โรงพยาบาลปราสาท จังหวัดสุรินทร์	สำนักการแพทย์ กระทรวงสาธารณสุข โรงพยาบาลปราสาท	นโยบายคุณภาพ (Quality Manual : QM) รหัส **QM-IMT-001-01**

เรื่อง : แผนการดำเนินงานกรณีระบบสารสนเทศล่ม โรงพยาบาลปราสาท (Business continuity Plan : BCP)

ชื่อหน่วยงาน : กลุ่มงานเทคโนโลยีสารสนเทศ	ฉบับแรก (จำนวน 78 หน้ารวมปก) **วันที่อนุมัติใช้** 26 ก.พ. 2569

คณะผู้จัดทำ	ตำแหน่ง	ลายมือชื่อ
1. นายเกียรติธนพัฒน์ มนตรี	นักวิชาการคอมพิวเตอร์ชำนาญการ	.....
2. นายคมน์ ชุ่มสูงเนิน	นักเทคโนโลยีสารสนเทศปฏิบัติการ	.....
3. นายปิยะ แจ่มใส	นักวิชาการคอมพิวเตอร์	.....
4. น.ส.วรรณธวัชก์ ธนกรเจริญศักดิ์	เจ้าพนักงานธุรการ	.....
5. นายสิทธิชัย จุฬา	เจ้าพนักงานเครื่องคอมพิวเตอร์	.....

ผู้ตรวจสอบ ..... (นายกิตติภพ แจ่มโสภณ) หัวหน้ากลุ่มภารกิจสุขภาพดิจิทัล	**ผู้อนุมัติ** ..... (นางสาวชูหงส์ มหรรทัศนพงศ์) ผู้อำนวยการโรงพยาบาลปราสาท

การควบคุมระบบเอกสารคุณภาพ

ประวัติการแก้ไข :

ครั้งที่	วันที่อนุมัติใช้	รายละเอียดการแก้ไข	เลขหน้า
00		ฉบับแรก	1-78

แผนการดำเนินงานกรณีระบบสารสนเทศล่ม
โรงพยาบาลปราสาท (Business Continuity Plan : BCP)

จัดทำโดย

กลุ่มงานเทคโนโลยีสารสนเทศ
กลุ่มภารกิจสุขภาพดิจิทัล โรงพยาบาลปราสาท

คำนำ

ด้วย โรงพยาบาลปราสาท ได้นำเทคโนโลยีสารสนเทศมาใช้ในการบริการจัดการภายในองค์กร และสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งาน และความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่าง ๆ จะมีจำนวนเพิ่มมากขึ้น

ดังนั้น องค์กรจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บ และการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัยและมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวมาใช้ จึงได้จัดทำแผนบริหารความต่อเนื่อง "Business Continuity Plan : BCP" ในการนำไปใช้งานได้อย่างต่อเนื่อง โดยคาดหวังว่าแผนบริหารความต่อเนื่องเล่มนี้ จะเป็นแนวทางในการบริหารความต่อเนื่องของการปฏิบัติงานในสภาวะวิกฤต และสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ

กลุ่มงานเทคโนโลยีสารสนเทศ

สารบัญ

แผนการดำเนินการกรณีระบบสารสนเทศล่ม (กรณีระบบทั่วไป) โรงพยาบาลปราสาท

(Business Continuity Plan : BCP)

แผนบริหารงานความต่อเนื่อง Business Continuity Plan : BCP จัดทำขึ้น เพื่อให้หน่วยงานภายในโรงพยาบาลปราสาท สามารถนำไปใช้ในการตอบสนองและปฏิบัติงานในสภาวะวิกฤติ หรือเหตุการณ์ฉุกเฉินต่าง ๆ ทั้งที่เกิดจากภัยธรรมชาติ อุบัติเหตุ หรือการมุ่งร้ายต่อองค์กร โดยไม่ให้การดำเนินงานต้องหยุดลง หรือไม่สามารถให้บริการได้อย่างต่อเนื่อง การที่หน่วยงานไม่มีกระบวนการรองรับให้การดำเนินงานเป็นไปอย่างต่อเนื่อง อาจส่งผลกระทบต่อหน่วยงานในด้านต่าง ๆ เช่น ด้านการให้บริการทางระบบงานคอมพิวเตอร์และระบบเครือข่าย ด้านการพัฒนาระบบสารสนเทศ ด้านการเข้าช่วยเหลือเพื่อซ่อมบำรุงอุปกรณ์ระบบคอมพิวเตอร์ ด้านการให้บริการระบบอินเทอร์เน็ต ดังนั้นการจัดทำแผนบริหารความต่อเนื่องจึงเป็นสิ่งสำคัญที่จะช่วยให้หน่วยงานสามารถรับมือกับเหตุการณ์ฉุกเฉินที่ไม่คาดคิด และทำให้กระบวนการสำคัญสามารถกลับมาดำเนินการได้อย่างปกติ ซึ่งจะช่วยให้สามารถลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นได้

กรอบแนวทางการดำเนินการเตรียมความพร้อมต่อสภาวะวิกฤต ๔ ขั้นตอน คือ

๑. การสร้างความรู้ความเข้าใจให้กับบุคลากรภายในโรงพยาบาลปราสาท

๒. การเตรียมความพร้อมของระบบเทคโนโลยีสารสนเทศ ในการจัดทำแผนรองรับการดำเนินภารกิจการให้บริการด้านเทคโนโลยีสารสนเทศ ตามบทบาทหน้าที่ได้อย่างต่อเนื่อง (Business Continuity Plan: BCP)

๓. การซักซ้อมแผนและนำไปปฏิบัติได้จริง

๔. การจัดการหลังเกิดภัย

โดยแนวคิดการบริหารความต่อเนื่องของกลุ่มงานเทคโนโลยีสารสนเทศ คือ การควบคุมดูแลและป้องกันทรัพยากรที่สำคัญต่อการดำเนินงานหรือการให้บริการ เพื่อสร้างประโยชน์สูงสุดสำหรับผู้รับบริการ

๑. วัตถุประสงค์

๑.๑ เพื่อใช้เป็นแนวทางในการบริหารความต่อเนื่อง

๑.๒ เพื่อให้กลุ่มงานเทคโนโลยีสารสนเทศ มีการเตรียมความพร้อมในการรับมือกับสภาวะวิกฤต ตามแผนที่ได้กำหนดไว้

๑.๓ เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินงานหรือการให้บริการ

๑.๔ เพื่อบรรเทาความเสียหายให้อยู่ในระดับที่ยอมรับได้

๒. นิยามระดับเหตุการณ์

๒.๑ ระบบสารสนเทศการให้บริการผู้ป่วยไม่สามารถใช้งานได้ (กรณีระบบล่มทั่วไป) แบ่งเป็น ๓ รหัสปฏิบัติการ ได้แก่

๒.๑.๑ รหัส **"IT ปาป้า ๑"** หมายถึง ระบบสารสนเทศหลักขัดข้องขั่วคราวสามารถแก้ไขได้ (กรณีระบบล่มทั่วไป) ภายใน ๔๕ นาที ให้ User ทุกระดับหยุดการบันทึกข้อมูลเข้าระบบ และรอประกาศต่อไป

๒.๑.๒ รหัส **"IT ปาป้า ๒"** หมายถึง ระบบสารสนเทศหลักขัดข้องไม่สามารถแก้ไขได้ (กรณีระบบล่มทั่วไป) ภายใน ๔๕ นาที ให้ทุกหน่วยงานดำเนินการตามแนวทางปฏิบัติสำหรับหน่วยงาน ในกรณีระบบสารสนเทศการให้บริการผู้ป่วยไม่สามารถใช้งานได้

๒.๑.๓ รหัส **"IT ปาป้า ๓"** หมายถึง ยกเลิกรหัสปฏิบัติการ **"IT ปาป้า ๑"** และ **"IT ปาป้า ๒"** ระบบสามารถใช้งานได้ปกติ

กรณีสามารถแก้ไขปัญหาได้ภายใน ๔๕ นาที (กรณีระบบล่มทั่วไป) รายงานสถานการณ์ต่อผู้บังคับบัญชาตามลำดับทราบ ถึงการประเมินความรุนแรงในเบื้องต้นและแนวทางการแก้ไขปัญหา ดังนี้

๑) แจ้งผู้ใช้งานให้ทราบ โดยประชาสัมพันธ์ประกาศเสียงตามสายและโทรแจ้งแต่ละหน่วยงาน กรณีปัญหาเกิดจากระบบสารสนเทศโรงพยาบาล ให้แจ้งว่า "ขณะนี้ ระบบสารสนเทศโรงพยาบาลขัดข้องใช้งานไม่ได้ (ทั้งโรงพยาบาล/บางจุด/บริเวณ.....) เจ้าหน้าที่กำลังดำเนินการแก้ไข ใช้เวลาในการดำเนินการแก้ไขประมาณ ๔๕ นาที" (ตัวอย่าง)

๒) ประเมินสถานการณ์เป็นระยะ

๓) หน่วยงานต่าง ๆ ยังสามารถปฏิบัติงานให้บริการผู้ป่วยได้ตามปกติ โดยจะรอใช้งานระบบสารสนเทศโรงพยาบาลเมื่อใช้งานได้ หรือใช้ระบบ Manual ก็ได้ ขึ้นอยู่กับบริบทของแต่ละหน่วยงาน (กรณี Manual หากมีค่าใช้จ่ายใดเกิดขึ้น ต้องนำข้อมูลการให้บริการบันทึกข้อมูลในเครื่องคอมพิวเตอร์ย้อนหลัง)

๒.๒ ระบบสารสนเทศการให้บริการผู้ป่วยไม่สามารถใช้งานได้ (กรณี Ransomware) แบ่งเป็น ๒ รหัสปฏิบัติการ ได้แก่

๒.๒.๑ รหัส **"IT เจ็บจี๊ด ๒"** หมายถึง เมื่อกลุ่มงานเทคโนโลยีสารสนเทศตรวจพบเหตุการณ์ผิดปกติที่สงสัยว่า Server หลักถูกโจมตีด้วย Ransomware เช่น ไฟล์บน Server ถูกเข้ารหัส (Encrypt), พบข้อความเรียกค่าไถ่ (Ransom Note), ฐานข้อมูลไม่สามารถเข้าถึงได้, ระบบ HIS/HOSxP หยุดทำงานทั้งระบบ หรือได้รับแจ้งจากหน่วยงานต่างๆ ให้ดำเนินการดังนี้

ก) Isolate Server ที่ถูกโจมตีออกจากเครือข่ายทันที โดยการถอดสาย Network แต่ห้ามปิดเครื่อง Server โดยเด็ดขาด (เพื่อรักษาหลักฐาน Memory Dump สำหรับ Digital Forensics)

ข) ตัดการเชื่อมต่อ Internet ขาออก (Outbound Traffic) ทั้งหมดของโรงพยาบาลทันที เพื่อป้องกัน Ransomware แพร่กระจายไปยังระบบอื่นและป้องกันการส่งข้อมูลออก (Data Exfiltration)

ค) ตรวจสอบ Backup Server/NAS ทันที ว่ายังปลอดภัยหรือไม่ หากยังไม่ถูกกระทบให้ Isolate ออกจากเครือข่ายทันทีเพื่อป้องกัน

ง) บันทึกหลักฐานเบื้องต้น ได้แก่ ภาพถ่ายหน้าจอ (Screenshot) ข้อความเรียกค่าไถ่ ชื่อ-นามสกุลไฟล์ที่ถูกเข้ารหัส วันเวลาที่พบ และ Server/ระบบที่ได้รับผลกระทบ

จ) ประเมินขอบเขตความเสียหาย ว่า Server ใดบ้างที่ถูกกระทบ (Database Server, Application Server, File Server, Domain Controller เป็นต้น)

ฉ) แจ้ง CISO ทันที เพื่อประกาศใช้รหัส **"IT เจ็บจี๊ด ๒"** ทันที โดยไม่ต้องรอประเมินระยะเวลา เนื่องจากการกู้คืน Server หลักต้องใช้เวลาหลายชั่วโมงถึงหลายวัน

ข้อห้ามสำคัญ: ห้ามจ่ายค่าไถ่ (Ransom) โดยเด็ดขาด ไม่ว่าในกรณีใด ๆ ห้ามติดต่อหรือจ่ายเงินค่าไถ่ให้กับผู้โจมตีและให้บันทึกข้อความเรียกค่าไถ่ไว้เป็นหลักฐานเท่านั้น

๒.๒.๒ รหัส **"IT เจ็บจี๊ด ๓"** หมายถึง ยกเลิกรหัสปฏิบัติการ **"IT เจ็บจี๊ด ๒"** เมื่อระบบสามารถใช้งานได้ปกติ

เนื่องจากกรณีถูกโจมตีด้วย Ransomware การแก้ไขปัญหาไม่สามารถแก้ไขได้ภายใน ๖๐ นาที จำเป็นต้องดำเนินการตอบสนองเหตุการณ์ตามช่วงเวลาดังนี้

๑) แจ้งผู้ใช้งานให้ทราบ โดยประชาสัมพันธ์ประกาศเสียงตามสายและโทรแจ้งแต่ละหน่วยงาน กรณีปัญหาเกิดจากระบบสารสนเทศโรงพยาบาล ให้แจ้งว่า "ขณะนี้ ระบบสารสนเทศโรงพยาบาลขัดข้องใช้งานไม่ได้ (ทั้งโรงพยาบาล/บางจุด/บริเวณ.....) เจ้าหน้าที่กำลังดำเนินการแก้ไขตั้งแต่เวลานี้เป็นต้นไป ให้ทุกหน่วยงานดำเนินการตามแนวทางปฏิบัติสำหรับหน่วยงาน ในกรณีระบบสารสนเทศการให้บริการผู้ป่วยไม่สามารถใช้งานได้

๒) ประเมินสถานการณ์เป็นระยะ

๓) หน่วยงานต่าง ๆ ยังสามารถปฏิบัติงานให้บริการผู้ป่วยได้ตามปกติ โดยจะรอใช้งานระบบสารสนเทศโรงพยาบาลเมื่อใช้งานได้ หรือใช้ระบบ Manual ก็ได้ ขึ้นอยู่กับบริบทของแต่ละหน่วยงาน (กรณี Manual หากมีค่าใช้จ่ายใดเกิดขึ้น ต้องนำข้อมูลการให้บริการบันทึกข้อมูลในเครื่องคอมพิวเตอร์ย้อนหลัง)

Time Line แผน BCP กรณี Ransomware โจมตี Server หลัก

ระยะที่ ๑: การตอบสนองฉุกเฉิน (๐-๖๐ นาที)

ช่วงเวลา	ผู้รับผิดชอบ	การดำเนินการ	หมายเหตุ
0 - 15 นาที	ทีม IT/Security	๑. แยกเครื่อง Server ที่ติดเชื้อออกจากเครือข่ายทันที (ถอดสาย Network) ๒. ตัด Internet ขาออกทั้งหมด (Block Outbound Traffic at Firewall) ๓. แยกอุปกรณ์ Backup Server/NAS ออกจากเครือข่ายเพื่อปกป้องข้อมูลสำรอง ๔. บันทึก Screenshot, Log, Ransom Note เป็นหลักฐาน ๕. ประเมินว่า Server ใดบ้างที่ถูกกระทบ	- ห้ามปิดเครื่อง Server ที่ติดเชื้อเพื่อรักษา Memory Dump - ห้ามใช้ Server ที่ติดเชื้อทำอะไรเพิ่มเติม
15 - 30 นาที	CISO / หัวหน้ากลุ่มงาน IT	๑. ประกาศ "IT เจ็บจี๊ด ๒" ทันที ๒. ประเมินขอบเขตความเสียหายเบื้องต้น รูปแบบ: - Database Server (MariaDB/MySQL)	ตรวจสอบ Backup ทุกชุด: - Full Backup ล่าสุด - Incremental/ Differential - Offsite Backup (ถ้ามี)

ช่วงเวลา	ผู้รับผิดชอบ	การดำเนินการ	หมายเหตุ
		- Application Server (HOSxP) - File Server / Shared Drive - Domain Controller/Active Directory - PACS Server / LIS Server ๓. ระบุประเภท Ransomware (ถ้าทำได้) ๔. ตรวจสอบความสมบูรณ์ของ Backup (Backup Integrity Check) ๕. รายงานสถานการณ์ต่อ CIO (ผอ.รพ.)	หาก Backup ถูกกระทบให้รายงานทันที
๓๐ - ๔๕ นาที		๑. ถ่ายทอดคำสั่งการ สั่งเปิด War Room ๒. แจ้งหน่วยงานภายนอก: - สกมช. ตาม พ.ร.บ.ไซเบอร์ พ.ศ. ๒๕๖๒ - ThaiCERT - สสจ.สุรินทร์ ๓. ประสานงานขอความช่วยเหลือจากผู้เชี่ยวชาญ (Incident Response Team) หากจำเป็น	แจ้งเหตุตามกฎหมาย พ.ร.บ.ไซเบอร์ พ.ศ. ๒๕๖๒
๔๕ - ๖๐ นาที	CISO / ทีมบริหารจัดการเหตุการณ์	๑. ประชุมทีมฉุกเฉิน (War Room) วางแผนกู้คืน ๒. ทุกหน่วยงานเริ่มปฏิบัติงานด้วยระบบ Manual เต็มรูปแบบ ๓. ฝ่ายประชาสัมพันธ์สื่อสารภายใน/ภายนอก ตาม Template ๔. ทีม IT เริ่มวางแผน Server Rebuild & Recovery ๕.ประเมิน Recovery Time Objective (RTO): - HIS (HOSxP): RTO ไม่เกิน ๔ ชั่วโมง - LIS: RTO ไม่เกิน ๘ ชั่วโมง - PACS: RTO ไม่เกิน ๒๔ ชั่วโมง	- ทุกหน่วยงานใช้แบบฟอร์มกรณี server ล่ม - กำหนด RTO/RPO ให้ชัดเจน เพื่อจัดลำดับการกู้คืน

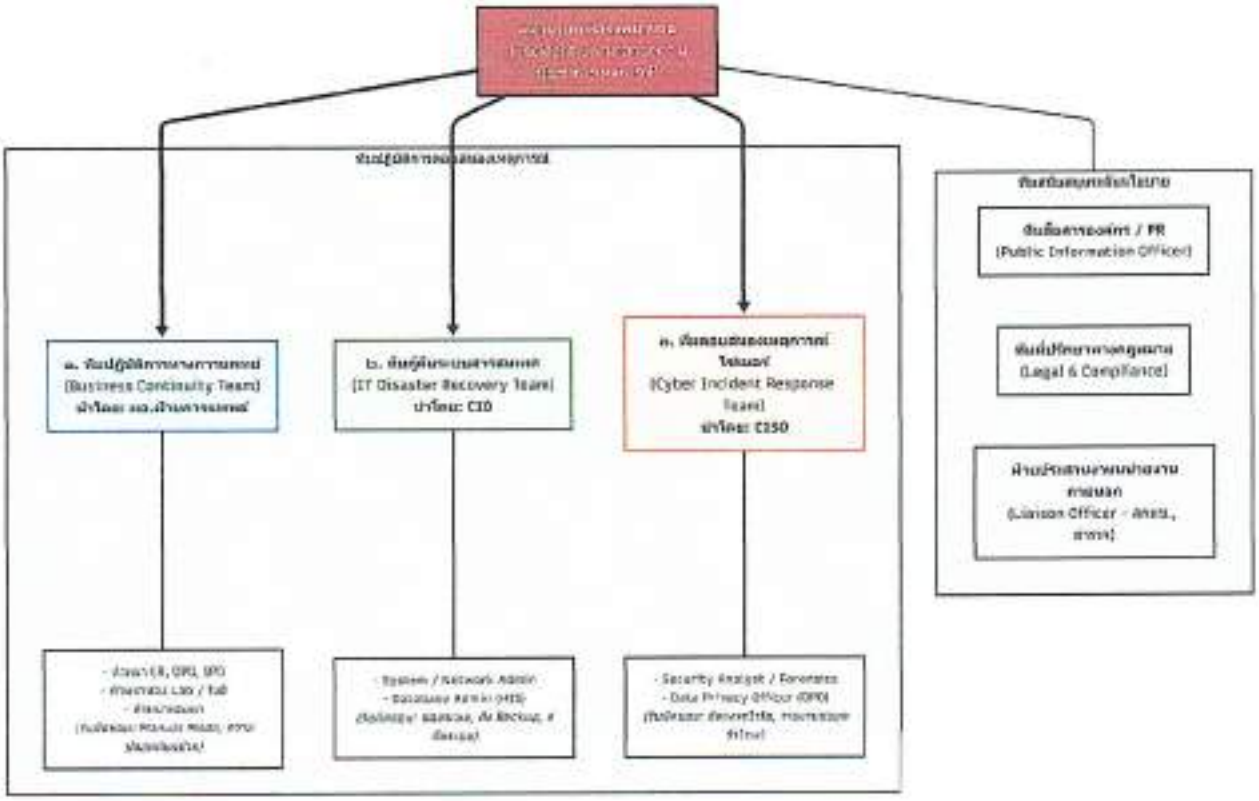
ระยะที่ ๒: การวิเคราะห์ ควบคุม และเตรียมกู้คืน (๑ - ๒๔ ชั่วโมง)

ช่วงเวลา	ผู้รับผิดชอบ	การดำเนินการ	หมายเหตุ
๑ - ๔ ชั่วโมง	ทีม IT/Security	**การวิเคราะห์ (Analysis)** ๑. วิเคราะห์ Ransomware Variant	- ใช้เครื่องมือ Antivirus/EDR ในการ

ช่วงเวลา	ผู้รับผิดชอบ	การดำเนินการ	หมายเหตุ
		(ชนิด/สายพันธุ์) ๒. ระบุ Attack Vector (ช่องทางโจมตี เช่น Phishing, RDP, VPN, Zero-Day) ๓. ตรวจหา Indicator of Compromise (IOC) ทั้งระบบ ๔. ประเมินว่ามีการขโมยข้อมูลออก (Data Exfiltration) หรือไม่ ๕. Scan เครื่อง Client/Workstation ทุกเครื่องเพื่อหาการติดเชื้อ	Scan - ตรวจสอบ Decryption Tool ที่ nomoreransom.org
๔ - ๑๒ ชั่วโมง	ทีม IT / CISO	**การควบคุม (Containment)** ๑. Containment เต็มรูปแบบ (ปิดกั้น การแพร่กระจายของ) ๒. ตรวจสอบ Active Directory, DNS, DHCP-Reset หากถูก Compromise ๓. ตรวจสอบ Firewall Rules ปิด Port ที่ไม่จำเป็น ๔. รายงานความคืบหน้าต่อ CIO ทุก ๒ ชั่วโมง	
๑๒ - ๒๔ ชั่วโมง	ทีม IT / DBA	**การเตรียมกู้คืน (Preparation for Recovery)** ๑. ตรวจสอบ Backup Integrity — ยืนยันว่า Backup สะอาดไม่ติดเชื้อ ๒. เตรียม Clean Hardware/VM สำหรับติดตั้ง Server ใหม่ ๓. เตรียมสิ่งที่ต้องใช้ในการ Rebuild Server - OS Installation Media (CentOS/Windows Server) - MariaDB/MySQL Installation Package - Configuration Files / Backup ของ Config - HOSxP Installation Package + License - Network Configuration (IP,	ห้าม Restore ลง Environment ที่ยังไม่ได้ทำ Clean

