	โรงพยาบาลเวียงแหง	รหัส SOP-IT-002 Version 1	ออกโดย งานช่างเทคนิค
	แนวทางการปฏิบัติหาเกิดเหตุฉุกเฉินเกี่ยวกับระบบอินเตอร์เน็ต หรือ ระบบสารสนเทศของหน่วยงาน	ประกาศวันที่ 1/2/2566	เขียนโดย : นายกฤตกร พรหมนิล นักวิชาการคอมพิวเตอร์
ผู้ตรวจสอบ : นายฐิติพงศ์ ศิริลักษณ์ (เภสัชกรชำนาญการ)		อนุมัติ : นายพิสิษฐ์วุฒิ อยุทธ์ (ผู้อำนวยการโรงพยาบาลเวียงแหง)	

แนวทางการปฏิบัติหากเกิดเหตุฉุกเฉินเกี่ยวกับระบบอินเตอร์เน็ต หรือ ระบบสารสนเทศของหน่วยงาน

วัตถุประสงค์

1. เพื่อเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบสารสนเทศขององค์กร
2. เพื่อลดระดับความเสียหายที่อาจจะเกิดขึ้นได้กับระบบเทคโนโลยีสารสนเทศ
3. เพื่อให้บริการผู้ป่วยได้ตามปกติโดยไม่กระทบต่อการบริการ
4. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติงาน ในการดูแลรักษาระบบสารสนเทศขององค์กร
5. เพื่อใช้เป็นแนวทางการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศในองค์กรให้มีเสถียรภาพและความพร้อมสำหรับการใช้งานรวมทั้งการบริการ

ขอบเขต

เป็นแนวทางปฏิบัติสำหรับการป้องกันความเสี่ยง ในเรื่องทางการปฏิบัติหาเกิดเหตุฉุกเฉินเกี่ยวกับระบบอินเตอร์เน็ต หรือ ระบบสารสนเทศของหน่วยงาน

ผู้รับผิดชอบ

เจ้าหน้าที่งาน IT และเจ้าหน้าที่ผู้ใช้คอมพิวเตอร์

ขั้นตอนทำงาน

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบสารเทคโนโลยีสารสนเทศ (IT Contingency Plan) จัดทำขึ้นสำหรับเป็นกรอบการแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อการบริการและระบบสารเทคโนโลยีสารสนเทศในองค์กร ประกอบด้วย

1. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น

3. การเตรียมความพร้อม
4. การกำหนดหน้าที่รับผิดชอบและผู้รับผิดชอบเมื่อเกิดเหตุการณ์ฉุกเฉิน
5. ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ
6. แผนการกู้คืนข้อมูล
7. การติดตามและรายงานผล

1. การวิเคราะห์ปัญหาความรุนแรงของเหตุการณ์ภัยพิบัติ

1.1 วิเคราะห์เหตุการณภัยพิบัติ ภัยพิบัติอาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารถสนเทศของโรงพยาบาล จำแนกเป็น 2 กลุ่มหลักๆ ได้แก่

<u>ภัยพิบัติจากภายนอก</u>

- ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่อสถานที่ตั้งของเครื่องแม่ข่าย ได้แก่ ภัยพิบัติอัคคีภัย อุทกภัย การจลาจล ชุมนุมประท้วง แผ่นดินไหว ฯลฯ
- ระบบเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง
- การบุกรุกหรือโจมตีระบบควบคุมเทคโนโลยีสารสนเทศจากภายนอก เพื่อสร้างความเสียหายหรือทำลายระบบข้อมูล
- ระบบกระแสไฟฟ้าขัดข้อง /ไฟฟ้าดับ /ไฟกระชาก
- ไวรัสคอมพิวเตอร์

<u>ภัยพิบัติจากภายใน</u>

- ระบบเครื่องแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย ถูกทำลาย
- ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในโรงพยาบาล
- เจ้าหน้าที่หรือบุคลากรของโรงพยาบาล ขาดความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์ทั้งด้าน ฮาร์ดแวร์และซอฟต์แวร์อาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย

1.2 การประเมินสถานการณ์และกำหนดลักษนะความรุนแรง

การวิเคราะห์เหตุการณ์ฉุกเฉินและภัยพิบัติแล้ว จะทำให้เกินประเมินลำดับคำวามรุนแรงของภัยพิบัติหรืออุบัติการที่เกิดขึ้น เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ไม่ปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ โดยเจ้าหน้าที่งาน IT มาสรุปเป็นข้อมูลดังนี้

