แนวทางการประเมินด้านที่ 9
การรักษาความมั่นคงปลอดภัยไซเบอร์

อ้างอิงจาก กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข
พ.ศ. 2565

5 หัวข้อ ตามเกณฑ์การประเมินด้านที่ 9

1. โครงสร้างและบทบาท ระบบเทคโนโลยีสารสนเทศ (5 ข้อ)

2. การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ (5 ข้อ)

3. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ (6 ข้อ)

4. การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ (5 ข้อ)

5. การจัดการห้อง Data Center (เฉพาะที่มีห้อง Data Center) (5 ข้อ)

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

1. โครงสร้างและบทบาท ระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : โรงพยาบาลมีการจัดให้มีเป้าหมาย นโยบาย แผนงาน และโครงสร้างหน่วยงาน ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศที่มีความชัดเจน รวมทั้ง มีอัตรากำลังบุคลากรที่ทำงานด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจได้ว่าระบบเทคโนโลยีสารสนเทศของโรงพยาบาลจะสามารถตอบสนองการดูแลผู้ป่วยได้อย่างต่อเนื่องปลอดภัย

1.1 มีการจัดทีมดูแลระบบสารสนเทศของโรงพยาบาลประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ

1.2 มีการจัดทำแผนแม่บทหรือแผนพัฒนาของโรงพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน

1.3 มีนโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

1.4 มีการจัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของโรงพยาบาลที่เหมาะสม

1.5 มีการกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศต่างๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล

เกณฑ์ที่ได้ 1 คะแนน	**มีทีมดูแลระบบสารสนเทศของโรงพยาบาลประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศและแสดงเอกสารคำสั่งแต่งตั้งเป็นลายลักษณ์อักษร**
เอกสารประกอบตัวอย่าง เช่น	- คำสั่งแต่งตั้งทีมดูแลระบบสารสนเทศของโรงพยาบาลประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

1. โครงสร้างและบทบาท ระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : โรงพยาบาลมีการจัดให้มีเป้าหมาย นโยบาย แผนงานและโครงสร้างหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศที่มีความชัดเจน รวมทั้งมีอัตรากำลังบุคลากรที่ทำงานด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจได้ว่าระบบเทคโนโลยีสารสนเทศของโรงพยาบาลจะสามารถตอบสนองการดูแลผู้ป่วยได้อย่างต่อเนื่องปลอดภัย

1.1 มีการจัดทีมดูแลระบบสารสนเทศของโรงพยาบาล ประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ

1.2 มีการจัดทำแผนแม่บทหรือแผนพัฒนาของโรงพยาบาล โดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน

1.3 มีนโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

1.4 มีการจัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของโรงพยาบาลที่เหมาะสม

1.5 มีการกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศต่างๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล

เกณฑ์ที่ได้ 1 คะแนน	**มีแผนแม่บท หรือแผนพัฒนาของโรงพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน (แผนดังกล่าวครอบคลุมปีที่ทำการประเมิน)**
เอกสารประกอบตัวอย่าง เช่น	- แผนแม่บทของโรงพยาบาล , โครงการหรือแนวทางการพัฒนางานและการใช้เทคโนโลยีสารสนเทศ

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

1. โครงสร้างและบทบาท ระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : โรงพยาบาลมีการจัดให้มีเป้าหมาย นโยบาย แผนงานและโครงสร้างหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศที่มีความชัดเจน รวมทั้งมีอัตรากำลังบุคลากรที่ทำงานด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจได้ว่าระบบเทคโนโลยีสารสนเทศของโรงพยาบาลจะสามารถตอบสนองการดูแลผู้ป่วยได้อย่างต่อเนื่องปลอดภัย

1.1 มีการจัดทีมดูแลระบบสารสนเทศของโรงพยาบาล ประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ

1.2 มีการจัดทำแผนแม่บทหรือแผนพัฒนาของโรงพยาบาล โดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน

1.3 มีนโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

1.4 มีการจัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของโรงพยาบาลที่เหมาะสม

1.5 มีการกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศต่างๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล

เกณฑ์ที่ได้ 1 คะแนน	**มีนโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล (Action Plan) (แผนการปฏิบัติของปีปัจจุบัน)**
เอกสารประกอบตัวอย่าง เช่น	- นโยบายด้านเทคโนโลยีสารสนเทศต่างๆ ของโรงพยาบาล , แผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

1. โครงสร้างและบทบาท ระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : โรงพยาบาลมีการจัดให้มีเป้าหมาย นโยบาย แผนงานและโครงสร้างหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศที่มีความชัดเจน รวมทั้งมีอัตรากำลังบุคลากรที่ทำงานด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจได้ว่าระบบเทคโนโลยีสารสนเทศของโรงพยาบาลจะสามารถตอบสนองการดูแลผู้ป่วยได้อย่างต่อเนื่องปลอดภัย

1.1 มีการจัดทีมดูแลระบบสารสนเทศของโรงพยาบาล ประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ

