



ด้านที่ 9 ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

พ.ศ. 2564

แนวทางประเมินมาตรฐานระบบบริการสุขภาพ ด้านที่ 9 ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

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)



1. โครงสร้างและบทบาท ระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : โรงพยาบาลมีการจัดให้มีเป้าหมาย นโยบาย แผนงานและโครงสร้างหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศที่มีความชัดเจนรวมทั้งมีอัตรากำลังบุคลากรที่ทำงานด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจได้ว่าระบบเทคโนโลยีสารสนเทศโรงพยาบาลจะสามารถตอบสนองการดูแลผู้ป่วยได้อย่างต่อเนื่องปลอดภัย





1.1 มีการจัดทีมดูแลระบบสารสนเทศของโรงพยาบาลประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ

0 คะแนน	ไม่มีการแสดงคำสั่งแต่งตั้งทีมดูแลระบบสารสนเทศของโรงพยาบาลประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ
0.5 คะแนน	มีทีมดูแลระบบสารสนเทศของโรงพยาบาลประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศแต่ขาดคำสั่งแต่งตั้ง
1 คะแนน	มีการแสดงคำสั่งแต่งตั้งทีมดูแลระบบสารสนเทศของโรงพยาบาลประกอบด้วยผู้บริหารและฝ่ายเทคโนโลยีสารสนเทศ



1.2 มีการจัดทำแผนแม่บทหรือแผนพัฒนาของโรงพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน

0 คะแนน	ไม่มีแผนแม่บทหรือแผนพัฒนาของโรงพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน
0.5 คะแนน	มีแผนแม่บทหรือแผนพัฒนาของโรงพยาบาลโดยมีการกำหนดเป้าหมาย หรือแนวทางการพัฒนาหรือการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน
1 คะแนน	มีแผนแม่บทหรือแผนพัฒนาของโรงพยาบาลโดยมีการกำหนดเป้าหมายและแนวทางการพัฒนาและการใช้งานเทคโนโลยีสารสนเทศไว้อย่างชัดเจน

ACTION PLAN



1.3 มีนโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล

0 คะแนน	ไม่มีนโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล
0.5 คะแนน	มีนโยบายหรือแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล
1 คะแนน	มีนโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล



1.4 มีการจัดโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศ ของโรงพยาบาลที่เหมาะสม

0 คะแนน	ไม่มี	การแสดงผลโครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของโรงพยาบาลที่เหมาะสม
0.5 คะแนน	มีการแสดงผลโครงสร้าง	หรืออัตรากำลังของหน่วยงานสารสนเทศของโรงพยาบาลที่เหมาะสม
1 คะแนน	มีการแสดงผลโครงสร้างและอัตรากำลัง	ของหน่วยงานสารสนเทศของโรงพยาบาลที่เหมาะสม

1.5 มีการกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล ได้แก่ มาตรฐานข้อมูล มาตรฐานรหัสข้อมูล มาตรฐานการปฏิบัติงาน มาตรฐานความปลอดภัยและความลับของผู้ป่วย มาตรฐานระบบเครือข่ายคอมพิวเตอร์ มาตรฐานทางกายภาพและสภาพแวดล้อม

0 คะแนน	<p>ไม่มีการแสดงผลหลักฐาน ระเบียบหรือมาตรฐานด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล ได้แก่ มาตรฐานข้อมูล มาตรฐานรหัสข้อมูล มาตรฐานการปฏิบัติงาน มาตรฐานความปลอดภัยและความลับของผู้ป่วย มาตรฐานระบบเครือข่ายคอมพิวเตอร์ มาตรฐานทางกายภาพและสภาพแวดล้อม</p>
0.5 คะแนน	<p>มีการแสดงผลหลักฐาน ระเบียบหรือมาตรฐานด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล เช่น มาตรฐานข้อมูล มาตรฐานรหัสข้อมูล มาตรฐานการปฏิบัติงาน มาตรฐานความปลอดภัยและความลับของผู้ป่วย มาตรฐานระบบเครือข่ายคอมพิวเตอร์ มาตรฐานทางกายภาพและสภาพแวดล้อม ไม่น้อยกว่า กึ่งหนึ่ง</p>
1 คะแนน	<p>มีการแสดงผลหลักฐาน ระเบียบหรือมาตรฐานด้านเทคโนโลยีสารสนเทศต่าง ๆ ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล ได้แก่ มาตรฐานข้อมูล มาตรฐานรหัสข้อมูล มาตรฐานการปฏิบัติงาน มาตรฐานความปลอดภัยและความลับของผู้ป่วย มาตรฐานระบบเครือข่ายคอมพิวเตอร์ มาตรฐานทางกายภาพและสภาพแวดล้อม และมีความสมบูรณ์ของหลักฐานของระเบียบหรือมาตรการมาตรฐานด้านเทคโนโลยีสารสนเทศด้านต่าง ๆ</p>

