เอกสารประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ (CTAM : Cybersecurity Technical Assessment Matrix)

โรงพยาบาลสองแคว

อำเภอสองแคว จังหวัดน่าน

จัดทำโดย

กลุ่มงานสุขภาพดิจิทัล

4 มกราคม 2569

สารบัญ

หน้า

บทนำ

ตามที่กระทรวงสาธารณสุข มีนโยบายยกระดับ “30 บาท รักษาทุกที่ ด้วยบัตรประชาชนใบเดียว” เพื่อให้ประชาชนเข้าถึงข้อมูลสุขภาพตนเอง บน Application หมอพร้อม เพิ่มความสะดวก รวดเร็ว และลดความแออัดในโรงพยาบาล ตลอดจนการยกระดับความมั่นคงปลอดภัยทางไซเบอร์ในโรงพยาบาลให้มีความสามารถป้องกัน รับมือกับสถานการณ์ด้านภัยคุกคามจากผู้ไม่หวังดี โรงพยาบาลท่าวังผาได้เห็นความสำคัญของการกำกับ ดูแล การรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cyber Security) ในโรงพยาบาล โดยประสานบริษัท โทรคมนาคมแห่งชาติ จำกัด เข้าประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ทางกลุ่มงานสุขภาพดิจิทัลจึงได้จัดทำเอกสารประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ (CTAM : Cybersecurity Technical Assessment Matrix) ปี 2568 ไว้สำหรับการประเมินของหน่วยงาน

เกณฑ์ประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์
(CTAM : Cybersecurity Technical Assessment Matrix)

<u>หัวข้อประเมินที่ 1 : ความเสี่ยงสูง</u>

1. Backup : การสำรองข้อมูลเก็บไว้ที่อื่น เพื่อให้สามารถใช้เพื่อกู้คืนข้อมูลเดิมหลังจากเหตุการณ์ข้อมูลสูญหาย

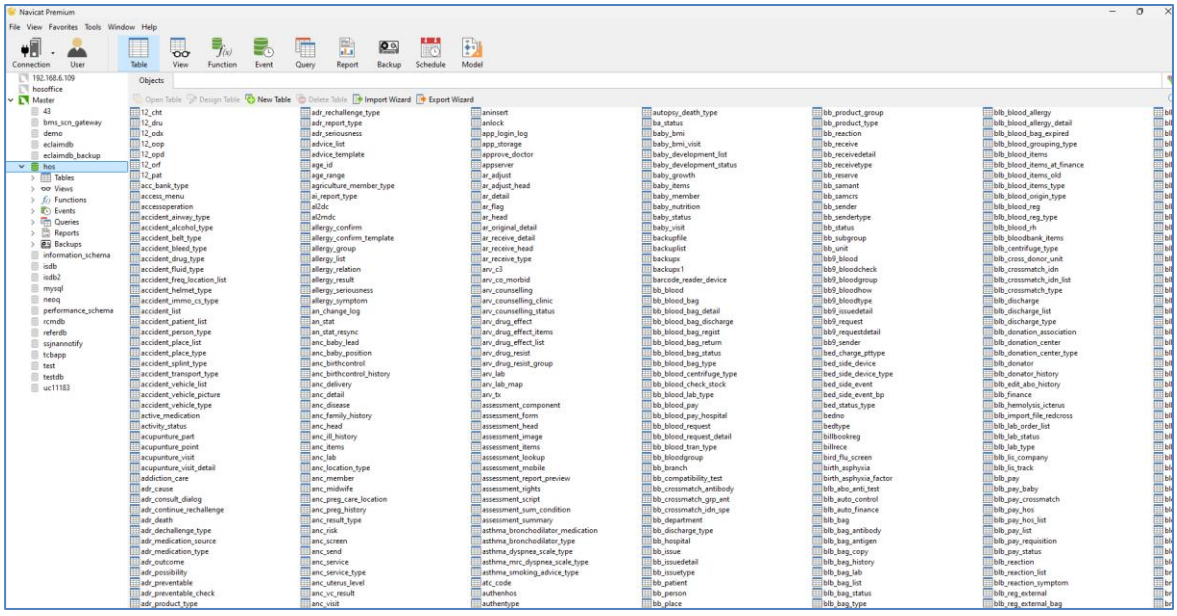
รายละเอียดหัวข้อการประเมิน

มีการสำรองข้อมูลอย่างน้อย 1 วัน และย้อนหลังได้ 7 วัน เป็นอย่างน้อยตามมาตรฐานโดยจัดเก็บบนระบบ Logical HDD หรือ Physical HDD

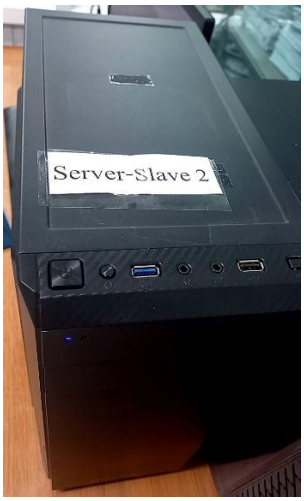
1.1. การสำรองข้อมูล (Backup) ไว้บนระบบ 3 ชุด

