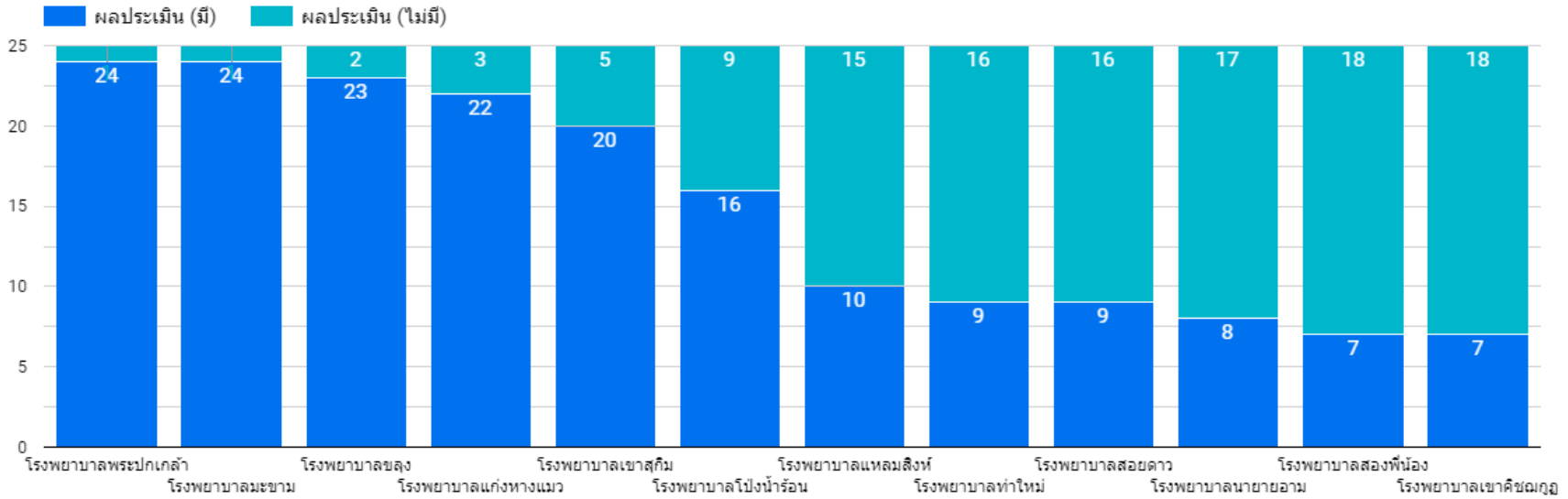
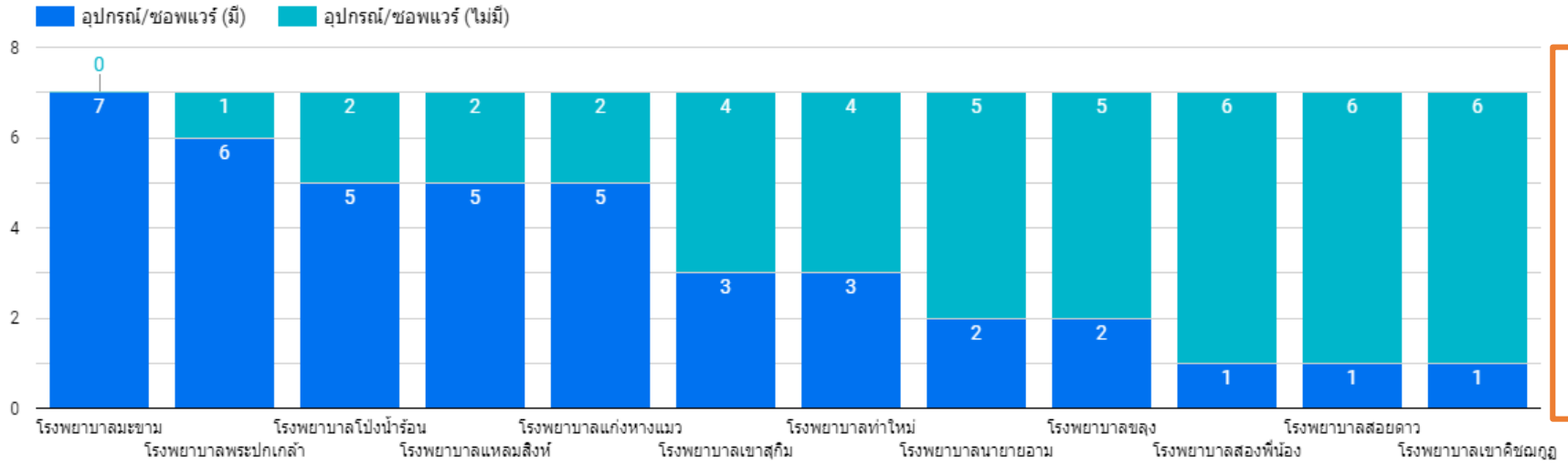
การรักษาความมั่นคงปลอดภัยไซเบอร์ (CYBER SECURITY)

1. การเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์



2. การสำรวจความพร้อมอุปกรณ์/ซอฟต์แวร์ด้านความมั่นคงปลอดภัยไซเบอร์



ประเด็น

1. การประเมินความเสี่ยง (Risk Assessment)
2. แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
3. กรอบมาตรฐาน Cyber security

1. อุปกรณ์Firewall
2. อุปกรณ์จัดเก็บ Log file
3. อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System)
4. อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)
5. โปรแกรมป้องกันไวรัสคอมพิวเตอร์
6. โปรแกรม Endpoint Antivirus
7. โปรแกรมการตรวจจับเหตุการณ์และเฝ้าระวังภัยคุกคามทางไซเบอร์

การยกระดับ CYBER SECURITY

- แผนพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ ระยะ 5 ปี
  - การจัดทำ Network Diagram And Network Security Diagram
  - การจัดซื้ออุปกรณ์/ซอฟต์แวร์
  - การอบรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- การจัดทำนโยบายและคู่มือแนวทางการจัดทำแผนตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนการรับมือภัยคุกคามทางไซเบอร์ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ให้เป็นมาตรฐานเดียวกัน)

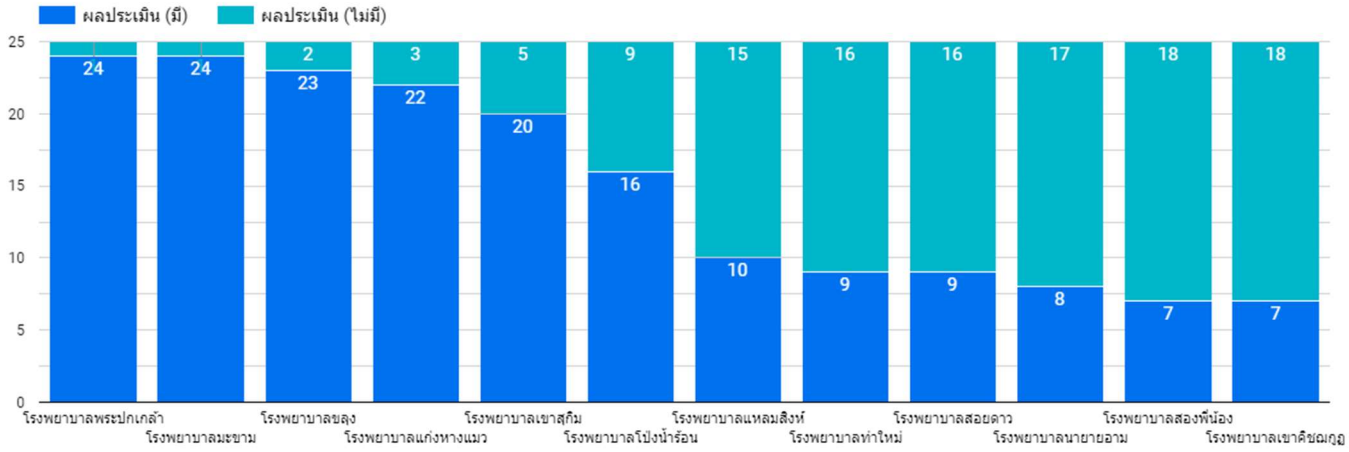
- จัดตั้งที่ปรึกษาในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีความเชี่ยวชาญ

