กลุ่มงานเทคนิคการแพทย์

20 พฤษภาคม 2569

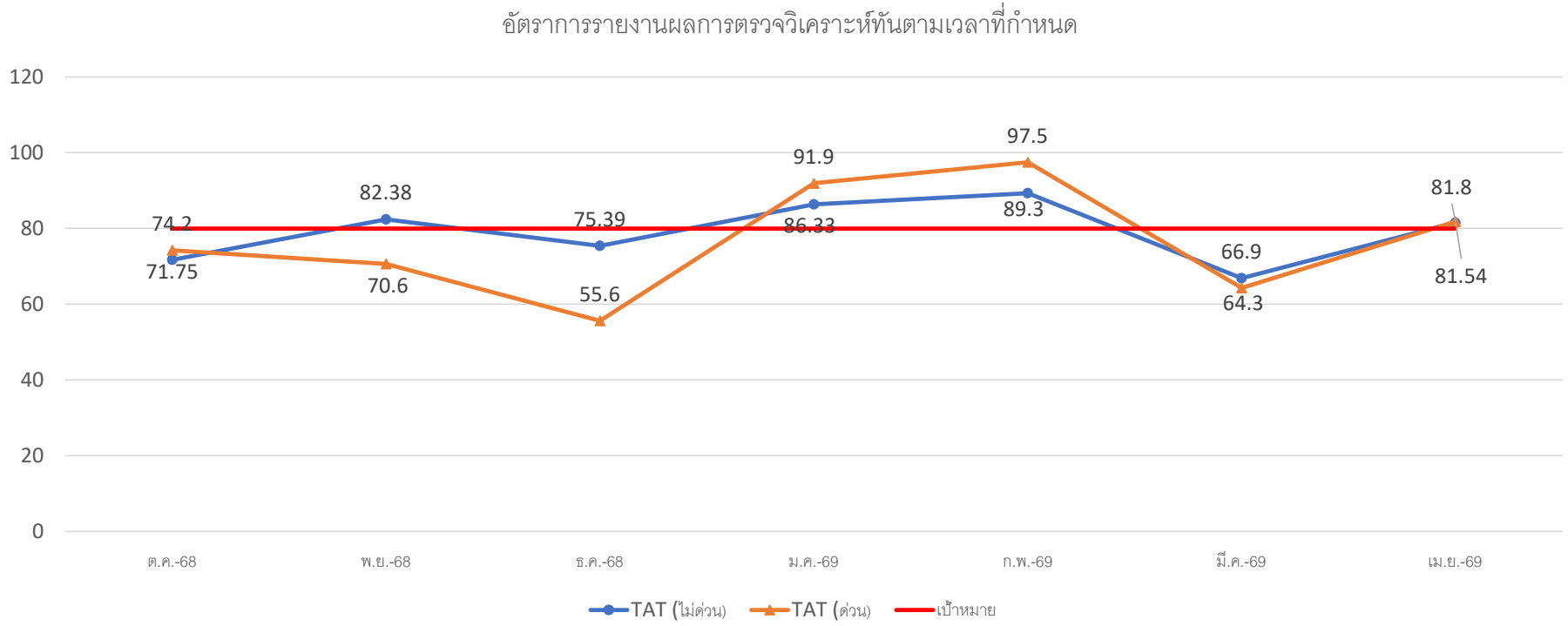
เรื่องเสนอเพื่อทราบ

- ผลการชดเชยค่าตรวจ TB-DNA (Molecular) เริ่มตรวจ 23 มีนาคม 2569
  - ตรวจ 27 ราย ต้นทุน 550*27 = 14,850
  - ชดเชย 22 ราย เป็นเงิน 13,200 บาท
  - ไม่แจ้งเหตุผลของการไม่ชดเชย ไม่มีรายละเอียดใน REP
- งานรังสีวิทยา รับการตรวจประเมินภายใน (Internal survey) ตามมาตรฐานห้องปฏิบัติการรังสีวินิจฉัย กระทรวงสาธารณสุข (MOPH X-ray) วันที่ 20 พฤษภาคม 2569 โดยทีมวิทยากรจากโรงพยาบาลสรรพสิทธิประสงค์และโรงพยาบาลโพธิ์ไทร

ผลการดำเนินงานตามข้อเสนอแนะ

- ไม่มี

ผลการดำเนินงานตัวชี้วัดสำคัญ (KPI)