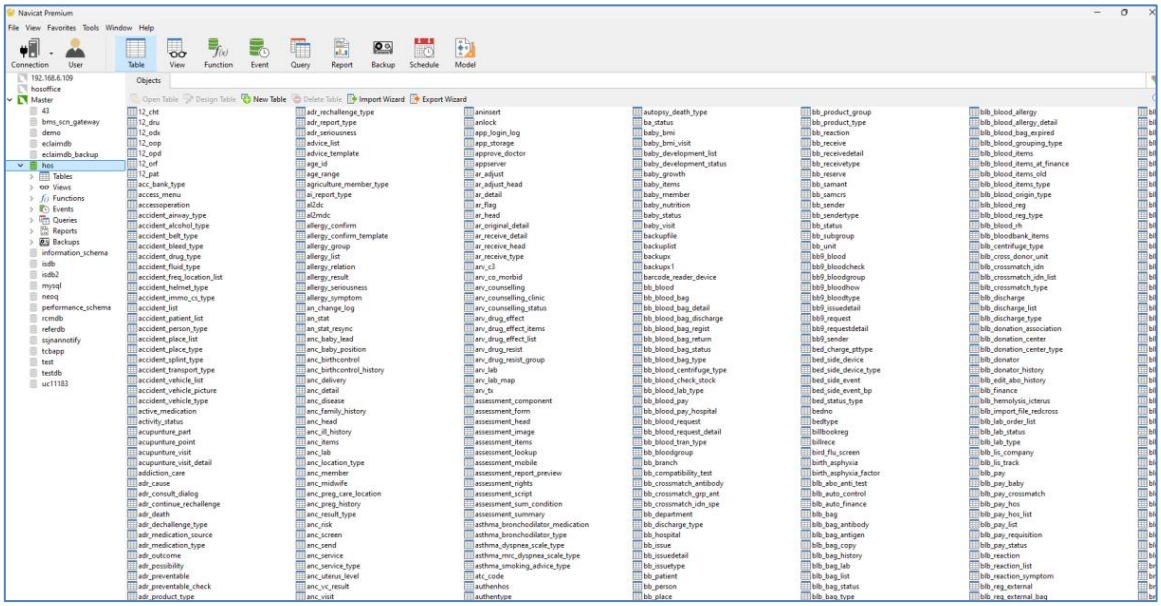
มีการสำรองข้อมูล (Backup) บนระบบ 3 ชุด เป็นอย่างน้อย โดยสำรองไว้ที่

1. HOSxP Master Server

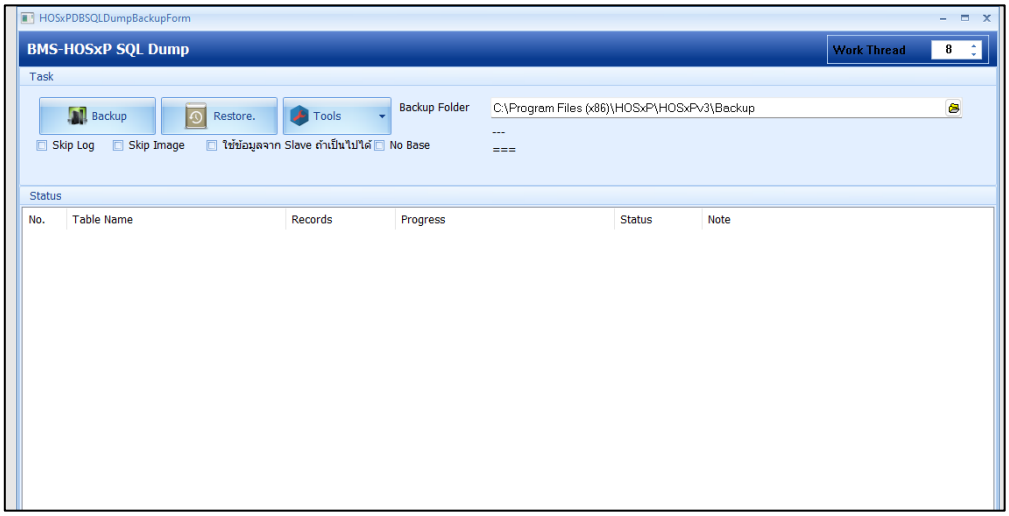


2. HOSxP Slave Sever





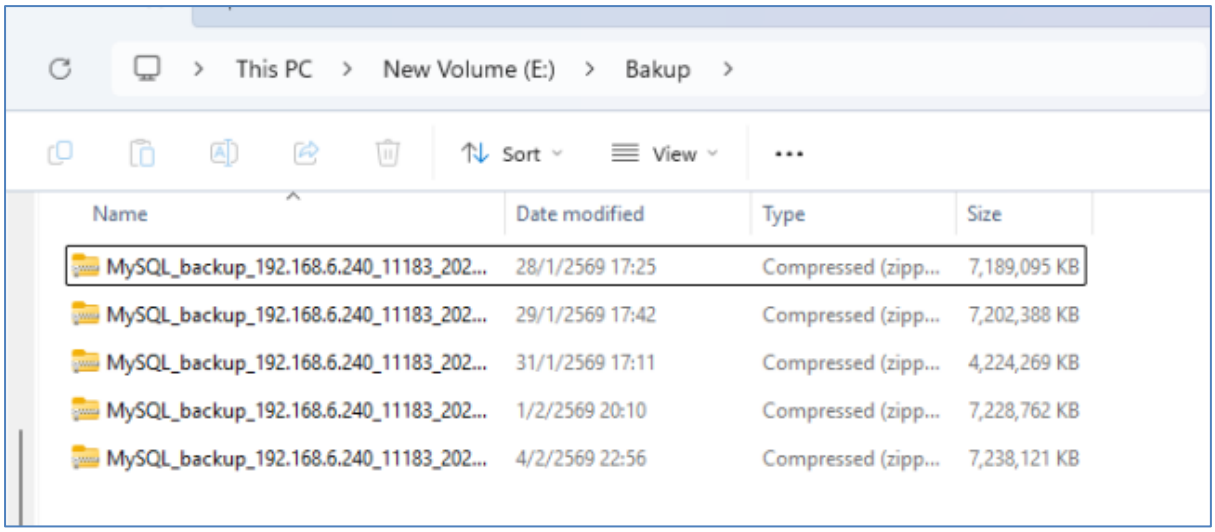
3. Backup on local (Server)