ช่วงเวลา	ผู้รับผิดชอบ	การดำเนินการ	หมายเหตุ
		Gateway, DNS) ๔. จัดลำดับการกู้คืน: Database Server → HIS → LIS → PACS → อื่น ๆ	

๓. โครงสร้างการบังคับบัญชาแผนบริหารงานต่อเนื่องระบบสารสนเทศ



สำเนาคู่ฉบับ

คำสั่งโรงพยาบาลศรีราชา
ที่ ๒๐๙/ ๒๕๖๖
เรื่อง แต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)
ประจำโรงพยาบาลศรีราชา

ตามพระราชกฤษฎีกาว่าด้วยการบริหารและการจัดการระบบดิจิทัลภาครัฐ พ.ศ. ๒๕๖๖ กำหนดให้หน่วยงานของรัฐ ต้องแต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) เพื่อทำหน้าที่บริหารจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารภายในหน่วยงานของรัฐ ให้เป็นไปอย่างมีประสิทธิภาพ สอดคล้องกับนโยบายและยุทธศาสตร์ที่เกี่ยวข้อง โรงพยาบาลศรีราชา จึงแต่งตั้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ดังต่อไปนี้

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)
นายสาธุพงษ์ มหรรฆพันธุ์ ตำแหน่ง ผู้อำนวยการโรงพยาบาลศรีราชา

อำนาจหน้าที่

๑. **วางแผนและกำหนดยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ**
- จัดทำแผนยุทธศาสตร์เทคโนโลยีสารสนเทศของโรงพยาบาลให้สอดคล้องกับพันธกิจและเป้าหมายขององค์กร
- บูรณาการแผน IT เข้ากับการพัฒนาระบบบริการสุขภาพทั้งในและเครือข่ายสหวิชาชีพ

๒. **กำกับดูแลและบริหารระบบเทคโนโลยีสารสนเทศ**
- ดูแลโครงสร้างพื้นฐานด้าน IT (Hardware, Software, Network, Security, Cloud, ฯลฯ)
- จัดการและประเมินประสิทธิภาพของระบบสารสนเทศที่ใช้งานในโรงพยาบาล เช่น HOSxP, PACS, LIS, Telemedicine ฯลฯ
- ตรวจสอบความพร้อมของระบบสารสนเทศให้สามารถให้บริการได้อย่างต่อเนื่องและปลอดภัย

๓. **ส่งเสริมนวัตกรรมและการพัฒนาดิจิทัล**
- สนับสนุนการนำนวัตกรรมเทคโนโลยีใหม่ ๆ เช่น AI, IoT, Big Data, Health Information Exchange (HIE) มาใช้
- พัฒนาการบริการพัฒนา Smart Hospital Platform และ Digital Health Solution ให้เกิดผลในทางปฏิบัติ

๔. **บริหารความเสี่ยงและความมั่นคงปลอดภัยไซเบอร์**
- ร่วมกำหนดนโยบายความมั่นคงปลอดภัยของข้อมูล (Cybersecurity Policy)
- ให้คำปรึกษาด้านมาตรฐานและข้อกำหนดของระบบบริการหรือข้อมูลผู้ป่วย
- ประสานกับ CISO และทีม IT ในการดำเนินการตอบสนองเหตุการณ์ฉุกเฉินด้าน IT

๕. **ส่งเสริมการเรียนรู้และพัฒนาศักยภาพดิจิทัล**
- วางแผนการฝึกอบรมพัฒนาศักยภาพบุคลากรในด้านเทคโนโลยีและการใช้ระบบสารสนเทศ
- สนับสนุนวัฒนธรรมการใช้เทคโนโลยีอย่างมีประสิทธิภาพทั่วทั้งองค์กร

๖. บูรณาการ...

๖. **บูรณาการและประสานงานกับหน่วยงานที่เกี่ยวข้อง**
เป็นศูนย์กลางในการประสานงานกับหน่วยงานภายนอก เช่น สำนักงานปลัดกระทรวง, สำนักงานสุขภาพฯ, กรมการแพทย์ ฯลฯ
ทำงานร่วมกับ CISO, CDO, DPO, CAIO และผู้บริหารท่านอื่น ๆ ในการพัฒนาองค์กรดิจิทัล

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๖ สิงหาคม พ.ศ.๒๕๖๖

นายสาธุพงษ์ มหรรฆพันธุ์
ผู้อำนวยการโรงพยาบาลศรีราชา

สำเนาคู่ฉบับ

คำสั่งโรงพยาบาล[illegible]

ที่ ๒๕๕ /๒๕๖๔

เรื่อง แต่งตั้งผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (Chief Information Security Officer : CISO) ประจำโรงพยาบาล[illegible]

[illegible] (CISO)

เพื่อให้การขับเคลื่อนนโยบาย[illegible] โดยมีหน้าที่และอำนาจ ดังนี้

๑. ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง

[illegible]

หน้าที่และอำนาจ

๑. [illegible]

๒. [illegible]

๓. [illegible]

๔. [illegible] (Cyber Security) [illegible] (Data Privacy) [illegible]

๕. [illegible] (Cyber Security) [illegible] (Data Privacy) [illegible]

๖. ปฏิบัติงานอื่นตามที่ได้รับมอบหมาย

๒. คณะทำงานบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ประจำโรงพยาบาล[illegible]

องค์ประกอบ

๑.	[illegible]	[illegible]	ประธาน
๒.	[illegible]	[illegible]	คณะทำงานและผู้ปฏิบัติ
๓.	[illegible]	[illegible]	คณะทำงานและผู้ปฏิบัติ
๔.	[illegible]	[illegible]	คณะทำงานและผู้ปฏิบัติ
๕.	[illegible]	[illegible]	คณะทำงานและผู้ปฏิบัติ
๖.	[illegible]	[illegible]	คณะทำงานและผู้ปฏิบัติ[illegible]
๗.	[illegible]	[illegible]	คณะทำงานและผู้ปฏิบัติ[illegible]
๘.	[illegible]	[illegible]	คณะทำงานและผู้ปฏิบัติ[illegible]
๙.	[illegible]	[illegible]	คณะทำงานและผู้ปฏิบัติ[illegible]
๑๐.	[illegible]	[illegible]	คณะทำงานและเลขานุการ
๑๑.	[illegible]	[illegible]	คณะทำงานและเลขานุการ

หน้าที่และอำนาจ

๑. [illegible] (Cyber Security)

๒. [illegible] (Cyber Security) [illegible]

๓. [illegible] (Cyber Security) [illegible]

๔. [illegible] (Cyber Security) [illegible]

๕. ปฏิบัติงานอื่นตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๖ [illegible]

(นาย[illegible])

ผู้อำนวยการโรงพยาบาล[illegible]

[illegible]

คำสั่งโรงพยาบาลบางสลาก
ที่ ๒๓๘ /๒๕๖๘
เรื่อง แต่งตั้งผู้บริหารข้อมูลระดับสูง (Chief Data Officer: CDO)
ประจำโรงพยาบาลบางสลาก

เพื่อให้การดำเนินงานของโรงพยาบาลบางสลาก เป็นไปอย่างมีประสิทธิภาพ และเป็นไปตามนโยบายของกระทรวงและกฎหมายที่เกี่ยวข้อง จึงแต่งตั้ง

นายวโรดม สวสุริยเทว์ ตำแหน่งนายแพทย์ชำนาญการ

ให้ดำรงตำแหน่ง ผู้บริหารข้อมูลระดับสูง (Chief Data Officer: CDO) ประจำโรงพยาบาลบางสลาก

อำนาจและหน้าที่ ดังนี้

๑. จัดทำนโยบาย มาตรฐาน และแนวปฏิบัติในการกำกับดูแลข้อมูลทั่วทั้งองค์กร เพื่อให้การจัดการข้อมูลมีคุณภาพและสอดคล้องกับเป้าหมายของโรงพยาบาล

๒. กำหนดและควบคุมมาตรฐานคุณภาพของข้อมูลให้มีความถูกต้อง (Accuracy) สมบูรณ์ (Completeness) และเป็นปัจจุบัน (Timeliness) เพื่อให้สามารถนำไปใช้บริหารจัดการและตัดสินใจได้อย่างมีประสิทธิผล

๓. กำกับดูแลการออกแบบโครงสร้างการจัดเก็บ การประมวลผล และการบูรณาการข้อมูลของโรงพยาบาล ให้มีประสิทธิภาพและเหมาะสมกับข้อมูลที่รวบรวมและแลกเปลี่ยน

๔. ผลักดันและส่งเสริมให้บุคลากรในโรงพยาบาลมีความรู้ความเข้าใจ (Data Literacy) และสามารถนำข้อมูลไปใช้ในการพัฒนากระบวนการทำงานและคุณภาพการให้บริการผู้ป่วย

๕. กำหนดนโยบายและระบบการจัดการข้อมูลตั้งแต่การสร้าง การจัดเก็บ การใช้งาน การเก็บรักษา ไปจนถึงการทำลายข้อมูลอย่างเหมาะสมและปลอดภัย

๖. ทำงานร่วมกับฝ่ายเทคโนโลยีสารสนเทศและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อกำหนดนโยบายและมาตรการในการป้องกันและรักษาความปลอดภัยของข้อมูลทั้งหมดของโรงพยาบาล

๗. เป็นผู้นำในการวิเคราะห์และสังเคราะห์ข้อมูลเพื่อสร้างองค์ความรู้ใหม่ ที่สามารถนำไปสนับสนุนการวางแผนกลยุทธ์ พัฒนานวัตกรรมทางการแพทย์ และปรับปรุงประสิทธิภาพการทำงานของโรงพยาบาล

๘. ปฏิบัติงานอื่น ๆ ที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๘ สิงหาคม พ.ศ.๒๕๖๘

(นางสาวสุพรรษ มหาชัยคุณค่า)
ผู้อำนวยการโรงพยาบาลบางสลาก

รับ
พิมพ์
ตรวจ

สำเนาคู่ฉบับ

คำสั่งโรงพยาบาลบางสาย
ที่ ๒๒๘ /๒๕๖๔
เรื่อง แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)
ประจำโรงพยาบาลบางสาย

ด้วย โรงพยาบาลบางสาย เป็นหน่วยงานที่มีการดำเนินกิจการที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งนี้ตามมาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO : Data Protection Officer) อาศัยอำนาจตามความใน มาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ จึงแต่งตั้ง ดังนี้

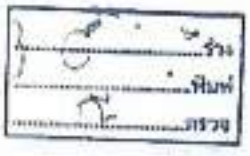
นายหมน์ ชุ่มสูงเป็น ตำแหน่งนักเทคโนโลยีสารสนเทศปฏิบัติการ

เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO : Data Protection Officer) ประจำโรงพยาบาลบางสาย โดยให้มีอำนาจหน้าที่ตามมาตรา ๔๒ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๒๐ สิงหาคม พ.ศ.๒๕๖๔

(นางสาวบุหงา มหรรฆัศนงค์)
ผู้อำนวยการโรงพยาบาลบางสาย



สำเนาคู่ฉบับ

คำสั่งโรงพยาบาลนพรัตนราชธานี

ที่ ๒๕๒ /๒๕๖๔

เรื่อง แต่งตั้งเจ้าหน้าที่ผู้ประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
(CIRT : Cybersecurity Incident Response Team) ประจำโรงพยาบาลนพรัตนราชธานี

ด้วยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้ประกาศกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจ หรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๗ ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านเวชภัณฑ์และเครื่องมือแพทย์ บริการตรวจหรือวิเคราะห์ทางการแพทย์และชีววิทยา และบริการข้อมูลสุขภาพดิจิทัล ต้องดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยให้อยู่ภายใต้การควบคุมหรือกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุข

เพื่อให้การดูแลและให้บริการระบบงานดิจิทัล เป็นไปตามกำหนดหลักเกณฑ์ที่กำหนด จึงขอแต่งตั้งผู้มีรายนามดังต่อไปนี้ เป็นผู้ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (CIRT : Cyber Incident response Team) โรงพยาบาลนพรัตนราชธานี

นายเกียรติยศพัฒน์ มนตรี ตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการ

โทรศัพท์สำนักงาน [illegible] มือถือ [illegible] อีเมล์ [illegible]

บทบาทและหน้าที่

๑. เฝ้าระวังตรวจสอบช่องโหว่ของระบบเครือข่าย และเครื่องคอมพิวเตอร์ทั้งฮาร์ดแวร์และซอฟต์แวร์
๒. ประสานงานกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health sectoral CERT) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ทันทีเมื่อพบเหตุการณ์ทางไซเบอร์
๓. ติดตามการแจ้งข่าวสารเหตุการณ์จากเว็บ [illegible] และ Official Account : @health-cert

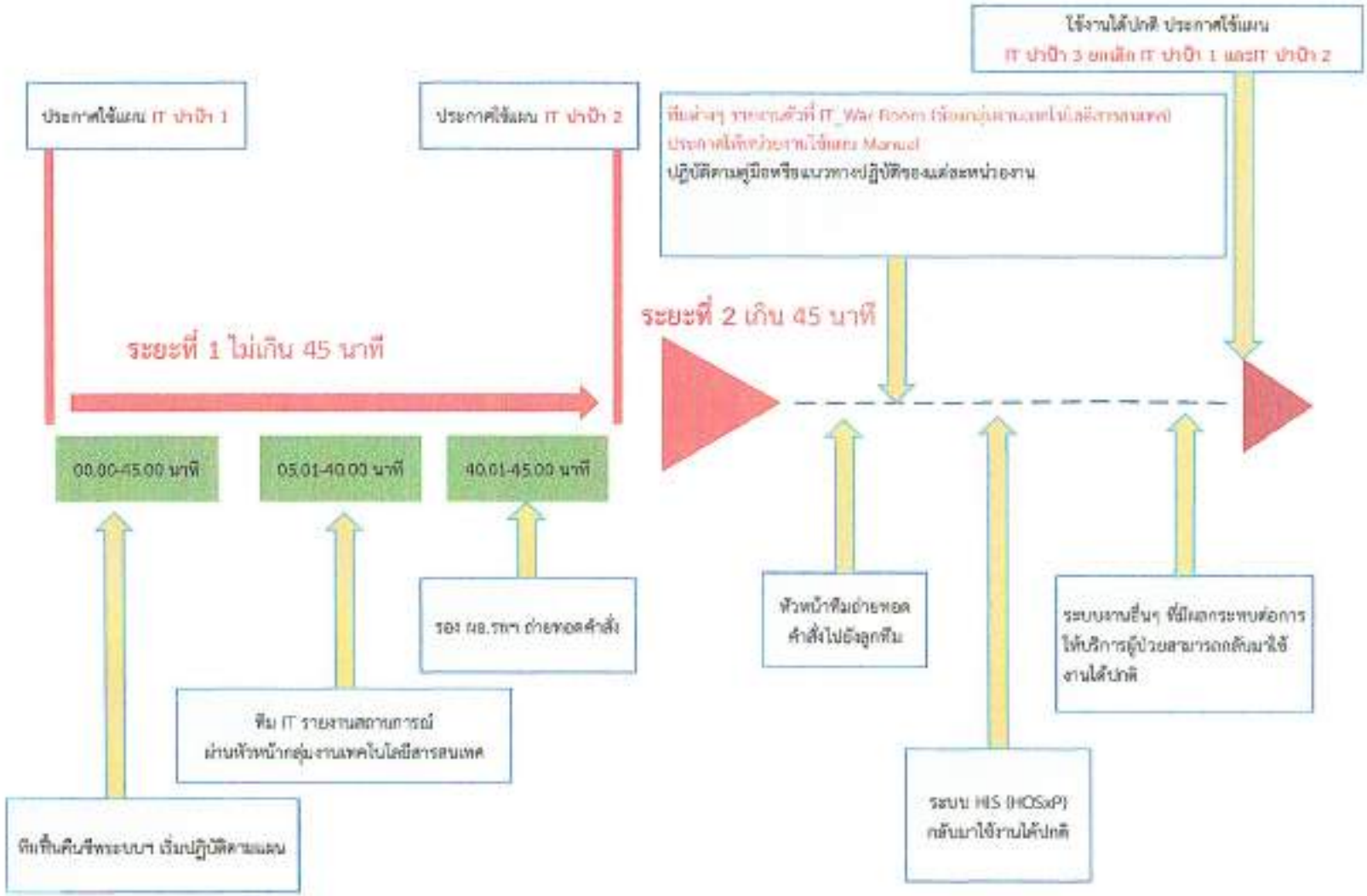
ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป และขอยกเลิกคำสั่งใดที่ขัดหรือแย้งกับคำสั่งนี้ ให้ใช้คำสั่งนี้แทน

สั่ง ณ วันที่ ๒๗ สิงหาคม พ.ศ. ๒๕๖๔

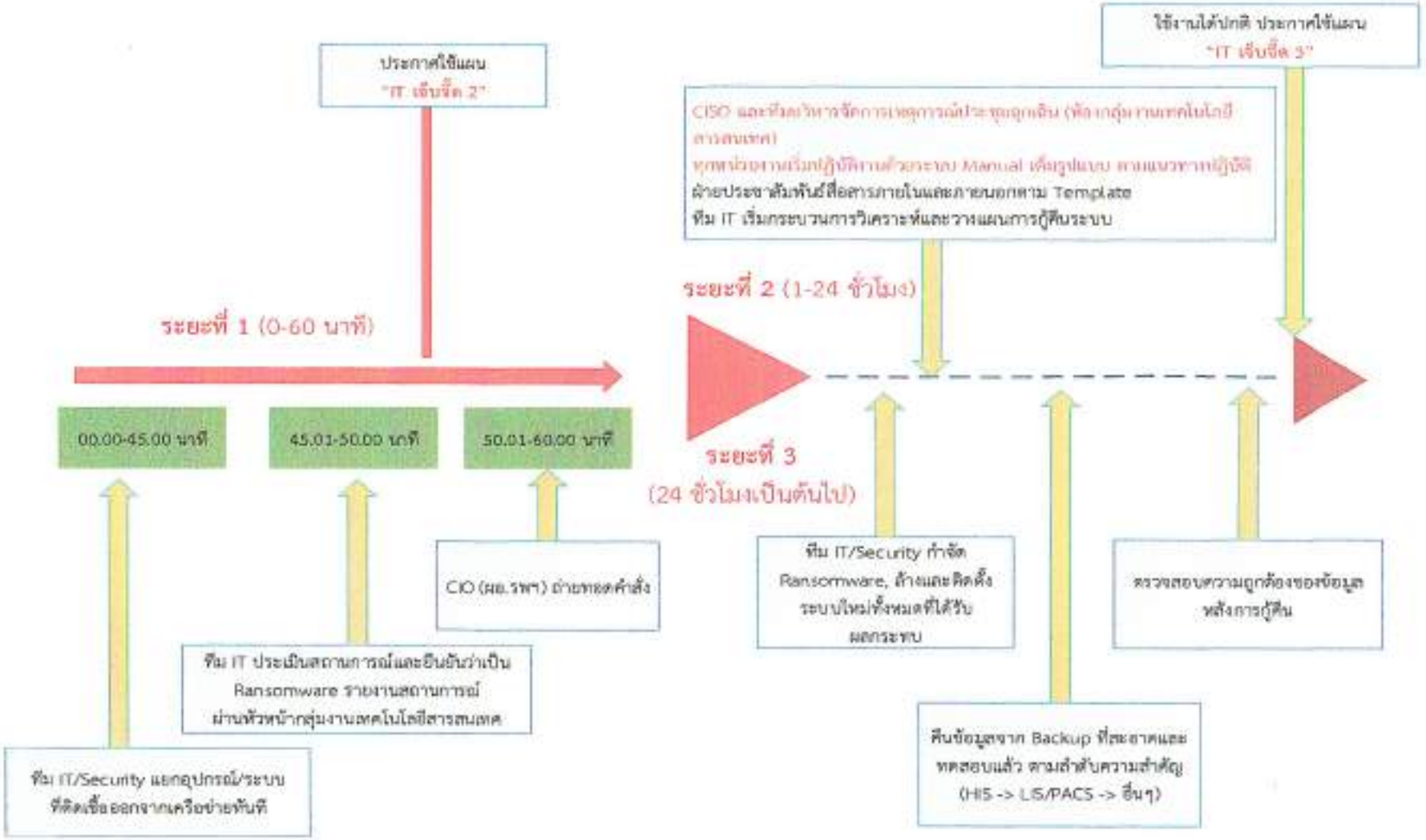
(นางสาว[illegible])
ผู้อำนวยการโรงพยาบาลนพรัตนราชธานี

ร่าง
พิมพ์

๙. Time line ประกาศใช้แผน BCP "IT ปาป๋า" (กรณีระบบล่มทั่วไป)



๕. Time line ประกาศใช้แผน BCP "IT เจ็บจี๊ด" (กรณี Ransomware)



๖. จุดแจ้งเหตุ

๖.๑ เจ้าหน้าที่ประจำหน่วยงานที่เกิดเหตุ แจ้งเจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ (help desk) ติดต่อโทรศัพท์ภายใน ๑๒๖๙ และเบอร์โทรศัพท์เคลื่อนที่ ดังนี้

๑.๑ นายเกียรติธนพัฒน์ มนตรี	๐๘๓ – ๑๒๔๕ ๙๙๐
๑.๒ นายคมน์ ชุ่มสูงเนิน	๐๘๔ – ๙๓๐๙ ๒๒๔
๑.๓ นายสิทธิชัย จุฬา	๐๙๘ – ๖๓๑๙ ๙๔๓
๑.๔ นายปิยะ แจ่มใส	๐๘๕ – ๗๗๔๖ ๐๐๔
๑.๕ นางสาววรรณธวัชก์ ธนกรเจริญศักดิ์	๐๙๓ – ๐๙๖๒ ๙๙๘

๖.๒ เจ้าหน้าที่ศูนย์คอมพิวเตอร์วิเคราะห์เหตุการณ์เบื้องต้นพร้อมประเมินระยะเวลาในการแก้ไข รายงานหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ หรือผู้อำนวยการด้านสารสนเทศ (chief information officer ; CIO) รับทราบและรายงานสถานการณ์เบื้องต้น