รายงานความเสี่ยงสำคัญ (The Must)

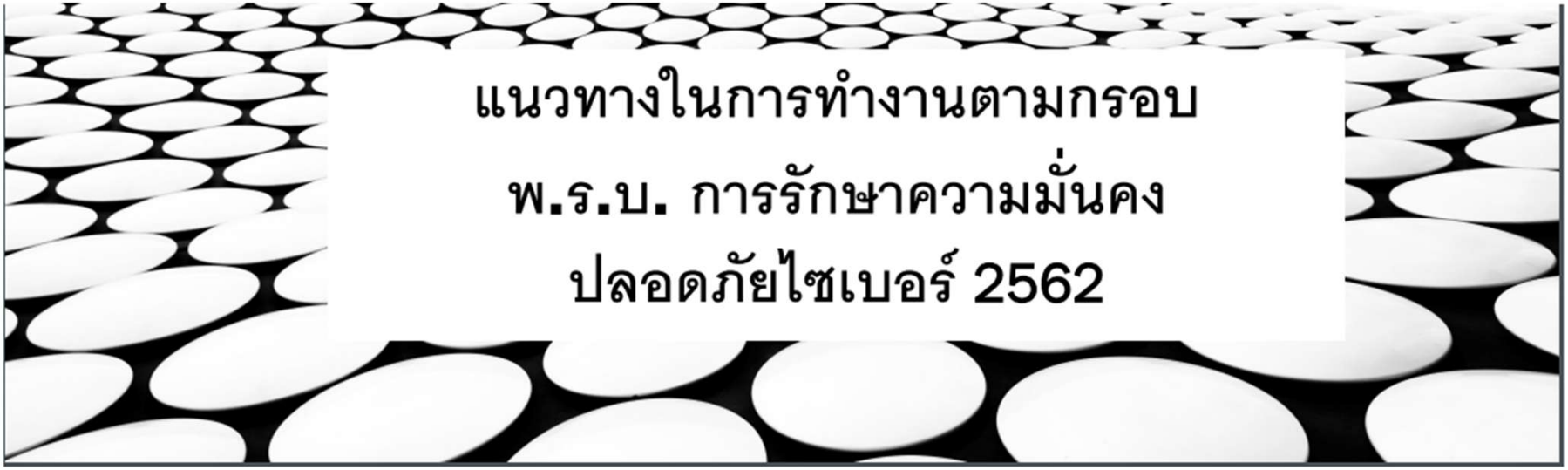
มาตรฐานสำคัญจำเป็นต่อความปลอดภัย	เป้าหมาย	ต.ค.-68	พ.ย.-68	ธ.ค.-68	ม.ค.-69	ก.พ.-69	มี.ค.-69	เม.ย.-69
การให้เลือดผิดคน ผิดหมู่ ผิดชนิด	0 ครั้ง	0	0	0	0	0	0	0
จำนวนครั้งของการการรายงานผลผิดพลาด Near miss	ไม่เกิน 5 ครั้งต่อเดือน	1	0	0	0	0	0	1
จำนวนครั้งของการการรายงานผลผิดพลาด Miss	0 ครั้ง/เดือน	0	0	0	0	0	0	0

ทีม IM นำเสนอ กกบ

30 เมษายน 2569

เรื่องเสนอเพื่อทราบ

การอบรมเชิงปฏิบัติการ
หลักสูตรผู้นำการปฏิบัติ (Lead Implementer)
(อุบลราชธานี – 27 หน่วยงาน)