ข้อมูล ณ วันที่ 19 มิถุนายน 2566

แบบสำรวจกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล ในสังกัดสำนักงานสาธารณสุขจังหวัดจันทบุรี

การสำรวจกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลในสังกัดสำนักงานสาธารณสุขจังหวัดจันทบุรี จำนวน 12 โรงพยาบาล ได้แก่ (1) โรงพยาบาลพระปกเกล้า (2) โรงพยาบาลมะขาม (3) โรงพยาบาลขลุง (4) โรงพยาบาลแก่งหางแมว (5) โรงพยาบาลเขาสุกิม (6) โรงพยาบาลโป่งน้ำร้อน (7) โรงพยาบาลแหลมสิงห์ (8) โรงพยาบาลท่าใหม่ (9) โรงพยาบาลสอยดาว (10) โรงพยาบาลนายายอาม (11) โรงพยาบาลสองพี่น้อง และ (12) โรงพยาบาลเขาคิชฌกูฏ มีผลการสำรวจดังนี้

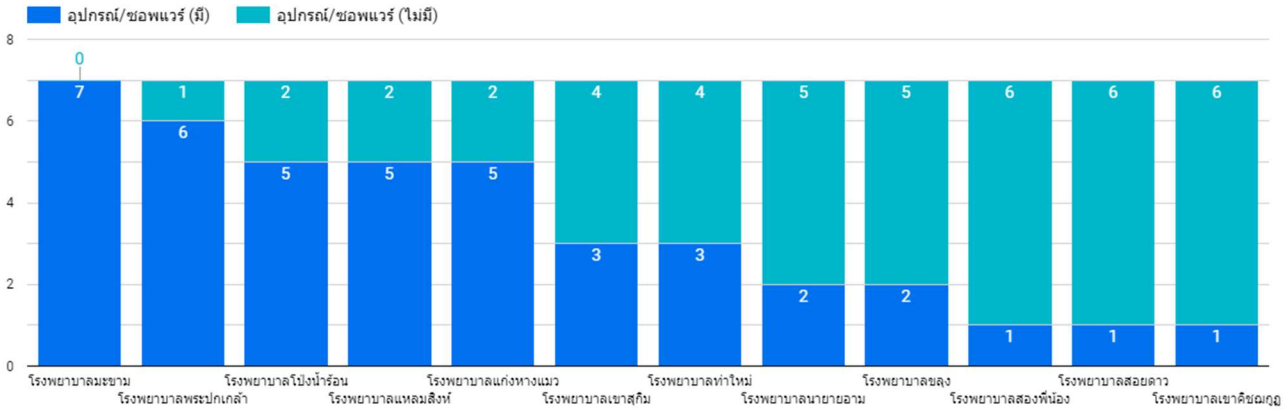
1. การเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์



ภาพที่ 1 การเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์

การเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงานมีการกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การจัดทำระเบียบวิธีปฏิบัติ และกระบวนการในการบริหารความเสี่ยง รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์ พบว่า โรงพยาบายที่มีความพร้อมรับมือภัยคุกคามทางไซเบอร์มากที่สุด ได้แก่ โรงพยาบาลพระปกเกล้า โรงพยาบาลมะขาม โรงพยาบาลขลุง ตามลำดับ ดังแสดงในภาพที่ 1

