

การกำหนดรอบการสำรองข้อมูล และการทดสอบการกู้คืนข้อมูล รวมถึงป้องกันสื่อบันทึกการสำรองข้อมูลจากความเสียหายและการสูญหาย และการเข้าถึงโดยไม่ได้รับอนุญาต
โรงพยาบาลแม่ลาว 2569

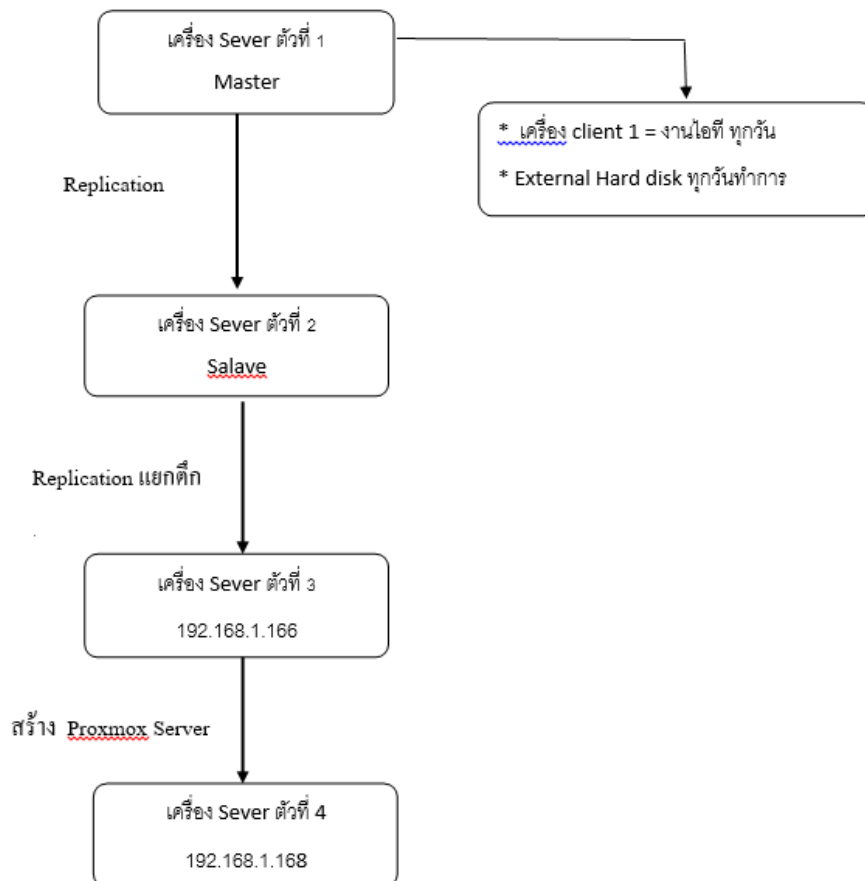
Backup

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

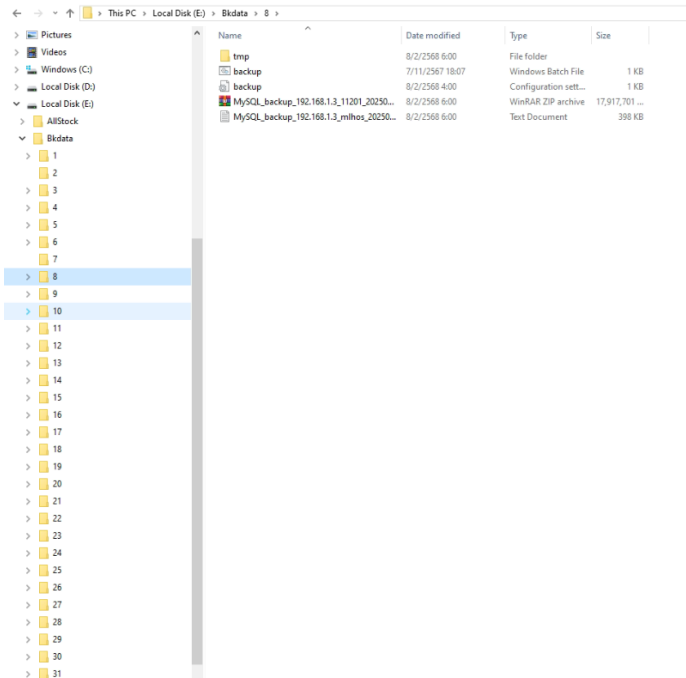
1. สำเนาข้อมูลไว้บนระบบ 3 ชุด

ดำเนินการทำ MySQL Replication แบบ Master-Slave จำนวน 2 ชุด

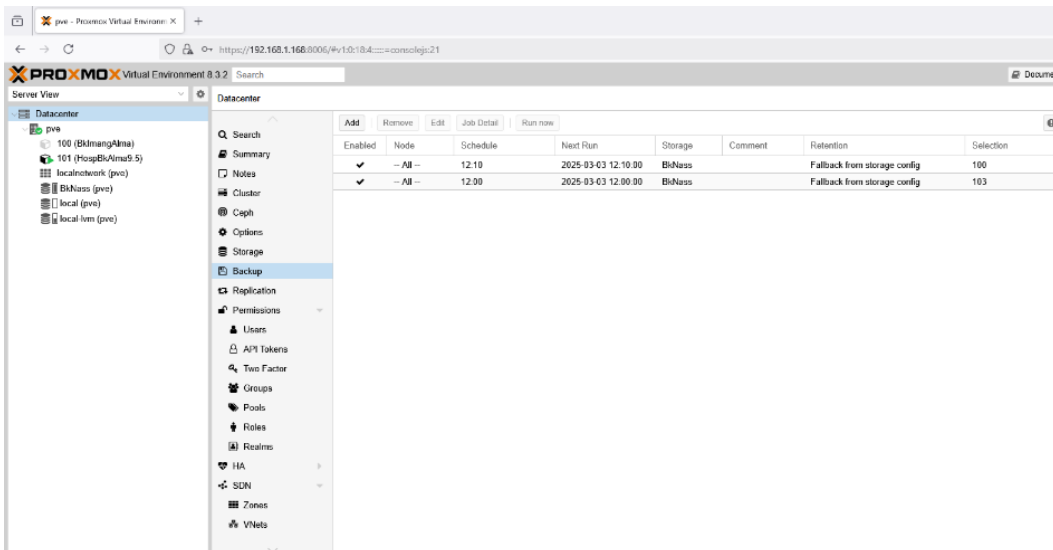
การสำรองข้อมูล



2. สำเนาข้อมูลไว้บนเทคโนโลยีต่างกัน 2 ชุด
HOSxPXE 4 Backup เวลา 01.00 น. ทุกวัน



Proxmox สำรองเวลา 12.00 น. ทุกวัน สำรองออกมาไว้ในเครื่อง SynoMlhp



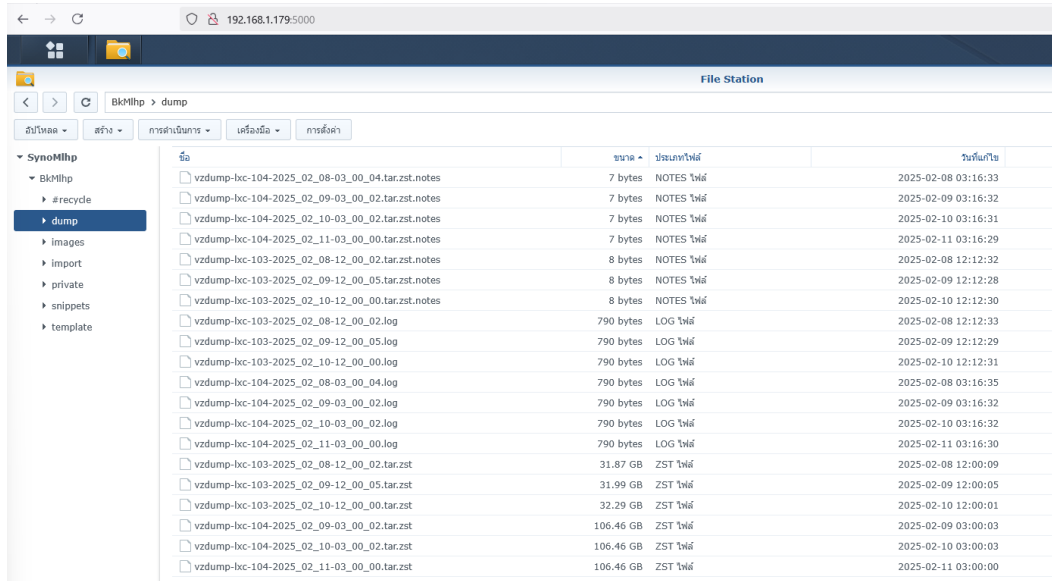
This PC > BKdata (E:) > BkPmmihp >

Name	Date modified	Type	Size
vzdump-lc-101-2024_12_18-03_00.tar.zst	18/12/2567 3:16	WinRAR	112,014,35...
vzdump-lc-104-2025_01_02-03_00_01.tar.zst	2/1/2568 3:00	WinRAR	111,503,03...
vzdump-lc-103-2025_02_10-12_00_00.tar.zst	11/2/2568 9:17	WinRAR	33,856,203 ...
vzdump-lc-100-2024_12_22-12_15_02.tar.zst	22/12/2567 12:26	WinRAR	27,266,166 ...
vzdump-lc-100-2024_12_22-18_00_01.tar.zst	22/12/2567 18:11	WinRAR	27,251,149 ...
vzdump-lc-100-2024_12_22-01_30_01.tar.zst	22/12/2567 1:41	WinRAR	27,248,180 ...
vzdump-lc-100-2024_12_18-12_15_00.tar.zst	18/12/2567 12:26	WinRAR	27,224,250 ...
vzdump-lc-100-2024_12_23-06_00_05.tar.zst	23/12/2567 6:11	WinRAR	27,223,963 ...
vzdump-lc-100-2024_12_23-01_30_05.tar.zst	23/12/2567 1:41	WinRAR	27,217,269 ...
vzdump-lc-100-2024_12_18-01_30_00.tar.zst	18/12/2567 1:41	WinRAR	27,200,416 ...
vzdump-lc-100-2024_12_22-06_00_01.tar.zst	22/12/2567 6:11	WinRAR	27,189,726 ...
vzdump-lc-100-2024_12_18-18_00_00.tar.zst	18/12/2567 18:11	WinRAR	27,186,169 ...
vzdump-lc-100-2024_12_17-01_30_03.tar.zst	17/12/2567 1:41	WinRAR	26,980,067 ...
vzdump-lc-100-2024_12_17-06_00_01.tar.zst	17/12/2567 6:11	WinRAR	26,919,994 ...
vzdump-lc-100-2024_12_16-01_30_03.tar.zst	16/12/2567 1:41	WinRAR	26,787,102 ...
vzdump-lc-100-2024_12_13-01_30_00.tar.zst	13/12/2567 1:40	WinRAR	26,079,910 ...