1.2 มีการจัดทำแผนแม่บทหรือแผนพัฒนาของโรงพยาบาล โดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน

1.3 มีนโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

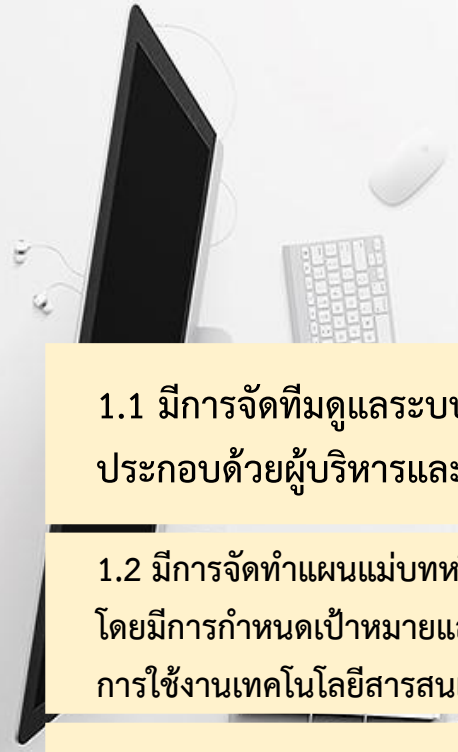
1.4 มีการจัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของโรงพยาบาลที่เหมาะสม

1.5 มีการกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศต่างๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล

เกณฑ์ที่ได้ 1 คะแนน	มีการแสดงโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของโรงพยาบาลที่เหมาะสม (จำนวนบุคลากร)
เอกสารประกอบตัวอย่าง เช่น	- แผนผังโครงสร้างองค์กร หรือหน่วยงานสารสนเทศของโรงพยาบาล

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ



1. โครงสร้างและบทบาท ระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : โรงพยาบาลมีการจัดให้มีเป้าหมาย นโยบาย แผนงานและโครงสร้างหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศที่มีความชัดเจน รวมทั้งมีอัตรากำลังบุคลากรที่ทำงานด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจได้ว่าระบบเทคโนโลยีสารสนเทศของโรงพยาบาลจะสามารถตอบสนองการดูแลผู้ป่วยได้อย่างต่อเนื่องปลอดภัย

1.1 มีการจัดทีมดูแลระบบสารสนเทศของโรงพยาบาล ประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ

1.2 มีการจัดทำแผนแม่บทหรือแผนพัฒนาของโรงพยาบาล โดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน

1.3 มีนโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

1.4 มีการจัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของโรงพยาบาลที่เหมาะสม

1.5 มีการกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศต่างๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล

เกณฑ์ที่ได้ 1 คะแนน	**มีการแสดงหลักฐาน ระเบียบหรือมาตรฐานด้านเทคโนโลยีสารสนเทศต่างๆ ที่จำเป็น สอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล ได้แก่ มาตรฐานข้อมูล มาตรฐานรหัสข้อมูล มาตรฐานการปฏิบัติงาน มาตรฐานความปลอดภัยและความลับของผู้ป่วย มาตรฐานระบบเครือข่ายคอมพิวเตอร์ มาตรฐานทางกายภาพและสภาพแวดล้อม และมีความสมบูรณ์ของหลักฐานของระเบียบหรือมาตรการมาตรฐานด้านเทคโนโลยีสารสนเทศด้านต่างๆ**
เอกสารประกอบตัวอย่าง เช่น	- เอกสาร ระเบียบ หรือมาตรฐานที่เกี่ยวกับเทคโนโลยีสารสนเทศของโรงพยาบาล

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

2. การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : ระบบการจัดการความเสี่ยงที่เริ่มจากการประเมินความเสี่ยงทุกด้านที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศโรงพยาบาล ให้คะแนนความเสี่ยงและจัดลำดับความสำคัญ จัดทำแผนการจัดการความเสี่ยงเป็นลายลักษณ์อักษร มีเลขหน้ากำกับ ประกอบด้วยผลการประเมินความเสี่ยง ยุทธศาสตร์การจัดการความเสี่ยงและแผนปฏิบัติการที่กำหนดระยะเวลาที่จะดำเนินการตามแผนในช่วง 1 ปี เมื่อจบการดำเนินการตามแผนต้องมีการประเมินผลการดำเนินงานและนำผลการประเมินมาปรับปรุงเป็นแผนในรอบปีต่อไป รวมทั้งการจัดการความเสี่ยงที่จะเกิดขึ้นกับผู้ป่วยจากการใช้เทคโนโลยีสารสนเทศด้วย

2.1 มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย

2.2 มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบอย่างชัดเจน

2.3 มีการดำเนินการตามแผนจัดการความเสี่ยง

2.4 มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยงและวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน

2.5 มีการนำผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น

เกณฑ์ที่ได้ 1 คะแนน	มีการประเมินความเสี่ยงและการให้คะแนนความเสี่ยงและการจัดลำดับความสำคัญ
เอกสารประกอบตัวอย่าง เช่น	- เอกสารหรือหลักฐานการประเมินความเสี่ยงของระบบสารสนเทศ

