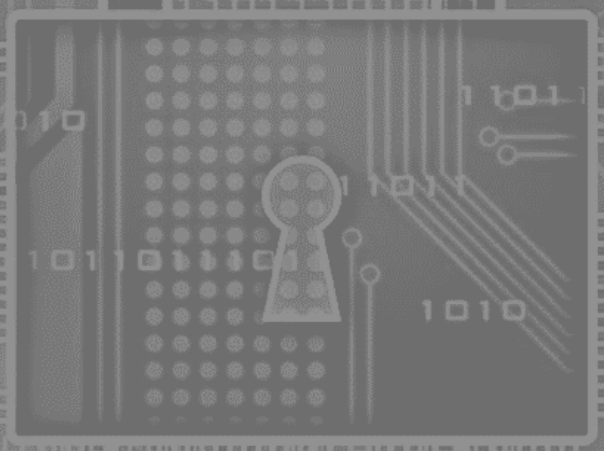
โรงพยาบาลแก่งหางแมว
KEANGHANGMEOW HOSPITAL

แผนบริหารความเสี่ยงในสภาวะวิกฤตด้านสารสนเทศ



โรงพยาบาลแก่งหางแมว

ระยะเวลา 5 ปี (พ.ศ. 2565- พ.ศ. 2569)

แผนบริหารความเสี่ยงในสภาวะวิกฤตด้านสารสนเทศ

โรงพยาบาลแก่งหางแมว พศ. 2566

1. บทนำ

การจัดการความเสี่ยงเป็นองค์ประกอบที่สำคัญของการจัดการวิกฤตด้านเทคโนโลยีสารสนเทศ (IT) โดยเฉพาะอย่างยิ่งในภาคส่วนการดูแลสุขภาพที่ความปลอดภัยของข้อมูลผู้ป่วยมีความสำคัญสูงสุด เน้นให้เห็นถึงความจำเป็นของแนวทางเชิงรุกในการบริหารความเสี่ยงเพื่อป้องกันไม่ให้เหตุการณ์ดังกล่าวเกิดขึ้นอีกในอนาคต การบริหารความเสี่ยงที่มีประสิทธิภาพเกี่ยวข้องกับการระบุภัยคุกคามและความเปราะบางที่อาจเกิดขึ้น การประเมินความเป็นไปได้และผลกระทบ และดำเนินมาตรการที่เหมาะสมเพื่อบรรเทาผลกระทบเหล่านั้น สิ่งนี้ทำให้มั่นใจได้ว่าองค์กรมีความพร้อมมากขึ้นในการตอบสนองและกู้คืนจากวิกฤตการณ์ด้านไอที ลดผลกระทบต่อผู้ป่วย เจ้าหน้าที่ และผู้มีส่วนได้ส่วนเสียให้น้อยที่สุด

แผนบริหารความเสี่ยงในสภาวะวิกฤตด้านสารสนเทศ โรงพยาบาลแก่งหางแมว ตามที่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 พระราชบัญญัติการ รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติว่า ด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 รวมทั้งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่เกี่ยวข้อง กับภารกิจของโรงพยาบาลแก่งหางแมว ในการเป็นหน่วยงานที่มีโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีผลกระทบ ต่อประชาชนโดยตรง จากการเชื่อมโยงข้อมูลกับหน่วยงานที่เกี่ยวข้อง ควรต้องผ่านเกณฑ์มาตรฐานเพื่อให้ประชาชนมีความปลอดภัย เชื่อมั่น ในการเข้าใช้บริการในระบบบริการสุขภาพรวมทั้งการทำธุรกรรมอิเล็กทรอนิกส์ จำเป็นต้องมีความมั่นคงปลอดภัยไซเบอร์ในระดับสูงเพื่อคุ้มครองประชาชนหรือประโยชน์ที่สำคัญของประเทศ นั้นโรงพยาบาลแก่งหางแมว ได้วิเคราะห์และประเมินความเสี่ยงด้านสารสนเทศ โดยพิจารณาจาก เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) และภัยพิบัติหรือสถานการณ์อื่นๆ รวมถึงได้ กำหนดแนวทางการบริหารความเสี่ยงด้านสารสนเทศ การเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต การสำรอง และการกู้คืนข้อมูลสารสนเทศ เพื่อจัดทำแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ ของโรงพยาบาลแก่งหางแมว สำหรับใช้เป็นแนวทางปฏิบัติงานต่อไป

2. วัตถุประสงค์

2.1 เพื่อให้ โรงพยาบาลแก่งหางแมวมีแนวทางในการระบุและประเมินความเสี่ยงด้านสารสนเทศ รวมถึงการกำหนดแนวทางบริหารความเสี่ยงด้านสารสนเทศ ในการป้องกัน จัดการและลดความเสี่ยงดังกล่าวให้อยู่ในระดับที่ยอมรับได้และทำให้โรงพยาบาลแก่งหางแมวสามารถดำเนินงานได้อย่างต่อเนื่อง

2.2 เพื่อให้ โรงพยาบาลแก่งหางแมวมีแนวทางในการบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศและสามารถเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤตที่อาจจะเกิดขึ้นกับระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงมีแนวปฏิบัติในการบริหารจัดการ กำกับ ตรวจสอบ และดูแลรักษาระบบคอมพิวเตอร์และระบบสารสนเทศ ให้มีความมั่นคง ปลอดภัย มีเสถียรภาพและพร้อมใช้งานตลอดเวลา

2.3 เพื่อให้ โรงพยาบาลแก่งหางแมวมีแนวทางในการสำรองระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ โดยสามารถกู้คืนระบบและข้อมูลดังกล่าวได้ทันที เพื่อให้ผู้ใช้งาน (User) สามารถปฏิบัติงานได้อย่างต่อเนื่อง

3. ขอบเขต

แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศ ของโรงพยาบาลแก่งหางแมว พ.ศ. 2566 ฉบับนี้ เพื่อรองรับสถานการณ์ฉุกเฉินในสภาวะวิกฤตในพื้นที่ของโรงพยาบาลแก่งหางแมว ดังนี้

3.1 เหตุการณ์หรือภัยที่เกิดจากบุคลากร (People)

3.1.1 บุคลากรของโรงพยาบาลแก่งหางแมว

3.1.2 บุคคลภายนอก ผู้ไม่ประสงค์ดี

3.2 เหตุการณ์หรือภัยที่เกิดจากกระบวนการ (Process)

3.2.1 การโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device)

3.2.2 เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค

3.2.3 เหตุการณ์ไฟฟ้าดับ

3.2.4 เหตุการณ์อัคคีภัย

3.2.5 เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง

3.3 เหตุการณ์ที่เกิดจากเทคโนโลยี (Technology)