vzdump-lc-100-2024_12_13-06_00_02.tar.zst	13/12/2567 6:10	WinRAR	26,023,029 ...
vzdump-lc-101-2024_12_22-03_00_01.tar.zst	22/12/2567 3:01	WinRAR	10,481,739 ...
vzdump-lc-101-2024_12_23-03_00_05.tar.zst	23/12/2567 3:01	WinRAR	10,374,534 ...

ทุกวันใช้อุปกรณ์ External Hard Disk (ฮาร์ดดิสก์พกพา) สำรองข้อมูลไว้



ทำการสำรองไว้ในเครื่อง SynoMlhp ตั้งเวลาสำรอง 12.00 น. ทุกวัน



ชื่อ	ขนาด	ประเภทไฟล์	วันที่แก้ไข
vzdump-lxc-104-2025_02_08-03_00_04.tar.zst.notes	7 bytes	NOTES ไฟล์	2025-02-08 03:16:33
vzdump-lxc-104-2025_02_09-03_00_02.tar.zst.notes	7 bytes	NOTES ไฟล์	2025-02-09 03:16:32
vzdump-lxc-104-2025_02_10-03_00_02.tar.zst.notes	7 bytes	NOTES ไฟล์	2025-02-10 03:16:31
vzdump-lxc-104-2025_02_11-03_00_00.tar.zst.notes	7 bytes	NOTES ไฟล์	2025-02-11 03:16:29
vzdump-lxc-103-2025_02_08-12_00_02.tar.zst.notes	8 bytes	NOTES ไฟล์	2025-02-08 12:12:32
vzdump-lxc-103-2025_02_09-12_00_05.tar.zst.notes	8 bytes	NOTES ไฟล์	2025-02-09 12:12:28
vzdump-lxc-103-2025_02_10-12_00_00.tar.zst.notes	8 bytes	NOTES ไฟล์	2025-02-10 12:12:30
vzdump-lxc-103-2025_02_08-12_00_02.log	790 bytes	LOG ไฟล์	2025-02-08 12:12:33
vzdump-lxc-103-2025_02_09-12_00_05.log	790 bytes	LOG ไฟล์	2025-02-09 12:12:29
vzdump-lxc-103-2025_02_10-12_00_00.log	790 bytes	LOG ไฟล์	2025-02-10 12:12:31
vzdump-lxc-104-2025_02_08-03_00_04.log	790 bytes	LOG ไฟล์	2025-02-08 03:16:35
vzdump-lxc-104-2025_02_09-03_00_02.log	790 bytes	LOG ไฟล์	2025-02-09 03:16:32
vzdump-lxc-104-2025_02_10-03_00_02.log	790 bytes	LOG ไฟล์	2025-02-10 03:16:32
vzdump-lxc-104-2025_02_11-03_00_00.log	790 bytes	LOG ไฟล์	2025-02-11 03:16:30
vzdump-lxc-103-2025_02_08-12_00_02.tar.zst	31.87 GB	ZST ไฟล์	2025-02-08 12:00:09
vzdump-lxc-103-2025_02_09-12_00_05.tar.zst	31.99 GB	ZST ไฟล์	2025-02-09 12:00:05
vzdump-lxc-103-2025_02_10-12_00_00.tar.zst	32.29 GB	ZST ไฟล์	2025-02-10 12:00:01
vzdump-lxc-104-2025_02_09-03_00_02.tar.zst	106.46 GB	ZST ไฟล์	2025-02-09 03:00:03
vzdump-lxc-104-2025_02_10-03_00_02.tar.zst	106.46 GB	ZST ไฟล์	2025-02-10 03:00:03
vzdump-lxc-104-2025_02_11-03_00_00.tar.zst	106.46 GB	ZST ไฟล์	2025-02-11 03:00:00

