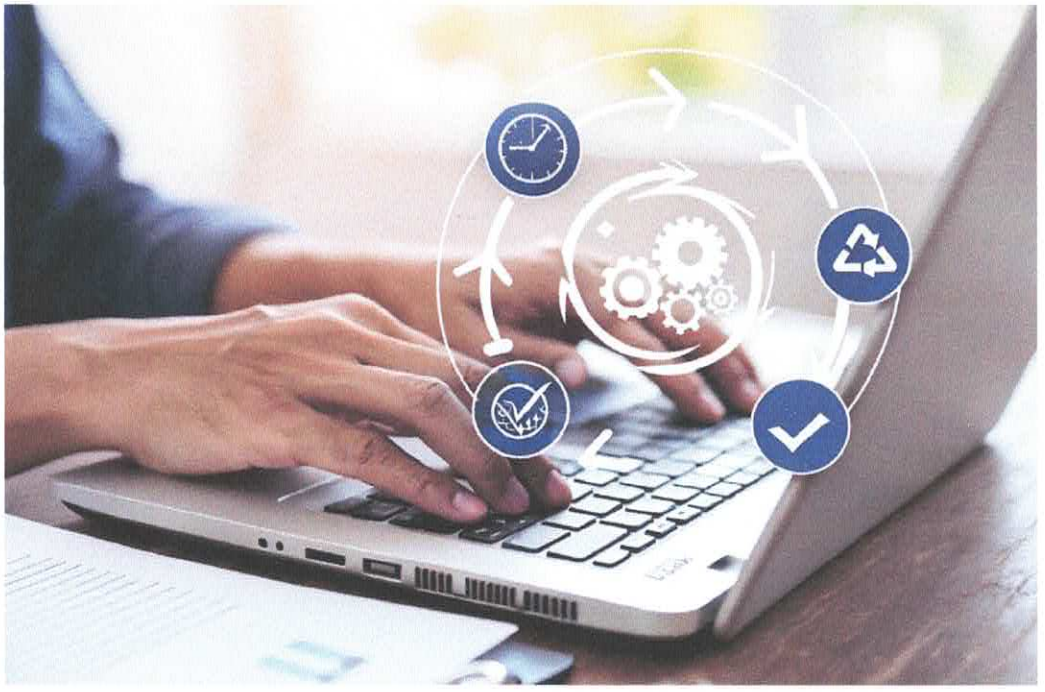
โรงพยาบาลพระมงกุฎเกล้า
Phramongketklao Hospital

แผนดำเนินงานกรณีระบบสารสนเทศล่มเมื่อเกิดภาวะวิกฤต

(Business Continuity Plan : BCP)

หน่วยงาน ศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า



สารบัญ

คำนำ

ศูนย์คอมพิวเตอร์โรงพยาบาลพระมงกุฎเกล้า ได้ตระหนักถึงความสำคัญของเทคโนโลยีสารสนเทศในการสนับสนุนการบริหารจัดการภายในองค์กรและการให้บริการทางการแพทย์ จึงได้มีการนำHospital Information system :HIS) ระบบสารสนเทศโรงพยาบาล มาใช้เพื่อเพิ่มประสิทธิภาพและความต่อเนื่องในการปฏิบัติงาน ทั้งในด้านการให้บริการบุคลากรของโรงพยาลบาลและการดำเนินงานของหน่วยงาน ขณะเดียวกันความก้าวหน้าของเทคโนโลยีสารสนเทศในปัจจุบันพัฒนาอย่างรวดเร็ว ประกอบกับความเปลี่ยนแปลงของภัยคุกคามทางไซเบอร์และเหตุการณ์ฉุกเฉินต่างๆ เช่น ภัยธรรมชาติ หรืออุบัติเหตุ ซึ่งอาจส่งผลกระทบต่อการทำงานที่ต้องอาศัยระบบสารสนเทศ ศูนย์คอมพิวเตอร์จึงเล็งเห็นถึงความสำคัญในเรื่องของการจัดการฐานข้อมูล การเฝ้าระวัง และการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัย และสามารถรองรับสถานการณ์วิกฤติได้

เพื่อให้การดำเนินการของโรงพยาบาลเป็นไปอย่างต่อเนื่องและลดผลกระทบที่อาจเกิดขึ้น ศูนย์คอมพิวเตอร์ จึงได้จัดทำแผนดำเนินงานกรณีระสารสนเทศล่มเมื่อเกิดภาวะวิกฤต(Business Continuity Plan : BCP) เพื่อใช้เป็นแนวทางสำหนับหน่วยงานต่างๆในการตอบสนองต่อสถานการณ์วิกฤติ หรือเหตุการณ์ฉุกเฉินได้อย่างทันท่วงที และสามารถให้บริการทางการแพทย์แก่ข้าราชการและพลเรือน ประชาชนได้อย่างต่อเนื่องและมีประสิทธิภาพ

1. บทนำ

แผนดำเนินงานสำหรับการบริหารความพร้อมต่อสภาวะวิกฤต (Business Continuity Plan : BCP) ของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้าจัดทำขึ้นเมื่อวันที่ ตุลาคม พ.ศ.2568 เพื่อให้ศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า การเตรียมความพร้อมของหน่วยงานในการตอบสนองและสามารถนำไปใช้ในการปฏิบัติงานในสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่างๆ ทั้งที่เกิดจากระบบสารสนเทศภายในขัดข้อง,การมุ่งร้ายต่อองค์กรโดยการเจาะระบบ,การเกิดจราจรในพื้นที่,เกิดจากภัยธรรมชาติต่างๆเป็นต้น เพื่อไม่ให้สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินดังกล่าวส่งผลกระทบให้ระบบสารสนเทศภายใต้การดูแลของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้าต้องหยุดการดำเนินงานหรือไม่สามารถให้บริการได้อย่างต่อเนื่องแบบไม่มีกระบวนการรองรับทำให้การดำเนินงานไม่เป็นไปอย่างต่อเนื่องอาจส่งผลกระทบต่อหน่วยงานภายในโรงพยาบาลพระมงกุฎเกล้าในการให้บริการการรักษาพยาบาลให้กับทหาร และพลเรือน รวมทั้งการประสานงานและการดำเนินงานร่วมกับ หน่วยตรวจโรคต่างๆดังนั้น

การจัดทำแผนดำเนินงานสำหรับการบริหารความพร้อมต่อสภาวะวิกฤต จึงเป็นสิ่งสำคัญที่จะช่วยให้หน่วยงานสามารถรับมือกับเหตุการณ์ที่ไม่คาดคิดและทำให้กระบวนการที่สำคัญ(Critical Business Process) กลับมาดำเนินงานได้อย่างปกติในระดับการให้บริการที่กำหนดไว้ รวมทั้ง ลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นต่อหน่วยงานได้ทางศูนย์คอมพิวเตอร์โรงพยาบาล จึงได้จัดทำแผน BCP ขึ้น

2 วัตถุประสงค์ (Objectives) ของการจัดทำแผนดำเนินธุรกิจอย่างต่อเนื่องฯ

2.1 เพื่อใช้เป็นแนวทางในการบริหารความต่อเนื่องในการดำเนินงานของกลุ่มพัฒนาระบบบริหาร

2.2 เพื่อให้กลุ่มพัฒนาระบบบริหารมีการเตรียมความพร้อมในการรับมือกับสภาวะวิกฤตและลดผลกระทบจากการหยุดชะงักในการดำเนินงานหรือการให้บริการ

2.3 เพื่อบรรเทาความเสียหายให้อยู่ระดับที่ยอมรับได้

2.4 เพื่อให้ผู้บริหารโรงพยาบาลพระมงกุฎเกล้าและผู้มีส่วนได้ส่วนเสีย (Stakeholders) มีความเชื่อมั่นในศักยภาพของหน่วยงาน แม้หน่วยงานต้องเผชิญกับเหตุการณ์ร้ายแรงและส่งผลกระทบจนทำให้การดำเนินงานต้องหยุดชะงัก

3. สมมติฐานของแผนดำเนินธุรกิจอย่างต่อเนื่องฯ (BCP Assumptions)

เอกสารฉบับนี้จัดทำขึ้นภายใต้สมมติฐาน ดังต่อไปนี้

3.1 แผนดำเนินธุรกิจอย่างต่อเนื่องฯของกลุ่มพัฒนาระบบบริหาร ต้องครอบคลุมถึงสถานการณ์หรือเหตุการณ์จะทำให้เกิดความเสียหายต่อสถานที่ระบบงานอุปกรณ์เครื่องมือเครื่องใช้ในการทำงานและเอกสารข้อมูลที่สำคัญที่เป็นไปได้ในแต่ละกรณี ทั้งนี้เหตุการณ์ฉุกเฉินที่เกิดขึ้นมิได้ส่งผลกระทบต่อสถานที่ปฏิบัติงานสำรองระบบงานอุปกรณ์เครื่องมือเครื่องใช้ในการทำงานและเอกสารข้อมูลที่สำคัญที่ได้มีการจัดเตรียมไว้

3.2 ผู้บริหารและทีมบริหารความต่อเนื่องเข้าใจบทบาทหน้าที่ตามแผน BCP เป็นอย่างดี

3.3 คำว่า “บุคลากร” ที่ระบุในเอกสารฉบับนี้ หมายถึง บุคลากรทั้งหมดของกลุ่มพัฒนาระบบบริหาร

4. ขอบเขตของแผนดำเนินธุรกิจอย่างต่อเนื่องฯ (Scope of BCP)

แผนดำเนินธุรกิจอย่างต่อเนื่องฯ (BCP) ฉบับนี้ ใช้สำหรับเป็นแนวทางในการปฏิบัติ กรณีเกิดสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน เหตุการณ์ที่มีผลกระทบต่อกิจกรรมหลักของโรงพยาบาลพระมงกุฎเกล้า ประกอบด้วยเหตุการณ์ต่อไปนี้

4.1 เหตุการณ์เกิดจากระบบไฟฟ้าขัดข้อง

4.2 เหตุการณ์เกิดจากภัยธรรมชาติต่างๆ

4.3 เหตุการณ์เกิดการชุมนุมประท้วง/จลาจล

4.4 เหตุการณ์เกิดด้านเทคโนโลยีดิจิทัล

5. การวิเคราะห์ทรัพยากรที่สำคัญ

สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินมีหลากหลายรูปแบบ ดังนั้น เพื่อให้ศูนย์คอมพิวเตอร์สามารถบริหารจัดการการดำเนินงานของหน่วยงานให้มีความต่อเนื่อง การจัดหาทรัพยากรที่สำคัญจึงเป็นสิ่งจำเป็น และต้องระบุไว้ในแผนดำเนินธุรกิจอย่างต่อเนื่องฯ ซึ่งการเตรียมการทรัพยากรที่สำคัญจะพิจารณาจากผลกระทบใน 5 ด้าน ดังนี้

1. **ผลกระทบด้านอาคาร/สถานที่ปฏิบัติงานหลัก** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้สถานที่ปฏิบัติงานหลักได้รับความเสียหายหรือไม่สามารถใช้สถานที่ปฏิบัติงานหลักได้และส่งผลให้บุคลากรไม่สามารถเข้าไปปฏิบัติงานได้ชั่วคราวหรือระยะยาว
2. **ผลกระทบด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ไม่สามารถใช้งานวัสดุอุปกรณ์ที่สำคัญได้
3. **ผลกระทบด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ** หมายถึงเหตุการณ์ที่เกิดขึ้นทำให้ระบบงานเทคโนโลยี หรือระบบสารสนเทศ หรือข้อมูลที่สำคัญไม่สามารถนำมาใช้ในการปฏิบัติงานได้ตามปกติ
4. **ผลกระทบด้านบุคลากรหลัก**หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้บุคลากรหลักไม่สามารถมาปฏิบัติงานได้ตามปกติ
5. **ผลกระทบด้านคู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสียที่สำคัญ** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้คู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย ไม่สามารถติดต่อหรือให้บริการหรือส่งมอบงานได้
6. **การวิเคราะห์เหตุการณ์สภาวะวิกฤตและผลกระทบจากเหตุการณ์**
   (ทำเครื่องหมาย ✓ ในด้านที่ได้รับผลกระทบ)

ตารางที่ 1 แสดงการวิเคราะห์เหตุการณ์สภาวะวิกฤตและผลกระทบจากเหตุการณ์

	เหตุการณ์สภาวะวิกฤต	ผลกระทบ				
		ด้านอาคาร/สถานที่ปฏิบัติงานหลัก	ด้านวัสดุอุปกรณ์ที่สำคัญและการจัดหา/จัดส่ง	ด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ	ด้านบุคลากรหลัก	คู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย
1	เหตุการณ์ระบบไฟฟ้าขัดข้อง	✓	✓	✓	✓	✓
2	เหตุการณ์เกิดจากภัยธรรมชาติต่างๆ	✓	✓	✓	✓	✓
3	เหตุการณ์ชุมนุมประท้วง/จลาจล	✓	✓	✓	✓	
4	เหตุการณ์ผลกระทบด้านเทคโนโลยีดิจิทัล			✓	✓	✓

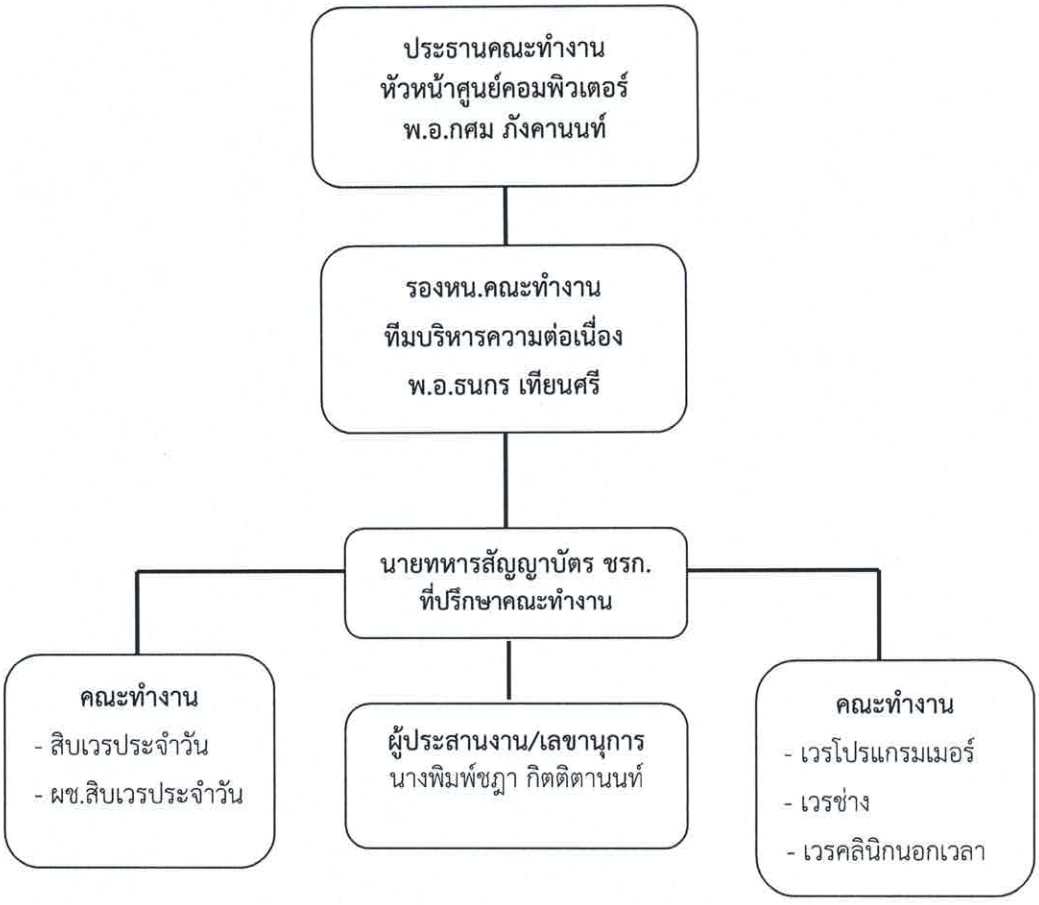
แผนดำเนินธุรกิจอย่างต่อเนื่องฯ (BCP) ฉบับนี้ ไม่รองรับการปฏิบัติงานในกรณีที่เหตุขัดข้องเกิดขึ้นจากการดำเนินงานปกติ และเหตุขัดข้องดังกล่าวไม่ส่งผลกระทบในระดับสูงต่อการดำเนินงานและการให้บริการของกลุ่มปฏิบัติงานระบบบริหารความต่อเนื่องจากหน่วยงานยังสามารถจัดการหรือปรับปรุงแก้ไขสถานการณ์ได้ภายในระยะเวลาที่เหมาะสม โดยผู้อำนวยการหรือหัวหน้าของแต่ละฝ่ายสามารถรับผิดชอบและดำเนินการได้ด้วยตนเอง

6. โครงสร้างและทีมงานบริหารความต่อเนื่องฯ (Business Continuity Plan Team)

ศูนย์คอมพิวเตอร์ฯได้แต่งตั้งคณะทำงานบริหารความต่อเนื่องของหน่วยงาน เพื่อให้สามารถปฏิบัติงานในภารกิจหลักหรืองานบริการที่สำคัญได้อย่างต่อเนื่องและมีประสิทธิภาพแม้เกิดสภาวะวิกฤติโดยมีองค์ประกอบดังนี้

1.พ.อ.กศม ภังคานนท์	ประธานคณะทำงาน
2.พ.อ.ธนกร เทียนศรี	รองหน.คณะทำงาน/หัวหน้าทีมบริหารความต่อเนื่อง
3.นายทหารสัญญาบัตร ชรก.	ที่ปรึกษาคณะกรรมทำงาน/ผู้ช่วยทีมบริหารความต่อเนื่อง
4.นางพิมพ์ชฎา กิตติตานนท์	ผู้ประสานงาน/คณะทำงานและเลขานุการ
5.สิบเวรประจำวัน	คณะทำงาน
6.ผู้ช่วยสิบเวรประจำวัน	คณะทำงาน
7.เวรช่างประจำวัน	คณะทำงาน
8.เวรโปรแกรมเมอร์ประจำวัน	คณะทำงาน
9.เวรคลินิกนอกเวลาประจำวัน	คณะทำงาน

โครงสร้างคณะทำงานบริหารความต่อเนื่องและบริหารจัดการแผนBCP



เพื่อให้แผน BCP ของศูนย์คอมพิวเตอร์สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและมีประสิทธิผล จึงได้กำหนดตัวบุคลากรหลัก บุคลากรสำรอง บทบาทหน้าที่ของและทีมบริหารความต่อเนื่อง ดังนี้

1. ประธานคณะทำงานบริหารความต่อเนื่อง รับผิดชอบงานอำนวยการ/สั่งการ

2. ผู้ประสานงาน/เลขานุการคณะทำงานบริหารความต่อเนื่อง รับผิดชอบในการติดต่อและประสานงานภายในทีมปฏิบัติงานตามกระบวนการแจ้งเหตุฉุกเฉิน (Call Tree)

3. ทีมบริหารความต่อเนื่องมีหน้าที่ในการร่วมมือ ดูแล ติดตาม ปฏิบัติงาน และกู้คืนเหตุการณ์ฉุกเฉินในส่วนงานของตนเองให้กลับสู่ภาวะปกติโดยเร็วตามแผน BCP

ซึ่งแต่ละตำแหน่งมีหน้าที่ในการร่วมมือดูแล ติดตาม ปฏิบัติงาน และกู้คืนเหตุการณ์ฉุกเฉินในแต่ละส่วนงานให้กลับสู่ภาวะปกติโดยเร็ว ตามรายชื่อบุคลากรและบทบาทของทีมงานบริหารความต่อเนื่อง(BCP Team) ที่กำหนดให้เป็นบุคลากรหลัก ในกรณีที่บุคลากรหลักไม่สามารถปฏิบัติหน้าที่ได้ให้บุคลากรสำรองรับผิดชอบบทบาทของบุคลากรหลักไปก่อน จนกว่าจะได้มีการมอบหมายและแต่งขึ้นขึ้นโดยหัวหน้าคณะทำงานบริหารความต่อเนื่องและทีมกอบกู้คืน

ตารางที่ 2 รายชื่อบุคลากรและทีมบริหารความต่อเนื่องฯ (BCP Team)

ทีมแผน BCP	บุคลากรหลัก	บุคลากรสำรอง
ทีม ปฏิบัติการ IT ภาวะฉุกเฉิน	**(1) เครือข่ายและความปลอดภัย**	
	ส.ท.ทศพลบวชชัยภูมิ (ฟลุ๊ค)	นายสิวะณัฐชื่นอารมย์ (กอล์ฟ)
	น.ส.สุวิดาสุขเรือนสุวรรณ (ส้ม)	นายอัมรินทร์จันทร์คทา (ซัน)
	นายภัทรพลศรีบุญขำ (โอม)	น.ส.จิราพรรณครีบภูบุตร (แคท)
	น.ส.สุวรรณีหงส์ฟ่องฟ้า (หมวย)	
	(2) เซิร์ฟเวอร์และฐานข้อมูล	
	จ.ส.อ.ณรงค์ศักดิ์ยาสี (ตั้ม)	นายพัชรพลชัยภักดี (ต่อ)
	นายสิวะณัฐชื่นอารมย์ (กอล์ฟ)	น.ส.สุวิดาสุขเรือนสุวรรณ (ส้ม)
	น.ส.ญาณิศาเชื้อมอญ (ผักกาด)	น.ส.กัญญาพรผงสี (อินดี้)
	นายอนุชาสารบาล (อ๊อฟ)	
	(3) สำรองข้อมูลและกู้คืนระบบ	
	จ.ส.อ.ชัยณรงค์แพทย์วงษ์ (ต้น)	นายอนุชาสารบาล (อ๊อฟ)
	นายพัชรพลชัยภักดี (ต่อ)	น.ส.สุวิดาสุขเรือนสุวรรณ (ส้ม)
	นายอัมรินทร์จันทร์คทา (ซัน)	นายเกษมคุณาอภิสิทธิ์ (บอส)
	นายมงคลคำปวน (เต)	
ทีม ประสานงานและสื่อสารภาวะฉุกเฉิน	ส.อ.หญิง อารยาบุรารักษ์ (สไปร์ท)	น.ส.สุจิตราฉายเสมแสง (แอน)
	น.ส.ภัทรารมย์ปินะถา (หญิง)	
	นางพิมพ์ชฎากิตติตานนท์ (บุ๋ม)	
	น.ส.วรายาคำเจริญ (เดียร์)	
	น.ส.ชูติมารัตนจิตเกษม (แก้ว)	
ทีมสนับสนุนการดำเนินงาน IT ฉุกเฉิน	จ.ส.อ.จักรพงษ์ฉัตรชานนท์ (โบ๊ท)	น.ส.อรอุษาตันโห (จอย)
	น.ส.กัญญาพรผงสี (อินดี้)	น.ส.สุวรรณีหงส์ฟ่องฟ้า (หมวย)
	น.ส.สุจิตราฉายเสมแสง (แอน)	
	นายสัมพันธ์พันธุ์เจริญ (เปี๊ยก)	
	น.ส.จิราพรรณครีบภูบุตร (แคท)	
	นายเกษมคุณาอภิสิทธิ์ (บอส)	
ทีมเฝ้าระวังและความปลอดภัยไซเบอร์	จ.ส.อ.พิษณุ ศรีสุลัย (เก่ง)	น.ส.ญาณิศาเชื้อมอญ (ผักกาด)
	น.ส.นัยนาสัมฤทธิ์ (นัย)	นายสัมพันธ์พันธุ์เจริญ (เปี๊ยก)
	นายธนะรัตน์ไกรทอง (ปอนด์)	
	น.ส.อรอุษาตันโห (จอย)	

7. ผลกระทบต่อกระบวนการทำงานหรือการให้บริการ

เกณฑ์การพิจารณาผลกระทบ เป็นเกณฑ์การพิจารณาความเสียหายหรือความรุนแรงของเหตุการณ์ที่เกิดขึ้นต่อการปฏิบัติงาน และส่งผลต่อขีดความสามารถในการดำเนินงานหรือการให้บริการลดลง โดยแบ่งระดับผลกระทบเป็น 4ระดับ ดังตารางเกณฑ์การพิจารณาระดับของผลกระทบ

ตารางที่ 3 เกณฑ์การพิจารณาระดับของผลกระทบการทำงานหรือการให้บริการของศูนย์คอมพิวเตอร์

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาผลกระทบ
สูงมาก	- ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลง มากกว่าร้อยละ 50
สูง	- ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลง ตั้งแต่ร้อยละ25 ไม่เกินร้อยละ 50
ปานกลาง	- ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลง ตั้งแต่ร้อยละ10 ไม่เกินร้อยละ 25
ต่ำ	- ส่งผลให้ขีดความสามารถในการดำเนินงานหรือการให้บริการลดลง ตั้งแต่ร้อยละ 5 ไม่เกินร้อยละ 10

หมายเหตุ: สามารถกำหนดระดับผลกระทบได้ตามความเหมาะสม เช่น สูง/ปานกลาง/ต่ำ หรือ สูงมาก/สูง/ปานกลาง/ต่ำ/ไม่เป็นสาระสำคัญ เป็นต้น