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

2. การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : ระบบการจัดการความเสี่ยงที่เริ่มจากการประเมินความเสี่ยงทุกด้านที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศโรงพยาบาล ให้คะแนนความเสี่ยงและจัดลำดับความสำคัญ จัดทำแผนการจัดการความเสี่ยงเป็นลายลักษณ์อักษร มีเลขหน้ากำกับ ประกอบด้วยผลการประเมินความเสี่ยง ยุทธศาสตร์การจัดการความเสี่ยงและแผนปฏิบัติการที่กำหนดระยะเวลาที่จะดำเนินการตามแผนในช่วง 1 ปี เมื่อจบการดำเนินการตามแผนต้องมีการประเมินผลการดำเนินงานและนำผลการประเมินมาปรับปรุงเป็นแผนในรอบปีต่อไป รวมทั้งการจัดการความเสี่ยงที่จะเกิดขึ้นกับผู้ป่วยจากการใช้เทคโนโลยีสารสนเทศด้วย

2.1 มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย

2.2 มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบอย่างชัดเจน

2.3 มีการดำเนินการตามแผนจัดการความเสี่ยง

2.4 มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยงและวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน

2.5 มีการนำผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น

เกณฑ์ที่ได้ 1 คะแนน	**มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์ โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบ อย่างชัดเจน**
เอกสารประกอบตัวอย่าง เช่น	- แผนการจัดการความเสี่ยง

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

2. การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : ระบบการจัดการความเสี่ยงที่เริ่มจากการประเมินความเสี่ยงทุกด้านที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศโรงพยาบาล ให้คะแนนความเสี่ยงและจัดลำดับความสำคัญ จัดทำแผนการจัดการความเสี่ยงเป็นลายลักษณ์อักษร มีเลขหน้ากำกับ ประกอบด้วยผลการประเมินความเสี่ยง ยุทธศาสตร์การจัดการความเสี่ยงและแผนปฏิบัติการที่กำหนดระยะเวลาที่จะดำเนินการตามแผนในช่วง 1 ปี เมื่อจบการดำเนินการตามแผนต้องมีการประเมินผลการดำเนินงานและนำผลการประเมินมาปรับปรุงเป็นแผนในรอบปีต่อไป รวมทั้งการจัดการความเสี่ยงที่จะเกิดขึ้นกับผู้ป่วยจากการใช้เทคโนโลยีสารสนเทศด้วย

2.1 มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย

2.2 มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบอย่างชัดเจน

2.3 มีการดำเนินการตามแผนจัดการความเสี่ยง

2.4 มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยงและวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน

2.5 มีการนำผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น

เกณฑ์ที่ได้ 1 คะแนน	**มีการดำเนินการตามแผนจัดการความเสี่ยง (ตามข้อ 2.2) และตามระยะเวลาที่กำหนดในแผนจัดการความเสี่ยง**
เอกสารประกอบตัวอย่าง เช่น	- หลักฐานการดำเนินงานตามแผนจัดการความเสี่ยง

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

2. การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : ระบบการจัดการความเสี่ยงที่เริ่มจากการประเมินความเสี่ยงทุกด้านที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศโรงพยาบาล ให้คะแนนความเสี่ยงและจัดลำดับความสำคัญ จัดทำแผนการจัดการความเสี่ยงเป็นลายลักษณ์อักษร มีเลขหน้ากำกับ ประกอบด้วยผลการประเมินความเสี่ยง ยุทธศาสตร์การจัดการความเสี่ยงและแผนปฏิบัติการที่กำหนดระยะเวลาที่จะดำเนินการตามแผนในช่วง 1 ปี เมื่อจบการดำเนินการตามแผนต้องมีการประเมินผลการดำเนินงานและนำผลการประเมินมาปรับปรุงเป็นแผนในรอบปีต่อไป รวมทั้งการจัดการความเสี่ยงที่จะเกิดขึ้นกับผู้ป่วยจากการใช้เทคโนโลยีสารสนเทศด้วย

2.1 มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย

2.2 มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบอย่างชัดเจน

2.3 มีการดำเนินการตามแผนจัดการความเสี่ยง

2.4 มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยงและวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน

2.5 มีการนำผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น

เกณฑ์ที่ได้ 1 คะแนน	**มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยงและวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน**
เอกสารประกอบตัวอย่าง เช่น	- วิธีการ หรือ ระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศ

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

2. การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : ระบบการจัดการความเสี่ยงที่เริ่มจากการประเมินความเสี่ยงทุกด้านที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศโรงพยาบาล ให้คะแนนความเสี่ยงและจัดลำดับความสำคัญ จัดทำแผนการจัดการความเสี่ยงเป็นลายลักษณ์อักษร มีเลขหน้ากำกับ ประกอบด้วยผลการประเมินความเสี่ยง ยุทธศาสตร์การจัดการความเสี่ยงและแผนปฏิบัติการที่กำหนดระยะเวลาที่จะดำเนินการตามแผนในช่วง 1 ปี เมื่อจบการดำเนินการตามแผนต้องมีการประเมินผลการดำเนินงานและนำผลการประเมินมาปรับปรุงเป็นแผนในรอบปีต่อไป รวมทั้งการจัดการความเสี่ยงที่จะเกิดขึ้นกับผู้ป่วยจากการใช้เทคโนโลยีสารสนเทศด้วย