Antivirus Software

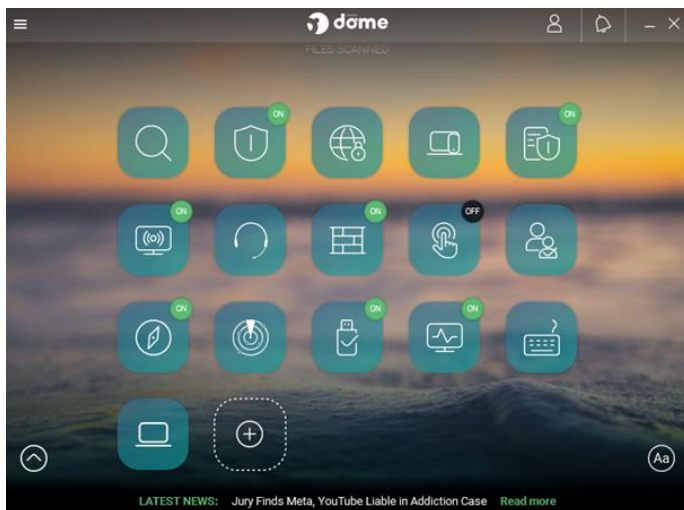
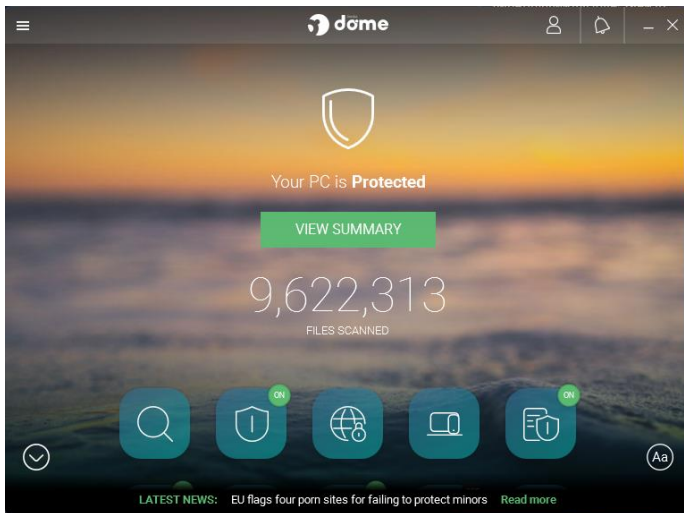
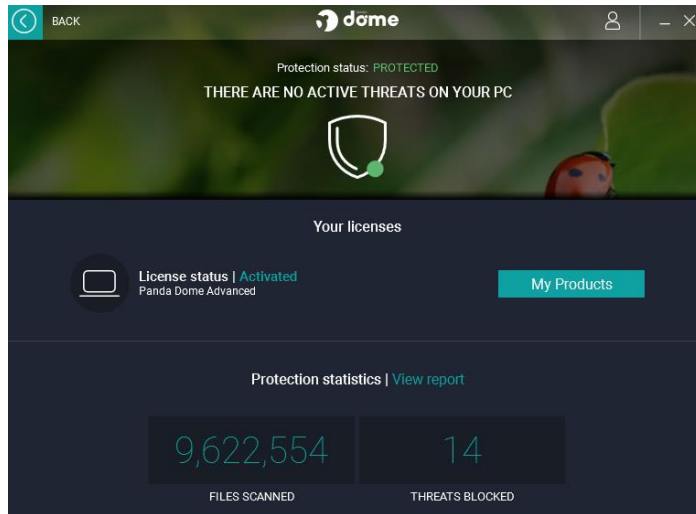
มีการติดตั้ง Next-gen Anti-virus หรือ EDR หรือ XDR ที่เครื่องฝั่ง Server ทุกเครื่อง และอัปเดต Signature ทุกวัน และมีเอกสารแนบระบุ Product และ Version อย่างละเอียดชัดเจน โดย Antivirus จะต้อง Active ตลอดเวลา ในการดำเนินการ Phase 1 จะตรวจสอบติดตั้งเฉพาะกลุ่ม Server ก่อน เท่านั้น โดยครอบคลุม Operating System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

โรงพยาบาลแม่ลาวใช้ซอฟต์แวร์ Antivirus เครื่อง Client มี 2 ตัวด้วยกัน

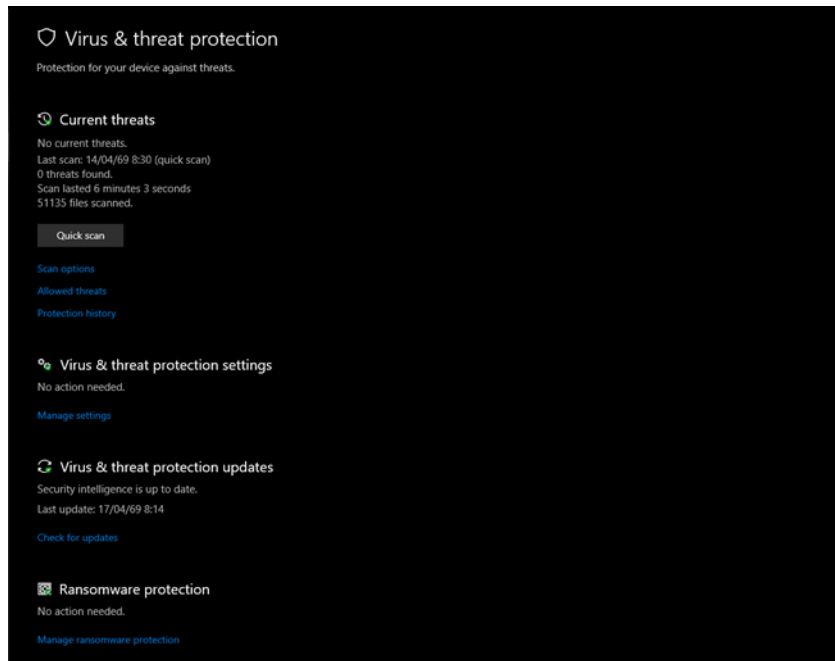
Panda Dome ลิขสิทธิ์แท้ที่มาพร้อมกับเครื่องคอมพิวเตอร์เครื่องเช่า โดยตัว Panda Dome ให้การปกป้องที่ครอบคลุมตั้งแต่ระดับพื้นฐานไปจนถึงระดับสูง โดยเน้นการรักษาความปลอดภัยใน 3 ด้านหลัก

