ด่วนที่สุด **บันทึกข้อความ**

ส่วนราชการ สำนักงานสาธารณสุขจังหวัดจันทบุรี โทร. ๐ ๓๙๓๑ ๑๑๖๖ ต่อ ๓๐๒, ๓๐๓

ที่ จบ ๐๐๓๓.๐๐๒ / ๗๕๑๒ **วันที่** ๑๙ ธันวาคม ๒๕๖๗

เรื่อง เร่งรัดการดำเนินการรักษาความมั่งคงปลอดภัยไซเบอร์

เรียน ผู้อำนวยการโรงพยาบาลชุมชน ทุกแห่ง

ด้วยกระทรวงสาธารณสุข เร่งรัดให้หน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อรองรับนโยบาย ๓๐ บาทรักษาทุกที่ เพื่อคนไทยสุขภาพดีถ้วนหน้า ครอบคลุมทั่วประเทศ ในวันที่ ๒๕ ธันวาคม พ.ศ. ๒๕๖๘ พร้อมกับประกาศเรื่องการเชื่อมโยงข้อมูลสุขภาพคนไทย การใช้เทคโนโลยีสารสนเทศมาสนับสนุนระบบสุขภาพดิจิทัลของคนไทย

สำนักงานสาธารณสุขจังหวัดจันทบุรี จึงขอเร่งรัดดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามเกณฑ์การประเมินระดับการรักษาความมั่งคงปลอดภัยไซเบอร์ (CTAM : Cybersecurity Technical Assessment Matrix) พร้อมทั้งให้รายงานผลการประเมิน ตามเกณฑ์ดังกล่าว ภายในวันที่ ๒๓ ธันวาคม ๒๕๖๗ ทั้งนี้สามารถดาวน์โหลดรายละเอียดได้ที่ https://cto.moph.go.th/ หัวข้อข่าวแจ้ง สสอ./ผอ.รพช.

จึงเรียนมาเพื่อทราบและดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นายอภิรักษ์ พิศุทธิ์อาภรณ์)
นายแพทย์สาธารณสุขจังหวัดจันทบุรี

แนวทางการประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์

เกณฑ์การประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ (CTAM: Cybersecurity Technical Assessment Matrix) ปี 2568

ลำดับ	ประเด็นการประเมิน	รายละเอียดการประเมิน	เอกสารประกอบการประเมิน	ดำเนินการแล้ว	ยังไม่ได้ดำเนินการ
1	**Backup** **: การสำรองข้อมูลเก็บไว้ที่อื่น เพื่อให้สามารถใช้เพื่อกู้คืนข้อมูลเดิมหลังจากเหตุการณ์ข้อมูลสูญหาย**	มีการสำรองข้อมูลอย่างน้อยวันละ 1 ครั้ง และสามารถย้อนหลังได้ 7 วัน เป็นอย่างน้อยตามมาตรฐาน 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	1. คู่มือการปฏิบัติงาน (options) 2. รายงานผลการดำเนินการการสำรองข้อมูล 3. รายการระบบที่สำรองข้อมูล (ภาพหลักฐาน หรือเอกสารประกอบอื่นๆ)		
2	**Antivirus Software** **: โปรแกรมป้องกันไวรัส หรือแอนติไวรัส คอยตรวจจับป้องกัน และกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์หรือมัลแวร์**	มีการติดตั้ง Anti-Virus หรือ EDR หรือ XDR บนเครื่องคอมพิวเตอร์ของระบบที่สำคัญ 1. Review Alert Report 2. Update Program Anti-Virus, EDR/XER 3. Schedule Update Database Signature	1. คู่มือการติดตั้ง (options) 2. ผลการดำเนินการติดตั้ง 3. รายการเครื่องคอมพิวเตอร์ของระบบที่สำคัญที่ทำการติดตั้ง (ภาพหลักฐานของเครื่องที่ติดตั้ง หรือเอกสารประกอบอื่นๆ)		
3	**Access Control (Public และ Private)** : การควบคุมอุปกรณ์หรือการเข้าถึงระบบผ่านทางช่องทาง Public/Private ทั้งภายในประเทศและต่างประเทศ	มีการควบคุม Policy การเข้าถึงระบบที่สำคัญทั้งทาง Public และ Private 1. Open Port Access จากภายนอกเท่าที่จำเป็น เช่น HTTPS (443) 2. IP Address Filter กำหนดขอบเขตการใช้งาน IP Address ที่สามารถเข้าใช้งานในระบบได้ เช่น IP Location, Geometric 3. Enable IDS/IPS 4. ใช้ระบบ VPN (Virtual Private Network) สำหรับการเข้าถึง Server/Application ภายใน ผ่านโปรดตคอล IPsec/SSL 5. มีการแบ่งโซน Network ภายในรวมถึงมี Firewall กั้นระหว่างโซนภายในที่สำคัญ 6. User Access Accounts กำหนดสิทธิการใช้งานเท่าที่จำเป็น เช่น Role Base / Group Base 7. User Password Policy กำหนดการใช้งานพาสเวิร์ด เช่น กำหนดความยาวอย่างน้อย 12 ตัวอักษร, Hash MD5, SHA-256 8. Time Sync 9. Change Default Accounts 10. Review Privilege Accounts 11. Review Logs Access 12. Feeds IOC (Option)	1. คู่มือการตั้งค่าอุปกรณ์ Firewall (options) 2. รายงานหรือเอกสารผลการดำเนินการตั้งค่าอุปกรณ์ Firewall โดยมีรายละเอียด ตามเงื่อนไขการควบคุม 12 ข้อ 3. ตารางกำหนดสิทธิแต่ละอุปกรณ์ (options) หมายเหตุ : เอกสารประกอบสามารถใช้ภาพหลักฐาน หรือเอกสารที่เกี่ยวข้องที่บ่งชี้ในแต่รายการ การประเมินได้		

