การตรวจราชการและนิเทศกระทรวงสาธารณสุข
กรณีปกติ จังหวัดสตูล
รอบที่ 1/2569

ประเด็นที่ 8 CYBERSECURITY

ประเด็นที่ 8 ร้อยละของหน่วยงาน ที่ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัย ไซเบอร์ระดับสูง

เชิงคุณภาพ

เชิงปริมาณ

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

เชิงคุณภาพ

ตัวชี้วัดที่ 2: หน่วยบริการภายในเขตสุขภาพ เกิดเหตุการณ์การโจมตีทางไซเบอร์ของระบบ HIS หรือ WEBSITE องค์กร หรือ FACEBOOK องค์กร จนทำให้ระบบไม่สามารถให้บริการได้ โดยใช้เวลากู้คืน 73 - 96 ชั่วโมง **(คะแนนเต็ม 50 คะแนน)**

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

เกณฑ์การประเมินความมั่นคงปลอดภัยไซเบอร์ สธ. ปี 2569

1.การประเมินเชิงปริมาณ 70%

วัดความสำเร็จของหน่วยงาน ที่ผ่านเกณฑ์มาตรฐานระดับสูง

หน่วยงานทั้งหมดของจังหวัดผ่าน เกณฑ์ CTAM+ 17 ข้อ

เกณฑ์การให้คะแนน (ตัวอย่าง)

10 คะแนน (ดีเยี่ยม)	ไม่น้อยกว่าร้อยละ 80 (รพ. ระดับ M1, S, A ผ่านเกณฑ์)
5 คะแนน (พอใช้)	ไม่น้อยกว่าร้อยละ 55
1 คะแนน (ปรับปรุง)	ไม่น้อยกว่าร้อยละ 35

2. การประเมินเชิงคุณภาพ (30%) ความปลอดภัยของผู้ป่วยและข้อมูล

ระดับ 5 : ดีเยี่ยม (86 - 100 คะแนน)

ไม่เกิดเหตุโจมตีทางไซเบอร์จมระบบล่ม และไม่มีเหตุข้อมูลรั่วไหลที่ถูกลงโทษ

ระดับ 4: ดี (71 - 85 คะแนน)

กู้คืนระบบจากการโจมตีได้ใน 24 ชม. และเหตุข้อมูลรั่วไหลมีโทษสถานเบา (ให้อบรม)

ระดับ 3: พอใช้ (56 - 70 คะแนน)

กู้คืมระบบได้ใน 25-48 ชม. และเหดุข้อมูลรั่วไหลมีโทษไม่ร้ายแรง (ให้แก้ไขกระบวนการ)

ระดับ 2: ต้องพัฒนา (41-55 คะแนน)

กู้คืนระบบใช้เวลา 49-72 ชม. และเหตุข้อมูลรั่วไหลมีโทษปรับไม่เกิน 1 ล้านบาท

ระดับ 1: ต้องเร่งแก้ไข (< 40 คะแนน)

กู้คืนระบบใช้เวลา 73-96 ชม. และเหตุข้อมูลรั่วไหลมีโทษปรับ 1-3 ล้านบาท

การคำนวณคะแนนผลการประเมินตัวชี้วัดการตรวจราชการ คิดอัตราส่วน 70 : 30

ระดับคะแนนเชิงปริมาณ (70%)	ระดับคะแนนเชิงคุณภาพ ด้านผลลัพธ์ (30%)
ระดับคะแนนที่ได้ x 0.7 = Score	(คะแนนที่ได้ ÷ 10) x 0.3 = Score
Score เชิงปริมาณ + Score เชิงคุณภาพ = (คะแนนเต็ม 10)	

มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

CYBERSECURITY TECHNICAL ASSESSMENT MATRIX PLUS : CTAM+

เชิงปริมาณ : เชิงคุณภาพ
70% : 30%

เชิงปริมาณ

0 X 0.7 = 0 คะแนน

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

หน่วยบริการ	จำนวนข้อที่ผ่าน (เต็ม 17 ข้อ)	แปลผล
สสจ.สตูล	15	ไม่ผ่าน
โรงพยาบาลสตูล	15	ไม่ผ่าน
โรงพยาบาลควนโดน	15	ไม่ผ่าน
โรงพยาบาล	15	ไม่ผ่าน
โรงพยาบาลท่าแพ	16	ไม่ผ่าน
โรงพยาบาลละงู	15	ไม่ผ่าน
โรงพยาบาลทุ่งหว้า	15	ไม่ผ่าน
โรงพยาบาลมะนัง	15	ไม่ผ่าน