8.กระบวนการทำงานสำคัญศูนย์คอมพิวเตอร์ รพ.รร.6

ศูนย์คอมพิวเตอร์ฯ ได้พิจารณากระบวนงานสำคัญ หากเกิดเหตุการณ์ฉุกเฉินภาวะวิกฤตและเกิดผลกระทบต่อการดำเนินงาน จำนวน 4 กระบวนงาน ดังนี้

1. งานด้านการรักษาพยาบาลและพัฒนาทางการแพทย์ของโรงพยาบาลพระมงกุฎเกล้า
2. งานพัฒนาปรับปรุงการจัดการระบบสารสนเทศของโรงพยาบาล
3. งานพัฒนาอบรมเพื่อรับมือสถานการฉุกเฉินให้กับบุคลากรของหน่วยงาน
4. งานจัดทำแผนโครงการและการส่งเสริมผลงานโรงพยาบาลพระมงกุฎเกล้าสู่

การประเมินระดับผลกระทบต่อกระบวนงานที่สำคัญของกลุ่มพัฒนาระบบบริหารได้กำหนดระยะเวลาเป้าหมายในการกลับมาดำเนินงาน หรือฟื้นคืนสภาพให้ได้ภายในระยะเวลาที่กำหนดเป็นช่วงเวลา 1 วัน 3 วัน 7 วัน 15 วันและ 30 วันซึ่งระยะเวลาดังกล่าว หมายถึง ระยะเวลาภายหลังจากเกิดอุบัติการณ์ขึ้น ที่ทำให้การดำเนินงานหรือการให้บริการต้องกลับคืนสภาพเดิม กิจกรรมต้องกลับมาดำเนินการได้และทรัพยากรต้องได้รับการฟื้นฟู ตามตารางดังนี้

ตารางที่ 4 ตารางแสดงผลกระทบต่อกระบวนงานที่สำคัญหรือการให้บริการ (Business Impact Analysis)

กระบวนงานที่สำคัญ/กิจกรรม	ระดับผลกระทบ	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ				
		1 วัน	3 วัน	7 วัน	15 วัน	30 วัน
1. งานด้านการรักษาพยาบาลและพัฒนาทางการแพทย์ของโรงพยาบาลพระมงกุฎเกล้า	ปานกลาง			✓		
2. งานพัฒนาปรับปรุงการจัดการระบบสารสนเทศของโรงพยาบาล	ปานกลาง			✓		
3. งานพัฒนาอบรมเพื่อรับมือสถานการฉุกเฉินให้กับบุคลากรของหน่วยงาน	ปานกลาง			✓		
4. งานจัดทำแผนโครงการและการส่งเสริมผลงานโรงพยาบาลพระมงกุฎเกล้าสู่	ปานกลาง			✓		

สำหรับกระบวนงานอื่นๆ ที่ประเมินแล้ว อาจไม่ได้รับผลกระทบในระดับสูงถึงสูงมากหรือมีความยืดหยุ่นสามารถชะลอการดำเนินงานและการให้บริการได้ โดยให้ผู้บริหารของฝ่ายงานประเมินความจำเป็นและเหมาะสม ทั้งนี้ หากมีความจำเป็นให้ปฏิบัติตามแนวทางการบริหารความต่อเนื่องเช่นเดียวกับกระบวนงานหลัก

9. กลยุทธ์ความต่อเนื่อง (Business Continuity Strategy)

กลยุทธ์ความต่อเนื่อง เป็นแนวทางในการจัดหาและบริหารจัดการทรัพยากรให้มีความพร้อมต่อการปฏิบัติงานให้เกิดความต่อเนื่องเมื่อเกิดสภาวะวิกฤต ซึ่งพิจารณาทรัพยากรใน 5 ด้าน ดังตารางที่ 5

ตารางที่ 5 กลยุทธ์ความต่อเนื่อง(Business Continuity Strategy)

ทรัพยากร		กลยุทธ์ความต่อเนื่อง
	**อาคาร/ สถานที่ปฏิบัติงานสำรอง**	▪ กำหนดให้ใช้พื้นที่ปฏิบัติงานสำรองที่ได้รับคัดเลือก โดยมีการสำรวจความเหมาะสมของสถานที่ ประสานงาน และการเตรียมความพร้อมกับหน่วยงานเจ้าของพื้นที่(ตึกสมเด็จพระนางเจ้าสิริกิติ์ฯ ชั้น3 ห้องปฏิบัติการ ,กรมแพทย์ทหารบกและกรมทหารสื่อสาร) ▪ กำหนดให้ปฏิบัติงานที่บ้าน สำหรับภารกิจที่ไม่ได้รับผลกระทบหรือมีลักษณะงานที่สามารถปฏิบัติงานที่บ้านได้ ▪ เหลื่อมเวลาการปฏิบัติราชการ ▪ ในกรณีที่ประเมินแล้วมีความเสียหายขยายเป็นวงกว้างและมีระยะเวลานานเกิน1เดือน กำหนดให้ใช้พื้นที่ปฏิบัติงานสำรอง กรมแพทย์ทหารบกหรือกรมทหารสื่อสาร ที่อยู่สามารถเดินทางสะดวกต่อการปฏิบัติงานโดยมีระยะทางไม่เกิน 120 กิโลเมตร ซึ่งมีการสำรวจความเหมาะสมของสถานที่ ประสานงาน และ การเตรียมความพร้อมล่วงหน้า

ทรัพยากร		กลยุทธ์ความต่อเนื่อง
	**วัสดุอุปกรณ์ที่สำคัญ / การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ**	▪ กำหนดให้มีการจัดหาคอมพิวเตอร์all in สำรอง พร้อมอุปกรณ์ที่สามารถเชื่อมโยงต่อผ่านอินเทอร์เน็ตเข้าสู่ระบบเทคโนโลยีของส่วนกลาง ▪ กำหนดให้ใช้คอมพิวเตอร์แบบพกพา (Tablet/PC All in one) ของเจ้าหน้าที่หน่วยงานได้เป็นการชั่วคราวหากมีความจำเป็นเร่งด่วนในช่วงระหว่างการจัดหาคอมพิวเตอร์สำรอง ▪ กำหนดให้งานพัสดุจัดเก็บวัสดุสิ้นเปลืองในปริมาณที่เหมาะสม
	**เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ**	▪ ระบบการบริหารเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญของหน่วยงานเป็นแบบรวมศูนย์และเชื่อมโยงระบบเครือข่ายผ่านอินเทอร์เน็ตเพื่อการใช้งานดังนั้นหากเกิดภาวะฉุกเฉินให้รอจนกว่าระบบการบริหารเทคโนโลยีสารสนเทศของส่วนกลางจะกลับมาใช้งานได้ตามปกติ ▪ กำหนดให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศจัดให้มีระบบการสำรองข้อมูลไว้ในสถานที่อื่น ▪ จัดเก็บข้อมูลเข้าสู่ระบบฐานข้อมูลกลางที่สามารถเข้าถึงได้จากสถานที่อื่นๆภายนอกสำนักงานเพื่อให้บุคลากรในหน่วยงานทุกคนสามารถเข้าถึงข้อมูลและนำไปใช้ในการปฏิบัติภารกิจของหน่วยงาน
	**บุคลากรหลัก**	▪ กำหนดให้ใช้บุคลากรทดแทนภายในหน่วยงานเดียวกันก่อน ▪ กำหนดให้มีการเปลี่ยนเวรบุคลากรเพื่อRotateงานและการปฏิบัติงานได้อย่างต่อเนื่อง ▪ จัดเตรียมพนักงานขับรถยนต์เพื่อติดต่อประสานงานกับบุคคลและส่วนราชการอื่น ๆ
	**คู่ค้า/ผู้ให้บริการที่สำคัญ/ผู้มีส่วนได้ส่วนเสีย**	▪ ประสานงาน/ประชุมโดยใช้ระบบสื่อสารในรูปแบบต่างๆโดยเน้นการ ติดต่อสื่อสารผ่านช่องทางอิเล็กทรอนิกส์ และออนไลน์ เช่น เว็บไซต์ Facebook ,e-mail, Line เป็นต้น ▪ มีรายชื่อผู้ประสานงานพร้อมระบุช่องทางการติดต่อเพื่อให้การบริการกับหน่วยงานอื่นๆเกิดความต่อเนื่องเช่นเบอร์โทรศัพท์ อีเมล์กลางฯลฯ ▪ การส่งหนังสือราชการผ่านรูปแบบอิเล็กทรอนิกส์ ▪ ประชาสัมพันธ์ข้อมูล ข่าวสาร ผ่านช่องทางการสื่อสารต่าง ๆ โดยเน้นการสื่อสารผ่านออนไลน์

10. การวิเคราะห์เพื่อกำหนดความต้องการทรัพยากรที่สำคัญ

1) ด้านสถานที่ปฏิบัติงานสำรอง (Working Space Requirement)

ตารางที่ 6 ระบุพื้นที่การปฏิบัติงานสำรอง

สถานที่ปฏิบัติงานสำรอง	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ				
	1 วัน	3 วัน	7 วัน	15 วัน	30 วัน
พื้นที่สำหรับสถานที่ปฏิบัติงานสำรอง (เฉพาะบุคลากรหลักที่ไปปฏิบัติงาน ณ พื้นที่สำรอง) - อาคารสมเด็จพระนางเจ้าสิริกิติ์ฯ ชั้น3 (ตามที่แผน BCP ของรพ.พระมงกุฎเกล้าที่กำหนด) - กรมแพทย์ทหารบก (สำรองที่1) (ตามที่แผน BCP ของรพ.พระมงกุฎเกล้าที่กำหนด) -กรมทหารสื่อสาร (สำรองที่2) (ตามที่แผน BCP ของรพ.พระมงกุฎเกล้าที่กำหนด)	50-220 ตารางเมตร				

2) ความต้องการด้านวัสดุอุปกรณ์(Equipment & Supplies Requirement) จัดเตรียมในกรณีสถานการณ์ฉุกเฉินที่ทำให้บุคลากรมาสามารถเข้ามาปฏิบัติงานที่อาคารของหน่วยงานได้

ตารางที่ 7 ระบุจำนวนวัสดุอุปกรณ์ที่ต้องการ

วัสดุอุปกรณ์ที่ต้องการ	แหล่งที่มาของวัสดุ	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ				
		1 วัน	3 วัน	7 วัน	15 วัน	30 วัน
Notebook ส่วนกลาง	กองอำนวยการรพ.	10เครื่อง สำหรับเจ้าหน้าที่ทีมปฏิบัติงาน				
วิทยุสื่อสารส่วนกลาง	กองอำนวยการรพ.	15 เครื่อง สำหรับเจ้าหน้าที่ทีมปฏิบัติงาน				
เครื่องถ่ายเอกสาร+ปริ้นเตอร์ส่วนกลาง	กองอำนวยการรพ.	1-3 ชุดสำหรับเจ้าหน้าที่ทีมปฏิบัติงาน				
รถยนต์ส่วนกลางพร้อมคนขับ	กองอำนวยการรพ.	1-2 คัน สำหรับเจ้าหน้าที่ทีมปฏิบัติงาน				

3) ความต้องการด้านเทคโนโลยีสารสนเทศและข้อมูลที่ต้องการ (IT & Information Requirement)

ตารางที่ 8 ระบุความต้องการด้านเทคโนโลยีสารสนเทศและข้อมูลที่ต้องการ

ระบบเทคโนโลยีสารสนเทศและข้อมูลที่ต้องการ	ผู้รับผิดชอบ	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ				
		1 วัน	3 วัน	7 วัน	15 วัน	30 วัน
สัญญาณเครือระบบอินเทอร์เน็ต/อินทราเน็ตเชื่อมต่อ WiFi	ทีมประสานงานและสื่อสารภาวะฉุกเฉิน และทีมสนับสนุนการดำเนินงาน ITฉุกเฉิน	✓				
นำออก-เข้าฐานข้อมูลสำรองระบบงานโรงพยาบาล(PMK-HMS)	ทีม เฝ้าระวังและความปลอดภัยไซเบอร์ และทีม ปฏิบัติการ IT ภาวะฉุกเฉิน	✓				

4) ความต้องการด้านบุคลากรสำหรับความต่อเนื่องเพื่อปฏิบัติงาน (Personnel Requirement)

ตารางที่ 9 ความต้องการด้านบุคลากรในการปฏิบัติงาน

บุคลากรที่ต้องการ	จำนวนบุคลากรที่ต้องการตามระยะเวลาเป้าหมายในการฟื้นคืนสภาพ				
	1 วัน	3 วัน	7 วัน	15 วัน	30 วัน
จำนวนบุคลากรปฏิบัติงานที่	หัวหน้า ศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า และทีมปฏิบัติงาน 4 ทีม จำนวน.....30.....คน				
สำนักงาน/สถานที่ปฏิบัติงานสำรอง	- อาคาร สมเด็จพระนางเจ้าสิริกิติ์ฯ ชั้น3 ห้องปฏิบัติการและศูนย์สารสนเทศ - กรมแพทย์ทหารบก (สำรองที่ 1) - กรมทหารสื่อสาร (สำรองที่ 2)				

จำนวนบุคลากรที่ปฏิบัติงานดังกล่าวได้แก่ผู้อำนวยการและเจ้าหน้าที่เท่าที่มีความจำเป็นต้องมาปฏิบัติหน้าที่ที่สำนักงาน/สถานที่ปฏิบัติงานสำรอง เพื่อความต่อเนื่องในการดำเนินงานในกรณีเกิดสถานการณ์ฉุกเฉิน

5) ความต้องการด้านผู้ให้บริการที่สำคัญ (Service Requirement)

ตารางที่ 10 ความต้องการด้านผู้ให้บริการที่สำคัญ

ผู้ให้บริการ	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ				
	1 วัน	3 วัน	7 วัน	15 วัน	30 วัน
ผู้ให้บริการเครือข่ายอินเตอร์เน็ต (ประสานกองแผนงาน ผู้ดูแลระบบ)	✓				
ผู้ให้บริการอุปกรณ์สื่อสารและสนับสนุนสัญญาณทางการทหาร(กรณี ออกนอกสถานที่)	✓				
ผู้ให้บริการไฟฟ้าและรถเครื่องสำรองไฟ (ประสานงานอาคารสถานที่)	✓				
ผู้ให้บริการขนส่งและเคลื่อนย้ายอุปกรณ์ (กรณี ออกนอกสถานที่เพื่อไป temporary workplace)	✓				

11. ขั้นตอนการบริหารความต่อเนื่องและกอบกู้กระบวนการ

ศูนย์คอมพิวเตอร์ฯกำหนดแนวทางการบริหารความพร้อมต่อสภาวะวิกฤตเป็น3ระยะได้แก่ การตอบสนองต่อเหตุการณ์ทันที (ภายใน 24 ชั่วโมง) การตอบสนองต่อเหตุการณ์ในระยะแรก (2-7วัน) การตอบสนองต่อเหตุการณ์ และการกู้คืนกระบวนการปฏิบัติงานระยะเวลาเกิน 7 วัน

ตามตารางท้ายนี้ คือการจัดเตรียมสำหรับทีมบริหารความต่อเนื่องในการดำเนินการรวบรวมตรวจสอบสถานการณ์และรายงานให้คณะทำงานบริหารความต่อเนื่องทราบเป็นระยะๆตามกรอบเวลา โดยตรวจสอบการดำเนินงานตามขั้นตอนและกิจกรรมของผู้รับผิดชอบดังนี้

ตารางที่ 11 ขั้นตอนการบริหารความต่อเนื่องสำหรับ ทีมบริหารความต่อเนื่องเพื่อรวบรวมตรวจสอบสถานการณ์และรายงานสถานการณ์

ในการปฏิบัติการใดๆ ให้บุคลากรคำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นๆและปฏิบัติตามแนวทางแผนฯ และขั้นตอนการปฏิบัติงานที่ศูนย์คอมพิวเตอร์กำหนดไว้อย่างเคร่งครัด

การตอบสนองต่อเหตุการณ์ทันที (ภายใน24ชั่วโมง)		
ขั้นตอนและกิจกรรม	**ผู้รับผิดชอบ**	**ดำเนินการแล้วเสร็จ**
▪ แจ้งผลการสำรวจเหตุการณ์และประเมินระยะเวลา	ทีมปฏิบัติการITภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪ แจ้งเหตุฉุกเฉิน วิกฤตตามกระบวนการ Call Tree ให้กับบุคลากรในหน่วยงานทราบ ภายหลังได้รับแจ้งจากหัวหน้าคณะทำงานของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	ทีมประสานงานและสื่อสารภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐

▪ จัดประชุมทีมงานบริหารความต่อเนื่องเพื่อประเมินความเสียหายผลกระทบต่อการดำเนินงาน การให้บริการ และทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง ▪ ทบทวนกระบวนงานที่มีความเร่งด่วนหรือส่งผลกระทบอย่างสูง (หากไม่ดำเนินการ) ดังนั้น จำเป็นต้องดำเนินงาน หรือปฏิบัติด้วยมือ (Manual Processing)	ทีมสนับสนุนการดำเนินงาน ITภาวะฉุกเฉิน และ ทีมปฏิบัติการ ITภาวะฉุกเฉิน ของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪ ระบุและสรุปรายชื่อบุคลากรในศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้าที่ได้รับบาดเจ็บหรือเสียชีวิต	ทีมสนับสนุนการดำเนินงาน ITภาวะฉุกเฉินของศูนย์ คอมพิวเตอร์ โรงพยาบาล พระมงกุฎเกล้า	☐
▪ รายงานคณะบริหารความต่อเนื่องของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้าโดยครอบคลุมประเด็นดังนี้ - จำนวนและรายชื่อบุคลากรที่ได้รับบาดเจ็บ/เสียชีวิต - ความเสียหายและผลกระทบต่อการดำเนินงานและการให้บริการ - ทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง กระบวนงานที่มีความเร่งด่วนและส่งผลกระทบอย่างสูงหากไม่ดำเนินการ และจำเป็นต้องดำเนินงานหรือปฏิบัติงานด้วยมือ(Manual Processing)	ทีมหน.คณะทำงานของ ศูนย์คอมพิวเตอร์กอ.รพ.รร.6	☐

ในการปฏิบัติการใดๆ ให้บุคลากรคำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นๆและปฏิบัติตามแนวทางแผนฯ และขั้นตอนการปฏิบัติงานที่ศูนย์คอมพิวเตอร์กำหนดไว้อย่างเคร่งครัด

➕ การตอบสนองในระยะสั้น (2-7 วัน)		
ขั้นตอนและกิจกรรม	**ผู้รับผิดชอบ**	**ดำเนินการแล้วเสร็จ**
▪ ติดตามสถานะภาพการกอบกู้คืนมาของทรัพยากร ที่ได้รับผลกระทบ ประเมินความจำเป็นและระยะเวลาที่ต้องใช้ในการกอบกู้คืน	ทีมปฏิบัติการIT ภาวะฉุกเฉินและ ทีมสนับสนุนการดำเนินงาน IT ภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪ ตรวจสอบความพร้อมและข้อจำกัดในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง ได้แก่	ทีมประสานงานและสื่อสาร IT ภาวะฉุกเฉินและ ทีมสนับสนุน การดำเนินงาน ITภาวะฉุกเฉินของศูนย์ คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
- สถานที่ปฏิบัติงานสำรอง		☐
- วัสดุอุปกรณ์ที่สำคัญ		☐
- เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ		☐
- บุคลากรหลัก		☐
- ผู้รับบริการและผู้มีส่วนได้ส่วนเสีย/คู่ค้า/ผู้ให้บริการที่สำคัญ		☐

▪ รายงานหัวหน้าคณะกรรมการบริหารความต่อเนื่องของหน่วยงานเกี่ยวกับความพร้อมข้อจำกัดและข้อเสนอแนะในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง	ทีมปฏิบัติการ ITภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪ ประสานงานและดำเนินการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง	ทีมประสานงานและสื่อสารภาวะฉุกเฉินกับทีมสนับสนุนการดำเนินงานIT ภาวะฉุกเฉิน ของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐

ในการปฏิบัติการใดๆ ให้บุคลากรคำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นๆและปฏิบัติตามแนวทางแผนฯ และขั้นตอนการปฏิบัติงานที่ศูนย์คอมพิวเตอร์กำหนดไว้อย่างเคร่งครัด

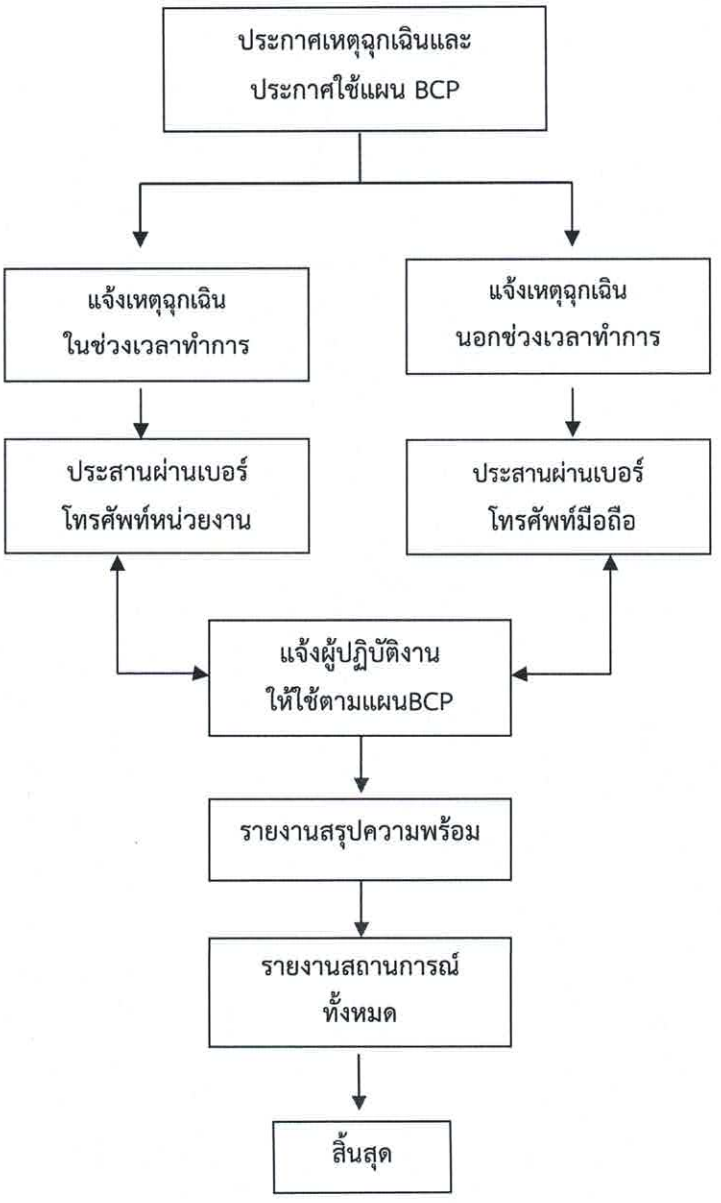
การตอบสนองต่อเหตุการณ์และการกู้คืนกระบวนการปฏิบัติงานระยะเวลาเกิน 7 วัน

ขั้นตอนและกิจกรรม	ผู้รับผิดชอบ	ดำเนินการแล้วเสร็จ
▪ ติดตามสถานภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบ และประเมินความจำเป็นและระยะเวลาที่ต้องใช้ในการกอบกู้คืน	ทีมปฏิบัติการIT ภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪ ระบุทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติ	ทีมประสานงานและสื่อสารภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪รายงานหัวหน้าคณะบริหารความต่อเนื่องของหน่วยงานสถานภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบและทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติ	ทีมสนับสนุนการดำเนินงาน IT ภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐ ☐ ☐ ☐
▪แจ้งสรุปสถานการณ์และการเตรียมความพร้อมด้านทรัพยากรต่าง ๆ เพื่อดำเนินงานและให้บริการตามปกติให้กับบุคลากรในหน่วยงาน	ทีมหน.คณะบริหารงาน ภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐

12. กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree)

เพื่อให้แผนดำเนินธุรกิจอย่างต่อเนื่องฯ (BCP) สามารถนำไปปฏิบัติใช้ได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล ศูนย์คอมพิวเตอร์จึงกำหนดให้มีกระบวนการแจ้งเหตุฉุกเฉิน (Call Tree) ขึ้น โดยกระบวนการ Call Tree คือกระบวนการแจ้งเหตุฉุกเฉินให้กับสมาชิกในทีมบริหารความต่อเนื่องเพื่อให้สามารถบริหารจัดการในการติดต่อบุคลากรของหน่วยงานภายหลังจากมีการประกาศเหตุการณ์ฉุกเฉินหรือสภาวะวิกฤต กระบวนการ Call Tree เริ่มต้นที่ประธานคณะบริหารความต่อเนื่องแจ้งให้ผู้ประสานงานคณะบริหารความต่อเนื่องทราบถึงเหตุการณ์ฉุกเฉินเพื่อให้ผู้ประสานงานฯ แจ้งให้ทีมบริหารความต่อเนื่องรับทราบเหตุการณ์ฉุกเฉินและการประกาศใช้แผนดำเนินธุรกิจอย่างต่อเนื่องฯ จากนั้นทีมบริหารความต่อเนื่องของแต่ละฝ่ายมีหน้าที่แจ้งไปยังบุคลากรภายในฝ่ายเพื่อรับทราบ **ตามผังกระบวนการแจ้งเหตุฉุกเฉินตาม Call Tree ดังนี้**