ลำดับ	ประเด็นการประเมิน	รายละเอียดการประเมิน	เอกสารประกอบการประเมิน	ดำเนินการแล้ว	ยังไม่ได้ดำเนินการ
4	**Privileged Access Management (PAM)** **: การรักษาความปลอดภัยของข้อมูล** **ติดตาม ตรวจหา และป้องกันการใช้สิทธิ์การเข้าถึงทรัพยากรที่สำคัญในระดับสูง**	มีการควบคุมการเข้าถึงระบบโดยใช้งานสิทธิ์ระดับ Least Privilege ดังนี้ 1. ดำเนินการ Disable Administrator / Root / Admin 2. มีการกำหนด Role-base access ในการเข้าถึงระบบเท่าที่มีจำเป็น 3. มี Access Rights Matrix ของระบบ 4. มีการตั้ง Password อย่างน้อย 12 ตัว (ตัวอักษรใหญ่, เล็ก, อักขระพิเศษ, ตัวเลข) 12 , มีการเข้ารหัส Password MD5,SHA-256 5. Expire Sessions Time out 6. Review Privilege Accounts 7. Review กิจกรรมผู้ใช้งานในระบบ	1. คู่มือการตั้งค่าระบบที่สำคัญ (options) 2. ผลการดำเนินการตั้งค่าการกำหนดสิทธิ 3. ตารางกำหนดสิทธิระบบที่สำคัญเทียบกับระบบจริง(options) หมายเหตุ : เอกสารประกอบสามารถใช้ภาพหลักฐาน หรือเอกสารที่เกี่ยวข้องที่บ่งชี้ในแต่รายการ การประเมินได้		
5	**Business Continuity Plan (BCP)** **Disaster Recovery Plan (DRP)** **: แผนที่กำหนดแนวทางการดำเนินการของหน่วยงานเมื่อเกิดสภาวะวิกฤตหรือภัยต่าง ๆ ที่ส่งผลให้กระบวนการทำงานของหน่วยงานหยุดชะงัก เพื่อให้สามารถกลับมาดำเนินการได้อย่างต่อเนื่อง**	มีการทดสอบ Business Continuity Plan (BCP) และ Disaster Recovery Plan (DRP) อย่างน้อย ปีละ 1 ครั้ง และ มีการจัดทำรายงานถึง ขั้นตอนการดำเนินการที่ชัดเจนรวมถึงระยะเวลาดำเนินการและผู้ที่เกี่ยวข้องในการดำเนินการงานดังนี้ 1. การบริหารจัดการความเสี่ยง (Risk Management) 2. การบริการจัดการด้าน Resource (Resource Management) 3. การวางแผนความต่อเนื่องจากธุรกิจที่เกิดขึ้น (Business Continuity Planning) 4. การทดสอบ (Testing) 5. การปรับปรุงและแก้ไข (Review & Update)	1. เอกสารแผน Business Continuity Plan (BCP) 2. เอกสารแผน Disaster Recovery Plan (DRP) 3. รายงานผลการทดสอบตามที่กำหนด หมายเหตุ : เอกสารประกอบสามารถใช้ภาพหลักฐาน หรือเอกสารที่เกี่ยวข้องที่บ่งชี้ในแต่รายการ การประเมินได้		
6	**OS Patching: การซ่อมแซมจุดบกพร่องของระบบปฏิบัติการ (OS)หรือปรับปรุงระบบปฏิบัติการให้ทันสมัย และเพิ่มเติมความสามารถในการใช้งานหรือประสิทธิภาพให้ดีขึ้น**	มีการอัปเดต Security Patching 1. Firewall patching (Firmware) 2. Operation patching 3. Application patching 4. Software patching 5. Change Management	1. คู่มือการอัปเดตรวมทั้ง Hardware และ Software (options) 2. ผลการดำเนินงาน หมายเหตุ : เอกสารประกอบสามารถใช้ภาพหลักฐาน หรือเอกสารที่เกี่ยวข้องที่บ่งชี้ในแต่รายการ การประเมินได้		
7	**Multi-Factor Authentication (2FA)** **: การยืนยันตัวตน 2 ชั้น เป็นการเข่าสู่ระบบบัญชีแบบหลายขั้นตอนที่กำหนดให้ผู้ใช้ป้อนข้อมูลเพิ่มเติมนอกเหนือจากรหัสผ่าน**	มีการใช้งานระบบ Multi-Factor Authentication (2FA) เพื่อยืนยันตัวตน 2 ชั้นในการเข้าถึงระบบต่างๆ สำหรับ Admin ที่ใช้งานระบบอย่างน้อยดังนี้ 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	1. คู่มือการติดตั้งและตั้งค่าการใช้งาน (options) 2. รายละเอียดของระบบที่ใช้ และผลการดำเนินงาน (แสดงรูปภาพหน้าจอ ของระบบ) หมายเหตุ : เอกสารประกอบสามารถใช้ภาพหลักฐาน หรือเอกสารที่เกี่ยวข้องที่บ่งชี้ในแต่รายการ การประเมินได้		

