่าง ๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากระยะไกล

**12. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (traffic log management)**

12.1. ต้องกำหนดผู้รักษาข้อมูลจราจรคอมพิวเตอร์ประจ าหน่วยงาน และมี Log server ของหน่วยงาน สำหรับรวบรวมข้อมูลจราจรคอมพิวเตอร์ที่พร้อมส่งมอบให้ผู้รักษาข้อมูลจราจรคอมพิวเตอร์เมื่อมีการร้องขอ

12.2. กำหนดวิธีการในการน าส่งข้อมูลจราจรคอมพิวเตอร์จากสื่อที่ใช้เก็บไปยัง Centralized Log Server ของหน่วยงาน

12.3. บันทึกการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย บันทึกการปฏิบัติงานของ ผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุกได้แก่ บันทึกการเข้าออก ระบบ ซึ่ง ประกอบด้วย บัญชีผู้ใช้ หมายเลขไอพีแอดเดรสต้นทาง หมายเลขไอพีแอดเดรสปลายทาง โปรโตคอล และหมายเลขพอร์ต เพื่อประโยชน์ในการใช้ตรวจสอบและเก็บบันทึกดังกล่าวไว้ตามที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

12.4. ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

12.5. กำหนดวิธีการป้องกันการแก้ไข เปลี่ยนแปลง หรือทำลาย ข้อมูลจราจรคอมพิวเตอร์ต่างๆ และจำกัด สิทธิ์การเข้าถึงข้อมูลจราจรคอมพิวเตอร์เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

**13. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (system administrator responsibilities)**

13.1. ผู้ดูแลระบบ แบ่งออกเป็น 3 กลุ่ม

13.1.1. ผู้ดูแลระบบเครือข่าย (system administrator)

13.1.2. ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (network administrator)

13.1.3. ผู้ดูแลระบบสารสนเทศ (application administrator)

13.2. ผู้ดูแลระบบเครือข่าย มีหน้าที่และความรับผิดชอบดังนี้

13.2.1. ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่ายและช่องทางการสื่อสารของระบบเครือข่ายอยู่ เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

13.2.2. เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้งาน นับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นระยะเวลาตามที่กฎหมายกำหนดนับตั้งแต่การใช้บริการสิ้นสุดลง และการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่ มั่นคงปลอดภัย ดังต่อไปนี้

(1) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับใน การเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความครบถ้วนถูกต้องและความน่าเชื่อถือของข้อมูล และไม่ให้ ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ ได้มีการกำหนดผู้ที่สามารถเข้าถึงข้อมูลได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน หรือบุคคลที่หน่วยงานมอบหมาย

(2) ข้อมูลจราจรทางคอมพิวเตอร์ต้องระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

(3) ข้อมูลจราจรทางคอมพิวเตอร์ต้องบันทึกอ้างอิงเวลากับเวลามาตรฐาน

13.3. ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย มีหน้าที่และความรับผิดชอบดังนี้

13.3.1. ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานให้เป็นไปด้วย ความเรียบร้อย และมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้รีบด าเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้น ในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายนี้ให้รีบ แจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่ จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานทันที

13.3.2. ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์ แม่ข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

13.3.3. ติดตั้งโปรแกรมสำหรับจัดการโปรแกรมไม่ประสงค์ดีต่างๆ ให้เหมาะสม

13.3.4. ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

13.3.5. ดูแลรักษาและปรับปรุงระบบบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายให้ถูกต้องและเป็น ปัจจุบันอยู่เสมอ

13.4. ผู้ดูแลระบบสารสนเทศ มีหน้าที่และความรับผิดชอบดังนี้

13.4.1. ดูแลรักษาและปรับปรุงบัญชีผู้ใช้ระบบสารสนเทศให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

13.4.2. ปรับปรุงรายการระบบสารสนเทศและรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศนั้น ให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

13.5. หลักธรรมาภิบาลของผู้ดูแลระบบ

13.5.1. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานโดยไม่มีเหตุผลอันสมควร

13.5.2. ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานหรือมี ข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร 13.5.3. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

**14. การใช้งานเครือข่ายสังคมออนไลน์ (social network)**

14.1. การใช้งานหรือใช้บริการเว็บไซต์เครือข่ายสังคมออนไลน์ ต้องใช้งานเพื่อประโยชน์ของทางราชการ เป็นสำคัญ