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

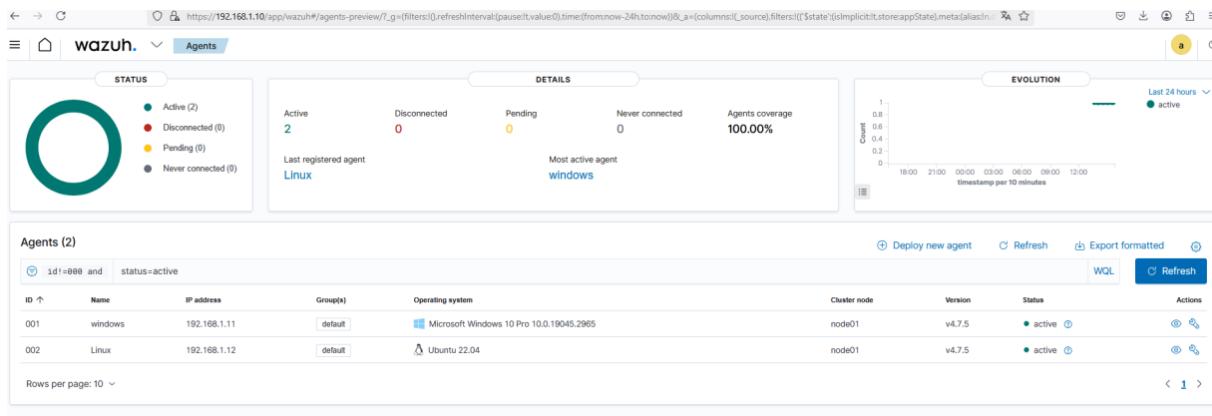
เหมาะสมและติดตามการใช้งานอินเทอร์เน็ตได้ Dark Web Scanner แจ้งเตือนหากพบว่ามีอีเมลหรือข้อมูลบัญชีรั่วไหลบน Dark Web



และโรงพยาบาลแม่ลาวยังใช้ซอฟต์แวร์ Antivirus Microsoft Defender ที่มีอยู่กับระบบปฏิบัติการ Windows License สำหรับเครื่องที่ไม่มีโปรแกรม Antivirus เสริม สำหรับตัว Microsoft Defender ก็สามารถใช้งานปกป้องระบบภัยคุกคามได้ เช่น มัลแวร์ Ransomware การสแกนไฟล์อันตราย ได้ครอบคลุม



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)

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type	
BlockIP	BlockIP104.21.1.180 BlockIP172.67.129.176 BlockIP185.229.191.41 BlockIP192.229.221.95 BlockIP62.233.50.25	all	always	ALL	DENY				All	0 B	Standard
WANCLto_LANCCI	Cloudflare_IPv4_Nets GEO LAN-NetworkLocal192	all	always	DNS FTP FTP_GET FTP_PUT HTTP HTTPS LDAP LDAP_UDP MS-SQL MYSQL PING RDP SNMP SQUID SSH HostXp	ACCEPT	Disabled	default		All	35.28 MB	Standard
SOWANtoLANCCI	GEO Cloudflare_IPv4_Nets LAN-NetworkLocal192	all	always	ALL	ACCEPT	Enabled	default		UTM	92.00 kB	Standard

มีการแบ่งโซน Network ระหว่างอุปกรณ์แม่ข่าย (Server) และ อุปกรณ์ลูกข่าย (Client)

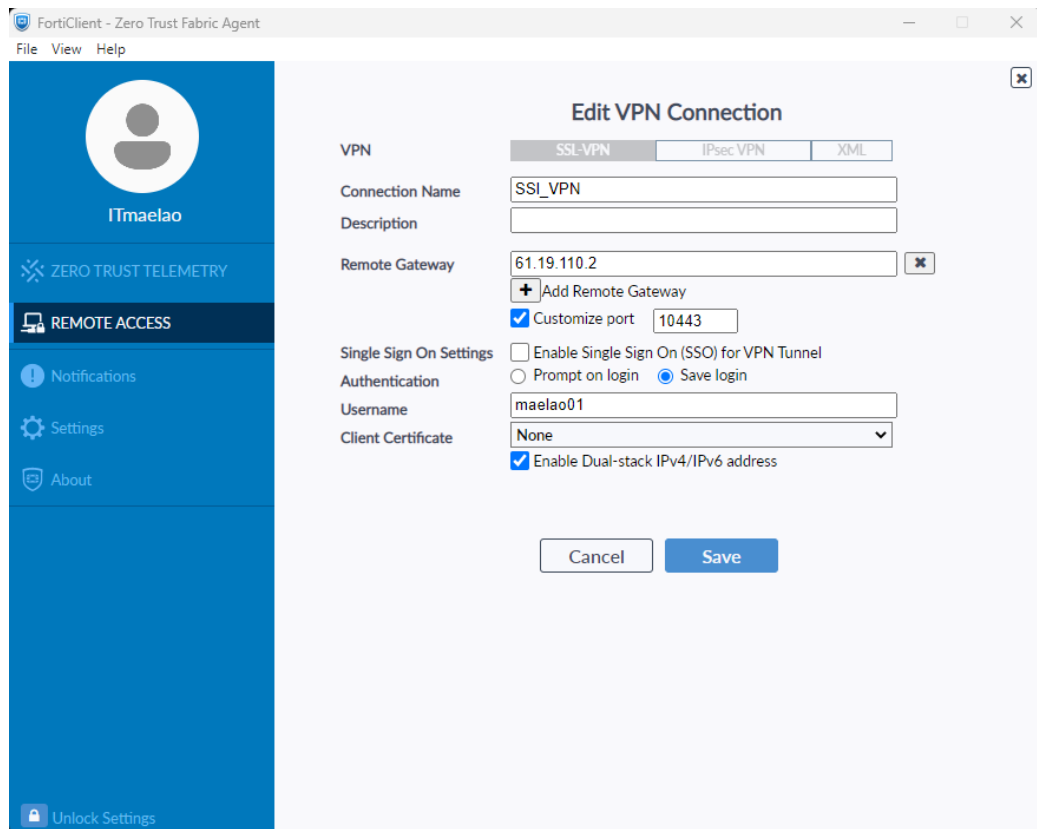
แบ่ง 2 VLAN อย่างน้อย Server client

Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges	Ref
802.3ad Aggregate	802.3ad Aggregate	port5 port6	10.0.5.1/255.255.255.252		PING HTTPS			19
ha2	Physical Interface		0.0.0.0/0.0.0.0					0
mgmt	Physical Interface		192.168.1.99/255.255.255.0		PING HTTPS SSH		192.168.1.110-192.168.1.210	1
NASLOG (port7)	Physical Interface		192.168.21.255.255.255.0		PING HTTPS HTTP			0
port13	Physical Interface		0.0.0.0/0.0.0.0					0
port14	Physical Interface		0.0.0.0/0.0.0.0					0
port15	Physical Interface		0.0.0.0/0.0.0.0					0
port16	Physical Interface		0.0.0.0/0.0.0.0					0
port17	Physical Interface		0.0.0.0/0.0.0.0					0
port18	Physical Interface		0.0.0.0/0.0.0.0					0
port19	Physical Interface		0.0.0.0/0.0.0.0					1
port20	Physical Interface		0.0.0.0/0.0.0.0					1
WAN1CC1 60M/4Mbps (wan1)	Physical Interface		61.19.110.2/255.255.255.252		PING HTTPS			3
WAN2 C Internet 1G/1Gb (wan2)	Physical Interface		134.236.89.204/255.255.255.255		PING HTTPS			2
WAN3 NT2 Fts (dmz)	Physical Interface		100.96.159.149/255.255.255.255		PING HTTPS			2
WAN4 MPLS MORPH (port1)	Physical Interface		200.157.215.42/255.255.255.248		PING HTTPS			1

