	ระเบียบปฏิบัติ : การปฏิบัติกรณีเครื่องคอมพิวเตอร์แม่ข่าย Server/Database มีปัญหา	หน่วยงาน:ศูนย์คอมพิวเตอร์ หน้าที่ 1 - 2
	ผู้อนุมัติ **รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลโป่งน้ำร้อน**	แก้ไขครั้งที่ 2 ลงวันที่ 10 ม.ค. 64

1. กรณีเครื่องคอมพิวเตอร์แม่ข่าย Server /Database มีปัญหา สามารถแก้ไขได้ภายใน 30 นาที

เจ้าหน้าที่ศูนย์คอมพิวเตอร์

- ตรวจสอบสาเหตุของปัญหาและประเมินระยะเวลาในการแกไข หาก สามารถแกไขไดภายในเวลา 30 นาที ดำเนินการแจ้งประกาศผ่านช่องทางไลน์กลุ่มโรงพยาบาลและประสานฝ่ายประชาสัมพันธ์ประกาศผ่านสื่อเสียงตามสายให้ทุกหน่วยงานหยุดการใช้งานโปรแกรม HOSxP ชั่วคราว
- ดำเนินการแกไข ตรวจสอบความพร้อมให้เรียบร้อย
- ประกาศให้ทุกหน่วยงานสามารถใช้งาน HOSxP ไดตามปกติ
- สรุปสาเหตุของปัญหา และลงบันทึกในโปรแกรมความเสี่ยง

เจาหน้าที่หน่วยงานต่างๆ

- เมื่อไดรับแจ้งจากศูนย์คอมพิวเตอร์ ให้หยุดการใช้งานคอมพิวเตอร์และโปรแกรม HOSxP ชั่วคราว
- ประชาสัมพันธ์ให้ประชาชนที่รอรับบริการทราบ และจัดบริการที่สามารถทำไดโดยบันทึกลงในแบบฟอร์มใบสั่งยาชั่วคราวและเก็บเอกสารเพื่อรอลงบันทึกในภายหลังหรือจากระบบกลับมาใช้งานได้ปกติ
- เมื่อไดรับแจ้งให้ใช้งานคอมพิวเตอร์ไดตามปกติ ให้เริ่มนำข้อมูลบริการลงบันทึกในโปรแกรม HOSxP

2. กรณีเครื่อง Server /Database มีปัญหา ไมสามารถแกไขไดภายใน 30 นาที

เจาหน้าที่ศูนย์คอมพิวเตอร์

- เจ้าหน้าที่ศูนย์คอมพิวเตอร์ตรวจสอบสาเหตุของปัญหาและประเมินระยะเวลาในการแก้ไข หากไม่สามารถแก้ไขไดภายใน 30นาที ให้แจ้งผู้อำนวยการ/ประธานคณะกรรมการสารสนเทศทราบ
- ประธาน คณะกรรมการสารสนเทศ เจ้าหน้าที่งานศูนย์คอมพิวเตอร์ประกาศใช้แผนฉุกเฉินกรณีระบบเครือข่ายใช้งานไม่ได้ โดยใช้มาตรการเดียวกับกรณีไฟฟ้าดับมากกว่า 30 นาที ให้ทุกหน่วยงานหยุดการใช้งานโปรแกรม HOSxP
- จุดบริการผู้ป่วยนอกจัดบริการที่สามารถทำได้โดยใช้แบบฟอร์มOPD CARD แบบบันทึกเวชระเบียนผู้ป่วยนอก และแบบฟอร์มใบสั่งยาชั่วคราวและเก็บเอกสารเพื่อรอลงบันทึกในภายหลังหรือจากระบบกลับมาใช้งานได้ปกติ
- ศูนย์คอมพิวเตอร์ดำเนินการแกไขปัญหา Server DataBase ให้สามารถใช้งานไดตามปกติภายในเวลา 24 ช.ม.
- ประสานผู้เกี่ยวข้องเพื่อทำการลงบันทึกข้อมูลในโปรแกรม HOSxP ย้อนหลัง

	ระเบียบปฏิบัติ : การปฏิบัติกรณีเครื่องคอมพิวเตอร์แม่ข่าย Server/Database มีปัญหา	หน่วยงาน:ศูนย์คอมพิวเตอร์ หน้าที่ 2 - 2
		แก้ไขครั้งที่ 2 ลงวันที่ 10 ม.ค. 64

- ตรวจสอบความเรียบร้อยของ Server DataBase และอุปกรณ์เครือข่าย เมื่อเครื่อง Server สามารถทำงานได้ตามปกติ ให้ประกาศแจ้งให้หน่วยงานต่างๆ เปิดคอมพิวเตอร์ใช้งาน HOSxP และเริ่มบันทึกข้อมูลย้อนหลัง

แบบฟอร์ม OPD CARD และ แบบบันทึกเวชระเบียนผู้ป่วยนอก

OPD CARD

โรงพยาบาลโป่งน้ำร้อน จังหวัดจันทบุรี (PONGNAMRON HOSPITAL CHANTABURI)

ชื่อ-สกุล.....นามสกุล.....ชื่อกลาง.....HN.....

วดป. ที่มารับบริการ..... เพศ ○ ชาย ○ หญิง วันเกิด...../...../..... อายุ.....ปี

สถานะภาพ ○ โสด ○ คู่ ○ หม้าย ○ หย่า ○ ร้าง ○ สมณะ อาชีพ.....

ภาษา.....เชื้อชาติ.....สัญชาติ.....ศาสนา.....

หมู่เลือด A B AB O ไม่ทราบ RH.....แพ้ยา.....ชื่อเล่น.....

เลขที่บัตรประชาชน _ - _ _ _ _ - _ _ _ _ _ - _ _ - _ เลขต่างด้าว _ _ - _ _ _ _ - _ _ _ _ _ - _

บ้านเลขที่..... .....หมู่.....ตรอก / ซอย / ถนน..... จังหวัด.....

อำเภอ.....ตำบล.....ประเทศ.....รหัสไปรษณีย์.....

○ อยู่ในเขตรับผิดชอบ ○ อยู่ในเขต CUP หมายเลขโทรศัพท์.....

สังกัดหลัก..... สังกัดรอง.....

เลขที่ ขรก. ..... เลขที่ กบก. ..... Passport.....

ข้อมูลนายจ้าง ชื่อ-นามสกุล..... ○ บุคคล ○ บริษัท หมายเลขโทรศัพท์.....

หน่วยขึ้นทะเบียน..... CID _ - _ _ _ _ - _ _ _ _ _ - _ _ - _

ผู้ที่สามารถติดต่อได้..... HN มารดา.....

ที่อยู่ผู้ติดต่อ.....

ความสัมพันธ์กับผู้ป่วย.....หมายเลขโทรศัพท์.....

บิดา.....นามสกุล.....CID _ - _ _ _ _ - _ _ _ _ _ - _ _ - _

มารดา.....นามสกุล.....CID _ - _ _ _ _ - _ _ _ _ _ - _ _ - _

ชื่อคู่สมรส.....นามสกุล..... CID _ - _ _ _ _ - _ _ _ _ _ - _ _ -

E-mail.....ที่ทำงาน.....

สถานะครอบครัว.....สถานะบุคคล.....การศึกษา.....

ประเภทบุคคล.....ตำแหน่งในชุมชน.....น้ำหนักแรกเกิด.....

แพทย์ประจำตัว..... ○ เป็นบุคลากรในโรงพยาบาล clinic.....

หมายเหตุ.....

.....

.....

.....

.....

.....

.....

.....

แบบบันทึกเวชระเบียนผู้ป่วยนอก

โรงพยาบาลโป่งน้ำร้อน จังหวัดจันทบุรี (PONGNAMRON HOSPITAL CHANTABURI)

ชื่อ-สกุล.....อายุ.....ปี วันที่รับบริการ.....HN.....

เลขบัตรประชาชน _ - ____ - _____ - __ - _ สิทธิ์การรักษา.....

V/S : นน.....kg. สูง.....Cm. T = ...°c P = .../m R = .../m BP .....mmHg.