สถานการณ์หรือ ภาวะฉุกเฉิน	**ระดับความรุนแรง (คะแนน 5 คะแนน)**			**จัดลำดับ**	
	ต่อระบบงาน	หน่วยงาน	ต่อผู้ป่วย	รวม	ลำดับ
กรณีไฟไหม้	5	5	5	15	1
กรณีโดนแทรกแซงระบบ	5	4	3	12	2
กรณีแผ่นดินไหว	5	3	2	10	3
กรณีไฟฟ้าดับ เกิน 24 ชั่วโมง	3	2	3	8	4
กรณีเกิดจลาจล ชุมนม/ความไม่สงบ สงคราม	2	2	3	7	5
กรณีระบบขัดข้อง เกิน 3 ชั่วโมง	2	2	2	6	6
กรณีระบบขัดข้อง ไม่เกิน 1 ชั่วโมง	2	2	1	5	7

แบบประเมินความรุนแรง

สถานการณ์หรือ ภาวะฉุกเฉิน	**ระดับความรุนแรง (คะแนน 5 คะแนน)**			รวม
	ต่อระบบงาน	ต่อหน่วยงาน	ต่อผู้ป่วย	
ผู้ประเมิน..... วันที่และเวลาที่ประเมิน.....				

การจัดลำดับสถานการณ์หรือฉุกเฉินโดยแบ่งคะแนนเป็น 3 กลุ่ม

1. สถานการณ์หรือฉุกเฉินระดับความรุนแรงไม่สามาถจัดการได้ในหน่วยงาน ต้องพึ่งพาหน่วยงานอื่น **ได้คะแนน 11-15 คะแนน (รุนแรง)**
2. สถานการณ์หรือฉุกเฉินสามาถจัดการได้ในหน่วยงาน **ได้คะแนน 6-10 คะแนน (ฉุกเฉิน)**
3. สถานการณ์หรือฉุกเฉินสามาถจัดการได้ในกลุ่มงานของตนเอง **ได้คะแนน 1-5 คะแนน (ทั่วไป)**

2.ขั้นตอนและแนวทางการป้องกันเบื้องต้น

2.1 การประกาศใช้แผน

โรงพยาบาลเวียงแหง มีการประกาศแผนการรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ อย่างเป็นทางการเพื่อให้เจ้าหน้าที่ทุกคนทราบถึงเหตุและปฏิบัติตามอย่างเคร่งครัดเหมาะสม โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการโรงพยาบาลจะทำการแจ้งไปยังหัวหน้างานและเจ้าหน้าที่ ทราบเพื่อพิจารณาประกาศใช้แผนต่อไป

- **ขั้นตอนหากเกิดสถานการณ์หรือฉุกเฉินที่ได้คะแนน 11-15 คะแนน (รุนแรง)**
  1. หากเกิดสถานการณ์หรือฉุกเฉิน ให้แจ้งหัวหน้างานและผู้อำนวยการหน่วยงานเพื่อให้ทราบถึงสถานการณ์หรือฉุกเฉินที่เกิดขึ้น
  2. ประกาศใช้แผนเพื่อแจ้งให้ทราบถึงสถานการณ์หรือฉุกเฉินที่เกิดขึ้น
  3. แจ้งงาน IT เพื่อเข้าตรวจสอบระบบเทคโนโลยีรสารสนเทศในความดูแล
  4. หากเป็นภัยพิบัติ เช่น ไฟไหม้ น้ำท่วม แผนดินไหว เหตุจลาจน ภาวะสงคราม ให้กลุ่มงานเคลื่อนย้ายอุปกรณ์ไปยังที่ปลอดภัยโดยเรียงลำดับตามการจัดลำดับความสำคัญ

  <u>นิยามความรุนแรง</u>

  ไม่สามารถแก้ไขปัญหาได้ในหน่วยงาน ต้องพึ่งพาหน่วยงานอื่น เกิดอันตรายต่อชีวิตหรือทรัพย์สิน ต้องมีการอพยพ
- **ขั้นตอนหากเกิดสถานการณ์หรือฉุกเฉินที่ได้คะแนน 6-10 คะแนน (ฉุกเฉิน)**
  1. หากเกิดสถานการณ์หรือฉุกเฉิน ให้แจ้งหัวหน้างาน
  2. ประกาศใช้แผนเพื่อแจ้งให้ทราบถึงสถานการณ์หรือฉุกเฉินที่เกิดขึ้น
  3. แจ้งงาน IT เพื่อเข้าตรวจสอบระบบเทคโนโลยีรสารสนเทศในความดูแล