๖.๓ กลุ่มงานงานเทคโนโลยีสารสนเทศ ประกาศใช้แผนปฏิบัติการฉุกเฉินกรณีระบบสารสนเทศล่ม ดำเนินการตามแผนกู้คืนระบบ

๖.๔ กลุ่มงานเทคโนโลยีสารสนเทศแจ้ง/สื่อสารและประชาสัมพันธ์ ประกาศแจ้งให้ผู้มาใช้บริการและเจ้าหน้าที่รับทราบความปัญหาและการดำเนินการแก้ไขของระบบสารสนเทศล่ม อาจได้รับความล่าช้าหรือได้รับความสะดวกน้อยลงขออภัยมา ณ ที่นี้ รวมทั้งประชาสัมพันธ์ให้เจ้าหน้าที่ดำเนินการตามแผนปฏิบัติการของหน่วยงาน

๖.๕ ภายหลังการสิ้นสุดแผนปฏิบัติการฉุกเฉินกรณีระบบสารสนเทศล่ม ให้แต่ละจุดบริการดำเนินการลงบันทึกข้อมูลย้อนลงเข้าสู่ระบบตามแผน กลุ่มงานเทคโนโลยีสารสนเทศร่วมประเมินความเสียหายและสรุปเพื่อรายงานต่อผู้บริหาร

๗.ขั้นตอนประกาศแผน BCP

(กรณีระบบล่มทั่วไป)

๑. เมื่อระบบสารสนเทศเกิดขัดข้องทางกลุ่มงานเทคโนโลยีสารสนเทศพบเอง หรือได้รับแจ้งจากหน่วยงานต่าง ๆ (User) ที่ใช้งาน ให้เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศเร่งตรวจสอบสาเหตุอย่างเร่งด่วน

๒. เมื่อพบสาเหตุแล้ว ให้วิเคราะห์ว่าเกิดจากสาเหตุอะไร และประเมินระยะเวลาที่จะต้องดำเนินการแก้ไขระบบ จากนั้นให้แจ้งหัวหน้ากลุ่มภารกิจสุขภาพดิจิทัล (CISO) เพื่อประกาศแผนรหัสปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ล่ม

a. หากพบว่าปัญหาหรือสาเหตุนั้นต้องใช้ระยะเวลาภายใน ๔๕ นาที ให้ประกาศใช้ **รหัส "IT ปาป้า ๑"** โดยกลุ่มงานเทคโนโลยีสารสนเทศแจ้งงานประชาสัมพันธ์ ให้ออกประกาศประชาสัมพันธ์ทางเสียงตามสายให้ประชาชนรับทราบ ให้แจ้งว่า "ขณะนี้ ระบบสารสนเทศโรงพยาบาลขัดข้อง ใช้งานไม่ได้ (ทั้งโรงพยาบาล/บางจุด/บริเวณ.....) เจ้าหน้าที่กำลังดำเนินการแก้ไข ใช้เวลาในการดำเนินการแก้ไขประมาณ ๔๕ นาที" (ตัวอย่าง)

b. หากพบว่าปัญหาหรือสาเหตุนั้น ต้องใช้ระยะมากกว่า ๔๕ นาที ให้ประกาศใช้ **รหัส "IT ปาป้า ๒"** โดยกลุ่มงานเทคโนโลยีสารสนเทศแจ้งงานงานประชาสัมพันธ์ ให้ออกประกาศประชาสัมพันธ์ทาง

เสียงตามสายให้ประชาชนรับทราบ ให้แจ้งว่า "ขณะนี้ ระบบสารสนเทศโรงพยาบาลขัดข้อง ใช้งานไม่ได้ (ทั้งโรงพยาบาล/บางจุด/บริเวณ.....) เจ้าหน้าที่กำลังดำเนินการแก้ไข ใช้เวลาในการดำเนินการแก้ไขประมาณ .... นาที" (ตัวอย่าง)

๓. หลังจากที่ประกาศ **รหัส "IT ปาป้า ๒"** เจ้าหน้าที่ศูนย์คอมพิวเตอร์แก้ไขปัญหา และระบบสามารถใช้งานได้ตามปกติแล้ว ให้ประกาศใช้ **รหัส "IT ปาป้า ๓"** (เข้าสู่ภาวะปกติ) โดยกลุ่มงานเทคโนโลยีสารสนเทศแจ้งงานประชาสัมพันธ์ ให้ออกประกาศประชาสัมพันธ์ทางเสียงตามสายให้ประชาชนรับทราบ ให้แจ้งว่า "ขณะนี้ ระบบสารสนเทศโรงพยาบาลใช้งานได้ปกติแล้ว เข้าสู่ภาวะการทำงานปกติ"

๔. ให้ทุกหน่วยงานหลังจากประกาศ **รหัส "IT ปาป้า ๓"** ปฏิบัติตามแนวทางของแต่ละหน่วยงาน พร้อมบันทึกข้อมูลการให้บริการผู้ป่วยในส่วนที่เกี่ยวข้องย้อนหลังในระหว่างระบบสารสนเทศล่มไม่สามารถใช้งานได้ให้ครบถ้วนในของการให้บริการภายใน ๒๔ ชั่วโมง

(กรณี Ransomware)

๑. เมื่อระบบสารสนเทศเกิดขัดข้องหรือตรวจพบเหตุการณ์ผิดปกติที่สงสัยว่า Server หลักถูกโจมตีด้วย Ransomware เช่น ไฟล์บน Server ถูกเข้ารหัส (Encrypt), พบข้อความเรียกค่าไถ่ (Ransom Note), ฐานข้อมูลไม่สามารถเข้าถึงได้, ระบบ HIS/HOSxP หยุดทำงานทั้งระบบ หรือได้รับแจ้งจากหน่วยงานต่างๆ (User) ที่ใช้งาน ให้เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศเร่งตรวจสอบสาเหตุอย่างเร่งด่วน

๒. เมื่อพบสาเหตุแล้วให้วิเคราะห์ว่าเกิดจากสาเหตุอะไร และประเมินระยะเวลาที่จะต้องดำเนินการแก้ไขระบบ จากนั้นให้แจ้งหัวหน้ากลุ่มภารกิจสุขภาพดิจิทัล (CISO) เพื่อประกาศแผนรหัสปฏิบัติการระบบสารสนเทศล่ม

เนื่องจากกรณีถูกโจมตีด้วย Ransomware ไม่สามารถแก้ไขได้ภายใน ๖๐ นาที จำเป็นต้องดำเนินการตอบสนองเหตุการณ์ ให้ประกาศใช้ **รหัส "IT เจ็บจี๊ด ๒"** โดยกลุ่มงานเทคโนโลยีสารสนเทศแจ้งงานงานประชาสัมพันธ์ ให้ออกประกาศประชาสัมพันธ์ทางเสียงตามสายให้ประชาชนรับทราบ ให้แจ้งว่า "ขณะนี้ ระบบสารสนเทศโรงพยาบาลขัดข้อง ใช้งานไม่ได้ (ทั้งโรงพยาบาล/บางจุด/บริเวณ.....) เจ้าหน้าที่กำลังดำเนินการแก้ไข ใช้เวลาในการดำเนินการแก้ไข ประมาณ .... นาที" (ตัวอย่าง)

๓. หลังจากที่ประกาศ **รหัส "IT เจ็บจี๊ด ๒"** เจ้าหน้าที่ศูนย์คอมพิวเตอร์แก้ไขปัญหา และระบบสามารถใช้งานได้ตามปกติแล้ว ให้ประกาศใช้ **รหัส "IT เจ็บจี๊ด ๓"** (เข้าสู่ภาวะปกติ) "โดยกลุ่มงานเทคโนโลยีสารสนเทศแจ้งงานประชาสัมพันธ์ ให้ออกประกาศประชาสัมพันธ์ทางเสียงตามสายให้ประชาชนรับทราบ ให้แจ้งว่า "ขณะนี้ ระบบสารสนเทศโรงพยาบาลใช้งานได้ปกติแล้ว เข้าสู่ภาวะการทำงานปกติ"

๔. ให้ทุกหน่วยงานหลังจากประกาศ **รหัส "IT เจ็บจี๊ด ๓"** ปฏิบัติตามแนวทางของแต่ละหน่วยงาน พร้อมบันทึกข้อมูลการให้บริการผู้ป่วยในส่วนที่เกี่ยวข้องย้อนหลังในระหว่างระบบสารสนเทศล่มไม่สามารถใช้งานได้ให้ครบถ้วนในของการให้บริการภายใน ๒๔ ชั่วโมง

๔. แนวทางปฏิบัติสำหรับหน่วยงาน กรณีระบบสารสนเทศล่ม

โรงพยาบาลปราสาท จังหวัดสุรินทร์		ระเบียบปฏิบัติ (System Procedure:SP) เลขที่ SP-IMT-๐๐๑
เรื่อง: แนวทางดำเนินการกรณีเครือข่าย HOSxP ล่ม		
จัดทำโดย: คณะกรรมการสารสนเทศ		ฉบับแรก (จำนวน ๑๑ หน้า รวมปก) ประกาศใช้เมื่อ: ๑๒ กุมภาพันธ์ ๒๕๖๒

หน่วยงานนำไปใช้:

๑) องค์กรแพทย์, องค์กรพยาบาล
๒) ER
๓) งานผู้ป่วยนอกทั้งหมด
๔) งานผู้ป่วยในทั้งหมด
๕) หอผู้ป่วยหนัก
๖) หอผู้ป่วยพิเศษ ชั้น ๕, ชั้น ๖
๗) ห้องคลอด
๘) ห้องผ่าตัด
๙) งานผู้ป่วยนอก
๑๐) งานทันตกรรม
๑๑) งานกายภาพบำบัด
๑๒) กลุ่มงานเภสัชกรรม
๑๓) กลุ่มงานตรวจรักษาทางห้องปฏิบัติการ

วัตถุประสงค์ : - เพื่อให้ระบบเครือข่ายสามารถใช้งานได้ตลอด ๒๔ ชม.
- เพื่อเป็นแนวทางปฏิบัติให้หน่วยงานต่าง ๆ กรณีใช้ระบบ HOSxP ไม่ได้
- หากเกิดปัญหาระบบล่มเจ้าหน้าที่สามารถปฏิบัติการกู้ระบบได้ทันที
- เพื่อเตรียมความพร้อมใช้งานต่อเนื่องในภาวะฉุกเฉิน

ขอบข่าย : สำหรับให้เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศและเจ้าหน้าที่ในหน่วยงานต่างๆ ในโรงพยาบาลปราสาท ใช้เป็นแนวทางในการดำเนินการกรณีระบบสารสนเทศโรงพยาบาลขัดข้องใช้งานไม่ได้ ครอบคลุม ๒ สถานการณ์ ได้แก่

๑) กรณีระบบสารสนเทศขัดข้องทั่วไป (ระบบ HOSxP หรือระบบเครือข่ายใช้งานไม่ได้)
๒) กรณีถูกโจมตีด้วย Ransomware ที่เครื่อง Server หลัก (ต้องหยุดระบบ ล้าง ติดตั้ง และกู้คืน)

ดำเนินการ : กรณีใช้ระบบ HOSxP ไม่ได้

อุปกรณ์/เครื่องมือ :

ลำดับ	อุปกรณ์/เครื่องมือ	รายละเอียด
๑	เครื่อง Server (Production)	เครื่องแม่ข่ายหลัก สำหรับให้บริการระบบ HIS (HOSxP), ฐานข้อมูล MariaDB/MySQL และระบบสารสนเทศอื่น ๆ ของโรงพยาบาล
๒	เครื่อง Server Slave / DR Server	เครื่องแม่ข่ายสำรองข้อมูล (Replication) สำหรับสำรองฐานข้อมูลแบบ Real-time และใช้เป็นระบบสำรองในกรณีเครื่องหลักใช้งานไม่ได้
๓	Backup Server / NAS	เครื่อง/อุปกรณ์จัดเก็บข้อมูลสำรอง (Backup) ทั้งแบบ Full Backup และ Incremental Backup สำหรับกู้คืนข้อมูลในกรณีฉุกเฉิน
๔	Core Switch / Distribution Switch	อุปกรณ์กระจายสัญญาณเครือข่ายหลัก (Core) และอุปกรณ์กระจายสัญญาณระดับอาคาร/ชั้น (Distribution) สำหรับเชื่อมต่อระบบเครือข่ายทั้งโรงพยาบาล
๕	Access Switch / Switch HUB	อุปกรณ์กระจายสัญญาณระดับจุดบริการ สำหรับเชื่อมต่อเครื่องคอมพิวเตอร์ลูกข่ายในแต่ละหน่วยงาน
๖	Firewall / Router	อุปกรณ์รักษาความปลอดภัยเครือข่าย ควบคุมการเข้า-ออกข้อมูล ป้องกันการโจมตีจากภายนอก และจัดการ VPN
๗	UPS (Uninterruptible Power Supply)	อุปกรณ์สำรองไฟฟ้า สำหรับจ่ายไฟให้ Server และอุปกรณ์เครือข่ายหลักในกรณีไฟฟ้าดับ
๘	สาย UTP CAT ๕e/๖, สาย Fiber Optic	สายเชื่อมต่อสัญญาณเครือข่าย ทั้งแบบทองแดง (UTP) สำหรับเชื่อมต่อภายในอาคาร และแบบใยแก้วนำแสง (Fiber) สำหรับเชื่อมต่อระหว่างอาคาร
๙	Hard Disk / SSD	อุปกรณ์จัดเก็บข้อมูลสำรอง สำหรับเปลี่ยนทดแทนกรณี Disk เสีย หรือใช้ในการกู้คืนระบบ
๑๐	OS Installation Media	สื่อบันทึกสำหรับติดตั้งระบบปฏิบัติการใหม่ (CentOS/Windows Server) ใช้ในกรณี Clean Install หลังถูก Ransomware โจมตี
๑๑	HOSxP Installation Package	ชุดติดตั้งโปรแกรม HOSxP พร้อม License Key สำหรับติดตั้งระบบใหม่กรณีต้อง Rebuild Server
๑๒	Antivirus / EDR Software	ซอฟต์แวร์ป้องกันไวรัสและตรวจจับภัยคุกคาม (Endpoint Detection and Response) สำหรับ Scan และกำจัด Malware/Ransomware

ความรับผิดชอบ :

ตำแหน่ง/บทบาท	ความรับผิดชอบ
CIO (ผอ.รพ.)	ผู้สั่งการสูงสุด อนุมัติการประกาศรหัส IT ปาป้า/ IT เจ็บจี๊ด (กรณียกระดับ), สั่งเปิด War Room, อนุมัติแจ้งหน่วยงานภายนอก
CISO (หัวหน้ากลุ่มภารกิจสุขภาพดิจิทัล)	ประเมินสถานการณ์, ประกาศรหัส IT ปาป้า/ IT เจ็บจี๊ด, สั่งการทีม IT, ประสานงานกับหน่วยงานภายนอก (สกมช., Thai CERT), เป็นประธาน AAR
นักวิชาการคอมพิวเตอร์	วิเคราะห์ปัญหา, ดำเนินการแก้ไข/กู้คืนระบบ, Rebuild Server, Restore Database, ดูแลระบบเครือข่าย, จัดทำ Incident Report
เจ้าพนักงานเครื่องคอมพิวเตอร์	สนับสนุนการแก้ไขปัญหา, ดูแลเครื่องลูกข่าย (Client), เปลี่ยนอุปกรณ์, ตรวจสอบสายเครือข่าย, ช่วยเหลือผู้ใช้งาน
งานประชาสัมพันธ์	ออกประกาศทางเสียงตามสายแจ้งเจ้าหน้าที่และประชาชน ตามรหัส "IT ปาป้า/ IT เจ็บจี๊ด" ที่ได้รับแจ้งจากกลุ่มงาน IT
หัวหน้าหน่วยงาน (ทุกหน่วยงาน)	- ถ่ายทอดคำสั่งให้เจ้าหน้าที่ในหน่วยงาน - กำกับดูแลการปฏิบัติงานตามแผน Manual - ตรวจสอบการบันทึกข้อมูลย้อนหลังให้ครบถ้วน
เจ้าหน้าที่ผู้ใช้งาน (User)	- ปฏิบัติตามแนวทาง Manual ของหน่วยงาน - บันทึกข้อมูลการให้บริการผู้ป่วยย้อนหลังภายใน ๒๔ ชั่วโมง - แจ้งทีม IT เมื่อพบความผิดปกติ

คำจำกัดความ :

ลำดับ	คำศัพท์	คำจำกัดความ
๑	เครื่อง Server (Production)	เครื่องแม่ข่ายหลักที่ติดตั้งระบบ HIS (HOSxP) และฐานข้อมูล MariaDB สำหรับให้บริการระบบสารสนเทศของโรงพยาบาล
๒	เครื่อง Server Slave / DR Server	เครื่องแม่ข่ายสำรองที่ทำ Database Replication แบบ Real-time จากเครื่อง Server หลัก ใช้เป็นระบบสำรองและกู้คืนข้อมูล
๓	Backup Server / NAS	เครื่อง/อุปกรณ์สำหรับจัดเก็บข้อมูลสำรอง (Backup) ทั้งแบบ Full, Incremental และ Differential เพื่อใช้กู้คืนข้อมูลในกรณีฉุกเฉิน
๔	Core Switch	อุปกรณ์กระจายสัญญาณเครือข่ายหลักของโรงพยาบาล เชื่อมต่อระบบเครือข่ายทุกอาคาร
๕	Access Switch / Switch HUB	อุปกรณ์กระจายสัญญาณเครือข่ายระดับจุดบริการ สำหรับเชื่อมต่อเครื่องลูกข่ายในแต่ละหน่วยงาน
๖	Firewall	อุปกรณ์รักษาความปลอดภัยเครือข่าย ทำหน้าที่ตรวจสอบและ

ลำดับ	คำศัพท์	คำจำกัดความ
		ควบคุม Traffic ที่เข้า-ออกระบบเครือข่ายโรงพยาบาล
๗	UPS	Uninterruptible Power Supply — อุปกรณ์สำรองไฟฟ้าสำหรับจ่ายไฟให้ Server และอุปกรณ์เครือข่ายหลักเมื่อไฟฟ้าดับ
๘	สาย UTP CAT ๕e/๖	สายเชื่อมต่อสัญญาณเครือข่ายแบบทองแดง (Unshielded Twisted Pair) สำหรับเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับ Switch
๙	สาย Fiber Optic	สายเชื่อมต่อสัญญาณเครือข่ายแบบใยแก้วนำแสง สำหรับเชื่อมต่อระหว่างอาคาร ให้ความเร็วสูงและระยะทางไกล
๑๐	Hard Disk / SSD	อุปกรณ์จัดเก็บข้อมูลภายในเครื่อง Server หรือเครื่องลูกข่าย
๑๑	HIS (Hospital Information System)	ระบบสารสนเทศโรงพยาบาล หมายถึงระบบ HOSxP ที่ใช้ในการบริหารจัดการข้อมูลผู้ป่วยและบริการทั้งหมดของโรงพยาบาล
๑๒	Ransomware	มัลแวร์เรียกค่าไถ่ - โปรแกรมอันตรายที่เข้ารหัส (Encrypt) ไฟล์ข้อมูลในเครื่องคอมพิวเตอร์หรือ Server ทำให้ไม่สามารถเข้าถึงข้อมูลได้ แล้วเรียกร้องให้จ่ายเงินเพื่อแลกกับรหัสถอดรหัส (Decryption Key)
๑๓	Isolate (แยกออกจากเครือข่าย)	การตัดการเชื่อมต่อเครื่องที่ต้องสงสัยว่าติดเชื้อออกจากระบบเครือข่าย โดยถอดสาย LAN หรือปิด Wi-Fi เพื่อป้องกันการแพร่กระจายของ Malware
๑๔	Clean Install	การล้างข้อมูลทั้งหมดในเครื่องแล้วติดตั้งระบบปฏิบัติการใหม่ตั้งแต่ต้นจาก Original Installation Media เพื่อให้มั่นใจว่าไม่มี Malware หลงเหลือ
๑๕	RTO (Recovery Time Objective)	ระยะเวลาเป้าหมายสูงสุดที่ยอมรับได้ในการกู้คืนระบบให้กลับมาใช้งานได้ นับจากเวลาที่ระบบหยุดทำงาน
๑๖	RPO (Recovery Point Objective)	ปริมาณข้อมูลสูงสุดที่ยอมรับได้ที่จะสูญหาย วัดเป็นระยะเวลาย้อนหลังจากจุดที่เกิดเหตุ เช่น RPO ๑ ชั่วโมง หมายถึงยอมรับข้อมูลหายได้ไม่เกิน ๑ ชั่วโมง
๑๗	Digital Forensics	กระบวนการเก็บรวบรวม วิเคราะห์ และรักษาหลักฐานทางดิจิทัลสำหรับการสืบสวนสอบสวนหาสาเหตุและผู้กระทำผิดทางไซเบอร์
๑๘	IT ปาป้า	รหัสปฏิบัติการตอบสนองเหตุการณ์ระบบสารสนเทศขัดข้อง แบ่งเป็น ๓ ระดับ: "IT ปาป้า ๑" (แก้ไขได้ภายใน ๔๕ นาที), "IT ปาป้า ๒" (ใช้เวลามากกว่า ๔๕ นาที ทุกหน่วยงานเข้าสู่แผน Manual), "IT ปาป้า ๓" (ระบบกลับสู่ภาวะปกติ)

ลำดับ	คำศัพท์	คำจำกัดความ
๑๙	IT เจ็บจี๊ด	รหัสปฏิบัติการตอบสนองเหตุการณ์ระบบสารสนเทศขัดข้อง แบ่งเป็น ๒ ระดับ: "IT เจ็บจี๊ด ๒" (ใช้เวลามากกว่า ๖๐ นาที ทุกหน่วยงานเข้าสู่แผน Manual), "IT เจ็บจี๊ด ๓" (ระบบกลับสู่ภาวะปกติ)

เอกสารอ้างอิง : แผนกู้คืนระบบ HOSxP และระบบเครือข่ายบริการ (กรณีรุนแรงเกินการควบคุม)

รายละเอียด : ความพร้อมใช้งานต่อเนื่องในภาวะฉุกเฉิน : ปัญหาระบบล่มซึ่งมีสาเหตุดังนี้