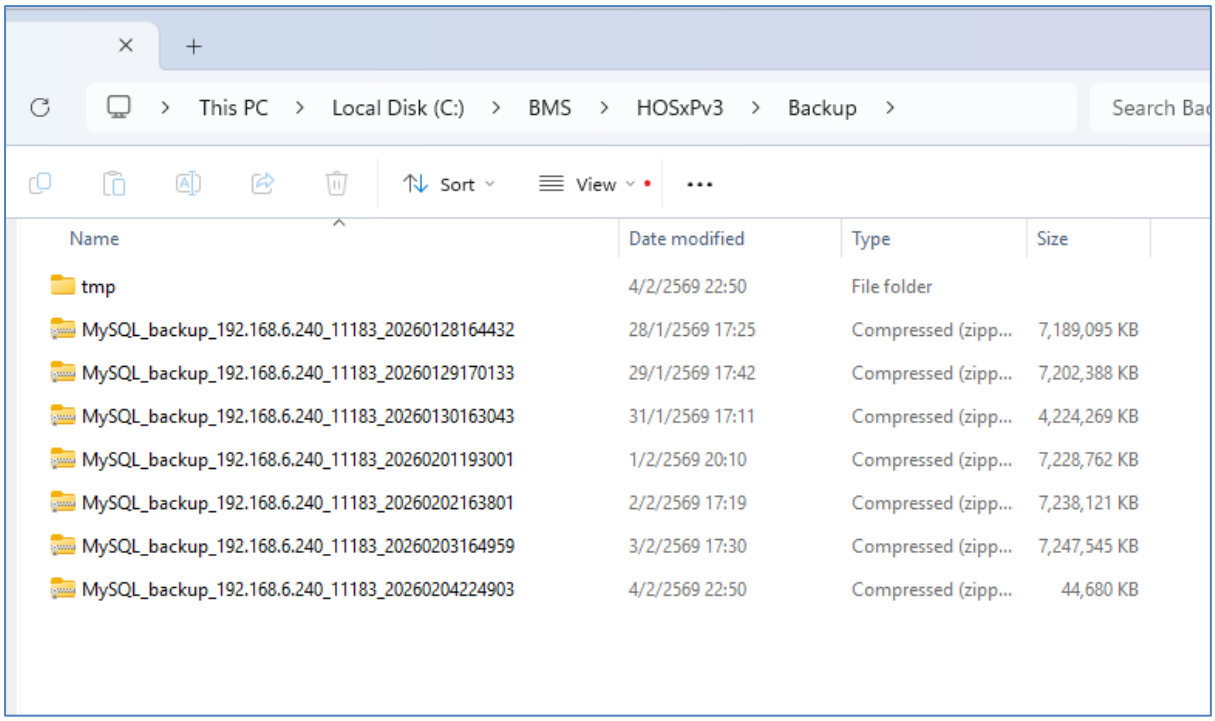
1.2 สำเนาข้อมูลไว้บนเทคโนโลยีต่างกัน 2 ชุด

มีการใช้เทคโนโลยีในการจัดเก็บ การสำรองข้อมูล (Backup) ที่ต่างกัน 2 ชุด ตามรายละเอียดดังนี้

1. Backup on External HDD/USB

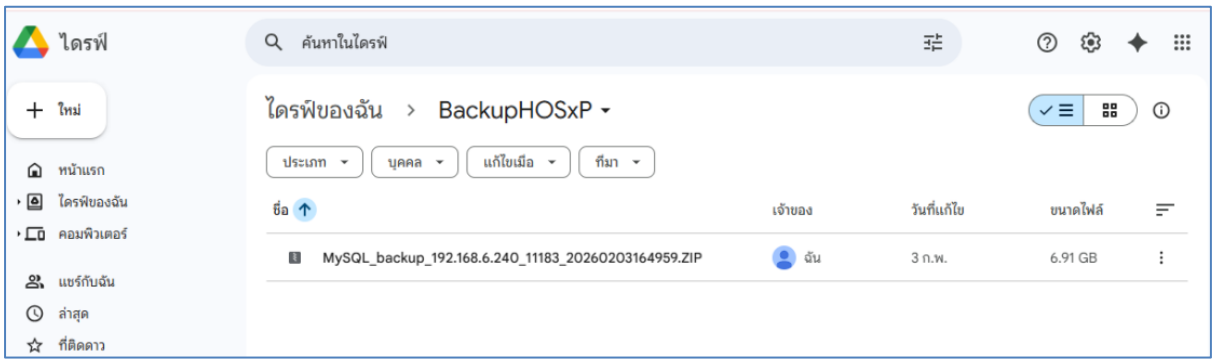


2. Backup on client



1.3 สำเนาข้อมูลไว้แบบ Offsite หรือ Cloud 1 ชุด

1. Backup on Cloud (Google Drive)

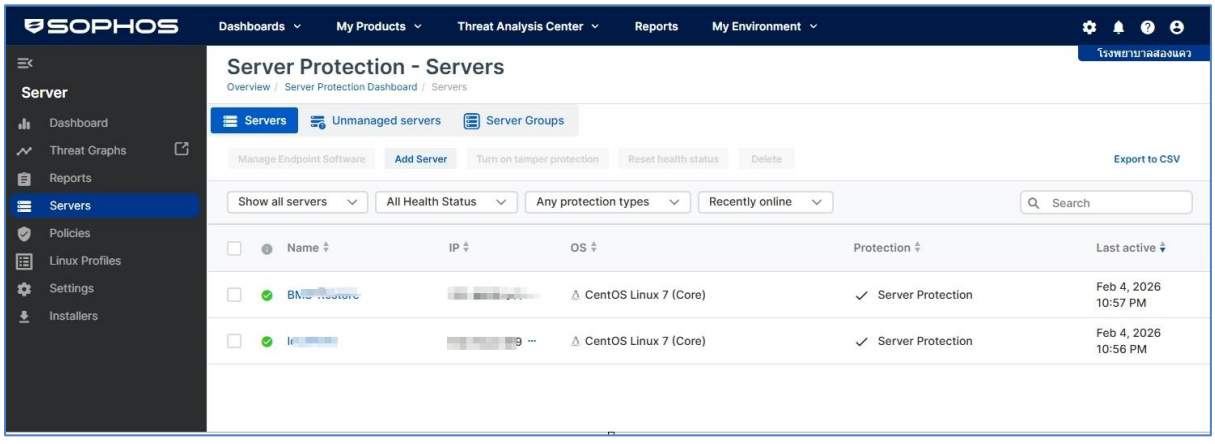


2. Antivirus Software : โปรแกรมป้องกันไวรัส หรือ แอนติไวรัส คอยตรวจจับ ป้องกัน และกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์หรือมัลแวร์

