การดำเนินงาน Cyber Security จังหวัดจันทบุรี (ข้อมูล ณ วันที่ 29 ส.ค. 2567)

หน่วยงาน	Cyber Working Teams (A)	Cyber Risk and BIA (B)	ส.ค.-ก.ย.2567							ต.ค.-ธ.ค.2567		
			Next Gen Firewall		1.2 Antivirus		1.1 Back Up (C)	1.3 Access Controls Public/Private (D)	1.4 Privileged Access Management (E)	DR site (เช่าคลาวด์)	SIEM	VA Scan
			ทำแผน+อนุมัติ	จัดซื้อ+ติดตั้ง	ทำแผน+อนุมัติ	จัดซื้อ+ติดตั้ง						
1. รพ.ขลุง			/	อยู่ระหว่างดำเนินการ	/	30 ก.ย. 67				1.พิจารณาจากใบเสนอราคาของบริษัท NT หรือ iNET หรืออื่น ๆ 2.ข้ออื่น ๆ มีแนวทางในเบื้องต้น		
2. รพ.ท่าใหม่		/	/	อยู่ระหว่างดำเนินการ	/	30 ก.ย. 67		13 ก.ย. 67	/			
3. รพ.เขาสุกิม			/	/	/	/	/	/	/			
4. รพ.สองพี่น้อง			/	อยู่ระหว่างดำเนินการ	/	30 ก.ย. 67	/	13 ก.ย. 67				
5. รพ.โป่งน้ำร้อน			/	อยู่ระหว่างดำเนินการ	/	30 ก.ย. 67		/				
6. รพ.มะขาม			/	อยู่ระหว่างดำเนินการ	/	30 ก.ย. 67						
7. รพ.แหลมสิงห์		13 ก.ย. 67	/	อยู่ระหว่างดำเนินการ	/	30 ก.ย. 67		13 ก.ย. 67				
8. รพ.สอยดาว			/	อยู่ระหว่างดำเนินการ	/	30 ก.ย. 67						
9. รพ.แก่งหางแมว			/	อยู่ระหว่างดำเนินการ	/	30 ก.ย. 67						
10. รพ.นายายอาม		13 ก.ย. 67	/	/	/	/	/	/	/			
11. รพ.เขาคิชฌกูฏ	2 ก.ย. 67	2 ก.ย. 67	/	อยู่ระหว่างดำเนินการ	/	30 ก.ย. 67	/	แบ่ง 3 VLAN เรียบร้อย				
รวม	10	8	11	2	11	2	11	8	11			

A = (เอกสาร) คำสั่ง คกก.และนโยบายด้านความปลอดภัย

B = (เอกสาร) ประกาศระเบียบความปลอดภัย, คู่มือ Admin และการบริหารความมั่นคง

C = แนวทาง 3 2 1

D = แบ่ง Vlan ให้กับ network ภายใน รพ.

E = กำหนดสิทธิผู้ใช้งานใน HosXP แยกเป็นกลุ่มต่างๆ

รวบรวมข้อมูล โดย เปรมฤทัย

แบบประเมินด้านด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
โรงพยาบาล..... จังหวัดจันทบุรี

