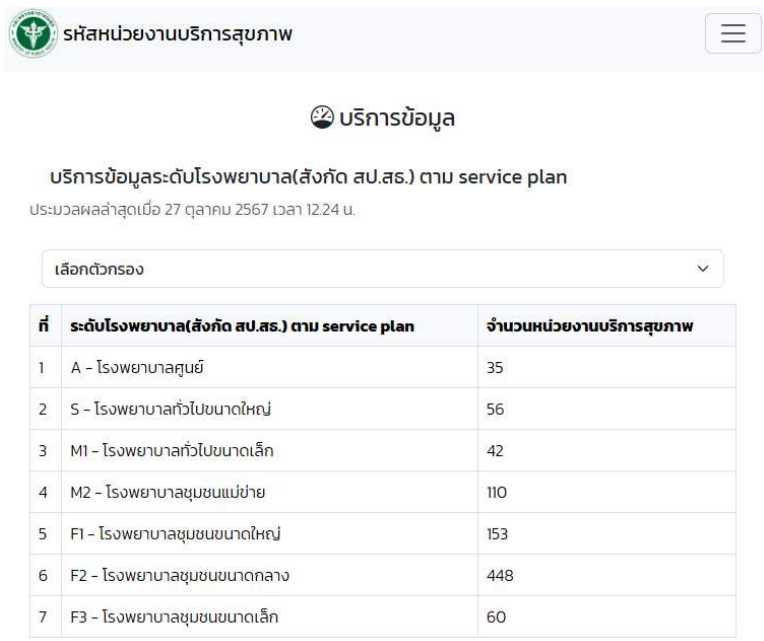


หมวด	Governance Excellence
แผนงาน	การพัฒนาระบบบริการสุขภาพดิจิทัล
โครงการ	โครงการยกระดับความมั่นคงปลอดภัยไซเบอร์
ระดับการแสดงผล	จังหวัด/เขต/ประเทศ
ชื่อตัวชี้วัด	26. ร้อยละของหน่วยงานที่ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง
คำนิยาม	<p>หน่วยงาน หมายถึง โรงพยาบาลศูนย์ โรงพยาบาลทั่วไป โรงพยาบาลชุมชนที่เปิดให้บริการแล้ว สำนักงานสาธารณสุขจังหวัด และ สำนักงานเขตสุขภาพที่ 1 - 12</p>  <p>มาตรฐานความมั่นคงปลอดภัยไซเบอร์ หมายถึง เกณฑ์การประเมิน Cybersecurity Assessment Matrix เช่นเดียวกับปีงบประมาณ พ.ศ. 2567 (จะมีหนังสือแจ้งเวียนเกณฑ์)</p> <div style="border: 1px solid green; padding: 10px; margin: 10px 0;"> <p style="text-align: center; background-color: #90EE90; margin: 0;">เกณฑ์การประเมิน</p> <div style="border: 2px solid red; padding: 5px; margin: 5px 0;"> <p>1. Backup 2. Antivirus Software 3. Access Control (Public และ Private) 4. Privileged Access Management (PAM)</p> </div> <div style="border: 2px solid orange; padding: 5px; margin: 5px 0;"> <p>5. Business Continuity Plan (BCP) และ Disaster Recovery Plan (DRP) 6. OS Patching 7. Multi-Factor Authentication (2FA) 8. Web Application Firewall (WAF) 9. Log Management 10. Security Information & Event Management (SIEM) 11. Vulnerability Assessment (VA Scan)</p> </div> <div style="border: 2px solid green; padding: 5px; margin: 5px 0;"> <p>12. Software Update -> Optional 13. Penetration Testing -> Optional 14. Disaster Recovery site (DR) -> Optional</p> </div> </div>