2.1 มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศอย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย

2.2 มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบอย่างชัดเจน

2.3 มีการดำเนินการตามแผนจัดการความเสี่ยง

2.4 มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยงและวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน

2.5 มีการนำผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น

เกณฑ์ที่ได้ 1 คะแนน	**มีผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น**
เอกสารประกอบตัวอย่าง เช่น	- สรุปผลการดำเนินงาน มีแนวทางในการจัดการความเสี่ยงที่ชัดเจน

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

3. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : ระบบการจัดการความมั่นคงปลอดภัยที่เริ่มจากการกำหนดนโยบายด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล การจัดทำระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่ผู้ใช้ระบบทุกคนต้องปฏิบัติตาม การสร้างความตระหนัก การประชาสัมพันธ์นโยบายและจัดอบรมให้ความรู้ระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ การตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด รวมถึงการจัดการ Data Center ของโรงพยาบาลให้มั่นคงปลอดภัย ได้มาตรฐานทางกายภาพตามแนวทางการปฏิบัติที่ดี

- 3.1 มีการจัดทำนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบ IT
- 3.2 มีนโยบายและระเบียบปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้
- 3.3 มีนโยบายและระเบียบปฏิบัติที่ป้องกันความลับผู้ป่วยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน
- 3.4 มีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ
- 3.5 มีการตรวจสอบว่าบุคลากรได้รับทราบเข้าใจยอมรับและปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด
- 3.6 มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติต่อไป

เกณฑ์ที่ได้ 1 คะแนน	มีนโยบายด้านความมั่นคงปลอดภัย และระเบียบปฏิบัติสำหรับผู้ใช้ระบบมีเป็นลายลักษณ์อักษร
เอกสารประกอบตัวอย่าง เช่น	- นโยบายด้านความมั่นคงปลอดภัย แนวปฏิบัติ/ระเบียบปฏิบัติสำหรับผู้ใช้ระบบ

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

3. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : ระบบการจัดการความมั่นคงปลอดภัยที่เริ่มจากการกำหนดนโยบายด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล การจัดทำระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่ผู้ใช้ระบบทุกคนต้องปฏิบัติตาม การสร้างความตระหนัก การประชาสัมพันธ์นโยบายและจัดอบรมให้ความรู้ระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ การตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด รวมถึงการจัดการ Data Center ของโรงพยาบาลให้มั่นคงปลอดภัย ได้มาตรฐานทางกายภาพตามแนวทางการปฏิบัติที่ดี

3.1 มีการจัดทำนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบ IT

3.2 มีนโยบายและระเบียบปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้

3.3 มีนโยบายและระเบียบปฏิบัติที่ป้องกันความลับผู้ป่วยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน

3.4 มีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ

3.5 มีการตรวจสอบว่าบุคลากรได้รับทราบเข้าใจยอมรับและปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด

3.6 มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติต่อไป

เกณฑ์ที่ได้ 1 คะแนน	**มีนโยบายและระเบียบปฏิบัติที่กำหนดห้ามแพทย์หรือพยาบาลเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบปัจจุบัน มีเป็นลายลักษณ์อักษร**
เอกสารประกอบตัวอย่าง เช่น	- นโยบาย แนวปฏิบัติ/ระเบียบปฏิบัติที่กำหนดห้ามแพทย์หรือพยาบาลเข้าถึงข้อมูลผู้ป่วย หรือ คำสั่งการเข้าถึงข้อมูล

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

3. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : ระบบการจัดการความมั่นคงปลอดภัยที่เริ่มจากการกำหนดนโยบายด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล การจัดทำระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่ผู้ใช้ระบบทุกคนต้องปฏิบัติตาม การสร้างความตระหนัก การประชาสัมพันธ์นโยบายและจัดอบรมให้ความรู้ระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ การตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด รวมถึงการจัดการ Data Center ของโรงพยาบาลให้มั่นคงปลอดภัย ได้มาตรฐานทางกายภาพตามแนวทางการปฏิบัติที่ดี

3.1 มีการจัดทำนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบ IT

3.2 มีนโยบายและระเบียบปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้

3.3 มีนโยบายและระเบียบปฏิบัติที่ป้องกันความลับผู้ป่วยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน

3.4 มีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ

3.5 มีการตรวจสอบว่าบุคลากรได้รับทราบเข้าใจยอมรับและปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด

3.6 มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติต่อไป

เกณฑ์ที่ได้ 1 คะแนน	**มีนโยบายและระเบียบปฏิบัติที่กำหนดการป้องกันความลับผู้ป่วย มิให้รั่วไหล มีเป็นลายลักษณ์อักษร**
เอกสารประกอบตัวอย่าง เช่น	- นโยบาย แนวปฏิบัติ/ระเบียบปฏิบัติที่กำหนดการป้องกันความลับผู้ป่วยมิให้รั่วไหล