3.3.1 ทรัพย์สิน ครุภัณฑ์ ระบบปฏิบัติการด้านเทคโนโลยี

3.3.2 การสื่อสารและเครือข่ายสารสนเทศ

3.3.3 โครงข่ายสารสนเทศ

3.3.4 ข้อมูลสารสนเทศ

4. การวิเคราะห์ความเสี่ยงด้านสารสนเทศ

โรงพยาบาลแก่งหางแมวเป็นหน่วยงานที่ให้บริการด้านสุขภาพแบบผสมผสาน คือ การรักษา การป้องกัน การส่งเสริมสุขภาพ และการฟื้นฟูสุขภาพ มีบุคลากรทางการแพทย์ เช่น แพทย์ พยาบาล และ สหสาขาวิชาชีพ ทำงานร่วมกันเพื่อให้การดูแลผู้ป่วยอย่างครอบคลุม การพัฒนานวัตกรรมดิจิทัลด้านระบบบริการสุขภาพตามนโยบายเศรษฐกิจ ดิจิทัล (Digital Economy) และภารกิจโรงพยาบาลแก่งหางแมวมีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ที่ต้องผ่านเกณฑ์มาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งการบริหารราชการของโรงพยาบาลด้านขับเคลื่อนการพัฒนารัฐบาลดิจิทัล (Digital Government) ผลจากการวิเคราะห์ดังกล่าว พบว่าความเสี่ยงที่อาจเป็นอันตรายต่อระบบคอมพิวเตอร์และสารสนเทศ รวมถึงข้อมูลสารสนเทศ มีดังนี้

4.1 ความเสี่ยงที่เกิดจากบุคคล (People) ดังนี้

4.1.1 เหตุการณ์หรือภัยที่เกิดจากบุคลากร โรงพยาบาลแก่งหางแมว หมายถึง บุคลากรของโรงพยาบาล ขาดความรู้ ความเข้าใจในการใช้งานเทคโนโลยีสารสนเทศ เช่น ด้านฮาร์ดแวร์ ด้านซอฟท์แวร์ และ ด้านเครือข่าย รวมถึงการใช้สิทธิในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ ข้อมูลสารสนเทศที่ไม่เหมาะสม

4.1.2 เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี หมายถึง ผู้ที่หวังก่อกวน เจาะทำลายระบบ เพื่อสร้างความ เสียหายแก่ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ หากไม่ได้รับการป้องกันด้วยเครื่องมือ หรืออุปกรณ์ที่มีมาตรฐานและอัพเดทให้ทันสมัย เช่น Firewall ระบบ IPS และระบบป้องกันไวรัส

4.2 ความเสี่ยงที่เกิดจากกระบวนการ (Process) ดังนี้

4.2.1 เหตุการณ์หรือภัยที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) หมายถึง ผู้ที่ลักลอบเข้าไปโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) ภายในห้องศูนย์กลางข้อมูล

ศูนย์ สำรองข้อมูล และห้องเซิร์ฟเวอร์ หากศูนย์ข้อมูลดังกล่าวไม่ได้รับการป้องกันที่ดี เช่น มาตรการในการเข้าถึงห้อง ศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ เครื่องอ่านบัตรแถบแม่เหล็ก กล้องวงจรปิด และเจ้าหน้าที่ รักษาความปลอดภัย เป็นต้น

4.2.2 ความเสี่ยงที่เกิดจากด้านเทคนิค หมายถึง เหตุการณ์หรือภัยที่เกิดจากอุปกรณ์ ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ ทำงานไม่เต็มประสิทธิภาพหรือไม่สามารถให้บริการได้ เช่น อุปกรณ์ประมวลผลข้อมูล (Process Device) ชำรุด เสียหาย เนื่องจากอุปกรณ์บางรายการเสื่อมสภาพตามอายุการใช้งาน ระบบ ปรับอากาศชำรุดส่งผลให้ อุณหภูมิภายในห้องสูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ที่ให้บริการ หยุดการทำงาน ส่งผลให้ระบบคอมพิวเตอร์และระบบสารสนเทศไม่สามารถใช้งานได้ หรืออาจได้รับความเสียหาย

4.2.3 ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ

4.2.3.1 เหตุการณ์ไฟฟ้าดับ หมายถึง เหตุการณ์หรือภัยที่เกิดจากไฟฟ้าดับ ซึ่งส่งผลให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ ไม่มีแหล่งพลังงานที่ใช้ในการเปิด ระบบคอมพิวเตอร์และระบบสารสนเทศสำหรับให้บริการ เช่น สายไฟฟ้าขาด ไฟฟ้า ช็อต หม้อแปลงไฟฟ้าที่ติดตั้งบริเวณโรงพยาบาลแก่งหางแมว ได้รับความเสียหาย

4.2.3.2 เหตุการณ์อัคคีภัย หมายถึง เหตุการณ์หรือภัยที่เกิดจากไฟไหม้ ซึ่งเป็นเหตุการณ์ที่สร้าง ความเสียหายร้ายแรงที่สุด ทำให้ระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลข้อมูล (Process Device) ในห้องศูนย์ข้อมูล (Data Center) ถูกไฟไหม้จนทำให้ไม่สามารถปฏิบัติงานได้ ซึ่งเกิดได้หลายสาเหตุ เช่น ไฟฟ้าลัดวงจร หรือไฟไหม้บริเวณอื่นแล้วไหม้ลุกลามมาที่ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์

4.2.3.3 เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุม ประท้วงหรือความไม่สงบเรียบร้อยทางการเมือง หมายถึง อันเกิดจากภัยตามธรรมชาติหรือสถานการณ์ที่เกิดจากกลุ่มบุคคล ซึ่งอาจไม่เกิดผลกระทบโดยตรงต่อการให้บริการของระบบคอมพิวเตอร์และระบบสารสนเทศ แต่จะเกิดผลกระทบต่อการเข้าไป ปฏิบัติงานภายในพื้นที่โรงพยาบาลแก่งหางแมว

4.3 ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology) เช่น

4.3.1 ทรัพย์สินครุภัณฑ์ ระบบปฏิบัติการด้านเทคโนโลยี (Hardware, Software)

4.3.2 เครือข่ายสารสนเทศ และเครือข่ายเสมือน (Information Network and Virtual Machine)

4.3.3 โครงข่ายการสื่อสาร (Communication Network)

4.3.4 ข้อมูลและสารสนเทศ (Information)

5. การประเมินความเสี่ยงด้านสารสนเทศ

การประเมินความเสี่ยงด้านสารสนเทศ โรงพยาบาลแก่งหางแมว ได้ประเมินความเสี่ยงที่เกิดจากบุคคล จากทางด้านเทคนิค และจากภัยพิบัติหรือสถานการณ์อื่นๆ ตามข้อ 3 และ 4 เป็นแนวทางในการดำเนินงาน โดย โรงพยาบาลแก่งหางแมวได้ประเมินสถานการณ์ความเสี่ยงด้านสารสนเทศของโรงพยาบาลแก่งหางแมวแล้ว ปรากฏ ดังนี้

