แนวทางการดำเนินงาน
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับโรงพยาบาลของรัฐ

พ.ศ. 2567

คำนำ

แนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาลของรัฐฉบับนี้ เป็นผลงานจากความร่วมมือของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งขาติ (สกมช.) และสมาคมเวชสารสนเทศไทย (Thai Medical Informatics Association – TMI) มีวัตถุประสงค์เพื่อให้โรงพยาบาลได้มีแนวทางพัฒนาระบบความมั่นคงปลอดภัยไซเบอร์ให้เกิดขึ้นในโรงพยาบาล ตามกฎหมาย และประมวลแนวทางปฏิบัติที่เกี่ยวข้อง และสามารถยกระดับการพัฒนาให้มีความมั่นคงปลอดภัยเพิ่มขึ้นอย่างต่อเนื่อง

การเรียบเรียงแนวทางนี้ ได้คำนึงถึง บริบทของโรงพยาบาลของรัฐในระดับต่าง ๆ ของประเทศไทย ข้อจำกัดที่ยังมีอยู่ในปัจจุบัน จึงอาจมิได้กำหนดแนวทางไปจนถึง การทำให้เกิดความมันคงปลอดภัยขั้นสูงสุด อย่างไรก็ตาม หากโรงพยาบาลต้องการเริ่มจากขั้นต้น ก็สามารถดำเนินการตามแนวทางฉบับนี้ได้ในระยะแรก จนดำเนินการได้อย่างมั่นคง และสามารถยกระดับของโรงพยาบาลไปสู่ความมั่นคงปลอดภัยใน ระดับที่เหนือกว่าที่กำหนดไว้ในแนวทางฉบับนี้ ก็จะเป็นเรื่องที่เหมาะสมอย่างยิ่ง

แนวทางนี้ถูกเรียบเรียงเป็นครั้งแรกจากคณะทำงานร่วม หากเกิดข้อบกพร่องผิดพลาดประการใด คณะทำงานขอรับผิดทุกประการ และยินดีรับคำชี้แนะเพิ่มเติมจากกัลยาณมิตรที่ต้องการช่วยพัฒนา โดยจะได้นำข้อเสนอแนะที่ได้มาปรับปรุงแนวทางให้ดียิ่งขึ้นในรุ่นต่อไป

นายแพทย์ วรรษา เปาอินทร์

พลอากาศตรี จเด็ด คูหะก้องกิจ

สารบัญ

สารบัญ (ต่อ)

บทที่ 1 การจัดตั้งคณะทำงาน

คณะทำงานเพื่อดำเนินการให้เกิดความมั่นคงปลอดภัยไซเบอร์ในโรงพยาบาล มีหน้าที่

1. สร้างระบบความมั่นคงปลอดภัยไซเบอร์ให้เกิดขึ้นในโรงพยาบาล
2. ดูแลรักษาระบบให้มั่นคงต่อเนื่อง
3. จัดทำรายงานเพื่อส่งให้หน่วยงานต้นสังกัด และหน่วยงานที่กำกับควบคุม
4. ประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้อง

คณะทำงานในโรงพยาบาลแต่ละระดับ จะมีจำนวนคนไม่เท่ากัน โรงพยาบาลขนาดเล็ก อาจมีคนในคณะทำงาน 3-5 คน โรงพยาบาลขนาดใหญ่ อาจมีคนในคณะทำงาน 10-20 คน คณะทำงานควรมีองค์ประกอบที่สำคัญดังนี้

1. ผู้อำนวยการโรงพยาบาล หรือ รองผู้อำนวยการด้านสารสนเทศ (Chief Information Officer)*
2. หัวหน้าฝ่ายพัฒนาคุณภาพโรงพยาบาล
3. ประธานองค์กรแพทย์
4. หัวหน้าฝ่ายการพยาบาล
5. หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ
6. ตัวแทนหน่วยงานฝ่ายปฏิบัติงานแผนกอื่น ๆ ตามความเหมาะสม

ในช่วงเวลาเริ่มสร้างให้เกิดระบบความมั่นคงปลอดภัยไซเบอร์ให้เกิดขึ้นในโรงพยาบาล ผู้อำนวยการโรงพยาบาลควรเป็นประธานคณะทำงาน, ผู้บริหารสารสนเทศ (Chief Information Officer – CIO) ควรเป็นรองประธาน และหัวหน้าฝ่ายเทคโนโลยีสารสนเทศควรเป็นฝ่ายเลขานุการ

แต่เมื่อระบบเกิดขึ้นแล้ว ควรปรับตำแหน่งรองประธานให้เป็น ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer) และฝ่ายเลขานุการให้เป็นหัวหน้าฝ่ายความมั่นคงปลอดภัยสารสนเทศ หรือเจ้าหน้าที่ความมั่นคงปลอดภัยสารสนเทศ โดยบุคคลทั้งสองตำแหน่งนี้ ต้องมีความเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ

* Chief Information Officer (CIO) จะเป็นผู้เริ่มวางระบบความมั่นคงปลอดภัยให้เกิดขึ้นในโรงพยาบาล แต่เมื่อเกิดระบบขึ้นแล้ว จะต้องมี Chief Information Security Officer (CISO) ทำหน้าที่บริหารจัดการความมั่นคง โดยเป็นอิสระจากงานด้านการปฏิบัติการเทคโนโลยีสารสนเทศ

บทที่ 2 การจัดทำแผนปฏิบัติการสร้างระบบความมั่นคงปลอดภัยไซเบอร์ให้เกิดขึ้น

เมื่อจัดตั้งคณะเพื่อดำเนินการให้เกิดความมั่นคงปลอดภัยไซเบอร์ในโรงพยาบาลแล้ว ควรวางแผนปฏิบัติการสร้างระบบระบบความมั่นคงปลอดภัยไซเบอร์ให้เกิดขึ้น โดยกำหนดกิจกรรมที่ต้องดำเนินการตามลำดับ รวมถึงช่วงเวลาที่ต้องใช้ในการดำเนินกิจกรรมนั้น ๆ โดยอาจจัดทำในรูปแบบแผนผังกิจกรรม (Gantt chart) ดังตัวอย่างในตารางต่อไปนี้

กิจกรรม	WEEK 1	WEEK 2	WEEK 3	WEEK 4	WEEK 5	WEEK 6	WEEK 7	WEEK 8	WEEK 9	WEEK 10	WEEK 11	WEEK 12
1. การจัดตั้งคณะทำงาน												
2. การจัดทำแผนปฏิบัติการ												
3. การจัดทำแผนการตรวจสอบ												
4. การประกาศนโยบาย												
5. การจัดการความเสี่ยง												
6. การทำให้ระบบแข็งแกร่ง												
7. การสร้างมาตรการที่จำเป็น												
8. การจัดทำรายงาน												
9. การดูแลรักษาระบบต่อเนื่อง												

เมื่อเริ่มดำเนินการตามแผนปฏิบัติการแล้ว คณะทำงาน ควรมีการประชุมติดตามความก้าวหน้าตามแผนปฏิบัติการดังกล่าวทุกสัปดาห์ เพื่อให้ได้รับทราบ ผลการดำเนินการ ปัญหาและอุปสรรคต่าง ๆ ที่อาจเกิดขึ้น เพื่อจะได้ช่วยกันแก้ปัญหา และ ทำให้มั่นใจได้ว่า กิจกรรมการสร้างระบบ จะดำเนินการไปได้อย่างราบรื่น และแก้ไขปัญหาอุปสรรคได้อย่างทันเวลา ไม่กระทบต่อผลสำเร็จของโครงการ และไม่ทำให้การดำเนินงานเกิดผลสำเร็จล่าช้าจนเกินควร

2.1 การจัดทำแผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

คณะทำงาน มีหน้าที่จัดทำแผนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ดำเนินการตามแผนและส่งผลสรุปรายงานการ ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานปลัดกระทรวงสาธารณสุข (กรณีโรงพยาบาลใดได้รับการแจ้งให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามประกาศมาตรา 49 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ให้ส่งผลสรุปดังกล่าวให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ด้วย โดยมีองค์ประกอบดังนี้

1. กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

2. บริการที่สำคัญที่โรงพยาบาลให้บริการ ตามผลการวิเคราะห์ในข้อ 1

3. ผลการดำเนินการตามกฎหมายที่เกี่ยวข้อง และการดำเนินการตามประมวลแนวทางปฏิบัติของ สกมช.

2.2 การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis -BIA)

การวิเคราะห์ผลกระทบทางธุรกิจของโรงพยาบาล เป็นกระบวนการที่ใช้ในการประเมินผลกระทบที่อาจเกิดขึ้นกับโรงพยาบาล ในกรณีเกิดภัยความเสี่ยง (risk) หรือสถานการณ์ฉุกเฉินที่อาจเกิดขึ้น เช่น ภัยพิบัติธรรมชาติ ไฟไหม้ ภัยความเสี่ยงด้านความปลอดภัยของข้อมูล ฯลฯ

วัตถุประสงค์หลักของ BIA คือการให้ข้อมูลที่ชัดเจนเกี่ยวกับการสำรวจโรงพยาบาล การแยกแยะกระบวนการที่เกี่ยวข้องและการพิจารณาผลกระทบที่อาจเกิดขึ้นในกรณีที่โรงพยาบาลประสบภัย ซึ่งสามารถช่วยให้โรงพยาบาล สามารถกำหนดยุทธวิธีในการดำเนินธุรกิจต่อไปในสถานการณ์ฉุกเฉินได้มากขึ้น และให้การสนับสนุนในกระบวนการต่าง ๆ เช่น วางแผนความต่อเนื่อง (business continuity planning) และวางแผนกู้คืน (disaster recovery planning) โดยการทำ BIA จะช่วยให้ผู้บริหารและทีมงานในโรงพยาบาลเข้าใจถึงความสำคัญและความเสี่ยงในกระบวนการที่สำคัญของโรงพยาบาล

องค์ประกอบที่สำคัญในกระบวนการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) ประกอบด้วย

1. การระบุระบบงานที่สำคัญของโรงพยาบาล

2. การระบุความเสี่ยงและสาเหตุ การพิจารณาความเสี่ยงที่อาจเกิดขึ้นในระบบงานต่าง ๆ และการระบุสาเหตุของความเสี่ยงเหล่านี้ เช่น ภัยพิบัติธรรมชาติ สูญเสียข้อมูล การหยุดชะงักในกระบวนการรักษาผู้ป่วย ฯลฯ

3. การประเมินผลกระทบ การทำความเข้าใจเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับกระบวนการที่สำคัญหากภัยความเสี่ยงเกิดขึ้น เช่น ความล่าช้าในการรักษาผู้ป่วย เกิดอันตรายต่อชีวิตและทรัพย์สิน ค่าของความเสียหายทางการเงิน (financial loss) ค่าใช้จ่ายในการซ่อมแซม ฯลฯ

4. การกำหนดเวลาก่อนและหลังภัยความเสี่ยง การตรวจสอบและทำความเข้าใจถึงระยะเวลาที่สำคัญในกระบวนการที่จะต้องก่อนและหลังภัยความเสี่ยงที่เกิดขึ้น เพื่อให้ทราบถึงความเคลื่อนไหวที่อาจเกิดขึ้น และกำหนดเวลาที่จำเป็นในการซ่อมแซมหรือนำกลับมาทำงานให้กับกระบวนการเหล่านั้น

5. การระบุและจัดการแนวทางความเสี่ยง การสำรวจและการพิจารณาความเสี่ยงต่าง ๆ ที่อาจเกิดขึ้นในกระบวนการและเตรียมความพร้อมในกรณีภัยความเสี่ยงเกิดขึ้น และการวางแผนการจัดการความเสี่ยงในอนาคต

การวิเคราะห์ผลกระทบทางธุรกิจหากเกิดภัยพิบัติไซเบอร์ต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาล อาจดำเนินการตามตัวอย่างตารางด้านล่างนี้

ตารางวิเคราะห์ผลกระทบทางธุรกิจหากเกิดภัยพิบัติไซเบอร์ต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

ระบบงาน	ความสำคัญ (สูง ปานกลาง ต่ำ)	ความเสียหายเมื่อเกิดภัยพิบัติที่ทำให้ไม่สามารถให้บริการระบบได้
1. ระบบ Hospital Information System (HIS)	สูง	ระบบงานตรวจรักษาผู้ป่วยนอกหยุดชะงัก การให้บริการผู้ป่วยที่มาตรวจช้าลงอย่างมาก กระทบต่อชีวิตและสุขภาพประชาชน
2. ระบบบริการภาพ X-Rays (PACS)	ปานกลาง	แพทย์ไม่สามารถเรียกดูภาพเอ็กซเรย์เดิมที่ผู้ป่วยเคยตรวจไว้ได้ อาจกระทบต่อคุณภาพการวินิจฉัยโรคและการรักษาผู้ป่วย
3. ระบบ Laboratory Information System (LIS)	ปานกลาง	แพทย์ไม่สามารถเรียกดูผลการตรวจทางห้องปฏิบัติการของผู้ป่วย อาจกระทบต่อคุณภาพการวินิจฉัยโรคและการรักษาผู้ป่วย
4. ระบบ Document Scan ของงานเวชระเบียน	ปานกลาง	ไม่สามารถเรียกดูภาพเอกสารเวชระเบียนที่ scan เก็บไว้ได้ อาจกระทบต่อคุณภาพการวินิจฉัยโรคและการรักษาผู้ป่วย
5. ระบบเชื่อมต่อข้อมูลจากเครื่องวัดความดันโลหิตเข้าสู่ระบบ HIS	ต่ำ	ไม่สามารถดึงข้อมูลจากเครื่องเข้าสู่ระบบ HIS ได้ เจ้าหน้าที่ต้องป้อนข้อมูลเข้าไปเอง อาจเกิดความผิดพลาดของข้อมูลได้ เกิดความล่าช้าของการให้บริการ
6. ระบบหน้าจอแสดงคิวอัตโนมัติ	ต่ำ	ไม่สามารถแสดงคิวผ่านหน้าจอให้ผู้ป่วยได้เห็นคิวได้ เจ้าหน้าที่ต้องดำเนินการเอง อาจเกิดความล่าช้าของการให้บริการ

บทที่ 3 การประกาศนโยบาย มาตรฐานการปฏิบัติงาน ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ และการสร้างความตระหนักรู้

3.1 การจัดทำนโยบาย มาตรฐานการปฏิบัติงานและ ระเบียบปฏิบัติ

นโยบายด้านความมั่นคงปลอดภัย (Security Policy) เป็นแนวทางที่ผู้บริหารระดับสูงกำหนดทิศทางการดำเนินงานเพื่อให้มั่นใจว่า ระบบเทคโนโลยีสารสนเทศโรงพยาบาลจะมีความมั่นคงปลอดภัย ข้อความในประกาศนโยบายฉบับนี้จึงเป็นการแสดงเจตจำนงค์ให้ทุกฝ่ายที่เกี่ยวข้องกับโรงพยาบาล ไม่ว่าจะเป็นผู้ป่วย ญาติผู้ป่วย เจ้าหน้าที่ทุกฝ่ายในโรงพยาบาล ตลอดจนคู่สัญญาภายนอกของโรงพยาบาลได้รับรู้แนวทางและจุดยืนของโรงพยาบาล

ตัวอย่าง ข้อความที่อาจจะประกาศไว้ในนโยบายด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลได้แก่

- โรงพยาบาล จะดำเนินการจัดการเพื่อป้องกันความลับและความเป็นส่วนตัวของผู้ป่วยอย่างเคร่งครัด

- โรงพยาบาลมีนโยบายใช้ซอฟท์แวร์ที่ไม่ละเมิดลิขสิทธิ์เท่านั้น

- การใช้ทรัพยากรเทคโนโลยีสารสนเทศของโรงพยาบาล ต้องเป็นไปเพื่อการดำเนินกิจกรรมตามพันธกิจและภารกิจของโรงพยาบาลเท่านั้น

มาตรฐานการปฏิบัติงาน (Standard Operation Procedures) คือ แนวทางการทำงานที่กำหนดไว้ให้ผู้ที่ต้องปฏิบัติ ทำงานตามขั้นตอนและแนวทางที่ได้กำหนดไว้ อย่างเคร่งครัด โดยต้องทำเป็นลายลักษณ์อักษรและสื่อสารไปยังผู้ปฏิบัติให้เข้าใจและปฏิบัติตาม โดยผู้ที่ไม่ปฏิบัติตามจะถูกประเมินว่าบกพร่องในหน้าที่ของตนเอง

ตัวอย่าง มาตรฐานการปฏิบัติงาน ได้แก่

-มาตรฐานการปฏิบัติงาน เรื่อง การสำรองข้อมูลจากฐานข้อมูลของโรงพยาบาล

- มาตรฐานการปฏิบัติงาน เรื่อง การใช้ LINE ส่งข้อมูลผู้ป่วยเพื่อการปรึกษาหารือในกลุ่มผู้รักษา

- มาตรฐานการปฏิบัติงาน เรื่อง การจัดการชื่อผู้ใช้ และรหัสผ่านในการเข้าสู่ระบบสารสนเทศ