เกณฑ์เป้าหมาย : ร้อยละของหน่วยงานที่ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง				
ปีงบประมาณ 68	ปีงบประมาณ 69	ปีงบประมาณ 70	ปีงบประมาณ 71	
ร้อยละ 100 ของหน่วยงานผ่านเกณฑ์ฯ ระดับสูง	ร้อยละ 100 ของหน่วยงานผ่านเกณฑ์ฯ ระดับสูง	ร้อยละ 100 ของหน่วยงานผ่านเกณฑ์ฯ ระดับสูง	ร้อยละ 100 ของหน่วยงานผ่านเกณฑ์ฯ ระดับสูง	
วัตถุประสงค์	<ol style="list-style-type: none"> 1. เพื่อให้หน่วยงานมีความพร้อมรับมือเหตุการณ์ฉุกเฉินทางคอมพิวเตอร์ ด้วยระบบป้องกัน ตรวจสอบ วิเคราะห์ และโต้ตอบต่อภัยคุกคามทางไซเบอร์ 2. เพื่อลดความรุนแรงของผลกระทบกรณีหน่วยงานถูกคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อการให้บริการประชาชน และอาจส่งผลต่อการคุ้มครองข้อมูลส่วนบุคคล 3. เพื่อลดปัจจัยเสี่ยงของโอกาสเกิดช่องโหว่ภัยคุกคามทางไซเบอร์ 4. เพื่อให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข (HealthCERT) ได้รับการประสานงานอย่างรวดเร็ว และโต้ตอบต่อภัยคุกคามทางไซเบอร์ได้ทันเวลา 			
ประชากรกลุ่มเป้าหมาย	<ol style="list-style-type: none"> 1. โรงพยาบาลศูนย์ 2. โรงพยาบาลทั่วไป 3. โรงพยาบาลชุมชน เฉพาะที่เปิดให้บริการแล้ว 4. สำนักงานสาธารณสุขจังหวัด 5. สำนักงานเขตสุขภาพที่ 1 - 12 			
วิธีการจัดเก็บข้อมูล	<ol style="list-style-type: none"> 1. หน่วยงานดำเนินการปรับปรุงระบบเครือข่ายคอมพิวเตอร์และสารสนเทศตามเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ และประเมินตนเอง หรือให้ผู้เชี่ยวชาญที่เป็นผู้ตรวจประเมิน (หากเป็นเอกชนต้องมีใบรับรองมาตรฐาน) 2. หน่วยงานส่งผลประเมินตนเองพร้อมหลักฐานให้คณะทำงานควบคุมคุณภาพ การตรวจประเมินความมั่นคงปลอดภัยไซเบอร์ระดับเขตสุขภาพ หรือ คณะทำงานควบคุมคุณภาพการตรวจประเมินความมั่นคงปลอดภัยไซเบอร์ระดับสำนักงานปลัดกระทรวงสาธารณสุข ตามช่องทางที่กำหนด ซึ่งจะแจ้งเวียนเป็นทางการต่อไป 3. คณะทำงานควบคุมคุณภาพการตรวจประเมินความมั่นคงปลอดภัยไซเบอร์ระดับเขตสุขภาพ หรือ คณะทำงานควบคุมคุณภาพการตรวจประเมินความมั่นคงปลอดภัยไซเบอร์ระดับสำนักงานปลัดกระทรวงสาธารณสุข พิจารณาให้ค่าคะแนนรายหน่วยงาน ระดับเขียว/สูง เหลือง/กลาง, แดง/ต่ำ และส่งผลให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารที่อีเมล health-cirt@moph.go.th ทุกวันพฤหัสบดี 4. กรณีหน่วยงานที่ผลประเมินระดับสูง (เขียว) ให้ส่งยืนยันการรักษาระดับรอบ 6 เดือน (มีนาคม) รอบ 9 เดือน (มิถุนายน) และ รอบ 12 เดือน (กันยายน) ไม่เกินวันพฤหัสบดีสุดท้ายของเดือน 			
แหล่งข้อมูล	Cybersecurity Dashboard (https://ict.moph.go.th/th/extension/1524)			
รายการข้อมูล 1	A = หน่วยงานที่ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง (สีเขียว)			
รายการข้อมูล 2	B = หน่วยงานทั้งหมด (หน่วยงานตามที่กำหนดไว้ในคำนิยาม)			
สูตรคำนวณตัวชี้วัด	$(A/B) \times 100$ <p>หมายเหตุ</p> <ol style="list-style-type: none"> 1) ผลคำนวณเป็น 0 ให้ปัดเป็น 1 2) ทศนิยมตั้งแต่ .5 ขึ้นไปให้ปัดขึ้น 			

ระยะเวลาประเมินผล	12 เดือน				
เกณฑ์การประเมิน :					
ปี 2568 :					
รอบ 3 เดือน	รอบ 6 เดือน	รอบ 9 เดือน	รอบ 12 เดือน		
โรงพยาบาลระดับ M1, S และ A ผ่านเกณฑ์ฯ ระดับสูง ร้อยละ 100	หน่วยงานผ่านเกณฑ์ฯ ระดับสูง ไม่น้อยกว่า ร้อยละ 60	- สำนักงานสาธารณสุข จังหวัด และสำนักงานเขต สุขภาพ ผ่านเกณฑ์ฯ ระดับสูง ร้อยละ 100 - โรงพยาบาลศูนย์/ทั่วไป ชุมชน ผ่านเกณฑ์ฯ ระดับสูง ไม่น้อยกว่า ร้อยละ 80	หน่วยงานผ่านเกณฑ์ฯ ระดับสูง ร้อยละ 100		
การคิดคะแนน :					
คะแนน	1	2	3	4	5
ผลดำเนินงาน	ร้อยละ 20	ร้อยละ 40	ร้อยละ 60	ร้อยละ 80	ร้อยละ 100
ตัวอย่าง	$(202 / 902) \times 100 = 22.39$ คิดเป็น 1.12 คะแนน $(875 / 902) \times 100 = 97.01$ คิดเป็น 4.85 คะแนน				
วิธีการประเมินผล :	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ตรวจสอบหลักฐาน และนำผลประเมิน เข้าสู่ Cybersecurity Dashboard ทุกสัปดาห์				
เอกสารสนับสนุน :	เกณฑ์การประเมิน Cybersecurity Assessment Matrix เผยแพร่ที่เว็บไซต์ https://cyber.moph.go.th/				
รายละเอียดข้อมูลพื้นฐาน	Baseline data	หน่วยวัด	ผลการดำเนินงานในรอบปีงบประมาณ พ.ศ.		
			2565	2566	2567
	หน่วยงานที่ผ่าน เกณฑ์มาตรฐาน ความมั่นคงปลอดภัย ไซเบอร์ระดับสูง	แห่ง	-	-	88
ผู้รับผิดชอบการรายงานผลการดำเนินงาน	ที่ปรึกษา : แพทย์หญิงสินสุชา บุญตันตราภิวัฒน์ รองผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โทรศัพท์ : 09 8905 0442 E-mail: sinsucha@moph.go.th ผู้จัดทำรายงาน : นางสาวสุธาทิพย์ คล้ายเหล็ง นักวิชาการคอมพิวเตอร์ชำนาญการ โทรศัพท์ : 0 2590 1213 E-mail: khilaileng@moph.mail.go.th นางสาวณัฐณิชา จันทร์ทอง นักวิชาการคอมพิวเตอร์ปฏิบัติการ โทรศัพท์ : 0 2590 2210 E-mail: health-cirt@moph.go.th นายสุทธิรักษ์ สงกา นักวิชาการคอมพิวเตอร์ โทรศัพท์ : 0 2590 1201 E-mail: health-cirt@moph.go.th ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สร.				