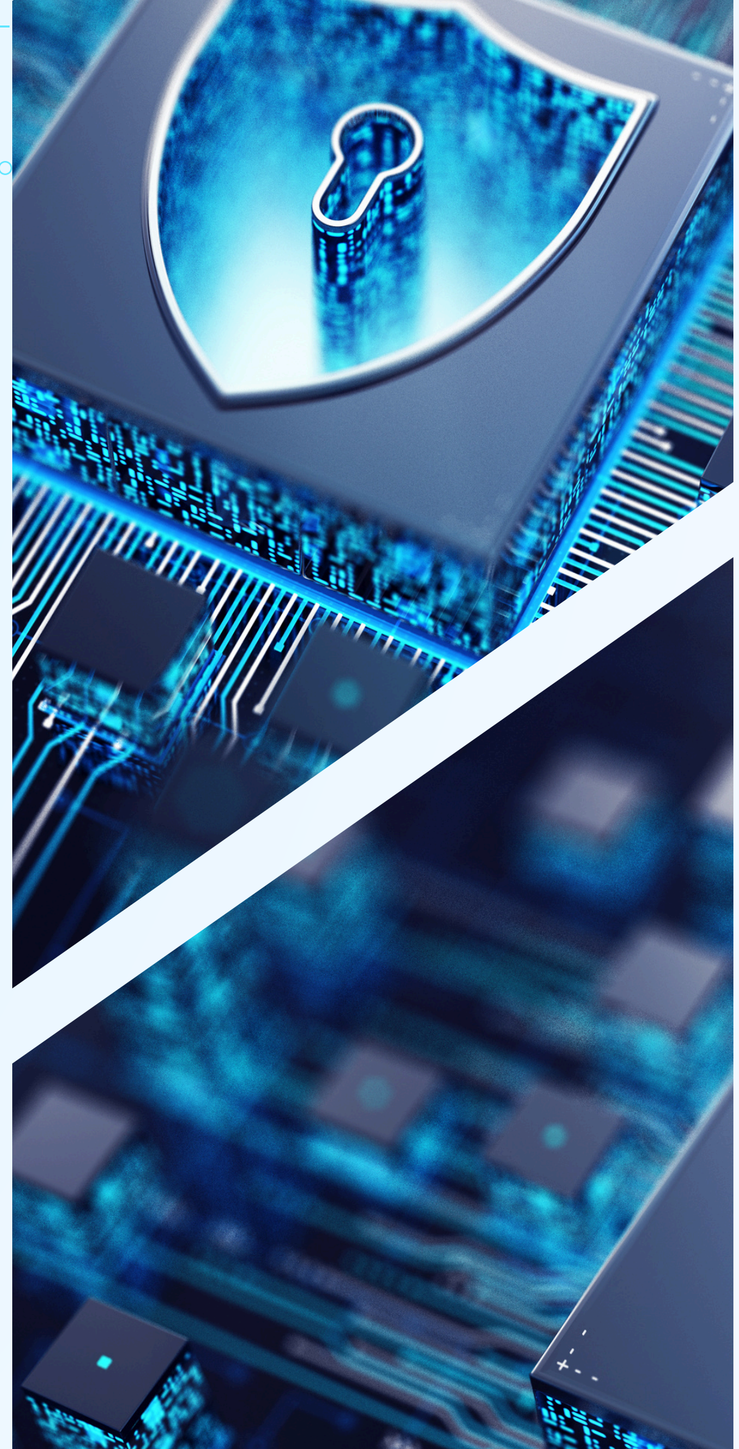
การตรวจราชการและนิเทศกระทรวงสาธารณสุข
กรณีปกติ จังหวัดสตูล
รอบที่ 2/2569

ประเด็นที่ 8 CYBERSECURITY

นพ.ประภัศร์ ติปยานนท์
ประธาน

นพ.ประวิทย์ วรรณโร
ประธานร่วม



เกณฑ์การประเมิน CTAM+ : มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง

เกณฑ์และสัดส่วนการประเมินความปลอดภัยไซเบอร์ภายใต้มาตรฐาน CTAM+ โดยเน้นการปฏิบัติตามมาตรฐานและการรับมือกับสถานการณ์จริง