  <u>นิยามความรุนแรง</u>

  สามารถแก้ไขปัญหาได้ด้วยตนเองในหน่วยงานโดยใช้เจ้าหน้าที่เฉพาะทาง เกิดความเสียหาต่อทรัพย์สินหรือข้อมูลผู้ป่วย
- **ขั้นตอนหากเกิดสถานการณ์หรือฉุกเฉินที่ได้คะแนน 1-5 คะแนน (ทั่วไป)**
  1. หากเกิดสถานการณ์หรือฉุกเฉิน ให้แจ้งหัวหน้างานทราบ
  2. แก้ไขปัญหาด้วยต้นเอง
  3. แจ้งงาน IT เพื่อขอคำแนะนำในการแก้ไขปัญหา

นิยามความรุนแรง

สามารถแก้ไขปัญหาได้ด้วยตนเองหรือเพียงแต่ขอคำแนะนำจากเจ้าหน้าที่เฉพาะทาง

2.2 กำหนดขั้นตอนการดำเนินงาน

โรงพยาบาลเวียงแหง จัดเตรียมขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ฉุกเฉินหรือผิดปกติในโรงพยาบาลโดยกำหนดขั้นตอนการปฏิบัติที่เหมาะสมต่อสถานการณ์ต่างๆ ที่เกิดขึ้น รวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุก เพื่อให้สามารถยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลา รวมถึงการเตรียมอุปกรณ์สำรองเพื่อใช้ในการกู้คืนระบบ

2.3 การติดต่อประสานงาน

มีการจัดทำข้อมูลรายชื่อหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัย กรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า , สถานีดับเพลิง , สถานีตำรวจ เป็นต้น

2.4 การจัดเตรียมอุปกรณ์

เจ้าหน้าที่สารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย คอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเกิดขัดข้องใช้งานไม่ได้ ดังนี้

- เครื่องคอมพิวเตอร์ PC/เครื่องคอมพิวเตอร์ Notebook
- แผ่นติดตั้งระบบปฏิบัติการ/ ระบบปฏิบัติการของเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
- อุปกรณ์สำรองข้อมูลและระบบงานที่สำคัญ
- โปรแกรม antivirus
- ระบบสำรองไฟฟ้าอัตโนมัติ
- อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

2.5 สำรองข้อมูล

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลเกิดความเสียหาย ถูกทำลายจากไวรัส หรือผู้บุกรุกแทรกแซง เปลี่ยนแปลงข้อมูล และสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยโรงพยาบาลเวียงแหง มีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์ และแผนการสำรองข้อมูล ดังนี้

1. การสำรองฐานข้อมูลผู้ป่วย ทุกวัน
2. การสำรองข้อมูลเครือข่าย (Configuration)

2.6 การป้องกันและกำจัดไวรัส

มีการติดตั้งซอฟต์แวร์ป้องกันและกำจัดไวรัส สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ ลูกข่ายที่เชื่อมต่อในระบบเครือข่าย โดยผู้ใช้งานต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่ออินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้บุกรุกสามารถเข้ามาทำลายระบบได้

2.7 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

1) กำหนดมาตรการควบคุมการเข้า – ออก ห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหายโดยห้องควบคุมจะมีกุญแจ เพียง 1 ชุดเท่านั้น กรณีที่ผู้เกี่ยวข้องต้องการเข้าไปในห้องควบคุมต้องลงชื่อเบิกกุญแจ ในสมุดควบคุมการเข้า – ออก ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็น ให้เจ้าหน้าที่ของเจ้าหน้าที่สารสนเทศ เป็นผู้รับผิดชอบพาเข้าไป ในห้องควบคุมมีการติดตั้งกล้องโทรทัศน์วงจรปิด

2) มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ได้ โดยกำหนดให้ Firewall ควบคุมการเข้า-ออก หรือการควบคุมการรับ-ส่งข้อมูล ในระบบเครือข่ายและเปิดใช้งานตลอดเวลา