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางแก้ไข
5.1 ความเสี่ยงที่เกิดจากบุคคล (People)						
(1) เหตุการณ์หรือ ภัยที่เกิดจากบุคลากรภายในโรงพยาบาล	ระบบคอมพิวเตอร์ติดไวรัส หรือหนอนอินเทอร์เน็ตจากอินเตอร์เน็ต หรือไฟล์ที่คัดลอกจากอุปกรณ์ บันทึกข้อมูลแบบ พกพา เช่น Flash Drive และ Externel Harddisk, Storage ส่งผลให้ระบบ คอมพิวเตอร์และระบบสารสนเทศประมวลผล ข้อมูลได้ช้าลง หรืออาจทำงาน ผิดพลาดได้	5	5	25	สูง	- ผู้ดูแลระบบ (System Administrator) ตัดการเชื่อมต่อเครื่อง ที่ติดไวรัสดังกล่าวออกจากระบบเครือ ขาย ภายใน และดำเนินการสแกนไวรัส เพื่อกำจัดไวรัสเครื่องดังกล่าว - หากไวรัสดังกล่าวไม่หายไป ให้ดำเนินการสแกนไวรัสที่เครื่องคอมพิวเตอร์แม่ข่าย (Server)
(2) เหตุการณ์หรือภัยที่เกิดจากผู้ไม่ประสงค์ดี	ระบบคอมพิวเตอร์และระบบสารสนเทศอาจถูกบุกรุกโจมตี หรือถูกขโมยข้อมูลสารสนเทศ หรือปรับแต่งแก้ไขระบบหน้าเว็บไซต์ ซึ่งอาจส่งผลให้ระบบสารสนเทศล่มได้	3	5	15	ค่อนข้างสูง	ตรวจพอร์ตทั้งหมดที่ใช้เชื่อมต่อแล้วให้ ปิดพอร์ตที่ไม่ได้ใช้งาน โดยทันที

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางแก้ไข
5.2 ความเสี่ยงที่เกิดจากกระบวนการ (Process)						
(1) เหตุการณ์หรือภัย ที่เกิดจากการโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device)	- อุปกรณ์ประมวลผลข้อมูล (Process Device)สูญหาย และอาจเสี่ยงต่อการถูกโจรกรรมข้อมูลบนอุปกรณ์ประมวลผล ข้อมูล (Process Device) ซึ่งส่งผลกระทบต่อ โรงพยาบาลแก่งหางแมว	3	5	15	ค่อนข้างสูง	- ผู้พบเหตุรายงานให้หัวหน้างานเทคโนโลยีสารสนเทศทราบ เพื่อรายงานตามลำดับชั้นและสั่งการต่อไป - ผู้ดูแลระบบ (System Administrator) ตรวจสอบความครบถ้วนและความเสียหาย
(2) ความเสี่ยงที่ เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ	- ระบบปรับอากาศชำรุดส่งผลให้อุณหภูมิ ในห้องศูนย์ข้อมูลและสารสนเทศสูงขึ้น ทำให้อุปกรณ์ประมวลผลข้อมูล (Process Device) ได้รับความเสียหาย	1	5	5	ค่อนข้างต่ำ	-รายงานให้ ผู้อำนวยการโรงพยาบาลทราบเพื่อสั่งการต่อไป - ผู้อำนวยการโรงพยาบาล ประชาสัมพันธ์ให้กับบุคลากรได้รับทราบถึงการหยุดให้บริการ ชั่วคราวเนื่องจากไฟฟ้าดับ - ผู้อำนวยการโรงพยาบาล ประสานงานกับกลุ่มเทคโนโลยี สารสนเทศเพื่อสอบถามปัญหา และ ระยะเวลา การแก้ไขที่จะสามารถ กลับมาให้บริการได้ - ผู้ดูแลระบบ (System Administrator) เปิดการใช้งานระบบคอมพิวเตอร์ และ

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางแก้ไข
						ระบบสารสนเทศ รวมทั้งรายงานให้ผู้อำนวยการทราบตามลำดับ - ผู้อำนวยการโรงพยาบาล ประชาสัมพันธ์ให้กับบุคลากร ได้รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศ สามารถกลับมาใช้งานได้ปกติ
	(3.2) เหตุการณ์อัคคีภัย - สินทรัพย์ (Asset)ที่ย้ายไม่ทันอาจถูกไฟไหม้ - อุปกรณ์ประมวลผลข้อมูล (Process Device) ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์ ไม่ สามารถให้บริการได้	1	5	5	ค่อนข้างต่ำ	แนวทางปฏิบัติตามแผนป้องกันและระงับอัคคีภัย ในการรักษาความมั่นคงปลอดภัยสารสนเทศ กรณีที่ 1 ไฟเริ่มไหม้หรือสามารถดับไฟได้ - ให้ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณที่เป็นต้นเพลิงของไฟไหม้จนไฟดับ

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางแก้ไข
(3)ความเสี่ยงที่เกิดจากภัยพิบัติหรือจากสถานการณ์อื่นๆ						- ผู้พบเหตุรายงานให้หัวหน้า เทคโนโลยีสารสนเทศทราบ และให้แจ้ง ผู้อำนวยการทราบโดยเร็ว - ผู้ดูแลระบบ (System Administrator) ประเมินสถานการณ์ในเบื้องต้นว่า ควรหยุดให้บริการระบบคอมพิวเตอร์ ระบบสารสนเทศหรือไม่ - ถ้าหยุดให้บริการผู้อำนวยการโรงพยาบาล สั่งการให้กับ บุคลากรได้รับทราบถึงการหยุดให้ บริการ ชั่วคราว เนื่องจากเหตุไฟไหม้ - ผู้ดูแลระบบ (System Administrator) ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ ประมวลผลข้อมูล (Process Device) ระบบปรับอากาศ และสภาพภายใน ห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ พร้อมทั้งรายงานให้ผู้อำนวยการโรงพยาบาล เพื่อสั่งการต่อไป

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางแก้ไข
						- หากเสียหายเล็กน้อยให้ผู้ดูแลระบบ (System Administrator) ดำเนินการ

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางแก้ไข
						แก้ไข และเปิดการใช้งานระบบคอมพิวเตอร์ และระบบสารสนเทศ - ประชาสัมพันธ์ให้กับบุคลากรได้ รับทราบว่าระบบคอมพิวเตอร์และระบบสารสนเทศสามารถกลับมาใช้งาน ได้แล้ว - หากเสียหายมากให้ผู้ดูแลระบบ (System Administrator) รายงานผู้อำนวยการโรงพยาบาล เพื่อสั่งการต่อไป กรณีที่ 2 ไฟไหม้เริ่มลุกลามถึงขั้นรุนแรง - ให้ผู้พบเหตุดำเนินการตามขั้นตอน ในแผนระงับอัคคีภัยของโรงพยาบาล - ผู้พบเหตุนำถังดับเพลิงฉีดบริเวณไฟที่เริ่มลุกลามและบริเวณโดยรอบ หากไม่สามารถระงับเหตุได้ ให้ออกจากพื้นที่โดยเร็ว -ประชาสัมพันธ์ให้กับบุคลากรได้ รับทราบถึงการหยุด ให้บริการเนื่องจาก เหตุไฟไหม้