OPD เวลา.....น. ผู้ป่วยเดินมาเอง ผู้ป่วยให้ประวัติว่า CC.....

PI.....

.....

.....

* รับประทานอาหารได้ ขับถ่ายปกติ นอนหลับพักผ่อนได้ *ประวัติการรักษาที่ได้รับมาแล้ว.....

Repeat BP ครั้งที่ 1 เวลา.....น. =.....mmHg. ครั้งที่ 2 เวลา.....น. =.....mmHg. Repeat T ซ้ำ เวลา.....น. = ...°c

ให้ผู้ป่วยรับประทานยา Paracetamol (.....mg.).....tab / Paracetamol Syr. .....ช้อนชา เวลา.....น.

ส่ง Tepid Sponge เวลา.....น. TT แขนซ้าย..... = ... ให้ผู้ป่วยผูก Mask และ Isolate .....

HPI ประเมินสภาพจิตใจ และเปิดโอกาสให้ผู้ป่วยและ.....ซักถาม เพื่อลดความวิตกกังวลเกี่ยวกับการเจ็บป่วย : ผู้ป่วยและ.....คลายความวิตกกังวล

PMH ปฏิเสธโรคประจำตัว * ไม่เคยได้รับการผ่าตัดใด ๆ * ได้รับวัคซีนครบตามเกณฑ์อายุ * มีการเจริญเติบโต และพัฒนาการปกติ * ประวัติประจำเดือน

LMP..... ไม่มีประวัติการแพ้ยาและประวัติการแพ้อื่นๆ ปฏิเสธการใช้สารเสพติด การดื่มสุราและสูบบุหรี่ของคนในครอบครัว.....

FH ไม่มีบุคคลในครอบครัวเจ็บป่วยด้วยอาการนี้ บิดามารดาไม่มีประวัติเป็นโรค HT / DM / DLP / Stroke / COPD / Asthma.....

SH ประเมินภาวะเศรษฐกิจสังคม ไม่มีปัญหาด้านเศรษฐกิจเมื่อเจ็บป่วย ไม่มีเพื่อนบ้านเจ็บป่วยด้วยอาการนี้ ไม่มีสภาพแวดล้อมที่เอื้อให้เกิดอาการนี้

*.....พยาบาลวิชาชีพชำนาญการ ผู้ซักประวัติ / .....พนักงานช่วยเหลือคนไข้ ผู้บันทึก

คำแนะนำ ให้คำแนะนำผู้ป่วยและ.....เกี่ยวกับการเจ็บป่วยและการปฏิบัติตัวที่เหมาะสม แนวทางการรักษาและการใช้ยาตามแผนการรักษา การป้องกันภาวะแทรกซ้อน การสังเกตอาการผิดปกติ การรับประทานอาหาร การออกกำลังกาย หากแพทย์นัดควรมาพบแพทย์ตามนัด : ผู้ป่วยและ.....เข้าใจ

Physical Exam.....

.....

.....

.....

การตรวจ Lab.....

.....

.....

.....

.....

.....

.....

การตรวจ X-ray.....

การตรวจอื่น ๆ.....

Diagnosis.....

การรักษา.....

.....

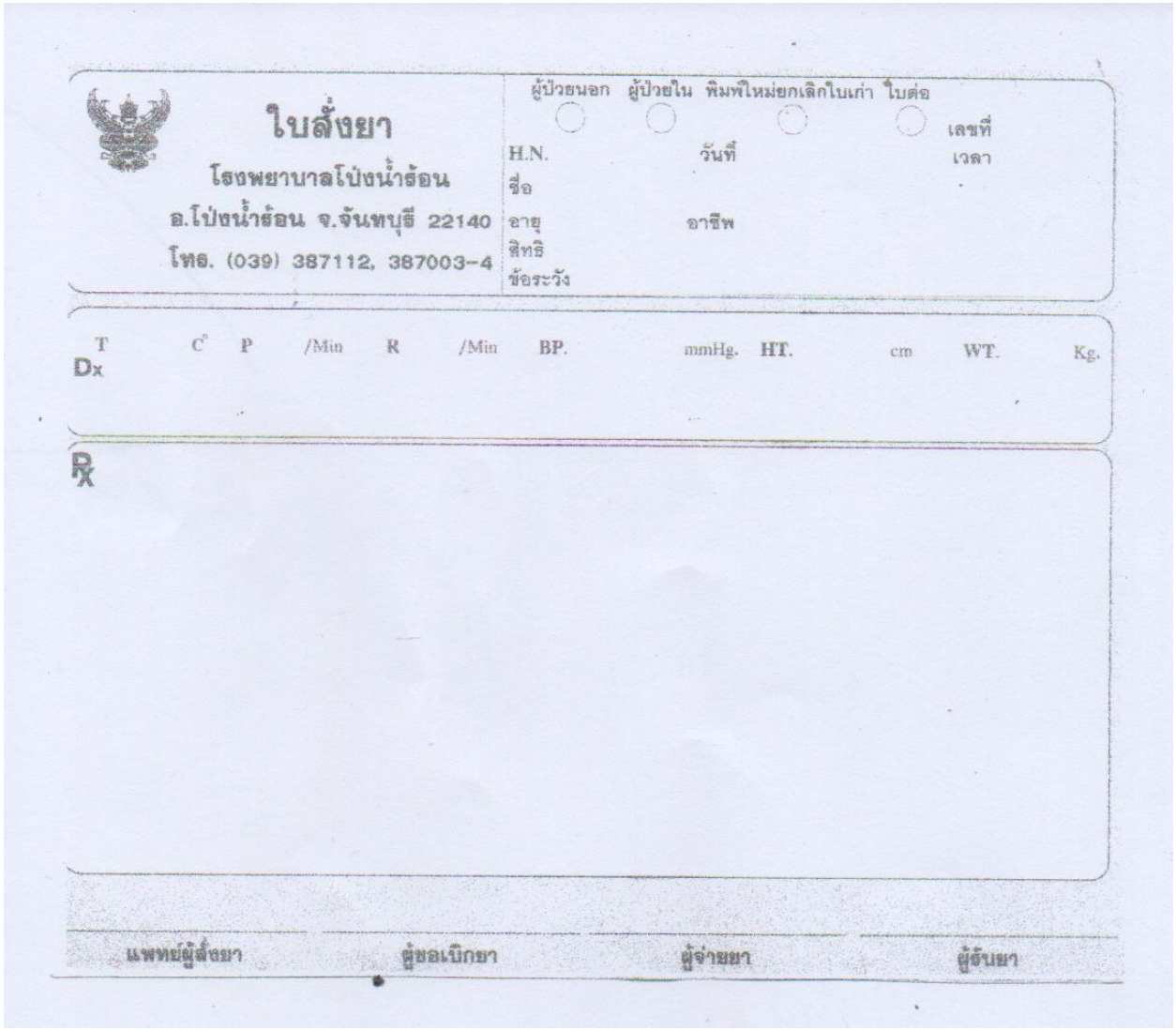
.....

.....

.....

.....**ผู้ให้การรักษา**.....