3) มีการติดตั้ง **IPS (Intrusion Prevention System)** เพื่อให้ตรวจสอบการบุกรุกโดยจะทำงานคล้ายๆกับ IDS แต่จะมีคุณสมบัติพิเศษในการจู่โจมกลับหรือหยุดยั้งผู้บุกรุกได้ด้วยตัวเองโดยที่ไม่จำเป็นต้องอาศัยโปรแกรมหรือ Hardware ตัวอื่นๆ

4) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบการใช้งานข้อมูลบนเครือข่ายอินเตอร์เน็ตของโรงพยาบาลเพื่อตรวจสอบการใช้งานบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและหาวิธีการป้องกันต่อไป

5) การดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยได้จัดหาระบบบริหารจัดเก็บข้อมูล Log (Central Log Management) เพื่อตรวจสอบ ติดตามการวิเคราะห์ (Log File) และการเฝ้าระวังในครือข่าย (Network Monitoring) เพื่อเพิ่มประสิทธิภาพในการดูแลระบบเครือข่ายของโรงพยาบาล

2.8 การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว จลาจล ชุมนุมประท้วง

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว โดยเตรียมอุปกรณ์ดังนี้

1) สำรองฐานข้อมูล ผู้ป่วย

2) ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน

3) ศึกษาแผน/ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจน

2.9 การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เพื่อเป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบเทคโนโลยีสารสนเทศและอุปกรณ์เครือข่ายคอมพิวเตอร์ ได้กำหนดแนวทาง ดังนี้

1) ติดตั้งเครื่องสำรองไฟฟ้าอัตโนมัติ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์อุปกรณ์เครือข่าย หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ 120 นาที

2) ติดตั้งเครื่องกำเนิดไฟฟ้าสำรอง (Generator)

3) เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

4) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

3. การเตรียมความพร้อม

3.1 การเตรียมความพร้อมกรณีเกิดการแทรกแซงจากภายนอก

เมื่อเกิดเหตุโจมตี บุกรุก ให้ดำเนินการ ดังนี้

1) สกัดกั้นการเข้าถึงเครื่องให้บริการ เพื่อไม่ให้เกิดการเปลี่ยนแปลงของข้อมูล ด้วยการถอดสาย Network ออกจากเครื่อง

2) ตรวจสอบความเปลี่ยนแปลงของข้อมูลในระบบ

3) ตรวจสอบ Log File หรือ แฟ้มกิจกรรมของระบบ เพื่อดูพฤติกรรมที่น่าสงสัย

4) ดำเนินการปิดช่องโหว่บนหน้าเว็บไซต์โดยให้คำนึงถึงสิ่งต่างๆ ดังนี้

- การตรวจสอบการป้อนข้อมูล - SQL Injection - XSS (Cross Site Scripting)

5) หากไม่สามารถดำเนินการแก้ไขได้โดยเร็ว ให้ทำการปิดการใช้งานในส่วนที่เกิดปัญหาก่อน ปรับปรุง ซอฟต์แวร์ที่เกี่ยวข้องให้เป็นรุ่นล่าสุดที่มีความมั่นคงปลอดภัยสูง

6) หากไม่สามาถแก้ไขได้ให้ขอความช่วยเหลือจากหน่วยงานอื่น

3.2 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากกรณีไฟฟ้าดับ เกิด 24 ชั่วโมง

กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศฯดังนี้

1) เปิดเครื่องสำรองไฟฟ้าอัตโนมัติ เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจ เกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์ แม่ข่าย (Server) ซึ่งมีระยะในเวลาในการสารองไฟฟ้าโดยประมาณ 120 นาที

2) ติดตั้งเครื่องกำเนิดไฟฟ้าสรอง (Generator) และ ตรวจสอบจำนวนน้ำมันเพื่อให้เพียงพอต่อการใช้งาน

3) เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษา เครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

4) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ

5) กำหนดให้มีการสำรองฐานข้อมูลโรงพยาบาลทุก 1 วัน และระบบงานต่าง ๆ ทุก 1 สัปดาห์ เป็นอย่างน้อย

3.3 การเตรียมความพร้อมรับสถานการณ์ภัยจากแผ่นดินไหว

เตรียมความพร้อม โดยติดตามสถานการณ์รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น ดังนี้

1) ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัยจาก หน่วยงานที่เกี่ยวข้องและข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทาง ปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง เชื่อมโยงไปถึงเว็บไซต์/ แอพพลิเคชั่น ของหน่วยงานต่างๆ เช่น กรมอุตุนิยมวิทยา ศูนย์เตือนภัยพิบัติแห่งชาติกรมป้องกันและบรรเทาสาธารณภัย

2) การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ ให้ดำเนินการแก้ไข เพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

3) อบรม ให้ความรู้เกี่ยวกับการปฏิบัติเมื่อเกิดแผ่นดินไหว แก่เจ้าหน้าที่ บุคลากรภายในองค์กร การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจล เพื่อติดตามสถานการณ์รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและ ก่อจลาจล

3.1) ดำเนินการค้นหาข่าวจากแหล่งข่าวต่าง ๆเช่น ตำรวจ นักข่าว โทรทัศน์และหน่วยงานที่ เกี่ยวข้อง

3.2) จัดเตรียมกำลังเจ้าหน้าที่ วัสดุอุปกรณ์เครื่องมือเครื่องใช้ระบบการสื่อสารยานพาหนะ และ มอบหมายหน้าที่ความรับผิดชอบ

3.3) ติดตั้งระบบกล้องวงจรปิดเพื่อรักษาความปลอดภัย เตรียมความพร้อมในการเสริมสร้างความมั่งคงปลอดภัยให้กับระบบระบบเครือข่าย ติดตั้งโปรแกรมสำหรับติดตามการทำงานของระบบคอมพิวเตอร์ และบริหารจัดการอุปกรณ์เครือข่าย (Solar Winds Network Monitoring) โดยอาศัยโปรโตคอล SNMP เพื่อตรวจสอบสถานะของอุปกรณ์ เครือข่ายในระบบ ซึ่งจะช่วยให้ผู้ดูแลระบบนั้นสามารถที่จะพบปัญหาหรือตรวจสอบปัญหาได้อย่างรวดเร็ว 10 การใช้งานโดยทั่วไป สำหรับผู้ใช้งานเครือข่าย

- จัดให้มีการอบรมเพื่อเสริมสร้างสมรรถนะในการใช้งานเทคโนโลยีสารสนเทศ เพื่อพัฒนาทักษะ ความรู้ ความเข้าใจ ในด้านเทคโนโลยีสารสนเทศให้แก่บุคลากรของโรงพยาบาล เพื่อให้ เจ้าหน้าที่ที่ได้รับการฝึกอบรมสามารถนำไปใช้ในการปฏิบัติงานได้อย่างเหมาะสมและมีประสิทธิภาพมากยิ่งขึ้น
- สร้างความรู้ ความเข้าใจ แก่เจ้าหน้าที่ ในหน่วยงานและองค์กร ให้มีความรู้ความเข้าใจกับการเตรียมความพร้อมหากเกิดภัยพิบัติ

3.4 การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและ ก่อจลาจล

1) ดำเนินการค้นหาข่าวจากแหล่งข่าวต่าง ๆเช่น ตำรวจ นักข่าว โทรทัศน์และหน่วยงานที่เกี่ยวข้อง

2) จัดเตรียมกำลังเจ้าหน้าที่ วัสดุอุปกรณ์เครื่องมือเครื่องใช้ระบบการสื่อสารยานพาหนะ และ มอบหมายหน้าที่ความรับผิดชอบ

3.5 เตรียมความพร้อมในการเสริมสร้างความมั่งคงปลอดภัยให้กับระบบระบบเครือข่าย

ติดตั้งโปรแกรมสำหรับติดตามการทำงานของระบบคอมพิวเตอร์ และบริหารจัดการอุปกรณ์เครือข่าย เพื่อตรวจสอบสถานะของอุปกรณ์ เครือข่ายในระบบ ซึ่งจะช่วยให้ผู้ดูแลระบบนั้นสามารถที่จะพบปัญหาหรือตรวจสอบปัญหาได้อย่างรวดเร็ว

