การกำหนดรอบการสำรองข้อมูล และการทดสอบการกู้คืนข้อมูล รวมถึงป้องกันสื่อบันทึกการสำรองข้อมูลจากความเสียหายและการสูญหาย และการเข้าถึงโดยไม่ได้รับอนุญาต

โรงพยาบาลแม่ลาว 2569

****

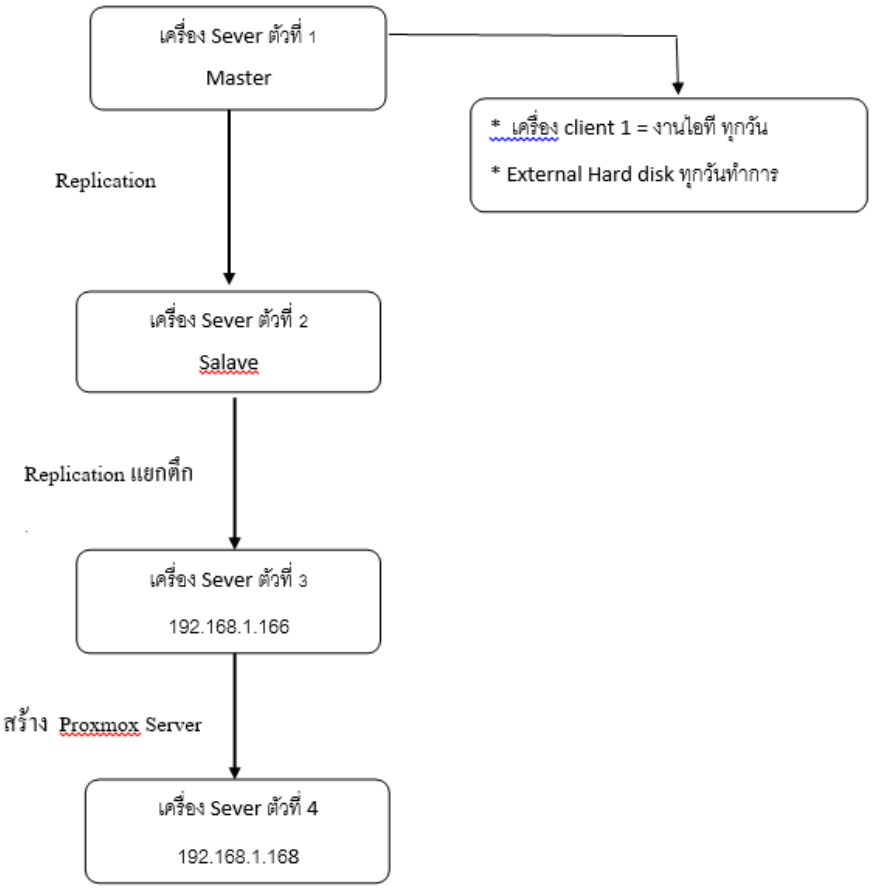
Backup

การสำรองข้อมูลเก็บไว้ที่อื่น เพื่อให้สามารถนำมาใช้กู้คืนข้อมูลเดิมได้หลังจากเกิดเหตุการณ์ข้อมูลสูญหาย โดยมีการสำรองข้อมูลอย่างน้อยวันละ 1 ครั้ง และสามารถเรียกดูข้อมูลย้อนหลังได้ไม่น้อยกว่า 7 วัน ตามมาตรฐานซึ่งจัดเก็บบนระบบ Logical HDD หรือ Physical HDD และมีการจัดเก็บ Backup ในรูปแบบ 3-2-1 โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย

1. สำเนาข้อมูลไว้บนระบบ 3 ชุด

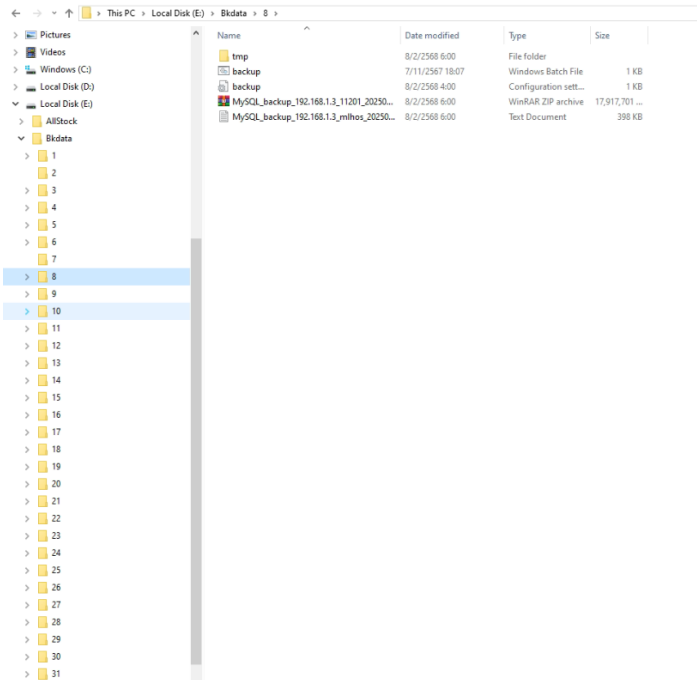
ดำเนินการทำ MySQL Replication แบบ Master-Slave จำนวน 2 ชุด

การสำรองข้อมูล

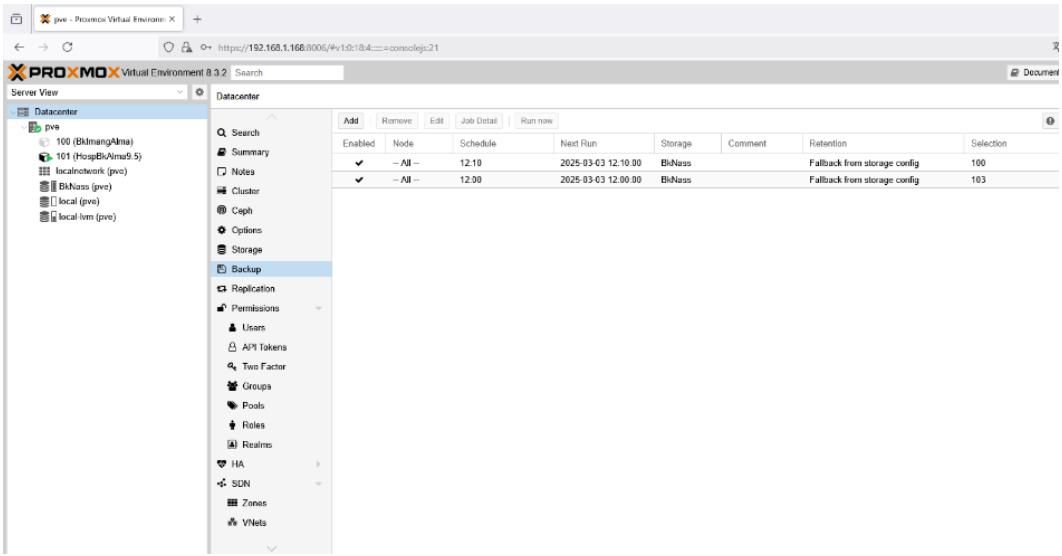


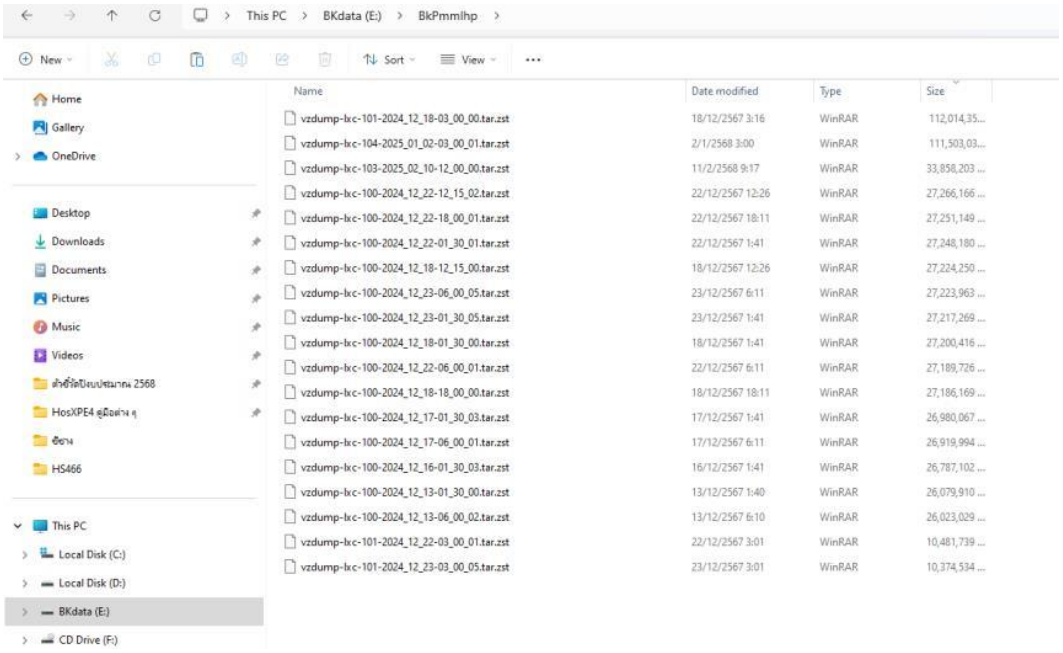
2. สำเนาข้อมูลไว้บนเทคโนโลยีต่างกัน 2 ชุด