รายละเอียดหัวข้อการประเมิน

มีการติดตั้ง Next-gen Anti-virus หรือ EDR หรือ XDR ที่เครื่องฝั่ง Server ทุกเครื่องและอัปเดท Signature ทุกวันและมีเอกสารแนบระบุ Product และ Version อย่างละเอียดชัดเจน โดย Anti-Virus จะต้อง Activate ตลอดเวลาในการดำเนินการ Phase1 จะต้องตรวจสอบติดตั้งเฉพาะกลุ่ม Server ก่อนเท่านั้น โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย

การติดตั้ง EDR และ XDR Sophos Server



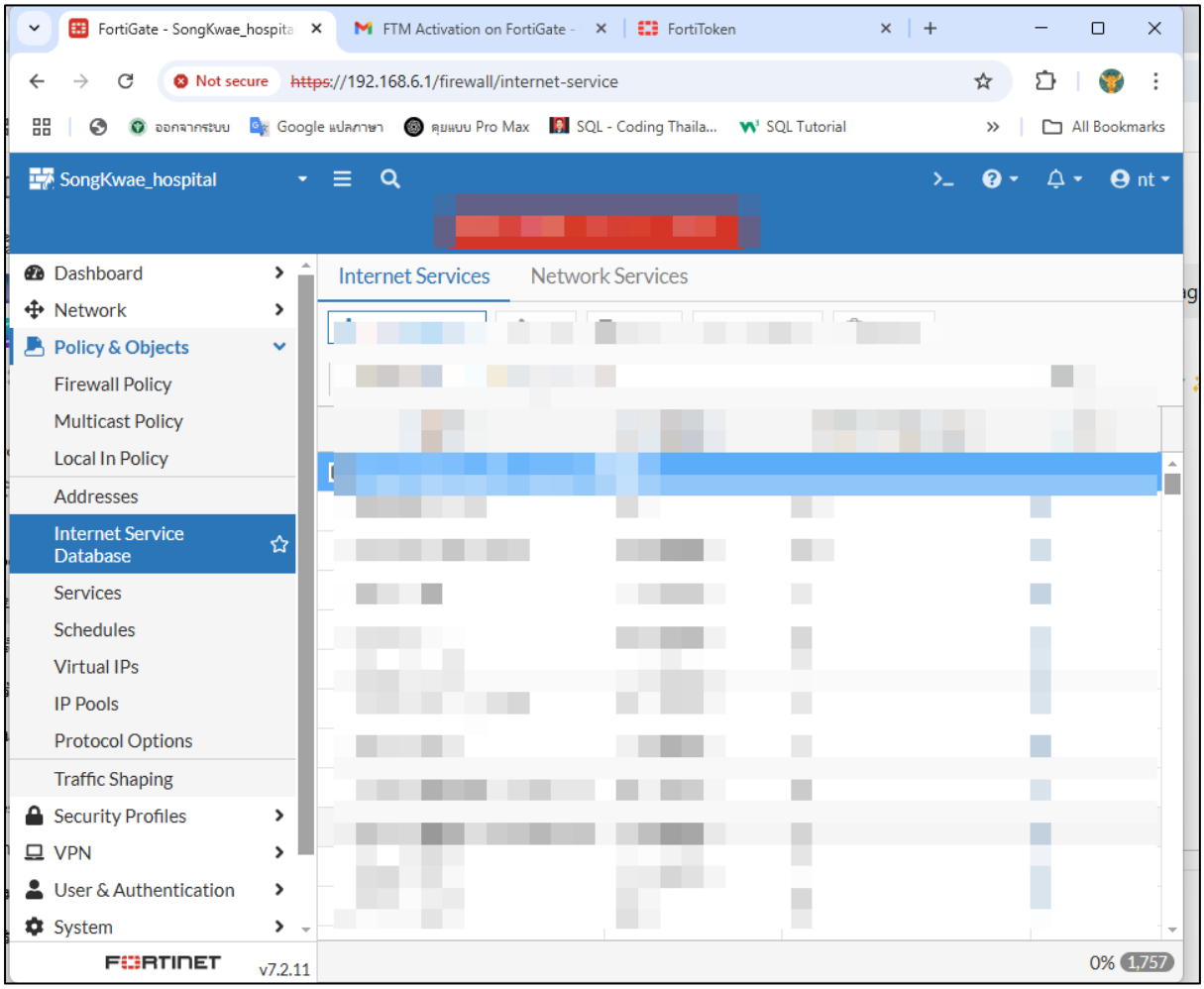
3. Access Control (Public และ Private) : การควบคุมอุปกรณ์หรือการเข้าถึงระบบผ่านทางช่องทาง Public/Private ทั้งภายในประเทศ และต่างประเทศ

รายละเอียดหัวข้อการประเมิน

มีระบบ Security ในการควบคุม Policy การเข้าถึงระบบที่สำคัญทั้งทาง Public และ Private โดยมีรายละเอียดดังนี้ โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย

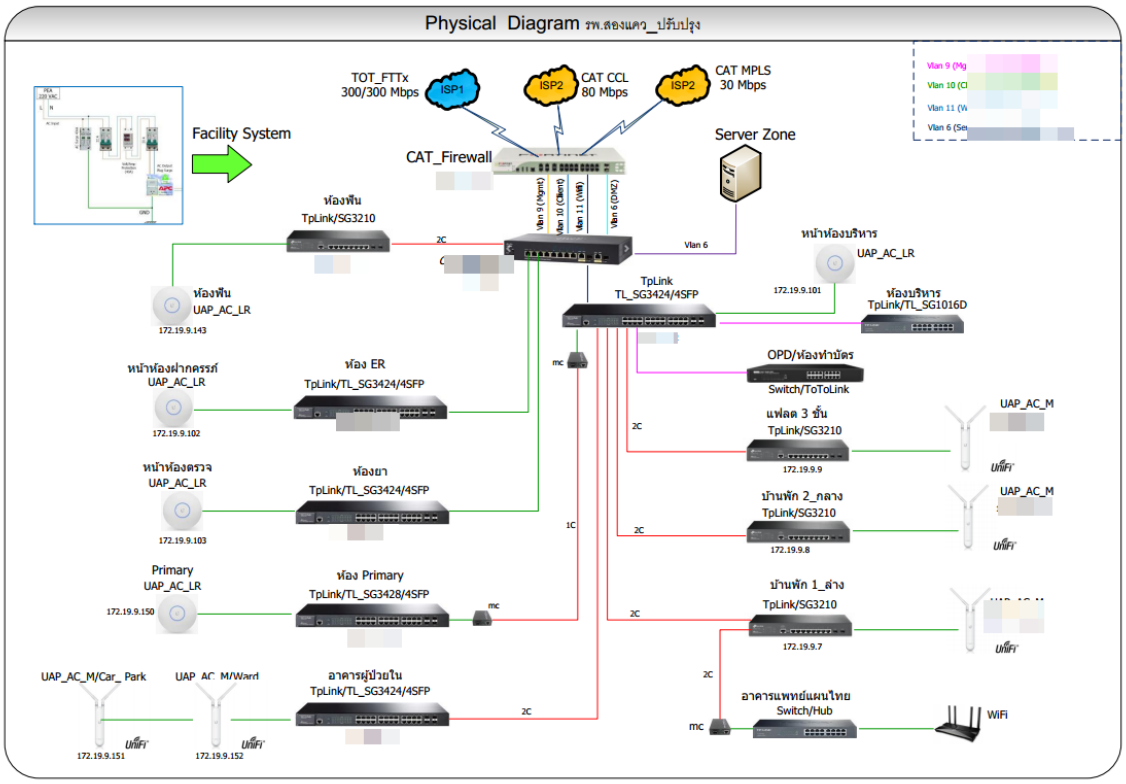
3.1 ดำเนินการกำหนด Whitelist Port และไม่เปิด Port ที่มีความเสี่ยง