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางแก้ไข
	(3.3) เหตุการณ์ที่เกิดจาก ภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง - เช่น กรณีการชุมนุมประท้วง หรือความ ไม่สงบเรียบร้อยทางการเมือง อาจถูกปิดกั้นการเข้าออกและอาจเสี่ยง ต่อการถูกตัดไฟฟ้า/น้ำาบริเวณกระทรวง สาธารณสุข ซึ่งส่งผลกระทบต่อห้อง ศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือ ห้องเซิร์ฟเวอร์ หรือสถานที่ปฏิบัติงาน บริเวณอาคาร โรงพยาบาลแก่งหางแมวสุขภาพ	1	5	5	ค่อนข้างต่ำ	- หากสามารถระงับเหตุได้ ให้ผู้ดูแล ระบบ (System Administrator) ตรวจสอบความเสียหาย ผลกระทบ และความพร้อมใช้งานของอุปกรณ์ ประมวลผลข้อมูล (Process Device) ระบบปรับอากาศ และสภาพภายใน ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรอง ข้อมูล หรือห้องเซิร์ฟเวอร์ รายงานให้ ผู้อำนวยการโรงพยาบาลเพื่อสั่งการต่อไป - ถ้าเกิดเหตุการณ์ไฟฟ้าดับ ให้ดำเนินการตามแนวทางแก้ไขตาม ข้อ 5 - กำหนดให้ผู้ใช้งาน (User) ปฏิบัติงานจากสถานที่ปฏิบัติงานสำรองหรือที่พักอาศัย ตามที่ โรงพยาบาลแก่งหางแมวกำหนด
5.3 ความเสี่ยงที่เกิดจากเทคโนโลยี (Technology)						

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางแก้ไข
5.3.1 ทรัพย์สินไม่เพียงพอต่อการใช้งาน ครุภัณฑ์ - ไม่พร้อมใช้งาน ค่อนข้างสูง ระบบปฏิบัติการด้านเทคโนโลยี (Hardware, Software)	- ไม่เพียงพอต่อการใช้งาน - ไม่พร้อมใช้งาน	1	5	5	ค่อนข้างต่ำ	- จัดทำแผนคุมทะเบียนทรัพย์สินตามระเบียบพัสดุ - สำรวจ จัดซื้อ/จัดหา ให้พร้อมใช้งานตามแผนที่กำหนด - กำหนดแนวทางการควบคุม กำกับติดตามประเมินการใช้งาน การเข้ารหัส ในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง - ปรับปรุงระบบการยืม-คืน เมื่อนำอุปกรณ์ระบบคอมพิวเตอร์ไปใช้นอกสำนักงาน - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
5.3.2 เครือข่ายสารสนเทศ และเครือข่ายเสมือน (Information Network and Virtual Machine)	- ไม่เพียงพอต่อการใช้งาน - ไม่พร้อมใช้งาน	1	5	5	ค่อนข้างต่ำ	- กำหนดแนวทางการควบคุม กำกับติดตามประเมินการใช้งาน การเข้ารหัส ในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ความเสี่ยง	ความสูญเสียที่คาดว่าจะเกิดขึ้น	โอกาสเกิด	ผลกระทบ	ระดับความเสี่ยง	ผลประเมินระดับความเสี่ยง	แนวทางแก้ไข
5.3.3 โครงข่าย การสื่อสาร (Communication Network)	- ไม่เพียงพอต่อการใช้งาน - ไม่พร้อมใช้งาน	1	5	5	ค่อนข้างต่ำ	- กำหนดแนวทางการควบคุม กำกับติดตามประเมินการใช้งาน การเข้ารหัส ในระบบเครื่องคอมพิวเตอร์ให้ครบทุกเครื่อง - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
5.3.4 ข้อมูลและสารสนเทศ (Information)		2	4	10	ค่อนข้างสูง	- กำหนดแนวทางการควบคุม กำกับติดตามประเมินการใช้งาน การเข้ารหัส - ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

<u>หมายเหตุ</u> เกณฑ์การประเมินให้คะแนนโอกาสที่จะเกิดและผลกระทบ

ระดับ 1 =รุนแรงน้อยที่สุด/โอกาสเกิดน้อยที่สุด

ระดับ 2 =รุนแรงน้อย/โอกาสเกิดน้อย

ระดับ 3 =รุนแรงน้อยปานกลาง/โอกาสเกิดปานกลาง

ระดับ 4 =รุนแรงมาก/โอกาสเกิดมาก

ระดับ 5 =รุนแรงมากที่สุด/โอกาสเกิดมากที่สุด

แผนผังประเมินความ

ผลกระทบของความเสี่ยง

๕	๑๐	๑๕	๒๐	๒๕
๔	๘	๑๒	๑๖	๒๐
๓	๖	๙	๑๒	๑๕
๒	๔	๖	๘	๑๐
๑	๒	๓	๔	๕

สีแดง ระดับความเสี่ยงสูง ค่าระหว่าง ๑๕ - ๒๕

สีเหลือง ระดับความเสี่ยงค่อนข้างสูง ค่าระหว่าง ๘ - ๑๔

สีเขียว ระดับความเสี่ยงค่อนข้างต่ำ ค่าระหว่าง ๔ - ๗

สีฟ้า ระดับความเสี่ยงต่ำ ค่าระหว่าง ๑ - ๓

6. การเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต

เนื่องจากเหตุการณ์ที่เป็นความเสี่ยงด้านสารสนเทศข้างต้น โรงพยาบาลแก่งหางแมว จึงได้ดำเนินการ จัดทำแนวทางการเตรียมความพร้อมกรณีฉุกเฉินในสภาวะวิกฤต เพื่อป้องกันภัยจากเหตุการณ์หรือภัยที่จะเกิดขึ้น ดังนี้

6.1 เหตุการณ์หรือภัยที่เกิดจากบุคลากร (People)

6.1.1 เหตุการณ์หรือภัยที่เกิดจากบุคลากรของโรงพยาบาลแก่งหางแมว มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(1) กำหนดให้ปฏิบัติตามประกาศโรงพยาบาลแก่งหางแมว เรื่อง นโยบายและแนวปฏิบัติในการ รักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.2566

(2) การสร้างความรู้ความเข้าใจในการใช้ระบบคอมพิวเตอร์และระบบสารสนเทศเบื้องต้น โดยการจัดอบรมให้กับบุคลากร หรือส่งไปอบรมร่วมกับหน่วยงานภายนอกที่จัดขึ้น เพื่อลดความเสี่ยงด้านสารสนเทศ

(3) มีการประชาสัมพันธ์ให้ความรู้แก่บุคลากรผ่านช่องทางสื่อสารต่างๆ ตามความเหมาะสม เช่น ผ่านระบบ Website ติดบอร์ดประชาสัมพันธ์ E-Mail, Line, Chat, Facebook หรือสื่อ Social Media อื่นๆ ของกลุ่ม เทคโนโลยีสารสนเทศ โรงพยาบาลแก่งหางแมว เป็นต้น

6.1.2 เหตุการณ์หรือภัยที่เกิดจากบุคคลภายนอก ผู้ไม่ประสงค์ดี มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(1) ติดตั้งและใช้งาน Firewall เพื่อป้องกันการบุกรุกจากผู้ไม่ประสงค์ดีต่อระบบคอมพิวเตอร์และ ระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ประมวลผลข้อมูล (Process Device)

(2) ติดตั้งซอฟต์แวร์ป้องกันไวรัส (Anti Virus)/ หนอนคอมพิวเตอร์ (Worm) หรือโปรแกรมไม่ประสงค์ดี (Anti Malware) ที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client)

6.2 เหตุการณ์หรือภัยที่เกิดจากกระบวนการ (Process)