1. โครงสร้างและบทบาท ระบบเทคโนโลยีสารสนเทศ

เอกสารที่ควรนำเสนอประกอบการประเมิน

1. คำสั่งแต่งตั้งทีมดูแลระบบสารสนเทศของโรงพยาบาล
2. แผนแม่บทหรือแผนพัฒนาของโรงพยาบาล
3. นโยบายและแผนการปฏิบัติด้านเทคโนโลยีสารสนเทศของโรงพยาบาล
4. โครงสร้างและอัตรากำลังของหน่วยงานสารสนเทศของโรงพยาบาล
5. ระเบียบหรือมาตรฐานด้านเทคโนโลยีสารสนเทศต่าง ๆ
ที่จำเป็นสอดคล้องกับมาตรฐานของประเทศหรือมาตรฐานสากล ได้แก่
มาตรฐานข้อมูล มาตรฐานรหัสข้อมูล มาตรฐานการปฏิบัติงาน
มาตรฐานความปลอดภัยและความลับของผู้ป่วย มาตรฐานระบบเครือข่ายคอมพิวเตอร์
มาตรฐานทางกายภาพและสภาพแวดล้อม



2. การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

คำอธิบาย : ระบบการจัดการความเสี่ยงที่เริ่มจากการประเมินความเสี่ยงทุกด้านที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศโรงพยาบาล ให้คะแนนความเสี่ยงและจัดลำดับความสำคัญ จัดทำแผนการจัดการความเสี่ยงเป็นลายลักษณ์อักษร มีเลขหน้ากำกับ ประกอบด้วยผลการประเมินความเสี่ยง ยุทธศาสตร์การจัดการความเสี่ยงและแผนปฏิบัติการที่กำหนดระยะเวลาที่จะดำเนินการตามแผนในช่วง 1 ปี เมื่อจบการดำเนินการตามแผนต้องมีการประเมินผลการดำเนินงานและนำผลการประเมินมาปรับปรุงเป็นแผนในรอบปีต่อไป รวมทั้งการจัดการความเสี่ยงที่จะเกิดขึ้นกับผู้ป่วย จากการใช้เทคโนโลยีสารสนเทศด้วย





2.1 มีกระบวนการประเมินและให้คะแนนความเสี่ยงของระบบสารสนเทศ อย่างเป็นระบบ โดยการมีส่วนร่วมของทุกฝ่าย

0 คะแนน	ไม่มีกระบวนการประเมินความเสี่ยงและการให้คะแนนความเสี่ยงและการจัดลำดับความสำคัญ
0.5 คะแนน	มีการประเมินความเสี่ยง แต่ขาดการให้คะแนนความเสี่ยงหรือการจัดลำดับความสำคัญ
1 คะแนน	มีการประเมินความเสี่ยงและการให้คะแนนความเสี่ยงและการจัดลำดับความสำคัญ



2.2 มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบ อย่างชัดเจน

0 คะแนน	ไม่มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบ อย่างชัดเจน
0.5 คะแนน	มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร แต่ขาดการกำหนดกลยุทธ์โครงการหรือระยะเวลาดำเนินการหรือผู้รับผิดชอบ
1 คะแนน	มีแผนจัดการความเสี่ยงเป็นลายลักษณ์อักษร โดยกำหนดกลยุทธ์โครงการ ระยะเวลาดำเนินการ ผู้รับผิดชอบ อย่างชัดเจน



2.3 มีการดำเนินการตามแผนจัดการความเสี่ยง

0 คะแนน	ไม่มีดำเนินการตามแผนจัดการความเสี่ยงตามข้อ 2.2
0.5 คะแนน	มีการดำเนินการตามแผนจัดการความเสี่ยง ตามข้อ 2.2 แต่ไม่เป็นไปตามระยะเวลาที่กำหนดในแผนจัดการความเสี่ยง
1 คะแนน	มีการดำเนินการตามแผนจัดการความเสี่ยง ตามข้อ 2.2 และตามระยะเวลาที่กำหนดในแผนจัดการความเสี่ยง