ARP List						
	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

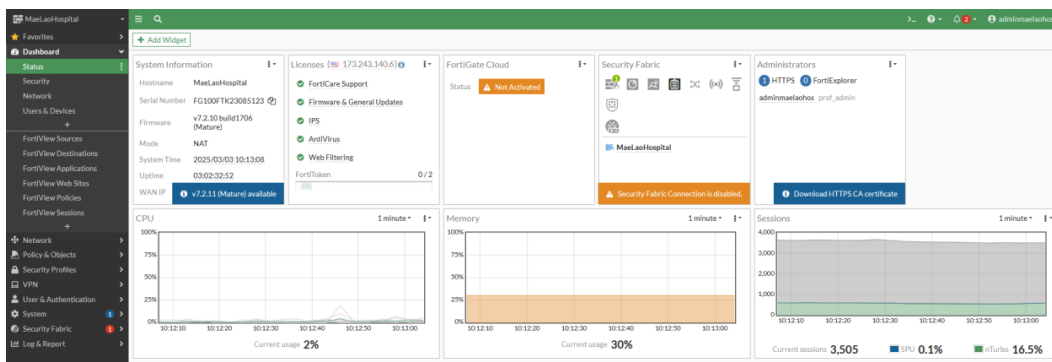
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type
BlockIP	BlockIP104.211.190 BlockIP172.67.129.176 BlockIP185.229.191.41 BlockIP192.229.221.95 BlockIP62.233.50.25	all	always	ALL	DENY			All	0B	Standard
WANCCI_to_LANCCI	Cloudflare_IPv4_Nets GEO LAN-NetworkLocal192	all	always	DNS FTP FTP_GET FTP_PUT HTTP HTTPS LDAP LDAP_LUDP MS-SQL MYSQL PING RDP SNMP SQUID SSH HostXp	ACCEPT	Disabled	default default certificate-inspection	All	281.35 MB	Standard
SDWANtoLANCCI	GEO Cloudflare_IPv4_Nets LAN-NetworkLocal192	all	always	ALL	ACCEPT	Enabled	default default certificate-inspection	UTM	872.34 kB	Standard

ภาพประกอบ แสดงการตั้งค่า Fire Wall

User Access Accounts กำหนดสิทธิ์ใช้งาน เท่าที่จำเป็น

Group Name	Group Type	Members	Ref
Guest-group	Firewall		0
SSL_VPN_Admin	Firewall	cator1 maelao01 maelao02	2
SSO_Guest_Users	Fortinet Single Sign-On (SSO)		1

Time Sync



Privileged Access Management (PAM)

โซลูชันการรักษาความปลอดภัยของข้อมูลประจำตัวที่ช่วยปกป้ององค์กรจากภัยคุกคามทางไซเบอร์ ด้วยการติดตาม ตรวจสอบ และป้องกันการใช้สิทธิ์การเข้าถึงทรัพยากรที่สำคัญในระดับสูง

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

```
HospBkAlma9 login: admlhp
Password:
Last failed login: Mon Mar 3 11:22:07 +07 2025 on tty1
There were 4 failed login attempts since the last successful login.
[admlhp@HospBkAlma9 ~]$
```

ภาพประกอบ แสดงการตั้งค่า

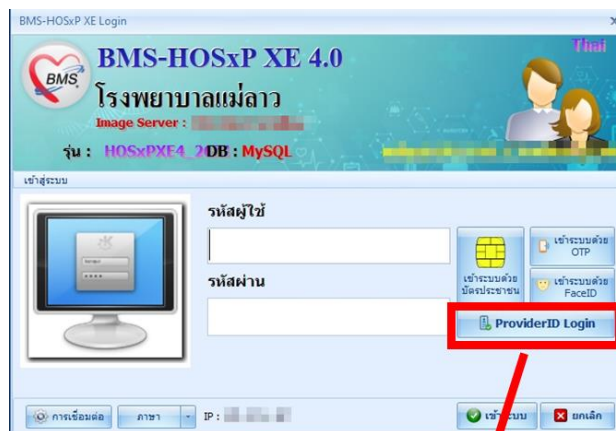
มีการกำหนด Role-based access ในการเข้าถึงระบบ

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 : จำกัดติดตามห้องตรวจ	1
29		User : SQL Query	6
30		User : ดูแลข้อมูลพื้นฐาน	5
31		ระบาดวิทยา	0
32		แพทย์จิตเวช	0
33		ผู้ช่วยทันตกรรม	0
34		User : ดูแลข้อมูลการเงิน	0

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

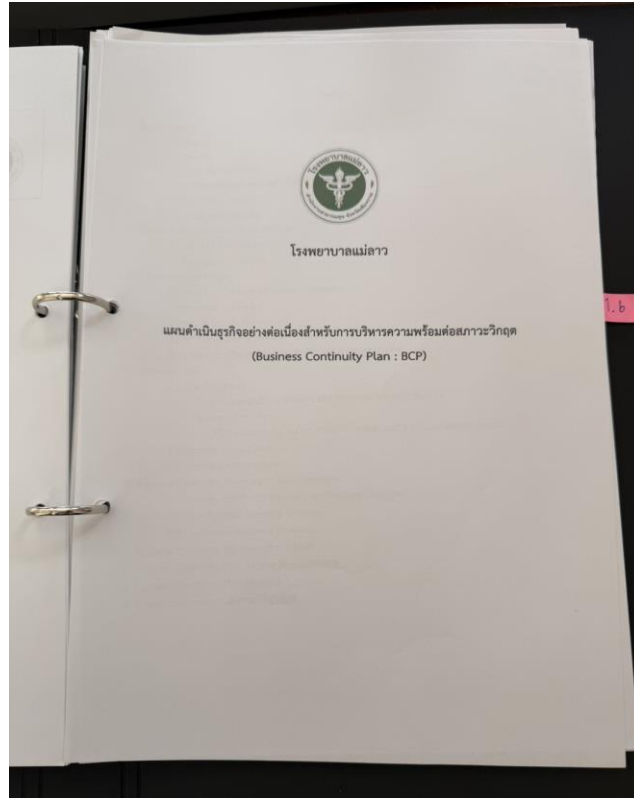
กำหนดค่า		
ลำดับ	ชื่อ	ค่าที่กำหนด
21	บังคับใช้รหัส DiagType รหัสที่ 2	4
22	บังคับใช้ข้อกำหนดการกำหนดรหัสผ่าน	✓
23	อายุของรหัสผ่านจากวันที่กำหนดครั้งสุดท้าย (วัน)	90
> 24	ความยาวต่ำสุดของรหัสผ่าน	12
25	บังคับรหัสผ่านต้องมีตัวอักษรพิมพ์ใหญ่และพิมพ์เล็ก	✓
26	รหัสผ่านที่กำหนดใหม่ห้ามซ้ำกับรหัสผ่านเดิม	✓