ลำดับ	กลุ่มสาเหตุ	ตัวอย่างปัญหา	ผลกระทบ
๑	อุปกรณ์เครือข่ายขัดข้อง / ระบบเครือข่ายขัดข้อง	- Core Switch / Access Switch เสีย - สาย Fiber Optic / UTP ขาด - DHCP Server หยุดทำงาน - Firewall / Router ขัดข้อง	เครื่องลูกข่ายไม่สามารถเชื่อมต่อ Server ได้ ทำให้ใช้ระบบ HOSxP ไม่ได้บางส่วนหรือทั้งหมด
๒	เครื่องคอมพิวเตอร์แม่ข่ายขัดข้อง (Server)	- Server OS Crash / Hang - Hardware Failure (Disk, RAM, PSU)	ระบบ HIS ทั้งหมดหยุดให้บริการ ทุกจุดบริการใช้งานไม่ได้
๓	ระบบฐานข้อมูลขัดข้อง	- MariaDB/MySQL Service หยุดทำงาน - Max Connections เต็ม - Table Corruption / Index เสียหาย - Disk Space เต็ม - Slow Query ผิดปกติ	ไม่สามารถอ่าน/เขียนข้อมูลได้ ระบบ HOSxP ทำงานผิดปกติหรือหยุดทำงาน
๔	ปัจจัยภายนอก	- ไฟฟ้าขัดข้อง / ไฟดับ - UPS เสีย / แบตเตอรี่หมด - แอร์ห้อง Server เสีย (อุณหภูมิสูง) - ภัยธรรมชาติ (น้ำท่วม, พายุ)	ระบบอาจหยุดให้บริการ หากไม่มีระบบสำรอง หรือ UPS ไม่เพียงพอ
๕	การโจมตีทางไซเบอร์ (Cyber Attack)	- Ransomware โจมตี Server หลัก (ระดับวิกฤต) - Ransomware โจมตีเครื่อง Client - Malware / Virus ติดเชื้อในระบบ - Phishing Attack ที่นำไปสู่การเข้าถึงระบบโดยไม่ได้รับอนุญาต - การโจมตี DDoS ทำให้ระบบเครือข่ายล่ม	ร้ายแรง - อาจทำให้ข้อมูลถูกเข้ารหัส สูญหาย หรือรั่วไหล ระบบหยุดให้บริการ ต้องล้างและติดตั้งใหม่ทั้งหมด ใช้เวลากู้คืน ๓-๗ วัน

๙.กำหนดผู้รับผิดชอบ

เมื่อเกิดเหตุการณ์ระบบสารสนเทศขัดข้อง กำหนดผู้รับผิดชอบตามบทบาทหน้าที่และช่วงเวลา ดังต่อไปนี้

๙.๑ ในเวลาราชการ

๙.๑.๑ เจ้าหน้าที่แก้ไขปัญหาระบบคอมพิวเตอร์ (Server)

- นายเกียรติธนพัฒน์ มนตรี ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
- นายคมน์ ชุ่มสูงเนิน ตำแหน่ง นักเทคโนโลยีสารสนเทศปฏิบัติการ

๙.๑.๒ เจ้าหน้าที่แก้ไขปัญหาเครื่องคอมพิวเตอร์และระบบเครือข่าย

- นายเกียรติธนพัฒน์ มนตรี ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
- นายคมน์ ชุ่มสูงเนิน ตำแหน่ง นักเทคโนโลยีสารสนเทศปฏิบัติการ
- นายปิยะ แจ่มใส ตำแหน่ง นักวิชาการคอมพิวเตอร์
- นายสิทธิชัย จุฬา ตำแหน่ง เจ้าพนักงานเครื่องคอมพิวเตอร์

๙.๑.๓ เจ้าหน้าที่แก้ไขปัญหาระบบคอมพิวเตอร์และฐานข้อมูล

<u>ด้าน HARDWARE</u>

- นายเกียรติธนพัฒน์ มนตรี ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
- นายคมน์ ชุ่มสูงเนิน ตำแหน่ง นักเทคโนโลยีสารสนเทศปฏิบัติการ
- นายปิยะ แจ่มใส ตำแหน่ง นักวิชาการคอมพิวเตอร์

<u>ด้าน SOFTWARE</u>

- นายเกียรติธนพัฒน์ มนตรี ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
- นายคมน์ ชุ่มสูงเนิน ตำแหน่ง นักเทคโนโลยีสารสนเทศปฏิบัติการ
- นายปิยะ แจ่มใส ตำแหน่ง นักวิชาการคอมพิวเตอร์

๙.๑.๔ เจ้าหน้าที่รับโทรศัพท์ / ตอบคำถามประจำหมายเลขโทรศัพท์

- นายสิทธิชัย จุฬา ตำแหน่ง เจ้าพนักงานเครื่องคอมพิวเตอร์
- นางสาววรรณธวัชก์ ธนกรเจริญศักดิ์ ตำแหน่ง เจ้าพนักงานธุรการ

๙.๑.๕ เจ้าหน้าที่ประสานงาน / ประชาสัมพันธ์

- นายสิทธิชัย จุฬา ตำแหน่ง เจ้าพนักงานเครื่องคอมพิวเตอร์
- นางสาววรรณธวัชก์ ธนกรเจริญศักดิ์ ตำแหน่ง เจ้าพนักงานธุรการ

๙.๒ นอกเวลาราชการ

๙.๒.๑ เจ้าหน้าที่แก้ไขปัญหาระบบคอมพิวเตอร์ (Server)

- เจ้าหน้าที่เวรปฏิบัติหน้าที่นอกเวลาราชการตามตารางเวร

๙.๒.๒ เจ้าหน้าที่แก้ไขปัญหาเครื่องคอมพิวเตอร์และระบบเครือข่าย

- เจ้าหน้าที่เวรปฏิบัติหน้าที่นอกเวลาราชการตามตารางเวร

๙.๒.๓ เจ้าหน้าที่รับโทรศัพท์ / ตอบคำถามประจำหมายเลขโทรศัพท์

- เจ้าหน้าที่เวรปฏิบัติหน้าที่นอกเวลาราชการตามตางรางเวร

๙.๒.๔ เจ้าหน้าที่ประสานงาน / ประชาสัมพันธ์

- เจ้าหน้าที่เวรปฏิบัติหน้าที่นอกเวลาราชการตามตางรางเวร

หมายเหตุ: ในกรณีที่เจ้าหน้าที่เวรไม่สามารถแก้ไขได้ สามารถติดต่อผู้ดูแลระบบ ดังนี้

- นายเกียรติธนพัฒน์ มนตรี ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
- นายคมน์ ชุ่มสูงเนิน ตำแหน่ง นักเทคโนโลยีสารสนเทศปฏิบัติการ

๑๐.การแก้ปัญหา

๑๐.๑ การแก้ปัญหาระบบเครือข่ายล่มในเวลาราชการเมื่อพบปัญหาดำเนินการตามลำดับ ดังนี้

ระดับที่ ๑ ประเมินสถานการณ์สามารถแก้ไขปัญหาได้ภายใน ๑๕ นาทีรายงานผู้บังคับบัญชาตามลำดับชั้นและเริ่มปฏิบัติการ ดังนี้

๑. ในเวลาราชการ (กรณีระบบล่มทั่วไป)

ขั้นตอนการปฏิบัติ

๑.๑ กรณีเครื่อง server มีปัญหา

๑. เจ้าหน้าที่ ๙.๑.๑ เข้าตรวจสอบเครื่อง Server Master เพื่อหาสาเหตุที่ทำให้เกิดปัญหา ซึ่งเกิดจากหลายสาเหตุ เช่น MariaDB/MySQL Service หยุดทำงาน ,Max Connections เต็ม ซึ่งบางครั้งอาจจำเป็นต้องดำเนินการในขั้นตอนที่๒ ร่วมด้วย

๒. เจ้าหน้าที่ ๙.๑.๑ Restart Server Master

๑.๒ กรณีเครื่อง อุปกรณ์ Network มีปัญหา

๑. เจ้าหน้าที่ ๙.๑.๓ ตรวจสอบ / เปลี่ยนอุปกรณ์เชื่อมต่อ Server Master

๒. เมื่อดำเนินการแก้ไขปัญหาเรียบร้อยแล้วเจ้าหน้าที่ ๙.๑.๒ ทดสอบการเชื่อมต่อระหว่าง Server – Client ว่าสามารถเชื่อมต่อใช้งานฐานข้อมูลปกติแล้วหรือไม่

๓. เจ้าหน้าที่ ๙.๑.๓ ลงบันทึกในแบบฟอร์มบันทึกการแก้ปัญหาระบบเครือข่าย HOSxP และบันทึกลงโปรแกรมความเสี่ยงของโรงพยาบาลปราสาท

ระดับที่ ๒ ประเมินสถานการณ์สามารถแก้ไขปัญหาได้ภายในเวลา ๑๖ – ๓๐ นาที รายงานผู้บังคับบัญชาตามลำดับชั้น และกำหนดหน้าที่รับผิดชอบ ดังนี้

๑. ในเวลาราชการ (กรณีระบบล่มทั่วไป)

ขั้นตอนการปฏิบัติ

๑.๑ เจ้าหน้าที่ ๙.๑.๕ แจ้งประชาสัมพันธ์เพื่อประกาศสถานการณ์ระบบคอมพิวเตอร์ขัดข้องและเวลาที่จะสามารถใช้งานระบบได้ทางเสียงตามสาย / ประสานหัวหน้าศูนย์เพื่อรายงานสถานการณ์ผู้บริหารตามลำดับชั้นพิจารณาตามสถาณการณ์

หมายเหตุ: กรณีเครื่อง server หลักสามารถแก้ไขได้ (คล้ายระดับที่๑ แต่ใช้เวลามากกว่า) ดำเนินการตามขั้นตอนกระบวนการระดับที่ ๑ และกรณีเครื่อง server ไม่สามารถแก้ไขปัญหาได้อาจจำเป็นต้องดำเนินการกู้คืนหรือติดตั้งใหม่

๑.๒ เจ้าหน้าที่ ๙.๑.๑ สลับเครื่องแม่ข่ายจาก Server Master เป็น Server Slave

๑.๓ เจ้าหน้าที่ ๙.๑.๒ สลับ IP เครื่อง Server Slave เป็น IP เครื่อง Server Master

๑.๔ เมื่อดำเนินการแก้ไขปัญหาเรียบร้อยแล้วเจ้าหน้าที่ ๙.๑.๒ ทดสอบการเชื่อมต่อระหว่าง Server – Client ว่าสามารถเชื่อมต่อใช้งานฐานข้อมูลปกติแล้วหรือไม่

๑.๕ เจ้าหน้าที่ ๙.๑.๓ เข้าตรวจสอบเครื่อง Server Master

๑.๖ เจ้าหน้าที่ ๙.๑.๔ ตอบคำถามและแจ้งสถานการณ์ทางโทรศัพท์ที่โทรเข้ามา

๑.๗ เจ้าหน้าที่ ๙.๑.๓ ลงบันทึกในแบบฟอร์มบันทึกการแก้ปัญหาระบบเครือข่าย HOSxP และบันทึกลงโปรแกรมความเสี่ยงของโรงพยาบาลปราสาท

ระดับที่ ๓ ประเมินสถานการณ์ไม่สามารถแก้ไขปัญหาได้ภายในเวลา ๓๐ นาที รายงานผู้บังคับบัญชาตามลำดับชั้น ขอใช้แผนกู้คืนระบบ HOSxP และระบบเครือข่าย (กรณีรุนแรงเกินการควบคุม) ประกาศ IT ปาป้า๒ / IT เจ็บจี๊ด๒ และปฏิบัติตาม Flow แล้วแต่กรณี

๑. การใช้ระบบ Manual สรุปหน้าที่ของหน่วยงานต่างๆ ดังนี้

<u>ศูนย์ข้อมูลข่าวสารและสารสนเทศ</u>

- เจ้าหน้าที่ ๙.๑.๕ ประกาศสถานการณ์ฉุกเฉิน ให้ทุกฝ่ายใช้งานระบบ Manual

<u>ห้องเวชระเบียน</u>

- ผู้ป่วยเก่า ค้น OPD Card ปั๊มวันที่และลงเวลา บันทึกในทะเบียน
- ผู้ป่วยใหม่ เขียนข้อมูลทั่วไปลงบนกระดาษ A๕ บันทึกในทะเบียน
- ตรวจสอบสิทธิการรักษาของผู้ป่วย ในกรณีอินเตอร์เน็ตใช้งานได้
- เขียนใบสั่งยา
- ส่ง OPD Card ไปยังห้องตรวจต่างๆ

<u>หมายเหตุ</u>: ในกรณีผู้ป่วยเก่าลืมนำบัตรผู้ป่วยมา ห้องบัตรมีแผนในการใช้งานโปรแกรม HOSxP ที่เรียกจากเครื่อง Stand alone เพื่อใช้ค้นเลข HN ของผู้ป่วย

<u>จุดซักประวัติ</u>

- OPD Card ที่ออกจากห้องบัตรก่อนระบบล่ม ให้ปั๊มวันที่และลงเวลา
- บันทึกอาการสำคัญต่างๆ ของผู้ป่วยลงบน OPD Card
- ตรวจสอบสิทธิการรักษาของผู้ป่วย ในกรณีอินเตอร์เน็ตใช้งานไม่ได้
- ส่งตรวจไปยังห้องตรวจแพทย์ต่าง ๆ

<u>หมายเหตุ</u> : ผู้ป่วยที่ซักประวัติแล้วไม่ต้องซักประวัติอีก ให้ส่งเข้าห้องตรวจได้เลย

ห้องตรวจแพทย์

- บันทึก Physical examination note/ลงผลการวินิจฉัย ใน OPD Card
- บันทึกการจ่ายเวชภัณฑ์และยาลงบนใบสั่งยา
- กรณีนัดผู้ป่วย ให้ลงนัดผู้ป่วยในสมุดทะเบียน พร้อมเขียนใบนัดให้ผู้ป่วย
- หากมีการส่ง Investigate ให้เขียนลงในใบ Request
- เขียนใบ Order หากแพทย์สั่ง Admission ผู้ป่วย แล้วส่งศูนย์ Admit เพื่อออกเลข AN ชั่วคราวและลงทะเบียนไว้เป็นหลักฐาน
- เขียนใบใช้ยานอกบัญชีฯ หากมีการสั่งจ่ายยานอกบัญชีฯ
- กรณีส่งต่อผู้ป่วย ให้เขียนใบส่งตัว และแจ้งศูนย์ Refer เพื่อลงทะเบียนผู้ป่วยไว้ เมื่อระบบใช้ได้ให้ออกเลข Refer ให้ผู้ป่วย

ห้อง Lab / X-ray / วิสัญญี / ห้องผ่าตัด และอื่นๆ

- บันทึกรายละเอียดกิจกรรมทั้งหมดลงในกระดาษ ได้แก่ ผลการตรวจทางห้องปฏิบัติการ ผล X-ray, EKG รายละเอียดการทำให้ยาระงับความรู้สึก การผ่าตัดหัตถการต่าง ๆ
- บันทึกรายการวัสดุอุปกรณ์ทั้งหมดที่ใช้

ผู้ป่วยนอก

- ผู้ป่วยที่มีบัตรนัดเจาะเลือด ห้อง lab สั่ง order พร้อมพิมพ์ Barcode ในโปรแกรม LIS
- พิมพ์ผล lab จากระบบ LIS พร้อมคิดราคาค่า lab ลงบนใบรายงานผล
- ส่งมอบผลให้แผนกที่ส่งตรวจ
- ผู้ป่วยที่มี order ในใบสั่งยา ห้อง lab สั่ง order พร้อมพิมพ์ Barcode ในโปรแกรม LIS ตามใบสั่งยา คิดราคาค่า lab ลงบนใบสั่งยา
- พิมพ์ผล lab จากระบบ LIS
- ส่งมอบผลให้แผนกที่ส่งตรวจ

ผู้ป่วยใน

- หอผู้ป่วยเจาะเลือด พร้อมส่งใบ request มาที่ห้อง lab พร้อมกับบันทึกรายการส่งตรวจลงในทะเบียนห้อง lab สั่ง order พร้อมพิมพ์ Barcode ในโปรแกรม LIS
- ห้อง lab รายงานผลในใบ request และสำเนาผลไว้ที่ห้อง lab
- ส่งมอบผลให้หอผู้ป่วยที่ส่งตรวจ
- การสั่ง X-ray ให้แผนกที่ส่งตรวจเขียน Order ลงบนใบสั่งยาแนบพร้อม OPD Card ส่งห้อง X-ray พร้อมสรุปราคาลงบนใบสั่งยา

ห้องจ่ายยา

- คิดค่ายาและเวชภัณฑ์ (ในรายที่ต้องเก็บเงิน) แล้วส่งให้ห้องเก็บเงิน
- จ่ายยาให้ผู้ป่วย

หมายเหตุ : ทางศูนย์คอมพิวเตอร์จะ set เครื่องคอมพิวเตอร์จำนวน ๑ เครื่องให้สามารถใช้งานโปรแกรม HOSxP แบบ Stand alone เพื่อใช้เรียกดูราคายา

ห้องชำระเงิน

- เก็บเงินผู้ป่วยโดยดูราคาในใบสั่งยา
- เขียนใบเสร็จรับเงินให้ผู้ป่วย
- การออกใบแสดงค่ารักษาพยาบาลสำหรับสิทธิเบิกจ่ายตรง เพื่อให้ผู้ป่วยเซ็นรับทราบค่าใช้จ่าย ให้ผู้ป่วยเซ็นบนใบสั่งยาแล้วใช้เป็นหลักฐาน

Admit Center

- ลงทะเบียนรับ Admit ในทะเบียนไว้เป็นหลักฐาน
- ส่งผู้ป่วยรับยา และเข้าหอผู้ป่วย

หมายเหตุ : Case ที่ใช้ระบบ Manual แล้ว ให้ใช้ระบบ Manual จนจบกระบวนการถึงแม้ระบบจะใช้งานได้แล้ว

๒. **การนำข้อมูลเข้าระบบ HOSxP เมื่อระบบใช้งานได้**

ศูนย์ข้อมูลข่าวสารและสารสนเทศ

- เจ้าหน้าที่ ศ.๑.๕ ประกาศสถานการณ์ปกติ ให้ทุกฝ่ายใช้งานระบบ HOSxP ได้ปกติ

ห้องเวชระเบียน

- เปิด Visit จากทะเบียนที่บันทึกไว้
- ประกาศให้หน่วยงานทราบว่าได้ออก Visit ให้ผู้ป่วยแล้วเพื่อดำเนินการต่อไป

ห้องตรวจแพทย์

- บันทึกข้อมูลนัดในโปรแกรม HOSxP จากสมุดทะเบียนนัด
- บันทึกการรับ Refer ในโปรแกรม HOSxP

ห้อง Lab / X-ray / วิสัญญี / ห้องผ่าตัด และอื่นๆ

ผู้ป่วยนอก

- ห้อง lab สั่ง order และลงผลในโปรแกรม HOSxP

ผู้ป่วยใน

- หอผู้ป่วย สั่ง order และลงผลในโปรแกรม HOSxP
- ห้อง lab รับ order จากโปรแกรม HOSxP และรายงานผลลงผลในโปรแกรม HOSxP

ห้องจ่ายยา

- นำใบสั่งยามาบันทึกในโปรแกรม HOSxP

ห้องชำระเงิน

- นำใบสั่งยา สิทธิเบิกจ่ายตรงมาขึ้นทะเบียนลูกหนี้ในโปรแกรม HOSxP ในรายที่มีการทำหัตถการ ส่งศูนย์ประกันสุขภาพเพื่อบันทึกในโปรแกรม HOSxP

<u>ศูนย์Refer</u>

- นำทะเบียนที่ลงข้อมูลการส่งต่อผู้ป่วย มาบันทึกในโปรแกรม HOSxP เพื่อให้ได้เลขที่ Refer พร้อมกับเขียนเลขที่ Refer ที่ได้จากโปรแกรมไว้ในสมุดทะเบียน

<u>Admit Center</u>

- ลงทะเบียน Admit ในโปรแกรม HOSxP ตรวจสอบสิทธิการรักษา
- พิมพ์ใบ Summary ส่งให้หอผู้ป่วย

<u>หอผู้ป่วยใน</u>

- รับใบ Summary จาก Admit Center และแก้ไข HN, AN ในแบบฟอร์มต่างๆ ให้ถูกต้อง
- บันทึกกิจกรรมต่างๆที่ทำในระบบ Manual เข้าโปรแกรม HOSxP

๑๐.๒ การแก้ปัญหาระบบเครือข่ายล่มนอกเวลาราชการเมื่อพบปัญหาดำเนินการตามลำดับ ดังนี้

ระดับที่ ๑ ประเมินสถานการณ์สามารถแก้ไขปัญหาได้ภายใน ๑๕ นาที รายงานผู้บังคับบัญชาตามลำดับขั้น และเริ่มปฏิบัติการ ดังนี้

๑. **นอกเวลาราชการ (กรณีระบบล่มทั่วไป)**

ขั้นตอนการปฏิบัติ

๑.๑ กรณีเครื่อง server มีปัญหา

๑. เจ้าหน้าที่เวร เข้าตรวจสอบเครื่อง Server Master เพื่อหาสาเหตุที่ทำให้เกิดปัญหา ซึ่งเกิดจากหลายสาเหตุ เช่น MariaDB/MySQL Service หยุดทำงาน, Max Connections เต็ม ซึ่งบางครั้งอาจจำเป็นต้องดำเนินการในขั้นตอนที่ ๒ ร่วมด้วย

๒. เจ้าหน้าที่เวร Restart Server Master

๑.๒ กรณีเครื่อง อุปกรณ์ Network มีปัญหา

๑. เจ้าหน้าที่เวร ตรวจสอบ / เปลี่ยนอุปกรณ์เชื่อมต่อ Server Master

๒. เมื่อดำเนินการแก้ไขปัญหาเรียบร้อยแล้วเจ้าหน้าที่เวร ทดสอบการเชื่อมต่อระหว่าง Server – Client ว่าสามารถเชื่อมต่อใช้งานฐานข้อมูลปกติแล้วหรือไม่

๓. เจ้าหน้าที่เวร ลงบันทึกในแบบฟอร์มบันทึกการแก้ปัญหาระบบเครือข่าย HOSxP และบันทึกลงโปรแกรมความเสี่ยงของโรงพยาบาลปราสาท

หมายเหตุ : ในกรณีที่เจ้าหน้าที่เวรไม่สามารถแก้ไขได้สามารถติดต่อผู้ดูแลระบบ ดังนี้

- นายเกียรติธนพัฒน์ มนตรี ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
- นายคมน์ ชุ่มสูงเนิน ตำแหน่ง นักเทคโนโลยีสารสนเทศปฏิบัติการ

ระดับที่ ๒ ประเมินสถานการณ์สามารถแก้ไขปัญหาได้ภายในเวลา ๑๖ – ๓๐ นาที รายงานผู้บังคับบัญชาตามลำดับขั้นและกำหนดหน้าที่รับผิดชอบดังนี้