HOSxPXE 4 Backup เวลา 01.00 น. ทุกวัน



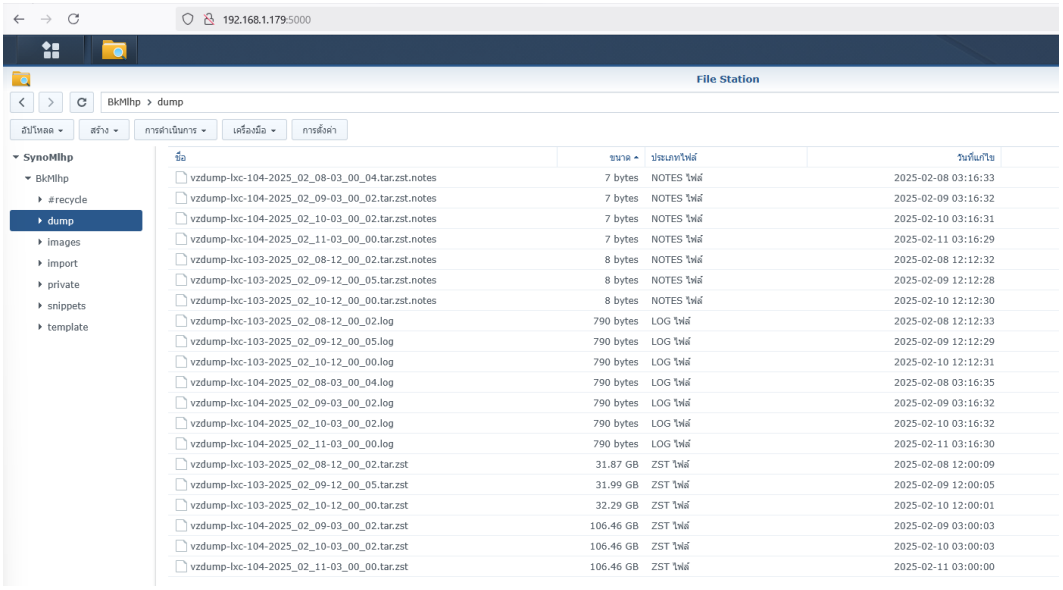
Proxmox สำรองเวลา 12.00 น. ทุกวัน สำรองออกมาไว้ในเครื่อง SynoMlhp





ทุกวันใช้อุปกรณ์ External Hard Disk (ฮาร์ดดิสก์พกพา) สำรองข้อมูลไว้

ทำการสำรองไว้ในเครื่อง SynoMlhp ตั้งเวลาสำรอง 12.00 น. ทุกวัน



Antivirus Software

มีการติดตั้ง Next-gen Anti-virus หรือ EDR หรือ XDR ที่เครื่องฝั่ง Server ทุกเครื่อง และอัปเดต Signature ทุกวัน และมีเอกสารแนบระบุ Product และ Version อย่างละเอียดชัดเจน โดย Antivirus จะต้อง Active ตลอดเวลา ในการดำเนินการ Phase 1 จะตรวจสอบติดตั้งเฉพาะกลุ่ม Server ก่อนเท่านั้น โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน นับเฉพาะ Server ทุกระบบ รวมถึงระบบของเอกชนที่เชื่อมต่อระบบบริการผู้ป่วยที่อยู่ใน VLAN เดียวกันกับ Server HIS

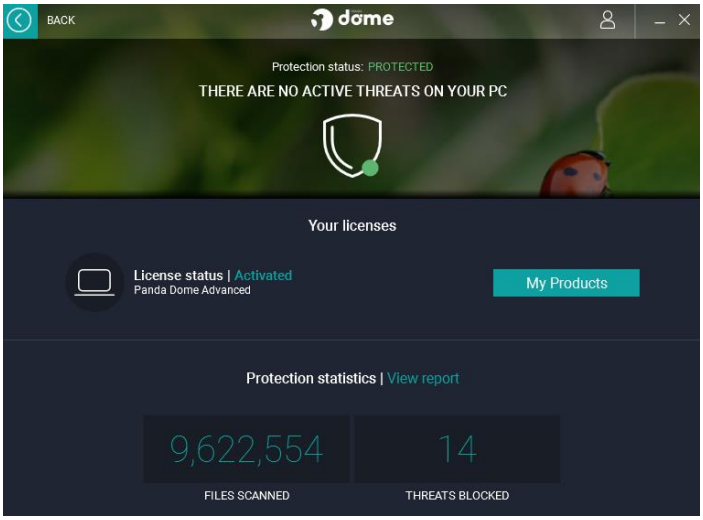
โรงพยาบาลแม่ลาวใช้ซอฟต์แวร์ Antivirus เครื่อง Client มี 2 ตัวด้วยกัน Panda Dome ลิขสิทธิ์แท้ที่มาพร้อมกับเครื่องคอมพิวเตอร์เครื่องเช่า โดยตัว Panda Dome ให้การปกป้องที่ครอบคลุมตั้งแต่ระดับพื้นฐานไปจนถึงระดับสูง โดยเน้นการรักษาความปลอดภัยใน 3 ด้านหลัก

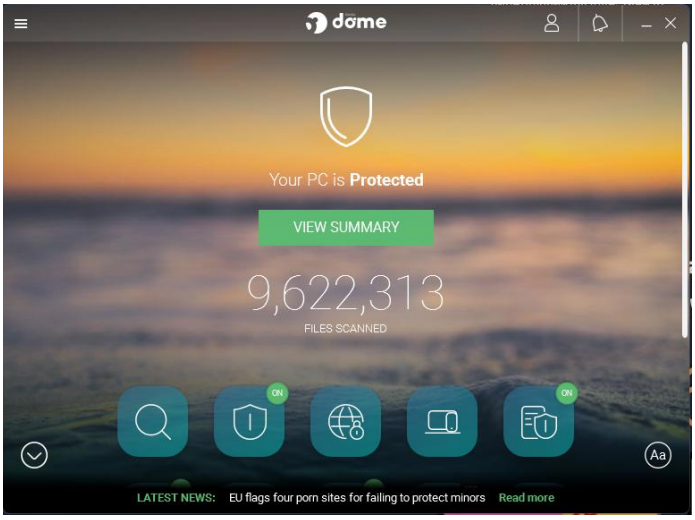
1. การป้องกันภัยคุกคามจากมัลแวร์และไวรัส แอนตี้ไวรัสแบบเรียลไทม์ ตรวจสอบไฟล์และกระบวนการทำงานในเครื่องตลอดเวลาเพื่อบล็อกไวรัส โทรจัน และสปายแวร์ ป้องกัน Ransomware USB Protection สแกนและป้องกันการติดเชื้อจากแฟลชไดรฟ์หรืออุปกรณ์ USB ที่นำมาเสียบกับเครื่อง

2. ความปลอดภัยบนเครือข่าย บล็อกเว็บไซต์ปลอมและการหลอกลวง ,ตรวจสอบความปลอดภัยของเครือข่าย Wi-Fi ,Personal Firewall ,VPN

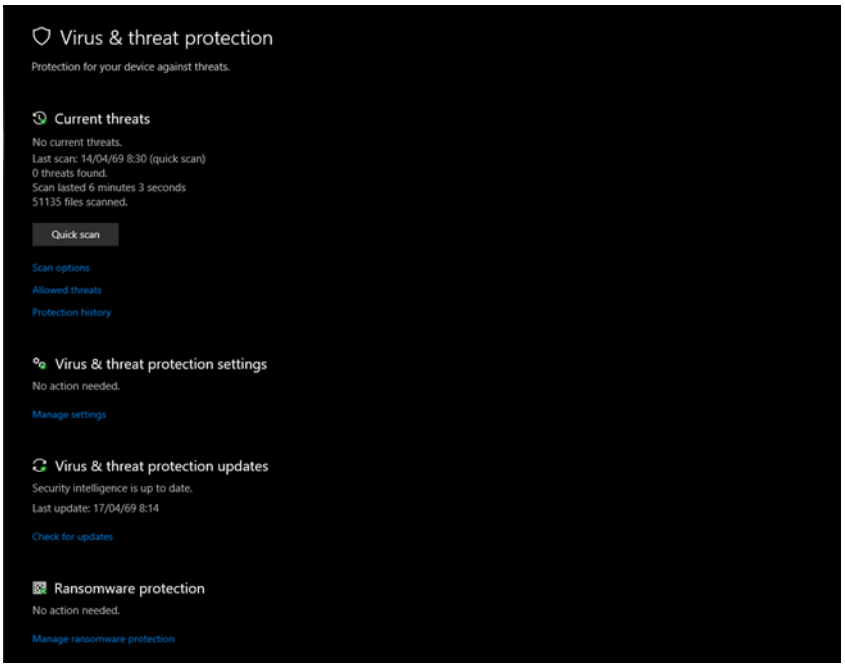
3. ฟีเจอร์เสริมสำหรับการใช้งานเฉพาะด้าน Parental Control สามารถบล็อกเนื้อหาที่ไม่

เหมาะสมและติดตามการใช้งานอินเทอร์เน็ตได้ Dark Web Scanner แจ้งเตือนหากพบว่าอีเมลหรือข้อมูลบัญชีรั่วไหลบน Dark Web

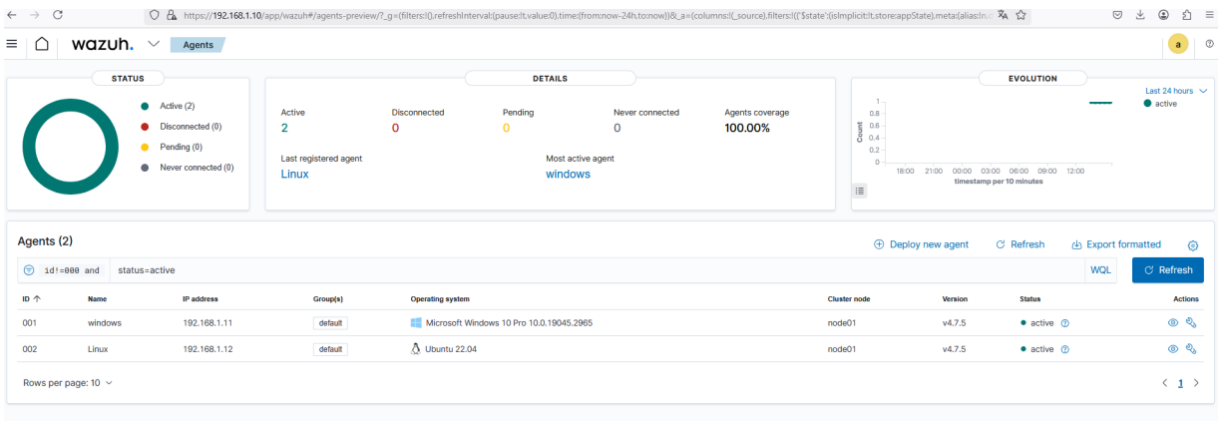




และโรงพยาบาลแม่ลาวยังใช้ซอฟต์แวร์ Antivirus Microsoft Defender ที่มีอยู่กับระบบปฏิบัติ Windows License สำหรับเครื่องที่ไม่มีโปรแกรม Antivirus เสริม สำหรับตัว Microsoft Defender ก็สามารถใช้งานปกป้องระบบภัยคุกคามได้ เช่น มัลแวร์ Ransomeware การแสกนไฟล์อันตราย ได้ครอบคุม