มีการติดตั้ง Next Gen Firewall All@Secure (FortiGate) ปรับแต่ง Policy โดยกำหนด Source Destination และ Port เพื่อป้องกันความเสี่ยงต่อการโดนโจมตี



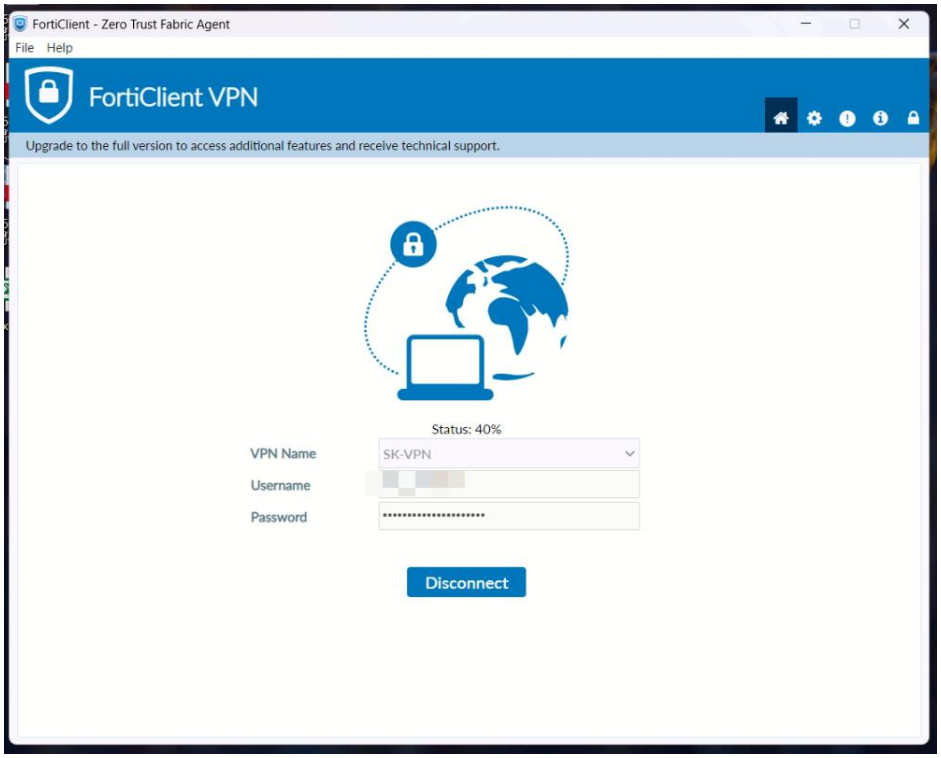
3.2 มีการแบ่งโซน Network ระหว่างอุปกรณ์แม่ข่าย (Server) และอุปกรณ์ลูกข่าย (Client)

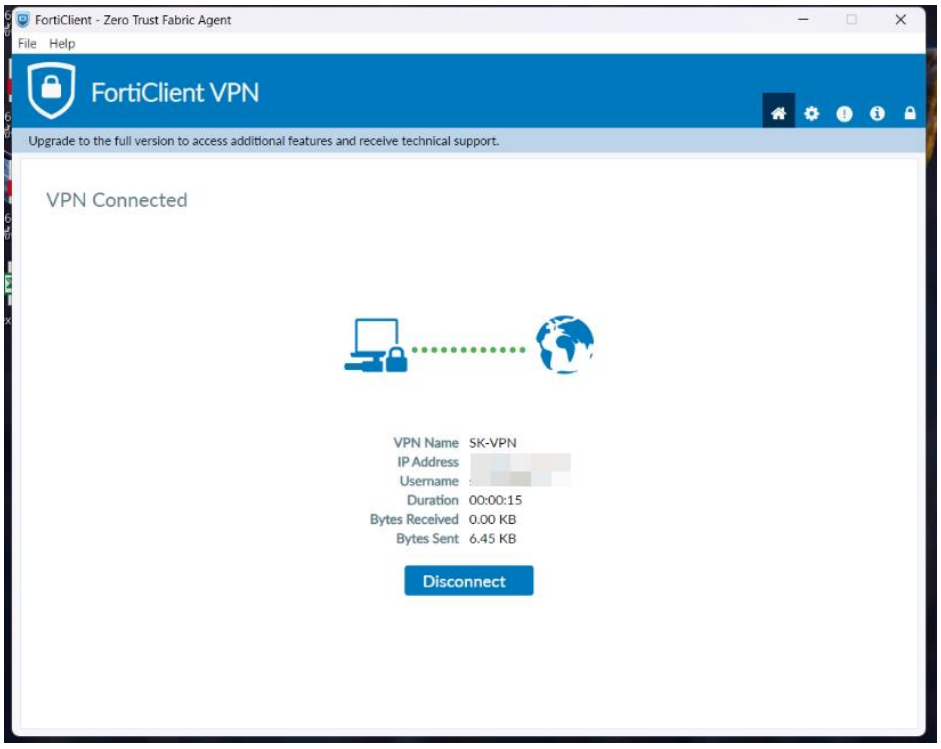
ติดตั้งและปรับปรุงระบบ Network จัดทำ VLAN มีการแบ่งโซน Network ระหว่างอุปกรณ์แม่ข่าย (Server) และอุปกรณ์ลูกข่าย (Client) อย่างชัดเจน