๑. **นอกเวลาราชการ (กรณีระบบล่มทั่วไป)**

ขั้นตอนการปฏิบัติ

๑.๑ เจ้าหน้าที่เวร แจ้งประชาสัมพันธ์เพื่อประกาศสถานการณ์ระบบคอมพิวเตอร์ขัดข้องและเวลาที่จะสามารถใช้งานระบบได้ทางเสียงตามสาย / ประสานหัวหน้าศูนย์ เพื่อรายงานสถานการณ์ผู้บริหารตามลำดับขั้นพิจารณาตามสถานการณ์

หมายเหตุ: กรณีเครื่อง server หลักสามารถแก้ไขได้ (คล้ายระดับที่ ๑ แต่ใช้เวลามากกว่า) ดำเนินการตามขั้นตอนกระบวนการระดับที่ ๑ และกรณีเครื่อง server ไม่สามารถแก้ไขปัญหาได้อาจจำเป็นต้องดำเนินการกู้คืนหรือติดตั้งใหม่

๑.๒ เจ้าหน้าที่เวร สลับเครื่องแม่ข่ายจาก Server Master เป็น Server Slave

๑.๓ เจ้าหน้าที่เวร สลับ IP เครื่อง Server Slave เป็น IP เครื่อง Server Master

๑.๔ เมื่อดำเนินการแก้ไขปัญหาเรียบร้อยแล้วเจ้าหน้าที่เวร ทดสอบการเชื่อมต่อระหว่าง Server – Client ว่าสามารถเชื่อมต่อใช้งานฐานข้อมูลปกติแล้วหรือไม่

๑.๕ เจ้าหน้าที่เวร เข้าตรวจสอบเครื่อง Server Master

๑.๖ เจ้าหน้าที่เวร ตอบคำถามและแจ้งสถานการณ์ทางโทรศัพท์ที่โทรเข้ามา

๑.๗ เจ้าหน้าที่เวร บันทึกในแบบฟอร์มบันทึกการแก้ปัญหาระบบเครือข่าย HOSxP และบันทึกลงโปรแกรมความเสี่ยงของโรงพยาบาลปราสาท

หมายเหตุ: ในกรณีที่เจ้าหน้าที่เวรไม่สามารถแก้ไขได้สามารถติดต่อผู้ดูแลระบบ ดังนี้

- นายเกียรติธนพัฒน์ มนตรี ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ
- นายคมน์ ชุ่มสูงเนิน ตำแหน่ง นักเทคโนโลยีสารสนเทศปฏิบัติการ

ระดับที่ ๓ ประเมินสถานการณ์ไม่สามารถแก้ไขปัญหาได้ภายในเวลา ๓๐ นาที รายงานผู้บังคับบัญชาตามลำดับขั้น ขอใช้แผนกู้คืนระบบ HOSxP และระบบเครือข่าย (กรณีรุนแรงเกินการควบคุม) ทีม IT ร่วมกันเพื่อแก้ไขปัญหา ประกาศ IT ปาป้า ๒ / IT เจ็บจี๊ด ๒ และปฏิบัติตาม Flow แล้วแต่กรณี

๑. **การใช้ระบบManual สรุปหน้าที่ของหน่วยงานต่างๆ ดังนี้**

<u>ศูนย์ข้อมูลข่าวสารและสารสนเทศ</u>

- เจ้าหน้าที่เวรประกาศสถานการณ์ฉุกเฉิน ให้ทุกฝ่ายใช้งานระบบ Manual

<u>ห้องเวชระเบียน</u>

- ผู้ป่วยเก่า ค้น OPD Card ปั๊มวันที่และลงเวลา บันทึกในทะเบียน
- ผู้ป่วยใหม่ เขียนข้อมูลทั่วไปลงบนกระดาษ A๕ บันทึกในทะเบียนตรวจสอบสิทธิการรักษาของผู้ป่วยในกรณีอินเตอร์เน็ตใช้งานได้

- เขียนใบสั่งยา
- ส่ง OPD Card ไปยังห้องตรวจต่าง ๆ

หมายเหตุ : ในกรณีผู้ป่วยเก่าลืมนำบัตรผู้ป่วยมา ห้องบัตรมีแผนในการใช้งานโปรแกรม HOSxP ที่เรียกจากเครื่อง Stand alone เพื่อใช้ค้นเลข HN ของผู้ป่วย

จุดซักประวัติ

- OPD Card ที่ออกจากห้องบัตรก่อนระบบล่ม ให้ ปั๊มวันที่และลงเวลา
- บันทึกอาการสำคัญต่าง ๆ ของผู้ป่วยลงบน OPD Card
- ตรวจสอบสิทธิการรักษาของผู้ป่วย ในกรณีอินเตอร์เน็ตใช้งานไม่ได้
- ส่งตรวจไปยังห้องตรวจแพทย์ต่าง ๆ

หมายเหตุ : ผู้ป่วยที่ซักประวัติแล้วไม่ต้องซักประวัติอีก ให้ส่งเข้าห้องตรวจได้เลย

ห้องตรวจแพทย์

- บันทึก Physical examination note/ ลงผลการวินิจฉัย ใน OPD Card
- บันทึกการจ่ายเวชภัณฑ์และยาลงบนใบสั่งยา
- กรณีนัดผู้ป่วย ให้ลงนัดผู้ป่วยในสมุดทะเบียน พร้อมเขียนใบนัดให้ผู้ป่วย
- หากมีการส่ง Investigate ให้เขียนลงในใบ Request
- เขียนใบ Order หากแพทย์สั่ง Admission ผู้ป่วย แล้วส่งศูนย์ Admit เพื่อออกเลข AN ชั่วคราวและลงทะเบียนไว้เป็นหลักฐาน
- เขียนใบใช้ยานอกบัญชีฯ หากมีการสั่งจ่ายยานอกบัญชีฯ
- กรณีส่งต่อผู้ป่วยให้เขียนใบส่งตัวและแจ้งศูนย์ Refer เพื่อลงทะเบียนผู้ป่วยไว้ เมื่อระบบใช้ได้ให้ออกเลข Refer ให้ผู้ป่วย

ห้อง Lab / X-ray / วิสัญญี / ห้องผ่าตัด และอื่นๆ

- บันทึกรายละเอียดกิจกรรมทั้งหมดลงในกระดาษ ได้แก่ ผลการตรวจทางห้องปฏิบัติการผล X-ray, EKG รายละเอียดการทำให้ยาระงับความรู้สึก การผ่าตัดหัตถการต่างๆ
- บันทึกรายการวัสดุอุปกรณ์ทั้งหมดที่ใช้

ผู้ป่วยนอก

- ผู้ป่วยที่มีบัตรนัดเจาะเลือด ห้อง lab สั่ง order พร้อมพิมพ์ Barcode ในโปรแกรม LIS พิมพ์ผล lab จากระบบ LIS พร้อมคิดราคาค่า lab ลงบนใบรายงานผล
- ส่งมอบผลให้แผนกที่ส่งตรวจ
- ผู้ป่วยที่มี order ในใบสั่งยา ห้อง lab สั่ง order พร้อมพิมพ์ Barcode ใน โปรแกรม LIS ตามใบสั่งยา คิดราคาค่า lab ลงบนใบสั่งยา
- พิมพ์ผล lab จากระบบ LIS
- ส่งมอบผลให้แผนกที่ส่งตรวจ

<u>ผู้ป่วยใน</u>

- หอผู้ป่วยเจาะเลือด พร้อมส่งใบ request มาที่ห้อง lab พร้อมกับบันทึกรายการส่งตรวจลงในทะเบียนห้อง lab สั่ง order พร้อมพิมพ์ Barcode ในโปรแกรม LIS
- ห้อง lab รายงานผลในใบ request และสำเนาผลไว้ที่ห้อง lab
- ส่งมอบผลให้หอผู้ป่วยที่ส่งตรวจ
- การสั่ง X-ray ให้แผนกที่ส่งตรวจเขียน Order ลงบนใบสั่งยาแนบพร้อม OPD Card ส่งห้อง X-ray พร้อมสรุปราคาลงบนใบสั่งยา

<u>ห้องจ่ายยา</u>

- คิดค่ายาและเวชภัณฑ์ (ในรายที่ต้องเก็บเงิน) แล้วส่งให้ห้องเก็บเงิน
- จ่ายยาให้ผู้ป่วย

<u>หมายเหตุ</u> : ทางศูนย์คอมพิวเตอร์จะ set เครื่องคอมพิวเตอร์จำนวน ๑ เครื่อง ให้สามารถใช้งานโปรแกรม HOSxP แบบ Stand alone เพื่อใช้เรียกดูราคายา

<u>ห้องชำระเงิน</u>

- เก็บเงินผู้ป่วยโดยดูราคาในใบสั่งยา
- เขียนใบเสร็จรับเงินให้ผู้ป่วย
- การออกใบแสดงค่ารักษาพยาบาลสำหรับสิทธิเบิกจ่ายตรง เพื่อให้ผู้ป่วยเซ็นรับทราบค่าใช้จ่าย ให้ผู้ป่วยเซ็นบนใบสั่งยาแล้วใช้เป็นหลักฐาน

<u>Admit Center</u>

- ลงทะเบียนรับ Admit ในทะเบียนไว้เป็นหลักฐาน
- ส่งผู้ป่วยรับยา และเข้าหอผู้ป่วย

หมายเหตุ : Case ที่ใช้ระบบ Manual แล้ว ให้ใช้ระบบ Manual จนจบกระบวนการถึงแม้ระบบจะใช้งานได้แล้ว

๒. **การนำข้อมูลเข้าระบบ HOSxP เมื่อระบบใช้งานได้**

<u>ศูนย์ข้อมูลข่าวสารและสารสนเทศ</u>

- เจ้าหน้าที่เวรประกาศสถานการณ์ปกติ ให้ทุกฝ่ายใช้งานระบบ HOSxP ได้ปกติ

<u>ห้องเวชระเบียน</u>

- เปิด Visit จากทะเบียนที่บันทึกไว้
- ประกาศให้หน่วยงานทราบว่าได้ออก Visit ให้ผู้ป่วยแล้วเพื่อดำเนินการต่อไป

<u>ห้องตรวจแพทย์</u>

- บันทึกข้อมูลนัดในโปรแกรม HOSxP จากสมุดทะเบียนนัด
- บันทึกการรับ Refer ในโปรแกรม HOSxP

<u>ห้อง Lab / X-ray / วิสัญญี / ห้องผ่าตัด และอื่นๆ</u>

- บันทึกรายละเอียดกิจกรรมทั้งหมดลงในกระดาษ ได้แก่ ผลการตรวจทางห้องปฏิบัติการผล X-ray, EKG รายละเอียดการทำให้ยาระงับความรู้สึก การผ่าตัดหัตถการต่าง ๆ
- บันทึกรายการวัสดุอุปกรณ์ทั้งหมดที่ใช้

<u>ผู้ป่วยนอก</u>

- ห้อง lab สั่ง order และลงผลในโปรแกรม HOSxP

<u>ผู้ป่วยใน</u>

- หอผู้ป่วย สั่ง order และลงผลในโปรแกรม HOSxP
- ห้อง lab รับ order จากโปรแกรม HOSxP และรายงานผลลงผลในโปรแกรม HOSxP

<u>ห้องจ่ายยา</u>

- นำใบสั่งยามาบันทึกในโปรแกรม HOSxP

<u>ห้องชำระเงิน</u>

- นำใบสั่งยา สิทธิเบิกจ่ายตรงมาขึ้นทะเบียนลูกหนี้ในโปรแกรม HOSxP ในรายที่มีการทำหัตถการ ส่งศูนย์ประกันสุขภาพเพื่อบันทึกในโปรแกรม HOSxP

<u>ศูนย์Refer</u>

- นำทะเบียนที่ลงข้อมูลการส่งต่อผู้ป่วยมาบันทึกในโปรแกรม HOSxP เพื่อให้ได้เลขที่ Refer พร้อมกับเขียนเลขที่ Refer ที่ได้จากโปรแกรมไว้ในสมุดทะเบียน

<u>Admit Center</u>

- ลงทะเบียน Admit ในโปรแกรม HOSxP ตรวจสอบสิทธิการรักษา
- พิมพ์ใบ Summary ส่งให้หอผู้ป่วย

<u>หอผู้ป่วยใน</u>

- รับใบ Summary จาก Admit Center และแก้ไข HN, AN ในแบบฟอร์มต่าง ๆ ให้ถูกต้อง
- บันทึกกิจกรรมต่าง ๆ ที่ทำในระบบ Manual เข้าโปรแกรม HOSxP

หมายเหตุ : กรณีระบบ HIS หลักล่มแต่เครือข่าย internet ยังสามารถใช้งานได้ กำหนดให้เจ้าหน้าที่ แพทย์ พยาบาลผู้ป่วยนอก เจ้าหน้าที่เภสัชกร สามารถเข้าดูประวัติผู้ป่วยได้ผ่านระบบ PHR Viewer ของ MOPH PHR Link: https://phr๑.moph.go.th/phr/ ตามเอกสารหมายเลข ๑๐

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของโรงพยาบาลปราสาท

๑. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของ (โรงพยาบาลปราสาท) ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือ กำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง (๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมินผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระจากภายนอกอย่างน้อยปีละหนึ่งครั้งและ (๒) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามแผนรับมือเหตุภัยคุกคามทางไซเบอร์ หน่วยงานโรงพยาบาลปราสาท ด้วย

๒. วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใน (โรงพยาบาลปราสาท) โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่าง ๆ ภายใต้ (โรงพยาบาลปราสาท) การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของ (โรงพยาบาลปราสาท)

๓. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของ (โรงพยาบาลปราสาท) รวมถึงบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศและข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

คณะกรรมการสารสนเทศ โรงพยาบาลปราสาท (Information: IM) มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ ถึงผู้บริหารสูงสุดหรือผู้ที่รับมอบอำนาจหน่วยงาน

๕. หน้าที่ในการดำเนินการตามแผน

โรงพยาบาลปราสาทด้านไซเบอร์ภายใต้กลุ่มภารกิจสุขภาพดิจิทัล มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้ โดยมีกลุ่มงานสนับสนุนประกอบด้วย กลุ่มงานเทคโนโลยีสารสนเทศ กลุ่มงานสุขภาพดิจิทัลและกลุ่มงานเวชระเบียนและข้อมูลทางการแพทย์

๖. **รายละเอียดการบังคับใช้เอกสาร**

หน่วยงานจะต้องระบุรายละเอียดที่เกี่ยวข้องกับเอกสาร ดังต่อไปนี้

๖.๑. รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	
ผู้ดำเนินการตามเอกสาร (Owner)	
วันที่จัดทำเอกสาร (Date created)	
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	

๖.๒. การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)

๗. **เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง**

๗.๑ แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล สำนักงานปลัดกระทรวงสาธารณสุข

๗.๒ การปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๗.๓ คำสั่ง สป.สธ ที่ ๒๑๐๓ ๒๕๖๕ เรื่อง มอบอำนาจให้หัวหน้าหน่วยงานลงนามในข้อตกลงการประมวลผลข้อมูล ส่วนบุคคล (DPA)

๗.๔ คำสั่ง ศทส. ที่ สธ. ๐๒๑๒.๐๗ ๒๔๒๓ ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล

๗.๕ นโยบายการคุ้มครองข้อมูลส่วนบุคคลจากกล้องวงจรปิด (CCTV)

๗.๕ ประกาศโรงพยาบาลปราสาทนโยบายคุ้มครองข้อมูลส่วนบุคคล

๘. นิยาม

"เหตุการณ์ (Event)" หมายความว่า เหตุการณ์ที่เกิดขึ้นจากการเฝ้าระวังสังเกตการณ์ (observable occurrence) ในระบบ เครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการหรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

"เหตุภัยคุกคามทางไซเบอร์ (Cyber incident)" หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมาย ให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่ จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

"ภัยคุกคามทางไซเบอร์ (Cyber threat)" หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง

"เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ๑" หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

๙. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

๙.๑. ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

หน่วยงานควรระบุข้อมูลการติดต่อของผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงานกรณีเมื่อมีการตรวจพบหรือมีการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยควรมีผู้รับแจ้งเหตุฯ หลัก รวมถึงช่องทางหลักในการติดต่อและเตรียมผู้รับแจ้งเหตุฯ คนที่สอง รวมถึงช่องทางสำรองสำหรับกรณีที่ไม่สามารถติดต่อผู้รับแจ้งเหตุคนแรกได้ โดยหน่วยงานควรจะกำหนดให้มีผู้ทำหน้าที่รับแจ้งเหตุฯ คลอบคลุมตลอดระยะเวลา ๒๔ ชั่วโมง/ ๗ วัน

ลำดับ	ชื่อ- นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายเกียรติธนพัฒน์ มนตรี	ในเวลาราชการ ๐๘.๐๐-๑๖.๐๐ น. นอกเวลาราชการ ๑๖.๐๐-๒๐.๐๐ น.	เบอร์โทรศัพท์ภายใน ๑๒๖๙, โทรศัพท์เคลื่อนที่ ๐๘๓ – ๑๒๔๕ ๔๙๐	รับแจ้งเหตุ แก้ไขเหตุเบื้องต้นและรายงานผู้บริหารและประสานงาน	- ดูแลระบบ คอมพิวเตอร์ - ดูแลระบบระบบ แม่ข่าย - ดูแลระบบเครือข่ายภายใน - ดูแลระบบความปลอดภัยของ ระบบ - ระบบกล้อง CCTV - ให้ความรู้แก่บุคลากรเจ้าหน้าที่

๙.๒. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team : CIRT)

โปรดระบุว่าหน่วยงานใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบใด เช่น แบบรวมศูนย์ (Centralize), แบบกระจาย (Distributed), แบบให้คำปรึกษา (Coordinating) หรือแบบอื่น ๆ ตามบริบทของหน่วยงาน ๒ โดยหน่วยงานจะต้องระบุรายชื่อของบุคลากรที่มีความเกี่ยวข้องกับการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งโครงสร้างทีมรับมือฯ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายเกียรติธนพัฒน์ มนตรี (นักวิชาการคอมพิวเตอร์ชำนาญการ)	เบอร์โทรศัพท์ภายใน ๑๒๖๙, โทรศัพท์เคลื่อนที่ ๐๘๓ – ๑๒๔๕ ๙๙๐	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
๒	นายคมน์ ชุ่มสูงเนิน (นักเทคโนโลยีสารสนเทศปฏิบัติการ)	เบอร์โทรศัพท์ภายใน ๑๒๖๙, โทรศัพท์เคลื่อนที่ ๐๘๙ – ๙๓๐๙ ๒๒๙	รองหัวหน้าทีมรับมือ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
๓	นายปิยะ แจ่มใส (นักวิชาการคอมพิวเตอร์)	เบอร์โทรศัพท์ภายใน ๑๒๖๙, โทรศัพท์เคลื่อนที่ ๐๘๕ – ๗๗๙๖ ๐๐๙	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ (โรงพยาบาลปราสาท เจ้าของระบบภายใต้หน่วยงานของท่าน) ให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
๔	นายสิทธิชัย จุฬา (เจ้าพนักงานเครื่องคอมพิวเตอร์)	เบอร์โทรศัพท์ภายใน ๑๒๖๙, โทรศัพท์เคลื่อนที่ ๐๙๘ – ๖๓๑๙ ๙๙๓	เจ้าหน้าที่เทคนิคฯ (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายกิตติภพ แจ่มโสภณ (นายแพทย์ชำนาญการพิเศษ)	เบอร์โทรศัพท์ ภายใน ๑๒๖๙, โทรศัพท์เคลื่อนที่ ๐๙๙ – ๓๖๓๕ ๕๖๑	ประธานคณะกรรมการสารสนเทศ (Information: IM)	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม
๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข	อาคาร ๒ ชั้น ๑ เลขที่๘๘/๒๐ หมู่ ๔ ถนนติวา นนท์ ตำบลตลาดขวัญ อำเภอเมือง จังหวัด นนทบุรี ๑๑๐๐๐ อีเมล health- cirt@moph.go.th Line Official : @health-cirt โทรศัพท์ ๐๘๓-๐๖๔-๙๘๖๗website เว็บไซต์ https://health-cirt.moph.go.th	เจ้าหน้าที่ด้านการปฏิบัติ ตามกฎหมาย (Compliance)	ศูนย์ประสานการรักษาความมั่นคง ปลอดภัยไซเบอร์ ด้านสาธารณสุข (Health CERT)
๓	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซ เบอร์แห่งชาติ	โทรศัพท์ : ๐๒ ๑๔๒ ๖๘๘๘ (ติดต่อเวลาทำการ)โทรสาร : ๐๒ ๑๔๓ ๗๕๙๓ Email: แจ้งเหตุภัยคุกคามไซเบอร์ :thaicert@ncsa.or.thศูนย์ประสานการรักษาความ มั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (NCERT): โทรศัพท์ ๐๒-๑๔๒-๖๘๘๕ (ติดต่อเวลาทำการ) ศูนย์แจ้งเหตุภัยคุกคามทางไซเบอร์: โทรศัพท์๐๒-๑๑๔-๑๔๓๑ (๒๔ชั่วโมง) ที่อยู่สำนักงาน : สำนักงานคณะกรรมการการรักษาความ มั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ๑๒๐ หมู่ ๓ อาคารรัฐประศาสน ภักดี (อาคารบี) ชั้น ๗ ศูนย์ ราชการเฉลิมพระเกียรติ ๘๐พรรษา ๕ ธันวาคม ๒๕๕๐ ถนน แจ้งวัฒนะ แขวงทุ่งสองห้อง เขต หลักสี่ กรุงเทพฯ ๑๐๒๑๐	ผู้ทดสอบเจาะระบบ	หน่วยงานกำกับดูแล การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๔	นายคมน์ ชุ่มสูงเนิน (นักเทคโนโลยีสารสนเทศปฏิบัติการ)	โรงพยาบาลปราสาท สำนักงานสาธารณสุข จังหวัดสุรินทร์ : ๖๐๒ หมู่ ๒ ต.กังแอน อ.ปราสาท จ.สุรินทร์ ๓๒๑๔๐ โทรศัพท์ : ๐๘๔ – ๙๓๐๙ ๒๒๔ โทรสาร : ๐๔๔ – ๕๕๑๒ ๙๕ ต่อ ๑๐๐๓	ผู้เชี่ยวชาญด้านกฎหมาย	คณะกรรมการ DPO โรงพยาบาลปราสาท
๕	นางวันทนีย์ มามูล (นายแพทย์ชำนาญการพิเศษ)	เบอร์โทรศัพท์ภายใน : ๑๒๘๔ เบอร์โทรศัพท์มือถือ : ๐๖๒ - ๕๔๖๐๔๑๗ Email : dr.wantanee๐๑๕๔@gmail.com	ประธานคณะกรรมการความเสี่ยง (Risk Management: RM)	ทำหน้าที่ควบคุมจัดการความเสี่ยงภายในโรงพยาบาล
๖	นายกิตติภพ แจ่มโสภณ (นายแพทย์ชำนาญการพิเศษ)	เบอร์โทรศัพท์ ภายใน ๑๒๖๙, โทรศัพท์เคลื่อนที่ ๐๙๔ – ๓๖๓๕ ๕๖๑	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่สื่อสารให้กับผู้บริหารและเจ้าหน้าที่ใน รพ.