2.4 มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน

0 คะแนน	ไม่มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน
0.5 คะแนน	มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน แต่ไม่มีการจัดทำเป็นรายงาน
1 คะแนน	มีการติดตาม ประเมินผลการดำเนินการจัดการความเสี่ยง และวิเคราะห์ผลการประเมิน จัดทำเป็นรายงาน



2.5 มีการนำผลการประเมินการดำเนินการจัดการ
ความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น

0 คะแนน	ไม่มีผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น
0.5 คะแนน	มีผลการประเมินการดำเนินการจัดการความเสี่ยง แต่ขาดการนำมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น
1 คะแนน	มีผลการประเมินการดำเนินการจัดการความเสี่ยงมาปรับแผนการจัดการความเสี่ยงให้ดีขึ้น

2. การจัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

เอกสารที่ควรนำเสนอประกอบการประเมิน

1. วิธีการและผลการประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศ
2. แผนยุทธศาสตร์การจัดการความเสี่ยง จัดลำดับความสำคัญตามผลการประเมินความเสี่ยง
3. แผนปฏิบัติการจัดการความเสี่ยงปีปัจจุบัน
4. รายงานผลการประเมินการจัดการความเสี่ยงในรอบปีที่ผ่านมา



3. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ

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





3.1 มีการจัดทำนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบ IT

0 คะแนน	ไม่มีนโยบายด้านความมั่นคงปลอดภัย และระเบียบปฏิบัติสำหรับผู้ใช้ระบบ
0.5 คะแนน	มีนโยบายด้านความมั่นคงปลอดภัยและระเบียบปฏิบัติสำหรับผู้ใช้ระบบ แต่ไม่มีเป็นลายลักษณ์อักษร
1 คะแนน	มีนโยบายด้านความมั่นคงปลอดภัย และระเบียบปฏิบัติสำหรับผู้ใช้ระบบมีเป็นลายลักษณ์อักษร



3.2 มีนโยบายและระเบียบปฏิบัติที่อนุญาตให้เฉพาะผู้ที่รับผิดชอบดูแลรักษาผู้ป่วยในช่วงเวลาปัจจุบันเท่านั้นที่จะเข้าถึงข้อมูลผู้ป่วยรายนั้นได้

0 คะแนน	ไม่มีนโยบายและระเบียบปฏิบัติที่กำหนดห้ามแพทย์หรือพยาบาลเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบปัจจุบัน
0.5 คะแนน	มีนโยบายและระเบียบปฏิบัติที่กำหนดห้ามแพทย์หรือพยาบาลเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบปัจจุบัน แต่ไม่มีเป็นลายลักษณ์อักษร
1 คะแนน	มีนโยบายและระเบียบปฏิบัติที่กำหนดห้ามแพทย์หรือพยาบาลเข้าถึงข้อมูลผู้ป่วยที่ไม่ได้อยู่ในความรับผิดชอบปัจจุบัน มีเป็นลายลักษณ์อักษร



3.3 มีนโยบายและระเบียบปฏิบัติที่ป้องกันความลับผู้ป่วย มิให้รั่วไหลทุกช่องทาง รวมทั้งช่องทาง Social Media ทุกด้าน

0 คะแนน	ไม่มีนโยบายและระเบียบปฏิบัติที่กำหนดการป้องกันความลับผู้ป่วยมิให้รั่วไหล
0.5 คะแนน	มีนโยบายและระเบียบปฏิบัติที่กำหนดการป้องกันความลับผู้ป่วยมิให้รั่วไหล แต่ไม่มีเป็นลายลักษณ์อักษร
1 คะแนน	มีนโยบายและระเบียบปฏิบัติที่กำหนดการป้องกันความลับผู้ป่วยมิให้รั่วไหล มีเป็นลายลักษณ์อักษร



3.4 มีการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ

0 คะแนน	ไม่มีหลักฐานการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ
0.5 คะแนน	มีหลักฐานการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ แต่ไม่ครบ (3.1-3.3)
1 คะแนน	มีหลักฐานการประชาสัมพันธ์นโยบายและระเบียบปฏิบัติให้บุคลากรทุกคนได้รับทราบ (3.1-3.3)



3.5 มีการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ และปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคง ปลอดภัยอย่างเคร่งครัด