3.3 มีการใช้งาน VPN ในการเข้าถึงเครื่องอุปกรณ์แม่ข่าย (Server) แทนการเข้าใช้งานผ่าน Public

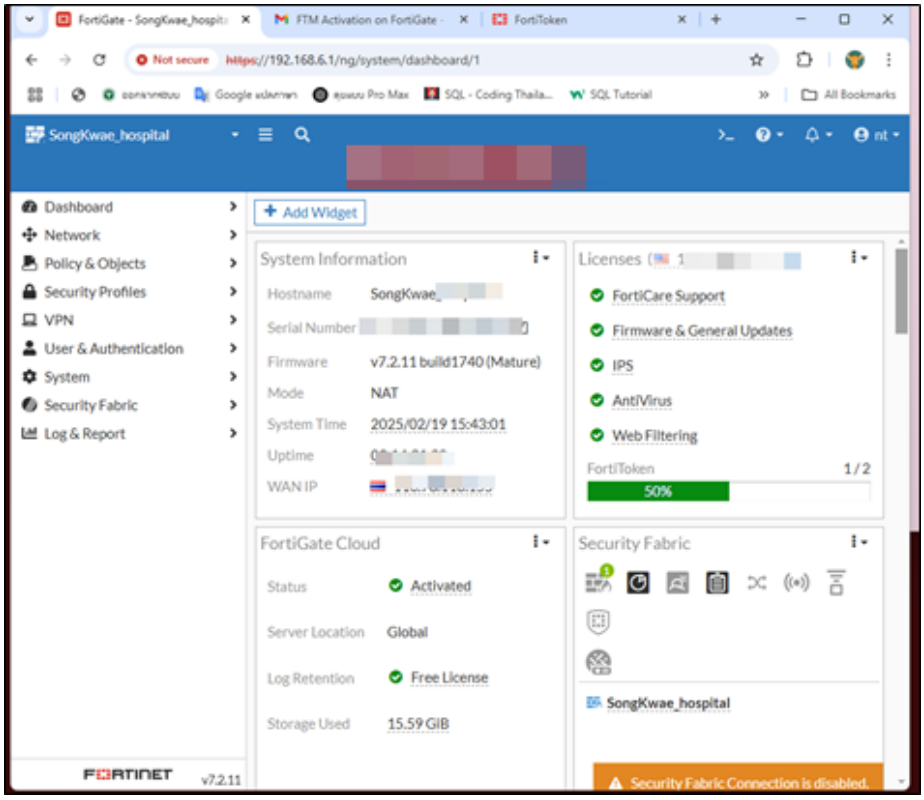
มีการใช้งาน VPN โดยได้ติดตั้ง FortiClient เพื่อรีโมทเข้ามาจัดการเครื่องแม่ข่าย (Server) แทนการเข้าใช้งานผ่าน Public


FortiClient - Zero Trust Fabric Agent
File Help
FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
Status: 40%
VPN Name
SK-VPN
Username
Password
Disconnect


FortiClient - Zero Trust Fabric Agent
File Help
FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
VPN Connected
VPN Name SK-VPN
IP Address
Username
Duration 00:00:15
Bytes Received 0.00 KB
Bytes Sent 6.45 KB
Disconnect

3.4 มีการ Block การใช้งาน International Traffic กรณีไม่มีความจำเป็นในการใช้งาน

มีการติดตั้ง Next Gen Firewall All@Secure (FortiGate) จึงทำให้สามารถจำแนกปลายทาง Traffic ว่าเป็นTraffic ภายในหรือภายนอกประเทศได้



<u>หัวข้อประเมินที่ 2 : ความเสี่ยงสูง</u>

5. Business Continuity Plan (BCP) และ Disaster Recovery Plan (DRP) : แผนที่กำหนดแนวทางการดำเนินการของหน่วยงาน เมื่อเกิดสภาวะวิกฤตหรือภัยต่างๆ ส่งผลให้กระบวนการทำงานของหน่วยงานหยุดชะงัก, เพื่อให้สามารถกลับมาดำเนินการได้อย่างต่อเนื่อง และแผนการกู้คืน

รายละเอียดหัวข้อการประเมิน

มีการทดสอบ Business Continuity Plan (BCP) และแผนกู้คืน Disaster Recovery Plan (DRP) ดังเอกสารแนบ

แผนบริหารความต่อเนื่องภายใต้สภาวะวิกฤต (Business Continuity Plan : BCP) และแผนกู้คืน (Disaster Recovery Plan : DRP)

โรงพยาบาลสองแคว

อำเภอสองแคว จังหวัดน่าน

จัดทำโดย

กลุ่มงานสุขภาพดิจิทัล

15 มกราคม 2568

สารบัญ

คำสั่ง โรงพยาบาลสองแคว

ที่ ๓๘ / ๒๕๖๘

เรื่อง แต่งตั้งคณะกรรมการทำงานจัดทำคู่มือแผนบริหารความต่อเนื่องภายใต้สภาวะวิกฤต (Business Continuity Plan : BCP) และแผนกู้คืน (Disaster Recovery Plan : DRP) โรงพยาบาลสองแคว

เพื่อเตรียมความพร้อมให้โรงพยาบาลสองแคว สามารถรับมือกับสถานการณ์ภัยพิบัติและเหตุฉุกเฉิน โดยเป็นการป้องกัน ตรวจค้น และตอบสนองต่อสถานการณ์วิกฤตเพื่อลดปัญหาที่อาจเกิดขึ้นในการขับเคลื่อนการดำเนินงานตามภารกิจขององค์กร