FAILED ไม่ผ่านเกณฑ์

เกณฑ์การประเมินผล ด้านผลกระทบตามกรอบ Result

ผลกระทบ	หัวข้อการประเมิน	เกณฑ์คุณภาพระดับ 1 0 - 40 คะแนน	เกณฑ์คุณภาพระดับ 2 41 - 55 คะแนน	เกณฑ์คุณภาพระดับ 3 56 - 70 คะแนน	เกณฑ์คุณภาพระดับ 4 71- 85 คะแนน	เกณฑ์คุณภาพระดับ 5 86 - 100 คะแนน	เอกสารหรือหลักฐานที่ใช้ประเมิน
ความปลอดภัยของผู้ป่วยและข้อมูล	ภายในจังหวัด หรือ ภายในเขตสุขภาพ สามารถดูแลกันเองได้ด้วยตัวเอง ลดการพึ่งพาหน่วยงานเอกชน ใช้ซอฟต์แวร์แบบ Opensource ในการดำเนินงาน รวมถึงช่วยกันต่อรองในส่วนที่จำเป็นต้องใช้งบประมาณ เช่น Firewall , Server ค่า MA หรือค่าใช้จ่ายอื่นๆ เป็นต้น	1. หน่วยบริการภายในเขตสุขภาพ เกิดเหตุการณ์การโจมตีทางไซเบอร์ของระบบ HIS หรือ Website องค์กร หรือ Facebook องค์กร จนทำให้ระบบไม่สามารถให้บริการได้ โดยใช้เวลากู้คืน 73 - 96 ชั่วโมง (20 คะแนน) 2. มีเหตุการณ์รั่วไหลของฐานข้อมูลของโรงพยาบาล (HIS Data Breach) หรือมีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ และ สคส.วินิจฉัยโทษทางปกครอง ระดับร้ายแรง ปรับ 3 ล้านบาท - 1 ล้านบาท (20 คะแนน)	1. หน่วยบริการภายในเขตสุขภาพ เกิดเหตุการณ์การโจมตีทางไซเบอร์ของระบบ HIS หรือ Website องค์กร หรือ Facebook องค์กร จนทำให้ระบบไม่สามารถให้บริการได้ โดยใช้เวลากู้คืน 49 - 72 ชั่วโมง (27.5 คะแนน) 2. มีเหตุการณ์รั่วไหลของฐานข้อมูลของโรงพยาบาล (HIS Data Breach) หรือมีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ และ สคส.วินิจฉัยโทษทางปกครองระดับร้ายแรง ปรับ ไม่เกิน 1 ล้านบาท (27.5 คะแนน)	1. หน่วยบริการภายในเขตสุขภาพ เกิดเหตุการณ์การโจมตีทางไซเบอร์ของระบบ HIS หรือ Website องค์กร หรือ Facebook องค์กร จนทำให้ระบบไม่สามารถให้บริการได้ โดยใช้เวลากู้คืน 25 - 48 ชั่วโมง (35 คะแนน) 2. มีเหตุการณ์รั่วไหลของฐานข้อมูลของโรงพยาบาล (HIS Data Breach) หรือมีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ และ สคส.วินิจฉัยโทษทางปกครองระดับไม่ร้ายแรง และให้แก้ไขหรือปรับปรุงกระบวนการหรือเอกสารที่เกี่ยวข้อง (35 คะแนน)	1. หน่วยบริการภายในเขตสุขภาพ เกิดเหตุการณ์การโจมตีทางไซเบอร์ของระบบ HIS หรือ Website องค์กร หรือ Facebook องค์กร จนทำให้ระบบไม่สามารถให้บริการได้ โดยใช้เวลากู้คืนไม่เกิน 24 ชั่วโมง (42.5 คะแนน) 2. มีเหตุการณ์รั่วไหลของฐานข้อมูลของโรงพยาบาล (HIS Data Breach) หรือมีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ และ สคส.วินิจฉัยโทษทางปกครองระดับไม่ร้ายแรง และให้อบรมเจ้าหน้าที่เพิ่มเติม (42.5 คะแนน)	1. หน่วยบริการภายในเขตสุขภาพ ไม่เกิดเหตุการณ์การโจมตีทางไซเบอร์ของระบบ HIS หรือ Website องค์กร หรือ Facebook องค์กร จนทำให้ระบบไม่สามารถให้บริการได้ (50 คะแนน) 2. ไม่มีเหตุการณ์รั่วไหลของฐานข้อมูลของโรงพยาบาล (HIS Data Breach) หรือไม่มีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ ที่ สคส.วินิจฉัยลงโทษทางปกครอง (50 คะแนน)	1. หลักฐาน Log จาก Firewall,SEIM, XDR/EDR, หรือ อื่นๆ ที่เกี่ยวข้อง 2. คำตัดสินของ สคส.