๙.๓ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

หน่วยงานควรจัดทำแผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ผู้บริหารหน่วยงาน หน่วยงานกำกับดูแล หน่วยงานรับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายและหน่วยงานภายนอก เป็นต้น รวมถึงกำหนดว่าหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติและกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมายและข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑๐.ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔, ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ ดังนี้

๑๐.๑ ขั้นการเตรียมการ (preparation)

หน่วยงานจะต้องดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อมการจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การ

ตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือโดยดำเนินการ ดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ ๙.๒

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ ๙.๔

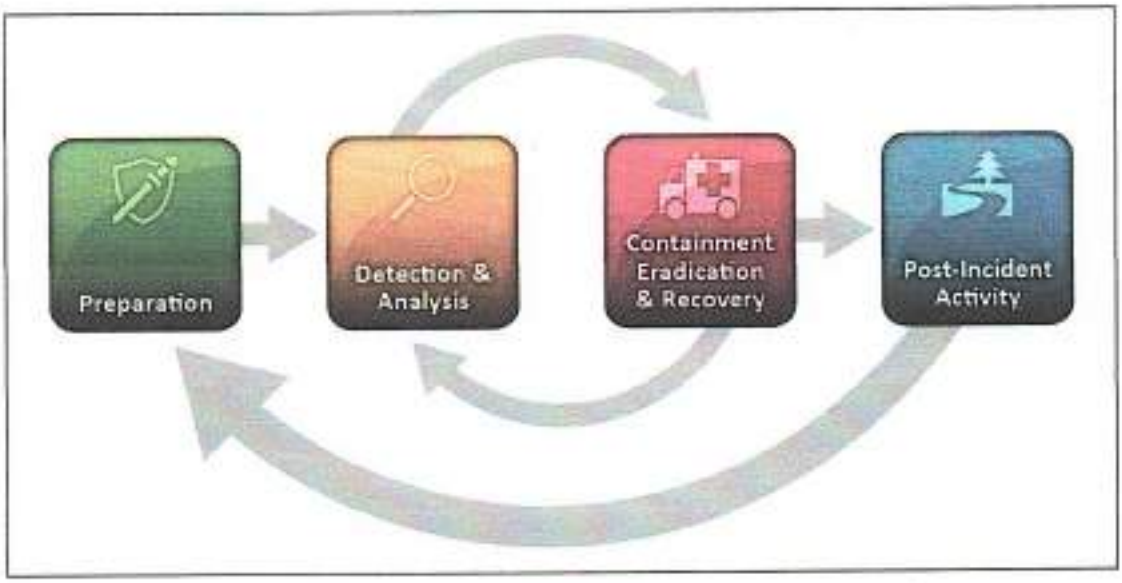
(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT

(๔) จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปกรณ์ ติดต่อสื่อสารของบุคลากร, กลไกรายงานเหตุการณ์, ห้องประชุม War room เป็นต้น

(๕) จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

(๖) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

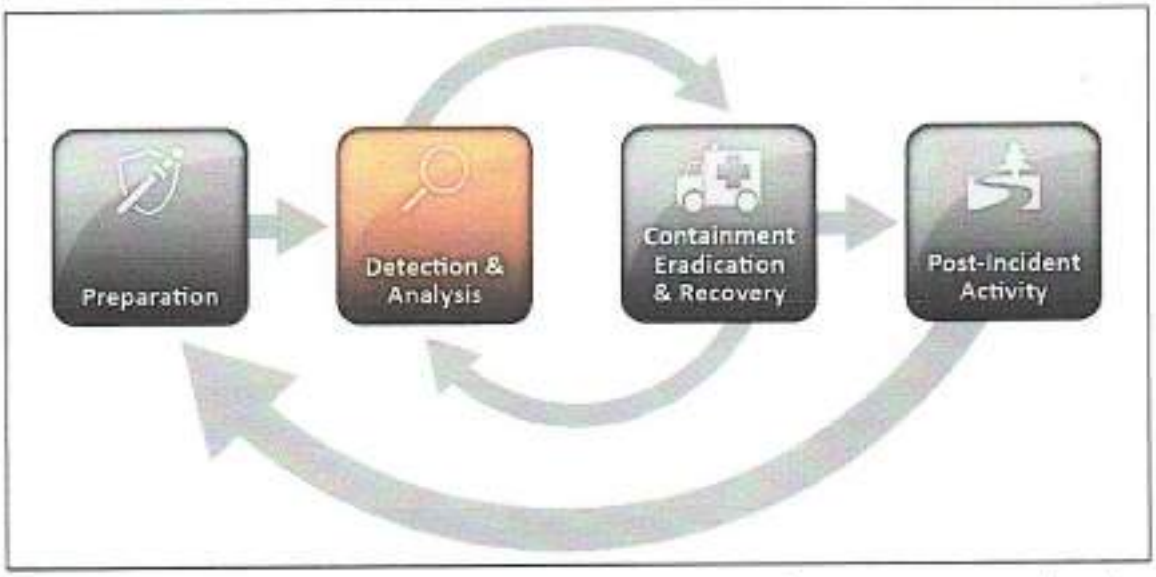
(๗) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของหน่วยงาน โดยหน่วยงานอาจดูตัวอย่างการจัดทำแผนผัง โครงสร้างขั้นตอนการรับมือฯ ได้ (รายละเอียดปรากฏตามภาคผนวก ๑)



นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๑ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

หน่วยงานจะต้องดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นโดยดำเนินการ ดังต่อไปนี้



(๑) หน่วยงานจะต้องดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้นกับหน่วยงาน (Common Attack Vectors/ Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น มีตัวอย่าง ดังนี้

ประเภท	อธิบาย	วิธีการรับมือ
อุปกรณ์แบบถอดได้ (External/Removable Media)	การโจมตีที่ดำเนินการจากอุปกรณ์แบบถอดได้หรืออุปกรณ์ต่อพ่วง ตัวอย่างเช่น โค้ดที่เป็นอันตรายแพร่กระจายไปยังระบบจากแฟลชไดรฟ์ที่ติดไวรัส	ดำเนินการถอนการติดตั้งอุปกรณ์แบบถอดได้ ที่เป็นสาเหตุของภัยคุกคามออกจากอุปกรณ์และระบบเครือข่ายของหน่วยงานและตรวจสอบสาเหตุและประเภทของภัยคุกคามว่าเป็นภัยคุกคามประเภทใด

ประเภท	อธิบาย	วิธีการรับมือ
การโจมตีทางระบบเครือข่ายอินเทอร์เน็ต	การโจมตีทางไซเบอร์มีจุดมุ่งหมายเพื่อสร้างความเสียหายหรือเข้าควบคุมหรือเข้าถึงเอกสารและระบบที่สำคัญภายในเครือข่ายคอมพิวเตอร์ของธุรกิจหรือของส่วนบุคคล การโจมตีทางไซเบอร์เกิดจากบุคคลหรือองค์กรที่มีจุดประสงค์ทางการเมืองอาชญากรรมหรือส่วนตัวในการทำลายหรือเข้าถึงข้อมูลที่เป็นความลับ ตัวอย่างบางส่วนของการโจมตีทางไซเบอร์มีดังต่อไปนี้: มัลแวร์ การโจมตีโดยปฏิเสธการให้บริการแบบ กระจาย (DDoS) ฟิชชิ่ง การโจมตีแบบแทรก SQL การเขียนสคริปต์ข้ามไซต์ (XSS) บอทเน็ต แรนซัมแวร์ การใช้ซอฟต์แวร์ที่เชื่อถือได้และกลยุทธ์ทางไซเบอร์ที่แข็งแกร่งสามารถลดโอกาสที่ ฐานข้อมูลของธุรกิจหรือของส่วนบุคคลจะ ได้รับผลกระทบจากการโจมตีทางไซเบอร์	จัดทำระบบป้องกันเครือข่าย แยกวงเครือข่ายภายในและภายนอกออกจากกัน และให้ทีมผู้เชี่ยวชาญดูแลระบบเครือข่ายภายนอก
การโจมตีแบบฟิชชิ่ง (Phishing)	การโจมตีแบบฟิชชิง มักกำหนดเป้าหมายเปลี่ยนเส้นทางของคุณไปยังเว็บไซต์ปลอมที่พยายามให้คุณกรอกข้อมูลที่มีค่า เช่น การเข้าสู่ระบบ และรหัสผ่าน ซึ่งเป็นอันตรายต่อระบบคอมพิวเตอร์ภายในระบบ	จัดทำระบบป้องกันเครือข่าย แยกวงเครือข่ายภายในและภายนอกออกจากกัน และให้ทีมผู้เชี่ยวชาญดูแลระบบเครือข่ายภายนอกและให้ความรู้เจ้าหน้าที่ในองค์กร พร้อมประกาศใช้นโยบายปฏิบัติและรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ
การเชื่อมต่อกับอุปกรณ์ภายนอก ที่ไม่อยู่ในระบบควบคุมภายใน	การนำอุปกรณ์ส่วนบุคคล เข้ามาแอบใช้งานเชื่อมต่อกับระบบเครือข่ายภายในองค์กร อาจทำให้ติดไวรัสคอมพิวเตอร์เข้าสู่ระบบภายในได้	แยกเครือข่ายภายในและภายนอกออกจากกันและให้ทีมผู้เชี่ยวชาญดูแลระบบเครือข่าย พร้อมประกาศใช้นโยบายปฏิบัติและรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ
ช่องโหว่ Zero-Days	คือช่องโหว่หรือจุดอ่อนในระบบคอมพิวเตอร์ประเภทหนึ่ง ซึ่งเกิดขึ้นจากความผิดพลาดในขั้นตอนการออกแบบและพัฒนาระบบ หากระบบปฏิบัติการไม่ได้ใช้โปรแกรมลิขสิทธิ์ทำให้ระบบคอมพิวเตอร์เสียหายได้	ติดตั้งโปรแกรมลิขสิทธิ์ และ อัพเดทอยู่เสมอ

(๒) หน่วยงานจะต้องดำเนินการจัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น

(๓) หน่วยงานจะต้องดำเนินการจัดให้มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และ ความสามารถในการกู้คืน (recoverability effort๓) เป็นต้น

ระดับความรุนแรง	คำอธิบาย	SLA(Hours)
๐(ต่ำ)	เหตุการณ์ที่มีผลกระทบน้อยที่สุด เช่น อีเมลล์แสปม การติดไวรัสที่แยกได้	
๑(ปานกลาง)	เหตุการณ์ที่มีผลกระทบอย่างมีนัยสำคัญเช่นความล่าช้าหรือความสามารถในการให้บริการที่จำกัด ที่ตรงตามภารกิจของรพ. การส่งอีเมลล์หรือการถ่ายโอนข้อมูลล่าช้า	
๒(สูง)	เหตุการณ์ที่มีผลกระทบอย่างรุนแรง เช่น การให้บริการภายในหยุดชะงัก ข้อมูลรั่วไหล	
๔(วิกฤติ)	เหตุการณ์ที่มีผลกระทบหายนะ เช่น การเข้าถึงมูลด้วยสิทธิ์ผู้ดูแลระบบ การโดน ransomware	

(๔) หน่วยงานจะต้องดำเนินการจัดให้มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก ๒)

(๕) หน่วยงานจะต้องจัดให้มีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยหน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่เกิดเหตุและระยะเวลาที่ใช้ด้วย บันทึกข้อมูลดังกล่าวที่เกี่ยวของกับเหตุการณ์ควรลงวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้น ๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก ๓)

(๖) กรณีหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะต้องจัดให้มีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ ดังนี้

(ก) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามข้อ ๔ แห่งประกาศฯ ฉบับดังกล่าวให้ใช้แบบฟอร์ม ก๑ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก๔)

(ข) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ ๕ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๒ รายงานไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา ๒๔ ชั่วโมง โดยใช้แบบฟอร์มการรายงานตาม กฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔)

(ค) หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแลจะต้องจัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปี ภายในวันที่ ๓๑ มกราคมของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก๓ โดยใช้แบบฟอร์มการรายงาน ตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔)

นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

หน่วยงานจะต้องดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ตลอดจนการฟื้นฟูระบบงานที่ได้รับ ผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึก การยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืน และการบังคับใช้กฎหมายเพื่อดำเนินคดี

นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๓ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๔. ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)

หน่วยงานควรกำหนดขั้นตอนวิธีปฏิบัติหรือกำหนดนโยบายภายในที่เกี่ยวของเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าวจะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมาและสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญาหรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมาย อื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่อง การทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

นอกจากนี้ หน่วยงานควรพิจารณาดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๔ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๕. การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

หน่วยงานจะต้องจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้แนวทางแก่หน่วยงานเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยหน่วยงานสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก ๕)

๑๐.๖ การเตรียมความพร้อมและการแบ่งปันข้อมูล

๑๐.๖.๑. ให้มีการจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) เพื่อรองรับเหตุการณ์ต่าง ๆ เช่น Ransomware, DDoS, Web Defacement และ Data Leak

๑๐.๖.๒ การแบ่งปันข้อมูล (Information Sharing): กำหนดให้มีขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ ในส่วนที่เกี่ยวกับบริการที่สำคัญรวมถึงมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าว ไปยังหน่วยงานกำกับดูแล หรือหน่วยงานเครือข่ายความร่วมมือ (เช่น Thai CERT หรือสำนักงานสาธารณสุขจังหวัด) เพื่อเป็นการเฝ้าระวังและป้องกันภัยคุกคามในภาพรวม

๑๐.๗ กระบวนการบริหารจัดการในภาวะวิกฤต (Crisis Management Procedure)

เมื่อได้รับรายงานเหตุการณ์ภัยคุกคามระดับรุนแรง (Critical Incident) เช่น ข้อมูลผู้ป่วยรั่วไหลจำนวนมากหรือระบบบริการหลักหยุดทำงานเกินกว่า ๔ ชั่วโมง ให้ดำเนินการตามขั้นตอน ดังนี้

๑๐.๗.๑ ผู้อำนวยการในฐานะผู้บัญชาการเหตุการณ์ (Incident Commander) รับรายงานเบื้องต้นจาก CISO (Chief information security officer)

๑) การตัดสินใจ (Decision Point): ประเมินระดับความรุนแรงของสถานการณ์ระดับเฝ้าระวัง (แก้ไขได้ภายใน ๑-๒ ชม.): มอบหมายให้ CIO และทีมกู้คืนระบบสารสนเทศ (IT Disaster Recovery Team) ดำเนินการแก้ไข

ระดับวิกฤต (กระทบวงกว้าง/ข้อมูลรั่วไหล): สั่งการเปิดศูนย์บัญชาการเหตุการณ์ (War Room) ทันที

๑๐.๗.๒ การเปิดศูนย์บัญชาการเหตุการณ์ (Activate War Room)

๑) เรียกประชุมคณะทำงานฉุกเฉิน ประกอบด้วย: ผู้อำนวยการ, รองผู้อำนวยการฝ่ายการแพทย์, CIO, CISO, ทีมปฏิบัติการทางการแพทย์, ทีมกู้คืนระบบสารสนเทศ, ทีมตอบสนองเหตุการณ์ (CIRT), ทีมที่ปรึกษาทางกฎหมาย (นิติกร), ฝ่ายประสานงานนอกหน่วยงานภายนอก (Liaison), และทีมสื่อสารองค์กร (PR)

๒) การสั่งการ (Directive): ประกาศใช้แผนความต่อเนื่องทางธุรกิจ (BCP) เต็มรูปแบบ

๑๐.๗.๓ การสื่อสารภาวะวิกฤต (Crisis Communication):

๑) แต่งตั้ง "ผู้แถลงข่าว (Spokesperson)จากทีมสื่อสารองค์กร" เพียง ๑ ท่าน เพื่อให้ข้อมูลเป็นไปในทิศทางเดียว

๒) การร่างแถลงการณ์ (Statement Drafting): ยึดหลัก "ข้อเท็จจริง - การดำเนินการ - ความห่วงใย" (Fact - Action - Care)

ข้อเท็จจริง: ระบุสิ่งที่เกิดขึ้นอย่างกระชับ (เช่น ระบบขัดข้องชั่วคราว)

การดำเนินการ: ระบุมาตรการแก้ไขที่กำลังดำเนินอยู่ (เช่น ทีมกู้คืนระบบสารสนเทศกำลังกู้คืนระบบ)

ความห่วงใย: ยืนยันความพร้อมในการให้บริการผู้ป่วย (เช่น เปิดใช้ระบบสำรองเพื่อให้การรักษาต่อเนื่อง)

๑๐.๗.๔ การยุติสถานการณ์ (De-escalation):

๑) เมื่อได้รับรายงานยืนยันความพร้อมของระบบจาก CIO และทีมกู้คืนระบบสารสนเทศ

๒) ผู้อำนวยการสั่งการ "ยกเลิกภาวะฉุกเฉิน" และให้ทุกหน่วยงานกลับมาปฏิบัติงานผ่านระบบปกติ

๑๑.การทบทวนและติดตามการซ้อมแผนความต่อเนื่อง (Testing the Plan)

๑๑.๑ มีการทดสอบแผนบริหารความต่อเนื่องฯ บางส่วนหรือทั้งหมดเป็นประจำทุกปี เพื่อให้มั่นใจว่าหน่วยงานมีการเตรียมตัวและมีความสามารถในการกู้คืนระบบสำคัญภายในระยะเวลาที่กำหนดไว้

๑๑.๒ ทดสอบแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ โดยการสร้างสถานการณ์จำลอง (Simulation Exercises) เป็นประจำทุกปี โดยต้องมีการปรับเปลี่ยนหมุนเวียนสถานการณ์จำลอง เพื่อให้แน่ใจว่าได้มีการทดสอบความสูญเสีย/เสียหายของปัจจัยหลักที่เกี่ยวข้องทุก ๆ ๑ ปี

๑๑.๓ ข้อบกพร่องใด ๆ (GAP) ที่เกิดจากการทดสอบบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศจะต้องมีการติดตามให้เสร็จสิ้นภายใน ๓ เดือน นับตั้งแต่วันที่ทดสอบ ถ้าไม่สามารถดำเนินการติดตามได้ตามเวลาที่กำหนดให้หัวหน้าทีมบริหารและผู้ประสานงานความต่อเนื่องด้านเทคโนโลยีสารสนเทศได้แจ้งผู้บริหารระดับสูงเพื่อพิจารณาแนวทางแก้ไขข้อบกพร่องนั้น ๆ ให้หมดไปโดยเร็ว

การทบทวนการดำเนินงาน การจัดการกับเหตุการณ์เพื่อเตรียมการป้องกันของการเกิดเหตุในครั้งนี้ หรือจะต้องปรับปรุงอย่างไรต่อไป

๑๒.การรายงานผล บันทึกข้อความสรุปรายงาน มีเนื้อหาประเด็นดังนี้

- ระบุสาเหตุของเหตุการณ์ที่เกิดขึ้น
- ประเมินค่าความเสียหายที่เกิดขึ้น
- ประเมินผลกระทบต่อระบบสารสนเทศ
- ระบุแนวทางการดำเนินการแก้ไข เพื่อป้องกันการเกิดขึ้นซ้ำอีกของเหตุการณ์นี้ในอนาคต
- ประเมินความเหมาะสมในการตัดสินใจดำเนินการ เพื่อรับมือและจัดการกับเหตุที่เกิดขึ้น
- ประเมินความเหมาะสมด้านระยะเวลาในการแก้ไข กระบวนการสำคัญและระบบสำคัญ เพื่อให้กลับคืนมาให้บริการได้
- ประเมินความเหมาะสมด้านสิ่งต่าง ๆ ที่ได้เตรียมการไว้ก่อนล่วงหน้า
- ทบทวนจากข้อมูลที่บันทึกไว้ระหว่างการเกิดเหตุว่ามีสิ่งใดที่มองข้ามไป คาดการณ์ผิดหรือเป็นข้อบกพร่องที่ต้องแก้ไข
- ทบทวนแผนการบริหารจัดการกับเหตุการณ์ความมั่นคงปลอดภัยนี้ ควรปรับปรุงให้ครอบคลุมในจุดไหนมากขึ้น หรือเพื่อให้ใช้งานหรือรับมือในสถานการณ์ได้ดีขึ้น
- ทบทวนว่าจำเป็นต้องมีการอบรม ฝึกฝน หรือสร้างความตระหนักเพิ่มเติมหรือไม่
- ระบุสิ่งที่ต้องดำเนินการปรับปรุงหรือแก้ไขเพิ่มเติม เช่น นโยบายขั้นตอนการปฏิบัติหรืออื่นๆ

๑๓.แบบรายงานการทดสอบแผนความต่อเนื่อง (ทบทวนและติดตาม)

การซ้อมแผนความต่อเนื่อง BCP (Testing the Plan) โรงพยาบาลปราสาท

หน่วยงานที่ซ้อมแผน.....จำนวนเจ้าหน้าที่ในหน่วยงาน..... คน

๑๓.๑ รายงานการฝึกซ้อมแผน

๑) วันที่ทำการฝึกซ้อมแผน.....

๒) สถานที่ฝึกซ้อม.....

๓) จำนวนเจ้าหน้าที่ ที่เข้าร่วมฝึกซ้อมแผน.....คน

(ให้แนบรายชื่อผู้เข้าร่วมการฝึกซ้อมแผนในครั้งนี้มาด้วย)

๔) ผลการดำเนินการฝึกซ้อมแผน

.....

.....

.....

.....

.....

๕) ปัญหา / อุปสรรคในการดำเนินการฝึกซ้อม

.....

.....

.....

.....

.....

ลงชื่อ.....ผู้รายงาน

(นายเกียรติธนพัฒน์ มนตรี)

ตำแหน่งนักวิชาการคอมพิวเตอร์ชำนาญการ

..... ๒๖ ก.พ. ๒๕๖๐ ..... / .....