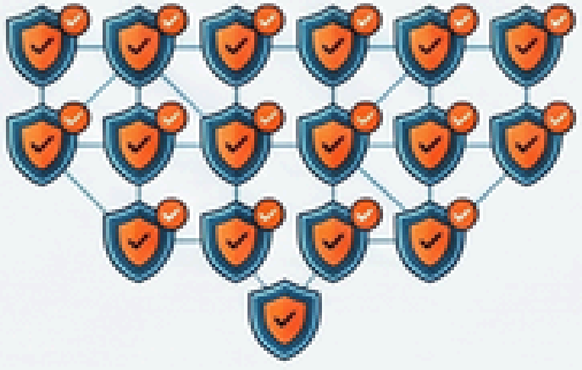
70%

ภาคส่วนเชิงปริมาณ (Quantitative): เน้นการปฏิบัติตามมาตรฐาน

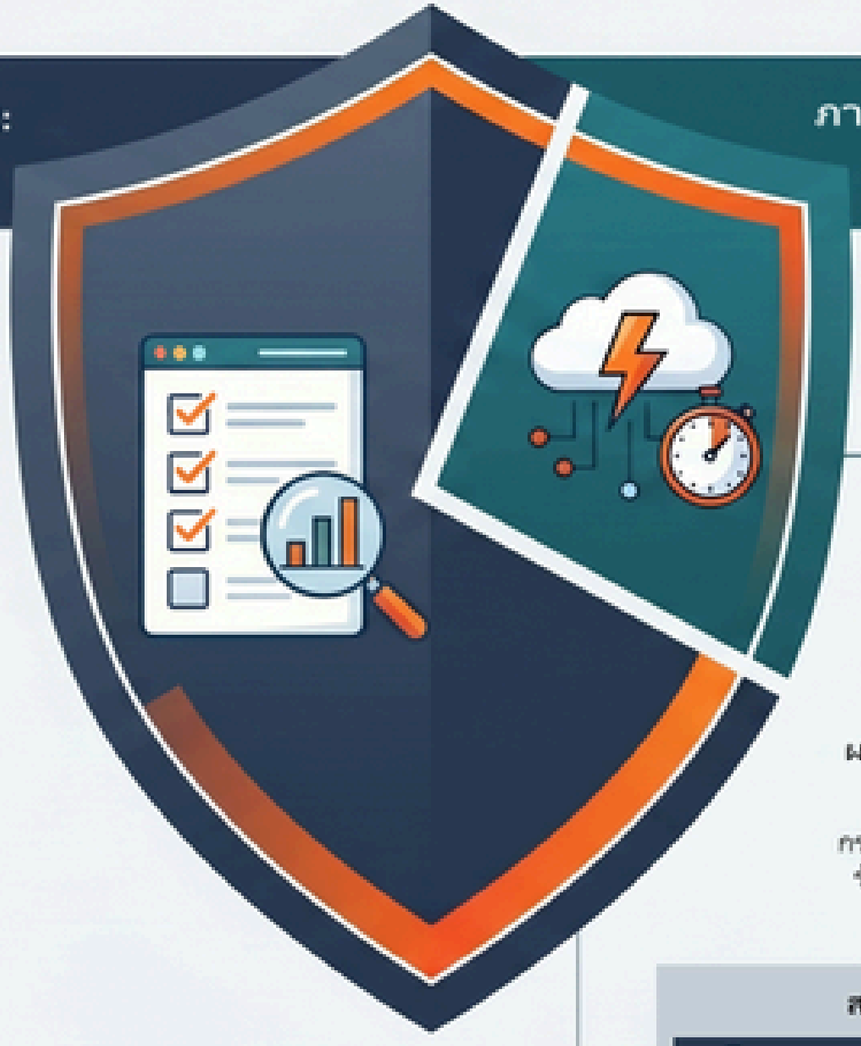
ของสัดส่วนคะแนนหลัก

มุ่งเน้นการตรวจสอบการปฏิบัติตามเกณฑ์ที่กำหนดไว้เป็นตัวเลขและหลักฐานเชิงประจักษ์

ต้องผ่านเกณฑ์มาตรฐานระดับสูง 17 ข้อ



หน่วยงานต้องดำเนินการให้ครบถ้วนทุกข้อตามมาตรฐาน 17 High-Level Standards



30%

ภาคส่วนเชิงคุณภาพ (Qualitative): เน้นการจัดการสถานการณ์จริง

พิจารณาจากประสิทธิภาพในการจัดการเหตุการณ์โจมตีและความปลอดภัยของข้อมูลอย่างรอบด้าน