เครื่อง Server ติดตั้ง Agents wazuh

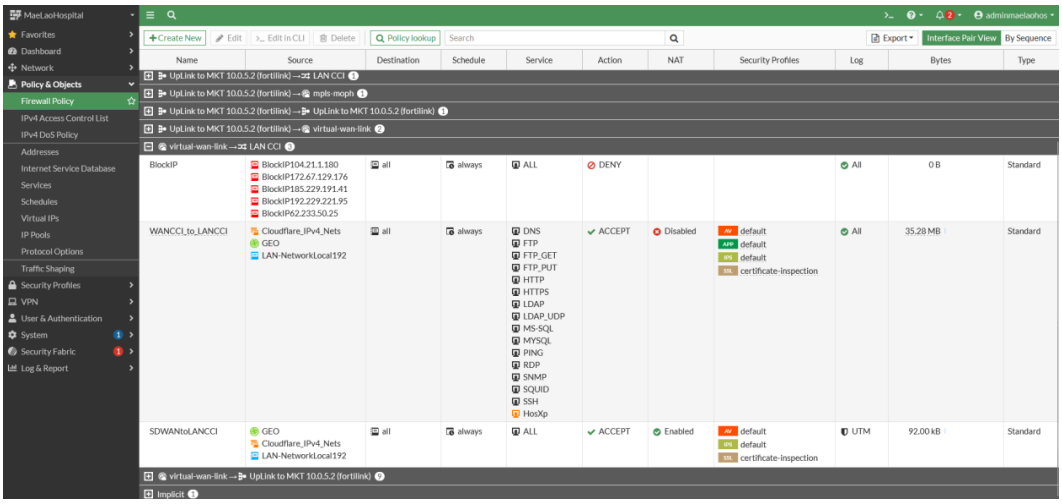


Access Control (Public และ Private)

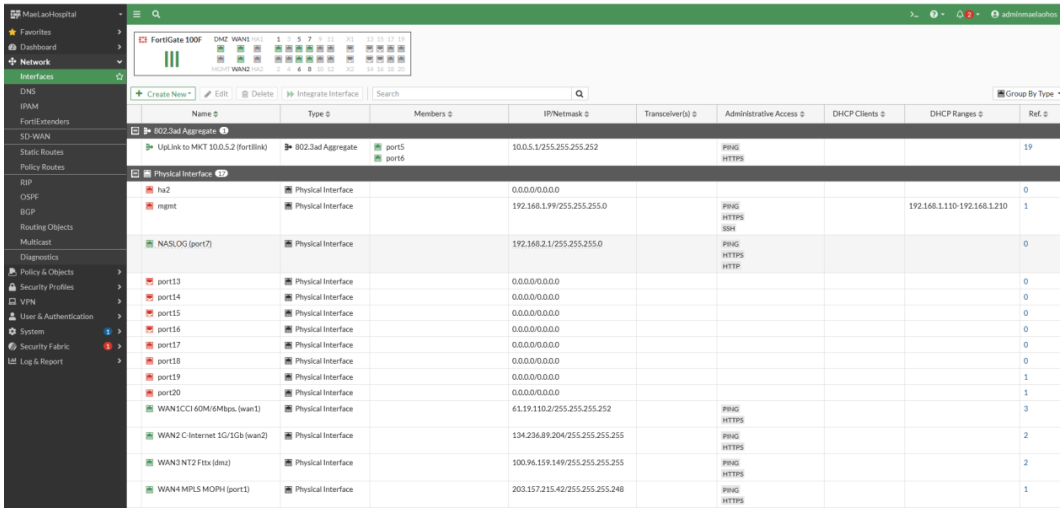
การควบคุมอุปกรณ์หรือการเข้าถึงระบบผ่านทางช่องทาง Public/Private ทั้งภายในประเทศและต่างประเทศ มีระบบ Security ในการควบคุม Policy การเข้าถึงระบบที่สำคัญทั้งทาง Public และ Private โดยมี

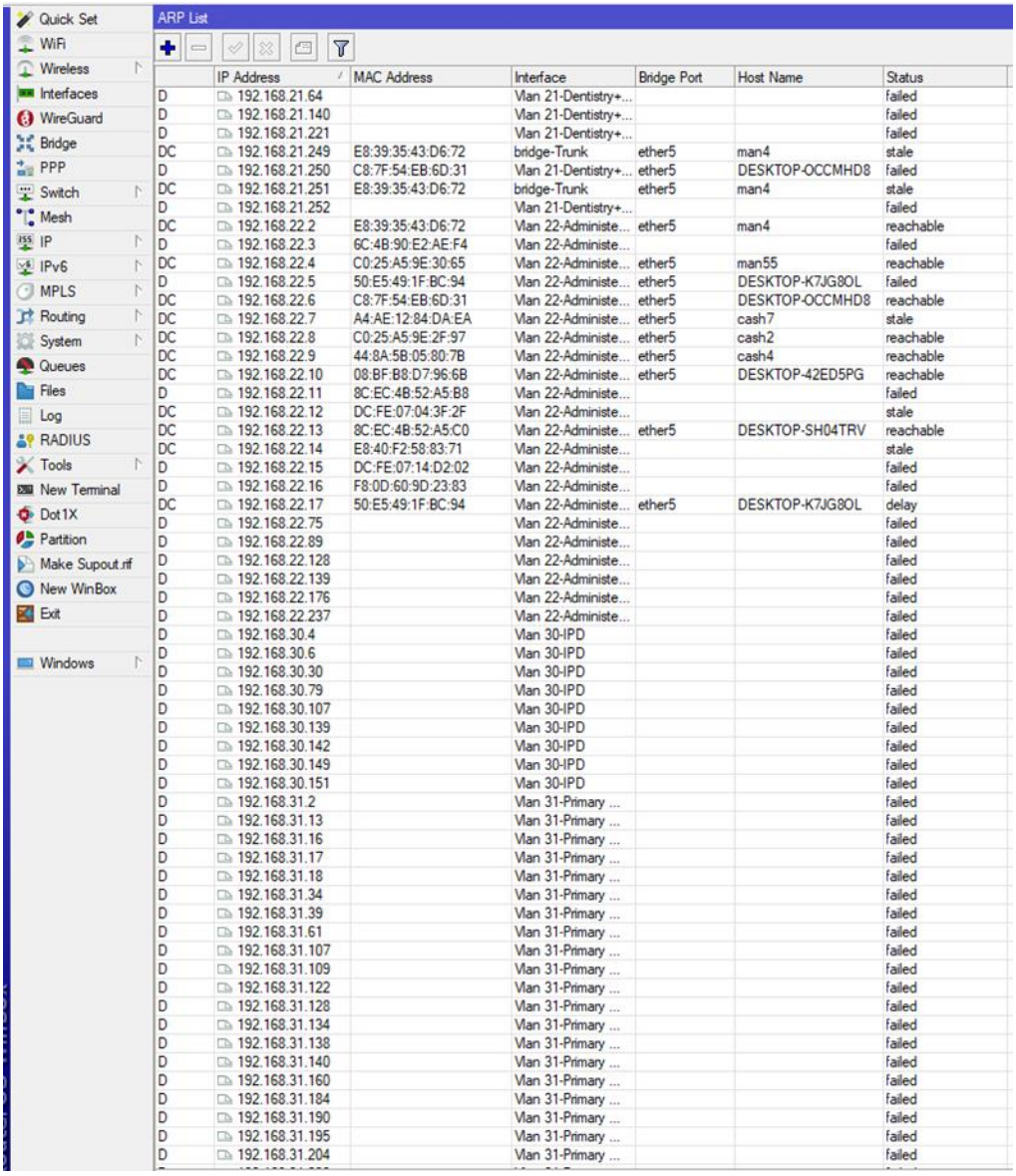
ดำเนินการกำหนด White list Port และไม่เปิด Port

Port ที่มีความเสี่ยงต่อการโดนโจมตีปัจจุบัน ได้แก่ 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, 3389, 8080 (หากมีความจำเป็นในการเปิดจะต้องทำการกำหนด Source และ Destination ให้ชัดเจน)



มีการแบ่งโซน Network ระหว่างอุปกรณ์แม่ข่าย (Server) และ อุปกรณ์ลูกข่าย (Client) แบ่ง 2 VLAN อย่างน้อย Server client