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 อีกทั้งการจัดทำแผนนี้ ยังช่วยสร้างความมั่นใจให้กับลูกค้าและผู้มีส่วนได้ส่วนเสียว่าโรงพยาบาลแม่ลาวมีความพร้อมในการรับมือกับสถานการณ์ฉุกเฉินต่าง ๆ ได้อย่างมีประสิทธิภาพและรวดเร็วทันเวลา

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

1.2 Purpose

1. วัตถุประสงค์

- เพื่อรับประกันความต่อเนื่องของบริการ ปลอดภัย ที่สำคัญ เช่น HOS&PCD ซึ่งเป็นส่วนสำคัญหลักของธุรกิจ
- ลดผลกระทบที่จะเกิดขึ้นกับข้อมูลและโครงสร้างพื้นฐานในกรณีฉุกเฉิน
- ฟื้นฟูกระบวนการดำเนินงานให้กลับมาทำงานได้ตามเวลาที่กำหนด เพื่อให้ไม่ส่งผลกระทบต่อภาพลักษณ์ขององค์กร
- สร้างทราเวลเชื่อมให้แก่ลูกค้าและผู้มีส่วนได้ส่วนเสีย โดยแสดงถึงความสามารถในการจัดการกับเหตุการณ์วิกฤติ
- ส่งเสริมการบริหารจัดการที่โปร่งใสและเป็นระบบในช่วงเวลาฉุกเฉิน รวมถึงการรายงานความคืบหน้าแก่ผู้บริหารและผู้เกี่ยวข้อง
- ส่งเสริมการมีชื่อเสียงและการปรับปรุงแผนอย่างต่อเนื่อง เพื่อให้แผนมีความเหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลง

2. ขอบเขต

แผนดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ฉบับนี้ ใช้สำหรับเป็นแนวทางในการปฏิบัติ กรณีเกิดสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน เหตุการณ์ที่มีผลกระทบต่อกิจกรรมหลักของโรงพยาบาลแม่ลาว ซึ่งประกอบด้วยเหตุการณ์ดังต่อไปนี้

3. ความรับผิดชอบ

- หัวหน้า IT Support (IT Manager/SMS/CSMR) : รับผิดชอบในการกำกับดูแลและตรวจสอบการดำเนินงานตามแผน BCM (Business Continuity Management) โดยใช้เมตริกของการทำงาน
- ทีม IT Support : รับผิดชอบในการดำเนินการตามแผน BCM (Business Continuity Management) และประสานงานกับหน่วยงานต่างๆ
- ผู้ชี้ : ปฏิบัติตามแนวทางและขั้นตอนที่กำหนดในแผน BCM (Business Continuity Management)

BCM Organization Chart



BCM - Business Continuity Management Team

ไฟล์ชื่อที่เกี่ยวข้องทั้งหมด มรวาไว้ในตาราง เพื่อขึ้นระบบใหม่ ให้ไว้ที่ดู

No	Name	Position	Department	Tel / Mobile Phone
1	นพ.สุชัย เข็มเสวตรตระกูล	CISO	Management	053-603100 ต่อ 2014
2	ทศ.เสกสรร <u>คุณวุฒิ</u> <u>เชิด</u>	CSIRT Manager	CSIRT Manager	053-603100 ต่อ 3116
3	พันจ่าเอกพรชัย บุญพิพิธ	Incident Handler	Incident Handler	053-603100 ต่อ 2015
4	น.ส. มณฑนา บุคเมือง	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	นางสาวรพีไท ขาววง	DPO	DPO	053-603100 ต่อ 3144
8	นายพทิต์ ตามวสุ	หัวหน้า IT Support	IT Support	081-4733415
9	นายสุชัย เสาร์สิงห์	เจ้าหน้าที่ IT Support	IT Support	061-3061590
10	ภก.ปชมน อุบลกาญจน์	Risk Team	Risk Team	053-603100 ต่อ 3115
11	ท.พญ. บงกช บัณฑิตศิลป์	Risk Team	Risk Team	053-603100 ต่อ 3116

1.3 Executive Summary

3. Communications Plan

3.1 Who Can Declare a Business continuity Plan

การประกาศใช้แผน/เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์และความมั่นคงปลอดภัยทางข้อมูลสารสนเทศในการโดย**โรงพยาบาลเม็ลลาร์** หากหัวหน้า IT Support (IT Manager/SMS/CSMR) ไม่อยู่ สามารถรายงานตรงไปยังหัวหน้าหน่วยงานแต่ละแผนก เพื่อทำการตัดสินใจโดยบุคลากรดังต่อไปนี้ จะเป็นผู้ตัดสินใจหลักอย่างต่อนี้

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

3.2 Emergency Funding

อาจจำเป็นต้องใช้เงินทุนก่อนที่ระบบ Application ทั่วทั้งกล่าว จะกลับมาออนไลน์อีกครั้ง ดังนั้นจึงจำเป็นต้องนำเสนองบประมาณที่จำเป็น ต่อคณะกรรมการต่อไป

3.3 Key IT Staff & Alternates

โครงสร้างของบุคลากร IT Support มีบทบาทสำคัญในการดำเนินการตามคู่มือแผนความต่อเนื่องทางธุรกิจ จะถูกนำมาใช้ทันทีหลังจากที่มีการประกาศเหตุภัยพิบัติ

- หัวหน้า IT Support (IT Manager/SMS/CSMR)
 - จุดศูนย์กลางสำหรับการสื่อสารและแผนปฏิบัติการ จัดตารางเวลาและบันทึกเหตุการณ์
 - ติดตามเกี่ยวกับกรจัดการกับความสำคัญและวิธีการกู้คืน สื่อสารกับผู้นำธุรกิจระดับสูง
 - ติดตั้งและกำหนดค่าแอปพลิเคชัน
 - ติดตั้งและกำหนดค่าแอปพลิเคชันบนเวิร์กสเตชัน
 - จัดเตรียมเครือข่ายที่เหมาะสม เป็นจุดติดต่อกับผู้บริหารเครือข่าย
- เจ้าหน้าที่ IT Support
 - รักษาความปลอดภัยและดำเนินการสร้างฐานของ**ซีรียัลไฟวอลล์** เเยื่อมูลปรแกรมสำหรับการติดตั้งแอปพลิเคชัน ติดตั้งและกำหนดค่าแอปพลิเคชันบนเวิร์กสเตชัน
 - รับผิดชอบด้านการสื่อสารโทรคมนาคมในสถานที่สำรอง
 - รับผิดชอบด้านดำเนินการในสถานที่สำรอง
 - รับผิดชอบด้านที่อำนวยความสะดวกในสถานที่สำรอง

ภาพประกอบ รายละเอียดในเอกสาร

1.4 Documentation and References (เอกสารประกอบ)

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

1.5 Document Location (ที่ตั้งในการเก็บเอกสารต่างๆ)

แนบนี้ถูกจัดเก็บไว้ในและจะถูกนำมาใช้จาก**เซิร์ฟเวอร์**ที่อยู่ในโฟลเดอร์ "แผนการกู้คืนจากภัยพิบัติ/ความมั่นคงปลอดภัยทางไซเบอร์หรือความมั่นคงปลอดภัยทางข้อมูลสารสนเทศ" ที่อยู่ใน Google Drive และเอกสารที่เป็นต้นฉบับที่ผู้ถือเอกสารในห้องแม่ข่าย Link : <https://drive.google.com/drive/folders/>