ผังกระบวนการแจ้งเหตุฉุกเฉินตาม Call Tree



ลำดับ	ผู้รับผิดชอบ	รายละเอียด
1	ประธานคณะทำงานศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	หัวหน้าศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า ประกาศเหตุฉุกเฉินและประกาศใช้แผนดำเนินธุรกิจอย่างต่อเนื่อง
2	รองหัวหน้าคณะทำงานทีมITภาวะฉุกเฉิน ของศูนย์คอมพิวเตอร์โรงพยาบาลพระมงกุฎเกล้า	ประธานคณะทำงานฯ แจ้งให้ทีมปฏิบัติการและประสานงานคณะทำงานฯ ทราบ
3	ทีมประสานงานและสื่อสาร ITภาวะ, ทีมปฏิบัติงานITภาวะฉุกเฉิน และ ทีมสนับสนุนการดำเนินงาน ITภาวะฉุกเฉินของศูนย์คอมพิวเตอร์โรงพยาบาลพระมงกุฎเกล้า	ทีมประสานงานศูนย์คอมพิวเตอร์โรงพยาบาลพระมงกุฎเกล้า ทราบ 1. **ถ้าเหตุการณ์เกิดขึ้นในเวลา** ทำการให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์ของหน่วยงานเป็นช่องทางแรก 2. **ถ้าเหตุการณ์เกิดขึ้นนอกเวลา** ทำการสถานที่ปฏิบัติงานหลักได้รับผลกระทบให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์มือถือเป็นช่องทางแรก ถ้าสามารถติดต่อได้ให้แจ้งข้อมูลแก่บุคลากรของ กพร. ทราบดังต่อไปนี้ - สรุปสถานการณ์ของเหตุการณ์ฉุกเฉินและการประกาศใช้แผนดำเนินธุรกิจอย่างต่อเนื่อง - เวลาและสถานที่สำหรับการนัดประชุมเร่งด่วนสำหรับผู้บริหารและคณะทำงานบริหารความต่อเนื่อง - ขั้นตอนและวิธีปฏิบัติเพื่อบริหารความพร้อมต่อสภาวะวิกฤตต่อไปเช่น สถานที่รวมพลในกรณีที่มีการย้ายสถานที่ทำงานฯลฯ
4	ทีมประสานงานและสื่อสารภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	ผู้ประสานงานแจ้งข้อมูลทั้งหมดของสถานการณ์ไปยังบุคลากรภายในทีมฯได้รับทราบเหตุการณ์ฉุกเฉิน
5	ทีมหน.คณะบริหารงานภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	ผู้ประสานงานคณะทำงานฯ รายงานสรุปความพร้อมของศูนย์คอมพิวเตอร์ ในการบริหารความพร้อมต่อสภาวะวิกฤตรวมทั้งความปลอดภัยในชีวิตและทรัพย์สิน
6	ทีมหน.คณะบริหารงานภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	ผู้ประสานงานคณะทำงานฯรายงานสถานการณ์ทั้งหมดของศูนย์คอมพิวเตอร์ให้คณะทำงานบริหารความต่อเนื่องทราบ

แบบตรวจสอบความครบถ้วนของแผนดำเนินธุรกิจอย่างต่อเนื่อง (BCP Checklist)

แบบฟอร์มนี้มีวัตถุประสงค์เพื่อใช้ในการสำรวจตนเองและทบทวนเพื่อให้มั่นใจว่าแผน BCP ของหน่วยงานมีความครบถ้วนและสมบูรณ์ตามแนวทางของการจัดทำแผน BCP ที่รองรับการบริหารงานภายในและงานบริการของหน่วยงานได้อย่างต่อเนื่องแม้ประสบสภาวะวิกฤต

รายการตรวจสอบ	มี	ไม่มี
ส่วนที่ 1 ข้อมูลพื้นฐาน		
1.1 ก่อนหน้านี้มีแผนเดิมอยู่	☐	☑
1.2 แผน BCP ที่จัดทำขึ้นในครั้งนี้สามารถรองรับเหตุการณ์ ดังต่อไปนี้		
• เหตุการณ์อุทกภัย	☑	☐
• เหตุการณ์อัคคีภัย	☑	☐
• เหตุการณ์วาตภัย	☐	☑
• เหตุการณ์ชุมนุมประท้วงจลาจล	☑	☐
• เหตุการณ์โรคระบาดต่อเนื่อง	☑	☐
• เหตุการณ์ผลกระทบด้านเทคโนโลยีดิจิทัล	☑	☐
• เหตุการณ์ไฟฟ้าดับวงกว้าง	☐	☑
• เหตุการณ์ก่อการร้าย	☐	☑
• เหตุการณ์แผ่นดินไหว	☐	☑
ส่วนที่ 2 องค์ประกอบตามแนวทางของการจัดทำ BCP		
2.1 ทีมงานแผนดำเนินธุรกิจอย่างต่อเนื่อง	☑	☐
2.2 ผลกระทบต่อกระบวนการทำงานหรือการให้บริการ (BIA)	☑	☐
2.3 ความต้องการทรัพยากรที่สำคัญ	☑	☐
2.4 กลยุทธ์และแนวทางในการบริหารความต่อเนื่อง		
• ด้านอาคาร สถานที่ปฏิบัติงานสำรอง/	☑	☐
• ด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหา จัดส่งวัสดุอุปกรณ์ที่สำคัญ	☑	☐
• ด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ	☑	☐
• ด้านบุคลากร	☑	☐
• ด้านคู่ค้า/ผู้ให้บริการที่สำคัญผู้มีส่วนได้ส่วนเสีย/	☑	☐
2.5 กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree)	☑	☐
2.6 ขั้นตอนการบริหารความต่อเนื่องและกอบกู้กระบวนการ	☑	☐

6. โครงสร้างและทีมงานแผนดำเนินธุรกิจอย่างต่อเนื่องฯ (Business Continuity Plan Team)

ทีมงานแผนดำเนินธุรกิจอย่างต่อเนื่อง(Business Continuity Plan Team)

เพื่อให้การบริหารงานในการใช้แผนBCPและการกำหนดบทบาทหน้าที่ของผู้ปฏิบัติตามการซักซ้อมของแบบแผนที่ศูนย์คอมพิวเตอร์ ได้จัดเตรียมไว้ทั้งหมด 5 ทีม ดังนี้

1. ทีมบริหารและควบคุมแผน IT ฉุกเฉิน (3คน)

ตำแหน่ง	หน้าที่หลัก
หัวหน้าศูนย์คอมฯ	ตัดสินใจเชิงนโยบาย, อนุมัติเปิดแผน BCP
รองหัวหน้าศูนย์คอมฯ	ประเมินเหตุการณ์, บริหารหน้างานฉุกเฉิน
นายทหารประจำชรก.ศูนย์คอมฯ	จัดประชุม, รวบรวมข้อมูล, ประสานงาน

2. ทีมปฏิบัติการ IT ภาวะฉุกเฉิน (12 คน)

ทีมย่อย : เครือข่ายและความปลอดภัย

บทบาท	หน้าที่หลัก	รายละเอียด
หัวหน้าชุดเครือข่ายฯ	บริหารจัดการทีมเครือข่าย, ตัดสินใจแยกโซนระบบ, ปิดกั้นการแพร่กระจายภัยคุกคาม	- ประเมินระดับความเสี่ยงของระบบเครือข่าย - สั่งปิด segment หรือ switch ที่ต้องการตัดวงจร - ประสานงานกับหัวหน้าทีมปฏิบัติการ IT ฉุกเฉิน
เจ้าหน้าที่วิเคราะห์และตัดการเชื่อมต่อระบบเครือข่าย	ควบคุมและแยกเครือข่ายระบบที่มีความเสี่ยงสูง	- ปิดใช้งาน switch/port ที่สงสัยว่าติดมัลแวร์ - แยก VLAN หรือเปลี่ยน IP Subnet ชั่วคราว - แยกระบบ Core จาก Network ภายนอกเพื่อจำกัดการแพร่
เจ้าหน้าที่ตรวจสอบ Firewall และจุดเข้าออกระบบ	ตรวจสอบ Firewall Rule, ตัดจุดเชื่อมต่อที่อาจถูกเจาะ	- วิเคราะห์ Log จาก Firewall, VPN, Internet Gateway - ปิด Rule ชั่วคราวที่เกี่ยวข้องกับจุดที่โดนเจาะ - เปลี่ยน Credentials ในการเข้าสู่ระบบ Gateway
เจ้าหน้าที่วิเคราะห์และจัดการภัยคุกคามเครือข่าย	ตรวจสอบพฤติกรรมผิดปกติ,วิเคราะห์ความพยายามโจมตีจากระบบภายนอก	- ตรวจสอบอุปกรณ์เครือข่าย (Switch, Router) หาช่องโหว่ - ตรวจสอบ abnormal traffic จาก SIEM หรือ Log ต่างๆ - ประสาน CERT ภายนอกในกรณีพบ IOC หรือ traffic ที่น่าสงสัย

หมายเหตุเพิ่มเติม:

ทำงานร่วมกับ:

- ทีม Cybersecurity ⟶เพื่อตรวจสอบว่า network ใดที่อาจถูกแทรกแซง
- ทีมสนับสนุน⟶เพื่อเคลื่อนย้ายอุปกรณ์อย่างปลอดภัย
- ทีมบริหาร⟶เพื่อขออนุมัติปิดระบบ critical network

ทีมย่อย : เซิร์ฟเวอร์และฐานข้อมูล

บทบาท	หน้าที่หลัก	รายละเอียด
หัวหน้าทีมเซิร์ฟเวอร์และฐานข้อมูล	วางแผนและควบคุมการกู้คืนระบบ server และฐานข้อมูล	- วิเคราะห์ผลกระทบและกำหนดลำดับการฟื้นฟูระบบ - ประสานกับทีมสำรองข้อมูลและทีมเครือข่าย - ตัดสินใจเลือกวิธีการกู้ - ตรวจสอบความพร้อมของเครื่อง serverก่อนเริ่มการ restore
เจ้าหน้าที่ฟื้นฟูเซิร์ฟเวอร์	ดำเนินการกู้คืนเครื่อง serverและบริการ	- Restore ระบบปฏิบัติการและ VM - ตรวจสอบ service ที่ run บนserver เช่น Web Server, File Server - ทดสอบการทำงานของ service ภายหลังการ restore - ปรับแต่งการตั้งค่าพื้นฐาน เช่น hostname, network config
เจ้าหน้าที่กู้คืนฐานข้อมูล	ฟื้นฟูฐานข้อมูลจากสำเนาสำรองให้พร้อมใช้งาน	- ดำเนินการ restore ฐานข้อมูล (เช่น Oracle, My SQL, MS SQL) - ตรวจสอบความสมบูรณ์ของ DB schema และข้อมูล - ทดสอบ query การดึงข้อมูลพื้นฐานหลัง restore - ตรวจสอบ log และตรวจจับ anomaly หรือ missing records
เจ้าหน้าที่ตรวจสอบและทดสอบระบบ	ตรวจสอบการทำงานของระบบหลังการกู้คืน	- ตรวจสอบการเชื่อมต่อของระบบกับฐานข้อมูล - ทดสอบการ login, ดึงรายงาน, การเชื่อมกับ front-end - ประสานกับผู้ใช้งานเพื่อรับ feedback เบื้องต้น - บันทึกผลการตรวจสอบและรายงานต่อหัวหน้าทีม

หมายเหตุเพิ่มเติม:

ทำงานร่วมกับ:

- ทีม DR ⟶ เพื่อเรียกใช้ backup
- ทีมNetwork⟶เพื่อเปิด path network หลัง server online
- ทีมบริหารฯ⟶เพื่อสั่งลำดับความสำคัญของระบบที่จะขึ้นก่อน-หลัง

ทีมย่อย : สำรองข้อมูลและกู้คืนระบบ

บทบาท	หน้าที่หลัก	รายละเอียด
หัวหน้าทีม Backup & DR	ควบคุมการวางแผนและบริหารจัดการการสำรองและกู้คืนข้อมูล	- ประเมินความเสียหายของข้อมูล/ระบบหลังเหตุการณ์ - สั่งการกู้คืนข้อมูลตามลำดับความสำคัญ - ประสานกับทีม serverและทีมบริหาร - อนุมัติการนำข้อมูลจาก DR Site มาใช้งานจริง
เจ้าหน้าที่ตรวจสอบข้อมูลสำรอง	จัดการ Restore job และตรวจสอบความสมบูรณ์ของข้อมูลสำรอง	- ตรวจสอบ log การสำรองข้อมูลย้อนหลัง - ตรวจสอบว่า backup ล่าสุดอยู่ในสถานะพร้อมกู้คืน - ตรวจสอบ media และ storage ที่เก็บข้อมูลสำรอง
เจ้าหน้าที่กู้คืนข้อมูล	ทำการกู้คืนระบบจาก backup ไปยังระบบหลักหรือระบบสำรอง	- เลือกจุดคืนค่าที่เหมาะสม (restore point) - ประสานงานกับทีม VM/Server เพื่อทดสอบการ restore - ทดสอบการทำงานของระบบหลัง restore แล้ว
เจ้าหน้าที่ทดสอบระบบหลังกู้คืนข้อมูล	ทดสอบระบบหลัง Restore และจัดทำ Checklist	- ตรวจสอบว่า VM หรือ DB ที่ restore กลับมาทำงานได้จริง - ทดสอบการเข้าระบบ, ฟังก์ชันสำคัญ, ความถูกต้องของข้อมูล - ทำ checklist ระบบที่ขึ้นแล้วและยังไม่สมบูรณ์ - รายงานผลให้หัวหน้าทีมและผู้บริหารรับทราบ

หมายเหตุเพิ่มเติม:

ทำงานร่วมกับ:

- ทีม Server ⟶เพื่อระบุ VM/DB ที่ต้อง restore
- ทีม Network⟶เพื่อเปิด path ไปยัง DR Site หรือระบบที่ restore แล้ว
- ทีมบริหารฯ⟶เพื่ออนุมัติการเปลี่ยนระบบหลักไป DR (Failover)

3. ทีมประสานงานและสื่อสารภาวะฉุกเฉิน (5 คน)

ภารกิจหลัก: แจ้งเตือนเหตุการณ์, ประสานงานกับทีมต่าง ๆ, ผู้บริหาร และหน่วยงานภายนอก

บทบาท	หน้าที่หลัก	รายละเอียด
หัวหน้าทีมประสานงาน	ควบคุมการแจ้งเหตุและการสื่อสารภายในองค์กร	- ประสานตรงกับผู้บริหาร BCP/หัวหน้าศูนย์คอมพิวเตอร์ - สั่งการทีมย่อยให้ส่งข่าวสารตามระดับความรุนแรง - สรุปรายงานความคืบหน้าเป็นระยะต่อผู้บริหาร
เจ้าหน้าที่สื่อสารภายใน	แจ้งเตือน/ติดต่อประสานงานภายในองค์กร	- เตรียม Template ข้อความฉุกเฉิน (SMS, LINE, Google Chat) - อัพเดทข่าวสารความคืบหน้าให้หน่วยงานที่เกี่ยวข้อง - บันทึกเวลาที่แจ้งและผู้รับสาร
เจ้าหน้าที่สื่อสารภายนอก	ติดต่อกับหน่วยงานภายนอก	- ติดต่อกับหน่วยงานภายนอกที่เกี่ยวข้อง - ขอคำปรึกษาทางเทคนิคหรือแนวทางแก้ไขเบื้องต้น - ประสานขอความช่วยเหลือในกรณีระบบล่มหรือโดนโจมตี
เจ้าหน้าที่บันทึกและรายงานสถานการณ์	สรุปรายงานเหตุการณ์และ log การสื่อสาร	- เก็บ log การแจ้งเตือน / คำสั่งจากผู้บริหาร - จัดทำ Timeline สถานการณ์และรายงานเป็นรอบ - เตรียมเอกสารสรุปเหตุการณ์ (Post-Incident Report)
ผู้ช่วยประสานสื่อสารภาคพื้น	สนับสนุนการประสานงานในพื้นที่และติดต่อแบบออฟไลน์	- เดินเอกสาร/แจ้งข่าวสารกรณีระบบสื่อสารล่ม - สนับสนุนการเคลื่อนย้ายเจ้าหน้าที่และอุปกรณ์ไปยังพื้นที่ปลอดภัย - ตรวจสอบการตอบสนองของหน่วยปฏิบัติการตามจุดต่าง ๆ - ช่วยยืนยันสถานะทางกายภาพ (เช่น ห้อง Server ยังปลอดภัยหรือไม่)

หมายเหตุเพิ่มเติม:

ทำงานร่วมกับ:

- ทีมบริหารฯ⟶เพื่อสรุปสถานการณ์และข้อความที่ใช้สื่อสาร
- ทีมปฏิบัติการ⟶เพื่อติดตามความคืบหน้าและจัดทำรายงานให้ทันต่อเหตุการณ์
- ทีมสนับสนุน⟶เพื่อส่งต่อข้อมูลและขอการสนับสนุนหากมีการเคลื่อนย้าย/กู้ระบบ

4. ทีมสนับสนุนการดำเนินงาน IT ฉุกเฉิน (6 คน)

ภารกิจหลัก: เตรียมอุปกรณ์และสภาพแวดล้อมเพื่อสนับสนุนการดำเนินงานของทีมปฏิบัติการและบุคลากรที่เกี่ยวข้อง

บทบาท	หน้าที่หลัก	รายละเอียด
หัวหน้าทีมสนับสนุน	วางแผนและควบคุมการสนับสนุนทั้งหมด	- ประสานงานกับหัวหน้าทีมปฏิบัติการเพื่อเข้าใจความต้องการ - ตรวจสอบและจัดลำดับการแจกจ่ายทรัพยากร - กำกับการขนย้ายอุปกรณ์หากมีการย้ายศูนย์สำรอง - รายงานความพร้อมของอุปกรณ์และเจ้าหน้าที่ให้ทีมบริหารทราบ
เจ้าหน้าที่จัดหาและแจกจ่ายอุปกรณ์	จัดหาและกระจายอุปกรณ์ IT สำรอง	- จัดเตรียม PC, notebook, switch, access point - ตรวจสอบเครื่องมือสำรองให้อยู่ในสภาพพร้อมใช้งาน - ดูแลการเบิก/คืน และเคลื่อนย้ายอุปกรณ์
เจ้าหน้าที่ติดตั้งระบบและเครื่องลูกข่าย	ติดตั้งระบบสำรองชั่วคราวให้ผู้ใช้	- ติดตั้ง Windows, Software พื้นฐาน - ตั้งค่าระบบให้เชื่อมต่อกับเครือข่ายหรือ server ใหม่ - ทดสอบการใช้งานเบื้องต้น
เจ้าหน้าที่สายสื่อสารและเครือข่าย	วางและเชื่อมต่อสายเครือข่าย	- ติดตั้ง/เดินสาย LAN ชั่วคราวหรือสายไฟสำรอง - ช่วยดูแลจุดที่ต้องการเชื่อมต่อด่วนในพื้นที่ชั่วคราว - ตรวจสอบจุดจ่ายไฟ (ปลั๊ก, UPS) ให้เพียงพอ
เจ้าหน้าที่ระบบสำรองและซ่อมแซม	ดูแลระบบสำรองและช่วยแก้ไขอุปกรณ์เบื้องต้น	- สนับสนุนการตั้งค่าเครื่องใช้ระบบสำรอง - แก้ปัญหา hardware/software หน้างานร่วมกับทีมอื่น
ผู้ช่วยภาคสนามและบันทึกข้อมูล	ช่วยงานภาคสนามและจัดทำบันทึก/รายงานสนับสนุน	- บันทึกกิจกรรมภาคสนาม, เวลาใช้งานอุปกรณ์ - ประสานการเคลื่อนย้ายอุปกรณ์, ถ่ายภาพ/หลักฐานประกอบ

5. ทีมเฝ้าระวังและความปลอดภัยไซเบอร์ (4 คน)

ภารกิจหลัก: ตรวจสอบ วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงการป้องกันล่วงหน้า

บทบาท	หน้าที่หลัก	รายละเอียด
หัวหน้าทีมความปลอดภัยไซเบอร์	วางแผนและควบคุมการตอบสนองด้านไซเบอร์	- กำหนดแนวทาง Incident Response Plan - ประเมินระดับภัยคุกคาม - สั่งการหากต้องตัดระบบหรือแยกโซนที่ถูกโจมตี - รายงานสถานการณ์ให้ทีมบริหารทราบ
เจ้าหน้าที่วิเคราะห์ log	ตรวจสอบ log และหาเหตุผิดปกติ	- ตรวจสอบข้อมูลจาก SIEM, firewall, antivirus, endpoint - ตรวจจับพฤติกรรมแปลก เช่น login ผิดปกติ, การ scan port - ตั้ง rule ใหม่ในระบบ monitor ตามความเสี่ยงที่เปลี่ยนไป
เจ้าหน้าที่วิเคราะห์มัลแวร์/ภัยคุกคาม	วิเคราะห์ไฟล์หรือพฤติกรรมของมัลแวร์	- แยก sample ไฟล์ต้องสงสัย (เช่น .exe, .dll) - ตรวจสอบ IOC (Indicators of Compromise) - อัปเดต Threat Intelligence และ block IP/DNS ที่เกี่ยวข้อง
เจ้าหน้าที่จัดการช่องโหว่ระบบ	ตรวจสอบและอุดช่องโหว่ระบบ	- ตรวจสอบ vulnerability scan report จากระบบต่าง ๆ - อัปเดต patch ระบบที่ยังไม่ปลอดภัย (OS, app, firmware) - ตรวจสอบ config ที่เปิด public port หรือ setting ไม่เหมาะสม

ตัวอย่าง บทบาทหน้าที่ในสถานการณ์ Ransomware

ประเภททีม	บทบาทหน้าที่
ทีมปฏิบัติการ IT ภาวะฉุกเฉิน **ทีมย่อย: เครือข่ายและความปลอดภัย**	**หัวหน้าทีม:** วิเคราะห์ปัญหาเน็ตเวิร์ก และสั่งแยก node ที่ถูกโจมตี **สมาชิกคนที่ 1:** ตรวจสอบ Firewall / ACL และ VPN **สมาชิกคนที่ 2:** ตรวจสอบความเสียหาย Switch / Access Point **สมาชิกคนที่ 3:** ฟื้นฟูระบบ network พื้นฐาน (LAN, Internet, Wi-Fi)
ทีมย่อย: เซิร์ฟเวอร์และฐานข้อมูล	**หัวหน้าทีม:** ประเมิน server ที่ถูก Ransomware และสั่ง snapshot **สมาชิกคนที่ 1:** Restore Server จาก Snapshot หรือ VM Backup **สมาชิกคนที่ 2:** ตรวจสอบและกู้คืน Database **สมาชิกคนที่ 3:** เชื่อมโยงระบบ App/DB/Storage ให้กลับมาใช้งานได้
ทีมย่อย: สำรองข้อมูลและกู้คืนระบบ	**หัวหน้าทีม:** ตรวจสอบความสมบูรณ์ของ Backup / DR Site **สมาชิกคนที่ 1:** เรียกคืนข้อมูลจาก Tape/Cloud/DR Site **สมาชิกคนที่ 2:** ทดสอบการ Restore ของระบบสำคัญ **สมาชิกคนที่ 3:** สนับสนุนการนำระบบเข้าสู่โหมด Production ชั่วคราว
ทีมประสานงานและสื่อสารIT ภาวะฉุกเฉิน	**หัวหน้าทีม:**ประสานงานกับผู้บริหารและควบคุมการแจ้งเตือนสาธารณะ **สมาชิกคนที่ 1-2:** ส่ง SMS/LINE/Email แจ้งหน่วยงานต่าง ๆ **สมาชิกคนที่ 3:** บันทึก log การติดต่อ **สมาชิกคนที่ 4:** ติดต่อหน่วยงานภายนอก
ทีมสนับสนุนการดำเนินงาน IT ภาวะฉุกเฉิน	**หัวหน้าทีม:** วางแผนการสนับสนุนทรัพยากรและประสานกับทีมปฏิบัติการ **สมาชิกคนที่ 1-2:** จัดหาอุปกรณ์สำรอง (PC, Server, สาย LAN ฯลฯ) **สมาชิกคนที่ 3:** จัดการเรื่องเวร/เวลาปฏิบัติงานในภาวะฉุกเฉิน **สมาชิกคนที่ 4-5:** ช่วยติดตั้ง, ลง software, deploy ระบบชั่วคราว
ทีมเฝ้าระวังและความปลอดภัยไซเบอร์ ITภาวะฉุกเฉิน	**หัวหน้าทีม:** ประเมินภัยคุกคามและควบคุมการตอบสนองความปลอดภัยไซเบอร์ **สมาชิกคนที่ 1:** ตรวจสอบ log และ IDS/IPS **สมาชิกคนที่ 2:** วิเคราะห์มัลแวร์ / Ransomware ตัวที่ใช้โจมตี **สมาชิกคนที่ 3:** ปิดช่องโหว่, อัปเดตแพตช์และแก้ไข config ที่ถูกเปลี่ยน