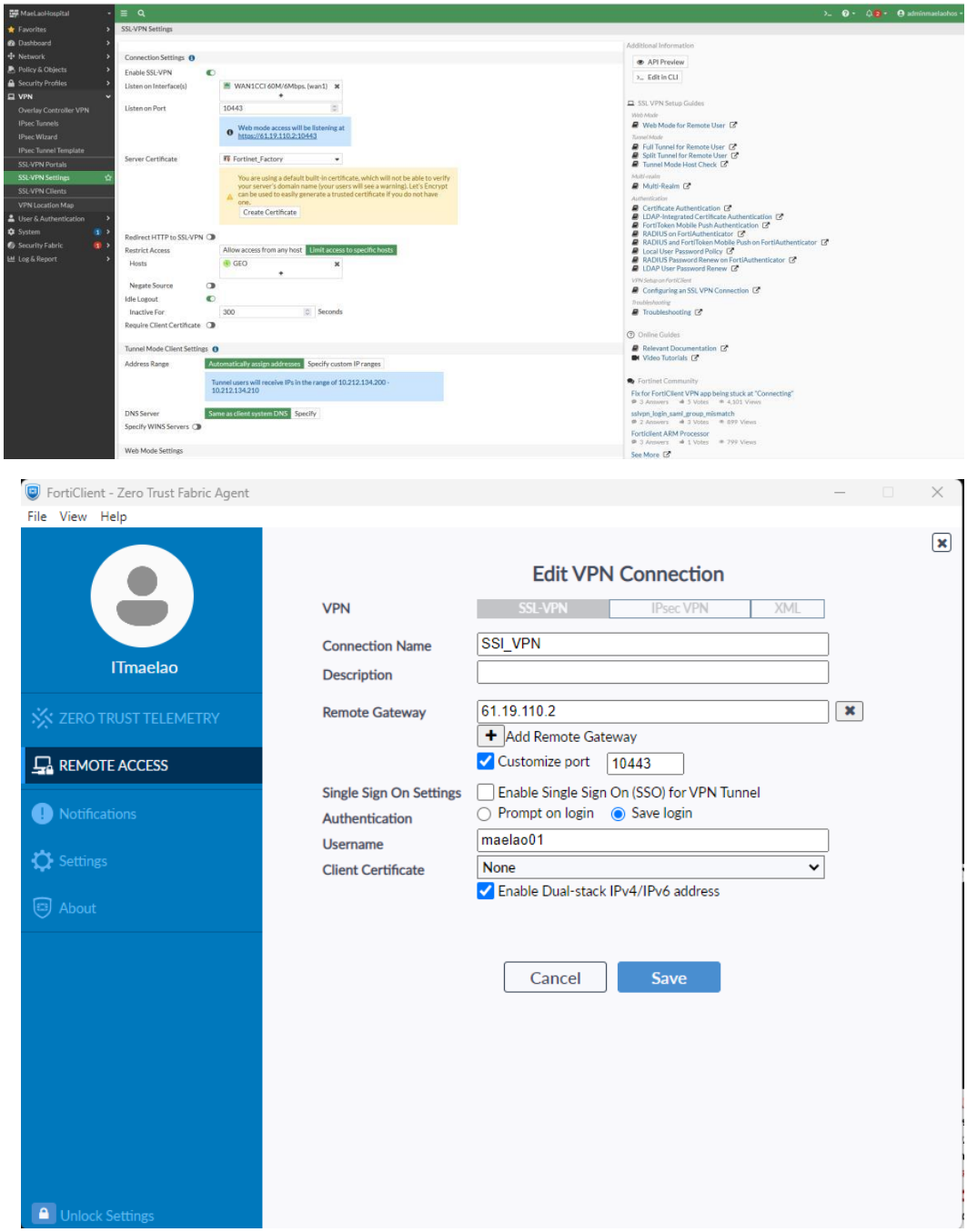




	IP Address	MAC Address	Interface	Bridge Port	Host Name	Status
D	192.168.21.64		Vlan 21-Dentistry+...			failed
D	192.168.21.140		Vlan 21-Dentistry+...			failed
D	192.168.21.221		Vlan 21-Dentistry+...			failed
DC	192.168.21.249	E8:39:35:43:D6:72	bridge-Trunk	ether5	man4	stale
D	192.168.21.250	C8:7F:54:EB:6D:31	Vlan 21-Dentistry+...	ether5	DESKTOP-OCCMHD8	failed
DC	192.168.21.251	E8:39:35:43:D6:72	bridge-Trunk	ether5	man4	stale
D	192.168.21.252		Vlan 21-Dentistry+...			failed
DC	192.168.22.2	E8:39:35:43:D6:72	Vlan 22-Administe...	ether5	man4	reachable
D	192.168.22.3	6C:4B:90:E2:AE:F4	Vlan 22-Administe...			failed
DC	192.168.22.4	C0:25:A5:9E:30:65	Vlan 22-Administe...	ether5	man55	reachable
D	192.168.22.5	50:E5:49:1F:BC:94	Vlan 22-Administe...	ether5	DESKTOP-K7JG8OL	failed
DC	192.168.22.6	C8:7F:54:EB:6D:31	Vlan 22-Administe...	ether5	DESKTOP-OCCMHD8	reachable
DC	192.168.22.7	A4:AE:12:84:DA:EA	Vlan 22-Administe...	ether5	cash7	stale
DC	192.168.22.8	C0:25:A5:9E:2F:97	Vlan 22-Administe...	ether5	cash2	reachable
DC	192.168.22.9	44:8A:5B:05:80:7B	Vlan 22-Administe...	ether5	cash4	reachable
DC	192.168.22.10	08:BF:B8:D7:96:6B	Vlan 22-Administe...	ether5	DESKTOP-42ED5PG	reachable
D	192.168.22.11	8C:EC:4B:52:A5:B8	Vlan 22-Administe...			failed
DC	192.168.22.12	DC:FE:07:04:3F:2F	Vlan 22-Administe...			stale
DC	192.168.22.13	8C:EC:4B:52:A5:C0	Vlan 22-Administe...	ether5	DESKTOP-SH04TRV	reachable
DC	192.168.22.14	E8:40:F2:58:83:71	Vlan 22-Administe...			stale
D	192.168.22.15	DC:FE:07:14:D2:02	Vlan 22-Administe...			failed
D	192.168.22.16	F8:0D:60:9D:23:83	Vlan 22-Administe...			failed
DC	192.168.22.17	50:E5:49:1F:BC:94	Vlan 22-Administe...	ether5	DESKTOP-K7JG8OL	delay
D	192.168.22.75		Vlan 22-Administe...			failed
D	192.168.22.89		Vlan 22-Administe...			failed
D	192.168.22.128		Vlan 22-Administe...			failed
D	192.168.22.139		Vlan 22-Administe...			failed
D	192.168.22.176		Vlan 22-Administe...			failed
D	192.168.22.237		Vlan 22-Administe...			failed
D	192.168.30.4		Vlan 30-IPD			failed
D	192.168.30.6		Vlan 30-IPD			failed
D	192.168.30.30		Vlan 30-IPD			failed
D	192.168.30.79		Vlan 30-IPD			failed
D	192.168.30.107		Vlan 30-IPD			failed
D	192.168.30.139		Vlan 30-IPD			failed
D	192.168.30.142		Vlan 30-IPD			failed
D	192.168.30.149		Vlan 30-IPD			failed
D	192.168.30.151		Vlan 30-IPD			failed
D	192.168.31.2		Vlan 31-Primary ...			failed
D	192.168.31.13		Vlan 31-Primary ...			failed
D	192.168.31.16		Vlan 31-Primary ...			failed
D	192.168.31.17		Vlan 31-Primary ...			failed
D	192.168.31.18		Vlan 31-Primary ...			failed
D	192.168.31.34		Vlan 31-Primary ...			failed
D	192.168.31.39		Vlan 31-Primary ...			failed
D	192.168.31.61		Vlan 31-Primary ...			failed
D	192.168.31.107		Vlan 31-Primary ...			failed
D	192.168.31.109		Vlan 31-Primary ...			failed
D	192.168.31.122		Vlan 31-Primary ...			failed
D	192.168.31.128		Vlan 31-Primary ...			failed
D	192.168.31.134		Vlan 31-Primary ...			failed
D	192.168.31.138		Vlan 31-Primary ...			failed
D	192.168.31.140		Vlan 31-Primary ...			failed
D	192.168.31.160		Vlan 31-Primary ...			failed
D	192.168.31.184		Vlan 31-Primary ...			failed
D	192.168.31.190		Vlan 31-Primary ...			failed
D	192.168.31.195		Vlan 31-Primary ...			failed
D	192.168.31.204		Vlan 31-Primary ...			failed

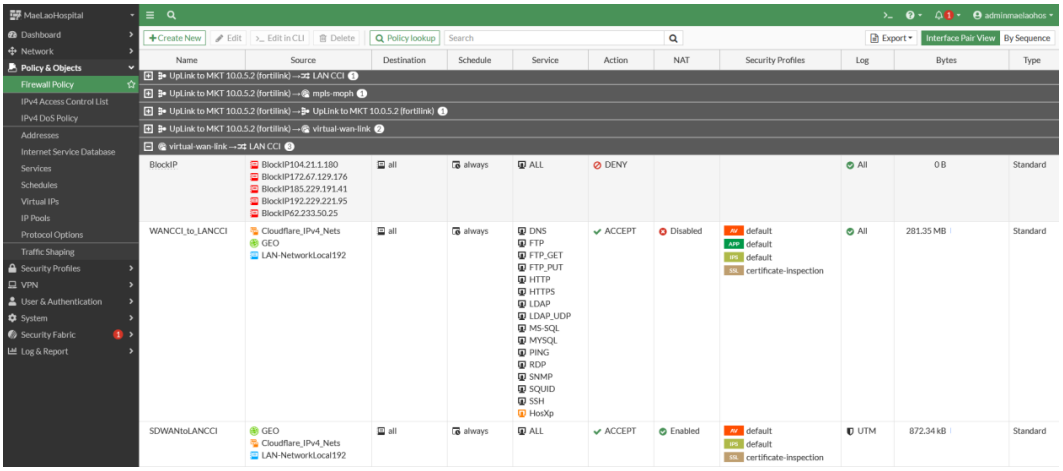
ภาพประกอบ แสดงการแบ่ง VLAN

Admin มีการใช้งาน VPN ในการเข้าถึงเครื่องอุปกรณ์แม่ข่าย (Server) แทนการใช้งานผ่าน Public