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 73 - 96 ชั่วโมง **(คะแนนเต็ม 50 คะแนน)**

[10 / 10] X 0.3 = 3 คะแนน

RESULTS ไม่เกิดเหตุการณ์ | 50 คะแนน | PASSED ผ่านเกณฑ์

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

RESULTS ไม่มีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ | 50 คะแนน | PASSED ผ่านเกณฑ์

SCORE เชิงปริมาณ + SCORE เชิงคุณภาพ = (คะแนนเต็ม 10)

ผลการประเมิน: 0 + 3 = 3 คะแนน

มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์

CYBERSECURITY TECHNICAL ASSESSMENT MATRIX PLUS : CTAM+

ร้อยละของหน่วยงานที่ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง ร้อยละ 100

FAILED ไม่ผ่านเกณฑ์

ปัญหา/อุปสรรค

- การใช้ซอฟต์แวร์ถูกลิขสิทธิ์มีค่าใช้จ่ายสูงและต้องมีการบำรุงรักษา(MA) ที่เป็นภาระทางการเงินอย่างต่อเนื่อง
- หลักสูตรอบรมการพัฒนาทักษะของผู้ดูแล โค้วต้าการอบรมของส่วนกลางไม่เพียงพอต่อ รพ.ที่มีอยู่

ข้อเสนอแนะ

- งบประมาณด้าน Cybersecurity ควรเป็นส่วนหนึ่งของงบดำเนินงานปกติ
- ควรมีการ workshop ร่วมกันเพื่อแลกเปลี่ยนความรู้และช่วยแก้ปัญหาร่วมกัน
- ใช้ซอฟต์แวร์ Opensource
- ควรหางบประมาณอบรมพัฒนาเพิ่มพูนทักษะ

การพัฒนาคุณภาพสารสนเทศโรงพยาบาล
HOSPITAL ACCREDITATION INFORMATION TECHNOLOGY :HAIT

รพ.รับการประเมินและผ่านการประเมินเพิ่มขึ้นร้อยละ 10 ของรพ.ที่ยังไม่ผ่านมาตรฐาน

FAILED **ไม่ผ่านเกณฑ์**

ปัจจัยความสำเร็จ

- ผู้บริหารให้ความสำคัญ ตั้งเป้าหมายให้ผ่านทุกหน่วย
- ใช้ระบบพี่เลี้ยงจากเครือข่ายจังหวัดปัตตานี มาเป็น Surveyor

ปัญหา/อุปสรรค

- ความเข้าใจการพัฒนามาตรฐาน HAIT+ เป็นการพัฒนาระบบ IT
- งบประมาณในการพัฒนา ความมั่นคงปลอดภัยด้านดิจิทัล รพ