50 คะแนน

ผลกระทบของข้อมูลรั่วไหลและบทลงโทษ

กรณีข้อมูลส่วนบุคคลรั่วไหลระดับร้ายแรง มีโทษปรับทางปกครองตั้งแต่ 1 - 3 ล้านบาท

50 คะแนน

ระยะเวลาการกู้คืนระบบ (Recovery Time)

ต้องกู้คืนระบบ (เช่น HIS, เว็บไซต์) ให้กลับมาใช้งานปกติภายใน 73 - 96 ชั่วโมง

สรุปเกณฑ์การวัดผลในภาคส่วนเชิงคุณภาพ

ข้อมูลรั่วไหล (Data Breach)	การกู้คืนระบบ (Recovery)
ความรุนแรงของผลกระทบและบทลงโทษทางปกครอง	ความรวดเร็วในการกู้คืนระบบ ภายในเวลาที่กำหนด


สรุปรายงานและรูปแบบการโจมตีทางไซเบอร์ของหน่วยงานในสังกัดสำนักงานสาธารณสุขจังหวัดสตูล
Province 91 Security Report
ช่วงเวลา: 10 ต.ค. 2025 00:00:00 – 1 มิ.ย. 2026 09:00:13 (ICT)
เหตุการณ์ทั้งหมด
36,621,196
เหตุการณ์
1 ระดับวิกฤต (Level 15–14)
29
เหตุการณ์
0.00%
Level 15:
Severe attack – 12 | Shellshock attack detected
Level 14:
High importance – 171 | Short-time multiple Windows Defender warning events
2 ระดับสูง (Level 13–11)
948
เหตุการณ์
Level 13:
720 | CVE-2026-23112 affects linux-image-6.8.0-110-generic
Level 12:
218 | Agent event queue is flooded (173), PUL detected (30), Memory risk (14), Suspicious behaviour (1)
Level 11:
10 | Possible kernel level rootkit
3 ระดับปานกลางค่อนสูง (Level 10–7)
21,800,936
เหตุการณ์
59.5%
Level 10 : 1,904,594
Multiple Windows error application events (1,047,725)
Multiple Windows Error Failures (606,149)
Multiple System error events (192,076)
Auditd promiscuous mode (28,918)
CVE-2022-32743 affects samba-vfs-modules (11,292)
Level 9 : 7,174,421
Windows application error event (7,173,139)
Agent event queue is full (455)
CIS Windows 11 password policy issue (268)
Unhandled exception (234)
Level 8 : 1,639,673
Windows Audit Policy changed (1,608,111)
New external device recognized (28,748)
User account changed (1,868)
Maximum authentication attempts exceeded (904)
sshd possible attack (17)
Level 7 : 11,082,248
Host-based anomaly detection / rootcheck (9,567,696)
Integrity checksum changed (1,470,768)
CVE-2023-24881 affects Microsoft Teams (20,955)
Listened ports status changed (4,606)
4 ระดับปานกลางค่อนต่ำ (Level 6–5)
10,853,261
เหตุการณ์
29.6%
Level 6 : 2,378,523
Common web attack (88,360)
Successful Remote Logon - Administrator
XSS attempt (904)
Suspicious URL access (626)
Level 5 : 8,474,738
Logon Failure - Unknown user or bad password (4,818,889)
Windows System error event (1,471,676)
Registry Value Entry Added (351,385)
Registry Value Entry Deleted (262,541)
5 ระดับต่ำ (Level 4–3)
3,966,022
เหตุการณ์
10.8%
Level 4 : 308,768
Summary event of the reports signature (264,717)
ssh: connection reset (37,476)
Skipped creation of restore point... (3,774)
sshd: connection reset by peer (2,216)
Level 3 : 3,657,254
Windows User Logoff (1,781,218)
Windows Logon Success (1,094,682)
Special privileges assigned to new logon (293,131)
Software protection service scheduled successfully (213,087)
รูปแบบเหตุการณ์เด่นที่พบ
สรุปภาพรวมตามระดับความรุนแรง (Executive Summary)
วิกฤต (Level 15–14) 29 เหตุการณ์ 0.00%
สูง (Level 13–11) 948 เหตุการณ์ 0.00%
ปานกลางค่อนสูง (Level 10–7) 21,800,936 เหตุการณ์ 59.5%
ปานกลางค่อนต่ำ (Level 6–5) 10,853,261 เหตุการณ์ 29.6%
ต่ำ (Level 4–3) 3,966,022 เหตุการณ์ 10.8%
ใช้งานปลอดภัย
ตรวจสอบยืนยันตัวตน
เฝ้าระวังและรายงาน
สายด่วน ICT: 074-711-XXX

มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

CYBERSECURITY TECHNICAL ASSESSMENT MATRIX PLUS : CTAM+

เชิงปริมาณ : เชิงคุณภาพ

70% : 30%

เชิงปริมาณ

ตัวชี้วัดที่ 1: ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง **(ทั้งหมด 17 ข้อ)**

หน่วยบริการ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	รวม	การประเมินผลสัมฤทธิ์
สสจ.สตูล	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	17	ผ่านการอนุมัติระดับกระทรวง
โรงพยาบาลสตูล	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	17	ผ่านการอนุมัติระดับกระทรวง
โรงพยาบาลควนโดน	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	17	ผ่านการอนุมัติระดับกระทรวง
โรงพยาบาลควนกาหลง	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	17	ผ่านการอนุมัติระดับกระทรวง
โรงพยาบาลท่าแพ	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	17	ผ่านการอนุมัติระดับกระทรวง
โรงพยาบาลละงู	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	17	ผ่านการอนุมัติระดับกระทรวง
โรงพยาบาลทุ่งหว้า	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	17	ผ่านการอนุมัติระดับกระทรวง
โรงพยาบาลมะนัง	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	17	ผ่านการอนุมัติระดับกระทรวง

MISSION COMPLETED

มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

CYBERSECURITY TECHNICAL ASSESSMENT MATRIX PLUS : CTAM+

เชิงปริมาณ : เชิงคุณภาพ
70% : 30%

เชิงคุณภาพ

ตัวชี้วัดที่ 2: หน่วยบริการภายในเขตสุขภาพ เกิดเหตุการณ์การโจมตีทางไซเบอร์ของระบบ HIS หรือ WEBSITE องค์กร หรือ FACEBOOK องค์กร จนทำให้ระบบไม่สามารถให้บริการได้ โดยใช้เวลากู้คืน 24 - 96 ชั่วโมง **(คะแนนเต็ม 50 คะแนน)**

RESULTS ไม่เกิดเหตุการณ์ → 50 คะแนน → PASSED ผ่านเกณฑ์

ตัวชี้วัดที่ 3: มีเหตุการณ์รั่วไหลของฐานข้อมูลของโรงพยาบาล (HIS DATA BREACH) หรือมีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ และ สคส.วินิจฉัยโทษทางปกครอง ระดับร้ายแรง ปรับ 1 ล้านบาท – 3 ล้านบาท **(คะแนนเต็ม 50 คะแนน)**

RESULTS ไม่มีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ → 50 คะแนน → PASSED ผ่านเกณฑ์

SCORE เชิงปริมาณ + SCORE เชิงคุณภาพ = (คะแนนเต็ม 10)