6.2.1 การโจรกรรมอุปกรณ์ประมวลผลข้อมูล (Process Device) มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(1) มีมาตรการควบคุมการเข้า - ออกห้องศูนย์ข้อมูล (Data Center) ดังนี้

(1.1) ปฏิบัติตามหลักเกณฑ์สำหรับการปฏิบัติงานภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ ตามที่ โรงพยาบาลรีไศลกำหนด

(1.2) การติดตั้ง ซ่อมแซม และนำอุปกรณ์ใดๆ ออกจากห้องศูนย์กลางข้อมูล ศูนย์ สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ ต้องได้รับอนุมัติจากหัวหน้างานเทคโนโลยีสารสนเทศ ก่อนเริ่มดำเนินการทุกครั้ง

(1.3) ห้ามผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ เว้นแต่ได้รับอนุญาตจากหัวหน้างานเทคโนโลยีสารสนเทศ

(1.4) ผู้ใช้งาน (User) หรือบุคคลภายนอก

(1.4.1) ต้องติดบัตรแสดงตนตลอดระยะเวลา ที่ปฏิบัติงาน โดยมีผู้ดูแลระบบ (System Administrator) ควบคุมการปฏิบัติงานของผู้ใช้งาน (User) หรือบุคคลภายนอกตลอดเวลา

(1.4.2) ต้องไม่นำอาหารหรือเครื่องดื่มเข้าไปในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์

(1.4.3) ห้ามสูบบุหรี่ ในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์

(1.5) มีเจ้าหน้าที่รักษาความปลอดภัยตลอด 24 ชั่วโมง

(1.6) มีการติดตั้งระบบควบคุมการเข้าถึง (Access Control) ห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ด้วยระบบอิเล็กทรอนิกส์

(1.7) มีการติดตั้งกล้องวงจรปิดบันทึกเหตุการณ์บริเวณทางเข้าและภายในห้อง ศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์เพื่อเฝ้าระวังเหตุการณ์หรือภัยที่จะเกิดขึ้น

6.2.2 เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(1) มีการตรวจความพร้อมอุปกรณ์ประมวลผลข้อมูล (Process Device) ทั้งทางกายภาพและด้านเทคนิคให้พร้อมใช้งานอยู่เสมออย่างน้อยเดือนละ 1 ครั้ง หากพบอุปกรณ์ประมวลผลข้อมูล (Process Device) หรืออุปกรณ์ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ชำรุดเสียหาย หรือใกล้เสื่อมสภาพการใช้งาน ให้รายงานให้ผู้อำนวยการโรงพยาบาลทราบ เพื่อรายงานตามลำดับขั้นและสั่งการแก้ไข ด้วยการซ่อมแซม หรือจัดซื้อ ทดแทนต่อไป

(2) มีการตรวจสอบปริมาณการเข้าถึงเครือข่ายภายนอก (Intemet) เพื่อสังเกตปริมาณ การใช้งาน อัตราความเร็วของข้อมูล เพื่อเฉลี่ยแบนด์วิดท์ (Bandwidth) ให้ทั่วถึงทั้งองค์กร และป้องกัน ไม่ให้ผู้ใช้งาน (User) มีการใช้แบนด์วิดท์ (Bandwidth) มากเกินไป

6.2.3 เหตุการณ์ไฟฟ้าดับ มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

มีการติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) จำนวน 4 เครื่อง ขนาดเครื่องละ 3 KVA ต่อให้ Server ซึ่งใช้ redundant Power Supply ตัวเพื่อช่วยแบ่งจ่ายไฟ ช่วยเซฟ Power Supply มากขึ้น ใช้สำรองถ้ามีตัวใดตัวหนึ่งเสียจะมี Power Supply อีกตัวซัพพอร์ตทำให้ทำงานได้อย่างต่อเนื่อง ซึ่งเหมาะสำหรับระบบควบคุมที่ต้องทำงานอย่างต่อเนื่องและไม่สามารถหยุดทำงานได้แม้ว่ามีปัญหาเกิดขึ้นป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมถึงอุปกรณ์ประมวลผลข้อมูล (Process Device) โดยทั้ง 4 เครื่อง สามารถสำรองไฟฟ้า ได้เป็นเวลา ประมาณ 30 นาที ซึ่งเพียงพอต่อการจัดเก็บและสำรองข้อมูลสารสนเทศในกรณีที่เกิดไฟฟ้าดับ

6.2.4 เหตุการณ์อัคคีภัย มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(1) มีการติดตั้งอุปกรณ์ตรวจจับควัน กรณีเกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้น ภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนเพื่อให้เจ้าหน้าที่รักษาความปลอดภัยหรือผู้พบเหตุทราบและเข้ามาระงับเหตุฉุกเฉินก่อนเกิดอัคคีภัยได้อย่างทันท่วงที เพราะเป็นภัยที่มีผลกระทบรุนแรงที่สุด

(2) มีการติดตั้งถังดับเพลิงชนิดที่ใช้สารเคมีไม่ทำอันตรายต่ออุปกรณ์ประมวลผลข้อมูล (Process Device) ไว้ในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ จำนวน 1 ถัง และห้องศูนย์กลางข้อมูล ศูนย์ สำรองข้อมูล หรือห้องเซิร์ฟเวอร์ จำนวน 2 ถัง เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยหรือผู้พบเหตุใช้ระงับเหตุก่อนไฟ เริ่มลุกลามถึงขั้นรุนแรง

6.2.5 เหตุการณ์ที่เกิดจากภัยพิบัติหรือสถานการณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(1) ให้ผู้ใช้งาน (User)สำรองข้อมูลสารเทศส่วนตัวลงในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externet Harddisk

(2) มีเจ้าหน้าที่รักษาความปลอดภัยตลอด 24 ชั่วโมง เพื่อป้องกันไม่ให้บุคคลภายนอกเข้า

ไปภายในห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล หรือห้องเซิร์ฟเวอร์โดยไม่ได้รับอนุญาต

(3) ตรวจสอบการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ เพื่อให้ผู้ใช้งาน (User) ปฏิบัติงานจากภายนอกโรงพยาบาล (Teleworking) โดยผ่านเครือข่ายภายนอก (Internet) ได้

(4) ตรวจสอบความพร้อมของข้อมูลสารสนเทศที่ได้สำรองระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศที่ได้บันทึกลงใน ฮาร์ดดิสต์ (External Hardisk Drive) หรืออุปกรณ์สำรอง ข้อมูลอื่นใด สำหรับเตรียมนำไปกู้คืน จากศูนย์สำรองข้อมูล (Disaster Recovery Site : DR Site) ตามที่ผู้บริหารเห็นชอบ หากเกิดเหตุการณ์ฉุกเฉินในสภาวะวิกฤตจนส่งผลให้ เครื่องคอมพิวเตอร์แม่ข่าย (Server) ต้องปิดระบบการให้บริการถูกปิดลง