14.2. ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของผู้รับบริการ

14.3. ในการใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะท าให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน

14.4. หากผู้ใช้งานทราบหรือรู้สึกในภายหลังว่าการใช้งานเครือข่ายสังคมออนไลน์ของท่านอาจมีผลกระทบ กับหน่วยงาน ผู้ใช้งานต้องแจ้งงานสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความ เหมาะสม

**15. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (physical and environmental security)**

15.1. การจัดการบริเวณแวดล้อมทางกายภาพ

15.1.1. กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน

15.1.2. กำหนดระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

15.1.3. ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพอย่างสม่ำเสมอ เพื่อตรวจสอบว่า ยังใช้งานได้ตามปกติ

15.2. การควบคุมการเข้า-ออกพื้นที่ทางกายภาพ

15.2.1. ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ

15.2.2. ต้องควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

15.2.3. มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและต้องมี เหตุผลที่เพียงพอในการเข้าถึงพื้นที่ดังกล่าว

15.2.4. ต้องพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เพื่อควบคุมการเข้า-ออกในพื้นที่หรือ บริเวณที่มีความสำคัญ เช่น ห้องศูนย์กลางข้อมูล (data center)

15.2.5. ต้องบันทึกวันและเวลาเข้า-ออก ของผู้ที่มาเยือน และจัดเก็บบันทึกไว้เพื่อใช้ในการ ตรวจสอบในภายหลังเมื่อมีความจำเป็น

15.2.6. มีบันทึกรายการอุปกรณ์ที่นำเข้า-ออก

15.2.7. ดูแลผู้ที่มาเยือนจนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สินและ ป้องกันการเข้าถึงพื้นที่ส่วนอื่นที่ไม่ได้รับอนุญาต

15.2.8. ต้องควบคุมหน่วยงานภายนอกในการนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการ ปฏิบัติงานมาปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

15.2.9. สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

15.2.10. เจ้าหน้าที่ของบริษัทผู้ได้รับการว่าจ้าง/ผู้ที่มาเยือน ต้องติดบัตรให้เห็นชัดตลอดระยะเวลา การปฏิบัติงาน

15.2.11. ต้องดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติการในพื้นที่หรือ บริเวณที่มีความสำคัญ

15.2.12. ต้องทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

15.3. การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

15.3.1. จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการ เข้าถึงโดยไม่ได้รับอนุญาต

15.3.2. จำกัดบุคคลซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

15.3.3. จัดพื้นที่หรือบริเวณที่ส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลียงการเข้าถึงพื้นที่อื่นๆ ภายในโรงพยาบาล

15.3.4. ให้ตรวจสอบผลิตภัณฑ์ที่เป็นอันตรายก่อนที่จะโอนย้ายไปยังพื้นที่ใช้งาน

15.3.5. ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอก ให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของ โรงพยาบาล

15.4. การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ

15.4.1. จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

15.4.2. ต้องควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศเฉพาะผู้เกี่ยวข้องเท่านั้น

15.4.3. ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บน เครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

15.5. การนำทรัพย์สินของโรงพยาบาลออกนอกสำนักงาน

15.5.1. ต้องขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินออกนอกโรงพยาบาล

15.5.2. บันทึกข้อมูลการนำอุปกรณ์ของโรงพยาบาลออกนอกสำนักงาน เพื่อใช้เป็นหลักฐาน ป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

15.5.3. ให้เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินของโรงพยาบาลเสมือนเป็น ทรัพย์สินของตนเอง

15.6. ระบบและอุปกรณ์สนับสนุนการทำงาน

15.6.1. ต้องสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาล ที่เพียงพอต่อความต้องการใช้งาน โดยให้มี

(1) ระบบสำรองกระแสไฟฟ้า

(2) เครื่องกำเนิดกระแสไฟฟ้าสำรอง

(3) ระบบระบายอากาศ

(4) ระบบปรับอากาศและควบคุมความชื้น

(5) ระบบป้องกันอัคคีภัย

15.6.2. ต้องตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบ ทำงานปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

15.6.3. ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงาน ทำงานผิดปกติหรือ หยุดทำงาน

15.6.4. จัดทำแผนผังแสดงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ผู้เกี่ยวข้อง รับทราบ