2. การสำรวจความพร้อมอุปกรณ์/ซอฟแวร์ด้านความมั่นคงปลอดภัยไซเบอร์



ภาพที่ 2 การสำรวจความพร้อมอุปกรณ์/ซอฟแวร์ด้านความมั่นคงปลอดภัยไซเบอร์

การสำรวจความพร้อมอุปกรณ์/ซอฟแวร์ด้านความมั่นคงปลอดภัยไซเบอร์ ได้แก่ อุปกรณ์Firewall อุปกรณ์จัดเก็บ Log file อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) โปรแกรมป้องกันไวรัสคอมพิวเตอร์ โปรแกรม Endpoint Antivirus และโปรแกรมการตรวจจับเหตุการณ์และเฝ้าระวังภัยคุกคามทางไซเบอร์ พบว่าโรงพยาบาลที่มีความพร้อมของอุปกรณ์/ซอฟแวร์ด้านความมั่นคงปลอดภัยไซเบอร์ มากที่สุด ได้แก่ โรงพยาบาลมะขาม โรงพยาบาลพระปกเกล้า โรงพยาบาลโป่งน้ำร้อน โรงพยาบาลแหลมสิงห์ โรงพยาบาลแก่งหาแมว ตามลำดับ ดังแสดงในภาพที่ 2

3. ข้อเสนอแนะ

1) ต้องการสนับสนุนงบประมาณเพื่อจัดซื้ออุปกรณ์ (Hardware) และโปรแกรม (software) ด้านการรักษาความปลอดภัยไซเบอร์ให้เหมาะกับขนาดของโรงพยาบาล

2) จัดอบรมความรู้ด้านการรักษาความปลอดภัยไซเบอร์ เช่น การจัดการระบบเครือข่ายคอมพิวเตอร์ (Network) การใช้อุปกรณ์ในการป้องกันการโจมตี การจัดการเมื่อถูกโจมตีระบบสารสนเทศ เป็นต้น

3) การจัดทำคู่มือแนวทางการจัดทำแผนตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนการรับมือภัยคุกคามทางไซเบอร์ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

4) จัดตั้งที่ปรึกษาในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีความเชี่ยวชาญ เช่น การตั้งค่าการจัดการบริหารระบบเครือข่ายคอมพิวเตอร์ เป็นต้น

ผลการสำรวจกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลในสังกัดสำนักงานสาธารณสุขจังหวัดจันทบุรี

ภาคผนวก

1. การวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1.1 การระบุความเสี่ยง (Risk Identification) ระบุความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ช่องโหว่ต่าง ๆ

หน่วยงาน	กระบวนการปฏิบัติงาน	ระบบงาน	บุคลากร	ปัจจัยภายนอก
โรงพยาบาลโป่งน้ำร้อน	ไม่มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลแหลมสิงห์	ไม่มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลแก่งหางแมว	ไม่มี	ไม่มี	มี	ไม่มี
โรงพยาบาลเขาสุกิม	มี	มี	มี	มี
โรงพยาบาลเขาคิชฌกูฏ	มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลสอยดาว	ไม่มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลสองพี่น้อง	ไม่มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลมะขาม	มี	มี	มี	มี
โรงพยาบาลพระปกเกล้า	มี	มี	มี	ไม่มี
โรงพยาบาลนายายอาม	ไม่มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลท่าใหม่	มี	มี	มี	มี
โรงพยาบาลขลุง	มี	มี	มี	มี

1.2 การแสดงรายละเอียดของความเสี่ยง

หน่วยงาน	ประเมินค่าความเสี่ยง	จัดการความเสี่ยง	ติดตามและทบทวนความเสี่ยง	รายงานความเสี่ยง
โรงพยาบาลโป่งน้ำร้อน	มี	มี	มี	มี
โรงพยาบาลแหลมสิงห์	ไม่มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลแก่งหางแมว	มี	มี	มี	มี
โรงพยาบาลเขาสุกิม	มี	มี	มี	มี
โรงพยาบาลเขาคิชฌกูฏ	มี	มี	ไม่มี	ไม่มี
โรงพยาบาลสอยดาว	ไม่มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลสองพี่น้อง	ไม่มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลมะขาม	มี	มี	มี	มี
โรงพยาบาลพระปกเกล้า	มี	มี	มี	มี
โรงพยาบาลนายายอาม	ไม่มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลท่าใหม่	ไม่มี	ไม่มี	ไม่มี	มี
โรงพยาบาลขลุง	มี	มี	มี	มี