ระเบียบปฏิบัติเพื่อความมั่นคงปลอดภัย (Security Regulations) เป็นข้อกำหนดที่ให้เจ้าหน้าที่ทุกคนต้องปฏิบัติตาม เพื่อให้มั่นใจว่า ระบบเทคโนโลยีสารสนเทศโรงพยาบาลจะมีความมั่นคงปลอดภัย ข้อความในประกาศระเบียบปฏิบัติจึงเป็นสิ่งที่เจ้าหน้าที่ทุกคนต้องรับรู้ และปฏิบัติตามโดยเคร่งครัด โดยหากไม่ปฏิบัติตามควรมีมาตรฐานตักเตือนหรือลงโทษตามสมควร

ตัวอย่าง ข้อความที่อาจจะประกาศไว้ในระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลได้แก่

- (เจ้าหน้าที่ทุกคน) ต้องเก็บรักษารหัสผ่านของตนเองไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น
- ห้ามใช้คอมพิวเตอร์ของโรงพยาบาลเพื่อความบันเทิง เช่น ดูหนัง ฟังเพลง เล่นเกมส์ ฯลฯ
- ห้ามติดตั้งโปรแกรมใด ๆ เพิ่มเติมลงในเครื่องคอมพิวเตอร์ของโรงพยาบาล หากมีความจำเป็นให้ขออนุมัติจากผู้อำนวยการหรือผู้ที่ได้รับมอบหมายหน้าที่จากผู้อำนวยการเท่านั้น

ระเบียบปฏิบัติเพื่อความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศโรงพยาบาลสามารถแบ่งกลุ่มตามลักษณะผู้ใช้ได้ 3 กลุ่มดังนี้

1. ระเบียบปฏิบัติสำหรับผู้บริหาร (ระดับสูง ระดับกลาง ระดับต้น)
2. ระเบียบปฏิบัติสำหรับผู้ดูแลระบบเทคโนโลยีสารสนเทศ
3. ระเบียบปฏิบัติสำหรับผู้ใช้งานระบบทุกคน

ระเบียบปฏิบัติสำหรับผู้ใช้งานระบบทุกคน เป็นระเบียบที่สำคัญที่สุด เพราะต้องบังคับใช้กับบุคคลหมู่มาก จึงต้องเขียนโดยใช้ข้อความที่ชัดเจน ไม่กำกวม เข้าใจได้ง่าย ไม่ตีความบิดเบือนเป็นอย่างอื่นได้

นโยบาย มาตรฐานการปฏิบัติงาน และระเบียบปฏิบัติ ต้องจัดทำเป็นประกาศของโรงพยาบาล โดยผู้อำนวยการลงนามและประกาศให้ผู้ที่เกี่ยวข้องทุกคนได้รับรู้โดยทั่วกัน โดยเมื่อประกาศใช้งานไปแล้วควรมีการทบทวนเป็นประจำทุกปี หรือสามารถทบทวนและปรับปรุงแก้ไขให้ทันสมัยหรือเหมาะสมต่อสถานการณ์ในอนาคตได้ต่อไป

3.2 การประชาสัมพันธ์นโยบายและระเบียบปฏิบัติไปสู่ผู้ใช้ระบบทุกคน (การสร้างความตระหนักรู้)

เมื่อมีการประกาศนโยบายและระเบียบปฏิบัติออกมาแล้ว ต้องมีการประชาสัมพันธ์ให้มั่นใจว่า ผู้ใช้ระบบเทคโนโลยีสารสนเทศโรงพยาบาลทุกคนตลอดจนคู่สัญญาภายนอกของโรงพยาบาล ได้รับรู้นโยบายและระเบียบปฏิบัติฉบับนี้ กิจกรรมประชาสัมพันธ์เป็นกิจกรรมที่สำคัญมาก เพราะการประกาศเรื่องราวใด ๆในโรงพยาบาลตามช่องทางปกติมักจะไม่สามารถสื่อสารไปสู่บุคลากรหมู่มากของโรงพยาบาลได้ โรงพยาบาลหลายแห่งใช้ช่องทางเครือข่ายภายใน (Intranet) เพื่อนำประกาศต่าง ๆไปใส่ไว้ แต่เรามักจะพบว่า เจ้าหน้าที่โรงพยาบาลส่วนใหญ่จะไม่สนใจอ่านประกาศต่าง ๆเหล่านั้น ดังนั้น หากนำระเบียบปฏิบัติที่สำคัญนี้ไปประกาศไว้ในช่องทางปกติ เจ้าหน้าที่ส่วนใหญ่จะยังคงไม่รับรู้ว่ามีระเบียบนี้ให้ปฏิบัติตาม

การประชาสัมพันธ์ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสำหรับผู้ใช้งานระบบทุกคน ควรใช้ช่องทางประชาสัมพันธ์หลายช่องทาง โดยช่องทางประชาสัมพันธ์ที่อาจเลือกใช้ ได้แก่

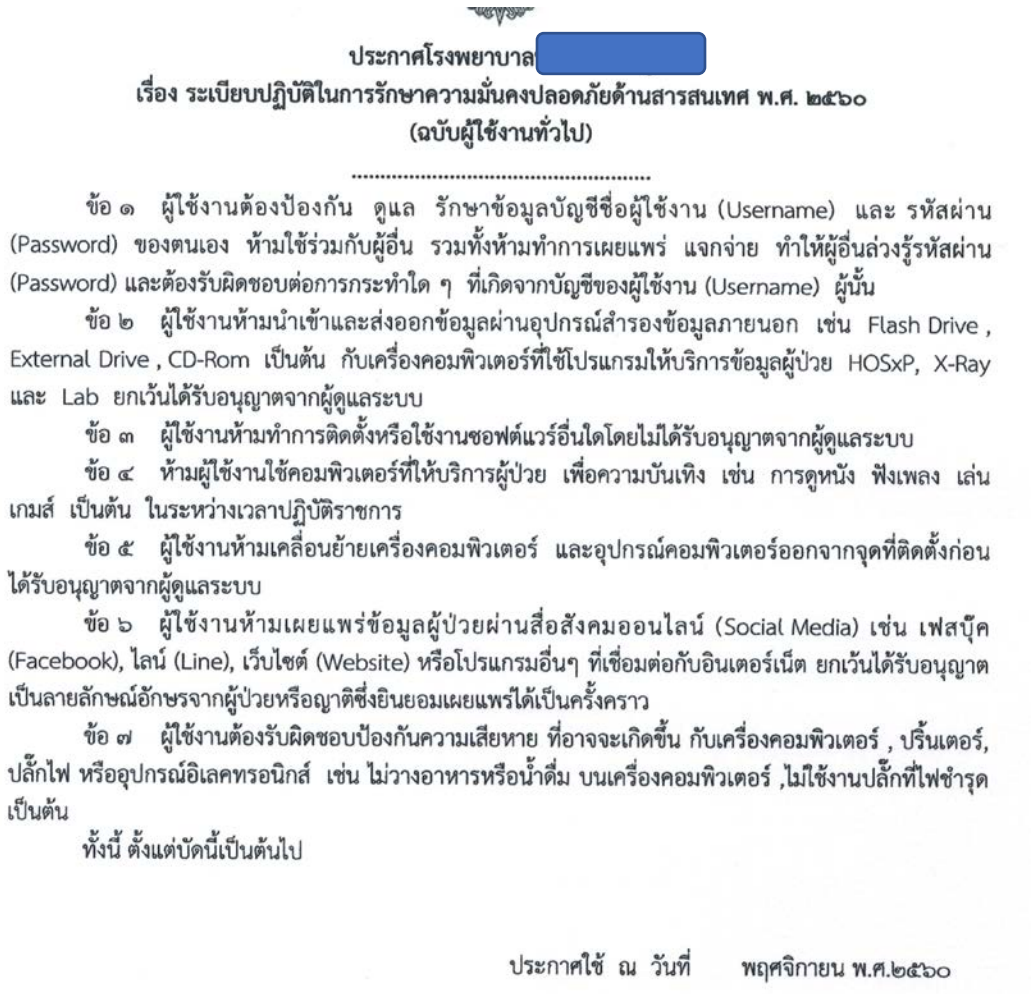
1. ประกาศตามช่องทางประชาสัมพันธ์ปกติของโรงพยาบาล เช่น บอร์ดติดประกาศ Intranet ฯลฯ

2. จัดทำเป็นโปสเตอร์ ทำไปติดไว้ในสถานที่ที่เจ้าหน้าที่ของโรงพยาบาลมองเห็นได้โดยง่าย

3. จัดอบรมเจ้าหน้าที่ นำเสนอระเบียบปฏิบัติ เปิดโอกาสให้ซักถาม อภิปรายร่วมกัน

4. มอบหมายให้หัวหน้าหน่วยงาน นำระเบียบไปแจ้งในที่ประชุมหน่วยงานให้เจ้าหน้าที่ทุกคนทราบ

ในกรณีที่ ระเบียบปฏิบัติสำหรับผู้ใช้งานระบบทุกคน มีข้อปฏิบัติมากเกินกว่า 1 หน้ากระดาษ เช่น มีข้อปฏิบัติ 30-50 ข้อ ควรคัดเลือกระเบียบปฏิบัติที่สำคัญที่สุด มาจัดทำเป็นหน้าเดียวดังตัวอย่างในภาพที่ 3.1



ประกาศโรงพยาบาล[redacted]
เรื่อง ระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐
(ฉบับผู้ใช้งานทั่วไป)

ข้อ ๑ ผู้ใช้งานต้องป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใด ๆ ที่เกิดจากบัญชีของผู้ใช้งาน (Username) ผู้นั้น

ข้อ ๒ ผู้ใช้งานห้ามนำเข้าและส่งออกข้อมูลผ่านอุปกรณ์สำรองข้อมูลภายนอก เช่น Flash Drive , External Drive , CD-Rom เป็นต้น กับเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมให้บริการข้อมูลผู้ป่วย HOSxP, X-Ray และ Lab ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๓ ผู้ใช้งานห้ามทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๔ ห้ามผู้ใช้งานใช้คอมพิวเตอร์ที่ให้บริการผู้ป่วย เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เล่นเกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๕ ผู้ใช้งานห้ามเคลื่อนย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ออกจากจุดที่ติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๖ ผู้ใช้งานห้ามเผยแพร่ข้อมูลผู้ป่วยผ่านสื่อสังคมออนไลน์ (Social Media) เช่น เฟสบุ๊ค (Facebook), ไลน์ (Line), เว็บไซต์ (Website) หรือโปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วยหรือญาติซึ่งยินยอมเผยแพร่ได้เป็นครั้งคราว

ข้อ ๗ ผู้ใช้งานต้องรับผิดชอบป้องกันความเสียหาย ที่อาจจะเกิดขึ้น กับเครื่องคอมพิวเตอร์ , ปริ้นเตอร์, ปลั๊กไฟ หรืออุปกรณ์อิเลคทรอนิกส์ เช่น ไม่วางอาหารหรือน้ำดื่ม บนเครื่องคอมพิวเตอร์ ,ไม่ใช้งานปลั๊กที่ไฟชำรุด เป็นต้น

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศใช้ ณ วันที่ พฤศจิกายน พ.ศ.๒๕๖๐

ภาพที่ 3.1 ตัวอย่าง ระเบียบปฏิบัติฉบับคัดเลือกข้อปฏิบัติให้เหลือเนื้อหาอยู่ในหน้าเดียว

3.3 การประเมินความรับรู้ระเบียบปฏิบัติของผู้ใช้ระบบทุกคน

เมื่อประชาสัมพันธ์ระเบียบปฏิบัติไปสู่ผู้ใช้ระบบแล้ว ต้องมีกระบวนการประเมินความรับรู้และเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน เพื่อให้ทราบว่า การประชาสัมพันธ์ระเบียบนั้นได้ผลมากน้อยเพียงใด โดยก่อนการประเมินจะต้องรวบรวมข้อมูลจากผู้ดูแลระบบมาให้ครบถ้วนเสียก่อนว่าผู้ใช้งานระบบมีทั้งหมดกี่คน ทำงานอยู่ในหน่วยงานใดบ้าง เพื่อจะได้ดำเนินการประเมินได้ครบทุกคน

วิธีการประเมินความรับรู้ระเบียบปฏิบัติทำได้หลายวิธี เช่น การให้ตอบแบบสอบถามหรือแบบประเมินตนเอง การสัมภาษณ์ หรือ การให้หัวหน้าหน่วยงานเป็นผู้ประเมินลูกน้องในหน่วยงานแต่ละหน่วย เมื่อประเมินความรับรู้เสร็จแล้ว ควรจัดทำรายการสรุปผลการประเมินดังตัวอย่างต่อไปนี้

รายงานการประเมินความรับรู้ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ..... ครั้งที่ 1/2566

จำนวนผู้ใช้งานระบบทั้งสิ้น 500 คน ดำเนินการประเมิน 499 คน คิดเป็นร้อยละ 99.80

การรับรู้ระเบียบ

ข้อที่ 1	รู้ 400 คน ไม่รู้ 99 คน	การรับรู้คิดเป็นร้อยละ 80.16
ข้อที่ 2	รู้ 450 คน ไม่รู้ 49 คน	การรับรู้คิดเป็นร้อยละ 90.18
ข้อที่ 3	รู้ 420 คน ไม่รู้ 79 คน	การรับรู้คิดเป็นร้อยละ 84.17
ข้อที่ 4	รู้ 350 คน ไม่รู้ 149 คน	การรับรู้คิดเป็นร้อยละ 70.14

(รายงานผลจนครบทุกข้อ.....)

<u>สรุปผลการประเมิน</u>

ระเบียบข้อที่รับรู้มากที่สุดคือข้อที่ 2 ข้อที่ไม่รับรู้มากที่สุดคือข้อที่ 4

สาเหตุที่ไม่รู้ระเบียบ เป็นเพราะไม่ได้อ่านโดยละเอียด อ่านแล้วจำไม่ได้ ขาดสมาธิตอนเข้ารับการอบรม หรือ เข้ารับการอบรมไม่ครบทุกหัวข้อ

<u>เสนอแนะแนวทางแก้ไข</u>

เพิ่มการให้ความรู้แก่บุคลากรที่ยังขาดความรู้ด้านระเบียบปฏิบัติ โดยกำหนดเป้าหมายให้การรับรู้ทุกหัวข้อ มีสัดส่วนการรับรู้ไม่ต่ำกว่า ร้อยละ 95

3.4 การประเมินความเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน

เมื่อประเมินความรับรู้แล้ว ต้องมีกระบวนการประเมินความเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคนด้วย เพื่อให้ทราบว่า ผู้ใช้ระบบเข้าใจระเบียบแต่ละข้ออย่างถูกต้องหรือไม่ เพราะบางครั้ง ผู้ใช้อาจจะเข้าใจความหมายของระเบียบปฏิบัติแต่ละข้อไม่ถูกต้อง

วิธีการประเมินความเข้าใจระเบียบปฏิบัติทำได้หลายวิธี เช่น การให้ตอบแบบสอบถามหรือแบบประเมินตนเอง การสัมภาษณ์ หรือ การให้หัวหน้าหน่วยงานเป็นผู้ประเมินลูกน้องในหน่วยงานแต่ละหน่วย เมื่อประเมินความเข้าใจเสร็จแล้ว ควรจัดทำรายการสรุปผลการประเมินดังตัวอย่างต่อไปนี้

รายงานการประเมินความเข้าใจระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ..... ครั้งที่ 1/2566

จำนวนผู้ใช้งานระบบทั้งสิ้น 500 คน ดำเนินการประเมิน 500 คน คิดเป็นร้อยละ 100

ความเข้าใจระเบียบ

ข้อที่ 1 เข้าใจ 400 คน ไม่เข้าใจ 99 คน ความเข้าใจคิดเป็นร้อยละ 80.16

ข้อที่ 2 เข้าใจ 450 คน ไม่เข้าใจ 49 คน ความเข้าใจคิดเป็นร้อยละ 90.18

ข้อที่ 3 เข้าใจ 420 คน ไม่เข้าใจ 79 คน ความเข้าใจคิดเป็นร้อยละ 84.17

ข้อที่ 4 เข้าใจ 350 คน ไม่เข้าใจ 149 คน ความเข้าใจคิดเป็นร้อยละ 70.14

(รายงานผลจนครบทุกข้อ.....)