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

3. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : ระบบการจัดการความมั่นคงปลอดภัยที่เริ่มจากการกำหนดนโยบายด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล การจัดทำระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่ผู้ใช้ระบบทุกคนต้องปฏิบัติตาม การสร้างความตระหนัก การประชาสัมพันธ์นโยบายและจัดอบรมให้ความรู้ระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ การตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด รวมถึงการจัดการ Data Center ของโรงพยาบาลให้มั่นคงปลอดภัย ได้มาตรฐานทางกายภาพตามแนวทางการปฏิบัติที่ดี

3.1 มีการจัดทำนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบ IT

3.2 มีนโยบายและระเบียบปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้

3.3 มีนโยบายและระเบียบปฏิบัติที่ป้องกันความลับผู้ป่วยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน

3.4 มีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ

3.5 มีการตรวจสอบว่าบุคลากรได้รับทราบเข้าใจยอมรับและปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด

3.6 มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติต่อไป

เกณฑ์ที่ได้ 1 คะแนน	**มีหลักฐานการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ (ตามข้อ 3.1- ข้อ 3.3)**
เอกสารประกอบตัวอย่าง เช่น	- รูปถ่าย ประชาสัมพันธ์ผ่านเว็บไซต์ เอกสารแจ้งเวียนที่เกี่ยวข้อง

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

3. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : ระบบการจัดการความมั่นคงปลอดภัยที่เริ่มจากการกำหนดนโยบายด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล การจัดทำระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่ผู้ใช้ระบบทุกคนต้องปฏิบัติตาม การสร้างความตระหนัก การประชาสัมพันธ์นโยบายและจัดอบรมให้ความรู้ระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ การตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด รวมถึงการจัดการ Data Center ของโรงพยาบาลให้มั่นคงปลอดภัย ได้มาตรฐานทางกายภาพตามแนวทางการปฏิบัติที่ดี

- 3.1 มีการจัดทำนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบ IT
- 3.2 มีนโยบายและระเบียบปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้
- 3.3 มีนโยบายและระเบียบปฏิบัติที่ป้องกันความลับผู้ป่วยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน
- 3.4 มีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ
- 3.5 มีการตรวจสอบว่าบุคลากรได้รับทราบเข้าใจยอมรับและปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด
- 3.6 มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติต่อไป

เกณฑ์ที่ได้ 1 คะแนน	มีผลการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับและปฏิบัติตามระเบียบด้านความมั่นคงปลอดภัย
เอกสารประกอบตัวอย่าง เช่น	- หนังสือเวียน แบบสอบถาม แบบประเมิน แบบสำรวจฯ

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

3. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : ระบบการจัดการความมั่นคงปลอดภัยที่เริ่มจากการกำหนดนโยบายด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล การจัดทำระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่ผู้ใช้ระบบทุกคนต้องปฏิบัติตาม การสร้างความตระหนัก การประชาสัมพันธ์นโยบายและจัดอบรมให้ความรู้ระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ การตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด รวมถึงการจัดการ Data Center ของโรงพยาบาลให้มั่นคงปลอดภัย ได้มาตรฐานทางกายภาพตามแนวทางการปฏิบัติที่ดี

3.1 มีการจัดทำนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบ IT

3.2 มีนโยบายและระเบียบปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้

3.3 มีนโยบายและระเบียบปฏิบัติที่ป้องกันความลับผู้ป่วยมิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน

3.4 มีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ

3.5 มีการตรวจสอบว่าบุคลากรได้รับทราบเข้าใจยอมรับและปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างเคร่งครัด

3.6 มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติต่อไป

เกณฑ์ที่ได้ 1 คะแนน	มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติในครั้งถัดไป
เอกสารประกอบตัวอย่าง เช่น	- สรุปผลการประเมิน

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

4. การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : การวิเคราะห์สถานการณ์ปัจจุบันของทรัพยากรด้าน Hardware, software, network และบุคลากรด้าน IT การทำการวิเคราะห์ช่องว่าง (Gap analysis) การจัดทำแผนเพิ่มศักยภาพของทรัพยากร IT การกำหนดสมรรถนะ การประเมินสมรรถนะ และการดำเนินการพัฒนาสมรรถนะของบุคลากรในฝ่าย IT เพื่อให้มั่นใจว่าศักยภาพของระบบเทคโนโลยีสารสนเทศมีเพียงพอต่อการดำเนินงานตามแผนด้านเทคโนโลยีสารสนเทศ

4.1 มีการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร

4.2 มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network

4.3 มีการกำหนดสมรรถนะตามบทบาทหน้าที่ ที่จำเป็นของบุคลากรด้าน IT ทุกคน ประเมินสมรรถนะตามบทบาทหน้าที่และจัดทำแผนเพิ่มสมรรถนะรายบุคคล

4.4 มีการดำเนินการตามแผนเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) และ มีการประเมินวิเคราะห์ผลการดำเนินตามแผน

4.5 มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น

เกณฑ์ที่ได้ 1 คะแนน	**มีผลการวิเคราะห์สถานการณ์ปัจจุบัน และ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร**
เอกสารประกอบตัวอย่าง เช่น	- แบบวิเคราะห์ทรัพยากรฯ/กราฟ/ตาราง

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

4. การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : การวิเคราะห์สถานการณ์ปัจจุบันของทรัพยากรด้าน Hardware, software, network และบุคลากรด้าน IT การทำการวิเคราะห์ช่องว่าง (Gap analysis) การจัดทำแผนเพิ่มศักยภาพของทรัพยากร IT การกำหนดสมรรถนะ การประเมินสมรรถนะ และการดำเนินการพัฒนาสมรรถนะของบุคลากรในฝ่าย IT เพื่อให้มั่นใจว่าศักยภาพของระบบเทคโนโลยีสารสนเทศมีเพียงพอต่อการดำเนินงานตามแผนด้านเทคโนโลยีสารสนเทศ

4.1 มีการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร

4.2 มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network

4.3 มีการกำหนดสมรรถนะตามบทบาทหน้าที่ ที่จำเป็นของบุคลากรด้าน IT ทุกคน ประเมินสมรรถนะตามบทบาทหน้าที่และจัดทำแผนเพิ่มสมรรถนะรายบุคคล

4.4 มีการดำเนินการตามแผนเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) และ มีการประเมินวิเคราะห์ผลการดำเนินตามแผน

4.5 มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น

เกณฑ์ที่ได้ **1 คะแนน**	**มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน** Hardware, Software, Network
เอกสารประกอบตัวอย่าง เช่น	- แนวทางการเพิ่มศัพยภาพของทรัพยากร (จากผลข้อ 4.1)

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

4. การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : การวิเคราะห์สถานการณ์ปัจจุบันของทรัพยากรด้าน Hardware, software, network และบุคลากรด้าน IT การทำการวิเคราะห์ช่องว่าง (Gap analysis) การจัดทำแผนเพิ่มศักยภาพของทรัพยากร IT การกำหนดสมรรถนะ การประเมินสมรรถนะ และการดำเนินการพัฒนาสมรรถนะของบุคลากรในฝ่าย IT เพื่อให้มั่นใจว่าศักยภาพของระบบเทคโนโลยีสารสนเทศมีเพียงพอต่อการดำเนินงานตามแผนด้านเทคโนโลยีสารสนเทศ

4.1 มีการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร

4.2 มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network

4.3 มีการกำหนดสมรรถนะตามบทบาทหน้าที่ ที่จำเป็นของบุคลากรด้าน IT ทุกคน ประเมินสมรรถนะตามบทบาทหน้าที่และจัดทำแผนเพิ่มสมรรถนะรายบุคคล

4.4 มีการดำเนินการตามแผนเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) และ มีการประเมินวิเคราะห์ผลการดำเนินตามแผน

4.5 มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น

เกณฑ์ที่ได้ 1 คะแนน	**มีการกำหนดสมรรถนะตามบทบาทหน้าที่ของของบุคลากรด้าน IT ทุกคน ผลการประเมินสมรรถนะตามบทบาทหน้าที่ และมีแผนการเพิ่มสมรรถนะรายบุคคล**
เอกสารประกอบตัวอย่าง เช่น	- เอกสารกำหนดสมรรถนะของเจ้าหน้าที่ , เอกสารการประเมินสมรรถนะ , แผนเพิ่มสมรรถนะ (จากผลข้อ 4.1 ด้านบุคลากร)

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

4. การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : การวิเคราะห์สถานการณ์ปัจจุบันของทรัพยากรด้าน Hardware, software, network และบุคลากรด้าน IT การทำการวิเคราะห์ช่องว่าง (Gap analysis) การจัดทำแผนเพิ่มศักยภาพของทรัพยากร IT การกำหนดสมรรถนะ การประเมินสมรรถนะ และการดำเนินการพัฒนาสมรรถนะของบุคลากรในฝ่าย IT เพื่อให้มั่นใจว่าศักยภาพของระบบเทคโนโลยีสารสนเทศมีเพียงพอต่อการดำเนินงานตามแผนด้านเทคโนโลยีสารสนเทศ

4.1 มีการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร

4.2 มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network

4.3 มีการกำหนดสมรรถนะตามบทบาทหน้าที่ ที่จำเป็นของบุคลากรด้าน IT ทุกคน ประเมินสมรรถนะตามบทบาทหน้าที่และจัดทำแผนเพิ่มสมรรถนะรายบุคคล

4.4 มีการดำเนินการตามแผนเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) และ มีการประเมินวิเคราะห์ผลการดำเนินตามแผน

4.5 มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น

เกณฑ์ที่ได้ 1 คะแนน	**มีการดำเนินการตามแผนการเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) และมีการประเมิน วิเคราะห์ผลการดำเนินตามแผน**
เอกสารประกอบตัวอย่าง เช่น	- สรุปผลการดำเนินงาน รายงานแผนการเพิ่มสมรรถนะฯ