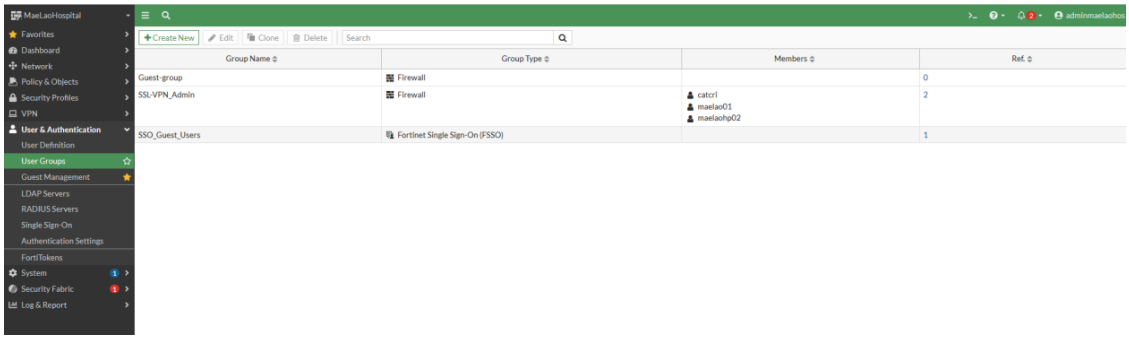
ภาพประกอบ การใช้งาน VPN

มีการ Block การใช้งาน International Traffic กรณีไม่มีความจำเป็นในการใช้งาน

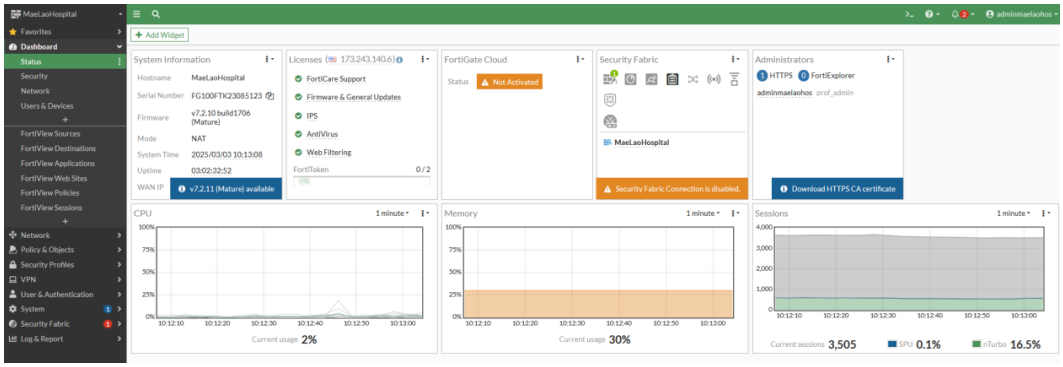


ภาพประกอบ แสดงการตั้งค่า Fire Wall

User Access Accounts กำหนดสิทธิใช้งาน เท่าที่จำเป็น



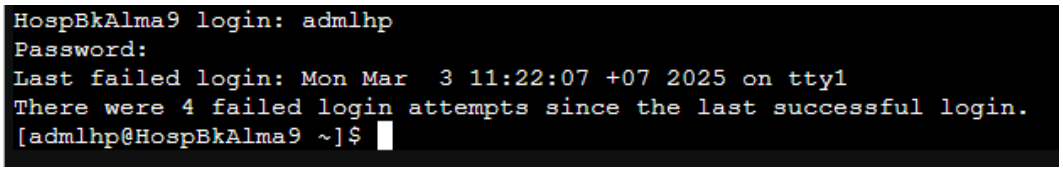
Time Sync



Privileged Access Management (PAM)

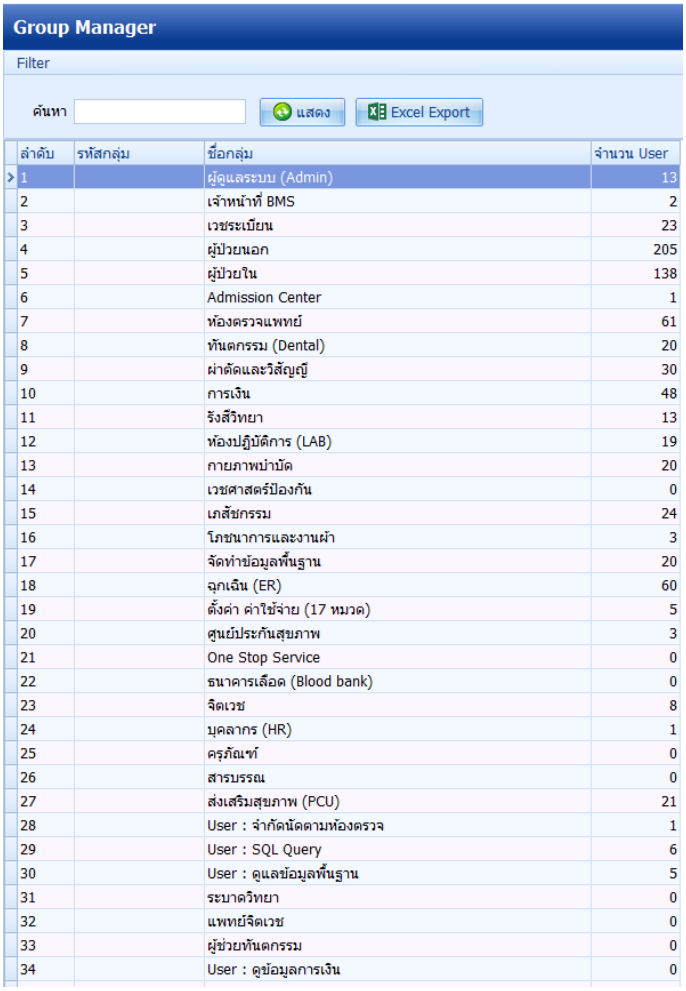
โซลูชันการรักษาความปลอดภัยของข้อมูลประจำตัวที่ช่วยปกป้องค์กรจากภัยคุกคามทางไซเบอร์ ด้วยการติดตาม ตรวจหา และป้องกันการใช้สิทธิ์การเข้าถึงทรัพยากรที่สำคัญในระดับสูง

ดำเนินการ Disable Administrator / Root / Admin บนระบบเพื่อป้องกันการโจมตีในรูปแบบ Brute Force บน OS Server หรือใช้ Private Key เฉพาะ HIS Server



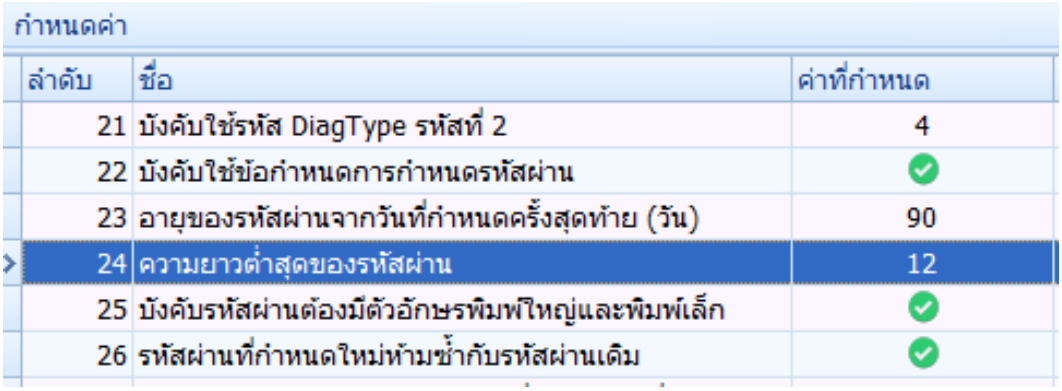
ภาพประกอบ แสดงการตั้งค่า

มีการกำหนด Role-based access ในการเข้าถึงระบบ

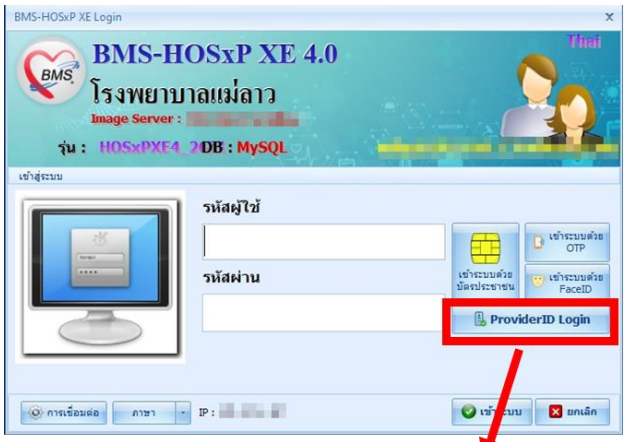


ลำดับ	รหัสกลุ่ม	ชื่อกลุ่ม	จำนวน User
1		ผู้ดูแลระบบ (Admin)	13
2		เจ้าหน้าที่ BMS	2
3		เวชระเบียน	23
4		ผู้ป่วยนอก	205
5		ผู้ป่วยใน	138
6		Admission Center	1
7		ห้องตรวจแพทย์	61
8		ทันตกรรม (Dental)	20
9		ผ่าตัดและวิสัญญี	30
10		การเงิน	48
11		รังสีวิทยา	13
12		ห้องปฏิบัติการ (LAB)	19
13		กายภาพบำบัด	20
14		เวชศาสตร์ป้องกัน	0
15		เภสัชกรรม	24
16		โภชนาการและงานผ้า	3
17		จัดทำข้อมูลพื้นฐาน	20
18		ฉุกเฉิน (ER)	60
19		ตั้งค่า ค่าใช้จ่าย (17 หมวด)	5
20		ศูนย์ประกันสุขภาพ	3
21		One Stop Service	0
22		ธนาคารเลือด (Blood bank)	0
23		จิตเวช	8
24		บุคลากร (HR)	1
25		ครุภัณฑ์	0
26		สารบรรณ	0
27		ส่งเสริมสุขภาพ (PCU)	21
28		User : จำกัดนัดตามห้องตรวจ	1
29		User : SQL Query	6
30		User : ดูแลข้อมูลพื้นฐาน	5
31		ระบาดวิทยา	0
32		แพทย์จิตเวช	0
33		ผู้ช่วยทันตกรรม	0
34		User : ดูข้อมูลการเงิน	0

มีการตั้ง Password ให้ Complex ตามมาตรฐานอย่างน้อย 10 Digit ตัวอักษรใหญ่, เล็ก, อักขระพิเศษ โดยครอบคลุม Operating System (OS) ของระบบ HIS หรือ Software HIS เป็นอย่างน้อย และต้องมีเอกสารแนบอย่างละเอียดให้ชัดเจน