(5) เมื่อ โรงพยาบาล ได้รับแจ้งว่าจะเกิดเหตุชุมนุมประท้วงหรือความไม่ สงบเรียบร้อยทางการเมืองบริเวณโรงพยาบาล ซึ่งอาจถูกปิดกั้นการเข้าออก และอาจเสี่ยงต่อการถูกตัดไฟฟ้า/น้ำให้ผู้ดูแลระบบ (System Administator) นำฮาร์ดดิสต์ (External Hardisk Drive) หรืออุปกรณ์สำรองข้อมูลอื่นใด ที่สำรองข้อมูลไว้ ไปเก็บในสถานที่ปลอดภัย

6.3 เหตุการณ์ที่เกิดจากเทคโนโลยี (Technology)

6.3.1 ทรัพย์สิน ครุภัณฑ์ ระบบปฏิบัติการด้านเทคโนโลยี

6.3.2 การสื่อสารและเครือข่ายสารสนเทศ

6.3.3 โครงข่ายสารสนเทศ

6.3.4 ข้อมูลสารสนเทศ

มีแนวปฏิบัติเพื่อเตรียมรับสถานการณ์ ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ โรงพยาบาล

7. กลยุทธความต่อเนื่องในสภาวะวิกฤต

หากเหตุการณ์หรือภัยได้เกิดขึ้นแล้ว ต้องมีการดำเนินกลยุทธ์ความต่อเนื่องในสภาวะวิกฤต เพื่อให้การปฏิบัติงานของบุคลากร ดำเนินการไปได้อย่างต่อเนื่องหรือได้รับผลกระทบน้อยที่สุด ดังนี้

ทรัพยากร	กลยุทธ์ความต่อเนื่อง
1.สถานที่ปฏิบัติงาน โรงพยาบาลแก่งหางแมว	1.กำหนดพื้นที่ปฏิบัติงานสำรอง ได้แก่ ห้องคอมพิวเตอร์หรือพื้นที่อื่นๆ โดยประสานงานและสำรวจความเหมาะสมของสถานที่ 2. ประสานขอใช้พื้นที่กับส่วนราชการอื่นเป็นสถานที่ปฏิบัติงาน สำรองเพิ่มเติม 3.หากพื้นที่ปฏิบัติงานสำรองมีพื้นที่จำกัด หรืออาจเกิดอันตรายระหว่างเดินทาง ไปปฏิบัติงาน ให้บุคลากรปฏิบัติงานจากที่พักอาศัย
2.วัสดุอุปกรณ์	1.จัดหาเครื่องคอมพิวเตอร์สำรองพร้อมอุปกรณ์ในการเข้าถึงระบบเครือข่าย เพื่อให้ผู้ใช้งาน (User) สามารถเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศได้ 2. จัดเตรียมอุปกรณ์สารสนเทศสำหรับนำมาใช้ในการปฏิบัติงาน เช่น เครื่องพิมพ์ (Printer)เครื่องสแกนเนอร์(Scaner)และสายเชื่อมต่อระบบเครือข่ายเฉพาะที่ (Lan) 3.ผู้ใช้งาน (User) สามารถใช้คอมพิวเตอร์แบบพกพาส่วนตัวในการปฏิบัติงานได้
3.ระบบคอมพิวเตอร์ ระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ	๑. ระบบคอมพิวเตอร์และระบบสารสนเทศ และข้อมูลสารสนเทศได้ติดตั้ง และระบบสารสนเทศ รวมถึงข้อมูล จัดเก็บไว้ใน ห้อง(Data Center) ตึกโอพีดีชั้น 3 และห้อง(Data Center) ตึกร่มไทรชั้น 4 ซึ่งรองรับการเข้าถึงจากภายนอก โดยการรับส่งข้อมูลผ่านเครือข่าย ส่วนตัวเสมือน (Virtual Private Network : VPN) และมีการเข้ารหัส รักษาความปลอดภัยแบบ Secure Sockets Layer (SSL) 2. จัดเตรียมไซต์สำรอง (Disaster Recovery Site : DR Site) เมื่อเกิดเหตุฉุกเฉิน หรือสภาวะวิกฤต 3. กลุ่มเทคโนโลยีสารสนเทศพิจารณาและนำ ฮาร์ดดิสต์ (External Hardisk Drive) หรืออุปกรณ์สำรองข้อมูลอื่นใด ที่สำรองระบบคอมพิวเตอร์ ระบบสารสนเทศ และข้อมูลสารสนเทศ ณ ห้องศูนย์กลางข้อมูล (Data Center) ไปไว้ในสถานที่ ปลอดภัย 4. สำหรับระบบ SMART ซึ่งเป็นระบบสารสนเทศตามภารกิจหลัก เพื่อ บริการแก่บุคลากรและส่วนราชการที่เกี่ยวข้อง ได้ 5. ให้ผู้ใช้งาน (User) สำรองข้อมูลสารสนเทศที่จำเป็นและสำคัญไว้ในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Flash Drive และ Externet Harddisk
4.บุคลากร	1. หากผู้ดูแลระบบ (System Administrator) มีจำนวนไม่เพียงพอต่อการปฏิบัติหน้าที่ ให้ผู้รับจ้างที่ดูแลระบบคอมพิวเตอร์และระบบสารสนเทศให้กาสนับสนุนด้านเทคนิค

ทรัพยากร	กลยุทธ์ความต่อเนื่อง
	อนุญาตให้ผู้ใช้งาน(User)ปฏิบัติงานจากภายนอกโรงพยาบาล(Teleworking) โดยเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านระบบคอมพิวเตอร์ลูกข่ายแบบเสมือน (Virtualization System)
5. ผู้รับบริการ และผู้ที่เกี่ยวข้อง	1. แจ้งสถานที่การติดต่อราชการสำรองผ่านทางหน้าเว็บไซต์ของ โรงพยาบาล 2. บุคลากรที่มีหน้าที่ปฏิบัติงานร่วมกับหน่วยงานอื่นๆ ให้ประสานงาน ทางโทรศัพท์เคลื่อนที่หรือจดหมายอิเล็กทรอนิกส์ (E - Mail) หรือหาก ระบบคอมพิวเตอร์และ ระบบสารสนเทศอยู่ระหว่างดำเนินการกู้คืน ให้พิจารณาใช้จดหมายอิเล็กทรอนิกส์ (E - Mail) จากภายนอกที่มีความน่าเชื่อถือ

8. ระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต

จากการวิเคราะห์ผลกระทบจากความเสี่ยงในข้อ 5 เพื่อให้บุคลากรสามารถปฏิบัติงานด้วยความต่อเนื่อง จึงกำหนดระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต ดังนี้

กระบวนงาน	ระดับผลกระทบ	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต		
		ภายใน 1 วัน	ภายใน 7 วัน	มากกว่า 7 วัน
8.1 เหตุการณ์หรือภัยที่เกิดจากบุคลากร (People)				
8.1.1 เหตุการณ์หรือภัยที่เกิดจากบุคลากรของโรงพยาบาลแก่งหางแมว	สูง	√		
8.1.2 เหตุการณ์หรือภัยที่เกิดจากบุคคลภายนอกหรือผู้ไม่ประสงค์ดี	ค่อนข้างสูง		√	
8.2 เหตุการณ์หรือภัยที่เกิดจากกระบวนการ (Process)				
8.2.1 เหตุการณ์หรือภัย ที่เกิดจากการโจรกรรมอุปกรณ์ ประมวลผลข้อมูล (Process Device)	ค่อนข้างสูง		√	
8.2.2 เหตุการณ์หรือภัยที่เกิดจากด้านเทคนิค	ค่อนข้างต่ำ		√	
8.2.3 เหตุการณ์ไฟฟ้าดับ	ค่อนข้างต่ำ	√		
8.2.4 เหตุการณ์อัคคีภัย	ค่อนข้างต่ำ			√
8.2.5 เหตุการณ์ที่เกิดจาก ภัยพิบัติหรือสถาน การณ์อื่นๆ เช่น อุทกภัย วาตภัย และการชุมนุมประท้วง หรือความไม่สงบเรียบร้อยทางการเมือง	ค่อนข้างต่ำ		√	
8.3 เหตุการณ์ที่เกิดจากเทคโนโลยี (Technology)				