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

4. การจัดการศักยภาพของทรัพยากรในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : การวิเคราะห์สถานการณ์ปัจจุบันของทรัพยากรด้าน Hardware, software, network และบุคลากรด้าน IT การทำการวิเคราะห์ช่องว่าง (Gap analysis) การจัดทำแผนเพิ่มศักยภาพของทรัพยากร IT การกำหนดสมรรถนะ การประเมินสมรรถนะ และการดำเนินการพัฒนาสมรรถนะของบุคลากรในฝ่าย IT เพื่อให้มั่นใจว่าศักยภาพของระบบเทคโนโลยีสารสนเทศมีเพียงพอต่อการดำเนินงานตามแผนด้านเทคโนโลยีสารสนเทศ

4.1 มีการวิเคราะห์สถานการณ์ปัจจุบันและ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร

4.2 มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network

4.3 มีการกำหนดสมรรถนะตามบทบาทหน้าที่ ที่จำเป็นของบุคลากรด้าน IT ทุกคน ประเมินสมรรถนะตามบทบาทหน้าที่และจัดทำแผนเพิ่มสมรรถนะรายบุคคล

4.4 มีการดำเนินการตามแผนเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) และ มีการประเมินวิเคราะห์ผลการดำเนินตามแผน

4.5 มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น

เกณฑ์ที่ได้ 1 คะแนน	**มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น**
เอกสารประกอบตัวอย่าง เช่น	- สรุปผลการดำเนินงาน สรุปผลการวิเคราะห์

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

5. การจัดการห้อง Data Center

คำอธิบาย : Data Center ของโรงพยาบาลได้แก่ ที่ตั้งของ Server และอุปกรณ์ที่เกี่ยวข้อง เช่น ระบบสำรองข้อมูล อุปกรณ์สำรอง Redundant system ระบบรักษาความปลอดภัย เป็นต้น จะต้องมีการจัดการอย่างเหมาะสม โดยระบบสามารถทำงานได้อย่างปลอดภัย และมีประสิทธิภาพ

5.1 มีการจัดการ Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัย

5.2 ห้อง สถานที่ และสิ่งแวดล้อมต้องจัดให้มีความปลอดภัยจากบุคคลภายนอก

5.3 มีระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงและระบบดับเพลิงอัตโนมัติ

5.4 มีระบบป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) , ระบบ RAID , Redundant Power supply , Redundant Server

5.5 มีการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยงและความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center

เกณฑ์ที่ได้ 1 คะแนน	**มีการจัดทำแผนในการจัดการห้อง Data Center และ มีการจัดการห้อง Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัย**
เอกสารประกอบตัวอย่าง เช่น	- เอกสารการจัดทำแผนในการจัดการห้อง Data Center พร้อมลงนามโดย CIO รูปถ่ายบางส่วนที่ได้ดำเนินการตรวจสอบ บำรุงรักษาเชิงป้องกัน (PM) เป็นต้น

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

5. การจัดการห้อง Data Center

คำอธิบาย : Data Center ของโรงพยาบาลได้แก่ ที่ตั้งของ Server และอุปกรณ์ที่เกี่ยวข้อง เช่น ระบบสำรองข้อมูล อุปกรณ์สำรอง Redundant system ระบบรักษาความปลอดภัย เป็นต้น จะต้องมีการจัดการอย่างเหมาะสม โดยระบบสามารถทำงานได้อย่างปลอดภัย และมีประสิทธิภาพ

5.1 มีการจัดการ Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัย

5.2 ห้อง สถานที่ และสิ่งแวดล้อมต้องจัดให้มีความปลอดภัยจากบุคคลภายนอก

5.3 มีระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงและระบบดับเพลิงอัตโนมัติ

5.4 มีระบบป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) , ระบบ RAID , Redundant Power supply , Redundant Server

5.5 มีการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยงและความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center

เกณฑ์ที่ได้ 1 คะแนน	**มีการแสดงหลักฐานห้อง สถานที่ และสิ่งแวดล้อม ต้องจัดให้มีความปลอดภัย จากบุคคลภายนอก**
เอกสารประกอบตัวอย่าง เช่น	1. รูปภาพโดยรอบห้อง Data Center โดยจะต้องไม่มีป้ายบอกว่าเป็นห้อง Data Center และต้องมีรูปป้ายห้ามบุคคลภายนอกเข้า 2. รูปทางเข้าห้อง Data Center อย่างน้อยต้องมีภาพกล้องวงจรปิดหรือเครื่องสแกนลายนิ้วมือ หรือเครื่องพิสูจน์ตัวตนที่ดีกว่า

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

5. การจัดการห้อง Data Center

คำอธิบาย : Data Center ของโรงพยาบาลได้แก่ ที่ตั้งของ Server และอุปกรณ์ที่เกี่ยวข้อง เช่น ระบบสำรองข้อมูล อุปกรณ์สำรอง Redundant system ระบบรักษาความปลอดภัย เป็นต้น จะต้องมีการจัดการอย่างเหมาะสม โดยระบบสามารถทำงานได้อย่างปลอดภัย และมีประสิทธิภาพ