ผลการประเมิน : 7 + 3 = 10 คะแนน

สรุปผลการประเมินโรงพยาบาล 4 จังหวัด

ผลการประเมินโรงพยาบาลตามเกณฑ์มาตรฐาน 17 ข้อ ในพื้นที่ 4 จังหวัดเป้าหมาย

1. ปัตตานี

7.7%

ผ่านเกณฑ์

ผ่านเพียง 1 แห่ง
จากโรงพยาบาลทั้งหมด
13 แห่ง

2. พัทลุง

83.3%

ผ่านเกณฑ์

ผ่านครบ 10 แห่ง
จากที่ได้รับการประเมิน
แล้ว 12 แห่ง

3. สงขลา

57.9%

ผ่านเกณฑ์

ผ่าน 11 แห่ง
จากที่ได้รับการประเมิน
แล้ว 19 แห่ง

4. สตูล

100%

ผ่านเกณฑ์

ผ่านครบถ้วนทั้ง 8 แห่ง
ที่ได้รับการประเมิน

การพัฒนาคุณภาพสารสนเทศโรงพยาบาล
HOSPITAL ACCREDITATION INFORMATION TECHNOLOGY : HAIT

🎯 **รพ.รับการประเมินและผ่านการประเมินเพิ่มขึ้นร้อยละ 10 ของรพ.ที่ยังไม่ผ่านมาตรฐาน**

ผ่านการประเมินแล้ว 4 แห่ง

ยังไม่ผ่านการประเมิน 3 แห่ง

ยื่นประเมินในปี 2569 1 แห่ง

จังหวัดสตูล จำนวน 7 โรงพยาบาล

หน่วยบริการ	การประเมิน	Level
โรงพยาบาลสตูล	✅ ผ่านการประ...	Level 1+
โรงพยาบาลควนโดน	✅ ผ่านการประ...	Level 1+
โรงพยาบาลท่าแพ	✅ ผ่านการประ...	Level 1+
โรงพยาบาลละงู	✅ ผ่านการประ...	Level 3+
โรงพยาบาลควนกาหลง	กำลังดำเนินการ	ยังไม่ผ่าน
โรงพยาบาลทุ่งหว้า	กำลังดำเนินการ	ยังไม่ผ่าน
โรงพยาบาลมะนัง	กำลังดำเนินการ	ยังไม่ผ่าน

แผนขับเคลื่อนมาตรฐาน HAIT จังหวัดสตูล (2569 - 2570)

รพ.ละงู ยื่นประเมิน Level 4

มุ่งสู่ระดับมาตรฐานความเชี่ยวชาญระดับสูง

รพ.สตูล เตรียม Pre-Survey Level 2-3

ประเมินความพร้อมเบื้องต้น ก่อนก้าวสู่ระดับถัดไป

รพ.ท่าแพ ยื่นประเมิน Level 2-3

พัฒนามาตรฐานระบบสารสนเทศต่อเนื่อง

รพ.ควนโดน ยื่นประเมิน Level 3

ยกระดับมาตรฐานการจัดการข้อมูลให้มีประสิทธิภาพ

เป้าหมายปี 2569: 3 รพ. ประเมินตนเอง

รพ.ควนกาหลง, มะนัง, และทุ่งหว้า ต้องผ่านการประเมินจากทีมจังหวัด/เขต

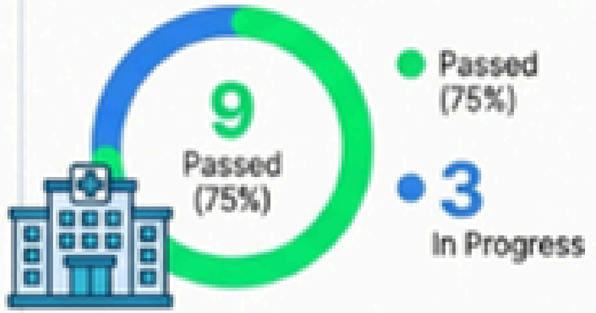
เป้าหมายปี 2570: ผ่าน TMI อย่างน้อย 1 แห่ง

โดยเน้นผลสำเร็จที่ รพ.ทุ่งหว้า ให้ผ่านการประเมินมาตรฐานสมาคมเวชสารสนเทศไทย (TMI)