ข้อเสนอแนะ

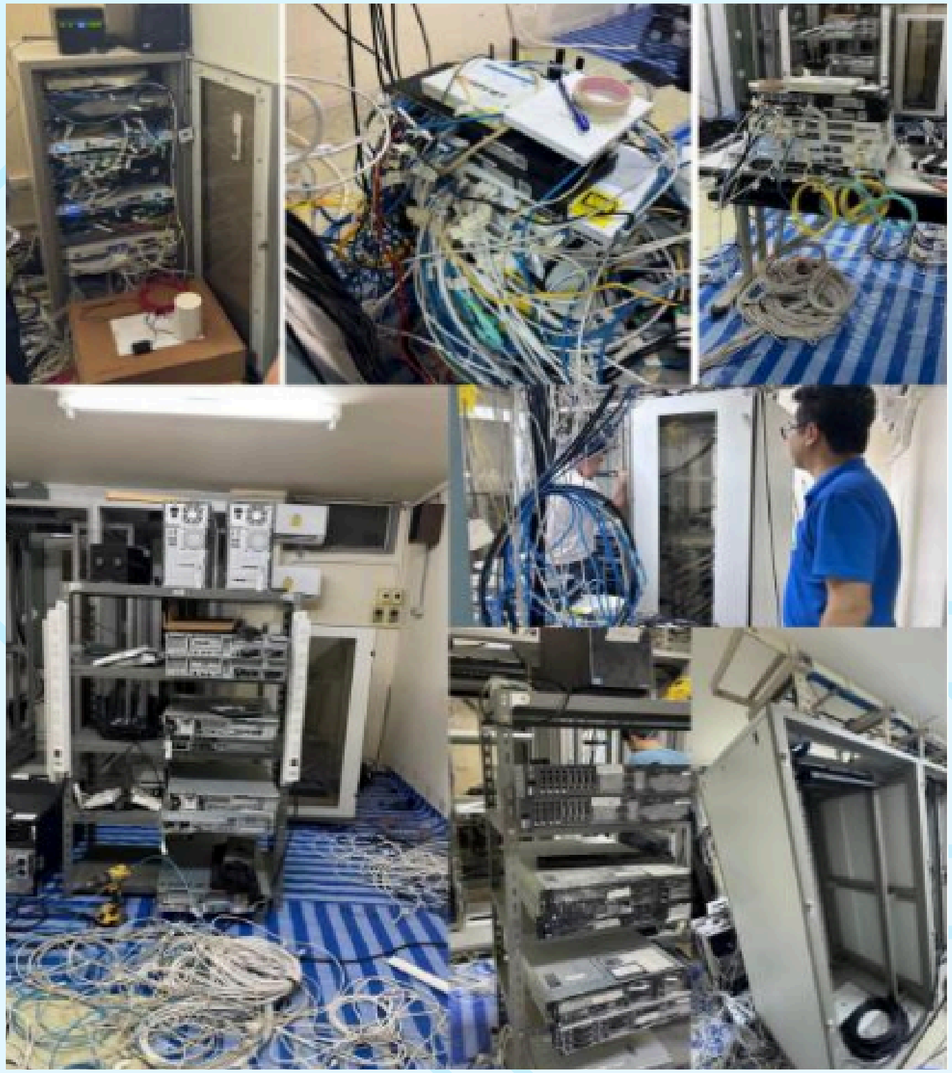
- ใช้การแชร์ประสบการณ์จากรพ.ที่ผ่านการประเมินแล้ว
- รับการประเมินเสมือนจริงจากเครือข่ายทีม Internal Surveyor
- ควรมีงบประมาณจากเขตหรือ จังหวัดให้กับ รพ.ที่พร้อมประเมินแต่ขาดงบประมาณ

หน่วยบริการ	การประเมิน	Level
รพ.สตูล	✅ ผ่านการประ...	Level 1+
รพ.ท่าแพ	✅ ผ่านการประ...	Level 1+
รพ.ควนโดน	✅ ผ่านการประ...	Level 1+
รพ.ละงู	✅ ผ่านการประ...	Level 3+
รพ.ควนกาหลง	กำลังดำเนินการ	ยังไม่ผ่าน
รพ.มะนัง	กำลังดำเนินการ	ยังไม่ผ่าน
รพ.ทุ่งหว้า	กำลังดำเนินการ	ยังไม่ผ่าน

เป้าหมาย

- **ปี 2569** 3 รพ.ที่ยังไม่ผ่าน ประเมินตนเองและรับ**ประเมินโดยทีมระดับจังหวัด/เขต**
- **ปี 2570** ผ่านการประเมินจาก TMI **อย่างน้อย 1 รพ.** (รพ.ทุ่งหว้า)