แบบฟอร์มใบสั่งยาชั่วคราวแบบที่ 1



ใบสั่งยา

โรงพยาบาลโป่งน้ำร้อน

อ.โป่งน้ำร้อน จ.จันทบุรี 22140

โทร. (039) 387112, 387003-4

ผู้ป่วยนอก ผู้ป่วยใน พิมพ์ใหม่ยกเลิกใบเก่า ใบต่อ

เลขที่

H.N. วันที่ เวลา

ชื่อ

อายุ อาชีพ

สิทธิ

ข้อระวัง

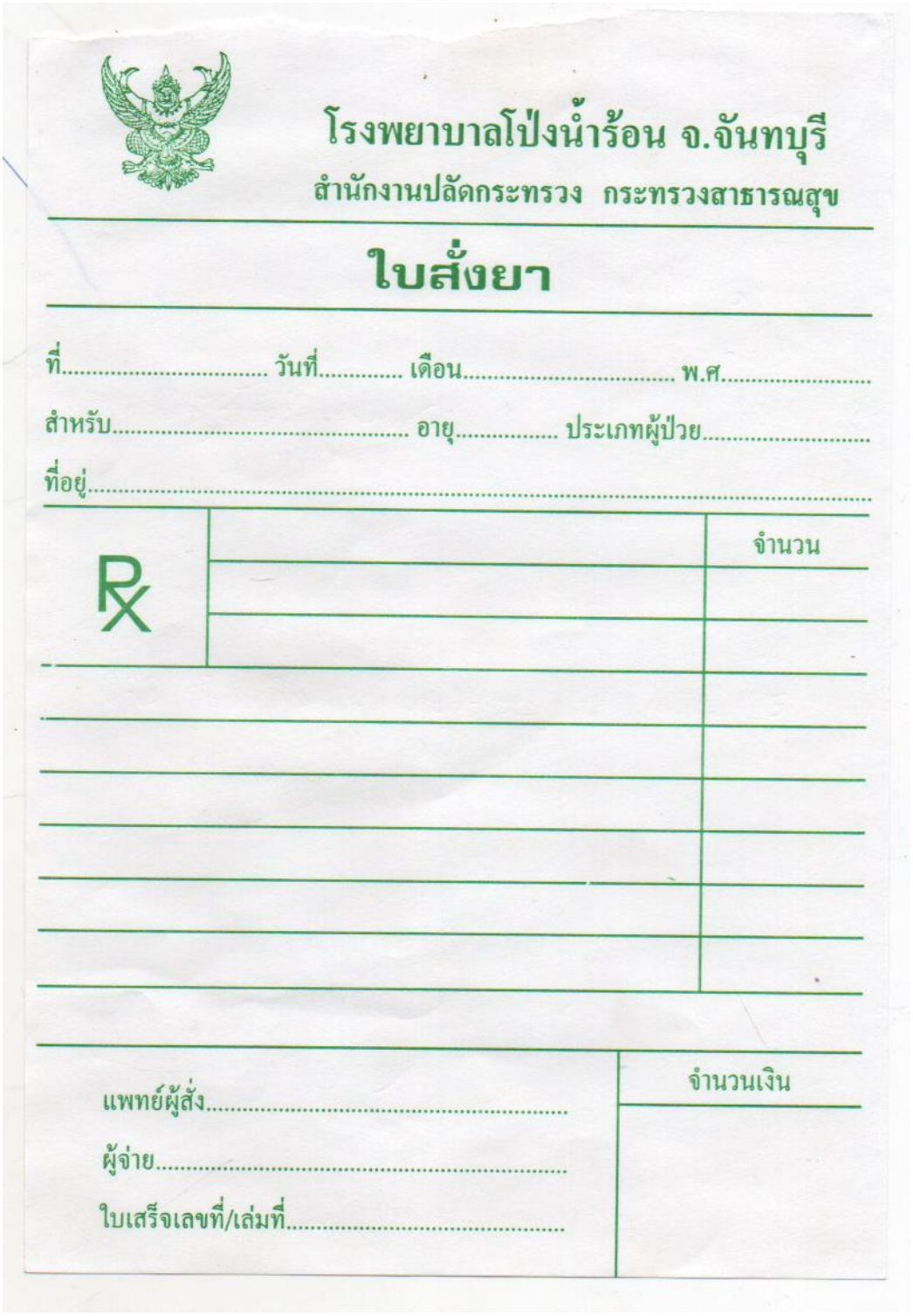
T C° P /Min R /Min BP. mmHg. HT. cm WT. Kg.

Dx

Rx

แพทย์ผู้สั่งยา ผู้ชอเบิกยา ผู้จ่ายยา ผู้รับยา

แบบฟอร์มใบสั่งยาชั่วคราวแบบที่ 2



โรงพยาบาลโป่งน้ำร้อน จ.จันทบุรี

สำนักงานปลัดกระทรวง กระทรวงสาธารณสุข

ใบสั่งยา

ที่..... วันที่..... เดือน..... พ.ศ.....

สำหรับ..... อายุ..... ประเภทผู้ป่วย.....

ที่อยู่.....

Rx

จำนวน

แพทย์ผู้สั่ง.....

ผู้จ่าย.....

ใบเสร็จเลขที่/เล่มที่.....

จำนวนเงิน

	ระเบียบปฏิบัติ : การปฏิบัติกรณีไฟฟ้าดับและเครื่องปั่นไฟสำรองไม่ทำงาน	หน่วยงาน:ศูนย์คอมพิวเตอร์ หน้าที่ 1 - 2
	ผู้อนุมัติ **รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลโป่งน้ำร้อน**	แก้ไขครั้งที่ 2 ลงวันที่ 10 ม.ค. 64

การปฏิบัติกรณีไฟฟ้าดับและเครื่องปั่นไฟสำรองไมทำงาน ระยะเวลาเกิน 30 นาที

เจ้าหน้าที่ศูนย์คอมพิวเตอร์

- ศูนย์คอมพิวเตอร์ประสานงานกับงานซ่อมบำรุง เพื่อขอทราบสาเหตุของปัญหาและระยะเวลาในการแก ไข หากไมสามารถแกไขไดภายในเวลา 30 นาที และไมมีระบบไฟฟ้าสำรอง ให้แจ้งประธานคณะกรรมการ สารสนเทศ/ผู้อำนวยการทราบ
- ประธานกรรมการสารสนเทศ/หัวหนา/รองศูนย์คอมพิวเตอร์ ประกาศใช้แผนฉุกเฉินกรณีระบบ เครือข่ายไมสามารถใช้งานไดให้หน่วยงานต่างๆทราบ
- สำรวจ/รับแจ้งปัญหาการทำงานของเครื่องสำรองไฟฟ้า(UPS) เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วงของ หน่วยงานต่างๆ
- เตรียมคอมพิวเตอร์โน๊ตบุ๊คของงานคอมพิวเตอร์ที่ติดตั้งฐานข้อมูล HOSxP สำหรับสืบค้นข้อมูล HN ของผู้ป่วย
- เมื่อระบบไฟฟ้าสามารถทำงานได้ปกติ ให้ตรวจสอบความเรียบร้อยของคอมพิวเตอร์แม่ข่าย Server และอุปกรณ์เครือข่าย และการใช้งานฐานข้อมูลโปรแกรม HOSxP
- ประธานกรรมการสารสนเทศ/หัวหนา/รองศูนย์ คอมพิวเตอร์ ประกาศแจ้งยกเลิกแผนฉุกเฉินกรณี ระบบเครือข่ายไมสามารถใช้งานได ให้หน่วยงานต่างๆทราบ เมื่อระบบสามารถใช้งานระบบเครือข่าย และระบบ โปรแกรม HOSxP ไดตามปกติ
- ติดตาม ตรวจสอบ การลงบันทึกข้อมูลของหน่วยงานต่างๆให้เรียบร้อย และเป็นปัจจุบัน จึงประกาศ ยกเลิกแผนฉุกเฉิน
- สรุปรายงานนำเสนอผู้อำนวยการ และคณะกรรมการบริหารทราบ