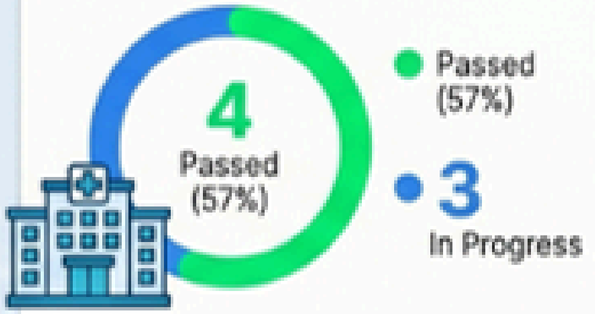
สรุปผลการดำเนินงาน HAIT: 4 จังหวัดภาคใต้และเป้าหมายปี 2569

สถานะการประเมินรายจังหวัด

ปัตตานี

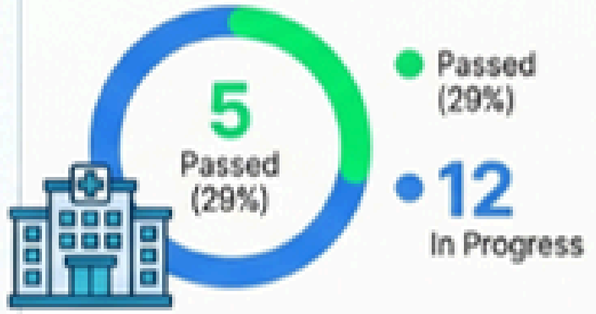


สตูล

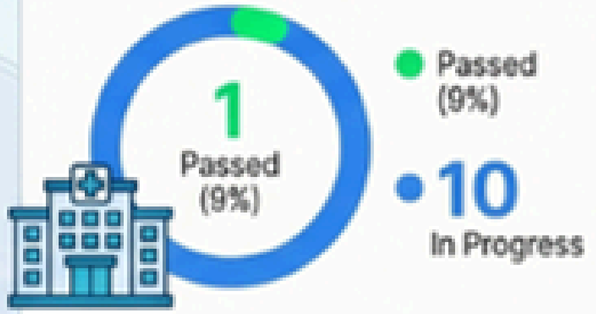


ปัตตานีและสตูลมีสัดส่วนการผ่านเกณฑ์สูงสุด

สงขลา



พัทลุง



สงขลาและพัทลุงเร่งขับเคลื่อนการประเมิน

รวมโรงพยาบาลที่อยู่ระหว่างดำเนินการถึง 22 แห่ง เพื่อให้บรรลุเป้าหมายการพัฒนา

เป้าหมายและไฮไลท์สำคัญปี 2569 (2026 Roadmap)

เป้าหมายเพิ่มอัตราการผ่านเกณฑ์ 10%

มุ่งเน้นให้โรงพยาบาลที่ยังไม่ผ่านมาตรฐานเดิม ได้รับการรับรองเพิ่มขึ้นในปีงบประมาณถัดไป

การยกระดับ L3 และ L4 ในปี 2569

- รพ.ปัตตานี เตรียมยื่น L3 — มิ.ย. 69
- รพ.สะอุ เตรียมยื่น L4 — 27 ส.ค. 69

การเตรียมความพร้อมยื่นประเมินใหม่

มีโรงพยาบาลที่มีกำหนดการยื่นประเมินในปี 2569 อย่างเป็นทางการแล้ว 2 แห่ง

ประเด็นปัญหาจากพื้นที่

- มีข้อจำกัดด้านโครงสร้างพื้นฐานและพื้นที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
- รพ.ท่าแพ และ รพ.ทุ่งหว้า ยังไม่มีตำแหน่งข้าราชการนักวิชาการคอมพิวเตอร์รองรับภารกิจด้านเทคโนโลยีสารสนเทศ

ข้อเสนอแนะ

- พัฒนาโครงสร้างพื้นฐานและพื้นที่ปฏิบัติงานด้าน IT ให้เหมาะสม
- สนับสนุนอัตรากำลังและพัฒนาศักยภาพบุคลากรด้านเทคโนโลยีสารสนเทศให้เพียงพอต่อภารกิจงาน


Thank you
โรงพยาบาลมะนัง