ลำดับ	ประเด็นการประเมิน	รายละเอียดการประเมิน	เอกสารประกอบการประเมิน	ดำเนินการแล้ว	ยังไม่ได้ดำเนินการ
8	**Web Application Firewall (WAF)** **: ระบบป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอพพลิเคชั่นโดยเฉพาะ เพื่อป้องกันการโจมตีไปยังระบบเว็บแอปพลิเคชันของหน่วยงาน**	มีการใช้งาน Web Application Firewall (WAF) กรณีที่มีระบบเป็น Web Application เพื่อป้องกันการโจมตีตามมาตรฐาน OWASP Top 10 ได้เป็นอย่างน้อยตามรายละเอียด 1. Review Attack Report 2. Add Source IP Blocklists	1. คู่มือการใช้งานและตั้งค่าการใช้งานของ WAF (options) 2. ผลการดำเนินการติดตั้ง หมายเหตุ : เอกสารประกอบสามารถใช้ภาพหลักฐาน หรือเอกสารที่เกี่ยวข้องที่บ่งชี้ในแต่รายการ การประเมินได้		
9	**Log Management** **: การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์**	มีระบบการจัดเก็บ Log อินเทอร์เน็ตและคอมพิวเตอร์ ตาม พ.ร.บ. คอมฯ อย่างน้อย 90 วัน 1. System Logs 2. Access Logs 3. Authentication Logs 4. Authorization Logs 5. Error Logs 6. Applications Logs	1. คู่มือการติดตั้งและตั้งค่าการใช้งานระบบ Log Management (options) 2. รายงานผล Log ย้อนหลัง วันที่ 90 ของ Log ที่เก็บ หมายเหตุ : เอกสารประกอบสามารถใช้ภาพหลักฐาน หรือเอกสารที่เกี่ยวข้องที่บ่งชี้ในแต่รายการ การประเมินได้		
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 หรือระบบวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อนำมาวิเคราะห์พฤติกรรมของ Cyber Attack บนระบบที่ให้บริการทั้งระดับ Infrastructure และ Operating system (OS) โดยจะต้องคลอบคลุมการตรวจจับพื้นฐาน ดังนี้ 1. ตรวจจับและแจ้งเตือนการบุกรุกที่เข้าถึงระบบเครือข่าย การพยายาม Brute force Login เข้า ระบบ และการ Scan port (port scanning) 2. Malware-Virus Detection ตรวจจับและแจ้งเตือน Malware หรือ Virus จากพฤติกรรมต่างๆ ที่เกิดขึ้น หรือจาก 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	1. รายละเอียดของระบบ SIEM และระบบหรืออุปกรณ์ที่ทำการส่ง LOG 2. คู่มือตั้งค่าการใช้งานระบบ SIEM 3. รายงานผลที่เกิดขึ้นจากระบบ SIEM ตรวจจับได้ หมายเหตุ : เอกสารประกอบสามารถใช้ภาพหลักฐาน หรือเอกสารที่เกี่ยวข้องที่บ่งชี้ในแต่รายการ การประเมินได้		
11	**Vulnerability Assessment (VA Scan)** **: การตรวจสอบช่องโหว่ของระบบ เพื่อให้ทราบถึงความเสี่ยง จุดอ่อน และระดับความรุนแรง ของผลกระทบที่อาจเกิดขึ้นจากการถูกโจรกรรมข้อมูลและการโจมตีทางไซเบอร์**	มีการดำเนินการ Vulnerability Assessment (VA Scan) อย่างน้อยปีละ 1 ครั้ง โดยจะต้องดำเนินการแก้ไข CVE และช่องโหว่ต่างๆ ที่เกิดขึ้นโดยให้ความสำคัญกับความเสี่ยงระดับ Critical, High เป็นลำดับแรก 1. Review Vulnerability Assessment Report	1. รายงานการผลการดำเนินการตรวจสอบช่องโหว่ของระบบที่สำคัญ โดยรายละเอียดอย่างน้อยต้องประกอบด้วยผลสรุปสำหรับผู้บริหาร รายละเอียดของช่องโหว่ที่ตรวจพบพร้อมแนวทางการแก้ไข		