เจาหน้าที่ตามจุดบริการผู้ป่วยที่เกี่ยวข้องกับระบบคอมพิวเตอร์

- เมื่อไดรับแจ้งประกาศใช้แผนฉุกเฉินกรณีระบบล่ม ให้หยุดการลงบันทึกข้อมูลในคอมพิวเตอร์ ปดเครื่องคอมพิวเตอร์ เครื่องสำรองไฟฟ้า(UPS) และอุปกรณ์ต่อพ่วง
- แจ้งประชาสัมพันธ์ให้ผู้รับบริการทราบ
- จัดเตรียมอุปกรณ์สำหรับบันทึกข้อมูลดังนี้
    - o แบบฟอร์ม OPD CARD
    - o แบบบันทึกเวชระเบียนผู้ป่วยนอก
    - o แบบฟอร์มใบสั่งยา
    - o ปากกา,ตราปั้มวันที่
- บริการผู้ป่วยนอกจัดบริการที่สามารถทำได้ โดยใช้แบบฟอร์มที่เตรียมไว้บันทึกข้อมูล เพื่อนำข้อมูลกลับมาบันทึกลงคอมพิวเตอร์ย้อนหลัง เมื่อระบบสามารถใช้งานได ตามปกติ
- งานเภสัชกรรมลงกิจกรรมในใบสั่งยาและใช้วิธีเขียนฉลากซองยาแทนการสั่งพิมพ์
- เก็บใบสั่งยาไวที่ห้องจ่ายยา เพื่อลงบันทึกข้อมูลลงคอมพิวเตอร์ย้อนหลังเมื่อระบบสามารถใช้งานได ตามปกติ
- กรณีมีค่าใช้จ่ายที่สามารถสรุปค่าใช้จ่ายได เช่น ใบรับรองแพทย์ ให้เก็บเงินโดยใช้ใบเสร็จเล่มเขียว
- กรณีไมสามารถสรุปค่าใช้จ่ายได ให้แยกใบสั่งยาไว และแจ้งผู้ป่วย/ญาติให้รับทราบ ว่าจะลงบันทึกเป็นผู้ป่วยค้างชำระไวก่อนชั่วคราว
- เมื่อระบบสามารถกลับมาใช้งานไดตามปกติ ให้นำข้อมูลจากแบบฟอร์มที่บันทึกไว้ มาลงบันทึกส่งตรวจย้อนหลังจนเป็นปัจจุบัน

	ระเบียบปฏิบัติ : การปฏิบัติกรณีเกิดอัคคีภัย	หน่วยงาน:ศูนย์คอมพิวเตอร์ หน้าที่ 1 - 1
	ผู้อนุมัติ **รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลโป่งน้ำร้อน**	แก้ไขครั้งที่ 2 ลงวันที่ 10 ม.ค. 64

การปฏิบัติกรณีเกิดอัคคีภัย

เจ้าหน้าที่ศูนย์คอมพิวเตอร์ ดำเนินการขนย้ายอุปกรณ์ตามลำดับความสำคัญตามแผนอัคคีภัย ดังนี้

1. ขนย้ายอุปกรณ์ในห้องคอมพิวเตอร์แม่ข่าย ดังนี้
    - o ตู้ Rack Server
2. ขนย้ายอุปกรณ์ในห้องคอมพิวเตอร์ดังนี้
    - o Computer PC ที่ติดสติ๊กเกอร์สีแดงหมายเลข 1
    - o Switch HUB
    - o Computer Notebook
    - o เครื่องสำรองไฟฟ้า
    - o อุปกรณ์ต่อพ่วงอื่นๆ
3. เมื่อสามารถควบคุมอัคคีภัยได้แล้ว ให้ดำเนินการตรวจสอบความเรียบร้อยของระบบเครือข่าย ,ระบบไฟฟ้า และติดตั้งอุปกรณ์ให้พร้อมใช้งาน
4. ตรวจสอบความพร้อมใช้ของเครื่องลูกข่าย หากยังไม่พร้อมใช้งานให้ดำเนินการตามระเบียบปฏิบัติกรณีไฟฟ้าดับ หรือ กรณีเครื่อง Server /Database มีปัญหา

เจ้าหน้าที่อื่นๆ หากเจ้าหน้าที่ศูนย์คอมพิวเตอร์ไม่อยู่ เจ้าหน้าที่อื่นสามารถดำเนินการได้ ดังนี้

- ให้เปิดประตูห้องคอมพิวเตอร์แม่ข่าย หรือพังประตูเพื่อเข้าไปในห้องคอมพิวเตอร์แม่ข่าย
- ทำการถอด หรือ ตัดสาย LAN โดยใช้คีมตัดสาย LAN ออกให้หมด
- ทำการถอดสายไฟที่อยู่ภายนอกตู้ Server ออกให้หมด
- ทำการเคลื่อนย้ายอุปกรณ์ตามแผนป้องกันอัคคีภัย

	ระเบียบปฏิบัติ : การใช้งานห้องเครื่องคอมพิวเตอร์แม่ข่าย	หน่วยงาน:ศูนย์คอมพิวเตอร์ หน้าที่ 1 - 1
	ผู้อนุมัติ **รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลโป่งน้ำร้อน**	แก้ไขครั้งที่ 2 ลงวันที่ 10 ม.ค. 64

วิธีปฏิบัติ การใช้งานห้องเครื่องคอมพิวเตอร์แม่ข่าย

1. ห้ามนำบุคคลภายนอกหรือผู้ไม่เกี่ยวข้องเข้าไปในห้องเครื่องคอมพิวเตอร์แม่ข่าย โดยไม่มีกิจที่จำเป็น

2. ห้ามนำอาหารและเครื่องดื่มเข้าไปในบริเวณห้องเครื่องคอมพิวเตอร์แม่ข่าย

3. ตรวจสอบประตูทางเข้า-ออก และหน้าต่างของห้องเครื่องคอมพิวเตอร์แม่ข่ายให้ปิดล็อกอยู่เสมอ

4. ตรวจสอบสภาพการทำงานของห้องคอมพิวเตอร์แม่ข่าย อุปกรณ์สนับสนุนการทำงานของ ระบบคอมพิวเตอร์ ได้แก่

- o ระบบกระแสไฟฟ้า
- o ระบบการควบคุมความชื้น
- o ระบบการระบายอากาศ
- o ระบบการปรับอุณหภูมิ
- o ระบบกระแสไฟฟ้าสำรอง (เครื่องปั่นไฟ)
- o ระบบเครื่องสำรองไฟ UPS ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ อย่างน้อยวันละ 1 ครั้ง ยกเว้นการตรวจสอบระบบ กระแสไฟฟ้าสำรองเครื่องปั่นไฟ ให้ตรวจสอบสัปดาห์ละ 1 ครั้ง

5. จัดวางเครื่องคอมพิวเตอร์ อุปกรณ์สื่อสาร หรือทรัพย์สินอื่นๆ ไว้ในบริเวณที่มีความปลอดภัย ระมัดระวังการจัดตั้งอุปกรณ์ให้อยู่ในสภาพที่ มั่นคงและไม่ล้มหรือโอนเอียงได้โดยง่าย

6. ติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) เพิ่มเติมตามความจำเป็น เช่น ในกรณีที่เป็นมุมอับรวมทั้งตรวจสอบการทำงานของกล้องให้มีการทำงานอย่างถูกต้อง ต่อเนื่องและให้สามารถเก็บภาพได้ในมุม กว้าง และไม่มีสิ่งกีดขวาง โดยบันทึกภาพล่าสุดไว้อย่างน้อย 7 วัน

7. ตรวจสอบการทำงานของอุปกรณ์ดับเพลิงอย่างน้อยเดือนละ 1 ครั้ง ว่ายังใช้งานได้เป็นปกติหรือไม่

8. ให้ดูแลความสะอาดและความเป็นระเบียบเรียบร้อย ของห้องเครื่องคอมพิวเตอร์แม่ข่าย อย่างสม่ำเสมอ ต้องไม่เก็บกล่องกระดาษหรือสิ่งที่จะเป็นเชื้อเพลิงไว้ในห้องเครื่อง

9. ตรวจสอบและจัดเก็บสายไฟฟ้า สายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย

10. จัดทำหรือต่อสัญญา Sofeware หรือการบำรุงรักษาระบบงาน สำคัญไฟร์วอลล์ เราท์เตอร์ อุปกรณ์ UPS สำหรับระบบงานสำคัญ และเครื่องปรับอากาศในห้องเครื่องคอมพิวเตอร์แม่ข่าย ให้ครบถ้วน

11. จัดให้ระบบงานสำคัญ เครื่องคอมพิวเตอร์แม่ข่าย เซิร์ฟเวอร์ และอุปกรณ์ที่มีความสำคัญต้องมีอุปกรณ์สำรองไฟ UPS และระบบกระแสไฟฟ้าสำรองเครื่องปั่นไฟ (electricity power generator) เพื่อสนับสนุนการทำงานอย่างครบถ้วน