ตัวอย่างบทบาทหน้าที่ในสถานการณ์ Network Down

ประเภททีม	บทบาทหน้าที่
ทีมปฏิบัติการ IT ภาวะฉุกเฉิน **ทีมย่อย: เครือข่ายและความปลอดภัย**	**หัวหน้าทีม:** วินิจฉัยต้นเหตุ (เช่น switch/router เสีย, uplink ขาด, firewall block) **สมาชิกคนที่ 1-3:** ตรวจสอบอุปกรณ์ Layer 2–3, เปลี่ยนอุปกรณ์เสีย, config ใหม่, reroute การเชื่อมต่อ
ทีมย่อย: เซิร์ฟเวอร์และฐานข้อมูล	**หัวหน้าทีม:** ตรวจสอบว่า server ยังทำงานอยู่ใน LAN หรือถูกตัดด้วย **สมาชิกคนที่ 1-3:** เตรียมระบบทำงาน offline (เช่น HIS ภายใน), ปรับ connection
ทีมย่อย: สำรองข้อมูลและกู้คืนระบบ	**หัวหน้าทีม:** ประเมินความจำเป็นในการโยกไป DR site (ถ้า network ภายนอกล่ม) **สมาชิกคนที่ 1-3:** เชื่อมโยงระบบภายในที่ยังใช้ได้, sync ข้อมูลภายในโรงพยาบาล
ทีมประสานงานและสื่อสารIT ภาวะฉุกเฉิน	**หัวหน้าทีม:** ประกาศเหตุผ่านช่องทางที่ยังใช้งานได้ เช่น โทรศัพท์มือถือ/ประกาศภายใน **สมาชิกคนที่ 1-2:** แจ้งผู้ปฏิบัติงานว่าใช้ระบบใดได้/ไม่ได้, ให้คำแนะนำการทำงาน manual **สมาชิกคนที่ 3-4:** ประสานงานกับบริษัทที่เกี่ยวข้อง
ทีมสนับสนุนการดำเนินงาน IT ภาวะฉุกเฉิน	**หัวหน้าทีม:** จัดเตรียมอุปกรณ์ network สำรอง (สายแลน, switch, AP) **สมาชิกคนที่ 1-2:** นำอุปกรณ์ไปเปลี่ยนหน้างาน,ย้ายเครื่องจาก VLAN เสียไป VLAN ปกติ **สมาชิกคนที่ 3:** จัดการเวรเฝ้า/การลงพื้นที่ของทีม **สมาชิกคนที่ 4-5:** ช่วย config อุปกรณ์ใหม่ตามคู่มือ/backup config
ทีมเฝ้าระวังและความปลอดภัยไซเบอร์ ITภาวะฉุกเฉิน	**หัวหน้าทีม:** ตรวจสอบว่า network down เกิดจาก cyberattack หรือไม่ **สมาชิกคนที่ 1-2:** วิเคราะห์ firewall log, SIEM, ตรวจสอบ DDOS หรือACL ผิดพลาด **สมาชิกคนที่ 3:**ปรับ rule ชั่วคราว (เช่น whitelist IP), ป้องกันเหตุซ้ำ

ตัวอย่างบทบาทหน้าที่ในสถานการณ์แผ่นดินไหว

ประเภททีม	บทบาทหน้าที่
ทีมปฏิบัติการ IT ภาวะฉุกเฉิน **ทีมย่อย: เครือข่ายและความปลอดภัย**	**หัวหน้าทีม:** วางแผนและควบคุมการปิดระบบเครือข่ายหลัก **สมาชิกคนที่ 1-3:** ถอด Switch, Firewall, จัดการการเชื่อมต่อ, แยก VLAN, ตรวจสอบเส้นทางสำรอง
ทีมย่อย: เซิร์ฟเวอร์และฐานข้อมูล	**หัวหน้าทีม:** ประเมินสภาพเซิร์ฟเวอร์, ลำดับความสำคัญระบบ **สมาชิกคนที่ 1-3:** ปิดเครื่อง, ถอด Server/Storage ออกจาก Rack, จัดการฐานข้อมูล
ทีมย่อย: สำรองข้อมูลและกู้คืนระบบ	**หัวหน้าทีม:** ตรวจสอบความพร้อมของระบบสำรอง **สมาชิกคนที่ 1-3:** ตรวจสอบ Backup integrity, เตรียมข้อมูลสำหรับ recovery, เชื่อมต่อกับ DR Site
ทีมประสานงานและสื่อสารIT ภาวะฉุกเฉิน	**หัวหน้าทีม:** ประสานงานผู้บริหาร, หน่วยงานความปลอดภัย, วิศวกรอาคาร **สมาชิกคนที่ 1-2:** แจ้งเตือนผ่านระบบแจ้งเตือนด่วน (LINE, SMS, GOOGLE CHAT), จัดทำประกาศ **สมาชิกคนที่ 3:** ติดต่อ CERT, Vendor, ฝ่ายดูแลอาคาร, รถรับอุปกรณ์ **สมาชิกคนที่ 4:** จดบันทึก log การสื่อสารทั้งหมด, จัดทำรายงานอัพเดตสถานการณ์ทุก 2 ชั่วโมง
ทีมสนับสนุนการดำเนินงาน IT ภาวะฉุกเฉิน	**หัวหน้าทีม:** วางแผนลำดับการเคลื่อนย้าย, ประสานรถขนย้าย **สมาชิกคนที่ 1-2:** เตรียมอุปกรณ์เคลื่อนย้าย (ลัง, แท่นกันกระแทก, สายไฟสำรอง) **สมาชิกคนที่ 3:** ตรวจสอบ UPS แบบพกพา, ตรวจสอบอุปกรณ์กันไฟฟ้าสถิต **สมาชิกคนที่ 4-5:** ช่วยขนย้ายอุปกรณ์จาก Data Center ออกนอกรัศมีอาคาร, นำขึ้นรถขนย้ายไปยัง DR Site
ทีมเฝ้าระวังและความปลอดภัยไซเบอร์ ITภาวะฉุกเฉิน	**หัวหน้าทีม:**กำกับดูแลการปิดระบบให้ปลอดภัย, ปิดช่องทางเชื่อมต่อภายนอก **สมาชิกคนที่ 1:**วิเคราะห์เหตุการณ์ผิดปกติทางไซเบอร์ที่อาจเกิดขึ้นช่วงวิกฤต **สมาชิกคนที่ 2:**วิเคราะห์ความเสี่ยงการโจมตีเพิ่มเติมจากภัยแฝง (เช่น ransomware) **สมาชิกคนที่ 3:**ปิด VPN, หยุดบริการ Internet-facing, แจ้งเตือนผู้ใช้ภายในให้หยุดใช้ระบบ

7.การวิเคราะห์ผลกระทบและขั้นตอนการบริหาความต่อเนื่อง

1. ผลกระทบต่อกระบวนการทำงานหรือการให้บริการ (Business Impact Analysis)

การวิเคราะห์ผลกระทบต่อกระบวนการทำงานหรือการให้บริการ (Business Impact Analysis) โดยใช้เกณฑ์ในการกำหนดระดับผลกระทบ ดังนี้

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
สูงมาก	• เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับสูงมาก • ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงมากกว่า ร้อยละ 50 • เกิดการสูญเสียชีวิตและ/หรือภัยคุกคามต่อสาธารณชน • ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับประเทศและนานาชาติ
สูง	• เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับสูง • ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงร้อยละ 25-50 • เกิดการบาดเจ็บต่อผู้รับบริการ/บุคคล/กลุ่มคน • ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับประเทศ
ปานกลาง	• เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับปานกลาง • ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการ ลดลงร้อยละ 10-25 • ต้องมีการรักษาพยาบาล • ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับท้องถิ่น
ต่ำ	• เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับต่ำ • ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการ ลดลงร้อยละ 5-10 • ต้องมีการปฐมพยาบาล • ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับท้องถิ่น
ไม่เป็นสาระสำคัญ	• ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการ ลดลงน้อยกว่าร้อยละ 5

หมายเหตุ : สามารถกำหนดระดับผลกระทบได้ตามความเหมาะสม เช่น สูง/ปานกลาง/ต่ำ หรือ สูงมาก/สูง/ปานกลางต่ำ/ไม่เป็นสาระสำคัญ เป็นต้น พบว่ากระบวนการทำงานที่หน่วยงานต้องให้ความสำคัญและกลับมาดำเนินงานหรือฟื้นคืนสภาพให้ได้ภายในระยะเวลาตามที่กำหนด

ตารางทรัพยากรในการบริหารความต่อเนื่องและระยะเวลาในการฟื้นคืนสภาพ

กระบวนการหลัก	แหล่งเก็บระบบ/ข้อมูล	ระดับผลกระทบ/ความเร่งด่วน	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ			
		(สูงมาก/สูง/ปานกลาง/ต่ำ)	4 – 24 ชั่วโมง	1 - 2 วัน	1 สัปดาห์	2 สัปดาห์
ระบบ HIS (PMK HMS)	ห้อง Data Center ชั้น10ฉก., ชั้น 3 สก.	สูงมาก	✓			
ระบบ PACS (X-ray)	ห้อง Server PACS ชั้น10ฉก., ชั้น 3 สก.	สูงมาก	✓			
ระบบ LIS (Lab)	กองพยาธิ ชั้น2 ฉก.	สูงมาก	✓			
ระบบสำรองข้อมูล (Back up)	Server backup ชั้น 10 ฉก., ชั้น 3 สก.	สูงมาก	✓			
เครือข่ายภายใน	ห้องnetwork ชั้น10,ตึกต่างๆ	สูงมาก	✓			
เครือข่ายภายนอก (UniNet, Cat)	ห้อง network ชั้น10, ห้อง network ชั้น1 ฉก.	สูง		✓		
Server VM ware	ห้อง Data Center ชั้น10 ฉก.	สูง		✓		
ระบบ Security, Firewall	ห้อง network ชั้น10	สูง		✓		
PMK Smart App (Telemed)	ห้อง Data Center ชั้น10ฉก., ชั้น 3 สก.	สูง		✓		
ระบบ VPN ,TS plus	ห้อง network ชั้น10	ปานกลาง		✓		
ระบบไฟฟ้าหลัก ไฟฟ้าสำรองในห้อง Server	ห้อง Data Center ชั้น10ฉก., ชั้น 3 สก.	ปานกลาง		✓		
ระบบปรับอากาศ ในห้อง Server	ห้อง Data Center ชั้น10 ฉก ชั้น 3 สก.	ปานกลาง		✓		
ระบบอื่นๆ (เปล, คิวออนไลน์, web app ต่างๆ)	ห้อง Data Center ชั้น10 ฉก.	ต่ำ			✓	

กระบวนการหลัก	แหล่งเก็บระบบ/ข้อมูล	ระดับผลกระทบ/ความเร่งด่วน	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ			
		(สูงมาก/สูง/ปานกลาง/ต่ำ)	4 – 24 ชั่วโมง	1 - 2 วัน	1 สัปดาห์	2 สัปดาห์
การซ่อมบำรุงเครื่องคอมพิวเตอร์อื่นๆ	ศูนย์คอมพิวเตอร์	ต่ำ			✓	

หมายเหตุ :

1.ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ หมายถึงระยะเวลาภายหลังจากเกิดอุบัติการณ์ขึ้นที่ทำให้ผลิตภัณฑ์หรือบริการต้องกลับคืนสภาพเดิม กิจกรรมต้องกลับมาดำเนินการได้ และทรัพยากรต้องได้รับการฟื้นฟู

2. การกำหนดช่วงของระยะเวลาเป้าหมายในการฟื้นคืนสภาพ สามารถปรับเปลี่ยนได้ตามความเหมาะสม สำหรับกระบวนงานอื่นๆที่ประเมินแล้วอาจไม่ได้รับผลกระทบในระดับสูงถึงสูงมากหรือมีความยืดหยุ่นสามารถชะลอการดำเนินงานและการให้บริการได้ โดยให้ ผอ.กอง/หัวหน้าหน่วยงาน/แผนกประเมินความจำเป็นและเหมาะสม ทั้งนี้หากมีความจำเป็น ให้ปฏิบัติตามแนวทางการบริหารความต่อเนื่องเช่นเดียวกับกระบวนงานหลัก

2. สำหรับระบบงานบริการผู้ป่วย โรงพยาบาลพระมงกุฎเกล้า

ทางศูนย์คอมพิวเตอร์ ได้จัดทำแผนฉุกเฉิน สำหรับระบบงานบริการผู้ป่วย เพื่อเตรียมรองรับเหตุการณ์ฉุกเฉินในภาวะที่เกิดการหยุดชะงักทางธุรกิจเพื่อสร้างความมั่นใจว่าการบริการที่สำคัญด้านระบบข้อมูลสารสนเทศจะฟื้นคืนกลับมาตามเวลาที่กำหนดลดผลกระทบที่เกิดจากการหยุดชะงักทางธุรกิจ แผนรองรับการบริหารอย่างต่อเนื่อง(BCP) สำหรับระบบงานบริการผู้ป่วยฉบับนี้จัดทำขึ้นเพื่อให้เจ้าหน้าที่ของโรงพยาบาลใช้งานในกรณีที่ เกิดเหตุฉุกเฉินหรือภัยพิบัติทำให้ระบบ ITล่มไม่สามารถปฏิบัติงานได้เกิดผลกระทบจากประกาศใช้แผน

ขั้นตอนหลักการกู้คืนระบบ

- แผนกสารสนเทศโรงพยาบาลตรวจพบหรือได้รับรายงานจากผู้ใช้งานว่าระบบสารสนเทศโรงพยาบาลไม่ใช้งานได้
- เจ้าหน้าที่แผนกสารสนเทศโรงพยาบาล ตรวจสอบปัญหาว่าขัดข้องโรงพยาบาลหรือเฉพาะบางจุด/บริเวณ และเป็นปัญหาจากระบบเครือข่ายหรือระบบสารสนเทศโรงพยาบาล
- กรณีปัญหาเกิดจากระบบเครือข่ายขัดข้องให้ประสานเจ้าหน้าที่เทคโนโลยีสารสนเทศเพื่อตรวจสอบและแก้ไขปัญหาระบบเครือข่ายทันที
- กรณีปัญหาเกิดจากระบบสารสนเทศโรงพยาบาล ให้แจ้งหัวหน้าแผนกสารสนเทศโรงพยาบาลทราบในโอกาสแรกและดำเนินการตรวจสอบเพื่อประเมินปัญหาอย่าง เร่งด่วน

- เจ้าหน้าที่แผนกเทคโนโลยีสารสนเทศและ/หรือเจ้าหน้าที่แผนกสารสนเทศโรงพยาบาล

ตารางการประกาศแจ้งเมื่อเกิดสถานการณ์ภายในระยะเวลาต่างๆ

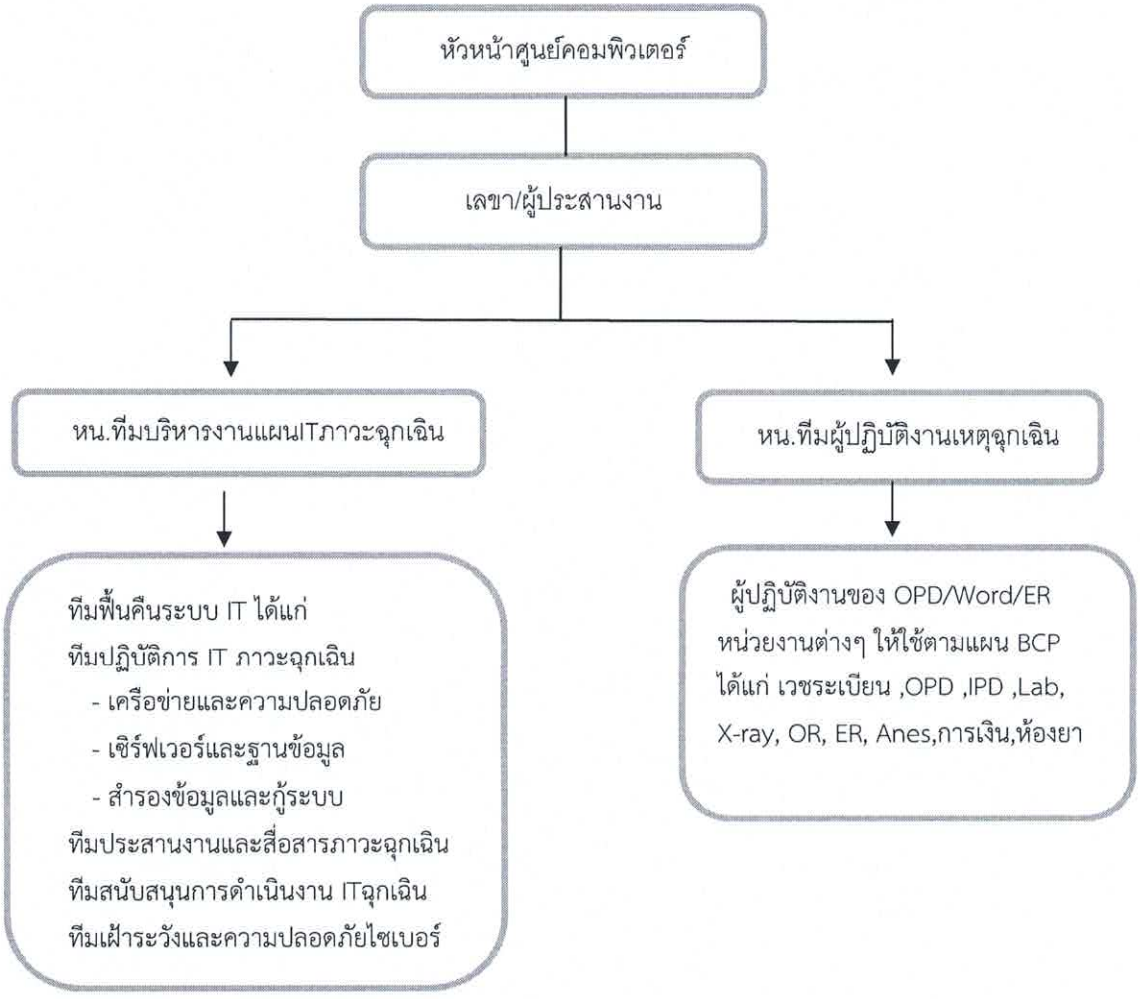
ช่วงระยะเวลาแก้ปัญหา	ขั้นตอนและประกาศแจ้ง
กรณีสามารถแก้ไขปัญหาได้ภายใน 30นาที	- รายงานสถานการณ์ต่อผู้บังคับบัญชาตามลำดับทราบในโอกาสแรกถึงการประเมินความรุนแรง - ในเบื้องต้นและแนวทางการแก้ไขปัญหา ดังนี้ 1) ผู้อำนวยการโรงพยาบาลฯ 2) หัวหน้างานสารสนเทศและเวชระเบียนฯ 3) หัวหน้าระดับผู้ปฏิบัติงานของOPD, Ward และ หน่วยที่เกี่ยวข้องอื่นๆ 4) นายทหารเวรสั่งการ 5) นายทหารเวรประจำวัน - แจ้งผู้ใช้งานทราบโดยประชาสัมพันธ์ประกาศเสียงตามสาย - ให้เตรียมใช้แผนฉุกเฉินระบบ IT ล่ม - ประเมินสถานการณ์เป็นระยะ - หน่วยงานต่างๆ สามารถให้บริการได้ตามปกติโดยจะรอใช้งานระบบสารสนเทศโรงพยาบาลเมื่อใช้งานได้แล้วหรือใช้ระบบ Manual ก็ได้ขึ้นอยู่กับ บริบทของแต่ละหน่วย (กรณี Manual - หากมีค่าใช้จ่ายใดเกิดขึ้นต้องนำข้อมูล การให้บริการบันทึกข้อมูลในคอมพิวเตอร์ย้อนหลัง)
กรณีปัญหาเกิดจากระบบเครือข่ายขัดข้องให้แจ้งว่า	"ขณะนี้ระบบเครือข่ายขัดข้องเป็นเหตุให้ระบบสารสนเทศโรงพยาบาลใช้งานไม่ได้ทั้ง โรงพยาบาล/บางจุด/บริเวณ..... เจ้าหน้าที่กำลังดำเนินการแก้ไขหากแก้ไขเสร็จจะแจ้งให้ทราบ"
กรณีปัญหาเกิดจากระบบสารสนเทศโรงพยาบาลให้แจ้งว่า	"ขณะนี้ระบบสารสนเทศโรงพยาบาล ขัดข้องใช้งานไม่ได้ทั้งโรงพยาบาล/บางจุด/บริเวณ.....เจ้าหน้าที่กำลังดำเนินการแก้ไขหากแก้ไขเสร็จจะแจ้งให้ ทราบ"
กรณีไม่สามารถแก้ไขปัญหาได้ภายใน 30 นาที แต่ไม่เกิน 6 ชั่วโมง	- รายงานสถานการณ์ต่อผู้บังคับบัญชาตามลำดับ ให้รับทราบถึงความรุนแรงและการแก้ไขปัญหาที่ดำเนินการอยู่ - แจ้งผู้ใช้งานทราบโดยประชาสัมพันธ์ประกาศเสียงตามสาย - ให้เตรียมใช้แผนฉุกเฉินระบบ IT ล่ม - ประเมินสถานการณ์เป็นระยะ

ช่วงระยะเวลาแก้ปัญหา	ขั้นตอนปฏิบัติและข้อความประกาศแจ้ง
กรณีไม่สามารถแก้ไขปัญหาได้ภายใน 30 นาที แต่ไม่เกิน 6 ชั่วโมง(ต่อ)	- หน่วยงานต่างๆ สามารถให้บริการได้ตามปกติโดยจะรอใช้งานระบบสารสนเทศโรงพยาบาลเมื่อใช้งานได้แล้วหรือใช้ระบบ Manual ก็ได้ขึ้นอยู่กับ บริบทของแต่ละหน่วย (กรณี Manual หากมีค่าใช้จ่ายใดเกิดขึ้นต้องนำข้อมูล การให้บริการบันทึกข้อมูลในคอมพิวเตอร์ย้อนหลัง)
กรณีปัญหาเกิดจากระบบเครือข่ายขัดข้องให้แจ้งว่า	"ขณะนี้ระบบเครือข่ายขัดข้องเป็นเหตุให้ระบบสารสนเทศโรงพยาบาลใช้งานไม่ได้ทั้งโรงพยาบาล/บางจุด/บริเวณ..... ต้องใช้เวลาแก้ไขเกิน30นาที ขอให้หน่วยต่างๆให้บริการโดยใช้ระบบ Manual หากแก้ไขเสร็จจะแจ้งให้ ทราบ"
กรณีปัญหาเกิดจากระบบสารสนเทศโรงพยาบาลให้แจ้งว่า	"ขณะนี้ระบบสารสนเทศโรงพยาบาล ขัดข้องใช้งานไม่ได้ทั้งโรงพยาบาล/บาง จุด/บริเวณ.....ต้องใช้เวลาแก้ไขเกิน30นาทีขอให้หน่วยต่างๆ ให้บริการ โดยใช้ระบบ Manual หากแก้ไขเสร็จจะแจ้งให้ทราบ"
กรณีไม่สามารถแก้ไขปัญหาได้ภายใน 6 ชั่วโมง	- รายงานสถานการณ์ต่อผู้บังคับบัญชาตามลำดับ ให้รับทราบถึงความรุนแรงและการแก้ไขปัญหาที่ดำเนินการอยู่ - แจ้งผู้ใช้งานทราบและใช้แผนฉุกเฉินระบบ IT ล่ม โดยประชาสัมพันธ์ประกาศเสียงตามสาย
กรณีปัญหาเกิดจากระบบเครือข่ายขัดข้องให้แจ้งว่า	"ขณะนี้ระบบเครือข่ายขัดข้องเป็นเหตุให้ระบบงานของโรงพยาบาลใช้งานไม่ได้ทั้งโรงพยาบาล/บางจุด/บริเวณ..... ต้องใช้เวลาแก้ไขเกิน 6 ชั่วโมงขอให้หน่วยต่างๆปฏิบัติตามแผน IT ล่ม"
กรณีปัญหาเกิดจากระบบสารสนเทศโรงพยาบาลให้แจ้งว่า	"ขณะนี้ระบบงานของโรงพยาบาล ขัดข้องใช้งานไม่ได้ทั้งโรงพยาบาล/บาง จุด/บริเวณ..... ต้องใช้เวลาแก้ไขเกิน 6 ชั่วโมง ขอให้หน่วยต่างๆ ปฏิบัติตาม แผน IT ล่ม" (โรงพยาบาลหยุดให้บริการตรวจรักษา หน่วยงานต่างๆปฏิบัติตามแผนIT ล่ม (ต้องนำข้อมูลการให้บริการบันทึกข้อมูลในระบบสารสนเทศย้อนหลัง)