4.การใช้งานโดยทั่วไป

สำหรับผู้ใช้งานเครือข่าย

1. จัดให้มีการอบรมเพื่อเสริมสร้างสมรรถนะในการใช้งานเทคโนโลยีสารสนเทศ เพื่อพัฒนาทักษะ ความรู้ ความเข้าใจ ในด้านเทคโนโลยีสารสนเทศให้แก่บุคลากรของกรมส่งเสริมคุณภาพสิ่งแวดล้อม เพื่อให้เจ้าหน้าที่ที่ได้รับการฝึกอบรมสามารถนำไปใช้ในการปฏิบัติงานได้อย่างเหมาะสมและมีประสิทธิภาพมากยิ่งขึ้น

2. สร้างความรู้ ความเข้าใจ แก่เจ้าหน้าที่กรมส่งเสริมคุณภาพสิ่งแวดล้อม ให้มีความตระหนักในการใช้งาน เทคโนโลยีสารสนเทศอย่างปลอดภัย โดยกำหนดให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ของข้อมูลและปลอดภัยสารสนเทศของกรมส่งเสริมคุณภาพสิ่งแวดล้อม แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความ รับผิดชอบของผู้ใช้งาน

ข้อ 1 ผู้ใช้งาน ปฏิบัติตามแนวทางการใช้งานหรือห้ามใช้งานโปรแกรมคอมพิวเตอร์

ข้อ 2 ผู้ใช้งาน ปฏิบัติตามเงื่อนไขการใช้งานและไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น

ข้อ 3 ผู้ใช้งาน กำหนดหรือใช้งานรหัสผ่านโดยปฏิบัติ (แนวปฏิบัติสำหรับการตั้งและใช้งาน รหัสผ่าน)

ข้อ 4 ผู้ใช้งาน ตรวจสอบและป้องกันไวรัสโดยปฏิบัติ (แนวปฏิบัติสำหรับการป้องกันไวรัส)

ข้อ 5 ผู้ใช้งาน ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การขโมย การสูญหาย หรือการเสียหายของข้อมูล เอกสาร คอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์ของโรงพยาบาล

ข้อ 6 ผู้ใช้งาน ป้องกันอุปกรณ์หรือเครื่องคอมพิวเตอร์แบบพกพาซึ่งสินทรัพย์เป็นของโรงพยาบาล

ข้อ 7 ผู้ใช้งาน ใช้ระบบ HIS ของโรงพยาบาลจะต้องรักษาความลับและข้อมูลของผู้ป่วย

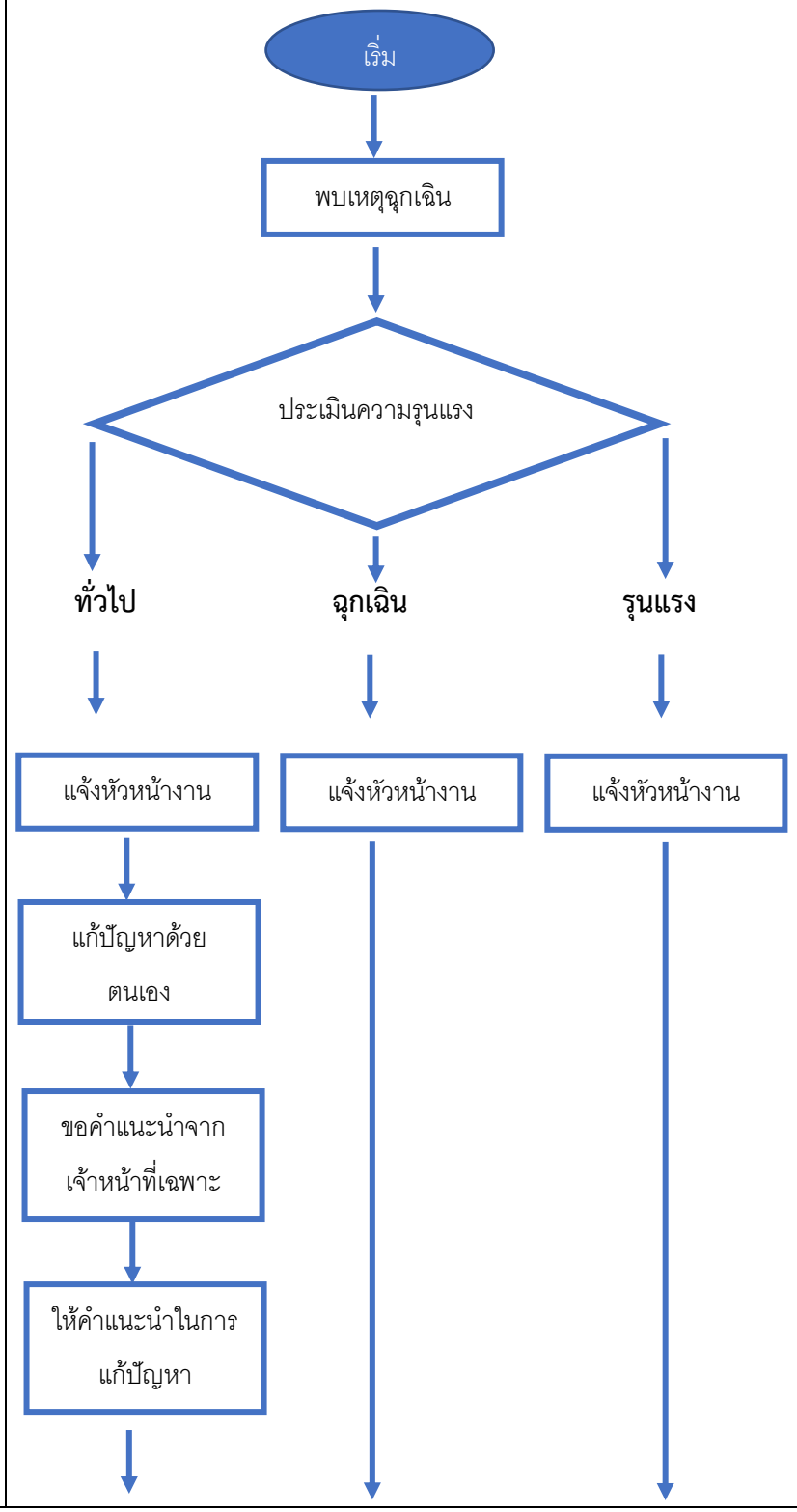
ข้อ 8 ผู้ใช้งาน ห้ามใช้งานระบบเทคโนโลยีสารสนเทศ อินเทอร์เน็ต และเครือข่ายของโรงพยาบาล ในลักษณะที่ผิดวัตถุประสงค์ (แนวปฏิบัติสำหรับการป้องกันการใช้งานระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์)