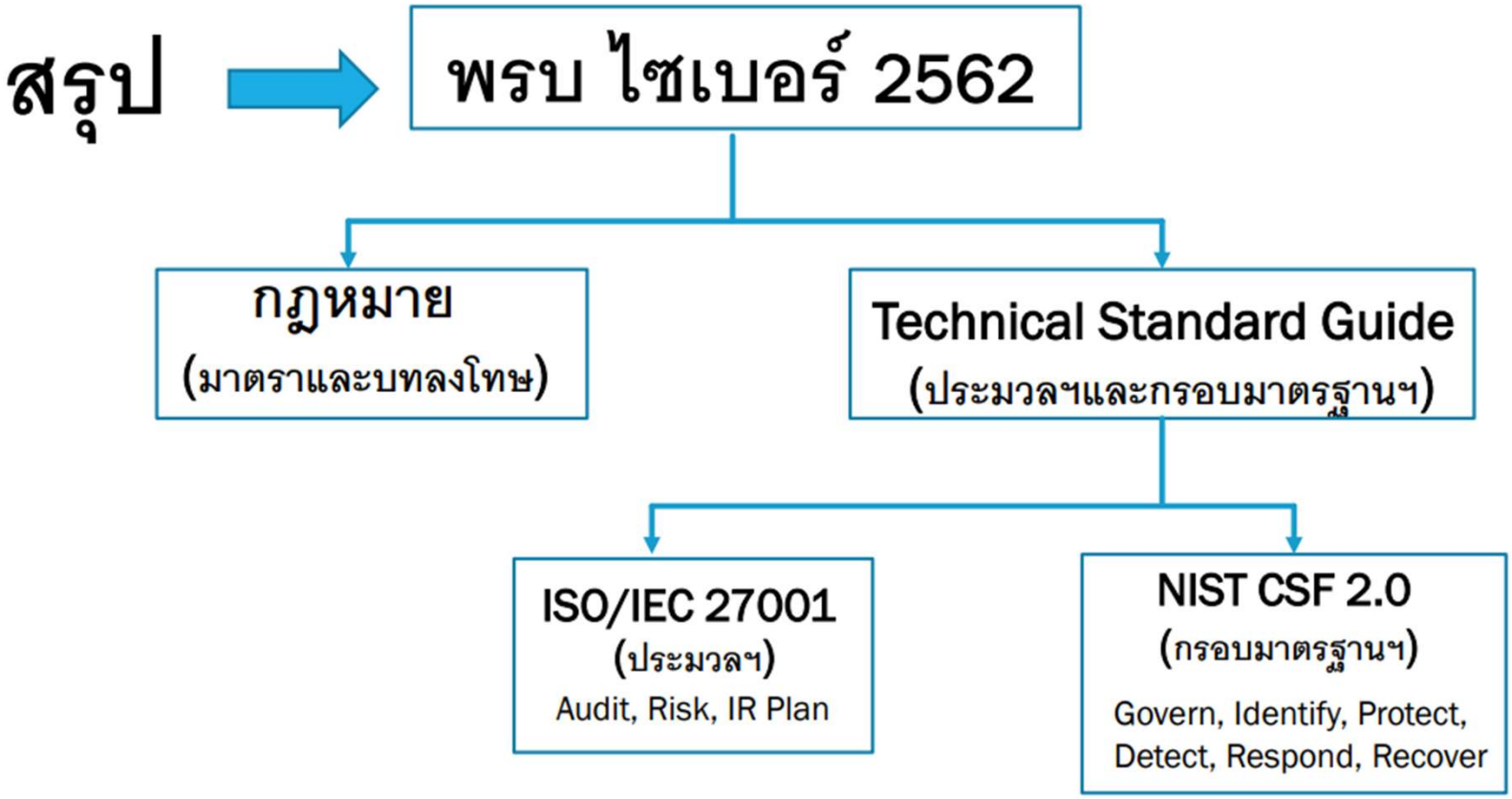


20 – 24 เมษายน 2569

เป้าหมาย

ทุก รพ และ สสจ ใน อุบลราชธานี

1. ขึ้นระบบ พรบ ไซเบอร์ ตามกฎหมาย
2. ผ่านการประเมิน CTAM+, EIA (มิติที่ 6), HS4 (ด้านที่ 9)
3. นำข้อมูลบางอย่างไปใช้กับ HAIT + ได้
4. สนับสนุน / ต่อยอดทำระบบมาตรฐานสากล
   ISO/IEC 27001 : 2022 ได้ไม่ยาก


สรุป
พรบ ไซเบอร์ 2562
กฎหมาย
(มาตราและบทลงโทษ)
Technical Standard Guide
(ประมวลฯและกรอบมาตรฐานฯ)
ISO/IEC 27001
(ประมวลฯ)
Audit, Risk, IR Plan
NIST CSF 2.0
(กรอบมาตรฐานฯ)
Govern, Identify, Protect,
Detect, Respond, Recover