การประเมินครั้งที่ 2

ลำดับ	รายการ	ดำเนินการแล้ว	ยังไม่ได้ดำเนินการ	เอกสารแนบ	หมายเหตุ
	ความเสี่ยงสูง				
1.1	**Backup:** การสำรองข้อมูลแบบ 3-2-1				
1.2	**Antivirus Software:** โปรแกรมป้องกันไวรัส ที่มีการอัพเดท และมีฟังก์ชั่น EDR หรือ XDR				
1.3	**Access Control:** การควบคุมอุปกรณ์หรือการเข้าถึงระบบผ่านทาง ช่องทาง Public/Private ทั้งภายในประเทศและ ต่างประเทศ 1. ดำเนินการกำหนด Whitelist Port และไม่เปิด Port ที่มีความเสี่ยงต่อการโดนโจมตีได้แก่ 7, 19, 20, 21, 22, 23, 25, 37, 53, 69, 79, 80, 110, 111, 135, 137, 138, 139, 445, 161, 443, 512, 513, 514, 1433, 1434, 1723,3 389, 8080 (หากมีความจำเป็นในการเปิดจะต้องทำการกำหนด Source และ Destination ให้ชัดเจน) 2. มีการแบ่งโซน Network ระหว่างอุปกรณ์แม่ข่าย (Server) และ อุปกรณ์ลูกข่าย (Client) 3. มีการใช้งาน VPN ในการเข้าถึงเครื่องอุปกรณ์แม่ข่าย (Server) แทนการเข้าใช้งานผ่าน Public 4. มีการ Block การใชOงาน International Traffic กรณีไม่มีความจำเป็นในใช้งาน 5. มีการใช้งาน Terminal server ในการเข้าถึงระบบ Server แทนที่ Computer ต้นทาง				
14	**Privileged Access Management (PAM):** การดำเนินงานการควบคุมการเข้าถึงระบบและการกำหนดสิทธิ์การเข้าถึง 1. ดำเนินการ Disable Administrator/Root / Admin บนระบบเพื่อป้องกันการโจมตีในรูปแบบ Brute Force 2. กำหนด Policy การเปลี่ยน Password อย่างน้อยทุก 3 เดือน 3. มีการกำหนด role-based access control (RBAC) ในการเข้าถึงระบบ 4. มีการสร้าง Account ตาม User ที่ใช้งานในระบบ 5. มีการตั้ง Password ตามมาตรฐานอย่างน้อย 10 Digi ตัวอักษรใหญ่, เล็ก, อักขระ พิเศษ				
	ความเสี่ยงปานกลาง				
2.1	**Business Continuity Plan (BCP):** มีการกำหนดแนวทางการดำเนินการของหน่วยงานเมื่อเกิดสภาวะวิกฤตหรือภัยต่างๆ พร้อมทั้งมีการทดสอบระบบตามหัวข้อต่อไปนี้ 1. การบริหารจัดการความเสี่ยง (Risk Management) 2. การบริการจัดการด้าน Resource (Resource Management)				

ลำดับ	รายการ	ดำเนินการแล้ว	ยังไม่ได้ดำเนินการ	เอกสารแนบ	หมายเหตุ
	3. การวางแผนความต่อเนื่องจากธุรกิจที่เกิดขึ้น (Business Continuity Planning) 4. การทดสอบ (Testing) 5. การปรับปรุงและแก้ไข (Review & Update)				
2.2	**Disaster Recovery site (DR):** การสำรองข้อมูลในกรณีฉุกเฉินที่ระบบหลักมีปัญหาและไม่สามารถใช้งานได้ โดยจะต้องมี DR-Site โดยยึดจากมาตรฐาน ISO27001 และนำมาปรับใช้งานดังนี้ 1. ระยะห่างระหว่าง DC-Site กับ DR-Site ต้องไม่น้อยกว่า 60 กิโลเมตร 2. ต้องมีระบบฐานข้อมูลที่สำคัญอยู่างน้อย 1 ระบบขึ้นบน DR-site 2. RTO ต้องเท่ากับหรือไม่มากกว่า = 24 ชั่วโมง หรือขึ้นอยู่กับ Solution 3. RPO ต้องเท่ากับหรือไม่มากกว่า = 24 ชั่วโมง 4. ต้องมีเอกสารสรุปผลการทดสอบการดำเนินการ DR-Site 5. ระบบต้องมีมาตรฐาน ISO ดังนี้เป็นอย่างน้อย 5.1 ISO27001 - Information Security Management System 5.2 ISO27799 - Health Informatics-Information Security Management				
2.3	**OS Patching:** มีการอัปเดต Security Patching ในระดับ Operating System ทั้ง Windows / Linux ทุกๆ 6 เดือน				
2.4	**Multi-Factor Authentication (2FA):** มีการใช้งานระบบ Multi-Factor Authentication (2FA) เพื่อยืนยันตัวตน 2 ชั้นในการเข้าถึงระบบต่างๆ สำหรับ Admin ที่ใช้งานระบบดังนี้ 1. การ Login แบบ multi-factor ไปยังระบบ VPN Access 2. การ Login แบบ multi-factor ไปยังอุปกรณ์ Network 3. การ Login แบบ multi-factor ไปยังอุปกรณF Security 4. การ Login แบบ multi-factor ไปยัง Hypervisor 5. การ Login แบบ multi-factor ไปยัง Operating system				
2.5	**Web Application Firewall (WAF):** มีการใช้งาน Web Application Firewall (WAF) กรณีที่มีระบบเป็น Web Application ในรูปแบบ Cloud security เพื่อป้องกันการโจมตีตามมาตรฐาน OWASP Top 10 ได้เป็นอย่างน้อย				
2.6	**Log Management:** มีระบบการจัดเก็บ Log อินเตอร์เน็ต และคอมพิวเตอร์ ตาม พ.ร.บ.ฯ				