ฉะนั้นอาศัยอำนาจตามมาตรา ๓๘ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ จึงขอแต่งตั้งคณะทำงานจัดทำคู่มือแผนบริหารต่อเนื่องภายใต้สภาวะวิกฤต (Business Continuity Plan : BCP) และแผนกู้คืน (Disaster Recovery Plan : DRP) โดยมีรายชื่อคณะกรรมการฯ ดังนี้

๑. นายกุลพล ตั้งรัตนาพิบูล	นายแพทย์ชำนาญการ(ด้านเวชกรรม)ปฏิบัติหน้าที่	ประธานกรรมการ
๒. นางสาวณวัฒน์ เดชพุทธวัจน์	ทันตแพทย์ชำนาญการพิเศษ	รองประธานกรรมการ
๖. นายวรศิลป์ แสนสองสี	เจ้าพนักงานวิทยาศาสตร์การแพทย์ชำนาญงาน	กรรมการ
๓. นางสาวพนารัตน์ เจตีย์กอง	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๔. นางวิภารัตน์ บูรพาวิจิตรนนท์	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๕. ประพัฒน์ คีรีสันติกุล	เภสัชกรชำนาญการ	กรรมการ
๗. นางณัฐรดา แสนยอด	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๘. นางสาวภัคจิรัษญา พูลสวัสดิ์	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๙. นางสาวนารีรัตน์ สุริยสาร	นักกายภาพบำบัดปฏิบัติการ	กรรมการ
๑๐. นางสาวอรพรรณ ผาหลัก	นักวิชาการสาธารณสุขปฏิบัติการ	กรรมการ
๑๑. นางสาวตรีรัตน์ ทนันชัย	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการและเลขานุการ
๑๒. นายวรภพ ประสมทรัพย์	นักวิชาการคอมพิวเตอร์	กรรมการและผู้ช่วยเลขานุการ

บทบาทหน้าที่

๑. จัดทำคู่มือแผนแผนบริหารความต่อเนื่องภายใต้สภาวะวิกฤต (Business Continuity Plan : BCP) และแผนกู้คืน (Disaster Recovery Plan : DRP)

๒. วิเคราะห์สถานการณ์ภัยพิบัติและเหตุฉุกเฉินที่ส่งผลกระทบต่อการปฏิบัติงานขององค์กร

๓. ระบุผลกระทบที่อาจเกิดขึ้นกับองค์กร

๓. กำหนดกิจกรรม / วิธีการแก้ไขปัญหา / ผู้รับผิดชอบหลัก-ผู้รับผิดชอบรอง

๔. ติดตามและรายงานผลการดำเนินงาน เสนอผู้บังคับบัญชา

๖. อื่นๆ ตามที่ได้รับมอบหมาย

ทั้งนี้ ให้คณะทำงานที่ได้รับการแต่งตั้ง ปฏิบัติหน้าที่ ตามที่ได้รับมอบหมายอย่างเคร่งครัด ตั้งแต่บัดนี้เป็นต้นไป

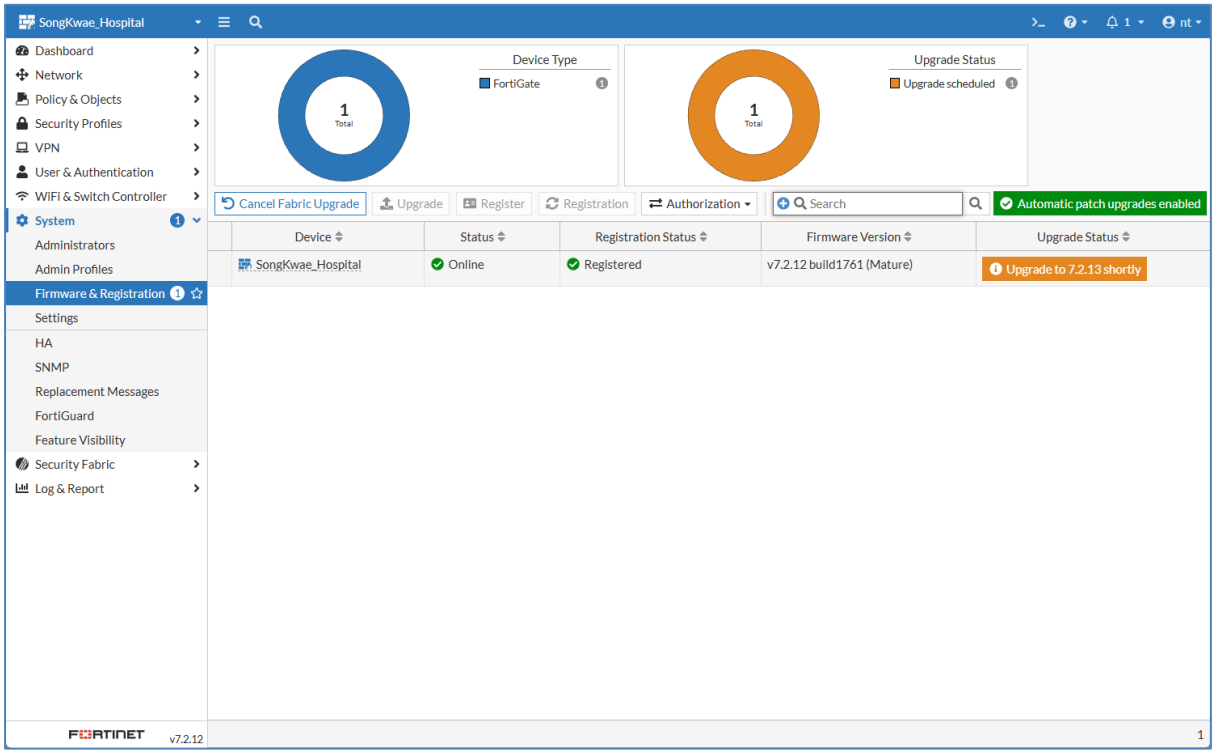
สั่ง ณ วันที่ ๑๕ เดือน มกราคม พ.ศ. ๒๕๖๘

(นายกุลพล ตั้งรัตนาพิบูล)
นายแพทย์ชำนาญการ(ด้านเวชกรรม) ปฏิบัติหน้าที่
ผู้อำนวยการโรงพยาบาลสองแคว