ลำดับ	ประเด็นการประเมิน	รายละเอียดการประเมิน	เอกสารประกอบการประเมิน	ดำเนินการแล้ว	ยังไม่ได้ดำเนินการ
		2. จัดลำดับความสำคัญ ความเสี่ยง ระดับ Critical, High, Medium, Low กำหนดระยะเวลาในการแก้ไขช่องโหว่ 3. การจัดการความเสี่ยง 3.1 ยอมรับความเสี่ยง (Risk Acceptance) 3.2 หลีกเลี่ยงความเสี่ยง (Risk Avoidance) 3.3 ลดความเสี่ยง (Risk Mitigation) 3.4 ถ่ายโอนความเสี่ยง (Risk Transfer)	หมายเหตุ : เอกสารประกอบสามารถใช้ภาพหลักฐาน หรือเอกสารที่เกี่ยวข้องที่บ่งชี้ในแต่รายการ การประเมินได้		
12	**Software Update : การตรวจสอบ Version ของ Software ให้เป็น Version Update ล่าสุด เพื่อปิดช่องโหว่ที่เกิดขึ้นใน Software Version ก่อนหน้า**	มีการอัปเดต Software Patching ของระบบที่สำคัญ เช่น HIS และมีการทำ Penetration Testing อย่างน้อยปีละ 1 ครั้ง หรือมีการออก Major version โดยจะต้องดำเนินการแก้ไขช่องโหว่ในระดับ Severity Critical และ High เป็นอย่างน้อย	1. รายงานการอัปเดท Patching ของระบบ หมายเหตุ : เอกสารประกอบสามารถใช้ภาพหลักฐาน หรือเอกสารที่เกี่ยวข้องที่บ่งชี้ในแต่รายการ การประเมินได้		
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	1. รายงานการทำ Penetration Testing โดยรายละเอียดอย่างน้อยต้องประกอบด้วยผลสรุปสำหรับผู้บริหาร รายละเอียดของช่องโหว่ที่ตรวจพบพร้อมแนวทางการแก้ไข หมายเหตุ : เอกสารประกอบสามารถใช้ภาพหลักฐาน หรือเอกสารที่เกี่ยวข้องที่บ่งชี้ในแต่รายการ การประเมินได้		
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 3. RTO ต้องเท่ากับหรือไม่มากกว่า = 24 ชั่วโมง หรือขึ้นอยู่กับ Solution 4. RPO ต้องเท่ากับหรือไม่มากกว่า = 24 ชั่วโมง 5. ต้องมีเอกสารสรุปผลการทดสอบการดำเนินการ DR-Site 6. ระบบต้องมีมาตรฐาน ISO ดังนี้เป็นอย่างน้อย 6.1 ISO27001 - Information Security Management System 6.2 ISO27799 - Health Informatics-Information Security Management			

2. <u>เกณฑ์การให้ระดับระดับการรักษาความมั่นคงปลอดภัยไซเบอร์สูง/ปานกลาง/ต่ำ</u>

โดยนำเกณฑ์การประเมิน CTAM มาจัดระดับได้ดังนี้

1) **ระดับความมั่นคงปลอดภัยไซเบอร์ต่ำ (สีแดง)** ไม่ได้ดำเนินการข้อ 1 – 4 ให้ครบถ้วนทุกข้อ
2) **ระดับความมั่นคงปลอดภัยไซเบอร์ปานกลาง (สีเหลือง)** ดำเนินการข้อ 1 - 4 ครบถ้วนทุกข้อ
3) **ระดับความมั่นคงปลอดภัยไซเบอร์สูง (สีเขียว)** ดำเนินการข้อ 1 – 11 ครบถ้วนทุกข้อ
4) ข้อ 12 – 14 ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารขอรวบรวมข้อมูลแต่ไม่มีผลต่อการประเมิน

3. <u>ติดต่อสอบถามข้อมูลเพิ่มเติม</u>

1. คุณบัญชา พร้อมดิษฐ์ นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ โทร. 089 009 3564
2. คุณศาสนา ผาสุข นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ โทร. 095 993 6298
3. คุณเปรมฤทัย เจริญพงษ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ โทร. 080 278 7322