ลำดับ	รายการ	ดำเนินการแล้ว	ยังไม่ได้ดำเนินการ	เอกสารแนบ	หมายเหตุ
	อย่างน้อย 90 วัน				
2.7	**Security Information & Event Management (SIEM):** มีระบบ SIEM เพื่อนำมาวิเคราะห์พฤติกรรมของ Cyber Attack บนระบบที่ให้บริการทั้งระดับ Infrastructure และ Operating system (OS) โดยจะต้องคลอบคลุมการตรวจจับพื้นฐานดังนี้ **Common Alert Trigger** 1. ตรวจจับและแจ้งเตือนการบุกรุกที่เข้าถึงระบบเครือข่าย การพยายาม Brute force Login เข้า ระบบ และ การ Scan port (port scanning) 2. Malware-Virus Detection ตรวจจับและแจ้งเตือน Malware หรือ Virus จากพฤติกรรมต่างที่เกิดขึ้นหรือจาก signature 3. Blacklist IP การตรวจจับและแจ้งเตือนการเข้าถึง IP Address ที่เป็น Blacklist และระบุการเปิด connection ได้ 4. Unauthorized Access การตรวจจับการเข้าถึงข้อมูลหรือระบบที่ไม่ได้รับอนุญาต หรือไม่มีสิทธิ์เข้าถึงระบบ 5. DDoS Attack การตรวจจับพฤติกรรมการโจมตีในรูปแบบของ DDoS ได้ทั้งภายนอกและภายใน 6. Data Breaches การตรวจจับและแจ้งเตือนการละเมิดการเข้าถึงข้อมูลที่สำคัญของระบบ ที่ไม่ อนุญาตให้เข้าถึง **Alert & Notification** 1. สามารถแจ้งเตือนภัยคุมคามต่างๆที่เกิดขึ้นได้ผ่านทาง Email, Chat 2. สามารถแจ้งเตือนผ่าน IOC ไปยังหน่วยงานอื่นๆ ได้				
2.8	**Vulnerability Assessment (VA Scan):** มีการดำเนินการ Vulnerability Assessment (VA Scan) อยเางน้อยปีละ 1 ครั้ง ในระดับ Operating system (OS) โดยจะต้องดำเนินการแก้ไข CVE และช่องโหว่ต่างๆที่เกิดขึ้นโดยจะต้องไม่มีความ				
	เสี่ยงระดับ Critical, High ในระบบที่ตรวจสอบโดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน				

ลำดับ	รายการ	ดำเนินการแล้ว	ยังไม่ได้ดำเนินการ	เอกสารแนบ	หมายเหตุ
	ความเสี่ยงต่ำ				
3.1	**Software Update:** มีการตรวจสอบ Version ของ Software ให้เป็น Version Update ล่าสุด เพื่อปิดช่องโหว่ที่เกิดขึ้น				
3.2	**Penetration Testing:** มีการทำ Penetration Testing ของ Web Application ในรูปแบบของ Gray box หรือ Block box อย่างน้อยปีละ 1 ครั้ง และดำเนินการแก้ไขโดยจะต้องไม่มีช่องโหว่ระดับ Severity Critical , High เกิดขึ้น และไม่มีช่องโหวที่เกิดขึ้นตามมาตรฐาน OWASP TOP10				

ผู้รับผิดชอบในการให้ข้อมูล จนท it รพ/หัวหน้ากลุ่มงานสุขภาพดิจิทัล

.....

( )

ผู้รับรองข้อมูล ผอ รพ

.....