กระบวนงาน	ระดับผลกระทบ	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพเมื่อเกิดสภาวะวิกฤต		
		ภายใน 1 วัน	ภายใน 7 วัน	มากกว่า 7 วัน
8.3.1 ทรัพย์สิน ครุภัณฑ์	ค่อนข้างต่ำ			√
8.3.2 การสื่อสารและเครือข่ายสารสนเทศ	ค่อนข้างสูง	√		
8.3.3 โครงข่ายสารสนเทศ	ค่อนข้างสูง	√		
8.3.4 ข้อมูลสารสนเทศ	ค่อนข้างสูง	√		

9. โครงสร้างและทีมบริหารความต่อเนื่อง (BCP Team)

เพื่อให้แผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ โรงพยาบาลรีไศล สามารถนำไป ปฏิบัติได้อย่างมีประสิทธิภาพ จึงต้องมีการจัดตั้งทีมบริหารความต่อเนื่อง (BCP Team) ซึ่งประกอบด้วยผู้อำนวยการโรงพยาบาล บุคลากรกลุ่มงานเทคโนโลยีสารสนเทศ เนื่องจากมีความรู้ความ สามารถด้านระบบคอมพิวเตอร์และระบบสารสนเทศ ประกอบกับปฏิบัติหน้าที่ เป็นผู้ดูแลระบบ (System Administrator) ของ โรงพยาบาล

9.1 หน้าที่ความรับผิดชอบทีมบริหารความต่อเนื่อง (BCP Team) ดังนี้

9.1.1 หัวหน้าทีมและรองหัวหน้าทีม มีหน้าที่ในการพิจารณาแนวทางการแก้ไขปัญหา กำหนดขอบเขต และสั่งการให้ผู้ที่รับผิดชอบดำเนินการแก้ไข พร้อมทั้งรายงานให้คณะผู้บริหาร ได้รับทราบ

9.1.2 ผู้ประสานงาน มีหน้าที่ในการติดต่อประสานงานภายในและหน่วยงานภายนอก โรงพยาบาล และจัดเตรียมเอกสารข้อมูลที่เกี่ยวข้อง รวมถึงจัดทำรายงานในแต่ละสถานการณ์

9.1.3 ผู้ดูแลระบบ (System Administrator) มีหน้าที่การพัฒนาและบริหารจัดการระบบคอมพิวเตอร์ และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนการรักษาความมั่นคงปลอดภัย ดูแลสิทธิของผู้ใช้งาน (User) แก้ไขปัญหาการใช้งาน และดูแลห้องศูนย์กลางข้อมูล ศูนย์สำรองข้อมูล และห้องเซิร์ฟเวอร์

9.2 รายชื่อทีมดูแลระบบ

นายศุภมิตร เตชะอำไพ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	082-980-4164
นายวรพรต พัฒนะพันธ์	นักวิชาการคอมพิวเตอร์	086-846-9389

10. กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree)

กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree) ตามแนวทางของแผนบริหารความต่อเนื่องในสภาวะวิกฤตด้านสารสนเทศของ โรงพยาบาลแก่งหางแมว หมายถึง ขั้นตอนการแจ้งเหตุฉุกเฉินหรือการแจ้งปัญหาระบบคอมพิวเตอร์และ ระบบสารสนเทศ เพื่อรายงานให้ผู้บังคับบัญชาทราบตามลำดับชั้นและสั่งการให้ผู้ที่มีหน้าที่รับผิดชอบ ดำเนินการแก้ไข ตามระดับความรุนแรงของเหตุนั้น เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศสามารถ ให้บริการสนับสนุนการ ปฏิบัติงานแก่บุคลากรได้อย่างต่อเนื่อง ที่กำหนดรายละเอียดไว้ตามรายชื่อทีมบริหารความต่อเนื่อง (BCP Team) และหน้าที่ ความรับผิดชอบ ทั้งนี้ ในกรณีที่บุคลากรหลักในแต่ละบทบาทไม่สามารถ ปฏิบัติหน้าที่ได้ให้บุคลากรสำรองรับผิดชอบ ปฏิบัติหน้าที่แทน

11.การสำรองข้อมูลและกู้คืนข้อมูลสารสนเทศ

เนื่องจากระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศส่วนใหญ่ ถูกติดตั้งและจัดเก็บบนระบบประมวลผลกลาง ณ ห้องเซิร์ฟเวอร์ ซึ่งเป็นการอำนวยความสะดวก แก่ผู้ใช้งาน (User) เป็นอย่างมาก แต่ก็มีความเสี่ยงสูงมากเช่นกัน ซึ่งเป็นผู้ดูแลรับผิดชอบหลัก จึงได้จัดทำแนว ปฏิบัติการสำรอง ข้อมูลและกู้คืนข้อมูลสารสนเทศ เพื่อให้ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูล สารสนเทศอยู่ในสภาพพร้อมใช้งานสามารถให้บริการได้อย่างต่อเนื่อง และสามารถกู้คืนกลับมาใช้งานได้โดยเร็วหากเกิดปัญหา

11.1 ผู้รับผิดชอบ

รายละเอียดบุคลากรและหน้าที่ความรับผิดชอบ ตามข้อ 9

11.2 แนวปฏิบัติในการดูแลระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนอุปกรณ์ประมวลผลข้อมูล (Process Device) ได้มอบหมายให้ผู้ดูแลระบบ (System Administrator) ดูแล ระบบคอมพิวเตอร์และระบบสารสนเทศ รวมถึงข้อมูลสารสนเทศ ตลอดจนให้ตรวจสอบอุปกรณ์ประมวลผลข้อมูล (Process Device) ณ ห้องเซิร์ฟเวอร์
อย่างสม่ำเสมออย่างน้อยสัปดาห์ละ 1 ครั้ง หากพบข้อผิดพลาดให้รายงานหัวหน้างานเทคโนโลยีสารสนเทศทราบโดยทันที

11.3 แนวปฏิบัติในการสำรองข้อมูลสารสนเทศ กำหนดดังนี้

11.3.1 ผู้ดูแลระบบ (System Administrator) ต้องดำเนินการสำรองข้อมูลสารสนเทศไว้ใน ฮาร์ดดิสต์ (External Hardisk Drive) หรืออุปกรณ์สำรองอื่นใด ตามขั้นตอนของโปรแกรมสำรองข้อมูล