1.6 Document Security (ความปลอดภัยในการจัดเก็บเอกสารต่างๆ)

แนบนี้เป็นข้อมูลธุรกิจที่ถือว่าเป็นความลับ 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

เอกสารนี้ถือเป็นการออกแบบที่เฉพาะสอดคล้องกับวิถีปฏิบัติและกิจกรรมการสำรองเพื่อรับมือกับภัยพิบัติ/ความมั่นคงปลอดภัยทางไซเบอร์และความมั่นคงปลอดภัยทางข้อมูลสารสนเทศ สำหรับ**บริษัทเม็ลลาร์** ที่ทาง**โรงพยาบาลเม็ลลาร์** ได้ใช้ร่วมกับบริการ IT หลักและแอปพลิเคชันหลักสำหรับระบบธุรกิจตามระดับต้นล่างและขั้นตอนระดับสูงที่จำเป็นในการดำเนินการ Fail over ในกรณีที่เกิดภัยพิบัติ/เหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์จริง

ข้างล่างนี้คือ บริการ IT หลักที่รวมอยู่ในแนบนี้ ได้แก่

Company/Organization Name	Services	Contact Person	Contact Information
บริษัท NT จำกัด	บริการ Internet	call center	Office : 18 อาคาร รุท ทาง 1001 ถนนวิภาวดีเอก แขวงหัวขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หจก.เซียงรายเทคโนโลยีคอม	บริการด้าน Hard ware	086-420-1849	25 ถนนเรืองนคร ตำบลเอื้อง อำเภอมือง จังหวัด เชียงราย 57000

3.5 Customers/Authorities/Media/Press Communications

สำหรับการสื่อสารกับหน่วยงานภายนอก (ลูกค้า, หน่วยงานราชการ, สื่อมวลชน) ควรใช้ขั้นตอนต่อไปนี้ ตามแนวทางของ**โรงพยาบาลเม็ลลาร์** สำหรับการสื่อสารในภาวะวิกฤต (Crisis Communication)

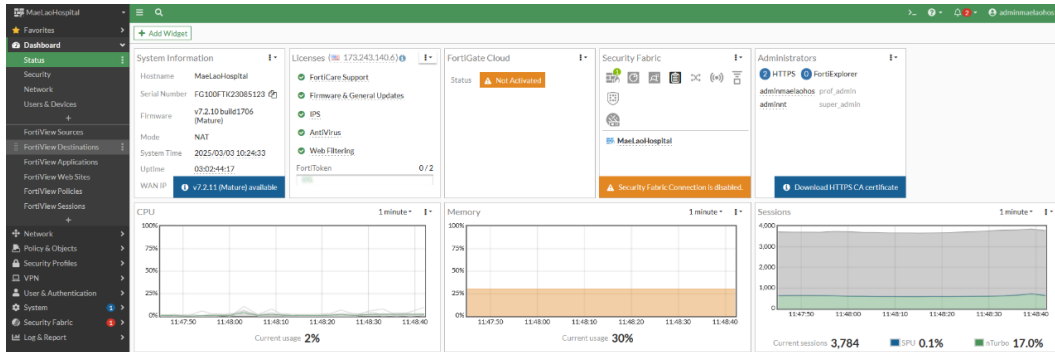
Company name	Contact Person	Contact Information
หัวหน้าทีมแพทย์ (นายวิชาญ)	083-5772287	
รศ.ศัลยแพทย์ศัลยกรรมกระดูก		0 5366 6694
รศ.ศัลยแพทย์ศัลยกรรมกระดูก		0 5377 8011
รศ.ศัลยแพทย์ศัลยกรรมกระดูก		0 53729074
สถานีตำรวจอุบลเม็ลลาร์		0 5377 8191
กฟผ.เม็ลลาร์		0 5318 3850-1
โรงพยาบาลพาน	06 4086 1450	
สสจ. เชียงราย		0 5391 0300

4. Risk Assessment

4.1 Risk Definitions

จำนวนภัยพิบัติทางธรรมชาติเกิดขึ้นเพิ่มขึ้นพร้อมกับผลกระทบที่เกิดขึ้น เนื่องจากกาเปลี่ยนแปลงภายนอก เช่น การรวมตัวของประชากรและทรัพย์สินในพื้นที่อันตราย และการขยายตัวของเมืองอย่างรวดเร็ว ภัยด้านสิ่งแวดล้อมให้ชื่อว่า "อันตราย" ตัวอย่างเช่น แผ่นดินไหวที่ระดับความเร่งไม่ก่อให้เกิดภัยพิบัติ เนื่องจากไม่มีประชากร หรือทรัพย์สินที่ได้รับผลกระทบ นอกจากอันตรายแล้ว อาจจะมี "ความเปราะบาง" บางประการต่อปรากฏการณ์ธรรมชาติ เพื่อให้เหตุการณ์นั้นถือเป็นการภัยพิบัติทางธรรมชาติ "ความเปราะบาง" หมายถึงสภาวะที่ลดจากปัจจัยหรือกระบวนการทางกายภาพ สังคม เศรษฐกิจ และสิ่งแวดล้อม ซึ่ง

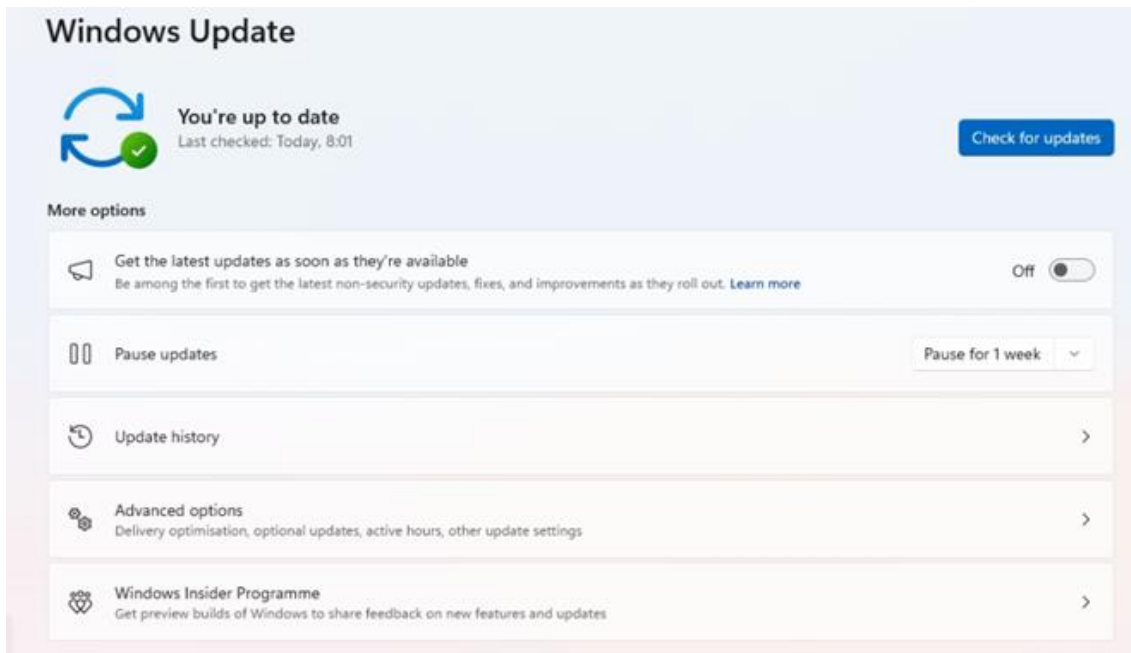
OS Patching การซ่อมแซมจุดบกพร่องของระบบปฏิบัติการ (OS) หรือปรับปรุงระบบปฏิบัติการให้ทันสมัย และเพิ่มเติมความสามารถในการใช้งานหรือประสิทธิภาพให้ดีขึ้น
Firewall patching (Firmware)