<u>สรุปผลการประเมิน</u>

ระเบียบข้อที่เข้าใจมากที่สุดคือข้อที่ 2 ข้อที่ไม่เข้าใจมากที่สุดคือข้อที่ 4

สาเหตุที่ไม่เข้าใจระเบียบ เป็นเพราะอ่านไม่รู้เรื่อง ไม่เข้าใจศัพท์ที่ใช้ ความหมายกำกวม

<u>เสนอแนะแนวทางแก้ไข</u>

ปรับปรุงแก้ไขข้อความที่ทำให้อ่านไม่รู้เรื่อง เพิ่มการอธิบายแก่บุคลากรที่ยังไม่เข้าใจระเบียบปฏิบัติ โดยกำหนดเป้าหมายให้ความเข้าใจทุกหัวข้อ มีสัดส่วนความเข้าใจไม่ต่ำกว่า ร้อยละ 95

3.5 การเพิ่มความรับรู้และเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน

ถ้าผลการประเมินการรับรู้และความเข้าใจระเบียบปฏิบัติของผู้ใช้ระบบทุกคน ยังไม่เป็นที่น่าพอใจ ต้องพิจารณาว่าสาเหตุที่ทำให้ผู้ใช้ระบบไม่รับรู้หรือไม่เข้าใจระเบียบเกิดจากอะไร เพื่อจะได้ดำเนินการแก้ไขให้ถูกทาง เช่น ระเบียบที่ประกาศใช้ไปแล้วมีบางข้อที่ผู้ใช้อ่านไม่รู้เรื่อง ก็ควรปรับปรุงข้อความให้อ่านแล้วเข้าใจได้โดยง่าย หรือ ผู้ใช้ระบบจำระเบียบไม่ได้เพราะการอบรมมีเนื้อหามากเกินไป ก็ควรปรับปรุงวิธีการอบรมให้ดีขึ้นกว่าเดิม

การเพิ่มความรับรู้และเข้าใจระเบียบปฏิบัติ ทำได้หลายวิธี เช่น การให้ความรู้ซ้ำหลายๆครั้ง เปลี่ยนช่องทางการให้ข้อมูล หรือเพิ่มช่องทางการให้ข้อมูล กำหนดมาตรการให้รางวัลแก่ผู้ที่สนใจและรับรู้ระเบียบได้อย่างดี ฯลฯ

3.6 การประเมินการปฏิบัติตามระเบียบปฏิบัติของผู้ใช้ระบบทุกคน

เมื่อมั่นใจว่าผู้ใช้ระบบทุกคน มีความรู้และความเข้าใจระเบียบปฏิบัติเป็นอย่างดีแล้ว ก็ควรติดตามประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้วย เพราะถึงแม้จะมีความรู้และความเข้าใจเรื่องระเบียบแล้ว แต่บางคนก็ยังคงไม่ปฏิบัติตามระเบียบ ทีมงานพัฒนาคุณภาพจึงต้องสร้างระบบตรวจสอบประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้วย

วิธีการประเมินผลการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบสารสนเทศของโรงพยาบาล สามารถดำเนินการได้หลายวิธี ได้แก่

1. แบบประเมินตนเอง ให้ผู้ใช้ระบบตอบคำถามว่า ระเบียบข้อใดบ้างที่ปฏิบัติตาม ระเบียบข้อใดที่ไม่ปฏิบัติ สาเหตุที่ทำให้ไม่ปฏิบัติตามระเบียบคืออะไร ฯลฯ การให้ตอบแบบประเมินตนเองนี้ มีข้อดีตรงที่ทำได้โดยง่าย และใช้ประเมินการปฏิบัติตามระเบียบข้อที่ไม่สามารถประเมินด้วยวิธีอื่นได้ แต่ข้อเสียของการประเมินด้วยวิธีนี้คือ การที่ผู้ประเมินตนเองอาจประเมินไม่ตรงตามการปฏิบัติจริง

2. การสังเกตโดยตรงจากผู้ประเมิน วิธีนี้ผู้ประเมินจะเข้าไปสังเกตวิธีปฏิบัติงานของผู้ใช้ระบบโดยตรง โดยอาจไม่บอกให้รู้ล่วงหน้าว่าจะมีการเข้าประเมิน การประเมินแบบนี้ มีข้อดีตรงที่ได้ข้อมูลเหตุการณ์การละเมิดระเบียบปฏิบัติที่เกิดขึ้นจริง ส่วนข้อเสียคือ อาจไม่สามารถประเมินด้วยวิธีนี้ได้ทุกหัวข้อของระเบียบที่ประกาศไป

3. การจำลองสถานการณ์ เป็นการสร้างสถานการณ์เพื่อทดสอบว่า ผู้ใช้ระบบปฏิบัติตามระเบียบปฏิบัติได้ตรงตามที่กำหนดไว้ เช่น มีระเบียบปฏิบัติให้ผู้ใช้ระบบต้อง log off จากระบบเมื่อไม่ได้ใช้งาน ก็อาจจะลองโทรศัพท์เรียกใช้ผู้ใช้ระบบให้ออกไปจากหน้าจอ แล้วสังเกตดูว่า ผู้ใช้ระบบ log off จากระบบหรือไม่ การจำลองสถานการณ์มีข้อดี คือ ใช้ประเมินการปฏิบัติตามระเบียบข้อที่ไม่สามารถประเมินด้วยวิธีอื่น ๆ แต่มีข้อเสียคือต้องใช้บุคลากรในการประเมินหลายคน และเสียเวลาในการประเมินมาก

การประเมินผลการปฏิบัติตามระเบียบปฏิบัตินี้ ควรกำหนดให้มีการประเมินโดยสม่ำเสมอ เช่น ทุก ๆ 1-3 เดือน เพื่อคอยติดตามสถานการณ์ว่า เกิดการละเมิดระเบียบปฏิบัติมากน้อยแค่ไหน หากเกิดการละเมิดระเบียบปฏิบัติเป็นจำนวนมาก ควรค้นหาสาเหตุและหาทางแก้ไขปัญหาโดยเร่งด่วน

เมื่อประเมินการปฏิบัติตามระเบียบปฏิบัติเสร็จแล้ว ควรจัดทำรายการสรุปผลการประเมินดังตัวอย่างต่อไปนี้

รายงานการประเมินการปฏิบัติตามระเบียบปฏิบัติด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของโรงพยาบาล ..... ครั้งที่ 1/2566

จำนวนผู้ใช้งานระบบทั้งสิ้น 500 คน ดำเนินการประเมิน 500 คน คิดเป็นร้อยละ 100

ความปฏิบัติตามระเบียบ

ข้อที่ 1 ปฏิบัติ 400 คน ไม่ปฏิบัติ 99 คน การปฏิบัติตามคิดเป็นร้อยละ 80.16

ข้อที่ 2 ปฏิบัติ 450 คน ไม่ปฏิบัติ 49 คน การปฏิบัติตามคิดเป็นร้อยละ 90.18

ข้อที่ 3 ปฏิบัติ 420 คน ไม่ปฏิบัติ 79 คน การปฏิบัติตามคิดเป็นร้อยละ 84.17

ข้อที่ 4 ปฏิบัติ 350 คน ไม่ปฏิบัติ 149 คน การปฏิบัติตามคิดเป็นร้อยละ 70.14

(รายงานผลจนครบทุกข้อ.....)

<u>สรุปผลการประเมิน</u>

ระเบียบข้อที่ปฏิบัติตามมากที่สุดคือข้อที่ 2 ข้อที่ละเมิดมากที่สุดคือข้อที่ 4

สาเหตุที่ละเมิดระเบียบ เป็นเพราะไม่สนใจที่จะทำตาม ไม่ตระหนักถึงความสำคัญที่จะต้องดำเนินการตามระเบียบ

<u>เสนอแนะแนวทางแก้ไข</u>

ให้รางวัลแก่บุคลากรที่สามารถปฏิบัติตามระเบียบปฏิบัติได้เป็นอย่างดี กำหนดมาตรการลงโทษผู้ที่ละเมิดระเบียบปฏิบัติ โดยกำหนดเป้าหมายให้การปฏิบัติตามระเบียบทุกหัวข้อ มีสัดส่วนการปฏิบัติไม่ต่ำกว่า ร้อยละ 95

บทที่ 4 การจัดการความเสี่ยง

ความแตกต่างระหว่าง ความเสี่ยง และอุบัติการณ์

ความเสี่ยง (Risks) คือ จุดอ่อนที่มีอยู่ในระบบ ซึ่งมีทั้งแบบที่ผู้ปฏิบัติงานรับรู้ และจุดอ่อนที่มีอยู่แต่ไม่มีใครรับรู้ว่าดำรงอยู่ โดยจุดอ่อนเหล่านี้เปรียบเสมือนเป็นช่องโหว่ที่จะทำให้ภัยอันตรายจากภายนอกเข้าไปทำความเสียหายให้เกิดขึ้นในระบบได้ หากทีมพัฒนาคุณภาพสามารถค้นหาจุดอ่อนทั้งหมด และลงมือปิดจุดอ่อนให้หมด ก็จะสามารถป้องกันความเสียหายมิให้เกิดขึ้นต่อระบบได้ โดยมักจะมีค่าใช้จ่ายถูกกว่าการแก้ไขความเสียหายในภายหลัง

อุบัติการณ์ (Incidents) คือ เหตุร้ายที่เกิดขึ้น ทำให้เกิดการชะงัก ติดขัด ของการปฏิบัติงาน โดยสาเหตุของอุบัติการณ์ส่วนใหญ่สามารถป้องกันได้จากการปิดจุดอ่อน เช่น เครื่องคอมพิวเตอร์ติดไวรัสทำให้ข้อมูลสำคัญหายไป เรื่องนี้เป็นอุบัติการณ์ที่เกิดจากจุดอ่อนหลายด้าน ได้แก่ การไม่มีระบบป้องกันไวรัส การนำอุปกรณ์บันทึกข้อมูลมาเชื่อมต่อโดยไม่มีการค้นหาและกำจัดไวรัส การไม่สำรองข้อมูลสำคัญเป็นระยะ เป็นต้น

ดังนั้น เราจะเห็นได้ว่าความเสี่ยงมีความแตกต่างจากอุบัติการณ์อย่างเห็นได้ชัด อุบัติการณ์คือเหตุร้ายที่เกิดขึ้นแล้ว แต่ความเสี่ยงคือจุดอ่อนที่มีอยู่โดยถ้าไม่เกิดอุบัติการณ์ก็อาจจะไม่มีใครสนใจ ดังนั้น การพัฒนาคุณภาพที่ถูกทางควรดำเนินการโดยค้นหาและปิดจุดอ่อนให้มากที่สุด เพื่อลดโอกาสการเกิดอุบัติการณ์ในอนาคตให้น้อยที่สุดเท่าที่จะทำได้

ระบบการจัดการความเสี่ยง

การจัดการความเสี่ยง (Risk Management) เป็นกลไกสำคัญ สำหรับการควบคุมคุณภาพระบบงานทุกระบบ เพราะหากเราต้องการให้ระบบงานมีคุณภาพ เราต้องประเมินและตรวจสอบความเสี่ยงที่จะให้ระบบงานของเราด้อยคุณภาพให้ครอบคลุมความเสี่ยงทุกด้าน แล้วจัดการป้องกันไม่ให้ความเสี่ยงเหล่านั้นมีโอกาสมารบกวนและทำให้ระบบงานของเราด้อยคุณภาพลงไปได้

ระบบเทคโนโลยีสารสนเทศโรงพยาบาลก็เป็นระบบหนึ่งที่ต้องใช้การจัดการความเสี่ยงเป็นกลไกสำคัญในการควบคุมเพื่อให้มั่นใจว่าระบบดำเนินไปได้อย่างมีคุณภาพ ดังนั้น ผู้บริหาร และผู้ปฏิบัติงานในระบบเทคโนโลยีสารสนเทศโรงพยาบาลจึงต้องมีความเข้าใจวิธีการจัดการความเสี่ยงเป็นอย่างดี เพื่อให้สามารถดำเนินการจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ

ปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงในระบบเทคโนโลยีสารสนเทศ

ปัจจัยสำคัญที่ทำให้เกิดความเสี่ยงในระบบเทคโนโลยีสารสนเทศ ประกอบไปด้วยปัจจัยดังนี้

1. จุดอ่อน หรือ ช่องโหว่ (Vulnerabilities)
2. ภัยคุกคาม (Threats)

จุดอ่อน (Vulnerabilities) หมายถึง ข้อบกพร่องทางด้าน กายภาพ การจัดระบบ ขั้นตอนการทำงาน บุคลากร การบริหารจัดการ ครุภัณฑ์ โปรแกรม หรือข้อมูลสารสนเทศสำคัญ ดังตัวอย่างต่อไปนี้

- ไม่มีการติดตั้งกุญแจประตูห้องเครื่องแม่ข่าย
- ไม่มีระบบดักจับควัน และระบบดับเพลิงอัตโนมัติในห้องควบคุมระบบเครื่องแม่ข่าย
- ไม่กำหนดขั้นตอนมาตรฐานในการสำรองข้อมูล
- บุคลากรไม่ทำตามระเบียบปฏิบัติด้านการตั้งรหัสผ่าน
- ไม่มีเครื่องแม่ข่ายสำรอง
- ใช้โปรแกรมระบบงานสำคัญร่วมกับโปรแกรมส่วนตัว
- ติดตั้งโปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ตได้โดยอิสระ
- ไม่มีการควบคุมการเข้าถึงข้อมูล สารสนเทศที่สำคัญ

ภัยคุกคาม (Threats) หมายถึง ภัยอันตรายต่าง ๆ ทั้งที่มีสาเหตุมาจากมนุษย์และสาเหตุอื่นๆ อันมีโอกาสจะทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ดังตัวอย่างต่อไปนี้

- ไฟไหม้
- น้ำท่วม
- ขโมย
- ไวรัสคอมพิวเตอร์
- กระแสไฟฟ้าขัดข้อง

ความเสี่ยง (Risk) คือความเป็นไปได้หรือโอกาสที่ภัยคุกคามจะเข้ามาสร้างความเสียหายให้กับระบบ โดยจุดอ่อนของระบบจะเพิ่มโอกาสให้ภัยคุกคามเข้ามาสร้างความเสียหายให้กับระบบเทคโนโลยีสารสนเทศได้ การจัดการความเสี่ยงจึงมีเป้าหมายสำคัญเพื่อ ลดโอกาส ที่ภัยคุกคามจะเข้ามาสร้างความเสียหายให้กับระบบนั่นเอง

ขั้นตอนสำคัญในการจัดการความเสี่ยง

ขั้นตอนที่สำคัญในการจัดการความเสี่ยง ประกอบไปด้วย ขั้นตอนดังต่อไปนี้

1. การค้นหาและประเมินความเสี่ยง (Risks Identification and Risks Assessment)
2. การวางแผนกลยุทธ์จัดการความเสี่ยง (Risks Management Strategic Planning)
3. การดำเนินการจัดการความเสี่ยง (Risks Treatment)

4.1 การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ทำโดยการสำรวจระบบเทคโนโลยีสารสนเทศของโรงพยาบาล เพื่อค้นหาจุดอ่อนและภัยคุกคามที่มีโอกาสจะเข้ามาทำความเสียหายให้กับระบบ แล้วประเมินระดับคะแนนความเสี่ยง เพื่อนำมาพิจารณาวางแผนจัดการความเสี่ยงต่อไป

มาตรฐาน ISO/IEC 27001 : 2013 [1] ซึ่งเป็นมาตรฐานนานาชาติสำหรับระบบบริหารความปลอดภัยของข้อมูล (Security Management Systems, ISMS) ได้กล่าวถึงความเสี่ยงในระบบเทคโนโลยีสารสนเทศไว้มากมาย ดังตัวอย่างเช่น

- acts of terrorism การก่อการร้าย
- air conditioning failure ระบบปรับอากาศหยุดทำงาน
- airborne particles/dust ฝุ่นละออง
- bomb attack การวางระเบิด
- breach of legislation or regulations การละเมิดนโยบายและระเบียบปฏิบัติด้านความปลอดภัย
- breaches of contractual obligations การละเมิดข้อตกลงหรือสัญญาที่ผูกพัน
- compromise of security การละเมิดความมั่นคงปลอดภัย
- damage caused by penetration tests ความเสียหายจากการทดสอบเจาะระบบ
- damage caused by third parties ความเสียหายจากบุคคลที่สาม
- destruction of records ข้อมูลถูกทำลาย
- destruction of the business continuity plans แผนกู้คืนถูกทำร้าย
- deterioration of media สื่อที่เก็บข้อมูลเสื่อมสภาพ
- disasters (natural or man-made) ภัยพิบัติ (จากธรรมชาติ หรือจากมนุษย์)
- ฯลฯ

การค้นหาและประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล จึงควรเริ่มจาก การตรวจสอบรายการความเสี่ยงที่อาจเกิดขึ้นได้ทั้งหมด โดยอาจใช้สถิติการเกิดอุบัติการณ์ด้านไซเบอร์ในโรงพยาบาล (Cyber incidents) การแจ้งเตือนจาก ThaiCERT หรือ HealthCERT รวมทั้งแบบประเมินความเสี่ยง เช่น แบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ที่พัฒนาโดย สมาคมเวชสารสนเทศไทย [2] (ดูแบบประเมินในหน้าถัดไป) โดยเมื่อคาดว่าอาจเกิดความเสี่ยงเรื่องใดแล้ว คณะผู้ประเมินจะต้องประเมินรายละเอียดเพิ่มเติม ได้แก่

1. โอกาสที่จะเกิดความเสี่ยงนั้น (Probability)
2. ความเสียหายที่จะเกิดขึ้น (Impact)