	ระเบียบปฏิบัติ : การสำรองข้อมูลเวชระเบียนที่จัดเก็บในรูปแบบ Electronic files	หน่วยงาน:ศูนย์คอมพิวเตอร์ หน้าที่ 1 - 1
	ผู้อนุมัติ **รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลโป่งน้ำร้อน**	แก้ไขครั้งที่ 3 ลงวันที่ 10 ม.ค. 67

วิธีปฏิบัติ การสำรองข้อมูล Backup ข้อมูลที่จัดเก็บในรูปแบบ Electronic files โรงพยาบาลโป่งน้ำร้อน ให้ปฏิบัติดังนี้

1. จัดเก็บข้อมูลในเครื่องคอมพิวเตอร์แม่ข่าย Server หลัก

2. จัดเก็บข้อมูลในเครื่องคอมพิวเตอร์แม่ข่าย Server รอง ตัวที่ 1 โดยใช้การทำ replication ข้อมูลจากเครื่อง Server หลักแบบ real time

3. จัดเก็บข้อมูลในเครื่องคอมพิวเตอร์แม่ข่าย Server รอง ตัวที่ 2 โดยใช้การทำ replication ข้อมูลจากเครื่อง Server หลักแบบ real time

4. ทำการ backup ข้อมูลเป็นรูปแบบไฟล์บีบอัด 7z ไว้ในเครื่องลูกข่ายห้องคอมพิวเตอร์ ทุกวัน

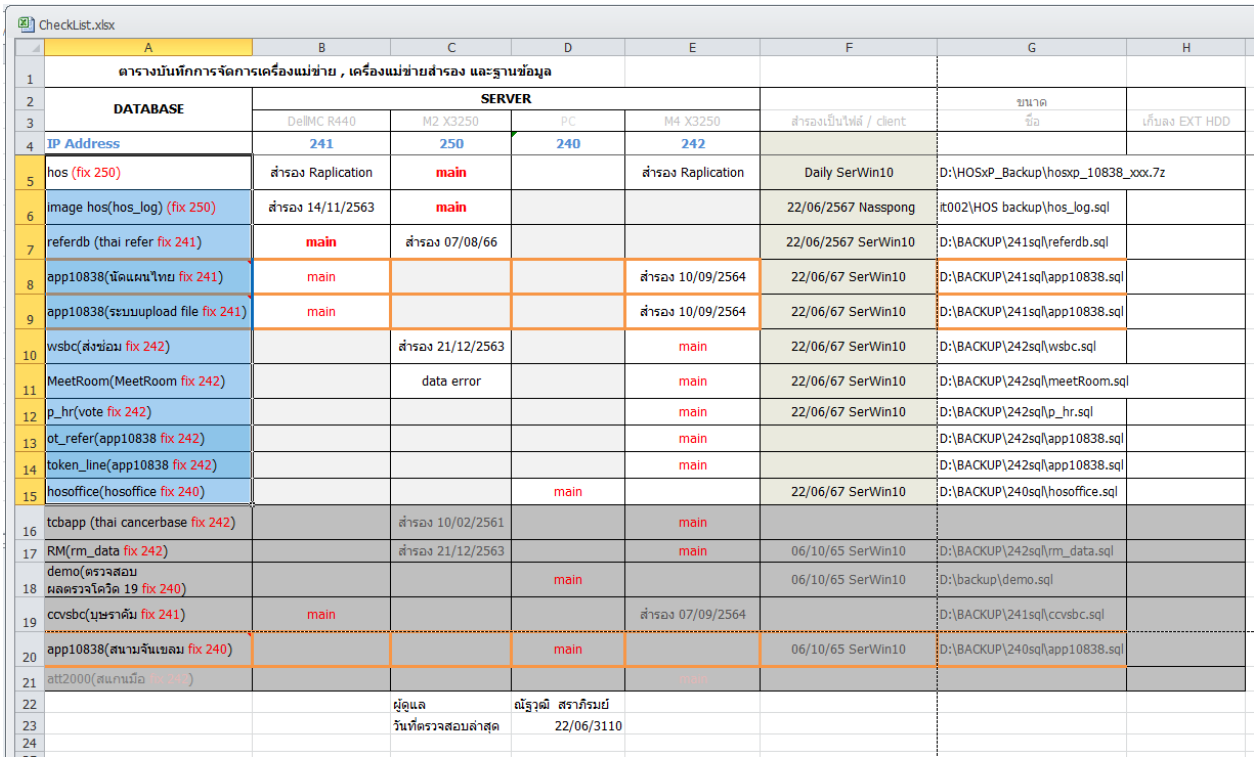
5. ทำการ Copy ข้อมูล Back up เก็บไว้ใน Hard disk ของเครื่องลูกข่ายเก็บไว้แยกจุด 2 จุด คือ

- ห้องคอมพิวเตอร์ 1 ชุด ตำแหน่ง D:\HOSxP_Backup
- ห้องพักเจ้าหน้าที่คอมพิวเตอร์ 1 ชุด
- Hard disk External ของศูนย์คอมพิวเตอร์
- Nass ของโรงพยาบาล ตำแหน่ง \\192.168.1.229\it002\HOSxP_Backup
- GoogleDive pong10838.2020@gmail.com > WorkHot > BK10838

ตารางการสำรองข้อมูลDatabase เครื่องคอมพิวเตอร์แม่ข่าย Server

ลำดับที่	โปรแกรม	DATABASE	ความถี่	สถานที่สำรอง
1	HOSxP	hos	ทุกวัน	Serverสำรอง,คอมศูนย์คอมฯ,hasdisk Extenal,Nass
2	HOSxP scan chat	hos_log	ทุกสัปดาห์	Serverสำรอง,คอมศูนย์คอมฯ,hasdisk Extenal,Nass
3	ไทยรีเฟอร์	referdb	ทุกสัปดาห์	คอมศูนย์คอมฯ,hasdisk Extenal,Nass
4	ระบบนัดรับบริการ	app10838	ทุกสัปดาห์	คอมศูนย์คอมฯ,hasdisk Extenal,Nass
5	Upload file	app10838	ทุกสัปดาห์	คอมศูนย์คอมฯ,hasdisk Extenal,Nass
6	ส่งซ่อม	wsbc	ทุกสัปดาห์	คอมศูนย์คอมฯ,hasdisk Extenal,Nass
7	จองห้องประชุม	MeetRoom	ทุกสัปดาห์	คอมศูนย์คอมฯ,hasdisk Extenal,Nass
8	ลงคะแนนในดวงใจ	p_hr	ทุกเดือน	คอมศูนย์คอมฯ,hasdisk Extenal,Nass
9	ระบบลงชื่อปฏิบัติงานรีเฟอร์	app10838	ทุกสัปดาห์	คอมศูนย์คอมฯ,hasdisk Extenal,Nass
10	แจ้งเตือนกำหนดนัดหมาย	app10838	ทุกสัปดาห์	คอมศูนย์คอมฯ,hasdisk Extenal,Nass

(รายละเอียด การจัดเก็บไฟล์สำรอง บันทึกเป็นไฟล์รูปแบบ Excel เครื่อง Serwin10 D:\Computer\CheckList.xlsx)