0 คะแนน	ไม่มีผลการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับและปฏิบัติตามระเบียบด้านความมั่นคงปลอดภัย
0.5 คะแนน	มีผลการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับ แต่ไม่ปฏิบัติตามระเบียบด้านความมั่นคงปลอดภัย
1 คะแนน	มีผลการตรวจสอบว่าบุคลากรได้รับทราบ เข้าใจ ยอมรับและปฏิบัติตามระเบียบด้านความมั่นคงปลอดภัย



3.6 มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติต่อไป

0 คะแนน	ไม่มีผลการประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติในครั้งถัดไป
0.5 คะแนน	มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติ แต่ไม่ได้นำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติในครั้งถัดไป
1 คะแนน	มีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติและนำผลการประเมินมาปรับกระบวนการบังคับใช้ระเบียบปฏิบัติในครั้งถัดไป

3. การจัดการความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ



เอกสารที่ควรนำเสนอประกอบการประเมิน

1. นโยบายด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศโรงพยาบาล
2. ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่ผู้ใช้ระบบทุกคนต้องปฏิบัติตาม
3. ผลการประเมินการปฏิบัติตามระเบียบปฏิบัติ
4. แนวทางปฏิบัติในการสำรองข้อมูลทุก ๆ ฐานข้อมูล

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

0 คะแนน	ไม่มีผลการวิเคราะห์สถานการณ์ปัจจุบัน และ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร
0.5 คะแนน	มีผลการวิเคราะห์สถานการณ์ปัจจุบัน และ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร แต่ขาดด้านใดด้านหนึ่ง
1 คะแนน	มีผลการวิเคราะห์สถานการณ์ปัจจุบัน และ Gap Analysis ของทรัพยากรด้าน Hardware, Software, Network, บุคลากร



4.2 มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของ ทรัพยากร ด้าน Hardware, Software, Network

0 คะแนน	ไม่มี	มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network
0.5 คะแนน	มี	มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network แต่ขาดด้านใดด้านหนึ่ง
1 คะแนน	มี	มีการจัดทำแผนเพิ่มหรือจัดการศักยภาพของทรัพยากรด้าน Hardware, Software, Network



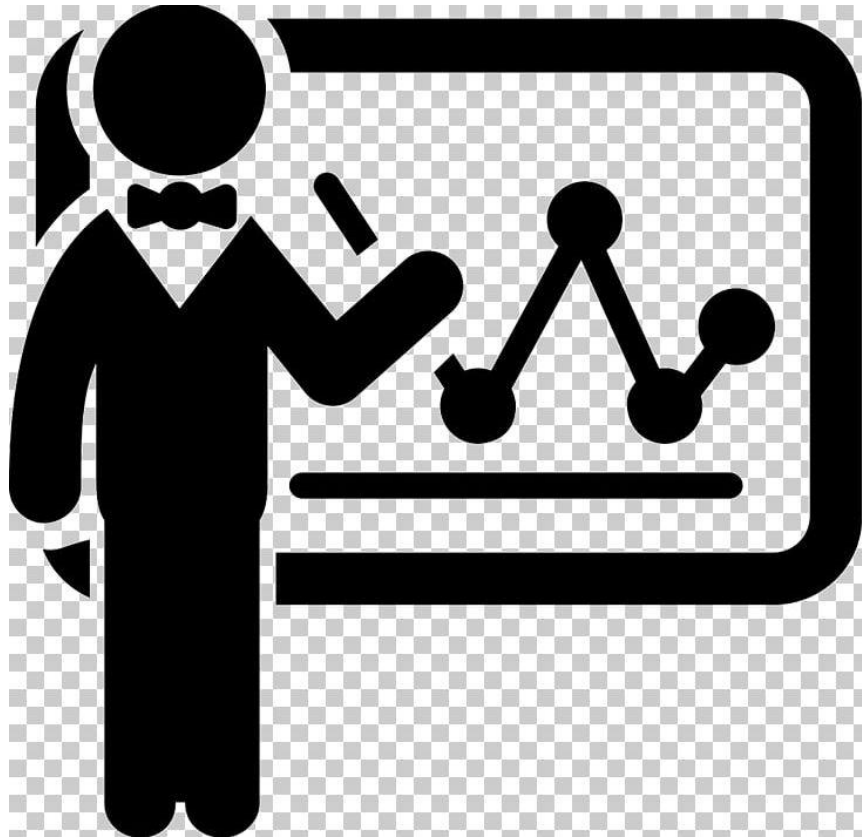
4.3 มีการกำหนดสมรรถนะตามบทบาทหน้าที่ที่จำเป็น (Functional Competency) ของบุคลากรด้าน IT ทุกคน ประเมินสมรรถนะตามบทบาทหน้าที่ และจัดทำแผนเพิ่มสมรรถนะรายบุคคล