6. OS Patching : การซ่อมแซมจุดบกพร่องของระบบปฏิบัติการ (OS) หรือปรับปรุงระบบปฏิบัติการให้ทันสมัย และเพิ่มเติมความสามารถในการใช้งาน หรือประสิทธิภาพที่ดีขึ้น

รายละเอียดหัวข้อการประเมิน

โรงพยาบาลมีการดำเนินการอัปเดต Security Patching ในระดับ Operating System (Windows / Linux) อย่างสม่ำเสมอทุก 6 เดือน หรือทันทีเมื่อมีการประกาศแพตช์ด้านความปลอดภัยระดับ Critical โดยมีการตรวจสอบให้มั่นใจว่าไม่มี Security Patch ค้างอยู่ในระดับ Critical และ High ครอบคลุมอย่างน้อยในระบบปฏิบัติการของเครื่องแม่ข่ายที่ให้บริการระบบ HIS (HOSxP)



8. Web Application Firewall (WAF) : ระบบป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอพพลิเคชั่นโดยเฉพาะ เพื่อป้องกันการโจมตีไปยังระบบเว็บแอพพลิเคชั่นขององค์กร

รายละเอียดหัวข้อการประเมิน

มีการใช้งาน Web Application Firewall (WAF) กรณีที่มีระบบเป็น Web Application ในรูปแบบ Cloud security เพื่อป้องกันการโจมตีตามมาตรฐาน OWASP Top 10 ได้เป็นอย่างน้อย

" โรงพยาบาลสองแควได้เลือกใช้บริการเช่าเว็บไซต์สำเร็จรูปจากบริษัท เรดดี้แพลนเน็ต จำกัด (มหาชน) ซึ่งเป็นผู้ให้บริการที่ได้รับการรับรองมาตรฐานความปลอดภัยของข้อมูลตามมาตรฐาน ISO 27001:2022 โดยมาตรฐานนี้ครอบคลุมถึงการจัดการความปลอดภัยของข้อมูลในทุกขั้นตอน รวมถึงการป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ นอกจากนี้ ระบบดังกล่าวยังมีการติดตั้ง Web Application Firewall (WAF) เพื่อป้องกันการโจมตีที่พุ่งเป้าไปที่ช่องโหว่ของเว็บแอปพลิเคชัน เช่น SQL Injection และ Cross-Site Scripting (XSS) ทำให้มั่นใจได้ว่าเว็บไซต์ของโรงพยาบาลมีความมั่นคงปลอดภัยและเป็นไปตามข้อกำหนดด้านความปลอดภัยที่ได้กำหนดไว้ "

9. Log Management : การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์

รายละเอียดหัวข้อการประเมิน

มีระบบการจัดเก็บ Log อินเตอร์เน็ต และคอมพิวเตอร์ ตาม พ.ร.บ.ฯ อย่างน้อย 90 วัน

10. Security Information & Event Management (SIEM) : ระบบที่ใช้ในการจัดการกับ Log และ Event ต่างๆ ที่คอยทำหน้าที่วิเคราะห์หาความเชื่อมโยงของ Event ต่างๆ ที่เกี่ยวข้องกับความปลอดภัย ทั้งหมดไปจนถึงการ Alert ระบุตำแหน่งของภัยคุกคามให้ทราบ เมื่อมี Event ที่ผิดปกติ ทำให้สามารถป้องกันและตอบสนองภัยคุกคามได้อย่างรวดเร็ว

รายละเอียดหัวข้อการประเมิน

มีระบบ SIEM เพื่อนำมาวิเคราะห์พฤติกรรมของ Cyber Attack บนระบบที่ให้บริการทั้งระดับ Infrastructure และ Operating system (OSX โดยจะต้องครอบคลุมการตรวจจับพื้นฐาน

มีการติดตั้งระบบ SIEM / CSM (Cyber Security Monitoring)

11. Vulnerability Assessment (VA Scan) : การตรวจสอบช่องโหว่ของระบบ เพื่อให้ทราบถึงความเสี่ยง จุด อ่อน และระดับความรุนแรง ของผลกระทบที่อาจเกิดขึ้นจากการถูกโจรกรรมข้อมูล และการโจมตีทางไซเบอร์

รายละเอียดหัวข้อการประเมิน

มีการดำเนินการ Vulnerability Assessment (VA Scan) อย่างน้อยปีลุ 1 ครั้ง ในระดับ Operating System (OS) โดยจะต้องดำเนินการแก้ไข CVE และช่องโหว่ต่างๆ ที่เกิดขึ้นโดยจะต้องไม่มีความเสี่ยงระดับ Critical, High ในระบบที่ตรวจสอบโดยคลอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน

12. Software Update : มีการตรวจสอบ Version ของ Software ให้เป็นVersion Update ล่าสุด เพื่อปิดช่องโหว่ที่เกิดขึ้นใน Software Version ก่อน

รายละเอียดหัวข้อการประเมิน

มีการตรวจสอบ Version ของ Software ให้เป็นVersion Update ล่าสุด เพื่อปิดช่องโหว่ที่เกิดขึ้นใน Software Version ก่อนหน้า มีการอับเดต Software Patching ของระบบ HIS และมีการทำ Penetration Testing อย่างน้อยปีละ 1 ครั้ง หรือ มีการออก Major version โดยจะต้องดำเนินการแก้ไขช่องโหว่ใน ระดับ Severity Critical และ High เป็นอย่างน้อย โดย ครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย

ระบบ HIS ที่มีการอัพเดทระบบ

13. Penteration Testing : การทดสอบเจาะระบบ

รายละเอียดหัวข้อการประเมิน

มีการทดสอบการเจาะระบบ มีการทำ Penetration Testing ของ Web Application ในรูปแบบของ Graybox หรือ Blockbox อย่างน้อยปีละ 1 ครั้ง และดำเนินการแก้ไขโดยจะต้องไม่มีช่องโหว่ระดับ Severity Critical , High เกิดขึ้นและไม่มีช่องโหว่ที่เกิดขึ้นตามมาตรฐาน OWASP TOP10

การทำระบบ Penetration Testing