CheckList.xlsx

	A	B	C	D	E	F	G	H
1	ตารางบันทึกการจัดการเครื่องแม่ข่าย , เครื่องแม่ข่ายสำรอง และฐานข้อมูล							
2	DATABASE	SERVER					ขนาด	
3		DellMC R440	M2 X3250	PC	M4 X3250	สำรองเป็นไฟล์ / client	ชื่อ	เก็บลง EXT HDD
4	IP Address	241	250	240	242			
5	hos (fix 250)	สำรอง Raplication	main		สำรอง Raplication	Daily SerWin10	D:\HOSxP_Backup\hosxp_10838_xxx.7z	
6	image hos(hos_log) (fix 250)	สำรอง 14/11/2563	main			22/06/2567 Nasspong	it002\HOS backup\hos_log.sql	
7	referdb (thai refer fix 241)	main	สำรอง 07/08/66			22/06/2567 SerWin10	D:\BACKUP\241sql\referdb.sql	
8	app10838(นัดแผนไทย fix 241)	main			สำรอง 10/09/2564	22/06/67 SerWin10	D:\BACKUP\241sql\app10838.sql	
9	app10838(ระบบupload file fix 241)	main			สำรอง 10/09/2564	22/06/67 SerWin10	D:\BACKUP\241sql\app10838.sql	
10	wsbc(ส่งซ่อม fix 242)		สำรอง 21/12/2563		main	22/06/67 SerWin10	D:\BACKUP\242sql\wsbc.sql	
11	MeetRoom(MeetRoom fix 242)		data error		main	22/06/67 SerWin10	D:\BACKUP\242sql\meetRoom.sql	
12	p_hr(vote fix 242)				main	22/06/67 SerWin10	D:\BACKUP\242sql\p_hr.sql	
13	ot_refer(app10838 fix 242)				main		D:\BACKUP\242sql\app10838.sql	
14	token_line(app10838 fix 242)				main		D:\BACKUP\242sql\app10838.sql	
15	hosoffice(hosoffice fix 240)			main		22/06/67 SerWin10	D:\BACKUP\240sql\hosoffice.sql	
16	tcbapp (thai cancerbase fix 242)		สำรอง 10/02/2561		main			
17	RM(rm_data fix 242)		สำรอง 21/12/2563		main	06/10/65 SerWin10	D:\BACKUP\242sql\rm_data.sql	
18	demo(ตรวจสอบผลตรวจโควิด 19 fix 240)			main		06/10/65 SerWin10	D:\backup\demo.sql	
19	ccvsbc(บุษราคัม fix 241)	main			สำรอง 07/09/2564		D:\BACKUP\241sql\ccvsbc.sql	
20	app10838(สนามจันเขลม fix 240)			main		06/10/65 SerWin10	D:\BACKUP\240sql\app10838.sql	
21	att2000(สแกนนิ้ว fix 240)				main			
22			ผู้ดูแล	ณัฐวุฒิ สราภิรมย์				
23			วันที่ตรวจสอบล่าสุด	22/06/3110				
24								

	ระเบียบปฏิบัติ : การควบคุมการเข้าถึงระบบข้อมูลผู้รับบริการ	หน่วยงาน:ศูนย์คอมพิวเตอร์ หน้าที่ 1 - 2
	ผู้อนุมัติ **รักษาการในตำแหน่งผู้อำนวยการโรงพยาบาลโป่งน้ำร้อน**	แก้ไขครั้งที่ 2 ลงวันที่ 10 ม.ค. 64

โรงพยาบาลโป่งน้ำร้อน เก็บข้อมูลเวชระเบียนและการเข้ารับบริการของผู้ป่วย ไว้ในรูปแบบฐานข้อมูล คอมพิวเตอร์ โดยมีระเบียบปฏิบัติดังนี้

1. กำหนดให้เจ้าหน้าที่และผู้ที่เกี่ยวข้อง ที่ทำหน้าที่บันทึกข้อมูลต่างๆ ลงในระบบคอมพิวเตอร์มี รหัสผ่าน Username/Accouunt และ password เพื่อการเข้าถึงระบบโปรแกรม HOSxP ของงาน ในแต่ละประเภท โดยรหัสที่กำหนดให้จะเข้าถึง(Access_menu) และใช้งานได้ เฉพาะงานในหน้าที่ ของตนเองเท่านั้นไม่สามารถใช้งานในด้านอื่นที่ไม่เกี่ยว ข้องได้

2. เจ้าหน้าที่ของโรงพยาบาลทุกคนได้รับ การอบรม ในเรื่องการรักษาข้อมูลผู้ป่วย จรรยาบรรณในการไม่ เปิดเผยข้อมูล ซึ่งจะต้องปฏิบัติตามระเบียบการขอประวัติการรักษาเวชระเบียนผู้ป่วย

3. กำหนดให้เจ้าหน้าที่ทุกคนที่ใช้งานระบบโปรแกรม HOSxP ต้อง Log out ออกจากโปรแกรมทุกครั้ง หากไม่ได้ปฏิบัติงานอยู่ที่หน้าเครื่องคอมพิวเตอร์ และงานคอมพิวเตอร์ได้ตั้งเวลาให้โปรแกรม Logout อัตโนมัติกรณีที่ไม่มีการใช้งานเป็นเวลานานเกิน 10 นาที

4. กำหนดให้เจ้าหน้าที่ทุกคนที่ใช้งานระบบโปรแกรม HOSxP ต้องเปลี่ยนรหัสผ่านใหม่ทุก 6เดือน และ ตั้งค่าโปรแกรมให้มีการแจ้งเตือนและล็อคค่า Password เดิมอัตโนมัติหากไม่มีการเปลี่ยนรหัสผ่าน ใหม่ภายในระยะเวลาที่กำหนด

5. กำหนดให้โปรแกรม HOSxP สามารถตรวจสอบเหตุผิดพลาด ของงานและสืบสวนย้อนกลับได้ว่ามี การเข้าถึง การบันทึกหรือแก้ไข ข้อมูลของผู้ป่วยที่อยู่ในคอมพิวเตอร์ โดยรหัสผู้ใช้ของใคร มีการ ดำเนินการเมื่อไหร่

6. กำหนดให้โปรแกรม HOSxP สามารถป้องกันการเข้าถึง ข้อมูลและการนำข้อมูลในคอมพิวเตอร์ไปใช้งานโดยไม่ได้รับอนุญาต เช่น จำกัดสิทธิการเข้าถึง เปิดเผย การ print รายงานข้อมูลประวัติผู้ป่วย, กำหนดเครื่องที่ใช้พิมพ์ใบเสร็จ เป็นต้น

7. กำหนดให้มีการติดตั้งโปรแกรมเพื่อป้องกัน และปกป้องข้อมูลจากไวรัส มัลแวร์ โทรจัน หนอน คอมพิวเตอร์ และตรวจสอบให้มีการ Update อัตโนมัติ

8. สำรวจสายไฟ สายแลน ในหน่วยงานไม่ให้ชำรุดสามารถใช้งานได้อย่างปลอดภัย เพื่อป้องกันอัคคีภัย

9. มีการจำลองเหตุการณ์ ร่วมซ้อมแผนภาวะฉุกเฉินของโรงพยาบาล และเตรียมความพร้อมเมื่อเกิด เหตุการณ์ฉุกเฉินและมีเหตุจำเป็นต้องขนย้ายเครื่องคอมพิวเตอร์แม่ข่าย Server

10. จัดให้มีอุปกรณ์ดับเพลิง และมีการตรวจสอบให้ใช้งานได้อย่างมีประสิทธิภาพเพื่อป้องกันหรือบรรเทา ความเสียหายทางกายภาพที่อาจเกิดขึ้นของเวชระเบียน

11. ห้องจัดเก็บคอมพิวเตอร์แม่ข่าย Server ปรับปรุงมาตรฐานเทคโนโลยีสารสนเทศ ของโรงพยาบาล โดยจัดเก็บคอมพิวเตอร์แม่ข่าย Server ไว้ในตู้ Rack สำหรับขนย้าย ภายในห้องคอมพิวเตอร์แม่ข่าย ติดตั้งเครื่องปรับอากาศ 2 ตัว เพื่อสลับการทำงานทุก 12 ชั่วโมง และล็อคห้องคอมพิวเตอร์แม่ข่าย Server เพื่อป้องกันบุคคลภายนอกหรือผู้ไม่เกี่ยวข้องเข้าไปโดยไม่ได้รับอนุญาต

12. กำหนดสิทธิรหัสผู้ใช้ username และ password สำหรับการใช้งาน server และการเข้าถึง database ข้อมูลเวชระเบียนผู้ป่วย