0 คะแนน	ไม่มีการกำหนดสมรรถนะตามบทบาทหน้าที่ของบุคลากรด้าน IT ทุกคน ผลการประเมินสมรรถนะตามบทบาทหน้าที่ และแผนการเพิ่มสมรรถนะรายบุคคล
0.5 คะแนน	มีการกำหนดสมรรถนะตามบทบาทหน้าที่ของบุคลากรด้าน IT ทุกคนหรือผลการประเมินสมรรถนะตามบทบาทหน้าที่หรือแผนการเพิ่มสมรรถนะรายบุคคล
1 คะแนน	มีการกำหนดสมรรถนะตามบทบาทหน้าที่ของบุคลากรด้าน IT ทุกคน ผลการประเมินสมรรถนะตามบทบาทหน้าที่ และมีแผนการเพิ่มสมรรถนะรายบุคคล



4.4 มีการดำเนินการตามแผนเพิ่มสมรรถนะและ ศักยภาพ (Hardware, software, network) และ มีการประเมิน วิเคราะห์ผลการดำเนินการตามแผน

0 คะแนน	ไม่มีดำเนินการตามแผนการเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) และ มีการประเมิน วิเคราะห์ผลการดำเนินการตามแผน
0.5 คะแนน	มีการดำเนินการตามแผนการเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) หรือการประเมินหรือ วิเคราะห์ผลการดำเนินการตามแผน
1 คะแนน	มีการดำเนินการตามแผนการเพิ่มสมรรถนะและศักยภาพ (Hardware, software, network) และมีการประเมิน วิเคราะห์ ผลการดำเนินการตามแผน



4.5 มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่ม ศักยภาพให้ดีขึ้น

0 คะแนน	ไม่มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น
0.5 คะแนน	มีการนำผลการวิเคราะห์มาปรับปรุงแผน แต่ไม่มีการปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น หรือขาดอย่างใดอย่างหนึ่ง
1 คะแนน	มีการนำผลการวิเคราะห์มาปรับปรุงแผนเพิ่มศักยภาพให้ดีขึ้น



เอกสารที่ควรนำเสนอประกอบการประเมิน

1. ทะเบียนทรัพยากรในระบบ IT
2. การกำหนดสมรรถนะและการประเมินสมรรถนะบุคลากรในฝ่าย IT
3. แผนการพัฒนาสมรรถนะรายบุคคล
4. แผนการเพิ่มศักยภาพระบบ IT

5. การจัดการห้อง Data Center

คำอธิบาย : Data Center ของโรงพยาบาลได้แก่ที่ตั้งของ SERVER และอุปกรณ์ที่เกี่ยวข้อง เช่นระบบสำรองข้อมูล อุปกรณ์สำรอง Redundant system ระบบรักษาความปลอดภัย เป็นต้น จะต้องมีการจัดการอย่างเหมาะสม โดยระบบสามารถทำงานได้อย่างปลอดภัย และมีประสิทธิภาพ



สถานพยาบาล มีห้อง Data Center

สถานพยาบาล ที่ไม่มีห้อง Data Center

สถานพยาบาล มีห้อง Data Center หมายถึง หน่วยงานที่มีการจัดการห้อง Data Center เป็นสัดส่วน ตามมาตรฐานความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
สถานพยาบาล ที่ไม่มีห้อง Data Center หมายถึง หน่วยงานใช้ระบบ Cloud Server ของหน่วยงานภาครัฐ หรือ ใช้บริการจาก จาก IDC อื่น ๆ หรือ ไม่มีการจัดเก็บข้อมูลด้วยเครื่อง Server