( )

ด่วนที่สุด

ที่ สธ ๐๒๑๒/ ว๒๖๖๗๒

สำนักงานปลัดกระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๒๗ สิงหาคม ๒๕๖๗

เรื่อง ขอเชิญประชุมหารือการประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์

เรียน ผู้อำนวยการสำนักงานเขตสุขภาพที่ ๑ - ๑๒/นายแพทย์สาธารณสุขจังหวัดทุกจังหวัด/ผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไปทุกแห่ง

สิ่งที่ส่งมาด้วย แนวทางการประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวน ๑ ชุด

ตามที่สำนักงานปลัดกระทรวงสาธารณสุข โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้จัดทำ Dashboard รายงานผลการประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ (Technology Cybersecurity Assessment Matrix : TAM) และได้นำเสนอผลการประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ (Technology Cybersecurity Assessment Matrix : TAM) ของสำนักงานปลัดกระทรวงสาธารณสุขในการประชุมติดตามผลการดำเนินงานตามนโยบายกระทรวงสาธารณสุข (Tuesday Morning Meeting) ครั้งที่ ๑๙/๒๕๖๗ เมื่อวันที่ ๒๓ กรกฎาคม ๒๕๖๗ โดยปลัดกระทรวงสาธารณสุข ได้มีข้อสั่งการเน้นยกระดับความมั่นคงปลอดภัย Cybersecurity ในทุกเขตสุขภาพให้เป็นระดับสีเขียวมากยิ่งขึ้น นั้น

ในการนี้ สำนักงานปลัดกระทรวงสาธารณสุข ขอเชิญ ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO) ระดับเขตสุขภาพ ระดับจังหวัด และระดับโรงพยาบาล รวมถึงเจ้าหน้าที่ที่เกี่ยวข้อง ร่วมประชุมหารือการประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อรับฟังความคิดเห็นแนวทางการประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์รายละเอียดตามเอกสารสิ่งที่ส่งมาด้วย ในวันที่ ๔ กันยายน ๒๕๖๗ เวลา ๐๙.๓๐ – ๑๐.๓๐ น. ผ่านโปรแกรม Cisco Webex Meeting number : 2511 399 6594 Password: 2331

จึงเรียนมาเพื่อโปรดพิจารณามอบหมายผู้ที่เกี่ยวข้องเข้าร่วมประชุมฯ ตามวัน และเวลาดังกล่าว และแจ้งไปยังหน่วยงานในสังกัดของท่านต่อไปด้วย จะเป็นพระคุณ

ขอแสดงความนับถือ

(นายพงศธร พอกเพิ่มดี)
รองปลัดกระทรวงสาธารณสุข
หัวหน้ากลุ่มภารกิจด้านพัฒนาการสาธารณสุข
ปฏิบัติราชการแทนปลัดกระทรวงสาธารณสุข

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กลุ่มธรรมาภิบาลข้อมูล
โทร. ๐ ๒๕๙๐ ๑๒๑๓
ไปรษณีย์อิเล็กทรอนิกส์ sarabano๒๑๒@moph.go.th

ลิงก์การประชุม https://moph.cc/TAHYyvSBp

ลิงก์ดาวน์โหลดเอกสาร https://moph.cc/xe76qfZqb

แนวทางการประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์

1. การรับรองผลการประเมิน

1) คณะกรรมการ/คณะทำงานบริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (CISO) ระดับเขตสุขภาพ เป็นผู้รับรองผลประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ (เขียว/ต่ำ, เหลือง/กลาง, แดง/สูง) และจัดส่งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารผ่านไปรษณีย์อิเล็กทรอนิกส์ health-cirt@moph.go.th ทุกวันพฤหัสบดีของแต่ละสัปดาห์ (กรณีมีการเปลี่ยนแปลง/แก้ไข/เพิ่มเติมข้อมูลหรือกรณีอื่นๆ) โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะนำขึ้น Dashboard การประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ (https://ict.moph.go.th/th/extension/1524) ทุกวันศุกร์ของแต่ละสัปดาห์

2) ในช่วงเดือนกรกฎาคม – กันยายน 2567 ใช้เกณฑ์การประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ (Technology Cybersecurity Assessment Matrix : TAM) โดยคณะกรรมการ/คณะทำงาน CISO ระดับเขตสุขภาพ สามารถรับรองผลได้จาก