การประเมินสถานการณ์เป็นระยะ

- ทีมปฏิบัติการITศูนย์คอมพิวเตอร์โรงพยาบาลดำเนินการแก้ไขปัญหาและกู้คืนระบบเมื่อได้รับแจ้งว่าระบบงานของโรงพยาบาลหรือระบบอินเทอร์เน็ตของเครื่องคอมพิวเตอร์เกิดขัดข้อง ทำให้หน่วยงานไม่สามารถให้บริการรักษาผู้ป่วยได้
- ประกาศเสียงตามสายภายในโรงพยาบาลตามข้อความที่กำหนดไว้
- การปฏิบัติงานของหน่วยงาน ให้คำนึงถึงความจำเป็นในการให้บริการผู้ป่วยเป็นหลัก โดยขั้นตอนใดที่จำเป็นต้องรอระบบIT ให้หยุดกิจกรรมหรือขั้นตอนนั้นไว้ก่อน หากกิจกรรมหรือบริการใดที่ไม่สามารถรอได้ให้ใช้ระบบ Manual ในการให้บริการผู้ป่วย
- เตรียมอุปกรณ์และเอกสารที่ต้องใช้ตามแผน IT ล่ม
- แจ้งประชาสัมพันธ์ให้ผู้รับบริการทราบเป็นระยะ
- เมื่อศูนย์คอมพิวเตอร์แก้ปัญหาได้แล้วแจ้งผู้ใช้งานทราบโดยประชาสัมพันธ์ประกาศเสียงตามสายว่า “ขณะนี้ ระบบสารสนเทศโรงพยาบาลใช้งานได้ปกติ”
- แจ้งผู้ปฏิบัติงานในหน่วยให้นำข้อมูลที่เกิดขึ้นระหว่างการใช้ระบบManualในการให้บริการกลับมาบันทึกเข้าสู่ระบบสารสนเทศ หากมีปัญหา/ข้อขัดข้องในการปฏิบัติให้ประสานเจ้าหน้าที่ศูนย์คอมพิวเตอร์ของโรงพยาบาล

ขั้นตอนการบริหารความต่อเนื่องและกอบกู้กระบวนการ



เพื่อให้การกู้คืนระบบเซิร์ฟเวอร์ของโรงพยาบาล (เช่น รพ.พระมงกุฎเกล้า) หลังจากเกิดภัยพิบัติหรือการโจมตีทางไซเบอร์เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ ควรมี “แผนฟื้นฟูระบบ” (Disaster Recovery Plan: DRP) ที่กำหนด ช่วงเวลาและขั้นตอนปฏิบัติอย่างแน่นอน ดังนี้:

8.การวิเคราะห์เพื่อกำหนดความต้องการทรัพยากรที่สำคัญ

สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน มีหลากหลายรูปแบบดังนั้นเพื่อให้ศูนย์คอมพิวเตอร์รพ.รร.6 สามารถบริหารจัดการการดำเนินงานของหน่วยงานให้มีความต่อเนื่องการดูแลและจัดหาทรัพยากรที่สำคัญจึงเป็นสิ่งจำเป็นและต้องระบุไว้ในแผนดำเนินธุรกิจอย่างต่อเนื่องฯซึ่งการเตรียมทรัพยากรที่สำคัญจากผลกระทบใน 5 ด้าน ดังนี้

1. ผลกระทบด้านอาคาร/สถานที่ปฏิบัติงานหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ สถานที่ปฏิบัติงานหลักได้รับความเสียหายหรือไม่สามารถใช้สถานที่ปฏิบัติงานหลักได้และส่งผลให้บุคลากรไม่สามารถเข้าไปปฏิบัติงานได้ชั่วคราวหรือระยะยาว
2. ผลกระทบด้านวัสดุอุปกรณ์ที่สำคัญ / การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ไม่สามารถใช้งานวัสดุอุปกรณ์ที่สำคัญหรือไม่สามารถจัดหา/จัดส่งวัสดุอุปกรณ์ที่สำคัญได้
3. ผลกระทบด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ระบบงานรพ.ระบบอินเตอร์เน็ทและระบบอื่น หรือข้อมูลที่สำคัญ ไม่สามารถนำมาใช้ในการปฏิบัติงานได้ตามปกติ
4. ผลกระทบด้านบุคลากรหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นซึ่งทำให้บุคลากรหลักไม่สามารถมาปฏิบัติงานได้ตามปกติ
5. ผลกระทบด้านคู่ค้า / ผู้ให้บริการ / ผู้มีส่วนได้ส่วนเสีย หมายถึง เหตุการณ์ที่เกิดขึ้นซึ่งทำให้คู่ค้า/ผู้ที่ศูนย์คอมพิวเตอร์ รพ.รร.6 ให้บริการหรือรับบริการ/ ผู้มีส่วนได้ส่วนเสียไม่สามารถติดต่อหรือให้บริการหรือส่งมอบงานได้

1. ด้านสถานที่ปฏิบัติงานสำรอง (Working Space Requirement)

ตารางที่ 1 ระบุพื้นที่การปฏิบัติงานสำรอง

ทรัพยากร	สถานที่	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ				
		1วัน	3วัน	7 วัน	15 วัน	30 วัน
พื้นที่สำหรับปฏิบัติงานสำรองภายในรพ.	ตึกสมเด็จพระนางเจ้าสิริกิติ์ฯ ชั้น 3 ห้องปฏิบัติการสารสนเทศ ตั้งเป็นฐานปฏิบัติการชั่วคราว	10 ตรม./ 5 คน	-	-	-	-
พื้นที่สำหรับปฏิบัติงานภายนอก	กรมแพทย์ทหารบก (สำรองที่1) ตั้งเป็นฐานปฏิบัติการชั่วคราว ใช้ DR-siteในการเชื่อมต่อระบบ	20 ตรม./20คน	-	-	-	-
	กรมทหารสื่อสาร (สำรองที่2) ตั้งเป็นฐานปฏิบัติการชั่วคราว ใช้ DR-siteในการเชื่อมต่อระบบ	30 ตรม./ 25คน	-	-	-	-

2. ความต้องการด้านอุปกรณ์ (Equipment & Supplies Requirement)

ตารางที่ 2 ระบุจำนวนอุปกรณ์ที่ต้องการตารางอุปกรณ์เพื่อสนับสนุนการจัดตั้งฐานปฏิบัติงานในสถานการณ์ฉุกเฉิน

ทรัพยากรสำหรับเพื่อใช้งานนอกสถานที่ (สำหรับผู้ให้บริการผู้ป่วย)		
ชนิดทรัพยากร	**ลักษณะการใช้งาน**	**จำนวน**
PC ชนิด All in one	เพื่อสำหรับใช้ในการปฏิบัติงานของบุคลากร	5-10เครื่อง
Notebook	เพื่อสำหรับใช้ในการปฏิบัติงานของบุคลากร	5-10เครื่อง
Flash drive	เพื่อสำหรับจัดเก็บข้อมูลอื่นๆนอกเหนือ	5-10 อัน
เครื่องปริ้นเตอร์เลเซอร์ ชนิดพิมพ์ร้อนและสแกนเอกสาร	เพื่อสำหรับใช้ในด้านงานเอกสาร	5เครื่อง

ทรัพยากรสำหรับเพื่อใช้งานนอกสถานที่ (สำหรับผู้ปฏิบัติงาน)		
ชนิดของทรัพยากร	**ลักษณะการใช้งาน**	**จำนวน**
Server main เครื่องแม่ข่าย	เพื่อจำลองขนาดกลางและใหญ่(แบบเคลื่อนที่)	2 เครื่อง
Core switch and Data center	สวิตช์สำหรับควบคุมและเชื่อมต่อระบบ	2 ตัว
Ethernet switch 24/48 port	สวิตช์สำหรับการเชื่อมต่ออุปกรณ์เข้ากับServer	3 ตัว
Wireless access point ขนาดกลางและใหญ่	เพื่อสำหรับรองรับผู้ใช้งาน200 Client ขึ้นไป	3 ตัว
Router	เพื่อสำหรับกระจายเข้ากับอุปกรณ์ต่างๆ	5ตัว
สายสัญญาณชั่วคราว (Lan)	เพื่อสำหรับเชื่อมต่อเข้ากับอุปกรณ์ต่างๆ	1กล่อง
หัวต่อ C6 และชุดอุปกรณ์เข้าหัว	เพื่อสำหรับเชื่อมต่อเข้ากับอุปกรณ์ต่างๆ	20-30 หัว
Hard disk อุปกรณ์เก็บข้อมูล (Bake up Data)	เพื่อสำหรับจัดเก็บไฟล์ข้อมูลผู้ป่วยเพื่อนำกลับเข้าสู่ระบบหลังการฟื้นฟู	2 อัน
A-tonal Hard disk/Flash drive	เพื่อสำหรับจัดเก็บข้อมูลอื่นๆนอกเหนือ	5-10อัน
Notebook / PC ชนิด All in one	เพื่อสำหรับใช้ในการปฏิบัติงานของบุคลากร	10-15 เครื่อง
เครื่องปริ้นเตอร์เลเซอร์ ชนิดพิมพ์ร้อนและสแกนเอกสาร	เพื่อสำหรับใช้ในด้านงานเอกสาร	5เครื่อง

3. ความต้องการด้านเทคโนโลยีสารสนเทศและข้อมูล (IT & information Requirement)

ตารางที่ 3 ระบุความต้องการด้านเทคโนโลยีสารสนเทศและข้อมูล

ระดับ	ระบุเทคโนโลยีสารสนเทศ	ผู้รับผิดชอบ	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ					
ผลกระทบ	และข้อมูลที่ต้องการ	กลุ่ม	4-24ชม.	1 วัน	3 วัน	7 วัน	15วัน	30 วัน
สูงมาก	ระบบ (HIS)	ทีมปฏิบัติการ IT ภาวะฉุกเฉิน	✓	-	-	-	-	-
	ระบบเครือข่าย (internet/intranet)	ทีมปฏิบัติการ IT ภาวะฉุกเฉิน	✓	-	-	-	-	-
สูง	เวชระเบียน (EMR)	ทีมปฏิบัติการ IT ภาวะฉุกเฉิน	✓	-	-	-	-	-
	Image ประวัติผู้ป่วย	ทีมปฏิบัติการ IT ภาวะฉุกเฉิน	✓	-	-	-	-	-

ระดับ ผลกระทบ	ระบุเทคโนโลยีสารสนเทศ และข้อมูลที่ต้องการ	ผู้รับผิดชอบ กลุ่ม	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ					
			4-24ชม.	1 วัน	3 วัน	7 วัน	15วัน	30 วัน
ปานกลาง	ระบบแล็ป(LIS)	ทีมปฏิบัติการ IT ภาวะฉุกเฉิน	✓	-	-	-	-	-
	ระบบภาพรังสี (PACS)	ทีมปฏิบัติการ IT ภาวะฉุกเฉิน	✓	-	-	-	-	-
ต่ำ	อุปกรณ์คอมพิวเตอร์อื่นๆ	ทีมสนับสนุนการดำเนินงาน IT ภาวะฉุกเฉิน	✓	-	-	-	-	-
	จัดหาโปรแกรมป้องกันความปลอดภัยของระบบ	ทีมเฝ้าระวังความปลอดภัยไซเบอร์ IT ภาวะฉุกเฉิน	✓	-	-	-	-	-

4. ความต้องการด้านบุคลากรสำหรับความต่อเนื่องเพื่อปฏิบัติงาน (Personnel Requirement)

ตารางที่ 4 ความต้องการด้านบุคคลในการปฏิบัติงาน

ทีมปฏิบัติงาน	**จำนวนบุคลากรที่ต้องการตามระยะเป้าหมายในการฟื้นคืนสภาพ**				
	1วัน	**3วัน**	**7 วัน**	**15 วัน**	**30 วัน**
ทีมบริหารและควบคุมแผน IT ภาวะฉุกเฉิน	3นาย	-	-	-	-
ทีมปฏิบัติการ IT ภาวะฉุกเฉิน - ดูแลด้านเครือข่ายและความปลอดภัย	4นาย	-	-	-	-
- ดูแลด้านเซิร์ฟเวอร์และฐานข้อมูล	4นาย	-	-	-	-
- ดูแลด้านสำรองข้อมูลและและกู้คืนระบบDR	4นาย	-	-	-	-
ทีมเฝ้าระวังและความปลอดภัยไซเบอร์ IT ภาวะฉุกเฉิน	5นาย	-	-	-	-
ทีมสนับสนุนการดำเนินงาน IT ภาวะฉุกเฉิน	5นาย	-	-	-	-
ทีมประสานงานและสื่อสารในภาวะฉุกเฉิน	4นาย	-	-	-	-
ทีมที่ปรึกษาและสนับสนุนการปฏิบัติงาน(บริษัทNominee)	4นาย	-	-	-	-
ทีมกำลังพลในการสนับสนุนเพิ่มเติม	7นาย	-	-	-	-

5. ความต้องการด้านผู้ให้บริการที่สำคัญ (Service Requirement)

การจัดการและวางแผนความพร้อมของ "ผู้ให้บริการจากภายนอก" ที่โรงพยาบาลจำเป็นต้องพึ่งพา ในกรณีฉุกเฉิน เช่น ระบบล่ม, อุปกรณ์เสีย หรือการกู้คืนข้อมูล การมีแผนที่ชัดเจนช่วยให้สามารถเรียกใช้บริการได้ทันท่วงที และลดผลกระทบจากเหตุการณ์ที่เกิดขึ้น

ตารางที่ 5 ความต้องการที่สำหรับติดต่อหรือผู้ให้บริการจากภายนอก

ประเภททรัพยากร	จำนวนผู้ให้บริการระยะเวลาเป้าหมายในการฟื้นคืนสภาพ				
	1วัน	3วัน	7 วัน	15 วัน	30 วัน
ผู้ให้บริการเชื่อมโยงระบบเครือข่ายInternet/Intranet	1หน่วย	-	-	-	-
ผู้ให้บริการดูแลอุปกรณ์คอมพิวเตอร์ของระบบงานรพ.	2หน่วย	-	-	-	-
ผู้ให้บริการดูแลเครื่องแม่ข่ายและสนับสนุนอุปกรณ์จัดเก็บข้อมูล	1หน่วย	-	-	-	-
ผู้ให้บริการด้านระบบไฟฟ้าและสนับสนุนรถปั่นไฟสำรอง	1หน่วย	-	-	-	-
ผู้ให้บริหารสัญญาณวิทยุสื่อสารและอุปกรณ์สนับสนุนกระจายสัญญาณระยะใกล้	1หน่วย	-	-	-	-

9.กลยุทธ์ความต่อเนื่อง(Business Continuity Strategy)

กลยุทธ์ความต่อเนื่องเป็นแนวทางในการจัดหาและบริหารจัดการทรัพยากรให้มีความพร้อมเมื่อเกิดสภาวะวิกฤตซึ่งพิจารณาจาก 5ด้าน ดังนี้

ทรัพยากร	กลยุทธ์ความต่อเนื่อง
อาคาร/สถานที่ปฏิบัติงาน	สถานที่ทำงานภายใน คือ อาคารสมเด็จพระนางเจ้าสิริกิติติ ชั้น3 ห้องปฏิบัติการและสารสนเทศ
	สถานที่ทำงานภายนอก คือ 1.กรมแพทย์ทหารบก 2.กรมทหารสื่อสาร
	ปฏิบัติงานที่บ้านเป็นการชั่วคราว (WFH)
	การจัดประชุมออนไลน์
วัสดุอุปกรณ์ที่สำคัญ/การจัดหา/จัดส่งอุปกรณ์ที่สำคัญ	จัดเตรียมจัดหาเครื่องคอมพิวเตอร์สำรองใช้งาน Notebook/ PC All in one
	เครื่องพิมพ์เอกสาร/เครื่องถ่ายเอกสารแบบ In one
	อินเทอร์เน็ต Internet/ Internet Roter -WiFi
	จัดเตรียมจัดหาวัสดุอุปกรณ์ต่างๆที่จำเป็นต้องใช้งาน ทั้งสิ้นเปลืองอื่นๆ ให้เพียงพอตามความเหมาะสม

เทคโนโลยีสารสนเทศและข้อมูลสำคัญ	ข้อมูลสำคัญจัดเก็บสำรองไว้ที่ DR-Site (Disaster Recovery Site) ณ กรมทหารสื่อสาร
	เครื่องServerเคลื่อนย้ายไปยังที่ปลอดภัย หรือพื้นที่ปฏิบัติงานสำรองในกรณีที่จำเป็นต้องดำเนินการและสามารถทำได้
	อุปกรณ์ระบบคอมพิวเตอร์และระบบเครือข่าย
	ระบบสารสนเทศภายในหน่วย
	ข้อมูลแผนงาน งบประมาณ และข้อมูลที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ
บุคลากร	กำหนดให้มีกำลังพลสำรองดังข้างต้นหรือกำหนดให้มีกำลังพลภายนอกหากไม่เพียงพอหรือขาดแคลน
ผู้ให้บริการที่สำคัญ/ผู้มีส่วนได้เสีย	ระบบLink Internet หากล่ม สามารถใช้เส้นทางสำรองของเอกชนหรือLinkคู่ขนาน
	ประสานงานผู้ให้บริการทั้งรายปัจจุบันและ/หรือรายใหม่เพื่อรองรับการให้บริการแทนภายในSLAที่กำหนดไว้
	ใช้ระบบ Internet แบบพกพา (Pocket WiFi) เพื่อใช้งานชั่วคราว
	ประสานงานติดต่อสื่อสารผู้เกี่ยวข้องผ่านทางระบบInternet

ตัวอย่าง ขั้นตอนการเมื่อเกิดสถาการณ์รูปแบบต่างๆและระยะเวลากอบการกู้คืนสภาพการปฏิบัติเมื่อเกิดกรณี Network Down

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ	หมายเหตุ
ขั้นตอนที่ 1: ตรวจพบปัญหา ขั้นตอนที่ 2: ประเมินสถานการณ์ ขั้นตอนที่ 3: แจ้งเตือนผู้เกี่ยวข้อง ขั้นตอนที่ 6: สื่อสารต่อเนื่อง ขั้นตอนที่ 5: ดำเนินแผนการทำงานชั่วคราว ขั้นตอนที่ 4: ดำเนินการแก้ไขเบื้องต้น ขั้นตอนที่ 7: ฟื้นฟูระบบ ขั้นตอนที่ 8: สรุปบทเรียนและปรับปรุง	ทีมปฏิบัติการ IT ภาวะฉุกเฉิน ทีมเฝ้าระวังและความปลอดภัยไซเบอร์ และทีมสนับสนุนการดำเนินงาน IT ภาวะฉุกเฉิน		

สรุปขั้นตอนการปฏิบัติเมื่อเกิดกรณี Network Down

1. ตรวจพบปัญหาและประเมินสถานการณ์
   - ตรวจพบปัญหา Network ใช้งานไม่ได้ เช่นได้รับรายงานมาจาก user ว่าเข้าระบบไม่ได้
   - ตรวจสอบขอบเขตของปัญหา (ทั้งองค์กร หรือเฉพาะบางแผนก)
   - ตรวจสอบและระบุระบบที่เกิดปัญหาว่าเป็นที่ระบบใด (ระบบPMK/NET) ในกรณีที่เป็นบางแผนก
   - ตรวจสอบและระบุระบบที่เกิดปัญหาว่าเป็นที่ระบบใด (ระบบPMK/NET)
   - แจ้งเตือนผู้เกี่ยวข้อง
   - ตรวจสอบและระบุระบบที่เกิดปัญหาว่าเป็นที่ระบบใด(ระบบPMK/NET) ในกรณีที่เป็นทั้งองค์กร
   - กรณีเป็นระบบ NET ตรวจสอบว่าเป็นปัญหาภายในหรือจากผู้ให้บริการ (UNI NET)
   - ประเมินระยะเวลาในการแก้ไขปัญหา
   - แจ้งเตือนผู้เกี่ยวข้อง
2. แจ้งเตือนผู้เกี่ยวข้อง
   - แจ้งผู้ใช้งานว่ากำลังมีปัญหาเครือข่าย
   - ดำเนินการแก้ไขเบื้องต้นบางแผนก
   - กรณีประเมินแล้วไม่สามารถแก้ไขในระยะเวลาอันสั้นทั้งองค์กร
   - แจ้งเตือนผู้บริหารหรือผู้ใช้งานตามช่องทางต่างๆ เช่น โทรศัพท์, LINE, Google chat
   - ดำเนินแผนการทำงานชั่วคราว
3. ดำเนินการแก้ไขเบื้องต้น
   - ทำการตรวจเช็คสาย Uplink หรือลอง restart อุปกรณ์ Network
   - ให้ทำการแจ้งบริษัทที่ดูแล Network เข้ามาดำเนินการแก้ไขแก้ไขไม่ได้
   - เมื่อระบบเครือข่ายกลับมาใช้งานได้ ให้ทดสอบระบบให้แน่ใจว่าเสถียร
   - ให้ User กลับมาใช้งานระบบตามปกติ
   - ให้ทดสอบระบบให้แน่ใจว่าเสถียรแก้ไขได้
   - ให้เจ้าหน้าที่กลับมาใช้งานระบบตามปกติ
4. ดำเนินแผนการทำงานชั่วคราว
   - วิธีการแก้ไขเบื้องต้นโดยวิธีการทำงานด้วยมือเช่น เขียนผลการตรวจลงกระดาษด้วยมือไปก่อน
   - ในกรณีที่มีปัญหาไม่สามารถแก้ไขปัญหาในระยะเวลาอันสั้นให้สลับการเชื่อมต่อไปยัง network สำรอง
   - สื่อสารต่อเนื่อง
5. สื่อสารต่อเนื่อง
   - ประสานงานบริษัทที่ดูแลระบบNetworkและคอยแจ้งสถานการณ์กับผู้บริหารหรือหน่วยงานที่เกี่ยวข้อง
   - แจ้งสถานะความคืบหน้าแก่ผู้บริหารและผู้ใช้งานทุก 30-60 นาทีผ่านช่องทาง โทรศัพท์, LINE, google chat
   - ฟื้นฟูระบบ

6.ฟื้นฟูระบบ

- เมื่อระบบเครือข่ายกลับมาใช้งานได้ ให้ทดสอบระบบให้แน่ใจว่าเสถียร
- ให้เจ้าหน้าที่กลับมาใช้งานระบบตามปกติ
- ซิงค์ข้อมูลจากเอกสารออฟไลน์กลับเข้าระบบ(scan opd card ที่เขียนด้วยมือเข้าระบบ)
- สรุปบทเรียนและปรับปรุง

7.สรุปบทเรียนและปรับปรุง

- สรุปสาเหตุของปัญหา
- นำปัญหาที่ได้จากการสรุปไปปรับปรุงแก้ไขเพื่อรับมือกับปัญหาที่อาจจะเกิดในอนาคต
- ทำรายงานสรุปให้ผู้บริหาร

การปฏิบัติเมื่อเกิดกรณีการบุกรุกหรือโจมตี Ransomware

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ	หมายเหตุ
ขั้นตอนที่ 1: ตรวจพบการโจมตี ขั้นตอนที่ 2: การระบุและประเมินสถานการณ์ ขั้นตอนที่ 3: เปิดใช้งานแผน BCP ขั้นตอนที่ 4: การควบคุมความเสียหายและจำกัดวงการโจมตี ขั้นตอนที่ 5: กู้คืนระบบที่สำคัญ ขั้นตอนที่ 6: การดำเนินธุรกิจต่อเนื่องในรูปแบบชั่วคราว ขั้นตอนที่ 7: สื่อสารกับผู้เกี่ยวข้อง ขั้นตอนที่ 8: ฟื้นฟูสู่ภาวะปกติ ขั้นตอนที่ 9: การทบทวนและปรับปรุงแผน	ทีมปฏิบัติการ IT ภาวะฉุกเฉินและทีมเฝ้าระวังและความปลอดภัยไซเบอร์		

สรุปขั้นตอนการปฏิบัติเมื่อเกิดกรณีถูกบุกรุกจาก Ransomware

1.ตรวจพบการโจมตีจาก Ransomware

- แจ้งเตือนและประสานงาน
- ประสานงานกับหน่วยงานภายนอก เช่น CERT, กสมช., หน่วยงานทางกฎหมาย
- แจ้งทีม IT Security/Incident Response ทันที⟶ แจ้งผู้บริหารที่เกี่ยวข้องตามลำดับชั้นความเร่งด่วน

2.การระบุและประเมินสถานการณ์ (Incident Identification & Assessment)

- การระบุและประเมินสถานการณ์
- ตรวจสอบประเภทการโจมตีจาก Ransomware เช่น ข้อมูลถูกเข้ารหัส และมีข้อความเรียกค่าไถ่
- ประสานงานกับหน่วยงานภายนอก เช่น CERT, สกมช., หน่วยงานทางกฎหมาย
- แจ้งเตือนทีมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Team)⟶ ประเมินผลกระทบต่อ
- กระบวนการธุรกิจหลัก

3.การเปิดใช้งานแผน BCP (BCP Activation)

- การเปิดใช้งานแผน BCP
- ผู้มีอำนาจตัดสินใจประกาศใช้ BCP
- จัดตั้งศูนย์ควบคุมวิกฤต (Crisis anagement Team)
- ประสานงานกับทีมที่เกี่ยวข้อง

4.การควบคุมความเสียหายและจำกัดวงการโจมตี (Containment)

- การควบคุมความเสียหายและจำกัดวงการโจมตี
- ตัดการเชื่อมต่อระบบที่ติด มัลแวร์ออกจากเครือข่ายแยกระบบที่ติดไวรัส
- ประสานงานกับทีม BCP ทำงานเพื่อรายงานสถานการณ์ประสานงานกับผู้ใช้งาน
- ปิดระบบที่ได้รับผลกระทบชั่วคราว⟶ วิเคราะห์พฤติกรรมของ Ransomware และ เส้นทางการแพร่กระจาย⟶

5.การกู้คืนระบบที่สำคัญ (Critical System Recovery)