๑๔.แบบประเมิน Checklist ของการกู้คืนบริการระบบสารสนเทศ

ลำดับที่	งานที่ต้องดำเนินการปฏิบัติ	ขั้นตอนการปฏิบัติ	ระยะเวลาที่ใช้ในการดำเนินการ	ระยะเวลาที่ทำได้จริง	ลายมือชื่อผู้ดำเนินการ
ขั้นตอนที่ ๑	ประเมินสาเหตุของปัญหา				
ขั้นตอนที่ ๒	แนวทางการแก้ไข การสื่อสาร ประชาสัมพันธ์ รายงาน สถานการณ์				
ขั้นตอนที่ ๓	ประเมิน สถานการณ์ หลังจากการแก้ไข การเฝ้าระวัง ติดตามการ ดำเนินงานและการ รายงานผล				
ขั้นตอนที่ ๔	สรุปการแก้ไข ปัญหาและอุปสรรค ที่พบ รายงาน ผู้บังคับบัญชา				

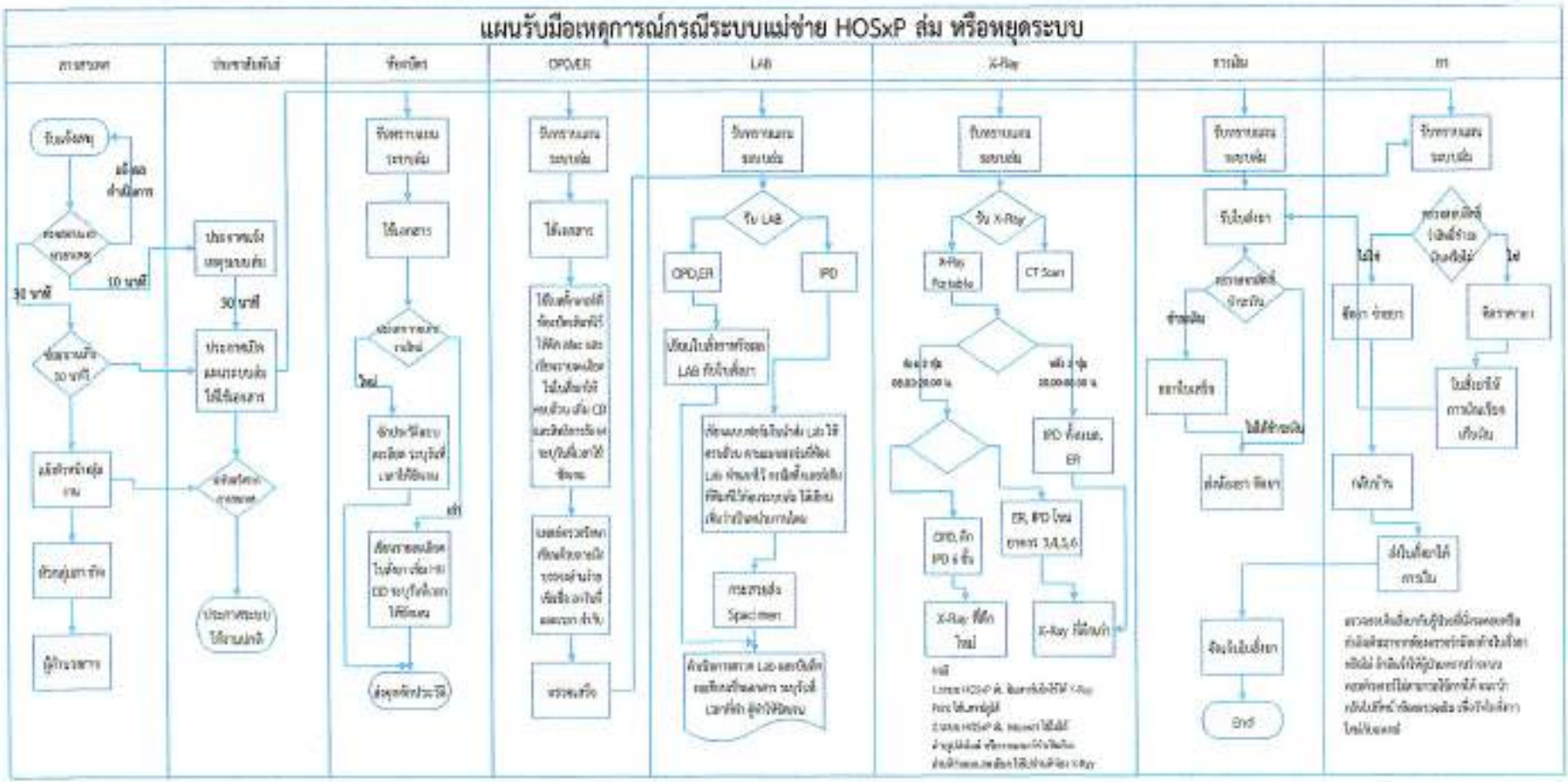
ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๑ มีนาคม พ.ศ. ๒๕๖๙ เป็นต้นไป

ประกาศ ณ วันที่ ๒๖ กุมภาพันธ์ พ.ศ. ๒๕๖๙

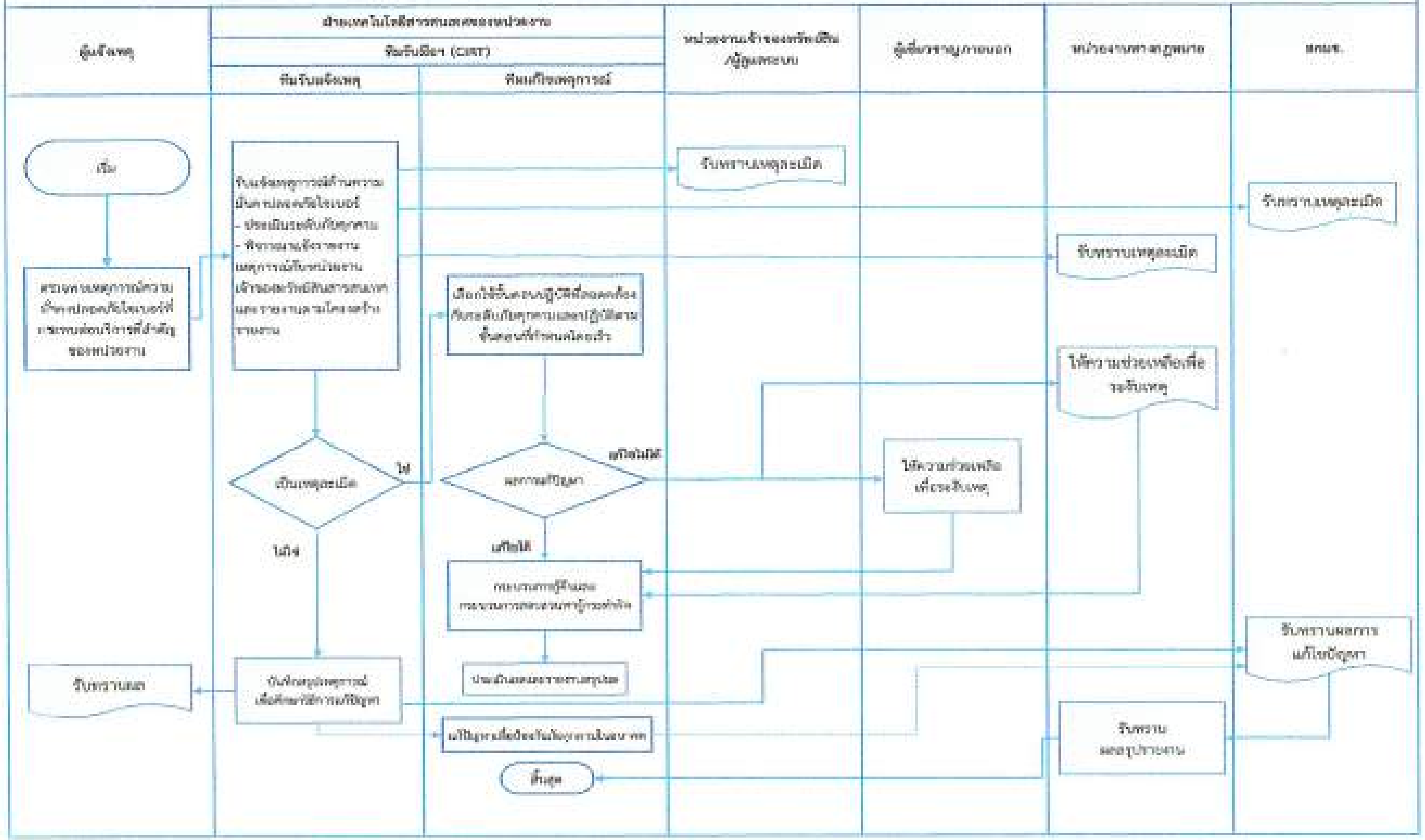
(นางสาวชูหงส์ มหรรทัศนพงศ์)
ผู้อำนวยการโรงพยาบาลปราสาท

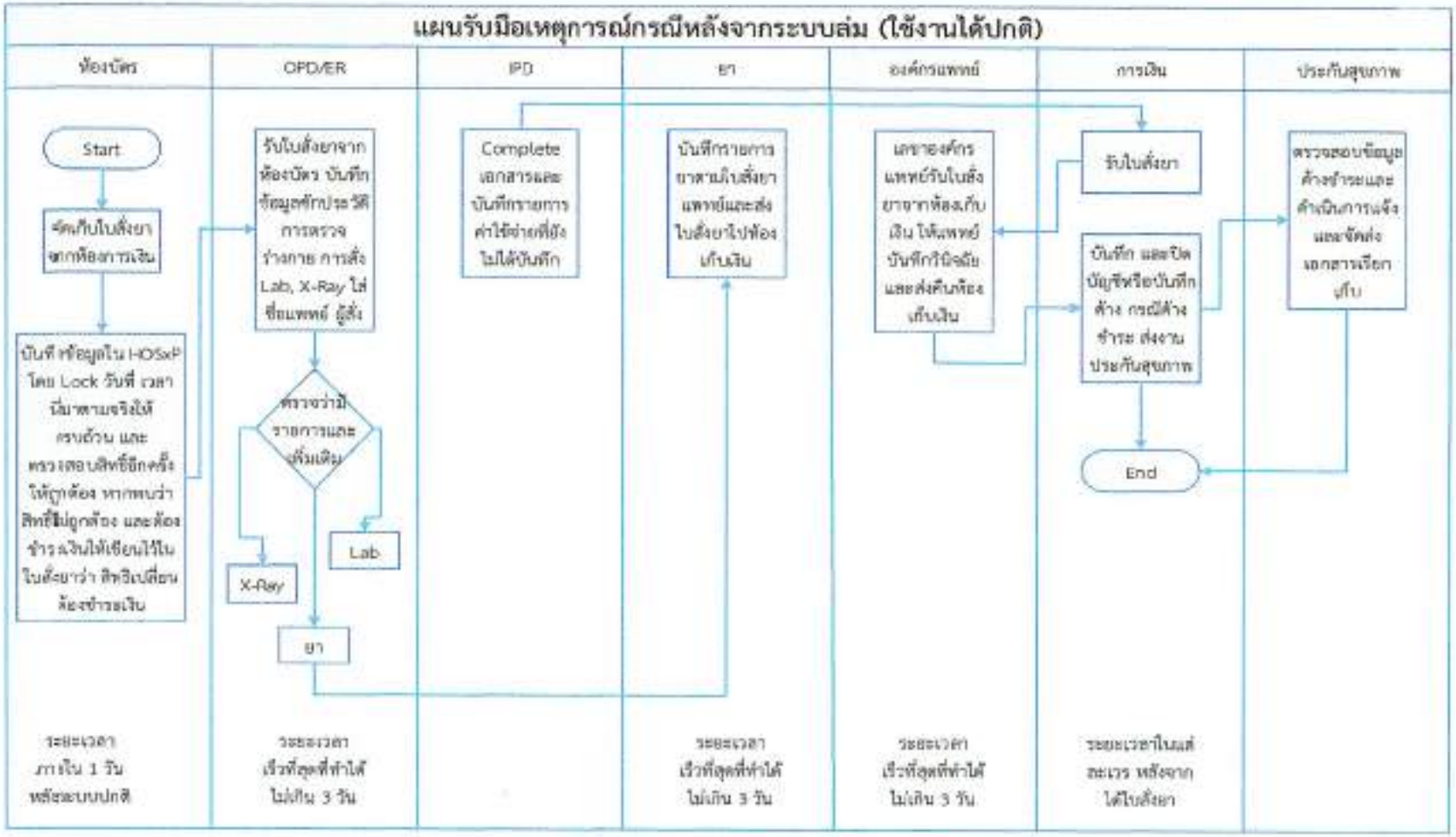
ภาคผนวก

ภาคผนวก ๑


แผนรับมือเหตุการณ์กรณีระบบแม่ข่าย HOSxP ล่ม หรือหยุดระบบ
ภาพรวม
ประชาสัมพันธ์
ห้องบัตร
OPD/ER
LAB
X-Ray
การเงิน
IPI

แผนรับมือเหตุการณ์กรณีภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)




แผนรับมือเหตุการณ์กรณีหลังจากระบบล่ม (ใช้งานได้ปกติ)
ห้องบัตร
OPD/ER
IPD
ยา
องค์กรแพทย์
การเงิน
ประกันสุขภาพ
Start
จัดเก็บใบสั่งยาจากห้องการเงิน
บันทึกข้อมูลใน HOSxP โดย Lock วันที่ เวลา นี่มาตามจริงให้ครบถ้วน และตรวจสอบสิทธิ์อีกครั้งให้ถูกต้อง หากพบว่าสิทธิ์ไม่ถูกต้อง และต้องชำระเงินให้เขียนไว้ในใบสั่งยาว่า สิทธิเปลี่ยน ต้องชำระเงิน
รับใบสั่งยาจากห้องบัตร บันทึกข้อมูลหัตถประวัติ การตรวจร่างกาย การสั่ง Lab, X-Ray ใส่ชื่อแพทย์ ผู้สั่ง
ตรวจว่ามีรายการและเพิ่มเติม
Lab
X-Ray
ยา
Complete เอกสารและบันทึกรายการค่าใช้จ่ายที่ยังไม่ได้บันทึก
บันทึกรายการยาตามใบสั่งยาแพทย์และส่งใบสั่งยาไปห้องเก็บเงิน
เลขาองค์กรแพทย์รับใบสั่งยาจากห้องเก็บเงิน ให้แพทย์บันทึกวินิจฉัย และส่งคืนห้องเก็บเงิน
รับใบสั่งยา
บันทึก และปิดบัญชีหรือบันทึกค้าง กรณีค้างชำระ ส่งงานประกันสุขภาพ
End
ตรวจสอบข้อมูลค้างชำระและดำเนินการเก็บและจัดส่งเอกสารเรียกเก็บ
ระยะเวลาภายใน 1 วัน หลังระบบปกติ
ระยะเวลาเร็วที่สุดที่ทำได้ไม่เกิน 3 วัน
ระยะเวลาเร็วที่สุดที่ทำได้ไม่เกิน 3 วัน
ระยะเวลาเร็วที่สุดที่ทำได้ไม่เกิน 3 วัน
ระยะเวลาในแต่ละเวร หลังจากได้ใบสั่งยา

ภาคผนวก ๒

ตัวอย่าง : บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

วันที่ :	เวลา :	ผู้บันทึกรายงาน : ติดต่อ :
วันและเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :		
ประเภทเหตุการณ์ :		
ระดับความรุนแรง :		
รายละเอียดเหตุการณ์ :		
ผลกระทบที่เกิดขึ้น :		
ความเสียหายที่เกิดขึ้น :		
การรายงานเหตุการณ์ :		
หน่วยงานที่ขอความช่วยเหลือ :		
การดำเนินการตอบสนองต่อเหตุการณ์ :		
รายละเอียดเพิ่มเติม :		
ผู้จัดการรับมือฯ เหตุการณ์ :		
ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ :		
วันและเวลาที่มีรายงานความคืบหน้าครั้งถัดไป :		

ภาคผนวก ๓

บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น (ข้อเท็จจริง, สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ)

ภาคผนวก ๔

เอกสาร กฉ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
๑. ข้อมูลการประสานงาน โรงพยาบาลปราสาทที่รับผิดชอบติดตามเหตุภัยคุกคาม วันที่และเวลาที่แจ้ง
๒. ด้านภารกิจหรือบริการของหน่วยงาน และโรงพยาบาลปราสาทที่เกิดเหตุภัยคุกคาม โรงพยาบาลปราสาทที่เกิดเหตุภัยคุกคาม ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม
๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล ..... ตำแหน่งงาน ..... โรงพยาบาลปราสาท อีเมล ..... โทรศัพท์ (ที่ทำงาน / มือถือ) .....
๔. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
๕. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ๔ ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ยังไม่สามารถระบุได้
๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ) หมวดหมู่* คำอธิบาย หมวดหมู่ที่ ๒ การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance) หมวดหมู่ที่ ๓ การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity) หมวดหมู่ที่ ๔ การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic) หมวดหมู่ที่ ๕ การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion) หมวดหมู่ที่ ๖ การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion) หมวดหมู่ที่ ๗ การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service) หมวดหมู่ที่ ๘ เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating) * อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑
หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ ..... หน่วยงานที่รับผิดชอบดิดตามเหตุภัยคุกคาม (ถ้ามี): โปรดระบุ ..... วันที่: เลือกวันที่ เวลา: โปรดระบุ .....
ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ โรงพยาบาลปราสาทที่เกิดเหตุภัยคุกคาม โรงพยาบาลปราสาทที่เกิดเหตุภัยคุกคาม: โปรดระบุ ..... ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ .....
ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ ..... โรงพยาบาลปราสาท: โปรดระบุ ..... อีเมล: โปรดระบุ ..... โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ .....
ก๓. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
ก๔. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน ☐ ใช่ ☐ ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์๕ ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ยังไม่สามารถระบุได้

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ ..... เวลา : โปรดระบุ .....

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ ..... เวลา : โปรดระบุ .....

ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว

ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน

ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง): โปรดระบุ .....

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ : โปรดระบุ .....

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน): โปรดระบุ .....

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่อง คอมพิวเตอร์): โปรดระบุรายละเอียด .....

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ .....

รายละเอียดอื่น ๆ: โปรดระบุ .....

หมวด ค: ข้อมูลการรับมือภัยคุกคาม

ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ

☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม

☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว

☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ .....

ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว

☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว

☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว

กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว

รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ

ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)

โปรดระบุ

ส่วนที่ ๒

หมวด ง: รายละเอียดภัยคุกคาม

ง๑. ข้อมูลการตรวจจับและการวิเคราะห์

ง๑.๑ วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (System Access)

วันที่: เลือกวันที่..... เวลา: โปรดระบุ..... ไม่ทราบ: ☐

ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของ ระบบ, ภัยธรรมชาติ, การจู่โจม, ความผิดพลาดจากคนนอกองค์กร): โปรดระบุ .....

บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ): โปรดระบุ .....

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด): โปรดระบุ .....

ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบบริการหรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ .....

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ .....

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย): .....

จำนวนบุคคลที่เป็นเจ้าของข้อมูล: โปรดระบุ ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

ข้อมูลทางการแพทย์

อื่น ๆ: โปรดระบุ .....

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ .....

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ .....

๑.๔ รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)

หมายเลข CVE: โปรดระบุ ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ .....

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น: โปรดระบุ .....

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ

บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุหรือบัญชีผู้ใช้มีความผิดปกติ

การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ

ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)

การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ

การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ

การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย

การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง

การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก

การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย

☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ

☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ

☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)

☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ

☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น

การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ

การตรวจพบโปรแกรมเจาะระบบ (Crack utility)

สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ .....

๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน

(เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ)

โปรดระบุ .....

๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ .....

๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ .....

๒.๒ การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ เวลา: โปรดระบุ .....

๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ .....

๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ .....

เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย	จำนวน
๐	เหตุการณ์จำลองและการฝึกซ้อมของหน่วยงาน (Training and Exercises)	
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	

ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

ทรัพย์สินที่ได้รับผลกระทบ	จำนวน
เครื่องแม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory)	
เครื่องเวิร์กสเตชัน (Workstation)	
สวิตช์ (Switch) /เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์

ระดับภัยคุกคาม	จำนวน
ไม่ร้ายแรง	
ร้ายแรง	
วิกฤต (ก)	
วิกฤต (ข)	

ภาคผนวก ๕

ตัวอย่าง: รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

รายการตรวจสอบการจัดการเหตุการณ์		Complete
ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
๑	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	
	๑.๑ วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์	
	๑.๒ ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน	
	๑.๓ ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่น ๆ เป็นต้น)	
	๑.๔ ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
๒	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
๓	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
๔	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
๕	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
๖	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
๗	ทำการกำจัดสาเหตุ (Eradicate the incident)	
	๗.๑ ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
	๗.๒ กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่นๆ	
	๗.๓ หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
๘	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
	๘.๑ ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
	๘.๒ ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	

๘	๘.๓ หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๙	จัดทำรายงานการติดตามผล	
๑๐	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	

เอกสาร ๑ ใบลงทะเบียนผู้ป่วยใหม่

แบบกรอกประวัติทำบัตรใหม่โรงพยาบาลปราสาท

ทำบัตรใหม่ (ไม่เคยมาโรงพยาบาลนี้) บัตรหาย/ลืมบัตร (เคยมาโรงพยาบาลนี้) HN.....

ชื่อ-สกุล นาย/นาง/นางสาว/ด.ญ./ด.ช. ..... วัน/เดือน/ปีเกิด.....อายุ.....ปี

หมายเลขบัตรประชาชน..... สถานภาพ โสด สมรส หย่าร้าง หม้าย สงฆ์

อาชีพ..... สัญชาติ ไทย กัมพูชา อื่นๆระบุ.....

เชื้อชาติ ไทย กัมพูชา อื่นๆระบุ..... ศาสนา พุทธ คริสต์ อิสลาม อื่นๆระบุ.....

ที่อยู่ตามทะเบียนบ้าน.....รหัสไปรษณีย์.....

สถานะตามทะเบียนบ้าน เจ้าบ้าน ผู้อาศัย เบอร์โทรศัพท์.....

วุฒิการศึกษา ประถมศึกษา ม.ต้น ม.ปลาย ปริญญาตรี ไม่ได้รับการศึกษา อื่นๆระบุ.....

ชื่อ-สกุล บิดา..... ชื่อ-สกุล มารดา.....

ชื่อ-สกุล คู่สมรส.....

ญาติที่สามารถติดต่อได้ ชื่อ-สกุล.....เกี่ยวข้องเป็น.....

ที่อยู่.....รหัสไปรษณีย์.....

เบอร์โทรศัพท์.....

แบบกรอกประวัติทำบัตรใหม่โรงพยาบาลปราสาท

ทำบัตรใหม่ (ไม่เคยมาโรงพยาบาลนี้) บัตรหาย/ลืมบัตร (เคยมาโรงพยาบาลนี้) HN.....

ชื่อ-สกุล นาย/นาง/นางสาว/ด.ญ./ด.ช. ..... วัน/เดือน/ปีเกิด.....อายุ.....ปี

หมายเลขบัตรประชาชน..... สถานภาพ โสด สมรส หย่าร้าง หม้าย สงฆ์

อาชีพ..... สัญชาติ ไทย กัมพูชา อื่นๆระบุ.....