5.1 มีการจัดการ Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัย

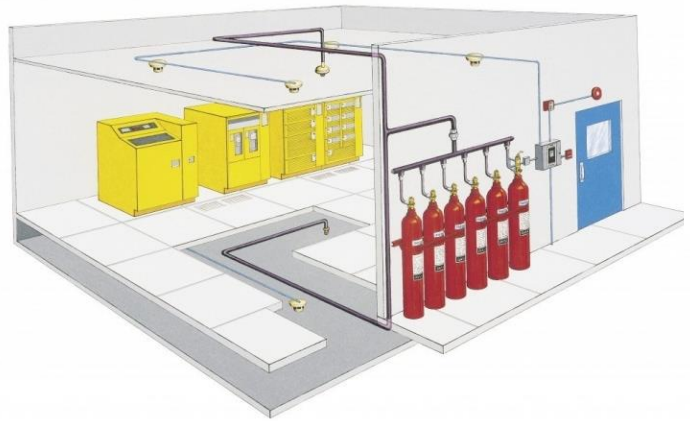
5.2 ห้อง สถานที่ และสิ่งแวดล้อมต้องจัดให้มีความปลอดภัยจากบุคคลภายนอก

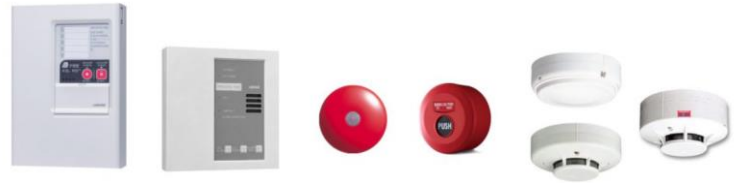
5.3 มีระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงและระบบดับเพลิงอัตโนมัติ

5.4 มีระบบป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) , ระบบ RAID , Redundant Power supply , Redundant Server

5.5 มีการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยงและความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center

เกณฑ์ที่ได้ 1 คะแนน	**มีการแสดงหลักฐานด้านระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงและระบบดับเพลิงอัตโนมัติ**
เอกสารประกอบตัวอย่าง เช่น	- ภาพถ่ายของระบบต่างๆ





แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

5. การจัดการห้อง Data Center

คำอธิบาย : Data Center ของโรงพยาบาลได้แก่ ที่ตั้งของ Server และอุปกรณ์ที่เกี่ยวข้อง เช่น ระบบสำรองข้อมูล อุปกรณ์สำรอง Redundant system ระบบรักษาความปลอดภัย เป็นต้น จะต้องมีการจัดการอย่างเหมาะสม โดยระบบสามารถทำงานได้อย่างปลอดภัย และมีประสิทธิภาพ

5.1 มีการจัดการ Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัย

5.2 ห้อง สถานที่ และสิ่งแวดล้อมต้องจัดให้มีความปลอดภัยจากบุคคลภายนอก

5.3 มีระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงและระบบดับเพลิงอัตโนมัติ

5.4 มีระบบป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) , ระบบ RAID , Redundant Power supply , Redundant Server

5.5 มีการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยงและความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center

เกณฑ์ที่ได้ 1 คะแนน	**มีการแสดงหลักฐานด้านการป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply , Redundant Server**
เอกสารประกอบตัวอย่าง เช่น	- ภาพถ่ายของระบบ / แสดงเอกสารหลักฐานของระบบนั้นๆ

แนวทางการประเมินด้านที่ 9 การรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์สนับสนุนบริการสุขภาพที่ ๑
กรมสนับสนุนบริการสุขภาพ

5. การจัดการห้อง Data Center

คำอธิบาย : Data Center ของโรงพยาบาลได้แก่ ที่ตั้งของ Server และอุปกรณ์ที่เกี่ยวข้อง เช่น ระบบสำรองข้อมูล อุปกรณ์สำรอง Redundant system ระบบรักษาความปลอดภัย เป็นต้น จะต้องมีการจัดการอย่างเหมาะสม โดยระบบสามารถทำงานได้อย่างปลอดภัย และมีประสิทธิภาพ

5.1 มีการจัดการ Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัย

5.2 ห้อง สถานที่ และสิ่งแวดล้อมต้องจัดให้มีความปลอดภัยจากบุคคลภายนอก

5.3 มีระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงและระบบดับเพลิงอัตโนมัติ

5.4 มีระบบป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) , ระบบ RAID , Redundant Power supply , Redundant Server

5.5 มีการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยงและความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center

เกณฑ์ที่ได้ 1 คะแนน	**มีการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยงและนำผลการวิเคราะห์มาวัดความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center**
เอกสารประกอบตัวอย่าง เช่น	- มีผลการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยงและความคุ้มค่า หรือแผนงานความเสี่ยงของอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ภายในห้อง Data Center