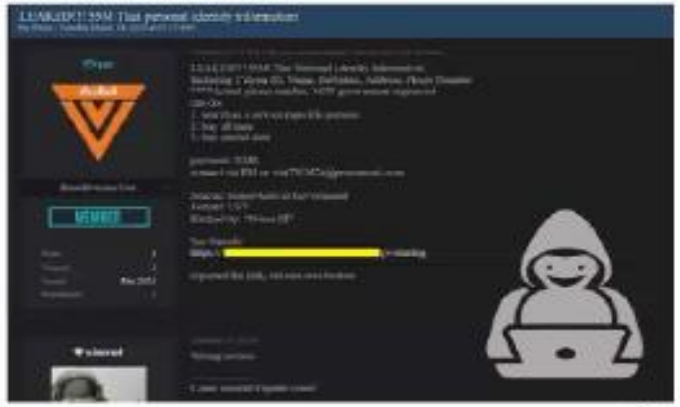
ความปลอดภัยทางไซเบอร์ (Cyber Security)

นายแพทย์อนันต์ กนกศิลป์
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงสาธารณสุข

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงสาธารณสุข



14/3/2023

แฮกเกอร์

เข้าถึงข้อมูล

เจ้าของข้อมูลส่วนบุคคล

เก็บรวบรวม ใช้ เปิดเผย

- Legal Compliance
- Lawful Basis
- Security Measures
- Operational Measures
- Etc...

???

หน่วยงานไหน ?
มาตรการยังไง ?

ข้อมูล 55 ล้านรายชื่อ

- ชื่อ-นามสกุล
- ที่อยู่
- วันเกิด
- เบอร์โทร
- เลขบัตรประชาชน

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

- เข้าถึงระบบคอมฯ ไม่ชอบ (ม.5)
- นำมาตรการป้องกันไปเปิดเผยไม่ชอบ (ม.6)
- เข้าถึงข้อมูลคอมฯ ไม่ชอบ (ม.7)
- ดักรับข้อมูลโดยไม่ชอบ (ม.8)
- กระทำต่อข้อมูลคอมฯ/ระบบคอมฯ เกี่ยวกับ ค.มั่นคง, ค.ปลอดภัยสาธารณะ (ม.12)

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

- หน่วยงานโครงร้างพื้นฐานสำคัญฯ ไม่รายงานเหตุภัยคุกคามทางไซเบอร์ (ม.73)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล

ประกาศคณะกรรมการฯ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมฯ

หน่วยงานของรัฐ

กรอบการดำเนินงานด้าน Cyber Security

0 Administrative Safeguard

1 Physical Safeguard

2 Technical Safeguard

เป้าหมายความปลอดภัยไซเบอร์ของหน่วยงาน

โรงพยาบาล

✓ ISO / IEC 27001
INFORMATION SECURITY MANAGEMENT

✓ ISO / IEC 27799
INFORMATION SECURITY MANAGEMENT
IN HEALTH

หน่วยงาน
ที่เก็บข้อมูล
สุขภาพ
ส่วนบุคคล

✓ HA_PDSC

เกณฑ์การประเมินตนเองตามมาตรฐานการรับรองเฉพาะโรค/เฉพาะระบบ
(Program and Disease Specific Certification)
ระบบพัฒนาคุณภาพสถานพยาบาลด้วยเทคโนโลยีดิจิทัล

ทุกหน่วยงานที่ประมวลผลข้อมูลสุขภาพส่วนบุคคล (จัดเก็บ, ใช้, เผยแพร่)
ต้องผ่านเกณฑ์ประเมินคุณภาพมาตรฐานอย่างน้อย ISO/IEC 27001 และ 27799

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงสาธารณสุข

เพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยไซเบอร์ในทุกมิติ

- ลงทุนติดตั้งอุปกรณ์และเครื่องมือป้องกันภัยคุกคาม
- จัดทำแผนการรับมือภัยคุกคาม
- เคร่งครัดปฏิบัติตามประกาศกระทรวงสาธารณสุข เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565 (ฉบับ ลว. 23 มี.ค.65)

บริหารจัดการข้อมูลส่วนบุคคล ให้สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ยกระดับมาตรฐาน และการเฝ้าระวังป้องกัน

- จัดให้มีเจ้าหน้าที่อย่างน้อย 1 คน ปฏิบัติงานด้านไซเบอร์โดยเฉพาะ (CIRT : Cyber Incident Response Team)
- ลงทุนด้านซอฟต์แวร์เครื่องมือเฝ้าระวัง
- ยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้เป็นไปตามมาตรฐานสากล (HAIT, HA, ISO/IEC 27001, ISO/IEC 27799)
- ให้ความร่วมมือกับ Health CERT (Cyber Emergency Response Team) ในการประสานงานและแก้ไขปัญหาทันที