เชื้อชาติ ไทย กัมพูชา อื่นๆระบุ..... ศาสนา พุทธ คริสต์ อิสลาม อื่นๆระบุ.....

ที่อยู่ตามทะเบียนบ้าน.....รหัสไปรษณีย์.....

สถานะตามทะเบียนบ้าน เจ้าบ้าน ผู้อาศัย เบอร์โทรศัพท์.....

วุฒิการศึกษา ประถมศึกษา ม.ต้น ม.ปลาย ปริญญาตรี ไม่ได้รับการศึกษา อื่นๆระบุ.....

ชื่อ-สกุล บิดา..... ชื่อ-สกุล มารดา.....

ชื่อ-สกุล คู่สมรส.....

ญาติที่สามารถติดต่อได้ ชื่อ-สกุล.....เกี่ยวข้องเป็น.....

ที่อยู่.....รหัสไปรษณีย์.....

เบอร์โทรศัพท์.....

เอกสาร ๒ ใบบันทึกการตรวจรักษาผู้ป่วยนอก ใบนำทาง และใบสั่งยา

แบบฟอร์มบันทึกการตรวจรักษาผู้ป่วยนอก (OPD Downtime Form)

โรงพยาบาลปราสาท จังหวัดสุรินทร์

(ใช้เมื่อระบบคอมพิวเตอร์ขัดข้อง หรือไม่สามารถเข้าถึงได้ชั่วคราว)

ส่วนที่ 1: ข้อมูลผู้ป่วยและสิทธิการรักษา (เจ้าหน้าที่ลงทะเบียน / พยาบาลจุดซักประวัติ)

วันที่: ____/____/_____ เวลาที่รับบริการ: ____:____ น. แผนก: _____

ชื่อ-นามสกุล: _____ อายุ: ____ ปี ____ เดือน

เพศ: [ ] ชาย [ ] หญิง

HN (เจ้าหน้าที่/ต้นสังกัดเดิม): _____

เลขบัตรประชาชน (13 หลัก): _____

สิทธิการรักษา: [ ] บัตรทอง (UC) [ ] เบิกจ่ายตรง (ข้าราชการ) [ ] ประกันสังคม

[ ] ชำระเงินเอง [ ] อื่นๆ _____

ประวัติการแพ้ยา/แพ้อาหาร (สำคัญมาก!!): [ ] ปฏิเสธการแพ้ [ ] เคยแพ้ ระบุ: _____

ส่วนที่ 2: การซักประวัติและสัญญาณชีพ (พยาบาล)

อาการสำคัญ (CC):

ประวัติปัจจุบัน (PI):

โรคประจำตัว (U/D):

Vital Signs:

T: _____ °C	PR: _____ /min	RR: _____ /min	BP: ____/____ mmHg	SpO2: _____ %

BW: _____ kg Height: _____ cm Pain Score (0-10): _____

ลงชื่อพยาบาลผู้ซักประวัติ: _____ (_____)

ส่วนที่ 3: บันทึกการตรวจรักษา (แพทย์)

Physical Exam (PE):

Diagnosis (การวินิจฉัยโรค):

1. _____ (ICD-10 ถ้ามีเวลา: _____)

เอกสาร ๒ ใบบันทึกการตรวจรักษาผู้ป่วยนอก ใบนำทาง และใบสั่งยา (ต่อ)

2. _____ (ICD-10 ถ้าทราบ: _____)

Treatment / Order (คำสั่งการรักษา):

[ ] Lab (เจาะเลือด/ตรวจปัสสาวะ): _____

[ ] X-Ray / Imaging: _____

[ ] Procedure (หัตถการ): _____

Medication (รายการยา):

ลำดับ	ชื่อยา	วิธีใช้	จำนวน
1.			
2.			
3.			
4.			

Disposition (การจำหน่าย):

[ ] รับยา - กลับบ้าน

[ ] นัดหมายครั้งต่อไป วันที่: ___/___/_____ เพื่อ: _____

[ ] รับไว้รักษาในโรงพยาบาล (Admit) แผนก/Ward: _____

[ ] ส่งต่อ (Refer) ไป รพ.: _____

ลงชื่อแพทย์ผู้ตรวจ: _____ (_____) โบนัสกอบวิชาชีพ: _____

ส่วนที่ 4: การเงินและห้องยา (สำหรับคิดค่าใช้จ่าย)

ค่าบริการทางการแพทย์ / หัตถการ	_____ บาท
ค่าเวชภัณฑ์ / อุปกรณ์	_____ บาท
ค่ายา	_____ บาท

[ ] ชำระเงินเรียบร้อย [ ] ค้างชำระ (เหตุผลเงิน/รอบบัตรเดือน) [ ] รอเรียกเก็บตามสิทธิ

ลงชื่อเจ้าหน้าที่การเงิน: _____	ลงชื่อเภสัชกรผู้จ่ายยา: _____

ส่วนที่ 5: ส่วนควบคุมข้อมูล (Data Recovery Tracking) - สำคัญมากสำหรับการกู้คืน

เมื่อระบบ HIS กลับมาใช้งานได้ตามปกติ ให้เจ้าหน้าที่นำข้อมูลในนี้ดีกลับเข้าระบบ (Backlog Data Entry)

[ ] บันทึกข้อมูลเข้าระบบ HIS เรียบร้อยแล้ว

Visit Number (VN) ที่ได้รับจากระบบ: _____

ผู้บันทึกข้อมูล: _____ วันที่บันทึก: ___/___/_____ เวลา: ___:___ น.

เอกสาร ๓ แบบแสดงความยินยอมผ่าตัด

หนังสือแสดงคำยินยอมรับการผ่าตัด
โรงพยาบาลปราสาท อ.ปราสาท จ.สุรินทร์

วันที่.....พ.ศ.....เวลา.....น.

1. ข้าพเจ้า นาย / นาง / นางสาว.....นามสกุล.....
บ้านเลขที่.....เบอร์โทรศัพท์.....
ขอให้คำยินยอมในฐานะ ☐ ผู้ป่วย
☐ ผู้มีอำนาจกระทำแทนผู้ป่วยเกี่ยวข้องเป็น.....
ผู้ป่วยชื่อ นาย / นาง / นางสาว / ด.ช. / ด.ญ. .....นามสกุล.....
ขอให้คำยินยอมแสดงความรู้สึกโดยสมัครใจให้แพทย์ผู้รักษา ชื่อ..... และ

2. แพทย์ของท่านได้ให้ความเห็นว่าควร ทำการผ่าตัด / หัตถการ (ชื่อการผ่าตัด/หัตถการ)
.....

3. แพทย์ผู้ทำการผ่าตัดได้อธิบายถึงข้อบ่งชี้ วิธีการและขั้นตอนการผ่าตัด ประโยชน์ที่คาดว่าจะได้รับ ทางเลือกอื่นๆ ในการรักษา
ข้อดี คือ .....
ข้อเสีย คือ .....
โดยมีความเสี่ยง / ผลแทรกซ้อนที่เกิดจากการผ่าตัดที่สำคัญ

4. ทีมให้การระงับความรู้สึกได้อธิบายถึงข้อบ่งชี้ วิธีการและขั้นตอนการให้การระงับความรู้สึก วิธีการระงับความรู้สึกและการปฏิบัติตัวทั้งก่อนการระงับความรู้สึก ระยะหลังการระงับความรู้สึก ตลอดจนทางเลือกอื่นๆ ในการระงับความรู้สึก ซึ่งจะทำการระงับความรู้สึกแบบ ☐ การดมยาสลบ ☐ การฉีดยาชาเฉพาะที่ร่วมกับยากล่อมประสาท ☐ การฉีดยาชาเฉพาะที่
โดยมีความเสี่ยงและผลแทรกซ้อนที่สำคัญจากการระงับความรู้สึกเพื่อการผ่าตัด คือ 1.)แพ้ยา 2.)ฟันหลอดลมช้ำ 3.)อุบัติเหตุขณะ
4.)ให้น้ำยาคลายกล้ามเนื้อ 5.)ตื่นไม่รู้ตัว/ฝันร้าย 6.)หนาวสั่น 7.)เจ็บคอ/เสียงแหบ 8.)คลื่นไส้อาเจียน 9.)ปวดโยก/ฟันหัก 10.)เกิดแผลบริเวณริมฝีปาก และ/หรือบริเวณอื่น 11.)ปวดศีรษะ 12.)ปวดหลัง 13.)พักต่อที่หอผู้ป่วยหนัก ICU เพื่อสังเกตอาการ

5. ข้าพเจ้าเข้าใจดีว่า คำยินยอมนี้ครอบคลุมถึงการกระทำต่างๆ อันเป็นขอการผ่าตัด การพิจารณาเปลี่ยนแปลงการระงับความรู้สึก การให้เลือด และอื่นๆ ของแพทย์ที่ทำการรักษา เพื่อประโยชน์ในการรักษา และ/หรือช่วยชีวิตผู้ป่วยไว้

6. ข้าพเจ้ายินยอมให้โรงพยาบาลปราสาท จัดการตามวิธีการแพทย์กับเนื้อเยื่อ ชิ้นส่วนของร่างกาย หรืออวัยวะที่ถูกตัดออกจากร่างกายของผู้ป่วย จากการตรวจรักษา และ / หรือผ่าตัด

ลงชื่อ.....ผู้อธิบาย
(.....)
แพทย์ผู้ทำการผ่าตัด

ลายนิ้วชี้ขวาหรือซ้าย
ของผู้ให้ความยินยอม

ลงชื่อ.....
(.....)
เกี่ยวข้องเป็น.....
พยานคนที่ 1

ลงชื่อ.....ผู้อธิบาย
(.....)
วิสัญญีแพทย์ / วิสัญญีพยาบาล
ผู้ให้การระงับความรู้สึก

ลงชื่อ.....
(.....)
ผู้ให้ความยินยอม

ลงชื่อ.....
(.....)
ตำแหน่ง.....
พยานคนที่ 2

เอกสาร ๔ แบบแสดงความยินยอมการตรวจรักษา

[illegible]

โรงพยาบาล[illegible]

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

1. ข้าพเจ้า..............................นามสกุล..............................
บ้านเลขที่..............................เบอร์โทรศัพท์..............................

ขอให้คำยินยอมในฐานะ ( ) ผู้ป่วย
( ) ผู้มีอำนาจกระทำการแทนผู้ป่วยเกี่ยวข้องเป็น..............................

ผู้ป่วยชื่อ..............................นามสกุล..............................
ขอให้คำยินยอมและอนุญาตโดยสมัครใจให้แพทย์ผู้รักษาชื่อ..............................
และคณะแพทย์ของท่าน ทำการรักษาพยาบาล ....
[illegible] คือ ....
โดยใช้วิธี ( ) รักษาตามอาการ ( ) รักษาโดยการใช้ยา ( ) รักษาโดยการผ่าตัด ( ) อื่นๆ..............................
ข้อดี คือ ....
ข้อเสีย คือ ....
ภาวะแทรกซ้อน ....
โดยคาดว่าจะนอนโรงพยาบาลประมาณ .... วัน

2. แพทย์ผู้รักษาได้อธิบายตามหลักวิชาการ และมาตรฐานของแพทย์แผนปัจจุบัน ข้าพเจ้าเข้าใจดีว่า คำยินยอมนี้ครอบคลุมถึงการกระทำ[illegible]ในการรักษาพยาบาล รวมทั้งการให้เลือด และอื่นๆของคณะแพทย์เพื่อประโยชน์ในการรักษาและ / หรือช่วยชีวิตผู้ป่วยได้
3. ข้าพเจ้าได้รับฟังคำอธิบายจนเข้าใจ [illegible]เพื่อเป็นหลักฐาน

ลงชื่อ ....ผู้ให้คำอธิบาย
(..............................)
ตำแหน่ง..............................
ลงชื่อ..............................ผู้ให้ความยินยอม
(..............................)
ชื่อ..............................พยานคนที่ 1
(..............................)
เกี่ยวข้องเป็น..............................
ชื่อ..............................พยานคนที่ 2
(..............................)
ตำแหน่ง..............................

ลายพิมพ์นิ้วหัวแม่มือขวา
ของผู้ให้ความยินยอม
(..............................)

FM-[illegible] แก้ไขครั้งที่ [illegible] ประกาศใช้ [illegible] พฤศจิกายน [illegible]

เอกสาร ๕ ใบส่งตรวจห้องปฏิบัติการ (LAB)

PSH PRASAT

ใบส่งตรวจและรายงานผลทางห้องปฏิบัติการ (Lab [illegible] Form)
โรงพยาบาลปราสาท จังหวัดสุรินทร์
(ใช้เฉพาะกรณีระบบสารสนเทศ [illegible] ขัดข้องเท่านั้น)

ส่วนที่ ๑ ข้อมูลผู้ป่วยและคำสั่งตรวจ (กรอกโดย แพทย์/พยาบาล ผู้สั่งตรวจ)

ความเร่งด่วน [ ] ด่วนมาก STAT [ ] [illegible] [ ] [illegible] [ ] ทั่วไป Routine

วันที่สั่งตรวจ ...... เวลา ...... น.

ชื่อ-นามสกุลผู้ป่วย ...... อายุ ...... ปี เพศ [ ] ชาย [ ] หญิง

HN ...... [illegible] ......

การวินิจฉัยโรคเบื้องต้น Dx ......

รายการที่ต้องการส่งตรวจ กรุณาทำเครื่องหมาย ✓ และระบุรายละเอียด

[illegible]

ลงชื่อผู้เจาะเก็บสิ่งส่งตรวจ ...... เวลาที่เก็บ ...... น.

ลงชื่อแพทย์ผู้สั่งตรวจ ......

ส่วนที่ ๒ การรับสิ่งส่งตรวจ (กรอกโดย เจ้าหน้าที่ห้องปฏิบัติการ)

สภาพสิ่งส่งตรวจ [ ] สมบูรณ์ [ ] ปฏิเสธการรับ Reject สาเหตุ ......

ลงชื่อผู้รับสิ่งส่งตรวจ ...... วันที่รับ ...... เวลารับ ...... น.

ส่วนที่ ๓ รายงานผลการตรวจวิเคราะห์ (กรอกโดย เจ้าหน้าที่ห้องปฏิบัติการ)

รายการตรวจ (Test)	ผลการตรวจ (Result)	หน่วย (Unit)	ค่าอ้างอิง (Reference Range)
1			
2			
3			
4			
5			

[ ] [illegible] ให้แนบ [illegible] หรือ [illegible] พร้อมเซ็นชื่อกำกับ

[ ] [illegible]

รายละเอียด [illegible]

[illegible] ...... ผู้รับสาย/แจ้ง ...... เวลาที่แจ้ง ...... น.

[illegible] ...... [illegible] แล้ว

ลงชื่อผู้ทำการตรวจ/รายงานผล ...... เวลาที่รายงานผล ...... น.

ลงชื่อผู้ตรวจสอบ [illegible] ......

ส่วนที่ ๔ การบันทึกข้อมูล [illegible] สำหรับหลังจากระบบกลับมาใช้งานได้

[ ] บันทึกข้อมูลลงระบบ [illegible] เรียบร้อยแล้ว [illegible]

เลขที่ใบสั่ง [illegible] ในระบบ ......

ผู้บันทึกข้อมูล ...... วันที่บันทึก ...... เวลา ...... น.

เอกสาร ๖ ใบส่งตรวจทางรังสีวินิจฉัย (X-RAY)

Request Form of Radiology Prasat Hospital

งานรังสีวิทยา โรงพยาบาลปราสาท จังหวัดสุรินทร์

ชื่อผู้ป่วย.....อายุ .....ปี HN.....☐ OPD / ☐ Ward.....

เบอร์โทรศัพท์ผู้ป่วยที่สามารถติดต่อได้.....

วันที่ส่งนัด.....เวลา.....น.

☐ นัดตามปกติ ☐ ขอด่วน

วันที่นัดตรวจU/S.....เวลา.....น.
(เจ้าหน้าที่ของแผนกฯเป็นผู้กรอก)

Request For	☐ ส่งข้อมูลภาพเอกซเรย์ (Refer) ☐ ขอข้อมูลภาพเอกซเรย์ จากโรงพยาบาลสุรินทร์	
	☐ นำภาพเอกซเรย์จากโรงพยาบาลอื่นลงในระบบ PACS (ไม่ได้ report ผลอ่าน)	
	☐ ผลอ่าน plain film.....ของวันที่.....	
	☐ IVP (Intravenous Pyelography)	
	☐ Ultrasound	Part to be Examined ☐ Upper Abdomen ☐ Neck / Thyroid ☐ Lower Abdomen ☐ Brain ☐ KUB ☐ Doppler..... ☐ Breast ☐ อื่นๆ.....
Clinical Diagnosis		
Clinical Information		
นัดฟังผล	☐ วันที่.....เวลา.....น.	

Request by Dr.....

เบอร์โทรศัพท์แพทย์.....

หมายเหตุ : หากมีข้อสงสัย กรุณาติดต่องานรังสีวิทยา โทร.044-56 1295 ต่อ 1289

FM-XRn-007ประกาศใช้วันที่ สิงหาคม 2559
แก้ไขวันที่ 1 มิถุนายน 2562

เอกสาร ๗ ใบส่งตรวจทางรังสีวินิจฉัย (CT)

โรงพยาบาลปราสาท
TOMOGRAPH.CO.,LTD
• PRASAT HOSPITAL

CT Scan Center

Request for: Emergency Urgency Non Urgency Follow up

HEAD & NECK

BODY

CTA

BONE & MUSCULOSKELETAL

CONTRAST MEDIA

ข้อควรระวังในการตรวจ

Clinic history

Referring physician

เอกสาร ๗ ใบส่งตรวจทางรังสีวินิจฉัย (CT) (ต่อ)

ศูนย์ตรวจเอกซเรย์คอมพิวเตอร์ความเร็วสูง โรงพยาบาลปราสาท

เลขที่ 602 หมู่ที่ 2 ถ.โชคชัย-เดชอุดม ตำบลกังแอน อำเภอปราสาท จังหวัดสุรินทร์ 32140 โทร.094-573-0988

CT. Scan Center

Tomograph co.,ltd.

ให้บริการตรวจวินิจฉัยโรค
ด้วยเครื่องเอกซเรย์คอมพิวเตอร์ ความเร็วสูง

เทคโนโลยีทันสมัยที่สุด
[illegible]

ดำเนินการโดย
บริษัท โทโมกราฟ จำกัด
[illegible]

ข้าราชการเบิกคืนได้เต็ม
[illegible]

ติดต่อสอบถามและยื่นใบส่งตรวจโดยตรงได้ที่
ศูนย์เอกซเรย์คอมพิวเตอร์ความเร็วสูง โรงพยาบาลปราสาท

เปิดให้บริการตลอด 24 ชม.
ทุกวันไม่เว้นวันหยุดราชการ
www.simahealthcare.com

Performance Check List (PCL)

สำหรับเตรียมผู้ป่วยที่จะได้รับการฉีดสารทึบรังสี

ชื่อผู้ป่วย .... ชื่อผู้ป่วย ....
HN .... อายุ ....ปี เพศ ....
ผลSerum Cr .... Bun .... eGFR .... (ผลตรวจวันที่) ....

ประวัติการแพ้	ใช่	ไม่ใช่
1. ประวัติการแพ้อาหารทะเล	☐	☐
2. ประวัติการแพ้สารทึบรังสี	☐	☐
3. โรคประจำตัวเช่น โรคหอบหืด โรคไต [illegible]	☐	☐
4. ตั้งครรภ์ (กรณีผู้ป่วยหญิง)	☐	☐
5. งดน้ำ งดอาหาร 4-6 ชั่วโมง	☐	☐

ปริมาณยา .... เวลาที่ฉีด ....

ลงชื่อ .... ผู้คัดกรอง

หนังสือแสดงความยินยอมรับการตรวจด้วยสารรังสี

วันที่ .... เดือน .... พ.ศ. ....

[illegible]

หมายเหตุ : [illegible]

[illegible]

ลงชื่อ .... ผู้ให้ความยินยอม (........................)

ลงชื่อ .... ผู้ให้ความยินยอม (........................)

(กรณีผู้ป่วยไม่อยู่ในสภาพให้ความยินยอมเองได้หรือเป็นผู้เยาว์)

ลงชื่อ .... ผู้ให้ข้อมูล (........................)

หนังสือฉบับนี้ ข้าพเจ้า .... หรือผู้มีอำนาจ .... (ความสัมพันธ์กับผู้ป่วย ....) ได้รับทราบเกี่ยวกับการรักษาและได้พิจารณาโดยละเอียดดีแล้ว [illegible]

ลงชื่อ .... ผู้ปฏิเสธความยินยอม (........................)

ลงชื่อ .... ผู้มีอำนาจ (........................)

ลงชื่อ .... พยาน (........................)

เอกสาร ๘ ใบนัดผู้ป่วย

ใบนัดหมายผู้ป่วย (Manual Appointment Slip)
โรงพยาบาลปราสาท จังหวัดสุรินทร์
(กรณีระบบอาจขัดข้อง)

ชื่อ-นามสกุล ผู้ป่วย: .....
HN: ..... เบอร์โทรศัพท์ติดต่อ: .....

ข้อมูลการนัดหมาย
นัดตามแพทย์ / คลินิก: .....
วันที่นัด: ..... เวลา ..... น.
ห้องตรวจ: .....

เพื่อ (กรุณาเขียนที่นัด):
( ) ตรวจรักษาตามอาการ ( ) ฟังผลเลือด/ผลตรวจ ( ) ทำหัตถการ ( ) อื่นๆ .....
การเตรียมตัวก่อนมาโรงพยาบาล
( ) ไม่ต้องงดน้ำงดอาหาร
( ) งดน้ำ และอาหารอย่างน้อย ..... ชั่วโมง (ตั้งแต่เวลา ..... น.)
( ) นำยาเดิมที่รับประทานอยู่มาด้วยทุกครั้ง
( ) อื่นๆ .....

ผู้ลงนามนัด: ..... วันที่ออกใบนัด: .....
หมายเหตุสำหรับเจ้าหน้าที่: กรุณาบันทึกข้อมูลการนัดหมายนี้ลงในระบบ (Computer) ของโรงพยาบาล เพื่อป้องกันปัญหาระบบขัดข้องในครั้งถัดไป

เอกสาร ๙ แบบบันทึกคำสั่งแพทย์ (ผู้ป่วยใน) แบบบันทึกประวัติและการตรวจวินิจฉัย (admission form)

Prasat Hospital
Doctor order Sheet

เอกสาร ๑๐ ระบบ MOPH PHR Viewer

https://phr๑.moph.go.th/phr/