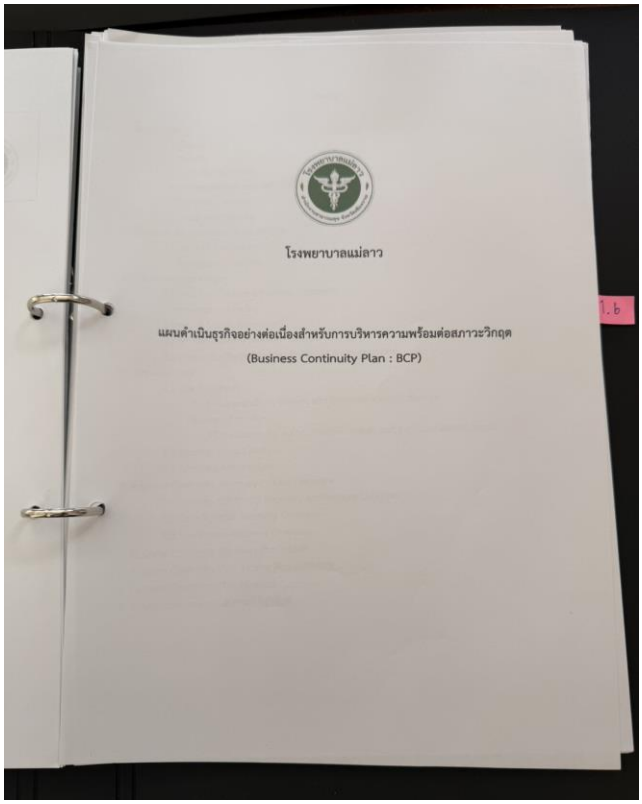


มี 2FA ระบบ HIS



Business Continuity Plan (BCP) Disaster Recovery Plan (DRP)

โรงพยาบาลแม่ลาวมีการจัดทำแผนดำเนินการธุรกิจต่อเนื่องสำหรับการบริหารความพร้อมต่อสภาวะวิกฤตทั้งในรูปแบบไฟล์เอกสารและทำเป็นรูปเล่ม



แผนดำเนินธุรกิจอย่างต่อเนื่องสำหรับการบริหารความพร้อมต่อสภาวะวิกฤต
(Business Continuity Plan : BCP)

1. Introduction

1.1 Title of Plan

แผน BCP ฉบับนี้จัดทำขึ้นเพื่อให้โรงพยาบาลแม่ลาว สามารถดำเนินธุรกิจด้านการบริการประชาชน ได้อย่างต่อเนื่อง แม้เกิดเหตุการณ์ฉุกเฉิน เช่น ความล้มเหลวของระบบเครือข่าย, ภัยธรรมชาติ, หรือการโจมตีทางไซเบอร์ โดยมุ่งเน้นการฟื้นฟูกระบวนการ (Recovery) และลดผลกระทบต่อบริการหลักขององค์กร เป็นหลัก อีกทั้งการจัดทำแผนนี้ยังช่วยสร้างความมั่นใจให้กับลูกค้าและผู้มีส่วนได้ส่วนเสียว่าโรงพยาบาลแม่ลาวมีความพร้อมในการรับมือกับสถานการณ์ฉุกเฉินต่าง ๆ ได้อย่างมีประสิทธิภาพและรวดเร็วมากแค่ไหน

การดำเนินงานตามแผนนี้เน้นการวิเคราะห์ความเสี่ยง (Risk Analysis) การเตรียมความพร้อมของทรัพยากร (Resource Preparation) และกระบวนการฟื้นฟู (Recovery) รวมถึงกระบวนการที่สำคัญภายใต้กรอบเวลาที่กำหนด เพื่อให้มั่นใจว่าองค์กรสามารถกลับมาดำเนินงานตามปกติได้ในเวลาอันรวดเร็วที่สุด

1.2 Purpose

1. วัตถุประสงค์

1. เพื่อรับประกันความต่อเนื่องของบริการแอปพลิเคชั่นหลัก ที่สำคัญ เช่น HOSxPXEผ่ซึ่งเป็นส่วนสำคัญหลักขององค์กร
2. ลดผลกระทบที่อาจเกิดขึ้นกับข้อมูลและโครงสร้างพื้นฐานในกรณีฉุกเฉิน
3. ฟื้นฟูกระบวนการดำเนินงานให้กลับมาทำงานได้ภายในเวลาที่กำหนด เพื่อไม่ให้ส่งผลกระทบต่อภาพลักษณ์ขององค์กร
4. สร้างความเชื่อมั่นให้แก่ลูกค้าและผู้มีส่วนได้ส่วนเสีย โดยแสดงถึงความสามารถในการจัดการกับเหตุการณ์วิกฤติ
5. ส่งเสริมการบริหารจัดการที่โปร่งใสและเป็นระบบในช่วงเวลาฉุกเฉิน รวมถึงการรายงานความคืบหน้าแก่ฝ่ายบริหารและผู้เกี่ยวข้อง
6. ส่งเสริมการฝึกซ้อมและการปรับปรุงแผนอย่างต่อเนื่อง เพื่อให้แผนมีความเหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลง

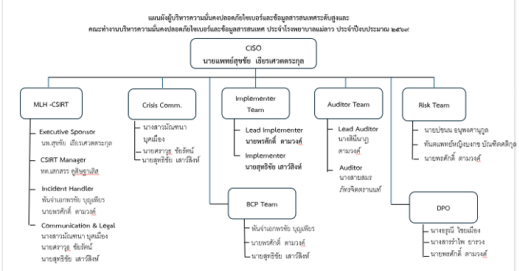
2. ขอบเขต

แผนดำเนินธุรกิจอย่างต่อเนื่องฯ (BCP) ฉบับนี้ ใช้สำหรับเป็นแนวทางในการปฏิบัติ กรณีเกิดสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน เหตุการณ์ที่มีผลกระทบต่อกิจกรรมหลักของโรงพยาบาลแม่ลา ซึ่งประกอบด้วยเหตุการณ์ต่อไปนี้

3. ความรับผิดชอบ

1. หัวหน้า IT Support (IT Manager/ISMS/CSMR) : รับผิดชอบในการกำกับดูแลและตรวจสอบการดำเนินงานตามแผน BCM (Business Continuity Management) โดยใช้มีมตอบสนองในการทำงาน
2. ทีม IT Support : รับผิดชอบในการดำเนินการตามแผน BCM (Business Continuity Management) และประสานงานกับหน่วยงานต่างๆ
3. ผู้ใช้ : ปฏิบัติตามแนวทางและขั้นตอนที่กำหนดในแผน BCM (Business Continuity Management)

BCM Organization Chart



BCM - Business Continuity Management Team

ให้ใส่ชื่อผู้ที่เกี่ยวข้องทั้งหมด มาวางใส่ในตาราง เพื่อชี้นระบบใหม่ ให้ไวที่สุด

No	Name	Position	Department	Tel / Mobile Phone
1	นพ.สุชชัย เอียรเศวตตระกูล	CISO	Management	053-603100 ต่อ 2014
2	ทต.เสกสรร คูตินธุวาเสิศ	CSIRT Manager	CSIRT Manager	053-603100 ต่อ 3116
3	พันจ่าเอกพรชัย บุญเพียร	Incident Handler	Incident Handler	053-603100 ต่อ 2015
4	น.ส มัณฑนา บุศเมือง	Communication & Crisis Comm	Communication & Crisis Comm	053-603100 ต่อ 3114
5	นายศราวุธ ชัยรัตน์	Communication & Crisis Comm	Communication & Crisis Comm	053-603100 ต่อ 3144
6	นางอรุณี ไชยเมือง	DPO	DPO	053-603100 ต่อ 3102
7	นางสาวรำไพ ยารวง	DPO	DPO	053-603100 ต่อ 3144
8	นายพรศักดิ์ ตามวงศ์	หัวหน้า IT Support	IT Support	081-4733415
9	นายสุทธิชัย เสาร์สิงห์	เจ้าหน้าที่ IT Support	IT Support	061-3061590
10	ภก.ปชนน อนุพงศานุกูล	Risk Team	Risk Team	053-603100 ต่อ 3115
11	ทต.ญ บงกช บัณฑิตศิกุล	Risk Team	Risk Team	053-603100 ต่อ 3116

1.3 Executive Summary

1.4 Documentation and References (เอกสารประกอบ)

1. Application and vendor contact List (แอพพลิเคชั่นและรายชื่อของผู้ให้บริการ พร้อมเบอร์ติดต่อ)
2. Hardware and software inventory (รายการทรัพย์สิน ไม่ว่าจะเป็น ฮาร์ดแวร์และซอฟแวร์)
3. Backup and Restore Manual / Scheduling (เอกสารคู่มือในการติดตั้งระบบ ต่างๆ)

1.5 Document Location (**ที่ตั้งในการเก็บเอกสารต่างๆ**)

แผนนี้ถูกจัดเก็บไว้และจะถูกนำมาใช้จากเวอร์ชั่นที่อยู่ในโฟลเดอร์ "แผนการกู้คืนจากภัยพิบัติ/ความมั่นคงปลอดภัยทางไซเบอร์หรือความมั่นคงปลอดภัยทางด้านข้อมูลสารสนเทศ" ที่อยู่ใน Google Drive และเอกสารที่เป็นต้นฉบับที่ตู้เก็บเอกสารในห้องแผนกไอที **Link : https://drive.google.com/drive/folders/**

1.6 Document Security (**ความปลอดภัยในการจัดเก็บเอกสารต่างๆ**)

แผนนี้เป็นข้อมูลธุรกิจที่ถือว่าเป็นความลับ ออกแบบมาสำหรับกลุ่มงาน IT และกลุ่มงานตรวจสอบที่เหมาะสม เท่านั้น

2. Scope of the business continuity plan

2.1 Users of this Procedure

- BCM Org chart
- CSIRT Org chart (Incident Response Team)
- Crisis Communication Team

2.2 Participating Systems

เอกสารนี้อธิบายการออกแบบที่เหมาะสมต่อการเกิดภัยพิบัติและกิจกรรมการสำรองเพื่อรับมือกับภัยพิบัติ/ความมั่นคงปลอดภัยทางไซเบอร์และความมั่นคงปลอดภัยทางด้านข้อมูลสารสนเทศ สำหรับเซิร์ฟเวอร์ ที่ทาง**โรงพยาบาลแม่ลาว** ได้ใช้พร้อมกับบริการ IT หลักและแอปพลิเคชันหลักสำหรับระบบธุรกิจตามที่ระบุด้านล่างและขั้นตอนระดับสูงที่จำเป็นในการดำเนินการ Fail over ในกรณีที่เกิดภัยพิบัติ/เหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์จริง
ข้างล่างนี้คือ บริการ IT หลักที่รวมอยู่ในแผนนี้ ได้แก่