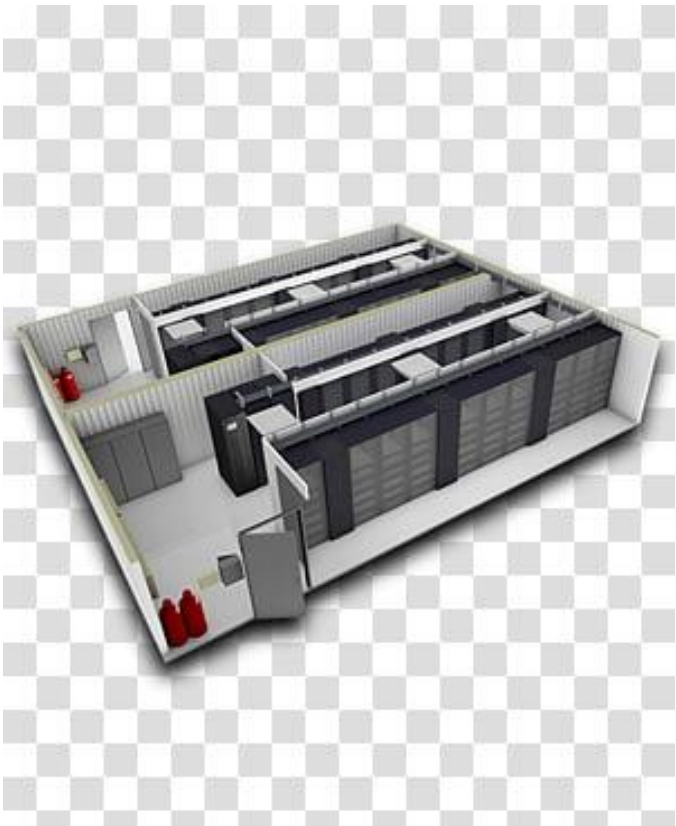
กดบันทึกข้อมูล

หมายเหตุ กรุณาเลือก หากใช้งานครั้งแรก(เลือกครั้งเดียว)



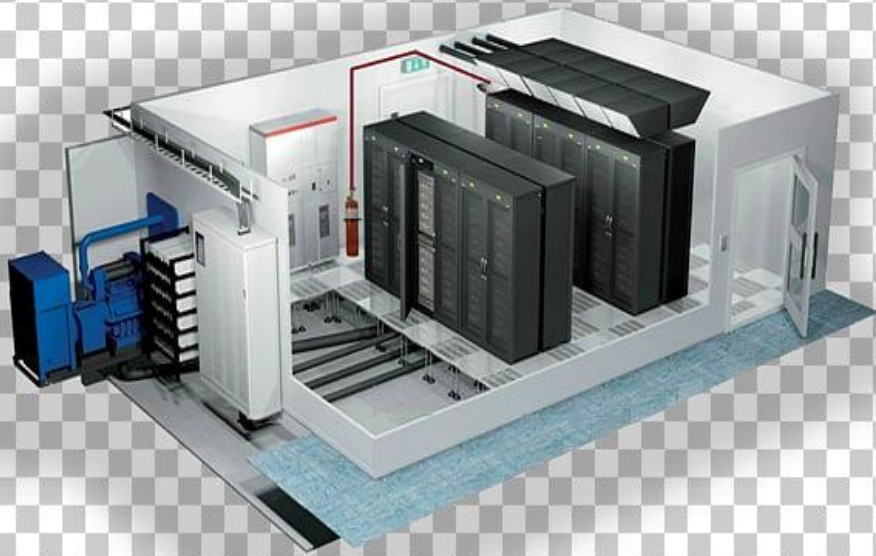
5.1 มีการจัดการ Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัย

0 คะแนน	ไม่มีแนวทางการจัดการห้อง Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัย
0.5 คะแนน	ไม่มีแนวทางการจัดการห้อง Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัยแต่มีการจัดการห้อง Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัย
1 คะแนน	มีแนวทางการจัดการห้อง Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัยและมีการจัดการห้อง Data Center ของโรงพยาบาลให้มีความมั่นคงปลอดภัย



5.2 ห้อง สถานที่ และสิ่งแวดล้อมต้องจัดให้มีความปลอดภัยจากบุคคลภายนอก

0 คะแนน	ไม่มี	การแสดงผลหลักฐานห้อง สถานที่ และสิ่งแวดล้อม ต้องจัดให้มีความปลอดภัย จากบุคคลภายนอก โดยอย่างน้อยมีแผนผังห้อง รูปถ่ายหรือรูปภาพประกอบ
0.5 คะแนน	มี	การแสดงผลหลักฐานห้อง สถานที่ และสิ่งแวดล้อม แต่ไม่มีความปลอดภัย จากบุคคลภายนอก โดยอย่างน้อยมีแผนผังห้อง รูปถ่ายหรือรูปภาพประกอบ
1 คะแนน	มี	การแสดงผลหลักฐานห้อง สถานที่ และสิ่งแวดล้อม ต้องจัดให้มีความปลอดภัย จากบุคคลภายนอก โดยอย่างน้อยมีแผนผังห้อง รูปถ่ายหรือรูปภาพ