2.1) ผลการประเมินจากบริษัทเอกชนที่หน่วยงานให้เป็นผู้ประเมิน

2.2) ผลการประเมินภายในแต่ละเขตสุขภาพ เช่น คณะกรรมการ/คณะทำงาน CISO ระดับจังหวัดเป็นผู้ประเมินและส่งผลการประเมินไปให้คณะกรรมการ/คณะทำงาน CISO ระดับเขตสุขภาพรับรองผล

3) ตั้งแต่เดือนตุลาคม 2567 เป็นต้นไป จะใช้เกณฑ์การประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับใหม่ที่ทำการตกลงร่วมกันกับเขตสุขภาพทั้ง 12 เขตสุขภาพ โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะขอประสานนัดหมายเพื่อประชุมหารือต่อไป

หมายเหตุ : **1. คณะกรรมการ/คณะทำงาน CISO ตามหนังสือ สธ 0212/ว31377 ลว. 14 พ.ย.66 เรื่องการจัดทำคำสั่งผู้บริหารจัดการความมั่นคงปลอดภัยสารสนเทศระดับสูง และคณะทำงาน (https://ict.moph.go.th/th/extension/1391)**

2. ในครั้งแรกที่ส่งข้อมูลมาให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารขอรบกวนให้ส่งสำเนาคำสั่งแต่งตั้งคณะกรรมการ/คณะทำงาน CISO และคณะกรรมการที่เกี่ยวข้อง มาด้วย

2. เกณฑ์การประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ (Technology Cybersecurity Assessment Matrix : TAM)

ลำดับ	ประเด็นการประเมิน	รายละเอียดการประเมิน
1	Backup **: การสำรองข้อมูลเก็บไว้ที่อื่น เพื่อให้สามารถใช้เพื่อกู้คืนข้อมูลเดิมหลังจากเหตุการณ์ข้อมูลสูญหาย**	มีการสำรองข้อมูลอย่างน้อย 1 วัน และย้อนหลังได้ 7 วันเป็นอย่างน้อยตามมาตรฐาน โดยจัดเก็บบนระบบ Logical HDD หรือ Physical HDD และ จัดเก็บ Backup ในรูปแบบ 3-2-1 1. สำเนาข้อมูลไว้บนระบบ 3 ชุด 2. สำเนาข้อมูลไว้บนเทคโนโลยีต่างกัน 2 ชุด 3. สำเนาข้อมูลไว้แบบ Offline หรือ Offsite หรือ Cloud 1 ชุด โดยครอบคลุม ระบบ HIS เป็นอย่างน้อย
2	Antivirus Software **: โปรแกรมป้องกันไวรัส หรือ แอนติไวรัส คอยตรวจจับป้องกัน และกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์หรือมัลแวร์**	มีการติดตั้ง Anti-virus หรือ EDR หรือ XDR ที่เครื่องฝั่ง Server ทุกเครื่องและอัปเดต Signature ทุกวันและมีเอกสารแนบระบุ Product และ version อย่างละเอียดชัดเจน โดย Anti-virus จะต้อง Active ตลอดเวลา ตรวจสอบติดตั้งเฉพาะกลุ่ม Server เป็นอย่างน้อย โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย

ลำดับ	ประเด็นการประเมิน	รายละเอียดการประเมิน
3	Access Control (Public และ Private) : การควบคุมอุปกรณ์หรือการเข้าถึงระบบผ่านทางช่องทาง Public/Private ทั้งภายในประเทศและต่างประเทศ	มีระบบ Security ในการควบคุม Policy การเข้าถึงระบบที่สำคัญทั้งทาง Public และ Private ดย ครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย 1. ดำเนินการกำหนด White list Port และไม่เปิด Port ที่มีความเสี่ยงต้อการโดนโจมตีปัจจุบันได้แก่ 7, 19, 20, 21, 22, 23, 25, 37, 53, 69, 79, 80, 110, 111, 135, 137, 138, 139, 445, 161, 443, 512, 513, 514, 1433, 1434,1723,3 389, 8080 (หากมีความจำเป็นในการเปิดจะต้องทำการกำหนด Source และ Destination ให้ชัดเจน) 2. มีการแบ่งโซน Network ระหว่างอุปกรณ์แม่ข่าย (Server) และ อุปกรณ์ลูกข่าย (Client) 3. มีการใช้งาน VPN ในการเข้าถึงเครื่องอุปกรณ์แม่ข่าย (Server) แทนการเข้าใช้งานผ่าน Public 4. มีการ Block การใช้งาน International Traffic กรณีไม่มีความจำเป็นในใช้งาน 5. มีการใช้งาน Terminal server ในการเข้าถึงระบบ Server แทนที่ Computer ต้นทาง
4	Privileged Access Management (PAM) : การรักษาความปลอดภัยของข้อมูล ติดตาม ตรวจหา และป้องกันการใช้สิทธิ์การเข้าถึงทรัพยากรที่สำคัญในระดับสูง	มีการควบคุมการเข้าถึงระบบโดยใช้งานสิทธิ์ระดับ High privileged ดังนี้ 1. ดำเนินการ Disable Administrator / Root / Admin บนระบบเพื่อป้องกันการโจมตีในรูปแบบ Brute Force 2. มี Policy การเปลี่ยน Password อย่างน้อยทุก 3 เดือน 3. มีการกำหนด Role-base access ในการเข้าถึงระบบ 4. มีการสร้าง Account ตาม User ที่ใช้งานในระบบ 5. มีการตั้ง Password อย่างน้อย 10 ตัว (ตัวอักษรใหญ่, เล็ก, อักขระพิเศษ, ตัวเลข) โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย
5	Business Continuity Plan (BCP) : แผนที่กำหนดแนวทางการดำเนินการของหน่วยงานเมื่อเกิดสภาวะวิกฤตหรือภัยต่าง ๆ ที่ส่งผลให้กระบวนการทำงานของหน่วยงานหยุดชะงัก เพื่อให้สามารถกลับมาดำเนินการได้อย่างต่อเนื่อง	มีการทดสอบ Business Continuity Plan (BCP) อย่างน้อย ปีละ 1 ครั้ง และ มีการจัดทำรายงานถึงขั้นตอนการดำเนินการที่ชัดเจนรวมถึงระยะเวลาดำเนินการและผู้ที่เกี่ยวข้องในการดำเนินการงานดังนี้ 1. การบริหารจัดการความเสี่ยง (Risk Management) 2. การบริการจัดการด้าน Resource (Resource Management) 3. การวางแผนความต่อเนื่องจากธุรกิจที่เกิดขึ้น (Business Continuity Planning) 4. การทดสอบ (Testing) 5. การปรับปรุงและแก้ไข (Review & Update)
6	OS Patching: การซ่อมแซมจุดบกพร่องของระบบปฏิบัติการ (OS) หรือปรับปรุงระบบปฏิบัติการให้ทันสมัย และเพิ่มเติมความสามารถในการใช้งานหรือประสิทธิภาพให้ดีขึ้น	มีการอัปเดต Security Patching ในระดับ Operating System ทั้ง Windows / Linux ทุกๆ 6 เดือน หรือทันทีหากมี Critical security patching โดยการตรวจสอบจะต้องไม่มี Security Patch ระดับ Critical, High เกิดขึ้น โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย
7	Multi-Factor Authentication (2FA) : การยืนยันตัวตน 2 ชั้น เป็นการเข่าสู่ระบบบัญชีแบบหลายขั้นตอนที่กำหนดให้ผู้ใช้ป้อนข้อมูลเพิ่มเติมนอกเหนือจากรหัสผ่าน	มีการใช้งานระบบ Multi-Factor Authentication (2FA) เพื่อยืนยันตัวตน 2 ชั้นในการเข้าถึงระบบต่างๆ สำหรับ Admin ที่ใช้งานระบบดังนี้ 1. การ Login แบบ Multi-factor ไปยังระบบ VPN Access 2. การ Login แบบ Multi-factor ไปยังอุปกรณ์ Network 3. การ Login แบบ Multi-factor ไปยังอุปกรณ์ Security 4. การ Login แบบ Multi-factor ไปยัง Hypervisor 5. การ Login แบบ Multi-factor ไปยัง Operating system โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย
8	Web Application Firewall (WAF) : ระบบป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอพพลิเคชั่นโดยเฉพาะเพื่อป้องกันการโจมตีไปยังระบบเว็บแอปพลิเคชันของหน่วยงาน	มีการใช้งาน Web Application Firewall (WAF) กรณีที่มีระบบเป็น Web Application เพื่อป้องกันการโจมตีตามมาตรฐาน OWASP Top 10 ได้เป็นอย่างน้อยตามรายละเอียด ดังนี้ 1. Broken Access Control 2. Cryptographic Failures 3. Injection 4. Insecure Design 5. Security Misconfiguration