3. Communications Plan

3.1 Who Can Declare a Business continuity Plan

การประกาศภัยพิบัติ/เหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์และความมั่นคงปลอดภัยทางด้านข้อมูลสารสนเทศดำเนินการโดย**โรงพยาบาลแม่ลาว** หากหัวหน้า IT Support (IT Manager/ISMS/CSMR) ไม่อยู่ สามารถรายงานตรงไปยังตัวแทนหน่วยงานแต่ละแผนก เพื่อทำการตัดสินใจโดยบุคลากรดังต่อไปนี้ จะเป็นผู้ตัดสินใจหลักอย่างต่อเนื่อง

- หัวหน้า IT Support
- เจ้าหน้าที่ IT Support
- หัวหน้า Implement
- เจ้าหน้าที่ Operation

3.2 Emergency Funding

อาจจำเป็นต้องใช้เงินทุนก่อนที่ระบบ Application หลักดังกล่าว จะกลับมาออนไลน์อีกครั้ง ดังนั้นจึงจำเป็นต้องนำเสนองบประมาณที่จำเป็น ต่อคณะผู้บริหารต่อไป

3.3 Key IT Staff & Alternates

โครงสร้างของบุคลากร IT Support มีบทบาทสำคัญในการดำเนินการตามคู่มือแผนความต่อเนื่องทางธุรกิจจะถูกนำมาใช้งานทันทีหลังจากที่มีการประกาศเหตุภัยพิบัติ

- หัวหน้า IT Support (IT Manager/ISMS/CSMR)
  - จุดศูนย์กลางสำหรับการสื่อสารและแผนปฏิบัติการ จัดตารางเวลาและบันทึกเหตุการณ์
  - ตัดสินใจเกี่ยวกับการจัดลำดับความสำคัญและวิธีการกู้คืน สื่อสารกับผู้นำธุรกิจระดับสูง
  - ติดตั้งและกำหนดค่าแอปพลิเคชัน
  - ติดตั้งและกำหนดค่าแอปพลิเคชันบนเว็บเซิร์ฟเวอร์
  - จัดเตรียมเครือข่ายที่เหมาะสม เป็นจุดติดต่อกับผู้ให้บริการเครือข่าย
- เจ้าหน้าที่ IT Support
  - รักษาความปลอดภัยและดำเนินการสร้างฐานของเซิร์ฟเวอร์ เตรียมอุปกรณ์สำหรับการติดตั้งแอปพลิเคชัน- ติดตั้งและกำหนดค่าแอปพลิเคชันบนเว็บเซิร์ฟเวอร์
  - รับผิดชอบด้านการสื่อสารโทรคมนาคมในสถานที่สำรอง
  - รับผิดชอบการดำเนินงานในสถานที่สำรอง
  - รับผิดชอบด้านสิ่งอำนวยความสะดวกในสถานที่สำรอง

Company/Organization Name	Services	Contact Person	Contact Information
บริษัท NT จำกัด	บริการ Internet	call center	Office : 18 อาคาร ทรู ทาวเวอร์ ถนนรัชดาภิเษก แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หจก.เชียงรายเทคโนคอม	บริการด้าน Hard ware	086-420-1849	25 ถนนเรืองนคร ตำบลเวียง อำเภอเมือง จังหวัด เชียงราย 57000

3.5 Customers/Authorities/Media/Press Communications

สำหรับการสื่อสารกับหน่วยงานภายนอก (ลูกค้า, หน่วยงานราชการ, สื่อมวลชน) ควรใช้ขั้นตอนต่อไปนี้ตามแนวทางของ**โรงพยาบาลแม่ลาว** สำหรับการสื่อสารในภาวะวิกฤต (Crisis Communication)

Company name	Contact Person	Contact Information
หัวหน้าทีมดับเพลิง (นายวิชาญ)	083-5772287	
รถดับเพลิงเทศบาลปากก่อดำ		0 5366 6694
รถดับเพลิง อบต.ปากก่อดำ		0 5377 8011
รถดับเพลิงเทศบาลแม่ลาว		0 53729074
สถานีตำรวจภูธรแม่ลาว		0 5377 8191
กฟภ.แม่ลาว		0 5318 3850-1
โรงพยาบาลพาน	06 4086 1450	
สสจ.เชียงราย		0 5391 0300

4. Risk Assessment

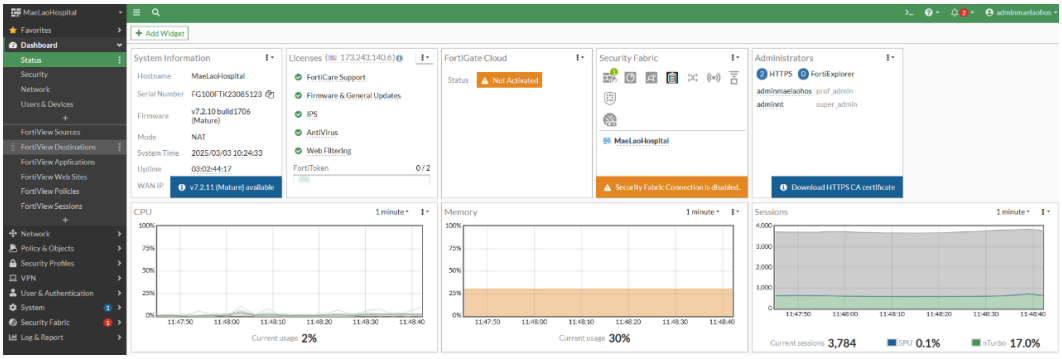
4.1 Risk Definitions

จำนวนภัยพิบัติทางธรรมชาติเกิดเพิ่มขึ้นพร้อมกับผลกระทบที่เกิดขึ้น เนื่องจากการเปลี่ยนแปลงภายนอก เช่น การรวมตัวของประชากรและทรัพย์สินในพื้นที่อันตราย และการขยายตัวของเมืองอย่างรวดเร็ว ภาพด้านล่างแสดงให้เห็นว่า "อันตราย" ตัวอย่างเช่น แผ่นดินไหวที่เกิดขึ้นบนเกาะร้างไม่ก่อให้เกิดภัยพิบัติ เนื่องจากไม่มีประชากร หรือทรัพย์สินที่ได้รับผลกระทบ นอกจากอันตรายแล้ว อาจจะต้องมี "ความเปราะบาง" บางประการต่อปรากฏการณ์ธรรมชาติ เพื่อให้เหตุการณ์นั้นมีอาเป็นภัยพิบัติทางธรรมชาติ "ความเปราะบาง" หมายถึงสภาวะที่เกิดจากปัจจัยหรือกระบวนการทางกายภาพ สังคม เศรษฐกิจ และสิ่งแวดล้อม ซึ่ง

ภาพประกอบ รายละเอียดในเอกสาร

OS Patching การซ่อมแซมจุดบกพร่องของระบบปฏิบัติการ (OS) หรือปรับปรุงระบบปฏิบัติการให้ทันสมัย และเพิ่มเติมความสามารถในการใช้งานหรือประสิทธิภาพให้ดีขึ้น

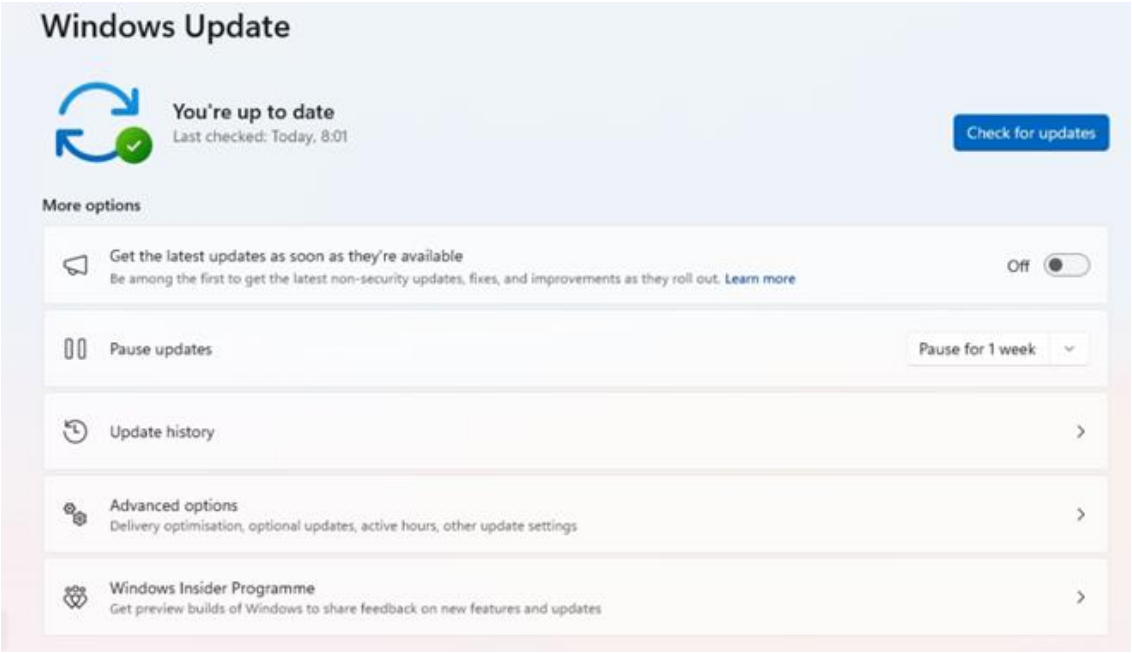
Firewall patching (Firmware)