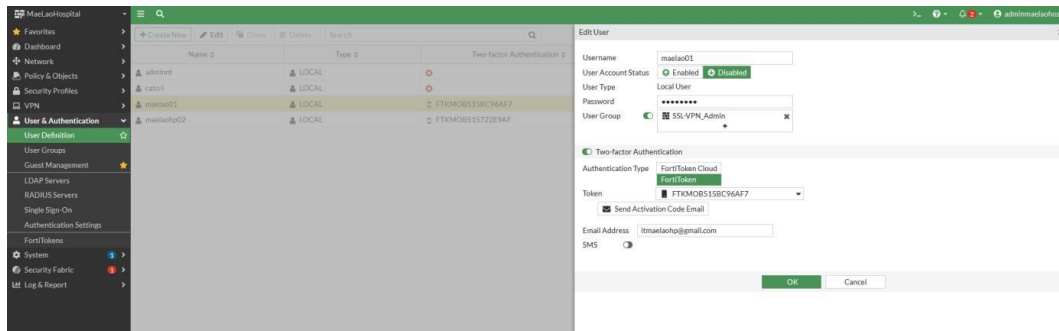
Operation patching

```
[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 ~]$
```

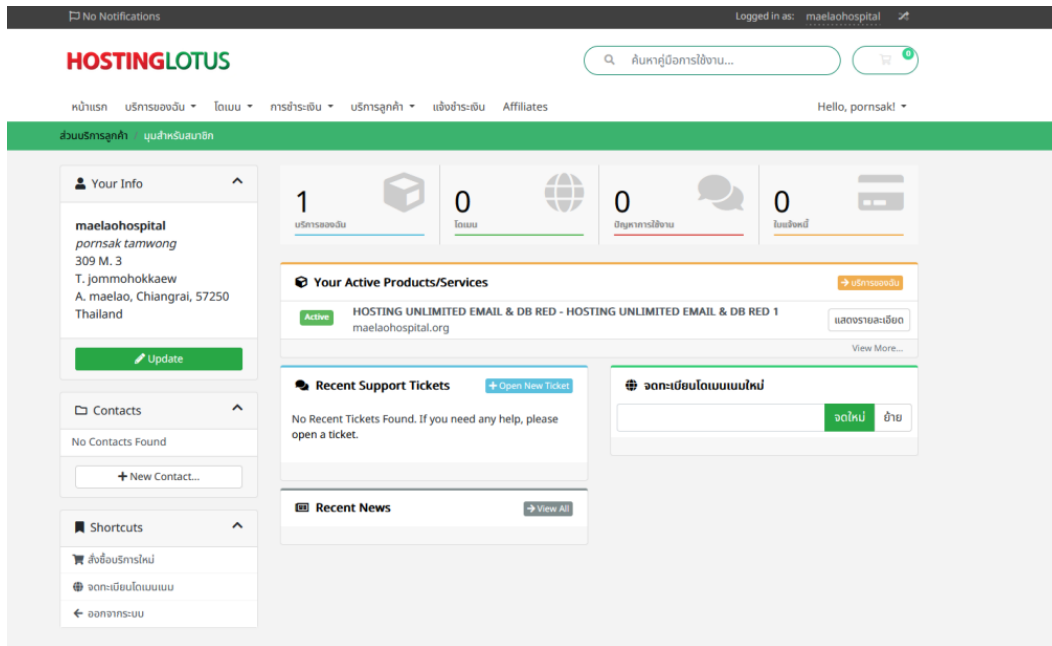


Multi-Factor Authentication (2FA)



Web Application Firewall (WAF)

ดำเนินการเช่า Hosting ภายนอกของ Web Hostinglotus

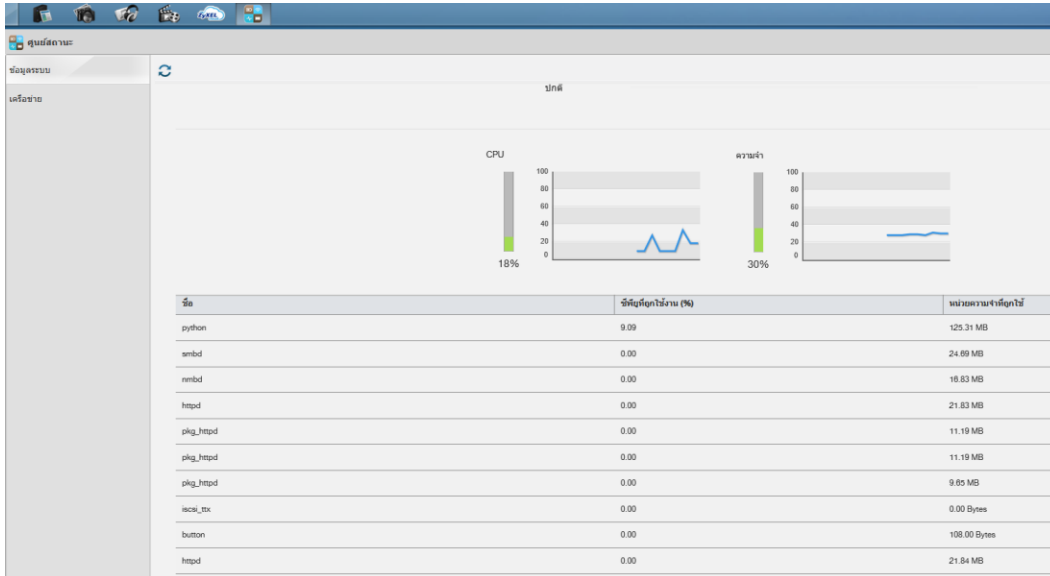


จดโดเมนภายใต้ <https://maelaohospital.moph.go.th/>



Log Management

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



The screenshot shows a ZyXEL file explorer interface. The left pane displays a directory tree with folders for 'admin', 'Authn-Log', 'music', 'photos', and 'video'. The right pane shows the contents of the 'Authn-Log' folder, which contains three files with their names, sizes, and timestamps.

ชื่อ	ขนาด	เปลี่ยนแปลงล่าสุด
192.168.2.1_20250301.txt	991.04 MB	01-03-2025 23:59
192.168.2.1_20250302.txt	946.10 MB	02-03-2025 23:59
192.168.2.1_20250303.txt	1.03 GB	03-03-2025 14:25

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 การตรวจจับพฤติกรรมโจมตีในรูปแบบของ 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 *****