ลำดับ	ประเด็นการประเมิน	รายละเอียดการประเมิน
		6. Vulnerable and Outdated Components 7. Identification and Authentication Failures 8. Software and Data Integrity Failures 9. Security Logging and Monitoring Failures 10. Server-Side Request Forgery (SSRF) Reference : https://owasp.org/www-project-top-ten/
9	Log Management : การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์	มีระบบการจัดเก็บ Log อินเทอร์เน็ต และคอมพิวเตอร์ ตาม พ.ร.บ. คอมฯ อย่างน้อย 90 วัน
10	Security Information & Event Management (SIEM) : ระบบที่ใช้ในการจัดการกับ Log และ Event ต่าง ๆ ที่คอยทำหน้าที่วิเคราะห์หาความเชื่อมโยงของ Event ต่าง ๆ ที่เกี่ยวข้องกับความปลอดภัยทั้งหมด ไปจนถึงการ Alert ระบุตำแหน่งของภัยคุกคามให้ทราบ เมื่อมี Event ที่ผิดปกติ ทำให้สามารถป้องกัน และตอบสนองภัยคุกคามได้อย่างรวดเร็ว	มีระบบ SIEM เพื่อนำมาวิเคราะห์พฤติกรรมของ Cyber Attack บนระบบที่ให้บริการทั้งระดับ Infrastructure และ Operating system (OS) โดยจะต้องคลอบคลุมการตรวจจับพื้นฐาน ดังนี้ <u>Common Alert Trigger</u> 1. ตรวจจับและแจ้งเตือนการบุกรุกที่เข้าถึงระบบเครือข่าย การพยายาม Brute force Login เข้าระบบ และ การ Scan port (port scanning) 2. Malware-Virus Detection ตรวจจับและแจ้งเตือน Malware หรือ Virus จากพฤติกรรมต่างๆ ที่เกิดขึ้นหรือจาก signature 3. Blacklist IP การตรวจจับและแจ้งเตือนการเข้าถึง IP Address ที่เป็น Blacklist และระบุการเปิด connection ได้ 4. Unauthorized Access การตรวจจับการเข้าถึงข้อมูลหรือระบบที่ไม่ได้รับอนุญาต หรือไม่มีสิทธิ์เข้าถึงระบบ 5. DDoS Attack การตรวจจับพฤติกรรมการโจมตีในรูปแบบของ DDoS ได้ ทั้งภายนอกและภายใน 6. Data Breaches การตรวจจับและแจ้งเตือนการละเมิดการเข้าถึงข้อมูลที่สำคัญของระบบ ที่ไม่อนุญาตให้เข้าถึง <u>Alert & Notification</u> 1. สามารถแจ้งเตือนภัยคุมคามต่างๆที่เกิดขึ้นได่ผ่านทาง Email , Chat 2. สามารถแจ้งเตือนผ่าน IOC ไปยังหน่วยงานอื่นๆ ได้ <u>Dashboard & Report</u> 1. มี Dashboard เพื่อควบคุมและตรวจสอบพฤติกรรมผิดปกติที่เกิดขึ้นกับระบบโดยสามารถแบ่งตาม severity ได้ชัดเจนรวมถึงมี Timestamp 2. มีการสรุป Report ประจำเดือนเพื่อรายงานเหตุการณ์ต่างๆ ที่เกิดขึ้นในระบบ โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย
11	Vulnerability Assessment (VA Scan) : การตรวจสอบช่องโหว่ของระบบ เพื่อให้ทราบถึงความเสี่ยง จุดอ่อน และระดับความรุนแรง ของผลกระทบที่อาจเกิดขึ้นจากการถูกโจรกรรมข้อมูลและการโจมตีทางไซเบอร์	มีการดำเนินการ Vulnerability Assessment (VA Scan) อย่างน้อยปีละ 1 ครั้ง ในระดับ Operating system (OS) โดยจะต้องดำเนินการแก้ไข CVE และช่องโหว่ต่างๆ ที่เกิดขึ้นโดยจะต้องไม่มีความเสี่ยงระดับ Critical, High ในระบบที่ตรวจสอบ โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย
12	Software Update : การตรวจสอบ Version ของ Software ให้เป็น Version Update ล่าสุด เพื่อปิดช่องโหว่ที่เกิดขึ้นใน Software Version ก่อนหน้า	มีการอัปเดต Software Patching ของระบบ HIS และมีการทำ Penetration Testing อย่างน้อยปีละ 1 ครั้ง หรือมีการออก Major version โดยจะต้องดำเนินการแก้ไขช่องโหว่ในระดับ Severity Critical และ High เป็นอย่างน้อย โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย
13	Penetration Testing : การทดสอบการเจาะระบบ	มีการทำ Penetration Testing ของ Web Application ในรูปแบบของ Gray box หรือ Black box อย่างน้อยปีละ 1 ครั้ง และดำเนินการแก้ไขโดยจะต้องไม่มีช่องโหว่ระดับ Severity Critical , High เกิดขึ้น และไม่มีช่องโหว่ที่เกิดขึ้นตามมาตรฐาน OWASP TOP10