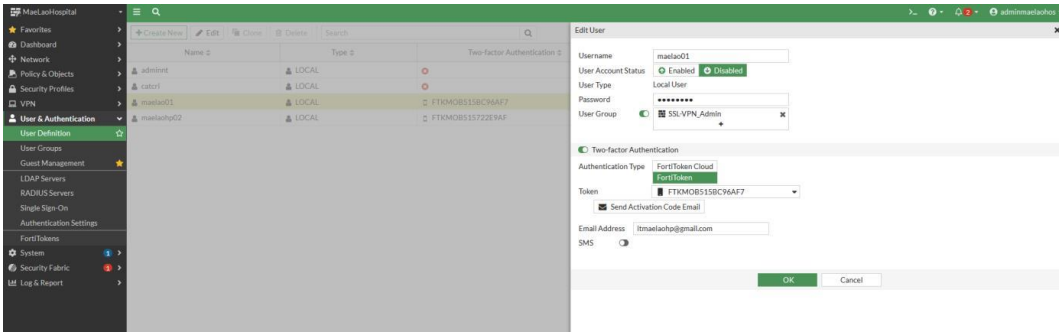
Operation patching

```
[admlhp@HospBkAlma9 ~]$ cat /etc/os-release
NAME="AlmaLinux"
VERSION="9.5 (Teal Serval)"
ID="almalinux"
ID_LIKE="rhel centos fedora"
VERSION_ID="9.5"
PLATFORM_ID="platform:el9"
PRETTY_NAME="AlmaLinux 9.5 (Teal Serval)"
ANSI_COLOR="0;34"
LOGO="fedora-logo-icon"
CPE_NAME="cpe:/o:almalinux:almalinux:9::baseos"
HOME_URL="https://almalinux.org/"
DOCUMENTATION_URL="https://wiki.almalinux.org/"
BUG_REPORT_URL="https://bugs.almalinux.org/"

ALMALINUX_MANTISBT_PROJECT="AlmaLinux-9"
ALMALINUX_MANTISBT_PROJECT_VERSION="9.5"
REDHAT_SUPPORT_PRODUCT="AlmaLinux"
REDHAT_SUPPORT_PRODUCT_VERSION="9.5"
SUPPORT_END=2032-06-01
[admlhp@HospBkAlma9 ~]$
```

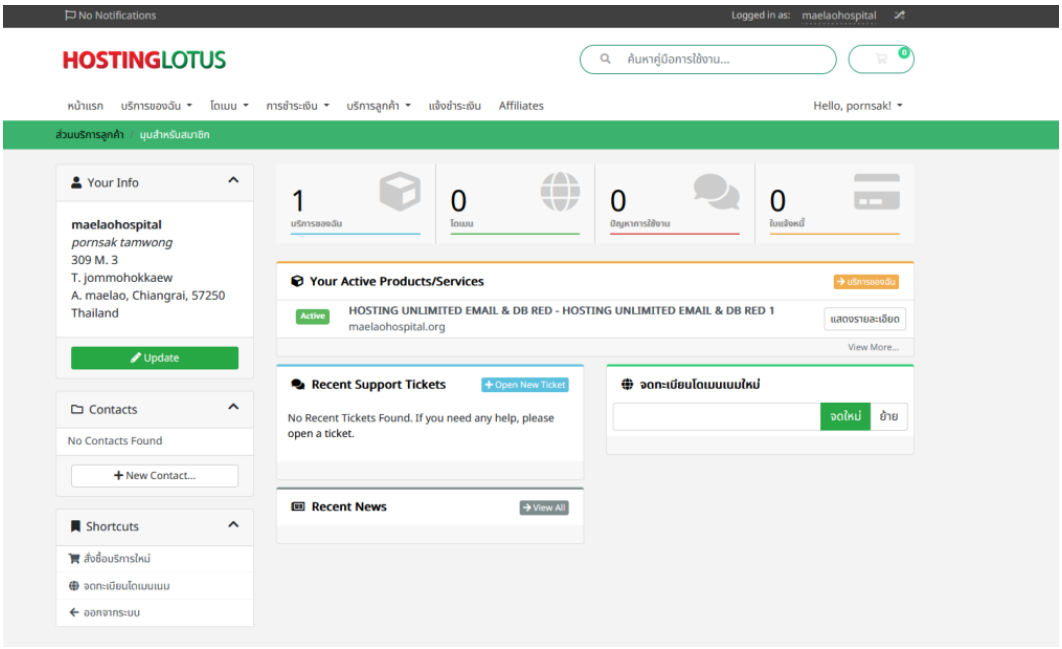


Multi-Factor Authentication (2FA)



Web Application Firewall (WAF)

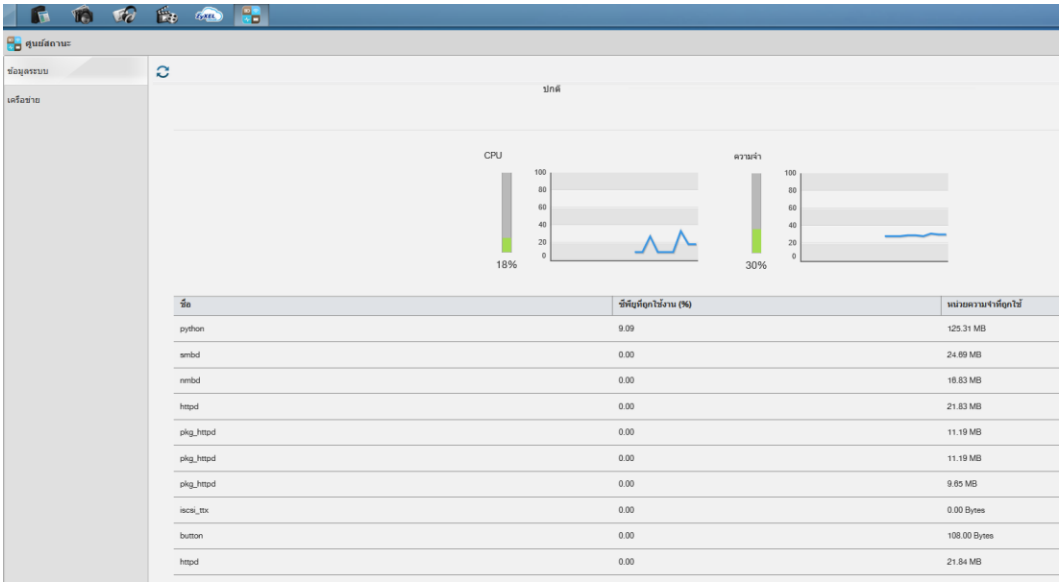
ดำเนินการเช่า Hosting ภายนอกของ Web Hostinglotus

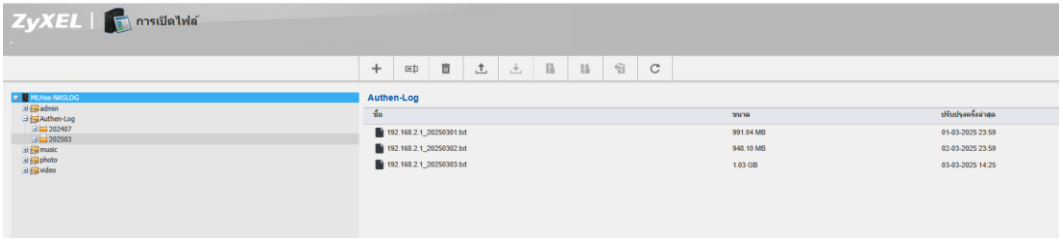


จดโดเมนภายใต้ https://maelaohospital.moph.go.th/

Log Management

มีระบบการจัดเก็บ Log อินเทอร์เน็ต และคอมพิวเตอร์ ตาม พ.ร.บ. คอมฯ อย่างน้อย 90 วัน





Security Information & Event Management (SIEM)

ระบบที่ใช้ในการจัดการกับ Log และ Event ต่างๆ ที่คอยทำหน้าที่วิเคราะห์หาความเชื่อมโยงของ Event ต่างๆ ที่เกี่ยวข้องกับความปลอดภัยทั้งหมดไปจนถึงการ Alert ระบุตำแหน่งของภัยคุกคามให้ทราบ เมื่อมี Event ที่ผิดปกติ ทำให้สามารถป้องกัน และตอบสนองภัยคุกคามได้อย่างรวดเร็ว มีระบบ SIEM หรือระบบวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อนำมาวิเคราะห์พฤติกรรมของ Cyber Attack บนระบบที่ให้บริการ ทั้งระดับ Infrastructure และ Operating System (OS) โดยจะต้องครอบคลุมการตรวจจับพื้นฐาน ดังนี้

• ตรวจจับและแจ้งเตือนการบุกรุกที่เข้าถึงระบบเครือข่ายระบบ และการ Scan port
• (port scanning) พยายาม Brute force Login เข้า
• Malware-Virus Detection ตรวจจับและแจ้งเตือน Malware หรือ Virus จากพฤติกรรมต่างๆ ที่เกิดขึ้นหรือจาก signature
• Blacklist IP การตรวจจับและเตือนการเข้าถึง IP Address ที่เป็น Blacklist และระบุการเปิด connection ได้
• Unauthorized Access การตรวจจับการเข้าถึงข้อมูลหรือระบบที่ไม่ได้รับอนุญาตหรือไม่มีสิทธิ์เข้าถึงระบบ
• DDoS Attack การตรวจจับพฤติกรรมการโจมตีในรูปแบบของ DDoS ได้ ทั้งภายนอกและภายใน
• Data Breaches การตรวจจับและแจ้งเตือนการละเมิดการเข้าถึงข้อมูลที่สำคัญของระบบ ที่ไม่อนุญาตให้เข้าถึง

Vulnerability Assessment (VA Scan)

การตรวจสอบช่องโหว่ของระบบ เพื่อให้ทราบถึงความเสี่ยง จุดอ่อน และระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจากการถูกโจรกรรมข้อมูลและการโจมตีทางไซเบอร์ มีการดำเนินการ Vulnerability Assessment (VA Scan) อย่างน้อยปีละ 1 ครั้ง โดยจะต้องดำเนินการแก้ไข CVE และช่องโหว่ต่างๆ ที่เกิดขึ้น โดยให้ความสำคัญกับความเสี่ยงระดับ Critical, High, Medium, Low เป็นลำดับแรก

1. Review Vulnerability Assessment Report
2. จัดลำดับความสำคัญ ความเสี่ยงระดับ Critical, High, Medium, Low กำหนดระยะเวลาในการแก้ไขช่องโหว่

การจัดการความเสี่ยง

3.1 ยอมรับความเสี่ยง (Risk Acceptance)
3.2 หลีกเลี่ยงความเสี่ยง (Risk Avoidance)
3.3 ลดความเสี่ยง (Risk Mitigation)
3.4 ถ่ายโอนความเสี่ยง (Risk Transfer)

****** ดำเนินการโดย สกมช. ดำเนินการประเมินในเดือน กุมภาพันธ์ 2569 ******