ลงทะเบียนผู้ใช้ใหม่

- กำหนดให้มีการลงทะเบียนสำหรับผู้ใช้ งานใหม่ตาม “แบบฟอร์มขอใช้บริการอินเตอร์เน็ต / HOSxP อื่นๆ และกำหนดสิทธิของผู้ใช้งานตามที่ระบุไว้ในแบบฟอร์มฯ ให้สิทธิความจำเป็นใน การใช้งานเท่านั้น กำหนดตามระดับของผู้ใช้งาน

- แนะนำ การตั้งพาสเวิร์ด (รหัสผ่าน) ให้ปลอดภัยแก่ผู้ใช้งานใหม่ โดยรหัสผ่านควรประกอบไปด้วย

- รหัสผ่านควรมีความยาวที่เหมาะสม ไม่น้อยกว่า 8characters ไม่ยาวเกินไปจนจำไม่ได้ แต่ก็ไม่ได้สั้นเกินไปจนสามารถคาดเดาได้ง่ายจนเกินไป
- ใช้ตัวอักษรเล็ก (abcd) ตัวอักษรใหญ่ (ABCD) ตัวเลข (1234) และสัญลักษณ์ ($#!?) เพื่อสร้างความหลากหลายให้กับรหัสผ่านของ
- ไม่ใช้ข้อมูลส่วนตัวในการตั้งรหัสผ่าน เช่น วันเกิด หมายเลขโทรศัพท์ ไปจนถึงชื่อของตัวเองเพราะเป็นข้อมูลที่ทุกคนสามารถรู้ได้อย่างง่ายดาย
- ไม่ควรใช้รหัสผ่านเดียวกัน

- ทบทวนบัญชีผู้ใช้งานและสิทธิของ ผู้ใช้งาน สำหรับเจ้าหน้าที่ของโรงพยาบาลอย่างน้อยปีละ 1 ครั้ง และให้ทำบันทึกการทบทวนดังกล่าว และจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง

- ทบทวนบัญชีผู้ใช้งานและสิทธิของ ผู้ใช้งาน สำหรับหน่วยงานภายนอก อย่างน้อยปีละ 1 ครั้ง และให้ ทำบันทึกการทบทวนดังกล่าว และจัดเก็บไว้เพื่อใช้ในการตรวจสอบในภายหลัง

ยกเลิกผู้ใช้ กรณีเจ้าหน้าที่ที่ลาออก โยกย้าย หลังได้รับการแจ้งโยกย้าย / ลาออกจากฝ่ายบริหารงานทั่วไป

1. ยกเลิกสิทธิการเข้าใช้งานออกจากทุกระบบของโรงพยาบาล ได้แก่ HOSxP อินเตอร์เน็ต
2. ตรวจสอบระบบความถูกต้องของข้อมูลผู้ใช้งานในระบบต่างๆ ทุก 1 สัปดาห์

วิธีปฏิบัติ การรับมือเหตุการณ์ถูกโจมตีจากภัยคุกคามทางไซเบอร์ โรงพยาบาลโป่งน้ำร้อน ให้ปฏิบัติดังนี้

1. ควบคุมความเสียหาย ตัดสินใจเลือกวิธีการที่เหมาะสม ดังนี้

- ปิดระบบ พร้อมแจ้งหน่วยงานที่เกี่ยวข้องรับมือตามแผนปฏิบัติงานรองรับกรณีระบบสารสนเทศเทคโนโลยีที่เกี่ยวกับการปฏิบัติงาน ไม่สามารถให้บริการ ให้การปฏิบัติงานของหน่วยงานงานสามารถแก้ไขการปฏิบัติงานเฉพาะหน้าไปได้

- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด(Network disconnection) ทั้งนี้อาจมียกเว้นการเชื่อมต่อสำหรับกระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัยใดๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์(Enpoint Detection & Response Agent)

- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง(Disabling Certain Functions)

- Redirect Network Traffic หรือความสนใจของผู้บุกรุกไปยังเส้นทางอื่น

โดยการตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายให้ขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญ, ประเภทภัยคุกคาม, ระบบงานหรือบริการที่ได้รับผลกระทบ, ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย

2. จัดเก็บข้อมูลและดูแลรักษาหลักฐานทางดิจิตอล

เพื่อให้การแก้ไขเหตุการณ์ส่งผลกระทบต่อการดำเนินงานของโรงพยาบาลให้น้อยที่สุด โดยต้องดำเนินการภายใต้หลักการเป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ได้ในชั้นศาล หลักฐานมีการบันทึกการเข้าถึงและการกระทำใดๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม และอาจมีการเปลี่ยนตัวผู้ดูแลงาน เครื่อง ข้อมูลที่ประสบเหตุการณ์เพื่อป้องกันการยุ่งเกี่ยวกับหลักฐาน หลักฐานที่ต้องจัดเก็บประกอบด้วย

2.1 ข้อมูลเฉพาะ เช่น ตำแหน่งที่ตั้งLocation, Serial Number, Model Number, Hostname, Media Access Control, MAC Address เป็นต้น

2.2 ชื่อตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือกับเหตุการณ์

2.3. สถานที่จัดเก็บข้อมูล หลักฐาน

3. กำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ

เมื่อมีการควบคุมความเสียหายและเก็บหลักฐานข้อมูลเพิ่มเติมทั้งหมดเรียบร้อยแล้ว ทำการกำจัดสาเหตุที่ทำให้เกิดเหตุการณ์และผลกระทบ

- ปิดช่องโหว่ของระบบ

- ยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ
- แจ้งผู้ใช้งานเปลี่ยนรหัสผ่าน
- ลบโปรแกรมที่มีสถานะก่อให้เกิดความเสี่ยงออกก่อน
- ใช้โปรแกรมAntivirusที่มีความเหมาะสมในการสแกนหา Malware หรือร่อยรอยอื่นๆ ในระบบที่คาดว่ายังหลงเหลือของผู้บุกรุกเพื่อดำเนินการกำจัดออกจากระบบทั้งหมด

4. ฟื้นฟูระบบการทำงาน
   - Restore Operating System หรือ Application Software ต่างจากแหล่งปลอดภัย
   - Restore ข้อมูลจากแหล่งข้อมูลสำรองที่มีความปลอดภัย และมีความใกล้เคียงหรือมีระยะเวลาการสำรองห่างจากเวลาที่เกิดเหตุการณ์น้อยที่สุด กลับเข้าระบบ
   - สุ่ม/ทดสอบ ระบบและข้อมูลให้แน่ใจถึงความถูกต้อง แล้วจึงเปิดให้ระบบกลับทำงานปกติ

5. ดำเนินกิจกรรมทบทวน ติดตาม ปรับปรุงแนวทางในการรับมือกับเหตุการณ์ที่เกิดขึ้น
   - นำเหตุการณ์ที่เกิดขึ้นเข้าสู่กระบวนการจัดการความเสี่ยงและปรับปรุงแก้ไข
   - ติดตามเฝ้าระวังให้แน่ใจว่าเหตุการณ์ยุติและการทำงานทุกอย่างเป็นปกติ ไม่มีการโจมตีหรือมีความเสี่ยง/ช่องโหว่ที่จะเกิดเหตุการณ์ซ้ำ
   - พิจารณาหลักฐานที่จัดเก็บรวบรวมไว้เพื่อดำเนินการต่อไปตามความเหมาะสม(การตักเตือน/ลงโทษ/ดำเนินคดี) และนำไปประกอบการจัดการความเสี่ยงรวมถึงอ้างอิงข้อมูลสถิติภัยคุกคามของหน่วยงาน

6. จัดทำรายงานเสนอหัวหน้าหน่วยงานลงนามตามFlow การแจ้งเหตุการณ์ภัยคุกคามไซเบอร์

Flow การแจ้งเหตุการณ์ภัยคุกคามไซเบอร์ ของหน่วยงาน โรงพยาบาลโป่งน้ำร้อน

สป. : คุณสุวันต์นา เสมอเนตร
โทร. 025902180 ต่อ 112
Email dpo@moph.go.th
คำสั่ง สป. ที่ 1189/2565 ลว. 25 พ.ค.65

Health Sector Regulator **	Health Sectoral CERT (ศทส.สป.)	CIRT / IT / SOC ของหน่วยงาน	ผู้ประสานงาน DPO ของหน่วยงาน	CEO / CIO / CDO / CISO ของหน่วยงาน	DPO (สป./กรม)	CEO / CIO / CDO / CISO (สป./กรม)

โทร. 025901169, 025901200, 0830649867
Email health-cirt@moph.go.th
Line: @health-cirt
https://health-cirt.moph.go.th

คุณณัฐวุฒิ สราภิรมย์ โทร.0861543181
คุณวีรพงษ์ บุญคงมาก โทร.0982682805

คุณเอนก เจริญนาม
โทร.0861543181

สป. : .....
โทร. 02590.....
Email .....@moph.go.th
คำสั่ง สป. ที่ .....