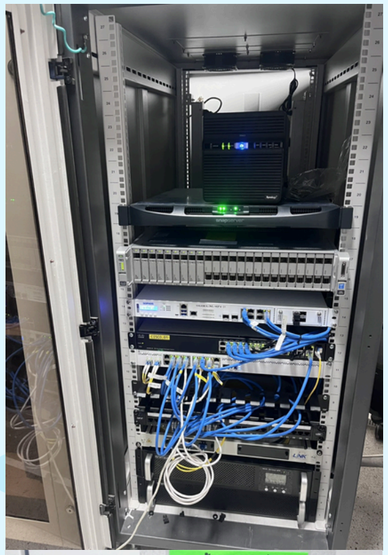
การปรับปรุง DATACENTER ให้ได้มาตรฐาน ของ สสจ.สตูล



รพ.ทุ่งหว้า

ห้อง DATACENTER ของโรงพยาบาลที่ไม่ผ่าน HAIT +

รพ.มะนัง



รพ.ควนกาหลง

รพ.ทุ่งหว้า


Thank you

เกณฑ์ประเมินไซเบอร์สำนักงานปลัดกระทรวงสาธารณสุข 2569

(Cybersecurity Technical Asessment Matrix Plus : CTAM +)

1. **Backup**
   การสำรองข้อมูลเก็บไว้ที่อื่น เพื่อให้สามารถใช้เพื่อกู้คืนข้อมูลเดิมหลังจากเหตุการณ์ข้อมูลสูญหาย
2. **Antivirus Software**
   โปรแกรมป้องกันไวรัส หรือ แอนติไวรัส คอยตรวจจับป้องกัน และกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์
3. **Acess Control**
   การควบคุมอุปกรณ์หรือการเข้าถึงระบบผ่านทางช่องทาง Public/Private ทั้งภายในประเทศและต่างประเทศ
4. **Privileged Access Management (PAM)**
   การรักษาความปลอดภัยของข้อมูล ติดตาม ตรวจหา และป้องกันการใช้สิทธิ์การเข้าถึงทรัพยากรที่สำคัญ
5. **Business Continuity Plan (BCP) Disaster Recovery Plan (DRP)**
   แผนที่กำหนดแนวทางการดำเนินการของหน่วยงาน เมื่อเกิดสภาวะวิกฤต
6. **OS Patching**
   การซ่อมแซมจุดบกพร่องของระบบปฏิบัติการ (OS)หรือปรับปรุงระบบปฏิบัติการให้ทันสมัย
7. **Multi-Factor Authentication (2FA)**
   การยืนยันตัวตน 2 ชั้น เป็นการเข้าสู่ระบบบัญชีแบบ หลายขั้นตอน
8. **Web Application Firewall (WAF)**
   ระบบป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอพพลิเคชั่นโดยเฉพาะ
9. **Log Management**
   จัดเก็บ Log การใช้งานให้เป็นไปตาม พ.ร.บ. คอมพิวเตอร์ฯ อย่างน้อย 90 วัน
10. **Security Information & Even Management (SIEM)**
    มีระบบวิเคราะห์และตรวจจับภัยคุกคามจาก log ของ Server
11. **Vulnerability Assessment (VA Scan)**
    สแกนหาช่องโหว่ประจำปี และดำเนินการปิดช่องโหว่ให้ได้ตามมาตรฐาน

+

01 สำรวจและปิดระบบงานที่ไม่ได้ใช้งานเพื่อป้องกันการเข้าถึงข้อมูล

02 อัปเดตซอฟต์แวร์หรือแพตช์ ด้านความปลอดภัยอยู่เสมอ

03 Network Segmentation การแบ่งแยกเครือข่ายระบบสำคัญ ออกจากเครือข่ายระบบอื่น

04 ใช้ซอฟต์แวร์ถูกลิขสิทธิ์

05 Penetration Testing ทดสอบเจาะระบบสำคัญ หรือ ที่มีความเสี่ยง และแก้ไขช่องโหว่หรือความเสี่ยงนั้น

06 มีนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล รวมถึง การส่งเสริมให้เกิดการพัฒนาบุคลากรด้านดังกล่าว