- การกู้คืนระบบที่สำคัญ
- ใช้ข้อมูลจากการสำรอง (Backup) ที่ปลอดภัยก่อนการโจมตี
- DATA Backup โดน Ransomware
- แจ้งฝ่ายบริหารระดับสูง
- ประเมินตัวเลือก (จ่ายค่าไถ่/ฟื้นระบบ /สื่อสาร)
- DATA Backup ไม่โดนโดน Ransomware
- นำระบบสำรองเข้าสู่ระบบปฏิบัติการตามแผน DR (Disaster Recovery)
- ทดสอบความสมบูรณ์ข้อมูล ทดสอบความถูกต้องของข้อมูลและระบบที่กู้คืน

6.การดำเนินธุรกิจต่อเนื่องในรูปแบบชั่วคราว(Alternative Business Operation)

- การดำเนินธุรกิจต่อเนื่องในรูปแบบชั่วคราว
- ใช้ระบบสำรอง (เช่น)manual process⟶ ดำเนินการโดยใช้กระดาษCloud DR Site⟶ ประเมินเวลาในการ Recover
- แจ้งผู้มีส่วนได้เสีย เช่น ลูกค้า คู่ค้า ให้ทราบสถานะ

7.การสื่อสารภายในและภายนอก (Communication Plan)

- การสื่อสารภายในและภายนอก
- สื่อสารกับพนักงานภายในองค์กรด้วยข้อมูลที่ถูกต้องและต่อเนื่อง
- ออกแถลงการณ์ต่อสาธารณะหากจำเป็น
- รักษาความโปร่งใสและความเชื่อมั่นของผู้เกี่ยวข้อง

8.การฟื้นฟูสู่ภาวะปกติ (Restoration to Normal Operations)

- การฟื้นฟูสู่ภาวะปกติ
- คืนค่าระบบจาก Backup ที่ปลอดภัย
- ตรวจสอบให้แน่ใจว่าระบบปลอดจากมัลแวร์

9.การทบทวนและปรับปรุงแผน BCP (Post-Incident Review) นำระบบหลักเข้าสู่กระบวนการปกติ

- การทบทวนและปรับปรุงแผน BCP
- วิเคราะห์จุดอ่อนที่ถูกโจมตี
- ปรับปรุงมาตรการด้าน Cybersecurity และ BCP
- ฝึกอบรมพนักงานและซ้อมแผน BCP ใหม่

การปฏิบัติเมื่อเกิดกรณีไฟฟ้าขัดข้อง(ภายในอาคาร/นอก)

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ	หมายเหตุ
ขั้นตอนที่ 1: ตรวจพบไฟฟ้าดับ ขั้นตอนที่ 2: ประเมินสถานการณ์ ขั้นตอนที่ 3: แจ้งเตือนและประสานงานผู้เกี่ยวข้อง ขั้นตอนที่ 4: ตรวจสอบระบบไฟฟ้าสำรอง ขั้นตอนที่ 5: ดำเนินแผนการทำงานชั่วคราว ขั้นตอนที่ 7: แผนการฟื้นฟูหลังไฟฟ้ากลับมาใช้งานได้ ขั้นตอนที่ 8: การทบทวนและปรับปรุงแผน	ทีมปฏิบัติการ IT ภาวะฉุกเฉินและทีมเฝ้าระวังและความปลอดภัยไซเบอร์		

สรุปขั้นตอนการปฏิบัติเมื่อเกิดกรณีไฟฟ้าขัดข้อง

1.พบปัญหา

- ผู้ใช้งานแจ้งปัญหาว่าใช้ไฟฟ้าไม่ได้

2. ประเมินสถานการณ์

- ตรวจสอบการใช้งานที่ไฟฟ้าดับ มีจุดใดบ้าง (ทั้งโรงพยาบาลหรือเฉพาะตึกนั้นๆ)

3. แจ้งเตือนประสานงานผู้ที่เกี่ยวข้อง

- ประสานMEE เรื่องเวลาที่ไฟฟ้าดับ จะดับนานกี่นาที
- ประสานหน่วยงานต่างๆ ที่เกี่ยวข้อง
- ประสานผู้ใช้งาน เช่น โทรศัพท์ , Line

4. ตรวจสอบระบบไฟฟ้าสำรอง

- Server pmk ไฟฟ้าสำรองอยู่ได้ 2 ชั่วโมง
- Server ตึก สก. ไฟฟ้าสำรองอยู่ได้ 2 ชั่วโมง 30 นาที
- Ups server net ไฟฟ้าสำรองอยู่ได้ 1 ชั่วโมง

5. ดำเนินการแผนการทำงานชั่วคราว

- ทราบเวลาที่ไฟฟ้าดับ ให้ใช้ไฟฟ้าสำรองที่มี
- ถ้าไม่ทราบเวลาที่ดับ ดับทุกตึกหรือบางตึก ให้ตรวจและลงประวัติด้วยกระดาษเพื่อลงประวัติภายหลัง

6. การฟื้นฟูระบบหลังไฟฟ้ากลับมาสู่สภาวะปกติ
   - เปิดเครื่องแม่ข่ายให้สามารถกลับมาใช้งานได้ตามปกติ
   - ทดสอบการใช้งานก่อนแจ้งผู้ใช้งาน
7. การทบทวนปรับปรุงแผนการทำงาน
   - ซ้อมแผนไฟฟ้าดับอย่างน้อย 2ครั้ง ต่อปี
   - ทดสอบและปรับปรุงแผน BCP

วิธีการตอบสนองสำหรับทีมปฏิบัติ

1. ตรวจพบปัญหาและประเมินสถานการณ์
   - ตรวจพบไฟฟ้าดับ เช่น ได้รับแจ้งจากuser ว่าไฟฟ้าดับ
   - ประสานงานกับผู้ที่เกี่ยวข้องเพื่อทราบเวลาที่ไฟฟ้าดับ ดับทั้งรพ. หรือดับบางตึก
   - ในกรณีที่เป็นทั้งรพ.⟶ แจ้งหน่วยงานที่เกี่ยวข้องในกรณีที่เป็นบางตึก⟶ แจ้งหน่วยงานที่เกี่ยวข้อง
2. กรณีดับทั้งรพ.
   - แจ้งเตือนผู้ที่เกี่ยวข้อง
   - ใช้ระบบไฟฟ้าสำรอง
   - Server pmk ไฟฟ้าสำรองอยู่ได้ 2 ชั่วโมง
   - Server ตึก สก. ไฟฟ้าสำรองอยู่ได้ 2 ชั่วโมง 30 นาที
   - Ups server net ไฟฟ้าสำรองอยู่ได้ 1 ชั่วโมง
   - ถ้าหากเกินกว่าที่ใช้ไฟฟ้าสำรองได้ ต้องทำการ chut down server
   - ถ้ามีการตรวจคนไข้อยู่ให้ manual process จนกว่าไฟฟ้าจะกลับมาใช้งานได้ตามปกติ
3. กรณีดับบางตึก
   - แจ้งเตือนผู้ที่เกี่ยวข้อง
   - ใช้ระบบไฟฟ้าสำรองที่มีอยู่
   - Server pmk ไฟฟ้าสำรองอยู่ได้ 2 ชั่วโมง
   - Server ตึก สก. ไฟฟ้าสำรองอยู่ได้ 2 ชั่วโมง 30 นาที
   - Ups server net ไฟฟ้าสำรองอยู่ได้ 1 ชั่วโมง
   - ไฟฟ้าดับมากกว่าที่กำหนด⟶ ถ้าหากเกินกว่าที่ใช้ไฟฟ้าสำรองได้ ต้องทำการ chut down server
   - ไฟฟ้าดับน้อยกว่าที่กำหนด⟶ ถ้ามีการตรวจคนไข้อยู่ให้ manual process จนกว่าไฟฟ้าจะกลับมาใช้งานได้ตามปกติ
4. ทำงานชั่วคราวระหว่างที่ไฟฟ้าดับ
   - แผนการทำงาน
   - ตรวจคนไข้อยู่ให้ manual process จนกว่าไฟฟ้าจะกลับมาใช้งานได้ตามปกติ

   Opd, Ward, Lab ,X-ray, Drug

5. การฟื้นฟูระบบ
   - การฟื้นฟูระบบ
   - ถ้าหากระบบสามารถกลับมาใช้งานตามปกติแล้ว
   - ตรวจสอบระบบไฟฟ้าก่อนว่าสามารถใช้งานได้ตามปกติหรือไม่
   - ถ้าหากมีการchut down server ให้ทำการ on server
   - ตรวจสอบระบบไฟฟ้าและอุปกรณ์ที่เกี่ยวข้องว่าชำรุดเสียหายหรือไม่
   - ทดสอบการใช้งานของอุปกรณ์
6. การทบทวนปรับปรุงแผนการทำงาน
   - การทบทวนปรับปรุง
   - ซ้อมแผนไฟฟ้าดับอย่างน้อย2 ครั้ง ต่อปี
   - ปรับปรุงแผน BCP

การปฏิบัติเมื่อเกิดกรณีภัยธรรมชาติ(แผ่นดินไหว)

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ	หมายเหตุ
ขั้นตอนที่ 1: พบปัญหาแผ่นดินไหว ขั้นตอนที่ 2: ประเมินความเสี่ยงวิเคราะห์ผลกระทบ ขั้นตอนที่ 3: การวางมาตรการป้องกันและเตรียมความพร้อม ขั้นตอนที่ 4: แผนการตอบสนองเมื่อเกิดเหตุ (Incident Response Plan) ขั้นตอนที่ 5: แผนการฟื้นฟูและดำเนินงานต่อ (Recovery Plan) ขั้นตอนที่ 6: การทดสอบ ทบทวนและปรับปรุงแผน	ทีมปฏิบัติการ IT ภาวะฉุกเฉิน และทีมเฝ้าระวังและความปลอดภัยไซเบอร์		

สรุปขั้นตอนการปฏิบัติเมื่อเกิดกรณีแผ่นดินไหว

1.พบปัญหา
   - ตรวจสอบแน่ใจว่าเป็นเหตุแผ่นดินไหว

2.ประเมินความเสี่ยง/วิเคราะห์ผลกระทบ
   - อาคารสำนักงานพัง/เสียหาย
   - บุคลากรได้รับบาดเจ็บ
   - ไฟฟ้าดับ / ระบบ IT ใช้งานไม่ได้

3.การวางมาตรการป้องกันและเตรียมความพร้อม

- ตรวจสอบโครงสร้างอาคารให้มั่นคง รับแรงสั่นสะเทือนได้
- ติดตั้งเซ็นเซอร์ตรวจจับแรงสั่นสะเทือน
- ยึดเฟอร์นิเจอร์หนัก/ชั้นวาง/ตู้เซิร์ฟเวอร์ให้มั่นคง
- จัดอบรมและฝึกซ้อมอพยพกรณีแผ่นดินไหว ทุก 6 เดือน
- สถานที่ชั่วคราวในการทำงานของระบบ IT

4.แผนการตอบสนองเมื่อเกิดเหตุ (Incident Response Plan)

- หยุดกิจกรรมทั้งหมด
- อพยพตามเส้นทางที่กำหนด
- รวมพล ณ จุดปลอดภัย (ตามแผนผัง)
- ตรวจสอบจำนวนพนักงาน
- ทีมกู้ภัยเบื้องต้นเข้าตรวจสอบอาคาร

5.แผนการฟื้นฟูและดำเนินงานต่อ (Recovery Plan)

- อาคาร: ตรวจสอบโครงสร้าง
- ระบบ IT: ตรวจสอบเซิร์ฟเวอร์/ระบบ Cloud
- บุคลากร: ตรวจสอบความปลอดภัยและสภาพจิตใจ

6.การทดสอบ ทบทวน และปรับปรุงแผน

- ทดสอบแผน BCP อย่างน้อยปีละ 1 ครั้ง
- ประเมินผลการซ้อม / เหตุการณ์จริง และปรับปรุงแผนให้ทันสมัย
- อบรมพนักงานใหม่ และทบทวนความรู้กับพนักงานเดิม

วิธีการตอบสนองสำหรับทีมปฏิบัติ

1.พบปัญหาแผ่นดินไหว

- เมื่อแน่ใจว่าแผ่นดินไหว ,ตึก/อาคารสั่นไหว
- สิ่งของร่วงหล่น เช่น ฝ้า,ไฟ,ป้าย ต่างๆ ตึก/อาคารเกิดรอยร้าว เศษปูนร่วงหล่น
- แจ้งเจ้าหน้าที่อาคารหรือเจ้าหน้าที่รัฐที่เกี่ยวข้อง

2.ประเมินความเสี่ยงวิเคราะห์ผลกระทบ

2.1 วิเคราะห์ผลกระทบ

- ทรัพยากร : ระบบ HIS ,ระบบInternet ,อาคาร/สถานที่
- ผลกระทบ: User ใช้งานไม่ได้ ,ใช้งานไม่ได้บางพื้นที่,งดใช้บริการบางพื้นที่
- ระยะเวลาที่รับได้: 6 ชั่วโมง ,24 ชั่วโมง, 48 ชั่วโมง
- แก้ปัญหา : Shutdown/On Server, แจ้งบริษัทแก้ปัญหา, แจ้งหน่วยที่เกี่ยวข้อง

2.2 ประเมินความเสี่ยง ความเสี่ยง ,อาคารถล่ม, ระบบ IT ล่ม

- ความเป็นไปได้: ปานกลาง, สูง
- ผลกระทบ: ปานกลาง, สูง
- ความเสี่ยงรวม: ตรวจสอบโครงสร้างทุกปี, วางระบบสำรอง

3.การวางมาตรการป้องกันและเตรียมความพร้อม

- มาตรการป้องกันล่วงหน้า
- ตรวจสอบโครงสร้างอาคารให้มั่นคง รับแรงสั่นสะเทือนได้
- ติดตั้งเซ็นเซอร์ตรวจจับแรงสั่นสะเทือนเมื่อเกิดแผ่นดินไหวหรือ After Shock
- ยึดเฟอร์นิเจอร์หนัก/ชั้นวาง/ตู้เซิร์ฟเวอร์ให้มั่นคงไม่ให้ล้มหรือร่วงหล่น
- จัดอบรมและฝึกซ้อมอพยพกรณีแผ่นดินไหวทุก 6 เดือน
- จัดหาสถานที่ชั่วคราว เพื่อเป็นสถานที่ใช้ทำงานในช่วงที่ไม่สามารถใช้สถานที่หลักได้
- เตรียมความพร้อม
- แต่งตั้งทีม BCP / Emergency Response
- การแจ้งเตือน/ประชาสัมพันธ์ภายใน
- การอพยพและรวมตัวในพื้นที่ปลอดภัย
- การตรวจสอบความปลอดภัยหลังเหตุการณ์ คน /ทรัพย์สิน / ระบบ

4.แผนการฟื้นฟูและดำเนินงานต่อ

- แผนการฟื้นฟูและดำเนินงานต่อ
    - รายการกระบวนการธุรกิจที่สำคัญและลำดับความสำคัญ
    - สร้างแผนการทำงานในสถานที่สำรอง / ทำงานจากที่บ้าน

ระบบ IT: ตรวจสอบเซิร์ฟเวอร์ /ระบบ Cloudการกู้คืนข้อมูลและระบบ IT

บุคลากร: ตรวจสอบความปลอดภัยและสภาพจิตใจ

5.แผนการฟื้นฟูและดำเนินงานต่อ

- แผนการฟื้นฟูและดำเนินงานต่อ
    - รายการกระบวนการธุรกิจที่สำคัญและลำดับความสำคัญ
    - สร้างแผนการทำงานในสถานที่สำรอง / ทำงานจากที่บ้าน
    - ระบบ IT: ตรวจสอบเซิร์ฟเวอร์ / ระบบ Cloudการกู้คืนข้อมูลและระบบ IT
    - บุคลากร: ตรวจสอบความปลอดภัยและสภาพจิตใจ

ตารางแผนช่วงระยะเวลาในการกู้คืนระบบสารสนเทศของโรงพยาบาล

ช่วงเวลา	ระยะเวลา	ขั้นตอนรายละเอียด
ช่วงที่ 0: (การเตรียมความพร้อมล่วงหน้า)	ดำเนินการเป็นประจำ (ทุกเดือน/ไตรมาส)	- วิเคราะห์ความเสี่ยง (Risk Assessment) ระบุภัยคุกคามและผลกระทบต่อระบบแต่ละระบบ - กำหนด RTO/ RPO RTO (Recovery Time Objective): เวลากู้ระบบกลับให้ใช้งานได้ RPO (Recovery Point Objective): ข้อมูลที่ยอมให้สูญหายได้ - จัดทำแผนสำรองข้อมูล แบ่งเป็น onsite/offsite และcloud - ทดสอบแผน DRP จำลองสถานการณ์ปีละ 1–2 ครั้ง - จัดตั้งทีม DR Team แต่งตั้งผู้รับผิดชอบแต่ละบทบาท
ช่วงที่ 1: (แจ้งเหตุและควบคุมสถานการณ์)	0–1 ชั่วโมงแรก	**เป้าหมาย**: รวบรวมข้อมูล เหตุการณ์ และยับยั้งการแพร่กระจายของความเสียหาย - แจ้งเหตุ / เหตุฉุกเฉิน เจ้าหน้าที่ไอที แจ้งหัวหน้าทีม / ผู้บริหาร - ประเมินความเสียหาย ตรวจสอบว่าระบบใดได้รับผลกระทบ (ไฟดับ, Server พัง, โดน ransomware) - แยกระบบ / ปิดระบบต้นเหตุ ตัดสายระบบเครือข่าย, ปิด server บางตัว - ติดต่อผู้ให้บริการ Cloud / DR Site ถ้ามีการ replication ข้ามไซต์
ช่วงที่ 2: (เริ่มกระบวนการกู้คืนระบบหลัก)	1–6 ชั่วโมง	**เป้าหมาย**: นำระบบที่จำเป็นต่อภารกิจกลับมาใช้งานได้ก่อน - กู้คืนระบบจาก Backup เรียกคืนข้อมูลจาก NAS, Tape, Cloud หรือ DR Site - เปิดระบบสำคัญก่อน เช่น ระบบเวชระเบียน (HIS), LAB, RIS, PACS - ตรวจสอบความสมบูรณ์ของข้อมูล เทียบ hash หรือ checksum - ประสานงานกับหน่วยงานภายนอก เช่น หน่วย CERT, บริษัทที่ปรึกษาCyber

ช่วงเวลา	ระยะเวลา	ขั้นตอนรายละเอียด
ช่วงที่ 3: (กู้คืนระบบทั้งหมด)	6–24 ชั่วโมง	**เป้าหมาย:** ให้บริการทางการแพทย์กลับมาเกือบ 100% - ฟื้นฟูระบบรอง เช่น ระบบบัญชี, HR, ระบบข้อมูลผู้ป่วยเก่า - เปลี่ยนเครื่องเซิร์ฟเวอร์กรณีเสียหาย กรณีเซิร์ฟเวอร์หลักถูกทำลายจากไฟไหม - ทดสอบระบบที่กู้กลับมาทำ UAT (User Acceptance Test) เบื้องต้น
ช่วงที่ 4: (ตรวจสอบความปลอดภัยและติดตามผล)	1–3 วัน	**เป้าหมาย:** ปรับปรุงระบบให้ปลอดภัยและป้องกันเหตุซ้ำ - สแกนหาช่องโหว่ ใช้เครื่องมือเช่น Nessus, Qualys - ปรับปรุงนโยบายสำรองข้อมูล เช่น เพิ่มระยะเวลาสำรอง, สร้าง immutable backup - รายงานต่อผู้บริหาร / หน่วยงานภาครัฐ ตามมาตรฐาน PDPA/พ.ร.บ.การรักษาความมั่นคงไซเบอร์ - ประชุม Post-Mortem หาข้อบกพร่องในขั้นตอนต่างๆ เพื่อปรับปรุงแผน DRP

ระบบที่ควรกู้คืนตามลำดับความสำคัญลำดับ

ระบบ RTO หมายเหตุ

1. ระบบเวชระเบียน (HIS) 2–4 ชม. ให้บริการผู้ป่วย
2. ระบบแลบ (LIS)/ภาพถ่ายทางรังสี (PACS) 4–6 ชม. ตรวจวินิจฉัยโรค
3. ระบบห้องยา/ ระบบนัดหมาย 6–12 ชม. จ่ายยาและนัดหมายแพทย์
4. ระบบ HR, บัญชี, การเงิน 24–48 ชม. ไม่กระทบการรักษาโดยตรง

ขั้นตอนการบริหารความต่อเนื่องและกอบกู้กระบวนการ

วันที่1 การสนองต่อเหตุการณ์ทันที (ภายใน 24 ชั่วโมง)

การปฏิบัติการใดๆให้บุคลากรของทีมงานบริหารศูนย์คอมพิวเตอร์คำนึงถึงความปลอดภัยในชีวิตของตนเองรวมทั้งบุคลากรอื่นๆและปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติที่หน่วยงานกำหนดขึ้นอย่างเคร่งครัด

➢ การตอบสนองต่อเหตุการณ์ทันที (ภายใน24ชั่วโมง)		
ขั้นตอนและกิจกรรม	**ผู้รับผิดชอบ**	**ดำเนินการแล้วเสร็จ**
▪ ตรวจสอบและแจ้งเหตุที่เกิดภาวะฉุกเฉิน หัวหน้าคณะทำงานของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้าและประเมินระยะเวลา	ทีมปฏิบัติการITภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪ แจ้งเหตุฉุกเฉินตามกระบวนการ Call Tree ให้กับผู้ปฏิบัติงานในโรงพยาบาลทราบ ภายหลังได้รับแจ้งจากหัวหน้าคณะทำงานของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	ทีมประสานงานและสื่อสารภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪ จัดประชุมทีมงานเพื่อประเมินความเสียหาย ผลกระทบต่อการดำเนินงาน การให้บริการ และ ทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง ▪ ทบทวนกระบวนงานที่มีความเร่งด่วนหรือส่งผลกระทบอย่างสูง (หากไม่ดำเนินการ) ดังนั้น จำเป็นต้องดำเนินงาน หรือปฏิบัติด้วยมือ (Manual Processing)	ทีมสนับสนุนการดำเนินงาน ITภาวะฉุกเฉิน และ ทีมปฏิบัติการ ITภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪ ระบุและสรุปรายชื่อบุคลากรในศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้าที่ได้รับบาดเจ็บหรือเสียชีวิต	ทีมสนับสนุนการดำเนินงาน ITภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪ รายงานคณะบริหารความต่อเนื่องของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้าโดยครอบคลุมประเด็นดังนี้ - จำนวนและรายชื่อบุคลากรที่ได้รับบาดเจ็บ/เสียชีวิต - ความเสียหายและผลกระทบต่อการดำเนินงานและการให้บริการ - ทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง กระบวนงานที่มีความเร่งด่วนและส่งผลกระทบอย่างสูงหากไม่ดำเนินการ และจำเป็นต้องดำเนินงานหรือปฏิบัติงานด้วยมือ(Manual Processing)	ทีมหน.คณะทำงานของศูนย์คอมพิวเตอร์กอ.รพ.รร.6	☐

วันที่ 2-7 การตอบสนองในระยะสั้น

การปฏิบัติการใดๆให้บุคลากรของทุกทีม คำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นและปฏิบัติตามแนวทาง แผนเผชิญเหตุ และขั้นตอนการปฏิบัติงานที่กำหนดอย่างเคร่งครัด

↓ การตอบสนองในระยะสั้น (2-7 วัน)		
ขั้นตอนและกิจกรรม	**ผู้รับผิดชอบ**	**ดำเนินการแล้วเสร็จ**
▪ ติดตามสถานการณ์กอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบ ประเมินความจำเป็นและระยะเวลาที่ต้องใช้ในการกอบกู้คืน	ทีมปฏิบัติการITภาวะฉุกเฉินและทีมสนับสนุนการดำเนินงาน IT ภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪ ตรวจสอบความพร้อมและข้อจำกัดในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง ได้แก่	ทีมประสานงานและสื่อสาร IT ภาวะฉุกเฉินและทีมสนับสนุนการดำเนินงาน ITภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
- สถานที่ปฏิบัติงานสำรอง		☐
- วัสดุอุปกรณ์ที่สำคัญ		☐
- เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ		☐
- บุคลากรหลัก		☐
- ผู้รับบริการและผู้มีส่วนได้ส่วนเสีย/คู่ค้า/ผู้ให้บริการที่สำคัญ		☐
▪ รายงานหัวหน้าคณะกรรมการบริหารความต่อเนื่องของหน่วยงานเกี่ยวกับความพร้อมข้อจำกัดและข้อเสนอแนะในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง	ทีมปฏิบัติการ ITภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪ ประสานงานและดำเนินการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง	ทีมประสานงานและสื่อสารภาวะฉุกเฉินกับทีมสนับสนุนการดำเนินงานIT ภาวะฉุกเฉิน ของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐

การตอบสนองระยะกลาง (1 สัปดาห์)

การปฏิบัติการใดๆให้บุคลากรของทุกทีม คำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่นและปฏิบัติตามแนวทาง แผนเผชิญเหตุ และขั้นตอนการปฏิบัติงานที่กำหนดอย่างเคร่งครัด