หลักปฏิบัติในการทำงาน

ท ทำทันที
ท ทำต่อเนื่อง
ท ทำและพัฒนา

ส่งเสริมให้ สธ. เป็น Healthcare Regulator ของประเทศ

- MCIO เป็นผู้รับผิดชอบสั่งการของกระทรวง และ DCIO เป็นผู้รับผิดชอบสั่งการของกรม
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของกรม เป็นผู้รับผิดชอบติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ ให้ข้อเสนอแนะ วิธีการและแนวทางแก้ไขปัญหาแก่เจ้าหน้าที่

MCIO = Ministry CIO
DCIO = Department CIO

พัฒนาบุคลากรให้มีทักษะด้านไซเบอร์ และมีความก้าวหน้า

- สนับสนุนงบประมาณฝึกอบรมและสอบใบประกาศนียบัตร
- สนับสนุนค่าตอบแทนการปฏิบัติงานล่วงเวลา

ICT MOPH Key of Success

ใครเป็นใคร ?
ใน PDPA

Liability

เจ้าของข้อมูลส่วนบุคคล
(Data Subject)

ประชาชนทุกคน

หากเป็นหน่วยง งานทั่วไปก็หมายถึง ลูกค้าพนักงาน รวมถึงเอาส์ซอสด้วย กล่าวอีกนัยคือ เป็นบุคคลที่มีข้อมูลชี้ไปถึงแต่ไม่รวมถึงคนตายและนิติบุคคล
*ทั้งนี้เจ้าของข้อมูลส่วนบุคคลไม่ใช่เจ้าของกรรมสิทธิ์ในข้อมูลนั้น

ผู้ควบคุมข้อมูลส่วนบุคคล
(Data Controller)

หน่วยงาน /องค์กร /สถาบัน ที่กำหนดวัตถุประสงค์ วิธีการประมวลผล และใช้ประโยชน์จากข้อมูลส่วนบุคคล บุคคลธรรมดาก็อาจเป็นผู้ควบคุมข้อมูลได้เช่นเดียวกัน

Data Processing Agreement (DPA)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
(Data Protection Officer: DPO)

คนที่ได้รับมอบหมายเพื่อทำหน้าที่ให้คำแนะนำหรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน / จงค์กร / สถาบัน ให้เป็นไปตามกฎหมาย

ผู้ประมวลผลข้อมูลส่วนบุคคล
(Data Processor)

ผู้ที่ทำตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล โดยหลักคือเอาส์ซอสที่รับจ้าง
*ไม่ใช่พนักงานหรือส่วนหนึ่งของหน่วยงาน /องค์กร / สถาบัน

1 Physical safeguard

- ★ ปรับปรุงอาคารสถานที่ มีมาตรการการป้องกันและควบคุมการเข้า-ออก
- ★ อุปกรณ์ตรวจจับควันและน้ำรั่ว (Smoke Detector , Leak Detector)
- ★ อุปกรณ์ควบคุมอุณหภูมิและความชื้น และแจ้งเตือน
- ★ มีเครื่องสำรองไฟฟ้า

2 Technical safeguard

2.1 มีระบบป้องกัน
Security Protection System

- ★ ติดตั้งอุปกรณ์ป้องกันภัยคุกคามไซเบอร์ เช่น Firewall ที่มีคุณสมบัติป้องกันภัยคุกคามที่เหมาะสม , Antivirus เป็นต้น
- ★ จัดให้มีเจ้าหน้าที่เฝ้าระวังภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง
- ★ มีระบบการสำรองข้อมูล ที่เหมาะสม
- ★ มีการปรับปรุง Update ระบบ , Monitor ช่องโหว่ และ ภัยคุกคาม
- ★ จัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์

(ดูรายละเอียดได้ที่ https://ict.moph.go.th/)

2.2 มี CSOC
Cyber Security Operation Center

- ★ รพ. จัดตั้งศูนย์ CSOC (Product Dependent , Dynamic)
  1. รพ.ลงทุนซื้อSolution + รพ. Operation (รพ.ต้องมีบุคลากร)
  2. รพ.ลงทุนซื้อSolution + ซื้อบริการ (SOC Service) จาก Provider
  3 เช่าอุปกรณ์ + ซื้อบริการ (SOC Service) จาก Provider
- ★ Active Monitoring และ แจ้งเหตุการณ์ภัยคุกคามไซเบอร์

รพ.ทุกแห่ง และหน่วยงานที่มีการเก็บข้อมูลสุขภาพส่วนบุคคล

IMPORTANT

Health Sectoral CERT
Cyber Emergency Response Team

- ★ **เครือข่าย** ของ Health Sectoral CERT
- ★ Sectoral **Active Monitoring**
- ★ **ตอบสนองเหตุฉุกเฉินทางไซเบอร์** ด้านสาธารณสุข