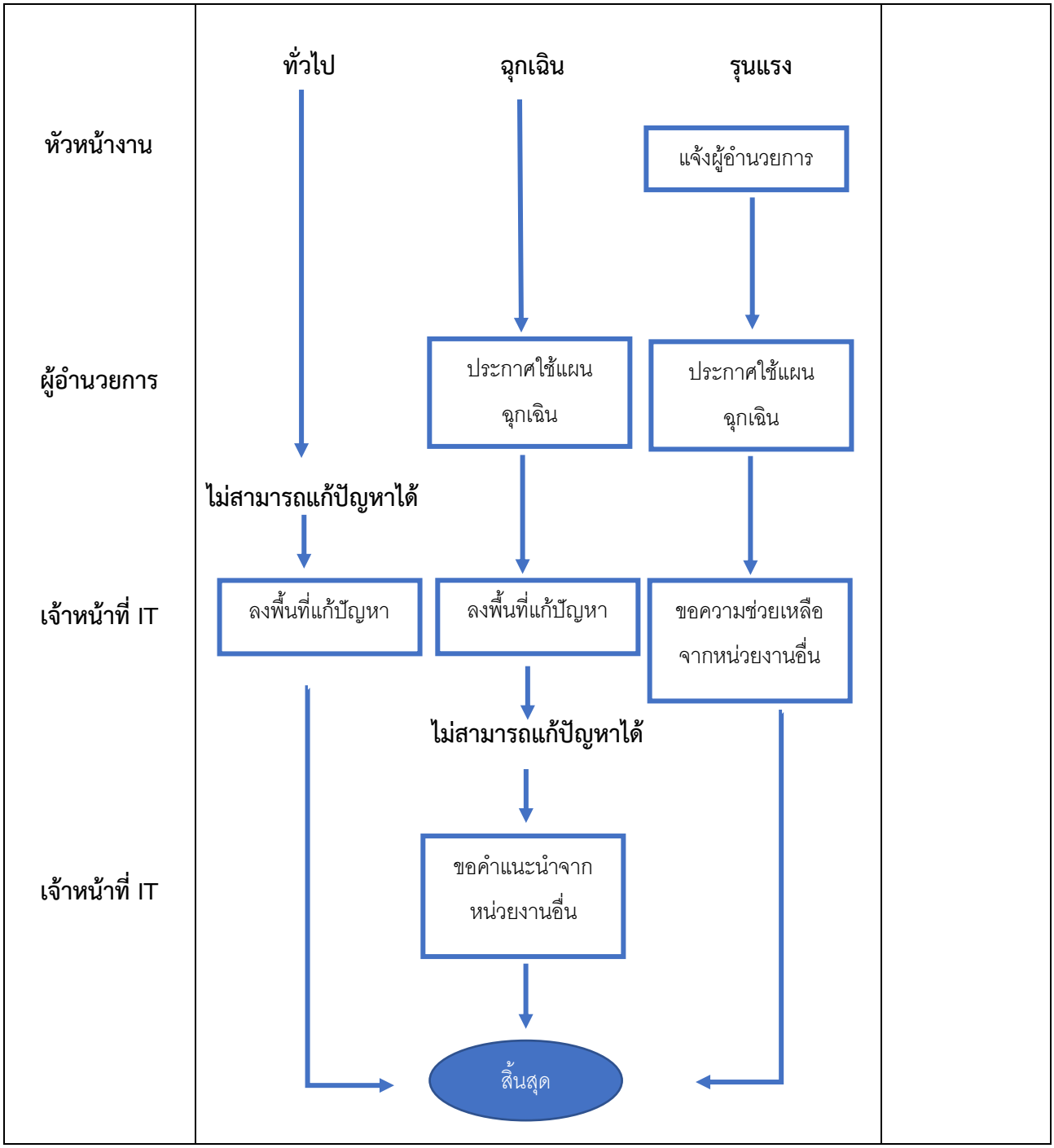
ข้อ 10 ในการจัดการในโรงพยาบาล ตามชั้นความลับ ผู้ใช้งานข้อมูล ปฏิบัติตามแนวปฏิบัติใน การบริหารจัดการข้อมูลตามระดับชั้นความลับ ที่โรงพยาบาล ได้กำหนดไว้