ลำดับ	ประเด็นการประเมิน	รายละเอียดการประเมิน
14	Disaster Recovery site (DR) : ศูนย์สำรองข้อมูล สำหรับแก้ไขปัญหาระบบสารสนเทศที่เกิดขึ้นจากภัยพิบัติต่างๆ ให้สามารถทำงานได้อย่างต่อเนื่อง	มีระบบ Disaster Recovery site (DR) ในกรณีฉุกเฉินที่ระบบหลักมีปัญหาและไม่สามารถใช้งานได้ โดยจะต้องมี DR-Site โดยยึดจากมาตรฐาน ISO27001 และนำมาปรับใช้งานดังนี้ 1. ระยะห่างระหว่าง DC-Site กับ DR-Site ต้องไม่น้อยกว่า 60 กิโลเมตร 2. ต้องมีระบบฐานข้อมูลที่สำคัญอย่างน้อย 1 ระบบขึ้นบน DR-site 2. RTO ต้องเท่ากับหรือไม่มากกว่า = 24 ชั่วโมง หรือขึ้นอยู่กับ Solution 3. RPO ต้องเท่ากับหรือไม่มากกว่า = 24 ชั่วโมง 4. ต้องมีเอกสารสรุปผลการทดสอบการดำเนินการ DR-Site 5. ระบบต้องมีมาตรฐาน ISO ดังนี้เป็นอย่างน้อย 5.1 ISO27001 - Information Security Management System 5.2 ISO27799 - Health Informatics-Information Security Management โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย

3. เกณฑ์การให้ระดับความเสี่ยงสูง/ปานกลาง/ต่ำ

โดยนำเกณฑ์การประเมิน TAM มาจัดระดับได้ดังนี้

1) **ระดับความเสี่ยงสูง (สีแดง)** ไม่ได้ดำเนินการข้อ 1 – 4 ให้ครบถ้วนทุกข้อ
2) ระดับความเสี่ยงปานกลาง (สีเหลือง) ดำเนินการข้อ 1 - 4 ครบถ้วนทุกข้อ
3) ระดับความเสี่ยงต่ำ (สีเขียว) ดำเนินการข้อ 1 – 11 ครบถ้วนทุกข้อ
4) ข้อ 12 – 14 ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารขอรวบรวมข้อมูลแต่ไม่มีผลต่อการประเมิน

4. ติดต่อสอบถามข้อมูลเพิ่มเติม

1. คุณสุธาทิพย์ คล้ายเหล็ง โทร. 0 2590 1213
2. คุณณัฐณิชา จันทร์ทอง โทร. 0 2590 1213
3. คุณสุทธิรักษ์ สงกา โทร. 0 2590 1201