พบเหตุ/ได้รับแจ้งเหตุ

รับแจ้งเหตุ /ตรวจสอบภัยคุกคามไซเบอร์

แจ้ง

- ตรวจสอบเหตุการณ์
- แก้ไขเหตุ/หยุดการโจมตี

เสนอ → หัวหน้าหน่วยงานรับทราบเหตุ

คาดว่าจะเกิดการละเมิดข้อมูลส่วนบุคคล

Yes → ตรวจสอบและจัดทำรายงานตามแบบฟอร์มเสนอหัวหน้าหน่วยงานลงนาม → เสนอ → หัวหน้าหน่วยงานลงนามภายใน 24 ชั่วโมง → แจ้ง → ตรวจสอบรายงานและนำเสนอ CEO ภายใน 24 ชั่วโมง → เสนอ → รับทราบเหตุการณ์และลงนามแจ้ง สคส. ภายใน 24 ชั่วโมง

No / ดำเนินการต่อ

พิจารณาขอความช่วยเหลือ

Yes → แจ้ง → ดำเนินการแก้ไขเหตุการณ์ร่วมกับหน่วยงานที่เกี่ยวข้อง (NCSA สกมช.)

ดำเนินการต่อ / No

- แก้ไขและป้องกันเหตุเกิดซ้ำ
- บันทึกเหตุการณ์และผล
- จัดทำรายงานโดยเร็ว

เสนอ → หัวหน้าหน่วยงานลงนาม → เสนอ → รับทราบเหตุการณ์และลงนามแจ้ง สกมช. / Regulator

แจ้ง → รับทราบเหตุการณ์และพิจารณาดำเนินการตามอำนาจหน้าที่

** Regulator ของ หน่วยบริการสุขภาพ (รพ. ,คลินิก) คือ กรมสนับสนุนบริการสุขภาพ (สบส.)
Regulator ของ หน่วยงานที่ดำเนินการเกี่ยวกับผลิตภัณฑ์สุขภาพ (ยา, เวชภัณฑ์, เครื่องมือแพทย์) คือ อย.
Regulator ของ หน่วยงานที่มีการดำเนินการกับข้อมูลสุขภาพ (Digital health) ยกเว้นหน่วยบริการสุขภาพ คือ สป.(ศทส.)

- คำสั่ง สป. ที่ 1480/2565 เรื่องแต่งตั้งเจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล (ประสาน DPO ระดับจังหวัด/หน่วยงาน)
- แบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ดาวน์โหลดได้ที่ https://pdpa.moph.go.th/

จำแนกประเภทภัยคุกคามที่พบ

ประเภท	ความหมาย
โปรแกรมไม่พึงประสงค์	มัลแวร์(Malware), Virus, Worm, Trojan, Ransomware, Spyware ต่างๆ โปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์
ความพยายามบุรุกเข้าระบบ	Login Attempt, Connection Attempt, Brute-force เป็นการดำเนินการเพื่อจะควบคุมหรือทำให้เกิดความขัดข้องกับบริการของระบบ
ความพร้อมใช้ของระบบ	การถูกโจมตีความพร้อมใช้งานของระบบ เช่น DDos (Denial of Service), Flood ทำให้เกิดความล่าช้าในการบริการ จนถึงทำให้ระบบไม่สามารถทำงานได้
การหลอกลวงโดยใช้อีเมลหรือหน้าเวปไซต์ปลอมเพื่อให้ได้ซึ่งข้อมูล (Phishing)	การถูกสร้างหน้าเวปไซต์ปลอม(Web Phishing) หรือหลอกลวงเพื่อให้ได้ข้อมูลผ่านอีเมล
Web Defacement	การถูกปรับเปลี่ยนหน้าเวปไซต์
SEO attack	เวปไซต์ถูกโจมตีด้วยการฝังสคริปโฆษณาเวปไซต์ไม่พึงประสงค์
Vulnerability	ช่องโหว่ของระบบบริหารจัดการเวปไซต์
Abuse	การละเมิดการใช้งานเครือข่าย เช่น Spam, Copyright

ระดับผลกระทบต่อการดำเนินงาน (การให้บริการ การรักษาผู้ป่วย)

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
None	ไม่ส่งผลกระทบต่อการดำเนินงาน
Low	ส่งผลให้การปฏิบัติงานตามภารกิจหลักมีความล่าช้า แต่ยังสามารถดำเนินงานต่อได้
Medium	ส่งผลให้การปฏิบัติงานตามภารกิจหลักไม่สามรถดำเนินการได้บางส่วน
High	ส่งผลให้การปฏิบัติงานตามภารกิจหลักไม่สามรถดำเนินการได้ทั้งหมด

ระดับผลกระทบต่อข้อมูล

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
None	ไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึงโดยที่ไม่ได้รับอนุญาต
Confidentialty Breach	การละเมิดความลับของข้อมูลส่วนบุคคลซึ่งมีการเข้าถึง หรือเปิดเผยข้อมูลส่วนบุคคล
Integrilty Breach	การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคลซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน
Availability Breach	การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคลซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

ระดับความสามารถในการกู้คืน

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
Regular	เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
Supplemented	เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาใช้ทรัพยากรเพิ่ม
Extended	เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาใช้ทรัพยากรและความช่วยเหลือจากภายนอก
Not Recoverable	เวลาในการกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะแล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจาย รวมถึงการเยียวยาผลกระทบ

แบบรานงานภัยคุกคามทางไซเบอร์

วันที่ :	เวลา :	ผู้บันทึก : ผู้รายงาน :

ข้อมูลทั่วไป

ชื่อหน่วยงาน .....

ชื่อระบบ .....

ชื่อผู้ประสานงานของหน่วยงาน	ระบบปฏิบัติการ .....
โทรศัพท์	IP Address .....
E-mail	MAC Address .....

ข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์

วันเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :	พึ่งพบเหตุการณ์ อยู่ในขั้นตอนการขอความช่วยเหลือ อยู่ในขั้นตอนการสอบสวน กำลังลุกลาม อยู่ระหว่างขั้นตอนการระงับภัย สามารถระงับภัยได้แล้ว รายงานปิดเหตุการณ์ภัยคุกคามแล้ว อื่นๆ :	
ประเภทเหตุการณ์ :	0	เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน
	1	การพยายามเข้าถึงระบบที่ไม่สำเร็จ
	2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี
	3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด
	4	การบุรุกโดยใช้มัลแวร์
	5	การบุรุกในระดับผู้ใช้งาน
	6	การบุรุกในระดับผู้ควบคุมระบบ
	7	การบุรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้
	8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน
	9	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม
	(ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ 0 1 และ 9 ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)	
รายละเอียดเหตุการณ์ :		
ความเสียหายที่เกิดขึ้น :		

ข้อมูลการรับมือภัยคุกคาม

การสำรองข้อมูล	มี ไม่มี
การดำเนินการตอบสนองต่อเหตุการณ์ :	ยังไม่ได้ดำเนินการแก้ไขใดๆ ยกเลิกการเชื่อมต่อระบบจากเครือข่ายแล้ว ตรวจสอบข้อมูลจราจร(Log)แล้ว ตรวจสอบโปรแกรม(แฟ้ม binaries/.exe)แล้ว กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม
รายละเอียดการรับมือภัยคุกคามอื่นๆ :	