ข้อ 11 เมื่อผู้ใช้งานพบเหตุการณ์หรือจุดอ่อนด้านความมั่นคงปลอดภัย ให้รีบแจ้งไปยังกลุ่มระบบคอมพิวเตอร์ หรือเจ้าหน้าที่สารสนเทศโดยทันทีที่พบเห็น

ข้อ 12 ผู้ดูแลเครื่องหรืออุปกรณ์คอมพิวเตอร์ ต้องดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ ที่ได้รับผิดชอบ เพื่อดูว่ายังอยู่ในสภาพที่ใช้งานได้ตามปกติหรือไม่ หากเกิดการชำรุดหรือเสียหาย ให้ตรวจสอบว่าเป็นการเสียหายตามสภาพการใช้งานหรือไม่ หากเป็นการชำรุดหรือเสียหายโดยประมาทหรือ เลินเล่อ ให้แจ้งหน่วยงานพัสดุหรือ แจ้งซ่อมหากเกิดความเสียหายเพื่อและให้ผู้รับผิดชอบในงานสารสนเทศและเทคโนโลยีดำเนินการสอบสวนต่อไป

6.แผนภาพแนวทางการปฏิบัติหาเกิดเหตุฉุกเฉินเกี่ยวกับระบบอินเตอร์เน็ต หรือ ระบบสารสนเทศของหน่วยงาน

ผู้รับผิดชอบ	แผนภาพปฏิบัติงาน	เอกสารที่เกี่ยวข้อง
เริ่ม เจ้าหน้าที่ เจ้าหน้าที่ เจ้าหน้าที่ เจ้าหน้าที่ เจ้าหน้าที่ เจ้าหน้าที่ IT		แบบประเมินความรุนแรง



6.ตัวชี้วัด

6.1 อุบัติการณ์ความเสี่ยง ฉุกเฉินเกี่ยวกับระบบอินเตอร์เน็ต หรือ ระบบสารสนเทศของหน่วยงาน ในระดับ **ฉุกเฉิน** 0 ครั้งต่อปี

6.2 อุบัติการณ์ความเสี่ยง ฉุกเฉินเกี่ยวกับระบบอินเตอร์เน็ต หรือ ระบบสารสนเทศของหน่วยงาน ในระดับ **รุนแรง** 0 ครั้งต่อปี