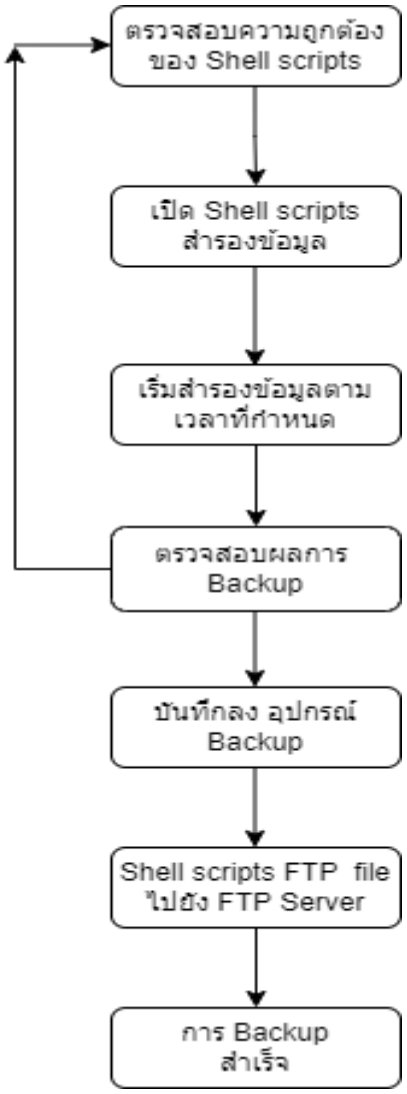
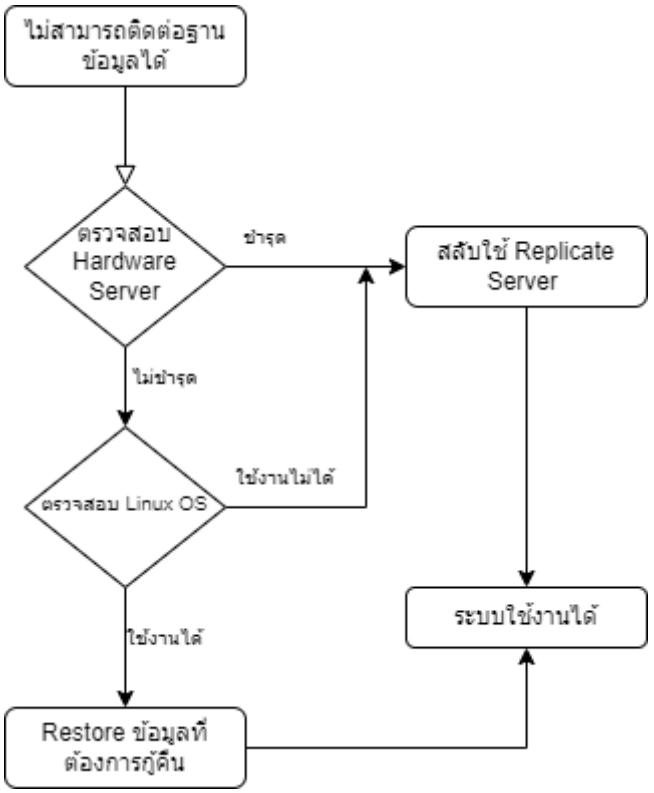
11.3.2 ผู้ดูแลระบบ (System Administrator) ต้องพิมพ์รายละเอียดไว้บน ฮาร์ดดิสต์ (External Hardisk Drive) หรืออุปกรณ์สำรองอื่นใดที่ใช้สำหรับการสำรองข้อมูล ได้แก่ รูปแบบการสำรองข้อมูลแบบ รายวันหรือรายสัปดาห์ หรือรายเดือน วันและเวลา และผู้รับผิดชอบพร้อมทั้งตรวจสอบความถูกต้องสมบูรณ์ของการ สำรองข้อมูล

11.3.3 รายละเอียดการสำรองข้อมูล กำหนดดังนี้

ลำดับ	รายการ
1.	เครื่องคอมพิวเตอร์แม่ข่าย Master Server HOSxP -ใช้ External Hardisk สำรองข้อมูล Mysql โดยแยกเป็น ตารางที่เก็บข้อมูลผู้รับบริการ และข้อมูลภาพทางการแพทย์ กำหนดให้ External เก็บข้อมูลย้อนหลัง แบบ Rotate ได้ 7 วัน และข้อมูลที่สำรองไว้แต่ละวันจะส่งไปเก็บที่ FTP Server ที่ตั้งอยู่คนละตึก เพื่อความปลอดภัย หากเกิดอัคคีภัย (สำรองข้อมูลอัตโนมัติ โดยใช้ Script ตามเวลาที่กำหนด และมีการตรวจสอบความครบถ้วน)
2.	เครื่องคอมพิวเตอร์แม่ข่าย Slave Server HOSxP เป็น Replicate Mysql สามารถปรับใช้งานได้ทันที เมื่อ Master Server เกิดปัญหา ไม่สามารถใช้งานได้

11.4 แนวปฏิบัติการกู้คืนระบบ

หากระบบคอมพิวเตอร์และระบบสารสนเทศหลักเกิดปัญหาไม่สามารถใช้งานได้ ให้ผู้ดูแลระบบ (System Administrator) ปรับเปลี่ยนให้ใช้ Replicate Server แทน Master Server ทันที ถ้าหากเกิดกรณีชำรุดทั้ง 2 เครื่อง ผู้ดูแลระบบจะนำฮาร์ดดิสต์ (External Hardisk Drive) หรืออุปกรณ์สำรองอื่นใด เพื่อนำข้อมูลสารสนเทศกลับมาใช้งาน ดำเนินการกู้คืน

การสำรองข้อมูล	การกู้คืนข้อมูล
	

11.6 โรงพยาบาลแก่งหางแมว ต้องดำเนินการทดสอบสภาพความพร้อมใช้งานของระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศและระบบสำรอง ตามระดับความเสี่ยงที่ยอมรับได้ อย่างน้อยปีละ 1 ครั้ง ดังนี้

11.6.1 พิจารณาคัดเลือกระบบคอมพิวเตอร์และระบบสารสนเทศที่สำคัญเพื่อดำเนินการ พร้อมทั้งเตรียมความพร้อมก่อนการทดสอบ เพื่อมิให้เกิดความเสี่ยงและความเสียหายแก่ทางราชการ

11.6.2 จัดทำรายงานเสนอผู้อำนวยการโรงพยาบาลก่อนดำเนินการทดสอบ

11.6.3 ดำเนินการทดสอบระบบคอมพิวเตอร์และระบบสารสนเทศตามที่กำหนดไว้

11.6.4 รายงานผลการทดสอบเสนอผู้อำนวยการโรงพยาบาล

(ลงชื่อ).....ผู้เสนอ

(นายวรพรต พัฒนะพันธ์)

นักวิชาการคอมพิวเตอร์

(ลงชื่อ).....ผู้เห็นชอบ

(นายศุภมิตร เตชะอำไพ)

หัวหน้างานกลุ่มงานสุขภาพดิจิทัล

(ลงชื่อ).....ผู้อนุมัติ

(นพ.อภิสิทธิ์ ดุจวรรณ์)

ผู้อำนวยการโรงพยาบาลแก่งหางแมว