นิยามที่สำคัญ

- CII = Critical Information Infrastructure

  หรือ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

  - CII หมายถึง หน่วยงานทั้งของรัฐและเอกชนที่มีภารกิจสำคัญ ซึ่งหากถูกโจมตีทางไซเบอร์จะส่งผลกระทบต่อความมั่นคงของรัฐ เศรษฐกิจ สาธารณะ หรือชีวิตของประชาชน โดย พ.ร.บ. ไซเบอร์ฯ ได้กำหนดกลุ่มหน่วยงาน CII ไว้หลายภาคส่วน
  - ในกระทรวงสาธารณสุข CII คือหน่วยงานที่มีข้อมูลสารสนเทศของผู้รับบริการ เช่น โรงพยาบาล, สสจ.
- CISO = Chief Information Security Officer
  - เป็นผู้บริหารระดับสูง :- ผู้อำนวยการโรงพยาบาล

บทลงโทษที่สำคัญ (สำหรับหน่วยงาน)

มาตรา	ความผิด	โทษปรับ	โทษจำคุก
73	CII **ไม่รายงานเหตุภัยคุกคามทางไซเบอร์** ที่พบต่อ สกมช. โดยไม่มีเหตุอันสมควร	ไม่เกิน 200,000 บาท	-
59	CII **ไม่ดำเนินการประเมิน/ทดสอบระบบ**ความมั่นคงปลอดภัยไซเบอร์ตามกรอบมาตรฐานที่ สกมช. กำหนด	ไม่เกิน 200,000 บาท + รายวัน ≤ 10,000 บาท	-

ส กม ช ย่อมาจาก **สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ**

บทลงโทษที่สำคัญ (สำหรับหน่วยงาน)

มาตรา	ความผิด	โทษปรับ	โทษจำคุก
74	ไม่ปฏิบัติตาม **หนังสือเรียกของพนักงานเจ้าหน้าที่** หรือไม่ส่งข้อมูล/คอมพิวเตอร์ที่ร้องขอ โดยไม่มีเหตุอันสมควร	ไม่เกิน 100,000 บาท	-

บทลงโทษที่สำคัญ (สำหรับผู้บริหาร/เจ้าหน้าที่ IT)

มาตรา	ความผิด	โทษปรับ	โทษจำคุก
77	กรรมการ/ผู้จัดการ/ผู้บริหาร **สั่งการ หรือละเว้นการสั่งการ** จนเป็นเหตุให้นิติบุคคลกระทำผิด	**รับโทษเท่ากับที่นิติบุคคลต้องรับ** ทุกกรณีที่หน่วยงานถูกลงโทษ	-
75	ไม่ให้ความร่วมมือในการ**รับมือภัยคุกคามระดับร้ายแรง**ตามที่ กกม. สั่ง	ไม่เกิน 200,000 บาท	≤ 1 ปี หรือทั้งจำทั้งปรับ

สรุปประเด็นสำคัญสำหรับผู้บริหาร

สิ่งที่โรงพยาบาลต้องดำเนินการ 3 ข้อหลัก:

1. จัดทำและรักษา Cybersecurity Framework ตามมาตรฐาน สกมช. (มาตรา 47) — หากไม่ทำ ปรับสูงสุด 200,000 บาท + รายวันอีก 10,000 บาท

2. มีระบบรายงานเหตุภัยคุกคาม ต่อ สกมช. (มาตรา 57) ทันทีเมื่อพบหรือสงสัยว่าจะเกิด — หากไม่รายงาน ปรับสูงสุด 200,000 บาท