2. แผนการรับมือภัยคุกคามทางไซเบอร์

หน่วยงาน	โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์	การรายงานเหตุการณ์กรณีถูกโจมตีระบบสารสนเทศ	มีขั้นตอนในการเรียกใช้งาน (Activate)	กระบวนการการกู้คืน	ขั้นตอนการสอบสวนสาเหตุ
โรงพยาบาลโป่งน้ำร้อน	ไม่มี	ไม่มี	ไม่มี	มี	มี
โรงพยาบาลแหลมสิงห์	ไม่มี	ไม่มี	ไม่มี	มี	มี
โรงพยาบาลแก่งหางแมว	มี	มี	มี	มี	มี
โรงพยาบาลเขาสุกิม	ไม่มี	ไม่มี	มี	มี	ไม่มี
โรงพยาบาลเขาคิชฌกูฏ	ไม่มี	ไม่มี	ไม่มี	มี	ไม่มี
โรงพยาบาลสอยดาว	ไม่มี	ไม่มี	ไม่มี	มี	ไม่มี
โรงพยาบาลสองพี่น้อง	ไม่มี	ไม่มี	ไม่มี	มี	ไม่มี
โรงพยาบาลมะขาม	มี	มี	มี	มี	มี
โรงพยาบาลพระปกเกล้า	มี	มี	มี	มี	มี
โรงพยาบาลนายายอาม	มี	ไม่มี	ไม่มี	มี	ไม่มี
โรงพยาบาลท่าใหม่	ไม่มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลขลุง	มี	มี	มี	มี	มี

3. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

หน่วยงาน	การควบคุมการเข้าถึง (Access Control)/ การจัดเก็บรักษาบันทึกของการเข้าถึงทั้งหมด	การกำหนดสิทธิ์การเข้าถึงข้อมูล	การยืนยันตัวบุคคล	การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน	การลบบัญชีที่ไม่ได้ใช้	มีการสำรวจและการบลบบริการและแอปพลิเคชั่นที่ไม่จำเป็น	การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน	การป้องกันมัลแวร์	การตรวจสอบการเชื่อมต่อระยะไกล	การอบรมการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์	การปรับปรุงซอฟต์แวร์และแพตช์
โรงพยาบาลโป่งน้ำร้อน	ไม่มี	มี	มี	ไม่มี	มี	มี	มี	มี	มี	มี	มี
โรงพยาบาลแหลมสิงห์	มี	มี	ไม่มี	ไม่มี	มี	มี	มี	มี	มี	ไม่มี	มี
โรงพยาบาลแก่งหางแมว	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี
โรงพยาบาลเขาสุกิม	มี	มี	มี	มี	มี	มี	มี	มี	มี	ไม่มี	มี
โรงพยาบาลเขาคิชฌกูฏ	ไม่มี	มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี	มี	ไม่มี	มี	ไม่มี	ไม่มี
โรงพยาบาลสอยดาว	มี	มี	มี	มี	มี	ไม่มี	มี	มี	ไม่มี	ไม่มี	มี
โรงพยาบาลสองพี่น้อง	มี	มี	ไม่มี	ไม่มี	มี	ไม่มี	มี	มี	ไม่มี	ไม่มี	มี
โรงพยาบาลมะขาม	มี	มี	มี	มี	ไม่มี	มี	มี	มี	มี	มี	มี
โรงพยาบาลพระปกเกล้า	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี
โรงพยาบาลนายายอาม	ไม่มี	มี	มี	ไม่มี	มี	ไม่มี	มี	มี	ไม่มี	ไม่มี	มี
โรงพยาบาลท่าใหม่	มี	มี	มี	มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลขลุง	มี	มี	มี	ไม่มี	มี	มี	มี	มี	มี	ไม่มี	มี

4. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

หน่วยงาน	การตรวจจับเหตุการณ์และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Monitoring)
โรงพยาบาลโป่งน้ำร้อน	มี
โรงพยาบาลแหลมสิงห์	ไม่มี
โรงพยาบาลแก่งหางแมว	มี
โรงพยาบาลเขาสุกิม	ไม่มี
โรงพยาบาลเขาคิชฌกูฏ	ไม่มี
โรงพยาบาลสอยดาว	ไม่มี
โรงพยาบาลสองพี่น้อง	ไม่มี
โรงพยาบาลมะขาม	มี
โรงพยาบาลพระปกเกล้า	มี
โรงพยาบาลนายายอาม	ไม่มี
โรงพยาบาลท่าใหม่	ไม่มี
โรงพยาบาลขลุง	มี

5. การสำรวจอุปกรณ์ที่จำเป็นด้านความมั่นคงปลอดภัยทางไซเบอร์

หน่วยงาน	Firewall	อุปกรณ์จัดเก็บ Log File	อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System)	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	โปรแกรมป้องกันไวรัสคอมพิวเตอร์	โปรแกรม Endpoint Antivirus	โปรแกรมการตรวจจับเหตุการณ์และเฝ้าระวังภัยคุกคามทางไซเบอร์
โรงพยาบาลพระปกเกล้า	Cisco 5508	NT Syslog	Sangfor	Sangfor	Sangfor Enpoint	Sangfor Enpoint	ไม่มี ใช้การดูผ่านหน้า Dashboard Sangfor
โรงพยาบาลมะขาม	Mikrotik	Computer และ external harddisk	Mikrotik	Mikrotik	Avast, Nod32, Avira, Window Defender	Avast, Nod32, Avira, Window Defender	Winbox Mikrotik
โรงพยาบาลแหลมสิงห์	Mikrotik	Mikrotik	Mikrotik	Mikrotik	Windows Security	ไม่มี	ไม่มี
โรงพยาบาลเขาคิชฌกูฏ	มี ในระดับการมีใช้งาน ไม่ใช่ระบบที่เป็นไปตามมาตรฐาน ICT	มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี
โรงพยาบาลสอยดาว	ไม่มี	ไม่มี	ไม่มี	ไม่มี	Windows Defender	ไม่มี	ไม่มี
โรงพยาบาลสองพี่น้อง	ไม่มี	ไม่มี	ไม่มี	ไม่มี	มี Windows Defender	ไม่มี	ไม่มี

หน่วยงาน	Firewall	อุปกรณ์จัดเก็บ Log File	อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System)	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	โปรแกรมป้องกันไวรัสคอมพิวเตอร์	โปรแกรม Endpoint Antivirus	โปรแกรมการตรวจจับเหตุการณ์และเฝ้าระวังภัยคุกคามทางไซเบอร์
โรงพยาบาลนายายอาม	MikroTik CCR1036-12G-4S	ไม่มี	ไม่มี	ไม่มี	Windows Security	ไม่มี	ไม่มี
โรงพยาบาลท่าใหม่	มี	มี Mikrotik	ไม่มี	ไม่มี	windows defender	ไม่มี	ไม่มี
โรงพยาบาลแก่งหางแมว	มี	มี	ไม่มี	มี	มี	มี	ไม่มี
โรงพยาบาลเขาสุกิม	ไม่มีอุปกรณ์ ใช้ Software Firewall	ไม่มีอุปกรณ์ ใช้ Software Firewall จัดเก็บ	ไม่มีอุปกรณ์	ไม่มีอุปกรณ์	Windows Defender	Windows Defender	Win Route
โรงพยาบาลขลุง	ยังไม่มี hardware .ใช้เป็น soft ware จากอุปกรณ์ Mikrotik	ไม่มีอุปกรณ์ในการจัดเก็บ ใช้การเก็บโดยดูจาก log ตัว fire wall ในระบบ	ไม่มี	ไม่มี	nod32 microsoft window defender	โปรแกรมฟรี	ไม่มี
โรงพยาบาลโป่งน้ำร้อน	Mikrotik / DCR1036-12G-4S	Mikrotik / DCR1036-12G-4S	ไม่มี	Mikrotik / DCR1036-12G-4S	Windows Security	Windows Security	ไม่มี