↓ การตอบสนองต่อเหตุการณ์และการกู้คืนกระบวนการปฏิบัติงานระยะเวลาเกิน 7 วัน		
ขั้นตอนและกิจกรรม	**ผู้รับผิดชอบ**	**ดำเนินการแล้วเสร็จ**
▪ ติดตามสถานภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบ และประเมินความจำเป็นและระยะเวลาที่ต้องใช้ในการกอบกู้คืน	ทีมปฏิบัติการIT ภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪ ระบุทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติ	ทีมประสานงานและสื่อสารภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐
▪รายงานหัวหน้าคณะบริหารความต่อเนื่องของหน่วยงาน สถานภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบ และทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติ	ทีมสนับสนุนการดำเนินงาน IT ภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐ ☐ ☐ ☐
▪แจ้งสรุปสถานการณ์และการเตรียมความพร้อมด้านทรัพยากรต่าง ๆ เพื่อดำเนินงานและให้บริการตามปกติให้กับบุคลากรในหน่วยงาน	ทีมหน.คณะบริหารงาน ภาวะฉุกเฉินของศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า	☐

10. สรุปขั้นตอนการตรวจสอบแผนการดำเนินงานกรณีระบบสารสนเทศล่ม(BCP :Executive Summary และRecovery Priority List)

1. บทสรุปผู้บริหาร (Executive Summary)

ศูนย์คอมพิวเตอร์ โรงพยาบาลพระมงกุฎเกล้า ได้จัดทำ “แผนดำเนินธุรกิจอย่างต่อเนื่อง (BCP)” เพื่อให้สามารถรับมือกับเหตุการณ์ฉุกเฉินและภาวะวิกฤตที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ โดยเฉพาะเหตุการณ์ที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

- แผนนี้มุ่งเน้นการรักษาความต่อเนื่องของภารกิจสำคัญ อาทิ ระบบ HIS, ระบบ PACS, ระบบเวชระเบียน, ระบบห้อง LAB และเครือข่ายคอมพิวเตอร์ในโรงพยาบาล รวมถึงการจัดเตรียมบุคลากร อุปกรณ์ และสถานที่สำรองให้สามารถทำงานได้แม้ในภาวะฉุกเฉิน

- มีการจัดตั้งทีมบริหารความต่อเนื่อง 5 ทีมหลัก ครอบคลุมทั้งการวิเคราะห์ วางแผน กู้คืนระบบและการสื่อสาร รวมถึงการกำหนดขั้นตอนการตอบสนองในช่วง 1–30 วัน พร้อมแนวทางการประสานงานกับหน่วยงานภายนอก

- แผน BCP ฉบับนี้ยังสามารถนำไปใช้เป็นแนวทางซ้อมจริง (drill) และปรับปรุงอย่างต่อเนื่องตามสถานการณ์ภัยคุกคามที่เปลี่ยนแปลงในอนาคต เพื่อให้มั่นใจว่าโรงพยาบาลสามารถให้บริการทางการแพทย์ได้อย่างต่อเนื่องและปลอดภัย

2. ลำดับความสำคัญของระบบที่ต้องฟื้นฟูก่อน (System Recovery Priority List)

เพื่อให้การกู้คืนระบบสามารถดำเนินการได้อย่างมีประสิทธิภาพ ทีม BCP ได้จัดลำดับความสำคัญของระบบสารสนเทศที่อยู่ภายใต้การดูแลของศูนย์คอมพิวเตอร์ ดังนี้:

ลำดับ	ระบบ / แอปพลิเคชัน	ความสำคัญ	ระยะเวลาเป้าหมายในการคืนสภาพ (RTO)
1	ระบบ HIS (PMK-HMS)	สูงมาก	ภายใน 1 วัน
2	ระบบ PACS/ภาพทางการแพทย์	สูงมาก	ภายใน 1 วัน
3	ระบบเวชระเบียน/ทะเบียนผู้ป่วย	สูง	ภายใน 3 วัน
4	ระบบห้องแล็บ (Lab)	สูง	ภายใน 3 วัน
5	ระบบยาและคลังเวชภัณฑ์	ปานกลาง	ภายใน 7 วัน
6	ระบบสารบรรณ/ระบบราชการ	ปานกลาง	ภายใน 15 วัน

แผนการทดสอบซ้อม BCP (BCP Testing Plan)

1. วัตถุประสงค์ของการทดสอบ

1.1 ทดสอบความพร้อมของบุคลากรในทีม BCP

1.2 ตรวจสอบความถูกต้องของ Call Tree และขั้นตอนการแจ้งเตือน

1.3 ประเมินความสามารถในการกู้คืนระบบสารสนเทศภายใต้เวลาที่กำหนด (RTO)

1.4 ตรวจสอบความพร้อมของสถานที่สำรอง (DR Site)

1.5 ปรับปรุงแผน BCP ตามผลการซ้อม

2. ประเภทการทดสอบและรายละเอียด

ลำดับ	ประเภทการทดสอบ	รายละเอียด	ความถี่	ผู้รับผิดชอบหลัก
1	Table-top Exercise	จำลองสถานการณ์ผ่านการประชุมแบบจำลอง	ทุก 6 เดือน	หัวหน้าทีมบริหาร BCP
2	Walkthrough Test	ทบทวนขั้นตอนตามแผน BCP โดยใช้ Checklists	ทุก 6 เดือน	หัวหน้าทีมแต่ละกลุ่ม
3	Communication Drill	ทดสอบ Call Tree, LINE, โทรศัพท์	ทุกไตรมาส	ทีมประสานงานและสื่อสาร
4	Restore & Recovery Drill	เรียกคืนระบบจาก Backup เช่น HIS	ปีละ 2 ครั้ง	ทีม Backup / Server
5	Cyber Attack Simulation	จำลอง Ransomware โจมตี	ปีละ 1 ครั้ง	ทีม Cybersecurity
6	DR Site Activation Drill	ซ้อมย้ายเจ้าหน้าที่ไป DR Site	ปีละ 1 ครั้ง	ทีมสนับสนุน

3. Checklist การซ้อม BCP สำหรับแต่ละทีม

ตัวอย่าง Checklist พื้นฐานที่ใช้ตรวจสอบในระหว่างการทดสอบ BCP

- ☐ ทีมรับแจ้งเหตุทันเวลา (Call Tree)
- ☐ ระบบสำรองสามารถนำกลับมาใช้งานได้
- ☐ ทีม Cybersecurity สามารถแยก network ได้ทัน
- ☐ DR Site พร้อมใช้งานและมีอุปกรณ์เพียงพอ
- ☐ แบบฟอร์มรายงานถูกจัดทำครบถ้วน

4. แบบฟอร์ม Post-Drill Report

ชื่อเหตุการณ์ซ้อม: _____

วันที่ดำเนินการ: _____

ผู้รับผิดชอบหลัก: _____

ระบบที่เกี่ยวข้อง: _____

ผลการดำเนินการ:

- จุดแข็ง: _____
- จุดอ่อน: _____
- เวลากู้คืน (RTO): _____ นาที

ข้อเสนอแนะเพื่อปรับปรุง: _____

5. ตารางทดสอบ BCP รายปี (Annual BCP Testing Calendar)

เดือน	ประเภทการทดสอบ	ผู้รับผิดชอบ	หมายเหตุ
มกราคม	Restore & Recovery Drill	ทีม Backup	
มีนาคม	Communication Drill	ทีมประสานงาน	
พฤษภาคม	Table-top Exercise	ทีมบริหาร	
กรกฎาคม	Cybersecurity Drill	ทีม Cybersecurity	
กันยายน	DR Site Activation Drill	ทีมสนับสนุน	
พฤศจิกายน	Walkthrough Test	ทุกทีม	

ผู้อนุมัติเอกสาร

พ.อ.

(กศม ภังคานนท์)

หัวหน้าศูนย์คอมพิวเตอร์รพ.รร.6

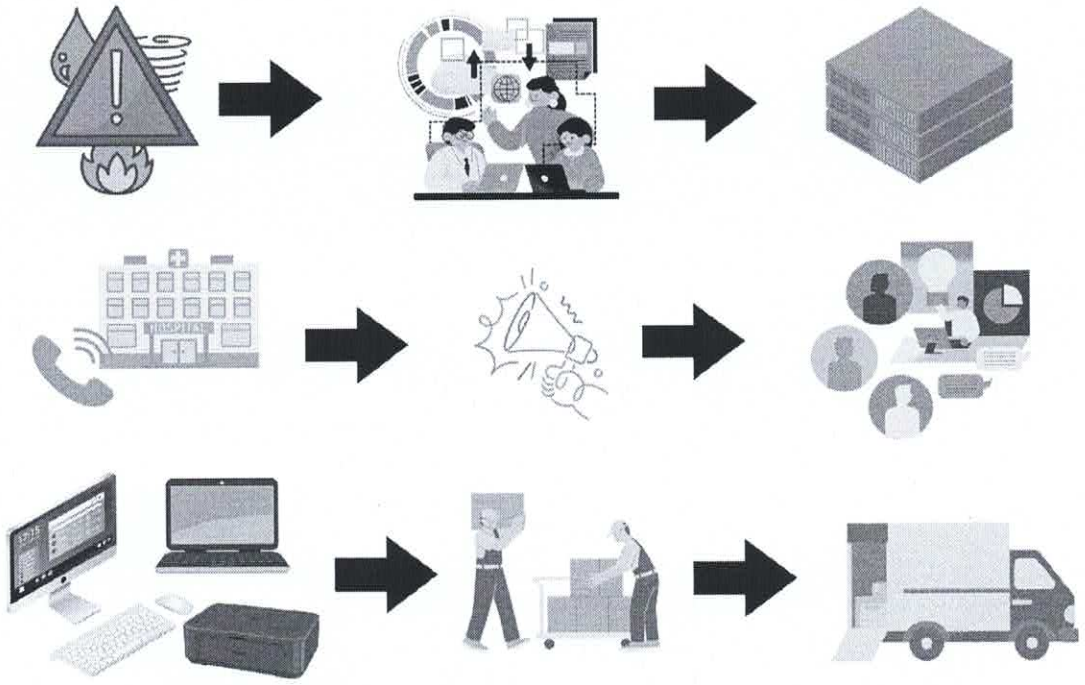
ผู้จัดทำเอกสาร

พ.อ.

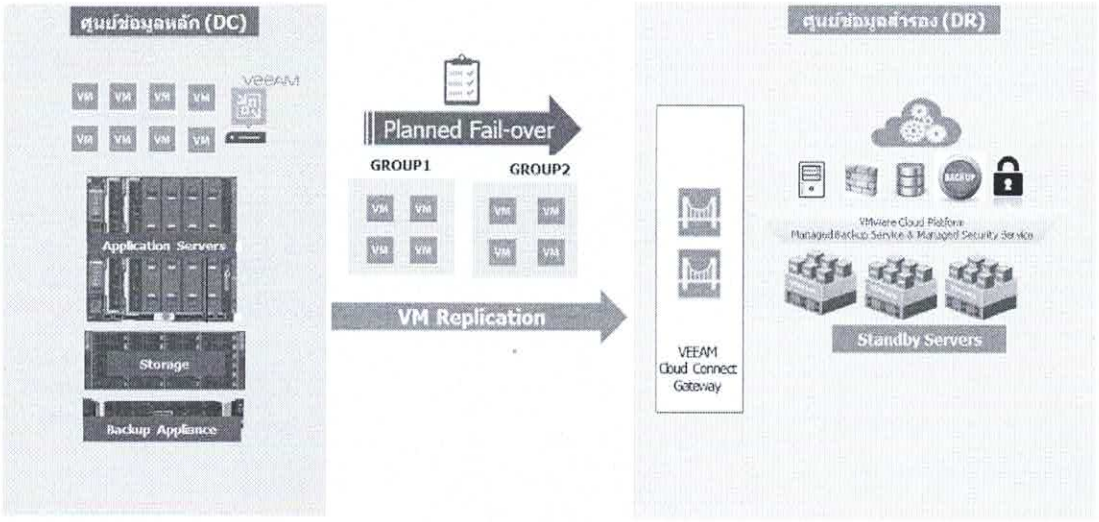
(ธนกร เทียนศรี)

รองหัวหน้าศูนย์คอมพิวเตอร์รพ.รร.6

แผนซ้อมซ้อมเผชิญเหตุในสถานการณ์ต่างๆ



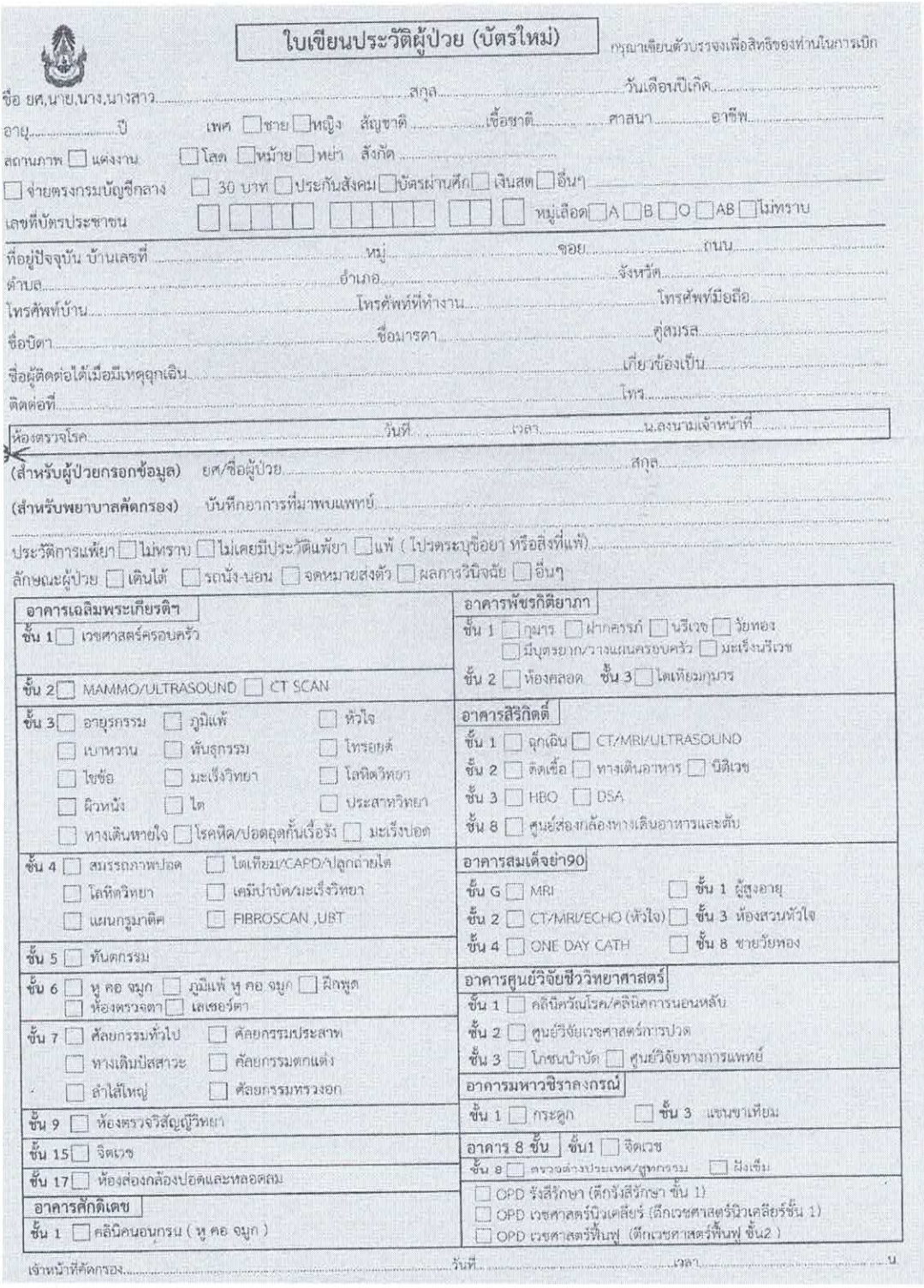
แผนภาพแสดงการทำแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน (Business Continuity Plan)



ภาคผนวก

ตัวอย่างแบบฟอร์มใช้งานตามแผนBCP

แบบฟอร์มลงทะเบียนผู้ป่วยใหม่ (ทำบัตรใหม่)



ใบเขียนประวัติผู้ป่วย (บัตรใหม่) กรุณาเขียนตัวบรรจงเพื่อสิทธิของท่านในการเบิก

ชื่อ ยศ,นาย,นาง,นางสาว.....สกุล.....วันเดือนปีเกิด.....

อายุ.....ปี เพศ ☐ชาย ☐หญิง สัญชาติ.....เชื้อชาติ.....ศาสนา.....อาชีพ.....

สถานภาพ ☐ แต่งงาน ☐โสด ☐หม้าย ☐หย่า สังกัด.....

☐ จ่ายตรงกรมบัญชีกลาง ☐ 30 บาท ☐ประกันสังคม ☐บัตรผ่านศึก ☐ เงินสด ☐อื่นๆ.....

เลขที่บัตรประชาชน ☐☐☐☐ ☐☐☐☐ ☐☐ ☐ หมู่เลือด ☐A ☐B ☐O ☐AB ☐ไม่ทราบ

ที่อยู่ปัจจุบัน บ้านเลขที่.....หมู่.....ซอย.....ถนน.....

ตำบล.....อำเภอ.....จังหวัด.....

โทรศัพท์บ้าน.....โทรศัพท์ที่ทำงาน.....โทรศัพท์มือถือ.....

ชื่อบิดา.....ชื่อมารดา.....คู่สมรส.....

ชื่อผู้ติดต่อได้เมื่อมีเหตุฉุกเฉิน.....เกี่ยวข้องเป็น.....

ติดต่อที่.....โทร.....

ห้องตรวจโรค.....วันที่.....เวลา.....น.ลงนามเจ้าหน้าที่.....

(สำหรับผู้ป่วยกรอกข้อมูล) ยศ/ชื่อผู้ป่วย.....สกุล.....

(สำหรับพยาบาลคัดกรอง) บันทึกอาการที่มาพบแพทย์.....

ประวัติการแพ้ยา ☐ไม่ทราบ ☐ไม่เคยมีประวัติแพ้ยา ☐แพ้ (โปรดระบุชื่อยา หรือสิ่งที่แพ้).....

ลักษณะผู้ป่วย ☐ เดินได้ ☐ รถนั่ง-นอน ☐ จดหมายส่งตัว ☐ ผลการวินิจฉัย ☐ อื่นๆ

อาคารเฉลิมพระเกียรติฯ

ชั้น 1 ☐ เวชศาสตร์ครอบครัว

ชั้น 2 ☐ MAMMO/ULTRASOUND ☐ CT SCAN

ชั้น 3 ☐ อายุรกรรม ☐ ภูมิแพ้ ☐ หัวใจ
☐ เบาหวาน ☐ ทันตกรรม ☐ โภชนบำบัด
☐ ไขข้อ ☐ มะเร็งวิทยา ☐ โลหิตวิทยา
☐ ผิวหนัง ☐ ไต ☐ ประสาทวิทยา
☐ ทางเดินหายใจ ☐ โรคหืด/ปอดอุดกั้นเรื้อรัง ☐ มะเร็งปอด

ชั้น 4 ☐ สมรรถภาพปอด ☐ ไตเทียม/CAPD/ปลูกถ่ายไต
☐ โลหิตวิทยา ☐ เคมีบำบัด/มะเร็งวิทยา
☐ แผนกรูมาติค ☐ FIBROSCAN ,UBT

ชั้น 5 ☐ ทันตกรรม

ชั้น 6 ☐ หู คอ จมูก ☐ ภูมิแพ้ หู คอ จมูก ☐ ฝึกพูด
☐ ห้องตรวจตา ☐ เลเซอร์ตา

ชั้น 7 ☐ ศัลยกรรมทั่วไป ☐ ศัลยกรรมประสาท
☐ ทางเดินปัสสาวะ ☐ ศัลยกรรมตกแต่ง
☐ ลำไส้ใหญ่ ☐ ศัลยกรรมทรวงอก

ชั้น 9 ☐ ห้องตรวจวิสัญญีวิทยา

ชั้น 15 ☐ จิตเวช

ชั้น 17 ☐ ห้องส่องกล้องปอดและหลอดลม

อาคารศักดิเดช

ชั้น 1 ☐ คลินิคนอนกรน (หู คอ จมูก)

อาคารพัชรกิติยาภา

ชั้น 1 ☐ กุมาร ☐ ฝากครรภ์ ☐ นรีเวช ☐ วัยทอง
☐ มีบุตรยาก/วางแผนครอบครัว ☐ มะเร็งนรีเวช

ชั้น 2 ☐ ห้องคลอด ชั้น 3 ☐ ไตเทียมกุมาร

อาคารสิริกิตติ์

ชั้น 1 ☐ ฉุกเฉิน ☐ CT/MRI/ULTRASOUND

ชั้น 2 ☐ ติดเชื้อ ☐ ทางเดินอาหาร ☐ นิติเวช

ชั้น 3 ☐ HBO ☐ DSA

ชั้น 8 ☐ ศูนย์ส่องกล้องทางเดินอาหารและตับ

อาคารสมเด็จย่า90

ชั้น G ☐ MRI ☐ ชั้น 1 ผู้สูงอายุ

ชั้น 2 ☐ CT/MRI/ECHO (หัวใจ) ☐ ชั้น 3 ห้องสวนหัวใจ

ชั้น 4 ☐ ONE DAY CATH ☐ ชั้น 8 ชายวัยทอง

อาคารศูนย์วิจัยชีววิทยาศาสตร์

ชั้น 1 ☐ คลินิควัณโรค/คลินิคการนอนหลับ

ชั้น 2 ☐ ศูนย์วิจัยเวชศาสตร์การปวด

ชั้น 3 ☐ โภชนบำบัด ☐ ศูนย์วิจัยทางการแพทย์

อาคารมหาวชิราลงกรณ์

ชั้น 1 ☐ กระดูก ☐ ชั้น 3 แขนขาเทียม

อาคาร 8 ชั้น ชั้น1 ☐ จิตเวช

ชั้น 8 ☐ ตรวจต่างประเทศ/ยุทธกรรม ☐ ฝังเข็ม

☐ OPD รังสีรักษา (ตึกรังสีรักษา ชั้น 1)
☐ OPD เวชศาสตร์นิวเคลียร์ (ตึกเวชศาสตร์นิวเคลียร์ชั้น 1)
☐ OPD เวชศาสตร์ฟื้นฟู (ตึกเวชศาสตร์ฟื้นฟู ชั้น2)

เจ้าหน้าที่คัดกรอง.....วันที่.....เวลา.....น.

แบบฟอร์มลงทะเบียนผู้ป่วยเก่า (ไม่มีนัด)

สำหรับผู้ป่วยเก่าที่ไม่มีบัตรนัด

ผู้ป่วย ☐ 30 บาท, ปกส. ออกสิทธิที่ช่อง 9,10,11

ผู้ป่วย ☐ จ่ายตรง/กทม./อปท./กสทช./เงินสด ออกสิทธิที่ช่อง 4,5,6,7,8

ยศ/ชื่อผู้ป่วย.....สกุล.....เลขที่ทั่วไป.....

บันทึกอาการที่มาพบแพทย์.....

.....

ประวัติการแพ้ยา ☐ ไม่ทราบ ☐ ไม่เคยมีประวัติแพ้ยา ☐ แพ้ (โปรดระบุชื่อยา หรือสิ่งที่แพ้).....

ลักษณะผู้ป่วย ☐ เดินได้ ☐ รถนั่ง-นอน ☐ จดหมายส่งตัว ☐ ผลการวินิจฉัย ☐ อื่นๆ .....