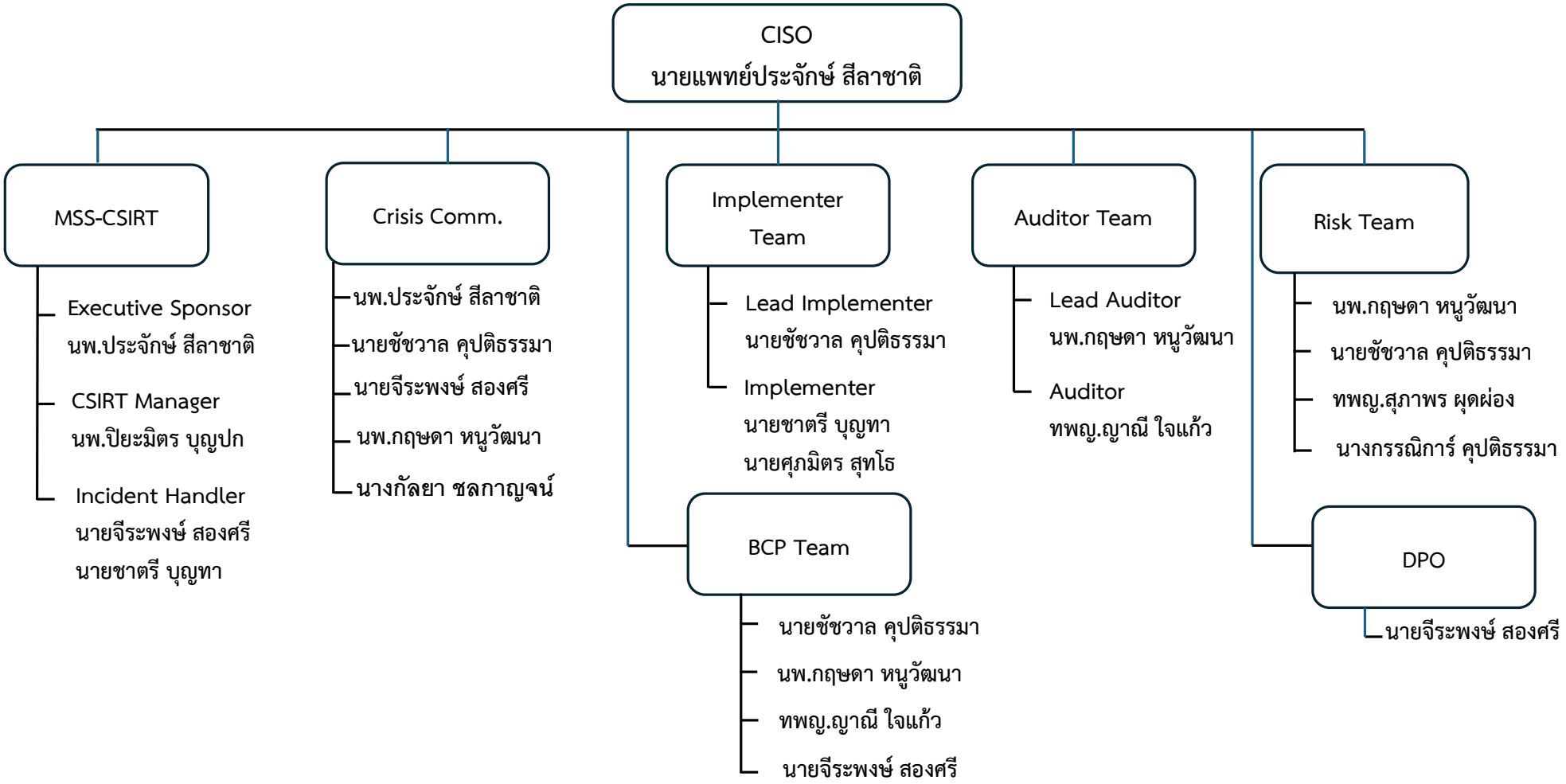
3. ให้ความร่วมมือเจ้าหน้าที่ เมื่อถูกเรียกตรวจสอบ (มาตรา 62) — หากขัดขวาง จำคุกสูงสุด 3 ปี

- **ประเด็นที่กระทบผู้อำนวยการโรงพยาบาลโดยตรงคือ มาตรา 77 ซึ่งกำหนดให้ผู้บริหารต้องรับโทษส่วนตัวร่วมกับโทษที่หน่วยงานได้รับ หากพิสูจน์ได้ว่าการกระทำผิดเกิดจากการละเว้นหน้าที่ในการกำกับดูแล**

สิ่งที่ได้ดำเนินการแล้ว

- กำหนดทีมที่เกี่ยวข้อง กำหนดบทบาทตาม พรบ.
- ส่งคำสั่งแต่งตั้งไปที่ สสจ.อุบลฯ → เขต → สป.
- ออกเอกสาร
  - Policy
  - Procedure
  - Manual
  - Form

แผนผังผู้บริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศระดับสูงและ
คณะทำงานบริหารความมั่นคงปลอดภัยไซเบอร์และข้อมูลสารสนเทศ ประจำโรงพยาบาลม่วงสามสิบ ประจำปีงบประมาณ ๒๕๖๙



ขั้นตอนต่อไป

- BCP
- User permission
- 3rd party