การคำนวนคะแนนความเสี่ยง

ประเมินโอกาสที่จะเกิดความเสี่ยง มีค่า 1 (ต่ำมาก) 2 (ต่ำ) 3 (ปานกลาง) 4 (สูง) 5 (สูงมาก)

ประเมินผลเสียหาย มีค่า 1 (ต่ำมาก) 2 (ต่ำ) 3 (ปานกลาง) 4 (สูง) 5 (สูงมาก)

คะแนนความเสี่ยง คำนวนได้จาก คะแนนโอกาส คูณ กับ คะแนนผลเสียหาย

เช่น โอกาสเกิดความเสี่ยง = 3 ผลเสียหาย = 5 ดังนั้น คะแนนความเสี่ยง = 3x5 = 15

การประเมินความเสี่ยง โอกาสที่จะเกิดความเสี่ยงและผลเสียหาย จะประเมินค่าเป็นระดับ 1-5 ดังนี้

ประเมินจุดอ่อนหรือโอกาสที่จะเกิดความเสี่ยง มีค่าได้เป็น

1 ต่ำมาก มีจุดอ่อนน้อยมาก หรือไม่น่าจะเกิดเหตุการณ์นี้ได้ หรือมีโอกาสเกิดได้น้อยมาก

2 ต่ำ มีจุดอ่อนน้อย หรือมีโอกาสเกิดเหตุการณ์ได้น้อย อาจพบได้สักครั้ง ในรอบ 1 ปี

3 ปานกลาง มีจุดอ่อนพอควร หรือมีโอกาสเกิดเหตุการณ์ได้บ้าง อย่างน้อย เดือนละ 1 ครั้ง

4 สูง มีจุดอ่อนมาก หรือ มีโอกาสเกิดเหตุการณ์ได้บ่อย เดือนละหลายครั้ง

5 สูงมาก มีจุดอ่อนรอบด้าน หรือ มีโอกาสเกิดเหตุการณ์ได้บ่อยมาก พบทุกๆสัปดาห์

ประเมินผลเสียหาย มีค่าได้เป็น

1 ต่ำมาก ไม่น่าจะเกิดผลกระทบต่อการให้บริการ หรือมีผลกระทบน้อยมาก

2 ต่ำ มีผลกระทบต่อการให้บริการของโรงพยาบาลในบางจุด

3 ปานกลาง มีผลกระทบต่อการให้บริการของโรงพยาบาลใน 1-2 แผนก

4 สูง มีผลกระทบต่อการให้บริการของโรงพยาบาล 3-4 แผนก

5 สูงมาก มีผลกระทบต่อการให้บริการของโรงพยาบาลเป็นวงกว้าง อาจเกิดอันตรายต่อผู้ป่วย

หลังจากนั้นให้ประเมินคะแนนความเสี่ยง คำนวนได้จาก คะแนนโอกาส คูณ กับ คะแนนผลเสียหาย

เช่น โอกาสเกิดความเสี่ยง = 3 ผลเสียหาย = 5 ดังนั้น **คะแนนความเสี่ยง = 3x5 = 15**

4.1.1 การประเมินช่องโหว่ หรือ จุดอ่อนของบริการที่สำคัญ

ให้ใช้แบบประเมินจุดอ่อนดังต่อไปนี้

B. แบบประเมินจุดอ่อนในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล พัฒนาโดยสมาคมเวชสารสนเทศไทย ปีพ.ศ. ***2565***

TMI Vulnerabilities Assessment

IT Components	Vulnerability	Score
1. IT – Hardware		
1.1 Servers and Main Switches Crash or Failure	อาจแยกประเมิน server แต่ละเครื่องหรือประเมินทั้งห้องร่วมกัน (เลือก 0 หรือ 1 แต่ละข้อ) 1. กายภาพของห้อง server ระบบล็อคประตู 0 1 ระบบสลับการทำงานเครื่องปรับอากาศ 0 1 ระบบวัดอุณหภูมิ 0 1 ระบบตรวจจับควัน 0 1 ระบบแจ้งเตือนอัคคีภัย 0 1 ถังดับเพลิงที่เหมาะสม 0 1 ความสะอาด 0 1 การกำจัดสิ่งของไม่จำเป็นและเชื้อไฟออกจากห้อง 0 1 2. การจัดระเบียบสายสัญญานและป้ายกำกับ สายสัญญานด้านหน้า 0 1 สายสัญญานด้านหลัง 0 1 ป้ายกำกับสายสัญญาน 0 1 ป้ายกำกับ server 0 1 แผนผังตำแหน่งสายและช่องสัญญาน 0 1 3. การป้องกันการโจมตีพื้นฐาน มี firewall 0 1 เก็บ log 0 1 ตรวจสอบ log เป็นระยะ 0 1	0 ถึง 4 5 5 ถึง 7 4 8 ถึง 11 3 12 ถึง 14 2 15 ถึง 16 1
1.2 Network Switches Crash or Failure	ประเมิน switches ที่อยู่ในจุดต่าง ๆ นอกห้อง (เลือก 0 หรือ 1 แต่ละข้อ) 1. กายภาพของตู้ switches มีตู้ 0 1 ระบบล็อคประตู 0 1 ความสะอาด 0 1 การกำจัดสิ่งของไม่จำเป็นและเชื้อไฟออกจากตู้ 0 1 2. การจัดระเบียบสายสัญญานและการป้องกันสัตว์กัดแทะ สายสัญญานด้านหน้า 0 1 สายสัญญานด้านหลัง 0 1 การป้องกันสัตว์กัดแทะ 0 1 3. ระบบบำรุงรักษา ตรวจสอบและบำรุงรักษาเป็นประจำ 0 1	0 ถึง 2 5 3 ถึง 4 4 5 ถึง 6 3 7 2 8 1
1.3 Workstations and Printers Failure	ประเมินภาพรวม PC ที่อยู่ในจุดต่าง ๆ ของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1. กายภาพของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ระบบป้องกันสายไฟสายสัญญาน 0 1 ระบบป้องกันไฟตกไฟกระชาก 0 1 ความสะอาด 0 1 การป้องกันน้ำและอาหารหกใส่ 0 1 ระบบป้องกันคนนอกเข้าถึง 0 1 2. ระบบปฏิบัติการและระบบขับเคลื่อน (driver) ถูกลิขสิทธิ์ทั้งหมด 0 1 เป็น version ที่ทันสมัยหรือเหมาะสมที่สุด 0 1 3. ระบบบำรุงรักษา ตรวจสอบและบำรุงรักษาเป็นประจำ 0 1	0 ถึง 2 5 3 ถึง 4 4 5 ถึง 6 3 7 2 8 1
1.4		
2. IT – System Software		
2.1 Operating System Failure	ประเมินภาพรวม OS ที่อยู่ใน server ทั้งหมด ของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1. ระบบปฏิบัติการและระบบขับเคลื่อน (driver) ถูกลิขสิทธิ์ทั้งหมด 0 1 เป็น version ที่ทันสมัยหรือเหมาะสมที่สุด 0 1 2. แผ่นติดตั้งระบบปฏิบัติการ ในกรณี ต้องกู้คืนระบบ มีแผ่นติดตั้งครบทั้งหมด 0 1	0 5 1 4 2 3 3 1
2.2		
3. IT – Applications		
3.1 Front Offices	ประเมินระบบ HIS ที่ใช้บริการส่วนหน้าทั้งหมดของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1. การใช้ทรัพยากรของ server CPU ไม่ overload 0 1 หน่วยความจำยังไม่หมด 0 1 พื้นที่ hard disk ยังเพียงพอ 0 1 2. แผ่นติดตั้งระบบ HIS ในกรณี ต้องกู้คืนระบบ มีแผ่นติดตั้งครบทั้งหมด 0 1 3. ระบบบำรุงรักษา ตรวจสอบและบำรุงรักษาเป็นประจำ 0 1	0 ถึง 1 5 2 4 3 3 4 2 5 1
3.2 Back Offices	ประเมินระบบที่ใช้บริการส่วนหลังทั้งหมดของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1. การใช้ทรัพยากรของ server CPU ไม่ overload 0 1 หน่วยความจำยังไม่หมด 0 1 พื้นที่ hard disk ยังเพียงพอ 0 1 2. แผ่นติดตั้งระบบ HIS ในกรณี ต้องกู้คืนระบบ มีแผ่นติดตั้งครบทั้งหมด 0 1 3. ระบบบำรุงรักษา ตรวจสอบและบำรุงรักษาเป็นประจำ 0 1	0 ถึง 1 5 2 4 3 3 4 2 5 1

3.3		
4. IT – Communications, Connectivity		
4.1 Intranet	ประเมินระบบเครือข่ายภายในของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1. การใช้ทรัพยากรของ ระบบเครือข่าย traffic ไม่เกินร้อยละ 80 0 1 bandwidth ไม่เกินร้อยละ 80 0 1 2. การแยกวง เช่น vlan มีการแยกวงที่เหมาะสม 0 1 แยกระบบ HIS ออกจากระบบอินเทอร์เน็ต 0 1 3. ระบบบำรุงรักษา ตรวจสอบและบำรุงรักษาเป็นประจำ 0 1	0 ถึง 1 5 2 4 3 3 4 2 5 1
4.2 Internet	ประเมินระบบเครือข่ายที่เชื่อมต่ออินเทอร์เน็ตของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ) 1. การใช้ทรัพยากรของ ระบบเครือข่าย traffic ไม่เกินร้อยละ 80 0 1 bandwidth ไม่เกินร้อยละ 80 0 1 2. การเพิ่มสายสำรอง กรณีผู้ให้บริการหยุดชะงัก มีสายสำรองที่ 2 0 1 มีสายสำรองที่ 3 0 1 3. ระบบบำรุงรักษา ตรวจสอบและบำรุงรักษาเป็นประจำ 0 1	0 ถึง 1 5 2 4 3 3 4 2 5 1
4.3		
5. IT – Operational (Human) Error		
5.1 Backup Error	ประเมินระบบงานที่ทำให้การสำรองข้อมูลเกิดความผิดพลาด (เลือก 0 หรือ 1 แต่ละข้อ) 1. ขั้นตอนการปฏิบัติงานที่เหมาะสม มีขั้นตอนการปฏิบัติงานชัดเจน 0 1 ผู้สำรองข้อมูลเข้าใจและปฏิบัติได้ถูกต้อง 0 1 2. ระบบตรวจสอบข้อมูลสำรอง มีระบบตรวจสอบความครบถ้วนสมบูรณ์ 0 1 มีการทดลอง restore กลับ 0 1 3. ระบบกำกับดูแลโดยผู้บังคับบัญชา กำกับดูแลเป็นประจำ 0 1	0 ถึง 1 5 2 4 3 3 4 2 5 1
5.2 Data Loss Error	ประเมินระบบงานที่ทำให้ข้อมูลที่ผู้ใช้บันทึกไม่เกิดความผิดพลาด (เลือก 0 หรือ 1 แต่ละข้อ) 1. ขั้นตอนการปฏิบัติงานที่เหมาะสม มีขั้นตอนการปฏิบัติงานชัดเจน 0 1 ผู้บันทึกข้อมูลเข้าใจและปฏิบัติได้ถูกต้อง 0 1 2. ระบบป้องกันข้อมูลสูญหายหรือผิดพลาด ปิดช่องว่างจากขั้นตอนการทำงาน 0 1 ปิดช่องว่างจากโปรแกรม 0 1 3. ระบบกำกับดูแลโดยผู้บังคับบัญชา กำกับดูแลเป็นประจำ 0 1	0 ถึง 1 5 2 4 3 3 4 2 5 1
5.3		
6. Data Loss and Privacy Breach		
6.1 Data Backup	ประเมินระบบงานที่ทำให้ข้อมูลสำรองสูญหาย (เลือก 0 หรือ 1 แต่ละข้อ) 1. ระบบ offline backup มีระบบ offline backup 0 1 อุปกรณ์เก็บข้อมูลสำรองมีจำนวนเพียงพอ 0 1 อุปกรณ์เก็บข้อมูลสำรองมีที่เก็บปลอดภัย 0 1 2. ระบบป้องกันข้อมูลสำรองถูกจารกรรม มีระบบห้ามบุคลากรนำข้อมูลสำรองออกสู่ภายนอก 0 1 3. ระบบกำกับดูแลโดยผู้บังคับบัญชา กำกับดูแลเป็นประจำ 0 1	0 ถึง 1 5 2 4 3 3 4 2 5 1
6.2 Data Protection Policy and Regulations	ประเมินการป้องกันความลับและความเป็นส่วนตัวของข้อมูล (เลือก 0 หรือ 1 แต่ละข้อ) 1. ระบบห้ามการเข้าถึงข้อมูลที่บุคลากรไม่มีส่วนเกี่ยวข้อง มีระบบล็อคหรือมีระเบียบห้ามการเข้าถึงข้อมูลที่ตนเองไม่มีส่วนเกี่ยวข้อง 0 1 2. ระบบอภิบาลข้อมูล มีการสำรวจและจัดทำทะเบียนข้อมูลสำคัญ 0 1 มีการจัดประเภทข้อมูลที่ต้องปกปิด 0 1 มีขั้นตอนการจัดการข้อมูลสำคัญตั้งแต่ต้นทางจนถึงปลายทาง 0 1 3. ระบบกำกับดูแลโดยผู้บังคับบัญชา กำกับดูแลเป็นประจำ 0 1	0 ถึง 1 5 2 4 3 3 4 2 5 1
6.3 PDPA Implementation	ประเมินการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ให้คะแนนน 0 ถึง 5	0 ถึง 1 5 2 4 3 3 4 2 5 1

6.4		
7. IT –Future Development		
7.1 No Data Dictionary	ประเมินเอกสารที่ใช้พัฒนาระบบต่อเนื่องในอนาคต (เลือก 0 หรือ 1)	0 5
	มีเอกสาร Data Dictionary ครบทุกตารางในฐานข้อมูล 0 1	1 1
7.2 No System Blueprint	ประเมินเอกสารที่ใช้พัฒนาระบบต่อเนื่องในอนาคต (เลือก 0 หรือ 1)	0 5
	มีเอกสาร วิเคราะห์และออกแบบระบบ ครบทุกระบบที่พัฒนาเอง 0 1	1 1
7.3 No Program Document or Comments	ประเมินการบันทึก comment และ version ของผู้พัฒนาโปรแกรม (เลือก 0 หรือ 1)	0 5
	มีเอกสาร version control และ source code comment 0 1	1 1
7.4		
8. IT – Vendor and Outsource Failure		
8.1 Vendor Stop Support	ประเมินสัญญาที่ทำกับบริษัทภายนอก (เลือก 0 หรือ 1)	0 5
	มีสัญญาที่บริษัทจะต้องส่งมอบเอกสารสำคัญและข้อมูลทั้งหมดเมื่อหมดสัญญา 0 1	1 1
8.2		
9. IT – Hacking, Unauthorized Intrusions	ประเมินภาพรวมจุดต่าง ๆ ของโรงพยาบาล (เลือก 0 หรือ 1 แต่ละข้อ)	0 ถึง 2 5
	1. เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	3 ถึง 4 4
	มีระบบหรือระเบียบล็อคหน้าจอเมื่อไม่มีผู้ใช้งาน 0 1 เข้ารหัสข้อมูลส่วนตัวผู้ป่วย 0 1	5 ถึง 6 3
	มีการป้องกันการถ่ายภาพหน้าจอในจุดที่คนนอกเข้าถึง 0 1	7 2
	2. ระบบเครือข่าย	8 1
	ปิดสัญญานช่องเชื่อมต่อเครือข่ายที่ไม่มีการใช้งาน 0 1	
	มีการเข้ารหัสและตั้งรหัสผ่านการใช้ wifi access 0 1 เปลี่ยนรหัส wifi บ่อย ๆ 0 1	
	3. ระเบียบปฏิบัติด้านความมั่นคงปลอดภัย	
	ห้ามใช้ username ร่วมกัน 0 1 ตั้ง username และ password ซับซ้อน 0 1	
	ห้ามติด password ไว้ในที่เปิดเผย 0 1	
10. Environment Factors		
10.1 Flooding – Internal	ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากน้ำรั่วในสำนักงาน (เลือก 0 หรือ 1)	0 5
	มีระบบป้องกันไม่ให้น้ำรั่วไหลลงสู่ทรัพย์สิน IT 0 1	1 1
10.2 Flooding – External	ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากอุทกภัยในพื้นที่ (เลือก 0 หรือ 1)	0 5
	มีระบบป้องกันไม่ให้อุทกภัยสร้างความเสียหายต่อทรัพย์สิน IT 0 1	1 1
10.3 Fire – Internal	ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากไฟไหม้ในโรงพยาบาล (เลือก 0 หรือ 1)	0 5
	มีระบบป้องกันไม่ให้ไฟไหม้ทรัพย์สิน IT 0 1	1 1
10.4 Fire – External	ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากอัคคีภัยในพื้นที่ (เลือก 0 หรือ 1)	0 5
	มีระบบป้องกันไม่ให้ไฟไหม้ทรัพย์สิน IT 0 1	1 1
10.5 Utilities – Electricity	ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากไฟฟ้าตกหรือกระชาก (เลือก 0 หรือ 1)	0 5
	มีระบบป้องกันไม่ให้ไฟฟ้าสร้างความเสียหายต่อทรัพย์สิน IT 0 1	1 1
10.6 Criminal – Theft	ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากโจรกรรม (เลือก 0 หรือ 1)	0 5
	มีระบบป้องกันไม่ให้มีโจรหรือขโมยสร้างความเสียหายต่อทรัพย์สิน IT 0 1	1 1
10.7 Criminal – Break-ins	ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากการจัดแจะหรือย่องเบา (เลือก 0 หรือ 1)	0 5
	มีระบบป้องกันไม่ให้มีโจรหรือขโมยสร้างความเสียหายต่อทรัพย์สิน IT 0 1	1 1
10.8 Civil Unrest – Protest, Mob	ประเมินจุดอ่อนที่ทรัพย์สิน IT อาจเสียหายจากเหตุจลาจล วัยรุ่นทะเลาะกัน (เลือก 0 หรือ 1)	0 5
	มีระบบป้องกันไม่ให้มีผู้สร้างความเสียหายต่อทรัพย์สิน IT 0 1	1 1
10.9		
11. Patient Risks due to IT Errors/Misuse	ประเมินจุดอ่อนการใช้ IT ที่อาจทำให้เกินอันตรายต่อผู้ป่วย (เลือก 0 หรือ 1 แต่ละข้อ)	0 ถึง 2 5
	1. ระบบแจ้งเตือนเมื่อพบค่าวิกฤต	3 ถึง 4 4
	มีระบบแจ้งเตือนเมื่อพบค่าวิกฤตของผู้ป่วย 0 1 มีการแจ้งเตือนผู้เกี่ยวข้องทันที 0 1	5 ถึง 6 3
	มีการตรวจสอบว่าระบบแจ้งเตือนทำงานได้ตามปกติ 0 1	7 2
	2. ระบบตรวจสอบการสั่งการรักษาหรือไม่สั่งการรักษาที่เหมาะสม	8 1
	มีระบบตรวจสอบการสั่งการรักษาที่เหมาะสม 0 1	
	มีระบบตรวจสอบการไม่สั่งการรักษาที่เหมาะสมและแจ้งเตือน 0 1	
	3. ระบบป้องกันความผิดพลาดในการบันทึกข้อมูล ตรวจสอบบุคคล หัวหน้าตรวจสอบ	
	มีระบบป้องกันความผิดพลาดในการบันทึกข้อมูล 0 1	
	มีระบบตรวจสอบบุคคลแบบ double check 0 1	
	มีระบบหัวหน้ายืนยันการดำเนินการกรณีสำคัญยิ่งยวด 0 1	
12. Other		

แบบประเมินความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล พัฒนาโดยสมาคมเวชสารสนเทศไทย ปีพ.ศ. *2565*

TMI Risk analysis worksheet (Range of 0.0 to 1.0 for P and I)

IT Components	Probability (P)	Impact (I)	Risk = P x I
1. IT – Hardware	1 2 3 4 5	1 2 3 4 5	
1.1 Servers Crash or Failure	1 2 3 4 5	1 2 3 4 5	
1.2 Network Switches Crash or Failure	1 2 3 4 5	1 2 3 4 5	
1.3 Workstations Failure	1 2 3 4 5	1 2 3 4 5	
1.4	1 2 3 4 5	1 2 3 4 5	
2. IT – System Software	1 2 3 4 5	1 2 3 4 5	
2.1 Operating System Failure	1 2 3 4 5	1 2 3 4 5	
2.2	1 2 3 4 5	1 2 3 4 5	
3. IT – Applications	1 2 3 4 5	1 2 3 4 5	
3.1 Front Offices	1 2 3 4 5	1 2 3 4 5	
3.2 Back Offices	1 2 3 4 5	1 2 3 4 5	
3.3	1 2 3 4 5	1 2 3 4 5	
4. IT – Communications, Connectivity	1 2 3 4 5	1 2 3 4 5	
4.1 Intranet	1 2 3 4 5	1 2 3 4 5	
4.2 Internet	1 2 3 4 5	1 2 3 4 5	
4.3	1 2 3 4 5	1 2 3 4 5	
5. IT – Operational (Human) Error	1 2 3 4 5	1 2 3 4 5	
5.1 Backup Error	1 2 3 4 5	1 2 3 4 5	
5.2 Data Loss Error	1 2 3 4 5	1 2 3 4 5	
5.3	1 2 3 4 5	1 2 3 4 5	
6. Data Loss and Privacy Breach	1 2 3 4 5	1 2 3 4 5	
6.1 Data Backup	1 2 3 4 5	1 2 3 4 5	
6.2 Data Protection Policy and Regulations	1 2 3 4 5	1 2 3 4 5	
6.3 PDPA Implementation	1 2 3 4 5	1 2 3 4 5	
6.4	1 2 3 4 5	1 2 3 4 5	
7. IT –Future Development	1 2 3 4 5	1 2 3 4 5	
7.1 No Data Dictionary	1 2 3 4 5	1 2 3 4 5	
7.2 No System Blueprint	1 2 3 4 5	1 2 3 4 5	
7.3 No Program Document or Comments	1 2 3 4 5	1 2 3 4 5	
7.4	1 2 3 4 5	1 2 3 4 5	
8. IT – Vendor and Outsource Failure	1 2 3 4 5	1 2 3 4 5	
8.1 Vendor Stop Support	1 2 3 4 5	1 2 3 4 5	
8.2	1 2 3 4 5	1 2 3 4 5	
9. IT – Hacking, Unauthorized Intrusions	1 2 3 4 5	1 2 3 4 5	
10. Environment Factors	1 2 3 4 5	1 2 3 4 5	
10.1 Flooding – Internal	1 2 3 4 5	1 2 3 4 5	
10.2 Flooding – External	1 2 3 4 5	1 2 3 4 5	
10.3 Fire – Internal	1 2 3 4 5	1 2 3 4 5	
10.4 Fire – External	1 2 3 4 5	1 2 3 4 5	
10.5 Utilities – Electricity	1 2 3 4 5	1 2 3 4 5	
10.6 Criminal – Theft	1 2 3 4 5	1 2 3 4 5	
10.7 Criminal – Break-ins	1 2 3 4 5	1 2 3 4 5	
10.8 Civil Unrest – Protest, Mob	1 2 3 4 5	1 2 3 4 5	
10.9	1 2 3 4 5	1 2 3 4 5	
11. Patient Risks due to IT Errors/Misuse	1 2 3 4 5	1 2 3 4 5	
12. Other	1 2 3 4 5	1 2 3 4 5	

เมื่อคำนวนคะแนนความเสี่ยงแล้ว ให้นำคะแนนความเสี่ยงมาพิจารณา ตามแผนผังประเมินความเสี่ยง ดังนี้

Risk Value			Probability				
			Very Low	Low	Medium	High	Very High
			1	2	3	4	5
Impact	Very High	5	5	10	15	20	25
	High	4	4	8	12	16	20
	Medium	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Very Low	1	1	2	3	4	5

จากแผนผังประเมินความเสี่ยง จะเห็นว่า เหตุการณ์ที่มีค่าคะแนนความเสี่ยงตั้งแต่ 17 ถึง 25 จะเป็นเหตุการณ์ที่เราต้องจัดการความเสี่ยงโดยเร่งด่วน (แสดงในตารางเป็นสีแดง) ส่วนเหตุการณ์ที่มีค่าคะแนนความเสี่ยง ตั้งแต่ 1-3 จะเป็นเหตุการณ์ที่ยังไม่ต้องเร่งรีบจัดการ (แสดงในตารางเป็นสีเหลือง)

4.2 การวางแผนกลยุทธ์จัดการความเสี่ยงในระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

เมื่อเสร็จสิ้นขั้นตอนการประเมินความเสี่ยงแล้ว ขั้นตอนต่อไปจะเป็นการวางแผนกลยุทธ์จัดการความเสี่ยง โดยเริ่มการจัดลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยง โดยใช้เกณฑ์ความสามารถในการยอมรับความเสี่ยงดังนี้

เกณฑ์ความสามารถในการยอมรับความเสี่ยง

ความเสี่ยง	**คะแนน**	**แถบสี**	**ความหมาย**
ต่ำ	1 - 3		Acceptable or Limited Focus ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม
ปานกลาง	4 - 9		Tolerable but caution or Management Discretion/Medium Risk ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
สูง	10 - 16		Intolerable or Attention Required/High Risk ระดับที่ไม่สามารถยอมรับได้โดยต้องจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
สูงมาก	17 - 25		Intolerable or Immediate Attention Require/High Risk ระดับที่ไม่สามารถยอมรับได้จำเป็นต้องเร่งจัดการควบคุมให้อยู่ในระดับที่ยอมรับได้ทันที

จากการใช้เกณฑ์ความสามารถในการยอมรับความเสี่ยง เราจะสามารถเรียงลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยงได้ โดย เหตุการณ์ที่มีค่าคะแนนความเสี่ยงสูงมาก (17-25) จะถือว่ามีค่าความเสี่ยงในระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการควบคุมให้อยู่ในระดับที่ยอมรับได้โดยทันที จึงต้องเขียนแผนจัดการความเสี่ยงเหตุการณ์ระดับนี้โดยกำหนดลำดับความสำคัญเป็นลำดับแรก ส่วนเหตุการณ์ที่มีค่าคะแนนความเสี่ยงสูง และปานกลาง จะกำหนดลำดับความสำคัญไว้เป็นลำดับต่อมา

เมื่อกำหนดลำดับความสำคัญของเหตุการณ์ที่ทำให้เกิดความเสี่ยงได้แล้ว ขั้นตอนต่อไป คือการกำหนดวิธีแก้ไขความเสี่ยง (Risk Treatment) ให้กับเหตุการณ์ต่างๆ โดยมีทางเลือกกลยุทธ์ในการแก้ไขความเสี่ยง [3] ทั้งหมด 4 กลยุทธ์ดังนี้

กลยุทธ์ในการแก้ไขความเสี่ยง

กลยุทธ์ที่ 1 การลดความเสี่ยง

กลยุทธ์ที่ 2 การย้ายความเสี่ยง

กลยุทธ์ที่ 3 การหลีกเลี่ยงความเสี่ยง

กลยุทธ์ที่ 4 การยอมรับความเสี่ยง

กลยุทธ์ที่ 1 การลดความเสี่ยง เป็นการกำหนดมาตรการควบคุมให้โอกาสเกิดเหตุการณ์ที่ทำให้เกิดความเสี่ยงลดน้อยลง และ/หรือ ร่วมกับมาตรการควบคุมให้ผลเสียหายลดลง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	เป้าหมายในการควบคุม	มาตรการควบคุม
1. ไฟไหม้เครื่องแม่ข่าย	ลดโอกาสที่จะเกิดเหตุการณ์	1. ติดตั้งเครื่องตัดไฟอัตโนมัติเมื่อเกิดกระแสไฟรั่วหรือกระแสไฟเกินในห้องเครื่องแม่ข่าย 2. เปลี่ยนฝ้าเพดานและผนังห้องเครื่องแม่ข่ายให้เป็นวัสดุไม่ติดไฟ 3. ห้ามสูบบุหรี่ ห้ามนำวัสดุติดไฟง่ายเข้าใกล้เครื่องแม่ข่าย
	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. ติดตั้งเครื่องแม่ข่ายสำรองที่สามารถกำหนดให้เป็นเครื่องแม่ข่ายจริงได้ทันทีเมื่อเครื่องแม่ข่ายจริงหยุดทำงาน โดยติดตั้งไว้อีกตึกหนึ่งของโรงพยาบาล 2. สำรองข้อมูลลงแถบแม่เหล็กทุกวัน นำแถบแม่เหล็กออกไปเก็บไว้นอกโรงพยาบาล 3. จัดทำแผนกู้คืนเครื่องแม่ข่ายและซ้อมแผนกู้คืนปีละ 2 ครั้ง

2. ไวรัสโจมตีระบบเครือข่าย	ลดโอกาสที่จะเกิดเหตุการณ์	1. แยกระบบเชื่อมต่ออินเทอร์เน็ตออกจากระบบงานโรงพยาบาล 2. ติดตั้งโปรแกรมสำรวจป้องกันและกำจัดไวรัสในระบบเครือข่าย 3. ห้ามผู้ใช้งานระบบ นำ USB Drive มาถ่ายโอนข้อมูลกับเครื่องคอมพิวเตอร์ของโรงพยาบาล
	ลดผลเสียหายเมื่อเกิดเหตุการณ์	1. ติดตั้งเครือข่ายสำรองที่สามารถกำหนดให้เป็นเครือข่ายจริงได้ทันทีเมื่อเครือข่ายหยุดทำงาน โดยติดตั้งไว้เป็นอิสระจากเครือข่ายจริง 2. ทำสัญญากับบริษัทผู้เชี่ยวชาญด้านระบบเครือข่ายให้ส่งผู้เชี่ยวชาญมาแก้ปัญหาให้ภายใน 4 ชั่วโมง 3. จัดทำแผนดำเนินงานเมื่อระบบเครือข่ายล่ม ซ้อมแผนปีละ 2 ครั้ง

กลยุทธ์ที่ 2 การย้ายความเสี่ยง เป็นการย้ายผลเสียหายที่เกิดขึ้นจากเหตุการณ์ที่ทำให้เกิดความเสี่ยงไปสู่บุคคลอื่น มักใช้ในกรณีที่องค์กรไม่สามารถลดความเสี่ยงได้ หรือไม่คุ้มค่าที่จะลงทุนลดความเสี่ยง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	**เป้าหมายในการควบคุม**	**มาตรการควบคุม**
1. เครื่องคอมพิวเตอร์ถูกขโมย	ย้ายผลเสียหายไปอยู่ในความรับผิดชอบของบริษัทประกันภัย	ทำประกันภัยเครื่องคอมพิวเตอร์ทุกเครื่องจากภัยโจรกรรม
2. เครื่องแม่ข่ายชำรุด	ย้ายกระบวนการกู้คืนเครื่องแม่ข่ายไปอยู่ในความรับผิดชอบของบริษัทภายนอก	1. ทำสัญญากับบริษัทขายเครื่องแม่ข่ายให้ต้องจัดเครื่องสำรองเตรียมไว้ให้ตลอด 24 ชม. ถ้า

		เครื่องเสียต้องยกเครื่องสำรองมาทดแทนทันที 2. ทำสัญญาจ้างบริษัทภายนอกให้รับผิดชอบกรณีเครื่องแม่ข่ายชำรุด ต้องรับดำเนินการกู้คืนให้สำเร็จภายใน 1 ชั่วโมง
3. เครื่องพิมพ์เสีย	ย้ายกระบวนการซ่อมและกระบวนการบริการเครื่องพิมพ์ให้พร้อมใช้ไปอยู่ในความรับผิดชอบของบริษัทภายนอก	1. ทำสัญญาเช่าเครื่องพิมพ์กับบริษัทภายนอก กำหนดให้บริษัทต้องตั้งเครื่องพิมพ์สำรองพร้อมทดแทนไว้ 5 เครื่อง ถ้ามีเครื่องเสียต้องยกเครื่องอื่นมาให้ใช้แทนได้ภายใน 24 ชั่วโมง

กลยุทธ์ที่ 3 การหลีกเลี่ยงความเสี่ยง เป็นการเปลี่ยนแปลงวิธีการทำงาน หรือกำหนดกิจกรรมเพิ่มเติมเพื่อให้โอกาสเกิดเหตุการณ์ที่ทำให้เกิดความเสี่ยงลดน้อยลง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	**เป้าหมายในการควบคุม**	**มาตรการควบคุม**
1. พัฒนาโปรแกรมเสร็จโดยเปล่าประโยชน์ (ผู้ใช้ไม่นำไปใช้งาน)	เปลี่ยนแปลงวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์	1. ในขั้นตอนวิเคราะห์ความต้องการของผู้ใช้ เพิ่มการทำรายงานผลการวิเคราะห์ความต้องการให้ผู้ใช้ตรวจสอบและรับรอง 2. ในการออกแบบระบบ เพิ่มการทำเอกสารการออกแบบหน้าจอ ขั้นตอนการบันทึกข้อมูลและการทำรายงานให้ผู้ใช้ตรวจสอบ ปรับปรุงแก้ไข และรับรอง
2. เครื่องคอมพิวเตอร์ติดไวรัส	เปลี่ยนแปลงวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์	1. ปิดการใช้งาน USB Drive 2. ตั้งเวลาให้โปรแกรมสแกนหาไวรัสในเครื่องทุกๆวัน ในช่วงเวลาพักรับประทานอาหารกลางวัน

3. เจ้าหน้าที่ลบข้อมูลผิดรายการ	เปลี่ยนแปลงวิธีการทำงานเพื่อลดโอกาสที่จะเกิดเหตุการณ์	เปลี่ยนแปลงโปรแกรมโดยกำหนดให้ไม่สามารถลบข้อมูลออกจากฐานข้อมูลได้ โดยให้ใช้การยกเลิกข้อมูลที่ผิดพลาดและเพิ่มข้อมูลใหม่ที่ถูกต้องเข้าไปทดแทนได้