อาคารเฉลิมพระเกียรติฯ

ชั้น 1 ☐ เวชศาสตร์ครอบครัว

ชั้น 2 ☐ MAMMO/ULTRASOUND ☐ CT SCAN

ชั้น 3 ☐ อายุรกรรม ☐ ภูมิแพ้ ☐ หัวใจ
☐ เบาหวาน ☐ พันธุกรรม ☐ ไทรอยด์
☐ ไขข้อ ☐ มะเร็งวิทยา ☐ โลหิตวิทยา
☐ ผิวหนัง ☐ ไต ☐ ประสาทวิทยา
☐ ทางเดินหายใจ ☐ โรคหืด/ปอดอุดกั้นเรื้อรัง ☐ มะเร็งปอด

ชั้น 4 ☐ สมรรถภาพปอด ☐ ไตเทียม/CAPD/ปลูกถ่ายไต
☐ โลหิตวิทยา ☐ เคมีบำบัด/มะเร็งวิทยา
☐ แผนกรูมาติค ☐ FIBROSCAN ,UBT

ชั้น 5 ☐ ทันตกรรม

ชั้น 6 ☐ หู คอ จมูก ☐ ภูมิแพ้ หู คอ จมูก ☐ ฝึกพูด
☐ ห้องตรวจตา ☐ เลเซอร์ตา

ชั้น 7 ☐ ศัลยกรรมทั่วไป ☐ ศัลยกรรมประสาท
☐ ทางเดินปัสสาวะ ☐ ศัลยกรรมตกแต่ง
☐ ลำไส้ใหญ่ ☐ ศัลยกรรมทรวงอก

ชั้น 9 ☐ ห้องตรวจวิสัญญีวิทยา

ชั้น 15 ☐ จิตเวช

ชั้น 17 ☐ ห้องส่องกล้องปอดและหลอดลม

อาคารศักดิเดช

ชั้น 1 ☐ คลินิคนอนกรน (หู คอ จมูก)

อาคารพัชรกิติยาภา

ชั้น 1 ☐ กุมาร ☐ ฝากครรภ์ ☐ นรีเวช ☐ วัยทอง
☐ มีบุตรยาก/วางแผนครอบครัว ☐ มะเร็งนรีเวช

ชั้น 2 ☐ ห้องคลอด ชั้น 3 ☐ ไตเทียมกุมาร

อาคารสิริกิตติ์

ชั้น 1 ☐ ฉุกเฉิน ☐ CT/MRI/ULTRASOUND

ชั้น 2 ☐ ติดเชื้อ ☐ ทางเดินอาหาร ☐ นิติเวช

ชั้น 3 ☐ HBO ☐ DSA

ชั้น 8 ☐ ศูนย์ส่องกล้องทางเดินอาหารและตับ

อาคารสมเด็จย่า90

ชั้น G ☐ MRI ☐ ชั้น 1 ผู้สูงอายุ

ชั้น 2 ☐ CT/MRI/ECHO (หัวใจ) ☐ ชั้น 3 ห้องสวนหัวใจ

ชั้น 4 ☐ ONE DAY CATH ☐ ชั้น 8 ขายวัยทอง

อาคารศูนย์วิจัยชีววิทยาศาสตร์

ชั้น 1 ☐ คลินิควัณโรค/คลินิคการนอนหลับ

ชั้น 2 ☐ ศูนย์วิจัยเวชศาสตร์การปวด

ชั้น 3 ☐ โภชนบำบัด ☐ ศูนย์วิจัยทางการแพทย์

อาคารมหาจิราลงกรณ์

ชั้น 1 ☐ กระดูก ☐ ชั้น 3 แขนขาเทียม

อาคาร 8 ชั้น ชั้น1 ☐ จิตเวช

ชั้น 8 ☐ ตรวจต่างประเทศ/สูทกรรม ☐ ฝังเข็ม

☐ OPD รังสีรักษา (ตึกรังสีรักษา ชั้น 1)
☐ OPD เวชศาสตร์นิวเคลียร์ (ตึกเวชศาสตร์นิวเคลียร์ชั้น 1)
☐ OPD เวชศาสตร์ฟื้นฟู (ตึกเวชศาสตร์ฟื้นฟู ชั้น2)

คลินิคนอกเวลา

อาคารเฉลิมพระเกียรติ

ชั้น 1 ☐ อายุกรรมและจิตเวช

ชั้น 3 ☐ หัวใจ
☐ ผิวหนัง

ชั้น 6 ☐ หู คอ จมูก
☐ ตา

อาคารเฉลิมพระเกียรติ

ชั้น 7 ☐ ศัลยกรรมทรวงอก
☐ ศัลยกรรมลำไส้ใหญ่
☐ ศัลยกรรมทั่วไป
☐ ทางเดินปัสสาวะ

อาคาร 8 ชั้น

ชั้น 8 ☐ ฝังเข็ม

อาคารพัชรกิติยาภา

ชั้น 1 ☐ กุมาร
☐ นรีเวช
☐ ฝังเข็ม (วันเสาร์)

อาคารมหาจิราลงกรณ์

ชั้น 1 ☐ กระดูก

เจ้าหน้าที่คัดกรอง.....วันที่.....เวลา.....น.

โรงพยาบาลพระมงกุฎเกล้า

ใบแจ้งค่ารักษาพยาบาล วันที่.....

HN..... ที่ทำการ.....

ขอแจ้งค่ารักษาพยาบาลของ.....ตามรายการต่อไปนี้

ค่าตรวจทางห้องปฏิบัติการ	
ค่าเอ็กซเรย์	
ค่าตรวจ	
ค่าผ่าตัด	
ค่ารักษา	
ค่ายา	
ค่าเวชภัณฑ์	
ค่าอุปกรณ์	
ค่าห้อง	
ค่าอาหาร	
รวมทั้งสิ้น	

ลงชื่อ.....ผู้แจ้ง

ตำแหน่ง.....

กองรังสีกรรม โรงพยาบาลพระมงกุฎเกล้า

ใบปรึกษา – รายงานทางรังสี

ชื่อ.....อายุ.....ปี
H.N. ..... A.N. .....
เพศ ☐ M. ☐ F. โทร. ของผู้ป่วย.....
☐ OPD ..... ☐ Ward .....

Requested by ..... Code.....
Department of ..... Tel. .....
Date...../ Time .....
Previous X-Ray ☐ Yes ☐ No
ผลเลือด Cr.....

ป้องกันอุบัติเหตุจากการตั้งครรภ์
ในสตรี อายุ 10-55 ปี
☐ ตั้งครรภ์
☐ ไม่ตั้งครรภ์
☐ ไม่แน่ใจ
ประจำเดือนครั้งสุดท้ายเมื่อ.....
.....ลายเซ็นผู้ป่วย
.....ลายเซ็นเจ้าหน้าที่

Clinical history .....
.....
Physical examination/Lab .....
.....
.....

☐ X-ray .....
(อาคารเฉลิมพระเกียรติฯ ชั้น 2 โทร. 93042, ตึกอุบัติเหตุ ชั้น 2 โทร. 93409)

☐ Barium Enema (BE) (โทร. 93815)
☐ Intravenous Pyelography (IVP) (โทร. 93820)
☐ DSI : (โทร. 93815)
☐ Barium swallow ☐ Upper GI ☐ GI Follow through ☐ Hysterosalphyngogram
☐ Myelogram ☐ Venogram ☐ Others .....
☐ DSA : (โทร. 93045)
☐ Angiogram.....
☐ Intervention.....
☐ Ultrasound : (โทร. 93817)
☐ Upper abdomen ☐ Lower abdomen ☐ Whole abdomen ☐ KUB system
☐ Thyroid ☐ Others .....
☐ Computed Tomography (CT) (โทร. 93414, 99366)
☐ Brain ☐ Chest ☐ Upper abdomen ☐ Lower abdomen
☐ Whole abdomen ☐ Others .....
☐ Magnetic Resonance Imaging (MRI) (โทร. 93708, 93813)
☐ Brain ☐ Nasopharynx ☐ Chest ☐ Upper abdomen
☐ Extermity ..... ☐ Spine ..... ☐ Others .....
☐ Magnetic Resonance Angiography (MRA) (โทร. 93708, 93813) .....
☐ Mammogram (โทร. 93811, 93933) .....
☐ Nuclear Medicine (โทร. 93197)
☐ Scan ..... ☐ Thyroid uptake ☐ T3 ☐ T4
☐ FT3 ☐ FT4 ☐ TSH ☐ Others .....

กรุณาเติม ICD 10.....

ทบ.๔๖๖ - ๖๑๑
(พ.๑๒)

ใบปรึกษาเกี่ยวกับการป่วยเจ็บ

หน่วยรักษาพยาบาล

วันที่.....เดือน.....พ.ศ.....

หน่วยวิทยาการ.....ขอให้หน่วยวิทยาการ.....ตรวจผู้ป่วยเจ็บ

คนป่วยเจ็บอยู่ที่อาคาร.....ห้อง.....เตียง.....

ชื่อ.....อายุ.....ปี เครื่องหมายสังกัด.....

เลขที่.....เลขที่ประจำแผนก.....ครั้งที่.....

อวัยวะที่ต้องการตรวจและรักษา.....

อาการเจ็บไข้ที่สำคัญ.....

รายงานการเจ็บป่วย

.....

ผู้ขอการวินิจฉัย และความเห็น

/ /

.....

แพทย์ผู้รักษา

/ /

รายงานการวินิจฉัย, และความเห็น

ชื่อ.....แพทย์ผู้รักษา

วันที่.....พ.ศ. ๒๕.....

Patient Registration Form

PHRAMONGKUTKLAO HOSPITAL

☐ New Card ☐ Loss Card ☐ Forget Card

Name.....Surname.....Date of Birth ☐☐-☐☐-☐☐☐☐

Age .....Year Sex ☐ Male ☐ Female Nationality ..... Religion .....Occupation.....

Status ☐ Married ☐ Single ☐ Widow ☐ Devote Under.....

ID Card / Passport NO. ☐-☐☐☐☐-☐☐☐☐☐-☐☐-☐

Address ..... Village..... Road .....

Sub/Rd..... District/Zone..... City.....Postal Code.....

Home Phone..... Office Phone..... Mobile Phone .....

Father name.....Mother name..... Spout's name .....

Contact Person In Case of Emergency .....

Address ..... Phone .....

OPD.....Date.....Time..... Signature.....

(For Office) Name .....Surname .....

Symptoms.....

Allergic History ☐ Don't Know ☐ No. ☐ Allergic Drug.....

Characteristics Of Patients ☐ Walking ☐ Car Ride-Lic ☐ Mail Sent ☐ The Diagnosis

☐ Other.....

Chaleumphrakiat Building

First Floor	☐ Family Medicine Clinic		
Second Floor	☐ Mammo gram	☐ CT.SCAN	☐ DSA
Third Floor	☐ Medical Clinic	☐ OPD.Skin	☐ OPD.Rheumatics
	☐ OPD.Cardiology	☐ OPD.Chest	☐ OPD.Diabetic
	☐ Asthma/Bronchiectasis	☐ Tumor Clinic	☐ Hemato Clinic
	☐ Thyriod/Rheumato	☐ OPD. Infection.	☐ Kidney
	☐ OPD.Gaotrointestinal	☐ OPD.Neuromedical	☐ Allergy
	☐ Genetic.	☐ Lung cancer.	
Four th Floor	☐ Pulmonary Function Clinic	☐ COPD	☐ GI Scope
	☐ Hemato Room 14	☐ Infection Room	
	☐ Chemotherapy	☐ Rheumatics Room	
Sixth Floor	☐ Eye Clinic	☐ Eye Laser	☐ Hearing Clinic
	☐ Allergy ENT Clinic	☐ OPD.Ear Nose Throat	
Seven Floor	☐ OPD.Sur gery/Breast	☐ OPD.Neurosurgery	
	☐ OPD.CVT	☐ OPD.Plastic Surgery	
	☐ OPD.URO	☐ OPD.Colon Surgery	
Ninth Floor	☐ Pain Clinic		

Mahavachiralongkorm Building

First Floor ☐ OPD.Orthopedic
Thrid Floor ☐ Artificial limb.

Patcharakitiyapa Building

First Floor ☐ OPD.Pediatrics. ☐ OPD.ANC.
☐ Infertility. ☐ Gyne cancer
☐ Bilderly. ☐ OPD.Gynaecology
Third Floor ☐ Pediatrics Hemodialysis

Somdetya 90 Building

Ground Floor ☐ MRI X - Rays Computer
First Floor ☐ Elderly.
Third Floor ☐ Cardio Cath ☐ Cardio Function
Eigth Floor ☐ Elderly Men. ☐ Aviation Medicine.

Medicine - Surgery Building

First Floor ☐ TB Clinic (Medical-Surgical Building)
Second Floor ☐ Forensic.
Third Floor ☐ Clinical Research.

Prapasri Building

Ground Floor ☐ Forensic ☐ C.T.Scan
First Floor ☐ Emergency room.

Chaleumphrabaramee Building

First Floor ☐ Check up For Foreign Country Second Floor
☐ Acupuncture.

Eight Building

First Floor ☐ OPD.Psychiatry

Others.

☐ OPD.Radiation.(Radiation Building First Floor)
☐ OPD.Nuclear Medicine.(Nuclear Medicine Building Third Floor)
☐ OPD.Rehabilitation Clinic (Rehabilitation Clinic Building Second Floor)

Officer .....
Date .....
Time .....

โรงพยาบาลพระมงกุฎเกล้า
แผนกโลหิตวิทยา
อาคารเฉลิมพระเกียรติฯ ชั้น 2
โทร.93802

ชื่อ..... อายุ.....ปี เพศ ☐ ช ☐ ญ
HN..... AN..... ตึกผู้ป่วย..... OPD.....
VN..... วันที่..... เวลา.....
การวินิจฉัยโรค..... แพทย์ผู้สั่ง

☐ HE 001 CBC (platelet count) ..... 00 บ.
☐ HE 003Hct .....% 30 บ.
☐ HE 005 RED CELL INDEX 90 บ.
☐ RBC Morphology

☐ HE 009 ESR 50 บ.
☐ HE 010 Retic Count 40 บ.
☐ HE 011 Inclusion Body 40 บ.
☐ HE 012 Heinz body 40 บ.
☐ HE 013 G-6-PD Qualitative 230 บ.
☐ HE 023 ย้อม 50 บ.
Wright Stain/2 Slide
☐ PM 002 Hb Typing 270 บ.

HE 001-013 ใช้เลือด EDTA blood 2 ml(หลอดจุกม่วง mix)

☐ HE 016 Bleeding Time 60 บ.
☐ HE 017 Clotting Time 50 บ.

HE 016-017 นำผู้ป่วยมาทำการทดสอบที่ห้องเจาะเลือด

☐ HE 041 Malaria Thin Film 50 บ.
☐ HE 040 Malaria Thick Film 50 บ.
☐ HE 020 APTT (ratio) 85 บ.
☐ HE 021 PT (INR) 75 บ.
☐ HE 022 TT (ratio) 80 บ.

HE 020-022 แช่น้ำแข็งขณะนำส่ง
(citrate blood 2.7ml จุกสีฟ้า mix)

☐ HE 038 ขอ Slide

ติดต่อแลปนอก โทร. 85095

☐ OL 509 Cystatin-c 500 บ.
☐ OL 510 ADA in fluid 900 บ.

OL 509 ส่ง Clotted blood 5 ml
Pre-albumin รับผล 7 วันทำการ
Cystatin-C รับผล 3 วันทำการ
ADA in fluid รับผล 5 วันทำการ

OTHERS.....
.....
.....
.....
.....

สาเหตุการปฏิเสธสิ่งส่งตรวจ
- ชื่อไม่ตรงกัน
- ปริมาณไม่ครบตามขีดกำหนด
- Clot หรือ Hemolysis

...ส่งผลการตรวจผ่านระบบคอมพิวเตอร์...

ผู้ตรวจ..... วันที่.....

รพ.รร.6 N-9

ใบขอตรวจทางห้องปฏิบัติการ
โรงพยาบาลพระมงกุฎเกล้า
แผนกชีวเคมี อาคารเฉลิมพระเกียรติฯ
ชั้น 2 โทร 93603
ห้องปฏิบัติการกลาง อาคาร สก.
ชั้น 3 โทร 95352

วันที่..... ตึกผู้ป่วย..... โทร.....
ชื่อ.....อายุ..... ปี เพศ ( ) หญิง ( ) ชาย
HN.....AN.....VN.....
เวลาเจาะเลือด.....การวินิจฉัยโรค.....แพทย์ผู้ส่งตรวจ.....

	ราคา
☐ 001 FBS(1)(9)(เจาะเลือดเวลา .....)	40 บ.
เมื่อเจาะเลือดหนึ่งหลอด	
และส่งรวมกับ test อื่น	
☐ 046 FPG(1)(10)NaF tube	40 บ.
☐ 002 BUN (9)	40 บ.
☐ 003 Creatinine(9)	40 บ.
☐ 004 Uric acid (9)	60 บ.
☐ 005 Lipid profile(2)(9)	200 บ.
☐ 006 Cholesterol	60 บ.
☐ 007 Triglycerides	60 บ.
☐ 008 HDL-c	100 บ.
☐ 205 Direct LDL-c	150 บ.
☐ 010 Liver Function Test (9)	290 บ.
☐ 011 Total protein	60 บ.
☐ 012 Albumin	30 บ.
☐ 013 Total bilirubin	40 บ.
☐ 014 Direct bilirubin	40 บ.
☐ 015 AST	40 บ.
☐ 016 ALT	40 บ.
☐ 017 ALP	40 บ.
☐ 019 LDH (9)	60 บ.
☐ 020 CPK (9)	75 บ.
☐ 053 hs-CRP (9)	250 บ.
☐ 073 CRP (9)	130 บ.
☐ 057 Troponin T (9)	260 บ.
((เจาะเลือดเวลา.....)	
☐ 058 CK-MB mass (9)	300 บ.
☐ 224 Lactate (NaF tube) (10)	50 บ.
แช่น้ำแข็งส่งทันที	

	ราคา
☐ 022 Electrolytes (9)	100 บ.
☐ 023 Sodium (Na+)	40 บ.
☐ 024 Potassium (K+)	40 บ.
☐ 025 Chloride (CL-)	40 บ.
☐ 026 Bicarbonate (CO2)	40 บ.
☐ 027 Calcium(9)	50 บ.
☐ 028 Ionized calcium(3)(9)	400 บ.
☐ 029 Phosphate,Inorganic(9)	50 บ.
☐ 030 Magnesium (9)	50 บ.
☐ 033 P-Amylase (9)	100 บ.
☐ 034 Lipase (9)	200 บ.
☐ 035 Gamma GT (9)	130 บ.
☐ 037 HbA1c(4)	150 บ.
☐ 043 Osmolarity(5)	130 บ.
☐ 044 Iron (9)	80 บ.
☐ 045 TIBC(8)(9)	80 บ.
☐ 051 Ketone (9)	150 บ.
☐ 039 Blood gases(3)	195 บ.
Patient temp.....°C	
Hb.....g/dL	
FiO.....%	
☐ 040 GTT 100 gm.(1)(10)	300 บ.
☐ 071 Glucose 2 hr PP (1)(10)	170 บ.
☐ 072 Glucose 2hr PP 75 gm (1)(10)	170 บ.
☐ 047 50 gm. GCT (10)	40 บ.
☐ 229 Vitamin D(5)	900 บ.
☐ 230 Vitamin B12 (5)	240 บ.
☐ 231 Pre Albumin (5)	300 บ.

	ราคา
CSF(7)	
☐ 201 Protein CSF	60 บ.
☐ 202 Glucose CSF	40 บ.
☐ 042 LDH CSF	100 บ.
☐ 225 Lactate CSF	150 บ.
Body fluid(7) ระบุ.....	
☐ 220 Protein	40 บ.
☐ 114 Albumin	50 บ.
☐ 206 Glucose	40 บ.
☐ 207 Urea N	40 บ.
☐ 208 Creatinine	40 บ.
☐ 209 Uric acid	60 บ.
☐ 210 Calcium	50 บ.
☐ 211 Phosphorus	50 บ.
☐ 212 Magnesium	50 บ.
☐ 213 P-amylase	80 บ.
☐ 214 LDH	100 บ.
☐ 216 Sodium (Na+)	40 บ.
☐ 217 Potassium (K+)	40 บ.
☐ 218 Chloride (CL-)	40 บ.
☐ 219 Osmolarity	120 บ.

(1) งดอาหาร 8 ชั่วโมง
(2) งดอาหารอย่างน้อย 12 ชั่วโมง
(3) Bloodgas syringe แช่น้ำแข็งส่งทันที
(4) EDTA tube (จุกม่วง)
(5) Clotted blood tube (จุกแดง)
(7) Steriled bottle
(8) TIBC = Iron + UIBC
ต้องเลือก Iron ด้วยเมื่อตรวจ TIBC
(9) : Heparinized tube (จุกเขียว)
(10) : NaF tube (จุกเทา)
-FBS, Electrolytes หลังเจาะเลือด เกิน 2 ชม. สั่งตรวจเพิ่มไม่ได้

Others

รงพยาบาลพระมงกุฎเกล้า

ใบเงินค่าอาหาร; ค่าห้องและค่ารักษาพยาบาลผู้ป่วย เลขที่ภายใน.....

ยศ, ชื่อ.....อายุ.....ปี สังกัด.....	ตึก.....ห้อง..... โรค.....
รับเมื่อ.....เวลา.....	จำหน่าย.....เวลา.....
อัตราต่อวัน ☐ ค่าอาหารสามัญ ๑๖๐ บาท ☐ ค่าอาหารพิเศษ ๔๐๐ บาท ☐ ค่าอาหารพิเศษวีไอพี ๕๖๐ บาท วิธีชำระเงิน ☐ ชำระโดยตรงทั้งหมด ☐ เฉพาะส่วนเกิน	☐ ค่าห้องสามัญ ๒๔๐ บาท ☐ ค่าห้องพิเศษ.....บาท ☐ ต้นสังกัด(ในส่วนองค์การหรือบริษัทที่เคยตกลงกันไว้)
บันทึกกรณีพิเศษ (ถ้ามี)	

รายการตรวจสอบ	รวมวัน	จำนวนเงิน	ผู้แจ้งรายได้	วัน เดือน ปี	ผู้รับเงิน	หมายเหตุ
๑. ค่าห้อง						
๒. ค่าอาหาร						
๓. ค่ายาและเวชภัณฑ์						
๔. ค่า Lab						
๕. ค่าอุปกรณ์บำบัดโรค						
๖. ค่าอวัยวะเทียม						
รวมเงิน		ยกไป				
ค่าตรวจรักษาพยาบาลและค่าบริการทางการแพทย์บันทึกด้านหลัง						

ปรับปรุงโดย ผวส.รพ.รร.๖ เมื่อ ม.ค. ๖๒

กรุณาลงจำนวนเงินทุกครั้งที่ตรวจรักษาพยาบาล และค่าบริการทางการแพทย์

รายการตรวจสอบ	รวมวัน	จำนวนเงิน	ผู้แจ้งรายได้	วัน เดือน ปี	ผู้รับเงิน	หมายเหตุ
รายการที่ ๑ ถึง ๖ ยอดยกมา						
๗. ค่าตรวจรักษาพยาบาลและ						
ค่าบริการทางการแพทย์						
ค่าเอ็กซเรย์						
ตรวจคลื่นไฟฟ้าหัวใจ						
ตรวจคลื่นสมอง						
ผ่าตัด						
ล้างไต						
เจาะหาจำนวนแก๊สในเลือด						
คลอด						
เวชศาสตร์ฟื้นฟู						
ตรวจทางพยาธิ						
ฉีดยา						
ล้างแผล						
เข้าเฝือก						
และอื่นๆ						
.....						
.....						
.....						
.....						
รวมทั้งสิ้น						

ตรวจสอบแล้วเป็นการถูกต้อง

(ลงชื่อ).....

(ตำแหน่ง).....

เจ้าหน้าที่ตึกรักษาพยาบาล

เจ้าหน้าที่ตรวจสอบ

(ลงชื่อ).....

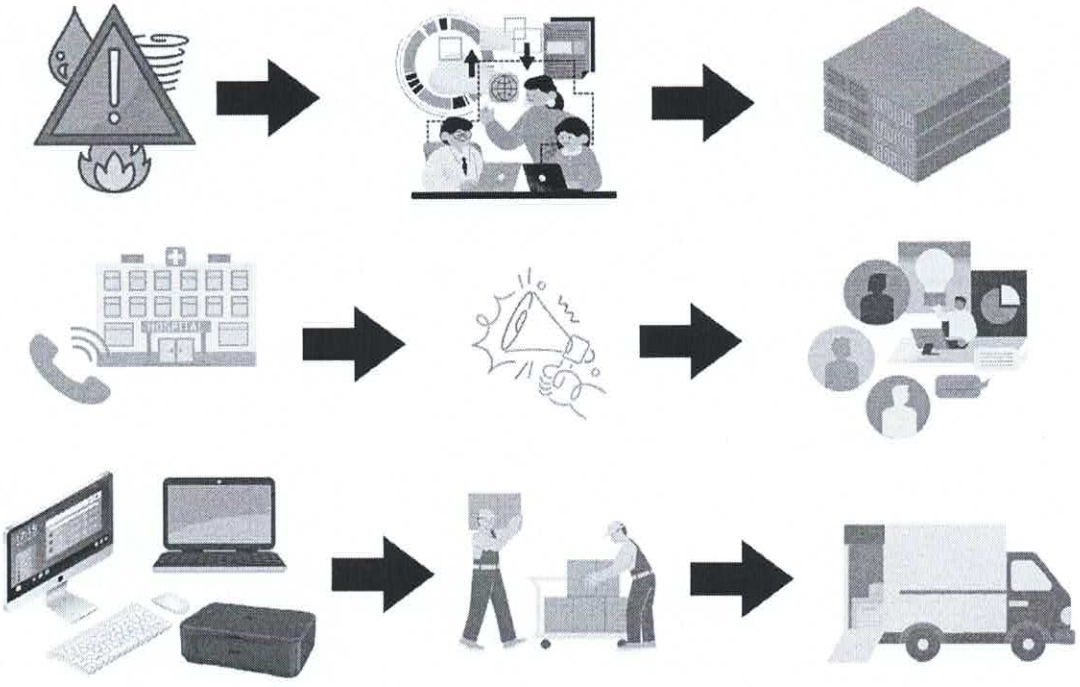
(ตำแหน่ง).....

...../...../.....

หมายเหตุ ให้เจ้าหน้าที่ที่เกี่ยวข้องบันทึกรายการและจำนวนเงินที่ต้องชำระทุกครั้ง พร้อมกับลงชื่อผู้แจ้งรายได้ไว้ด้วย สำหรับพนักงานเก็บเงินออก กง.๑ แล้ว ลงชื่อผู้รับเงินไว้เป็นหลักฐาน

ปรับปรุงโดย ผวส.รพ.รร.๖ เมื่อ ม.ค. ๖๒

แผนซ้อมซ้อมเผชิญเหตุในสถานการณ์ต่างๆ



แผนภาพแสดงการทำแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน (Business Continuity Plan)