5.3 มีระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงและระบบดับเพลิงอัตโนมัติ

0 คะแนน	ไม่มี	การแสดงหลักฐานด้านระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงและระบบดับเพลิงอัตโนมัติ
0.5 คะแนน	มี	การแสดงหลักฐานด้านระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย แต่ขาดเครื่องดับเพลิงหรือระบบดับเพลิงอัตโนมัติ ใดๆอย่างหนึ่ง
1 คะแนน	มี	การแสดงหลักฐานด้านระบบป้องกันอัคคีภัย ได้แก่ ระบบตรวจจับควัน ระบบเตือนภัย เครื่องดับเพลิงและระบบดับเพลิงอัตโนมัติ



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

0 คะแนน	ไม่มี การแสดงหลักฐานด้านการป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server
0.5 คะแนน	ไม่มี/มี การแสดงหลักฐานด้านการป้องกันความเสียหายของข้อมูลและระบบ หรือ ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server ขาดอย่างใดอย่างหนึ่ง
1 คะแนน	มีการแสดงหลักฐานด้านการป้องกันความเสียหายของข้อมูลและระบบ ซึ่งรวมถึง ระบบไฟฟ้าสำรอง (UPS) ระบบ RAID, Redundant Power supply, Redundant Server



5.5 มีการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยงและความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center

0 คะแนน	ไม่มี การวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยงและความคุ้มค่าในการเลือกใช้อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center
0.5 คะแนน	มีการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยง แต่ไม่ได้ นำผลการวิเคราะห์มาวัดความคุ้มค่าในการเลือกใช้ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center
1 คะแนน	มีการวิเคราะห์ความเหมาะสม มาตรฐาน ความเสี่ยงและ นำผลการวิเคราะห์มาวัดความคุ้มค่าในการเลือกใช้ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย ห้อง Data Center



เอกสารที่ควรนำเสนอประกอบการประเมิน

ข้อมูลขนาดห้องและสถานที่ตั้ง ห้อง Data Center (Server Room) รูปภาพภายใน
ด้านหน้าและหลังตู้เก็บเครื่องแม่ข่าย แสดงการจัดระเบียบสายสัญญาณ สายไฟฟ้า สายอื่น ๆ
ทั้งหมด อุปกรณ์ที่สำคัญ เช่น ระบบตรวจจับควัน ระบบวัดอุณหภูมิและความชื้น ระบบ
ดับเพลิง ระบบควบคุมการเข้าออกและระเบียบการควบคุม



Thank
you!

- https://ict.moph.go.th/upload_file/files/3927aa014c6853e7d6fdc02e224e0a60.pdf
- นโยบายและแผนด้านความมั่นคง
- http://ict.hss.moph.go.th/fileupload_doc/2020-09-22-1-20-3292017.pdf
- ความเสี่ยง
- http://ict.hss.moph.go.th/fileupload_doc/2020-09-22-1-20-3292019.pdf

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางการแก้ไข
๕.๓ ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology)						
๕.๓.๑ ทรัพย์สิน ครุภัณฑ์ ระบบปฏิบัติการ ด้านเทคโนโลยี (Hardware, Software)	- ไม่เพียงพอต่อการใช้งาน - ไม่พร้อมใช้งาน	๒	๕	๓๐	ค่อนข้างสูง	- จัดทำแผนคุ้มครองทรัพย์สินตาม ระเบียบพัสดุ - สำรวจ จัดซื้อ/จัดหา ให้พร้อมใช้งาน ตามแผนที่กำหนด - กำหนดแนวทางการควบคุม กำกับ ติดตามประเมินการใช้งาน การเข้ารหัส ในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง - ปรับปรุงระบบการยืม-คืน เมื่อนำ อุปกรณ์ระบบคอมพิวเตอร์ไปใช้นอก สำนักงาน - ประกาศใช้นโยบายและแนวปฏิบัติใน การรักษาความมั่นคงปลอดภัยด้าน สารสนเทศ