กลยุทธ์ที่ 4 การยอมรับความเสี่ยง เป็นการบันทึกผลการวิเคราะห์และยอมรับความเสี่ยงในเรื่องที่มีโอกาสเกิดได้น้อยและ/หรือไม่คุ้มค่าที่จะลงทุนในการจัดการความเสี่ยง ดังตัวอย่างต่อไปนี้

เหตุการณ์ที่ทำให้เกิดความเสี่ยง	**เป้าหมายในการควบคุม**	**เหตุผลในการยอมรับความเสี่ยง**
1. การสูญเสียข้อมูลในฐานข้อมูลและข้อมูลที่สำรองไว้จนหมดในเวลาเดียวกัน	ยอมรับความเสี่ยง	ฐานข้อมูลของโรงพยาบาลและข้อมูลที่สำรองเก็บไว้ที่คนละตึกของโรงพยาบาล ที่ไม่ได้อยู่ในหมู่ตึกเดียวกัน มีระยะห่างกัน 800 เมตร โอกาสที่จะสูญเสียข้อมูลทั้งสองพร้อมกัน เช่น ไฟไหม้ทั้งสองตึก มีโอกาสเกิดขึ้นได้น้อยมาก จึงยอมรับความเสี่ยง
2. สายเชื่อมต่ออินเทอร์เน็ตขาดการเชื่อมต่อพร้อมกันทั้ง 2 สาย	ยอมรับความเสี่ยง	การเชื่อมต่ออินเทอร์เน็ตของโรงพยาบาลมี 2 จุดเชื่อมต่อ คือ บริษัท A และบริษัท B โอกาสที่จุดเชื่อมต่อ 2 จุดจะขาดการเชื่อมต่อพร้อมกันมีโอกาสเกิดขึ้นได้น้อยมาก จึงยอมรับความเสี่ยง

4.3 การดำเนินการจัดการความเสี่ยง

การดำเนินการจัดการความเสี่ยงเริ่มจากการจัดสรรทรัพยากร บุคคล เงิน และเวลา ที่ต้องใช้ในการจัดการความเสี่ยงแต่ละเรื่อง โดยอาจจัดทำเป็นโครงการ และใช้การจัดการโครงการ (Project Management) เป็นเครื่องมือช่วยให้การดำเนินการจัดการความเสี่ยงประสบผลสำเร็จต่อไป โดยอาจใช้แผนกิจกรรมจัดการความเสี่ยงดังตัวอย่างในหน้าถัดไป เป็นเครื่องมือในการติดตามและควบคุมการดำเนินการจัดการความเสี่ยง ทั้งนี้ แผนการจัดการความเสี่ยงควรมีการรายงานถึงผู้อำนวยการโรงพยาบาลเพื่ออนุมัติทรัพยากรที่จำเป็นตามระดับความเสี่ยงที่ยอมรับได้ด้วย

4.4 การประเมินผลและการพัฒนาคุณภาพอย่างต่อเนื่อง

เมื่อหน่วยงานดำเนินการจัดการความเสี่ยงไปแล้ว ควรมีการประเมินผลกิจกรรมจัดการความเสี่ยงที่ได้ดำเนินการไปแล้วว่าได้ผลหรือไม่ทุก ๆ 3-6 เดือน ถึงผู้อำนวยการโรงพยาบาลในฐานะผู้รับผิดชอบสูงสุดต่อความเสียหายที่อาจเกิดขึ้นต่อระบบสารสนเทศจากความเสี่ยงดังกล่าว โดยการเก็บข้อมูลอุบัติการณ์ต่าง ๆอันเป็นเหตุการณ์ที่ทำให้เกิดความเสี่ยงทุกรายการ ทำสถิติอุบัติการณ์ และวิเคราะห์แนวโน้มการเปลี่ยนแปลงว่า มีการเปลี่ยนแปลงไปในทางที่ดีขึ้นหรือไม่ โดยต้องประเมินคะแนนความเสี่ยงใหม่ เพื่อตรวจสอบว่าคะแนนความเสี่ยงลดลงหรือไม่ ถ้าพบว่าแนวโน้มดีขึ้น ย่อมแสดงว่ากิจกรรมจัดการความเสี่ยงที่ได้ดำเนินมาแล้วเป็นไปอย่างถูกต้องสมควร แต่หากแนวโน้มความเสี่ยงใดไม่ลดลง หรือเพิ่มขึ้น ก็สมควรปรับแก้ไข หรือเพิ่มกิจกรรมจัดการความเสี่ยงให้ดีขึ้นกว่าเดิมอย่างต่อเนื่อง

(ตัวอย่าง) แผนดำเนินการจัดการความเสี่ยงในระบบสารสนเทศ

ชื่อกลุ่มงาน __เวชระเบียนและสถิติ_____หน่วยงาน_____เวชระเบียนผู้ป่วยใน_____ วันที่จัดทำ_1 มกราคม 2566__

ทรัพย์สิน	ภัยคุกคามทั้งหมดที่เป็นไปได้	แผนการจัดการ	ผู้รับผิดชอบ	งบประมาณ	ช่วงเวลาดำเนินการ
หมวด 1. ข้อมูลและเอกสารสำคัญ, อ้างอิง เวชระเบียนผู้ป่วยใน	ไฟไหม้ เปียกน้ำ ถูกขโมย ปลวกกัดกิน หนู แมลงสาบแทะ	1. จัดซื้อกุญแจล็อคแทนระบบล็อคเดิมที่ใช้การไม่ได้ ติดตั้งระบบกุญแจ 2. จัดซื้อเครื่อง scanner ความเร็วสูงเพื่อ scan เอกสารเข้าสู่ระบบอิเล็กทรอนิกส์ 3. scan เอกสารที่สำคัญเข้าระบบเวชระเบียนอิเล็กทรอนิกส์ (ประมาณการเอกสาร จำนวน 500,000 หน้า) 4. จัดทำตารางการเข้าตรวจสอบกำจัดหนู เพื่อให้บริษัทดำเนินการทุกเดือน ควบคุมดูแล 5. มอบนโยบายและระเบียบปฏิบัติการใช้เครื่องคอมพิวเตอร์ ตามมาตรฐานความปลอดภัยให้กับผู้ปฏิบัติงานทุกคน 6. กำกับดูแลให้เกิดการปฏิบัติตามระเบียบ สุ่มตรวจสอบการกระทำที่ละเมิดระเบียบ	นาย สมชาย นาง ดำเนิน นาย วิภาส	5,000 บาท 80,000 บาท 200,000 บาท -- -- --	มค. – กพ. 2566 มค. – กพ. 2566 กพ. – มีค. 2566 กพ. 2566 กพ. 2566 มีค. – ธค. 2566
หมวด 2. ครุภัณฑ์ระบบสารสนเทศ 2.1 เครื่องคอมพิวเตอร์ หมายเลข 1 2.2 เครื่องคอมพิวเตอร์ หมายเลข 2 2.3 เครื่องพิมพ์ HP2010 หมายเลข 1 2.4 เครื่องพิมพ์ EpsonLX800 หมายเลข 2	ถูกไวรัส ข้อมูลถูกลบโดยไม่ตั้งใจ	7. ติดตั้งโปรแกรมป้องกันไวรัส		200,000 บาท	มีค. – ธค. 2566

* Chief Information Officer (CIO) จะเป็นผู้เริ่มวางระบบความมั่นคงปลอดภัยให้เกิดขึ้นในโรงพยาบาล แต่เมื่อเกิดระบบขึ้นแล้ว จะต้องมี Chief Information Security Officer (CISO) ทำหน้าที่บริหารจัดการความมั่นคง โดยเป็นอิสระจากงานด้านการปฏิบัติการเทคโนโลยีสารสนเทศ

บทที่ 5 การทำให้ระบบมีความแข็งแกร่ง

การทำให้ระบบมีความแข็งแกร่ง มีวัตถุประสงค์เพื่อปิดจุดอ่อนหรือความเสี่ยงของระบบที่จะเป็นช่องทางให้ภัยคุกคามจากภายนอกเข้ามาทำอันตรายระบบเทคโนโลยีสารสนเทศของโรงพยาบาลได้ โดยการทำให้ระบบมีความแข็งแกร่งเป็นหน้าที่รับผิดชอบของผู้ดูแลระบบ โดยควบคุมด้วยการตั้งค่าในระบบ แต่มาตรการทั้งหมดไม่สามารถทำได้ด้วยการตั้งค่าในระบบอย่างเดียว หลายเรื่องที่ต้องอาศัยความร่วมมือจากผู้ใช้ระบบทุกคนด้วย

ไม่มีระบบเทคโนโลยีสารสนเทศใด สามารถป้องกันระบบตัวเองได้ โดยไม่อาศัยความร่วมมือจากผู้ใช้ระบบ ตัวอย่าง เช่น หากผู้ใช้ระบบประมาทเลินเล่อ ไม่เก็บรักษาชื่อผู้ใช้และรหัสผ่านเป็นความลับ ก็อาจเป็นช่องโหว่ใหญ่ให้ผู้ไม่ประสงค์ดีเจาะเข้าระบบได้โดยง่าย ดังนั้น คณะทำงานสร้างระบบความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล จึงต้องระบุรายการที่ผู้ใช้ระบบทุกคนต้องให้ความร่วมมือ กำหนดเป็นระเบียบปฏิบัติ และสื่อสารลงไปสู่ผู้ใช้ระบบทุกคนให้ปฏิบัติตามโดยเคร่งครัด จึงจะมั่นใจได้ว่า ระบบมีความแข็งแกร่งเพียงพอ

คณะทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล มีหน้าที่ต้องกำหนดมาตรฐานค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) โดยต้องระบุองค์ประกอบให้ครบ ทั้งระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมด และ ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

(ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

(ข) การแบ่งแยกหน้าที่ (Separation of Duties)

(ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

(ง) การลบบัญชีที่ไม่ได้ใช้

(จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

(ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

(ช) การป้องกันมัลแวร์ (Malware) และ

(ซ) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

การกำหนดมาตรฐานค่าขั้นต่ำด้านความมั่นคงปลอดภัย อาจทำเป็นตารางระบุองค์ประกอบ วิธีการและผู้รับผิดชอบดังตัวอย่าต่อไปนี้

ตารางการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards)

องค์ประกอบ	ข้อกำหนด	ผู้ดำเนินการ	วิธีการ	
			ควบคุมด้วยระบบ	กำหนดเป็นระเบียบ
1. ผู้ใช้ระบบ	1.1 เก็บรักษาชื่อผู้ใช้และรหัสผ่านเป็นความลับส่วนตัว	ผู้ใช้ทุกคน		✓
	1.2 ตั้งรหัสผ่านที่คาดเดาได้ยาก ไม่ต่ำกว่า 8 ตัวอักษร	ผู้ดูแลระบบ	✓	
	1.3 เปลี่ยนรหัสผ่านใหม่ เมื่อผ่านเวลา 90 วัน	ผู้ดูแลระบบ	✓	
	1.4 กำหนดสิทธิการเข้าถึงน้อยที่สุดที่จะทำงานได้	ผู้ดูแลระบบ	✓	
	1.5 ลบบัญชีผู้ใช้ เมื่อสถานะผู้ใช้ระบบสิ้นสุดลง	ผู้ดูแลระบบ	✓	
2. Computers	2.1 ติดตั้งระบบปฏิบัติการที่ถูกลิขสิทธิ์	ผู้ดูแลระบบ		✓
	2.2 Update patch ของระบบปฏิบัติการสม่ำเสมอ	ผู้ดูแลระบบ		✓
	2.3 ติดตั้งเฉพาะโปรแกรมที่กำหนดไว้เท่านั้น	ผู้ดูแลระบบ		✓
	2.4 ติดตั้งเฉพาะโปรแกรมที่ได้ลิขสิทธิ์ใช้งานเท่านั้น	ผู้ดูแลระบบ		✓
	2.5 ล็อคหน้าจอเมื่อไม่ใช้งานเกิน 5 นาที	ผู้ดูแลระบบ	✓	
	2.6 log out ออกจากระบบ เมื่อไม่ใช้งานเกิน 10 นาที	ผู้ใช้ทุกคน		✓
	2.7 ติดตั้งโปรแกรม antivirus ทุกเครื่อง	ผู้ดูแลระบบ	✓	
3. Servers	3.1 ปิดพอร์ตที่ไม่ได้ใช้งานทั้งหมด	ผู้ดูแลระบบ	✓	
	3.2 Update patch ของระบบปฏิบัติการสม่ำเสมอ	ผู้ดูแลระบบ		✓
	3.3 ปิด/ลบบริการที่ไม่จำเป็น	ผู้ดูแลระบบ		✓
	3.4 กำหนดมาตรการควบคุมการเชื่อมต่อระยะไกล	ผู้ดูแลระบบ		✓
4. เครือข่ายภายใน/ Wi-Fi	4.1 ไม่เชื่อมต่ออินเทอร์เน็ตกับระบบภายใน	ผู้ดูแลระบบ		✓
	4.2 ไม่นำอุปกรณ์ภายนอกมาเชื่อมต่อเครือข่ายภายใน	ผู้ใช้ทุกคน		✓
	4.3 กำหนดมีการเข้ารหัสข้อมูลที่ส่งผ่านเครือข่าย	ผู้ดูแลระบบ	✓	
	4.4 กำหนดให้มีการพิสูจน์ตัวตน และใช้รหัสผ่านเมื่อเข้าใช้งานระบบ Wi-Fi	ผู้ดูแลระบบ	✓	
5. สื่อเก็บข้อมูลแบบถอดได้	5.1 ปิดพอร์ต USB ของคอมพิวเตอร์ทุกเครื่อง และเปิดเมื่อจำเป็นต้องใช้ในบางเครื่อง/บางเวลา	ผู้ดูแลระบบ	✓	
	5.2 ถ้าต้องใช้สื่อเก็บข้อมูลแบบถอดได้ ต้อง Scan virus ทุกครั้งเมื่อเริ่มใช้	ผู้ใช้ทุกคน		✓
6. การใช้ LINE	6.1 ห้ามใช้ LINE ในการส่งข้อมูลผู้ป่วย	ผู้ใช้ทุกคน		✓
	6.2 ถ้าหลีกเลี่ยงการใช้ LINE ในการส่งข้อมูลผู้ป่วยไม่ได้ ให้ปฏิบัติตามมาตรฐานการปฏิบัติงานโดยเคร่งครัด	ผู้ใช้ทุกคน		✓

เมื่อกำหนด ค่าขั้นต่ำด้านความมั่นคงปลอดภัย เสร็จแล้ว ต้องนำไปดำเนินการให้เป็นตามที่กำหนดทุกประการ และตรวจสอบเป็นระยะให้มั่นใจว่า ทุกฝ่ายที่เกี่ยวข้องได้ดำเนินการครบถ้วนแล้ว และต้องทบทวนรายงานใหม่ทุกปี โดยอาจปรับปรุงเปลี่ยนแปลงเพิ่มเติมให้ทันสมัยตามสถานการณ์ที่เปลี่ยนไปแต่ละปี

5.1 การทดสอบการเจาะระบบ (Penetration Test)

ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญ ของโรงพยาบาล โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญของโรงพยาบาล โดยเฉพาะอย่างยิ่ง ทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

ระบบการดูแลรักษาผู้ป่วยและระบบเวชระเบียนอิเล็กทรอนิกส์ของโรงพยาบาล ไม่ควรอยู่ในเครือข่ายที่เชื่อมต่อกับอินเทอร์เน็ต แต่หากเชื่อมต่อก็ต้องดำเนินการทดสอบการเจาะระบบด้วยเช่นกัน

ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง ตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญในโรงพยาบาล ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศของโรงพยาบาล มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์ที่กระทรวงสาธารณสุขกำหนด

ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

บทที่ 6 การสร้างมาตรการตรวจสอบเฝ้าระวัง มาตรการเผชิญเหตุ แก้ไข เมื่อพบภัยคุกคามทางไซเบอร์ และการกู้คืนระบบ

6.1 มาตรการตรวจสอบเฝ้าระวัง

ผู้ดูแลระบบเทคโนโลยีสารสนเทศของโรงพยาบาล มีหน้าที่ที่สำคัญอย่างหนึ่ง คือการเฝ้าระวัง ภัยคุกคามทางไซเบอร์ โดยต้องตรวจสอบให้ครบทุกตำแหน่งของระบบ ได้แก่ ข้อมูล log ของ Firewall, Servers, ระบบ Anti-virus, ระบบ Network โดยต้องตรวจสอบเป็นประจำ โดยทั่วไป ควรทำทุกวัน โดยถือเป็นภาระงานที่สำคัญ และควรบันทึกผลการตรวจสอบทุกครั้ง เพื่อเป็นหลักฐานว่าได้ดำเนินการแล้ว ให้หัวหน้างาน และผู้บริหารได้รับทราบเป็นประจำ

การตรวจสอบเฝ้าระวัง อาจใช้โปรแกรม Security Monitoring รูปแบบต่าง ๆ ช่วยในการวิเคราะห์ อย่างไรก็ตาม การใช้โปรแกรมอาจมีค่าใช้จ่ายที่ผู้บริหารต้องพิจารณาอนุมัติ ผู้ดูแลระบบจึงควรจัดทำโครงการเสนอผู้บริหารให้เหมาะสม เพื่อให้ผู้บริหารพิจารณาโดยละเอียด โดยผู้บริหารจะต้องตัดสินใจว่า ค่าใช้จ่ายรายเดือนหรือรายปีของโปรแกรมต่าง ๆ ด้านความมั่นคงปลอดภัยนั้น คุ้มค่าต่อการป้องกันภัยคุกคามทางไซเบอร์หรือไม่ หากงบประมาณไม่เพียงพอ ก็เป็นหน้าที่ของผู้บริหารที่จะดำเนินการจัดหางบประมาณเพิ่มเติม

การตรวจสอบเฝ้าระวัง เป็นการมองหาเหตุการณ์ (Event) ที่ดูผิดปกติ เบี่ยงเบนไปจากวันก่อน ๆ โดยอาจทำเป็น รายการตรวจสอบ (checklist) ดังตัวอย่างในหน้าต่อไปนี้

เมื่อผู้เฝ้าระวัง พบเหตุการณ์ที่อาจเป็นร่องรอยของการโจมตี หรือเกิดภัยคุกคามต่อความมั่นคงปลอดภัยไซเบอร์ ให้แจ้งต่อหัวหน้า หรือผู้บังคับบัญชาในระดับสูงขึ้นไปโดยทันที โดยหัวหน้าหรือผู้บังคับบัญชาจะพิจารณาว่าเป็นเรื่องที่จะต้องจัดการโดยเร่งด่วนหรือไม่ หากเป็นเรื่องเร่งด่วน จะต้องแจ้ง ทีมตอบสนองเหตุร้าย (Incident Response Team) โดยทันที

โรงพยาบาลควรจัดตั้ง ทีมตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response Team : CIRT) ไว้ล่วงหน้า โดยประกอบไปด้วย ผู้บริหารด้านความมั่นคงปลอดภัย หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หัวหน้าฝ่ายความมั่นคงปลอดภัยสารสนเทศตัวแทน แพทย์ พยาบาล และเจ้าหน้าที่ในหน่วยงานทุกหน่วยที่มีส่วนเกี่ยวข้องในการตอบสนองต่อเหตุร้าย โดยการตอบสนองต่อเหตุร้าย จะมีกิจกรรมหลัก 3 กิจกรรมที่ต้องดำเนินการไปพร้อมกัน ดังนี้

1. การลดระดับความรุนแรงของเหตุร้าย ค้นหาต้นเหตุ และระงับเหตุ โดยเร็วที่สุด (ใช้แผนเผชิญเหตุร้าย หรือ Cyber Incident Response Plan)

2. การจัดการให้งานสำคัญของโรคพยาบาลดำเนินการต่อไปได้ (ใช้แผนดำเนินการอย่างต่อเนื่อง หรือ Business Continuity Plan)

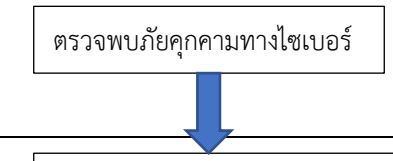
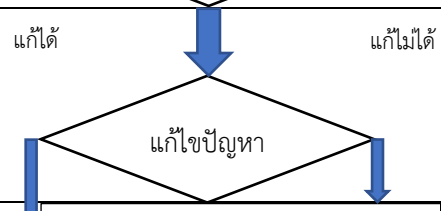
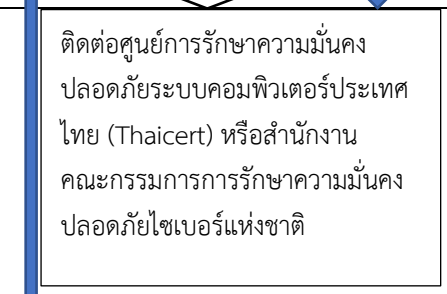
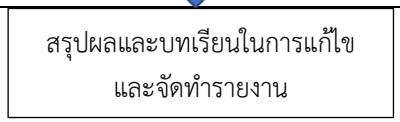
3. การกู้คืนระบบที่เสียหาย ให้กลับขึ้นมาดำเนินการต่อไปนี้ โดยเร็วต่อสุด (ใช้แผนกู้คืน หรือ Disaster Recovery Plan)

รายการตรวจสอบ เหตุการณ์ที่อาจเป็นร่องรอยของการละเมิดความมั่นคงปลอดภัยไซเบอร์ในโรงพยาบาล

เหตุการณ์	**วันเวลาที่รายงานขึ้นไป**
1. การจราจรใน network ของโรงพยาบาลหนาแน่นผิดปกติ ☐ ไม่พบ ☐ พบ	
2. พื้นที่ว่างใน hard disk ของเครื่องแม่ข่าย หายไปผิดปกติ ☐ ไม่พบ ☐ พบ	
3. CPU Usage สูงผิดปกติ ☐ ไม่พบ ☐ พบ	
4. พบการสร้างบัญชี user ใหม่ โดยผู้ดูแลระบบไม่ได้ดำเนินการ ☐ ไม่พบ ☐ พบ	
5. พบการใช้บัญชีผู้ดูแลระบบ โดยผู้ดูแลระบบไม่ได้ดำเนินการ ☐ ไม่พบ ☐ พบ	
6. พบการปิดบัญชีผู้ใช้งาน โดยผู้ดูแลระบบไม่ได้ดำเนินการ ☐ ไม่พบ ☐ พบ	
7. พบการใช้บัญชีผู้ใช้งานโดยเจ้าของบัญชีลาพักผ่อน ลาศึกษาต่อ ไม่อยู่ ☐ ไม่พบ ☐ พบ	
8. log files ถูกลบทิ้งไป ☐ ไม่พบ ☐ พบ	
9. log files เต็ม มีเหตุการณ์ไม่ธรรมดาบันทึกไว้ใน log file จำนวนมาก ☐ ไม่พบ ☐ พบ	
10. การแจ้งเตือนจาก antivirus หรือระบบตรวจจับการบุกรุก ☐ ไม่พบ ☐ พบ	
11. ระบบ antivirus หรือระบบป้องกันอื่น ๆ ถูกปิดไป ☐ ไม่พบ ☐ พบ	
12. มีการเปลี่ยนแปลงใน patch โดยผู้ดูแลรบบไม่ได้ดำเนินการ ☐ ไม่พบ ☐ พบ	
13. พบการเชื่อมโยงเครื่องมือแพทย์ใน network ของโรงพยาบาลไปยัง IP ภายนอก ☐ ไม่พบ ☐ พบ	
14. พบคำสั่งขอรายละเอียดเครื่องแม่ข่ายเข้ามาในระบบ ☐ ไม่พบ ☐ พบ	
15. ความเร็วของการส่งข้อมูลในระบบเครือข่ายลดลงมากเห็นได้ชัด ☐ ไม่พบ ☐ พบ	
16. เกิดหน้าจอแสดงผล error ในหน้า web, เครื่องแม่ข่าย หรือ ฐานข้อมูล ☐ ไม่พบ ☐ พบ	
17. ชื่อไฟล์หรือไดเร็กทอรีถูกเปลี่ยน แทรกด้วยอักขระผิดปกติ ☐ ไม่พบ ☐ พบ	
18. ค่าของระบบที่ตั้งไว้ (system configuration) เปลี่ยนแปลงไป ☐ ไม่พบ ☐ พบ	
19. มี email จำนวนมากส่งเข้ามา มีลักษณะเนื้อหาไม่ปกติ ☐ ไม่พบ ☐ พบ	
20. พบการส่งข้อมูลในเส้นทางที่ไม่เคยใช้ ☐ ไม่พบ ☐ พบ	
21. เครื่องคอมพิวเตอร์หรืออุปกรณ์เกิดอาการผิดปกติพร้อมกันจำนวนมาก ☐ ไม่พบ ☐ พบ	
22. พบการข้ามขั้นตอนการมาตรฐานการทำงานที่ตั้งไว้ ด้านการสำรองข้อมูล หรือ การ fail over ☐ ไม่พบ ☐ พบ	
23. มีเครื่องที่ส่งข้อมูลจำนวนมากผ่านเครือข่าย โดยผู้ใช้ไม่ได้ทำงานที่แปลกไป ☐ ไม่พบ ☐ พบ	
24. พบการใช้พลังงานจาก data center มากกว่าปกติ ☐ ไม่พบ ☐ พบ	
25. พบการแจ้งปัญหาขัดข้องในระบบจากผู้ใช้งานจำนวนมากพร้อม ๆ กัน ☐ ไม่พบ ☐ พบ	

6.2 มาตรการเผชิญเหตุ และแก้ไข เมื่อเกิดภัยคุกคามทางไซเบอร์

โรงพยาบาล ควรกำหนด มาตรการเผชิญเหตุ และแก้ไข เมื่อเกิดภัยคุกคามทางไซเบอร์ไว้ล่วงหน้า และซ้อมการดำเนินการตามมาตรฐาน เมื่อเกิดเหตุการณ์ ผู้ที่มีหน้าที่รับผิดชอบก็จะได้ปฏิบัติได้อย่างถูกต้อง ตรงตามที่กำหนดไว้ ตัวอย่าง มาตรการอาจเป็นดังต่อไปนี้

ขั้นตอน	รายละเอียด
	มีการแจ้งเหตุจากผู้ใช้งาน หรือตรวจพบเหตุการณ์ที่อาจเป็นภัยคุกคามความมั่นคงทางไซเบอร์ของโรงพยาบาล
	แจ้งหัวหน้าผู้ควบคุม และร่วมกันประเมินระดับความรุนแรง
	หากไม่รุนแรง แก้ไขเองได้ให้ดำเนินการทันที ถ้ารุนแรงให้เรียกระดมทีมเผชิญเหตุร้าย (Incident response team)
	ทีมเผชิญเหตุร้าย ดำเนินการแก้ไข หรือกำจัดภัยคุกคามโดยทันที
	ในกรณีที่ไม่สามารถแก้ไขปัญหาได้ จะดำเนินการติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อขอความช่วยเหลือ
	หลังการแก้ไขปัญหาภัยคุกคามแล้ว ทีมตรวจหาจุดอ่อน ช่วงโหว่ และหาวิธีปิดจุดอ่อนช่องโหว่ เพื่อป้องกันไม่ให้เกิดเหตุการณ์ลักษณะเดียวกันซ้ำอีก
	สรุปผลการจัดการ สรุปบทเรียนแนะแนวทางการป้องกัน จัดทำรายงานส่งให้ผู้เกี่ยวข้อง เช่น ผู้อำนวยการโรงพยาบาล สกมช.

6.3 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตครอบคลุม

(ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

(ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

(ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

(ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน และ

(จ) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย)สำหรับการเผยแพร่ข้อมูล

ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละครั้งเพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

6.4 การจัดทำแผนดำเนินการอย่างต่อเนื่อง เมื่อระบบคอมพิวเตอร์ใช้การไม่ได้

แผนดำเนินการอย่างต่อเนื่อง เมื่อระบบคอมพิวเตอร์ใช้งานไม่ได้ (Business Continuity Plan – BCP) เป็นเอกสารแสดงขั้นตอนต่าง ๆที่ผู้ใช้ระบบคอมพิวเตอร์ในแผนกต่าง ๆของโรงพยาบาลสำหรับบริการผู้ป่วยจะต้องนำมาปฏิบัติตามเมื่อเกิดเหตุใด ๆที่ทำให้ระบบล่ม หรือหยุดชะงัก การเขียนแผนนี้จะต้องระบุรายละเอียดขั้นตอนต่าง ๆที่เจ้าหน้าที่ในแต่ละตำแหน่งของทุกแผนกจะต้องเข้าใจและปฏิบัติตามได้ตลอดระยะเวลาที่ระบบล่มจนกว่าระบบจะกลับมาใช้งานได้อีกครั้งหนึ่ง

แผน BCP ที่สำคัญที่สุด คือแผน BCP กรณีระบบคอมพิวเตอร์ที่ให้บริการผู้ป่วยนอกล่ม โดยระบบคอมพิวเตอร์ที่ให้บริการผู้ป่วยนอกส่วนใหญ่จะครอบคลุมหน่วยงานของโรงพยาบาลดังต่อไปนี้

1. แผนกเวชระเบียนผู้ป่วยนอก
2. พยาบาลห้องตรวจโรคผู้ป่วยนอก

3. แพทย์ที่ปฏิบัติหน้าที่ตรวจรักษาผู้ป่วยนอก
4. ห้องปฏิบัติการชันสูตร (Lab)
5. แผนกรังสีวิทยา (Radiology service)
6. ห้องจ่ายยา (Pharmacy service)
7. แผนกการเงินผู้ป่วยนอก

ทุกแผนกนี้ต้องมีแผน BCP ของตนเอง ที่ระบุรายละเอียดขั้นตอนที่สำคัญที่ใช้บริการผู้ป่วยนอกของแต่ละแผนกโดยไม่มีระบบคอมพิวเตอร์สนับสนุน เช่น ในแผน BCP ของแผนกเวชระเบียน ต้องกล่าวถึงขั้นตอนการให้บริการผู้ป่วยนอกดังนี้

- การลงทะเบียนผู้ป่วยใหม่ การออกเลข HN
- การค้นหาบัตรผู้ป่วยเก่า
- การส่งบัตรผู้ป่วยไปยังห้องตรวจต่าง ๆ
- การรับบัตรกลับมาเมื่อสิ้นสุดการบริการ
- การบันทึกข้อมูลย้อนหลังเมื่อระบบคอมพิวเตอร์กลับมาสู่สถานะปกติ

นอกจากแผน BCP แล้ว ทุกแผนกต้องจัดเตรียมแบบฟอร์มที่เกี่ยวข้องเพื่อใช้บริการผู้ป่วยโดยการเขียนกระดาษ ทั้งนี้ต้องเตรียมแบบฟอร์มในปริมาณที่เพียงพอและจัดให้มีครบทุกแบบฟอร์มที่จำเป็นด้วย

6.5 การจัดทำแผนปฏิบัติการเมื่อเกิดภัยพิบัติแก่ห้อง Data Center

แผนปฏิบัติการเมื่อเกิดภัยพิบัติแก่ห้อง Data Center เป็นเอกสารแสดงขั้นตอนต่าง ๆ ที่ผู้ดูแล Data Center จะต้องนำมาปฏิบัติตามเมื่อภัยพิบัติ เช่น อัคคีภัย อุทกภัย ฯลฯ การเขียนแผนนี้จะต้องระบุรายละเอียดขั้นตอนต่าง ๆที่เจ้าหน้าที่จะต้องเข้าใจและปฏิบัติตามได้อย่างรวดเร็ว ถูกต้องตามขั้นตอน เมื่อเกิดภัยพิบัติ มีขั้นตอนต่าง ๆที่ระบุรายละเอียดไว้อย่างชัดเจน เช่น

- เมื่อพบไฟไหม้ในห้อง Data Center จะทำอย่างไร แจ้งใครบ้าง
- ระหว่างดับไฟ ต้องดำเนินการอย่างไรเพิ่มเติม
- กรณีไฟไหม้นอกห้อง Data Center จะประเมินสถานการณ์อย่างไร
- หากดับไฟไม่ได้จะขนย้ายอุปกรณ์ใดก่อน ขนอย่างไร

- เมื่อดับไฟได้แล้ว จะมีขั้นตอนในการฟื้นฟูระบบให้กลับสู่สถานการณ์ปกติอย่างไร

การซ้อมปฏิบัติการตามแผน BCP และแผนปฏิบัติการเมื่อเกิดภัยพิบัติ

ควรจัดให้มีการซ้อมปฏิบัติการตามแผน BCP และแผนปฏิบัติการเมื่อเกิดภัยพิบัติแก่ห้อง Data Center อย่างน้อยปีละ 1 ครั้ง โดยระหว่างการซ้อมจะต้องมีการบันทึกสิ่งที่เกิดขึ้นจริง รวมทั้งระยะเวลาที่ใช้ไปในแต่ละขั้นตอน ให้ละเอียด เพื่อนำผลการซ้อมมาวิเคราะห์และหาทางปรับปรุงแผนให้ดีขึ้นต่อไป

6.6 การจัดทำแผนกู้คืน

แผนกู้คืน (Disaster Recovery Plan – DRP) เป็นเอกสารแสดงขั้นตอนต่าง ๆที่เจ้าหน้าที่คอมพิวเตอร์จะต้องนำมาปฏิบัติตามเมื่อเกิดเหตุใด ๆที่ทำให้ server หยุดทำงาน การเขียนแผนนี้จะต้องระบุรายละเอียดขั้นตอนต่าง ๆที่เจ้าหน้าที่คอมพิวเตอร์ทุกคนเข้าใจและปฏิบัติตามได้เพื่อทำให้ได้ server ที่มีข้อมูลเดิมครบถ้วนนำกลับมาให้บริการเหมือนสภาวะปกติ โดยในแผนกู้คืนต้องกล่าวถึงขั้นตอนการดำเนินการดังตัวอย่างต่อไปนี้

- วิธีการจัดหา server ตัวใหม่โดยวิธีการเร่งด่วน (ในกรณีที่ server เดิมถูกทำลายทั้งหมด)
- การติดตั้งระบบปฏิบัติการให้เหมือนเครื่องเก่าทุกประการ
- การตั้งค่า configuration ของระบบปฏิบัติการให้เหมือนเครื่องเก่าทุกประการ
- การติดตั้งระบบฐานข้อมูลให้เหมือนเครื่องเก่าทุกประการ
- การตั้งค่า configuration ของระบฐานข้อมูลให้เหมือนเครื่องเก่าทุกประการ
- การนำข้อมูลสำรองลงให้เหมือนเครื่องเก่าทุกประการ
- การทดสอบว่าข้อมูลอยู่ครบทุกประการ
- การติดตั้งโปรแกรมให้เหมือนเครื่องเก่าทุกประการ
- การติดตั้ง driver ให้เหมือนเครื่องเก่าทุกประการ

การซ้อมปฏิบัติการตามแผนกู้คืน

ควรจัดให้มีการซ้อมปฏิบัติการตามแผนกู้คืนอย่างน้อยปีละ 1 ครั้ง โดยระหว่างการซ้อมจะต้องมีการบันทึกสิ่งที่เกิดขึ้นจริง รวมทั้งระยะเวลาที่ใช้ไปในแต่ละขั้นตอน ให้ละเอียด เพื่อนำผลการซ้อมมาวิเคราะห์และหาทางปรับปรุงแผนให้ดีขึ้นต่อไป

บทที่ 7 การจัดทำรายงานและการดูแลรักษาระบบอย่างต่อเนื่อง

การจัดทำรายงานการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล เป็นกิจกรรมที่สำคัญอย่างยิ่ง เพราะรายงานที่จัดทำจะเป็นหลักฐานที่สำคัญว่า โรงพยาบาลได้ดำเนินการครบถ้วน เหมาะสม ตามหลักเกณฑ์ มาตรฐาน และข้อกำหนดตามกฎหมายต่าง ๆ เรียบร้อยแล้ว โดยควรจัดทำรายงานเป็นรูปเล่มเอกสาร มีปก คำนำ สารบัญ และการอ้างอิงที่เหมาะสม จัดพิมพ์เป็นต้นฉบับเก็บไว้ในโรงพยาบาล เพื่อให้ผู้ตรวจสอบภายนอกได้ใช้ในการตรวจประเมินคุณภาพ หรือ ผลการดำเนินงานที่ผ่านมา

รายงานการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล ประกอบด้วย รายงาน 3 รูปแบบ ได้แก่

1. รายงานผลการดำเนินการให้เกิดความมั่นคงปลอดภัย
2. รายงานประจำปี
3. รายงานเมื่อเกิดเหตุภัยพิบัติ

7.1 รายงานผลการดำเนินการให้เกิดความมั่นคงปลอดภัย

รายงานรูปแบบนี้ จะแสดง ผลการทำกิจกรรมตั้งแต่การเริ่มต้นตรวจสอบสถานภาพปัจจุบันของระบบความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล ค้นหาช่องโหว่ จุดอ่อน ความเสี่ยง ทรัพยากรที่ขาดแคลน ต่อเนื่องไปสู่การปรับปรุง ปิดช่องโหว่ จุดอ่อน จัดการความเสี่ยง เสริมเติมทรัพยากรที่ขาดแคน สร้างเสริมความแข็งแกร่ง วางมาตรการป้องกัน กำหนดกระบวนการเฝ้าระวังและค้นหาภัยคุกคาม ต่อเนื่องไปสู่ การตอบสนองเมื่อเกิดเหตุวิกฤต แก้ไขปัญหา และฟื้นฟูระบบ รวมถึงการเรียนรู้และเกิดกลไกการพัฒนาอย่างต่อเนื่อง

รายงานผลการดำเนินการให้เกิดความมั่นคงปลอดภัย ควรมีรายงานฉบับต่าง ๆ ดังนี้

ก. รายงานการจัดทำและวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis)

ข. ทะเบียนทรัพยากรเทคโนโลยีสารสนเทศ (IT Assets) รวมทะเบียนข้อมูลที่สำคัญ

ค. รายงานผลการประเมินความเสี่ยงที่อาจเกิดขึ้นต่อทรัพยากรและข้อมูลที่สำคัญ

ง. แผนกลยุทธ์และแผนปฏิบัติการจัดการความเสี่ยง

จ. รายงานผลการดำเนินการจัดการความเสี่ยงในการพัฒนารอบแรก

ฉ. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ช. รายงานผลการเสริมสร้างการแข็งแกร่งของระบบ

ซ. รายงานผลการทดสอบการเจาะระบบ หลังการเสริมสร้างความแข็งแกร่ง

ซ. รายงานผลการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

ฌ. รายงานผลการซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์

ญ. รายงานผลการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ตามประมวลแนวทาง สกมช.

7.2 รายงานประจำปี

รายงานประจำปี เป็นการรายงานกิจกรรมที่ถูกกำหนดไว้ให้มีการดำเนินการเป็นประจำ อย่างน้อย ปีละ 1 ครั้ง เพื่อแสดงให้เห็นการดำเนินกิจกรรมด้านความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่า ไม่เกิดการหลงลืม หรือ ละเลยกิจกรรมที่สำคัญไป

รายงานประจำปี ควรมีรายงานฉบับต่าง ๆ ดังต่อไปนี้

ก. รายงานผลการประเมินความเสี่ยง ประจำปี

ข. รายงานผลการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ประจำปี

ค. รายงานผลการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ประจำปี

ง. รายงานผลการซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์ ประจำปี

จ. รายงานผลการซ้อมแผนดำเนินงานต่อเนื่อง (BCP) และแผนกู้คืน (DRP) ประจำปี

7.3 รายงานเมื่อเกิดเหตุภัยพิบัติ

รายงานเมื่อเกิดเหตุภัยพิบัติ ให้จัดทำรายงานเมื่อเกิดเหตุภัยพิบัติโดยทันที โดยภัยพิบัติที่ไม่รุนแรง สามารถแก้ไขได้โดยง่าย ให้จัดทำรายงานส่งให้ผู้บริหารองค์กร ส่วนภัยพิบัติที่รุนแรง ต้องส่งรายงานให้ สกมช. ได้รับทราบ และแบ่งปันข้อมูล บทเรียนให้ สังคมได้เรียนรู้และร่วมกันพัฒนาต่อไปนี้

รายงานเมื่อเกิดเหตุภัยพิบัติ ควรมีรายงานฉบับต่าง ๆ ดังต่อไปนี้

ก. รายงานเหตุภัยพิบัติ ส่งทันที เมื่อตรวจพบเหตุภัยพิบัติ

ข. รายงานผลการตรวจสอบภัยพิบัติ การแก้ไข และ การวางมาตรการป้องกันต่อไป ส่งเมื่อเสร็จสิ้นการจัดการภัยพิบัติแล้ว

7.4 การดูแลรักษาระบบอย่างต่อเนื่อง

ระบบงานใด ๆ ก็ตาม ไม่สามารถดำรงคงอยู่ได้ โดยปราศจากการดูแลรักษาระบบ เมื่อความตระหนักรู้ลดลง ความรู้สึกชาชินเริ่มเข้ามาเยือนผู้ปฏิบัติ มีอุปกรณ์หรือเครื่องมือใหม่เข้ามา ระบบที่เคยวางไว้อย่างดีก็อาจเสื่อมถอยลงได้ ดังนั้น ทีมดำเนินการให้เกิดความมั่นคงปลอดภัยไซเบอร์โรงพยาบาล จึงควรกำหนดมาตรการดูแลรักษาระบบให้สามารถป้องกันการเสื่อมถอยของระบบในอนาคตได้

การดูแลรักษาระบบอย่างต่อเนื่อง ควรมีองค์ประกอบอย่างน้อย ดังต่อไปนี้

1. มีระบบควบคุม กำกับ ติดตาม เช่น มีผู้ตรวจสอบงานว่า เจ้าหน้าที่ได้สำรองข้อมูลแบบ offline เป็นประจำหรือไม่ มีการวิเคราะห์ log file ตามกำหนดเวลาหรือไม่ ผู้ใช้งานระบบมีการตั้งรหัสผ่านให้ยากต่อการคาดเดาหรือไม่

2. กำหนดปฏิทินงาน ที่ต้องดำเนินการเป็นประจำทุกปี และประกาศให้ผู้เกี่ยวข้องได้รับทราบล่วงหน้า เช่น กำหนดวันซ้อมแผนแผนการรับมือภัยคุกคามทางไซเบอร์ วันสร้างความตระหนักรู้ประจำปี ฯลฯ

3. มีการทบทวนผลการดำเนินงานกิจกรรมด้านความมั่นคงปลอดภัยทุก ๆ วันสิ้นปีงบประมาณ แล้วสรุปผลการดำเนินงาน นำผลได้ที่มาปรับปรุงกิจกรรมในปีต่อไป ตามหลักการ Plan-Do-Check-Act (PDCA)

4. มีการนำเสนอผลการดำเนินกิจกรรมด้านความมั่นคงปลอดภัยไซเบอร์ที่สำคัญในที่ประชุมผู้บริหารทุกเดือน เช่น ผลการตรวจสอบเฝ้าระวังภัยคุกคาม ผลการจัดการความเสี่ยง ในแต่ละเดือน ผลการซ้อมแผนต่าง ๆ เป็นต้น

เอกสารอ้างอิง (REFERENCES)

1. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2564). ประกาศคณะกรรมการกากับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สาหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ. กรุงเทพฯ.ราชกิจจานุเบกษา เล่ม 138 ตอนพิเศษ 208 ง หน้า 9.

2. สมาคมเวชสารสนเทศไทย. (2565). แนวทางการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล. นนทบุรี. สมาคมเวชสารสนเทศไทย

3. Brown, Carol. (2012). Managing Information Technology, 7th Edition. New Jersey: Prentice Hall.

4. Ogu, Emmanuel C. (2022). Cybersecurity for eHealth. New York: Taylor & Francis Group.

5. Ayala, Luis. (2016). Cybersecurity for Hospitals and Healthcare Facilities. Las Vegas, Springer, Apress.

ภาคผนวก

โครงร่าง แผนดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan - BCP)

โครงร่าง แผนกู้คืน (Disaster Recovery Plan - DRP)

โครงร่าง แผนดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan - BCP)

แผนดำเนินธุรกิจอย่างต่อเนื่อง เป็นเอกสารรวบรวมขั้นตอนการทำงานของทุกหน่วยงานที่สำคัญในการให้บริการผู้ป่วย เมื่อเกิดเหตุการณ์ที่ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลล่ม ใช้การไม่ได้ทั้งระบบหรือบางส่วน แต่โรงพยาบาลยังคงต้องเปิดบริการผู้ป่วยให้ได้ใกล้เคียงกันสภาวะปกติ จึงต้องกำหนดขั้นตอนให้กับหน่วยงานต่าง ๆ ตามแนวทางดังนี้

1. เปลี่ยนขั้นตอนการใช้คอมพิวเตอร์ มาเป็นการเขียนข้อมูลลงในกระดาษ โดยควรมีแบบฟอร์มเปล่าที่จำเป็นเตรียมไว้จำนวนหนึ่ง ทุกหน่วยงาน

2. กำหนดขั้นตอน รายละเอียดการบันทึก ให้เจ้าหน้าที่ของทุกหน่วย สามารถอ่านขั้นตอน และทำตามได้โดยไม่ขาดขั้นตอนที่สำคัญ

3. ในกรณีที่ต้องเรียกดูข้อมูลบางอย่างจากคอมพิวเตอร์ ให้เตรียมข้อมูลนั้นในรูปแบบกระดาษ หรือเตรียมไว้ในเครื่อง notebook ที่ทำสำรองไว้ให้เปิดดูได้ เช่น รายการยาและราคายาทั้งหมดของโรงพยาบาล ฯลฯ

4. กำหนดขั้นตอนส่งต่อข้อมูลระหว่างหน่วยงานให้ชัดเจน

5. กำหนดวิธีการบันทึกข้อมูลจากกระดาษเข้าสู่ระบบ เมื่อระบบเทคโนโลยีกลับมาทำงานได้ตามปกติ โดยต้องคำนึงถึงการบันทึกเวลาที่เกิดกิจกรรมจริง ระมัดระวังการที่ระบบจะใช้เวลาของเครื่องบันทึกแทนเวลาทำกิจกรรม

หน่วยงานที่จำเป็นต้องมีแผน ในกรณีบริการผู้ป่วยนอกประกอบด้วยหน่วยงานดังต่อไปนี้

1. ห้องบัตร เวชระเบียน ฝ่ายตรวจสอบสิทธิ์
2. ห้องตรวจโรคผู้ป่วยนอก จุดพยาบาลบันทึกเวลา จุดแพทย์บันทึกข้อมูลวินิจฉัยและสั่งการรักษา
3. ห้อง Lab
4. ห้องเอ็กซเรย์
5. ห้องจ่ายยาผู้ป่วยนอก
6. แผนกการเงินผู้ป่วยนอก
7. ห้องฉุกเฉิน ห้องทำแผล ห้องทำหัตถการผู้ป่วยนอก

หากมีระบบเทคโนโลยีสารสนเทศที่ครอบคลุมไปถึงบริการผู้ป่วยใน ก็ต้องกำหนดทุกหน่วยงานที่เกี่ยวข้องเข้ามาในแผนด้วย โดยทุกหน่วยงานที่เกี่ยวข้อง ต้องมีเอกสารแบบฟอร์มเปล่า รวมถึงเอกสารขั้นตอนการปฏิบัติการชัดเจน อาจเก็บในกล่องฉุกเฉินเอาไว้ และสามารถนำไปใช้ได้เมื่อต้องการโดยทันที

โครงร่าง แผนกู้คืน (Disaster Recovery Plan - DRP)

แผนกู้คืน เป็นเอกสารที่แสดงรายละเอียดขั้นตอนต่าง ๆ ที่เขียนไว้ให้เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศสามารถอ่าน และดำเนินการตามขั้นตอนที่เขียนไว้ในแผน เพื่อนำระบบกลับมาดำเนินการเป็นปกติได้ อย่างไรก็ตาม การกู้คืนระบบ จะต้องมีการใช้ข้อมูลสำรองที่ได้เก็บสำรองไว้ล่วงหน้า หากไม่มีข้อมูลสำรอง ก็จะได้แต่ระบบที่กลับมาทำงาน โดยข้อมูลเก่าหายไปทั้งหมด

แผนกู้คืน มีหลายระดับ ตั้งแต่การกู้คืนบางส่วน ไปจนถึงการกู้คืนทั้งหมด โรงพยาบาลควรมีแผนกู้คืนที่ครอบคลุมการกู้คืนทั้งหมด โดยเฉพาะการกู้คืนเครื่องแม่ข่ายของระบบเทคโนโลยีสารสนเทศโรงพยาบาล (Hospital Information System – HIS Sever)

แผนกู้คืนทั้งหมด จะจำลองสถานการณ์ว่า เครื่องแม่ข่ายถูกโจมตีด้วย ransomware ระหว่างรอการแก้ไขจะสร้างเครื่องแม่ข่ายใหม่ให้ใช้ทดแทนเครื่องเก่าให้ได้ จึงต้องมีการกำหนดขั้นตอนที่สำคัญดังต่อไปนี้

1. การสรรหาเครื่องแม่ข่ายใหม่ ที่มีคุณลักษณะใกล้เคียงเครื่องเดิม (อาจต้องทำสัญญากับบริษัทภายนอก ให้เตรียมไว้ล่วงหน้า)
2. การติดตั้งระบบปฏิบัติการเข้าเครื่องแม่ข่าย (ต้องจัดเตรียมโปรแกรมติดตั้ง version เดิม ไว้ล่วงหน้า)
3. การทำ configuration ระบบปฏิบัติการให้เหมือนเดิม (ต้องบันทึก config ไว้ก่อนแล้ว)
4. การติดตั้งฐานข้อมูลล่าสุดที่สำรองไว้
5. การติดตั้งระบบ HIS
6. การทำ configuration ระบบ HIS ให้เหมือนเดิม (ต้องบันทึก config เดิมไว้ล่วงหน้า)
7. การทดสอบระบบว่ากลับมาเป็นปกติ ก่อนประกาศให้ผู้ใช้ทราบ

ขั้นตอนที่เขียนไว้ในแผนกู้คืน จะต้องมีรายละเอียดมากเพียงพอ โดยอาจทดสอบให้เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศจากโรงพยาบาลอื่น ที่ไม่เคยรู้จักระบบของโรงพยาบาลมาก่อน อ่านขั้นตอนและทำตามขั้นตอนในแผนกู้คืน หากสามารถทำได้และนำระบบกลับมาใช้งานได้จากการอ่านแผนนี้ ก็จะถือว่าแผนกู้คืนนี้เป็นแผนที่ใช้งานได้จริง