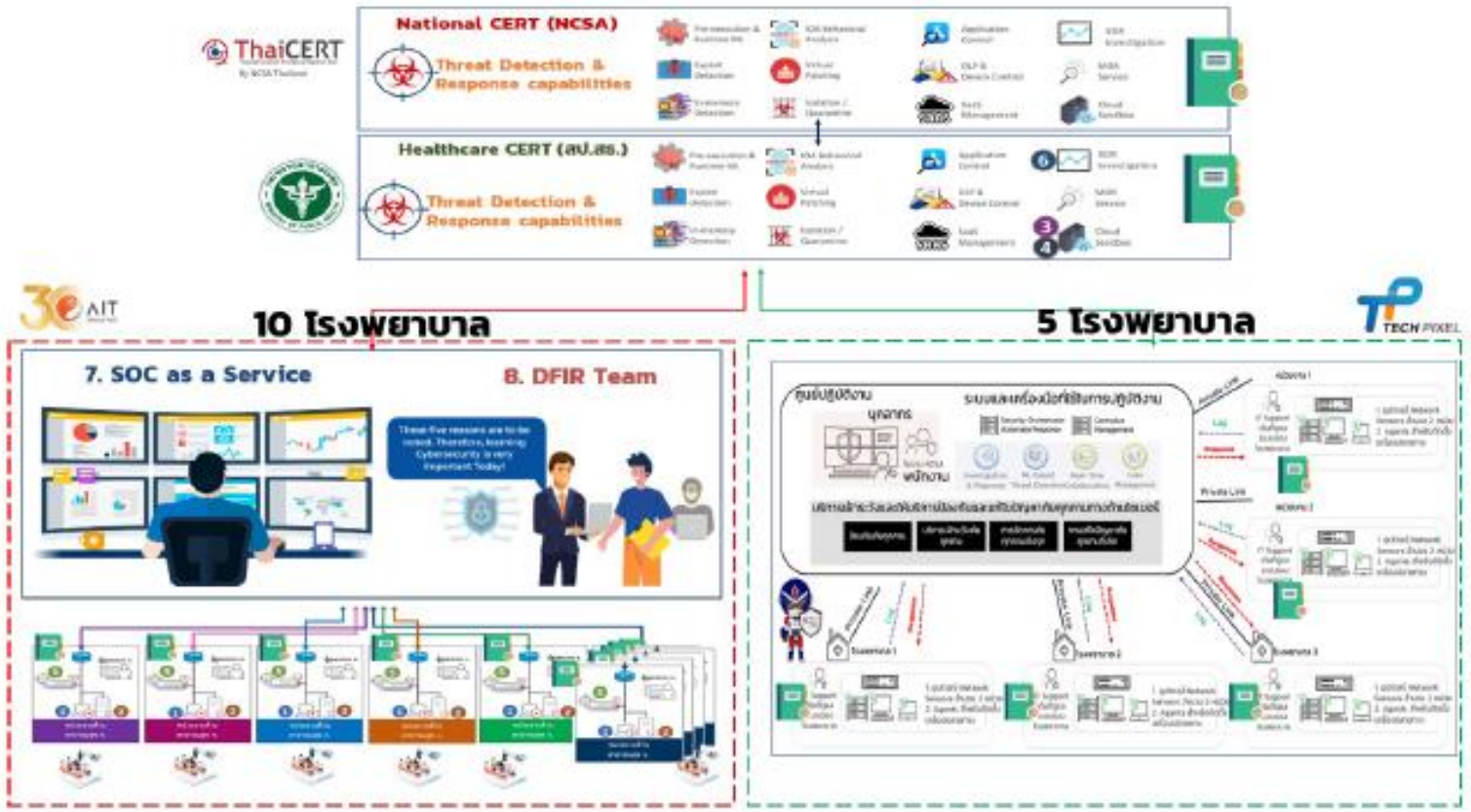
เครือข่ายของ Sectoral CERT
CSOC ของรพ.นอก สธ.
(เช่น รพ.ตำรวจ รพ.รามา รพ.เอกชน ฯลฯ)

Health-CIRT
Cyber Incident Response Team

- ★ จัดให้มีเครือข่าย CIRT ของ สธ.
- ★ Active Monitoring ค้นหาช่องโหว่ และภัยคุกคาม
- ★ ตอบสนองเหตุการณ์ภัยคุกคามไซเบอร์ สธ.

** Health-CIRT = ศทส.สป. และเครือข่ายผู้ประสานงานของหน่วยงานในสังกัด สป.

CSOC (Cyber Security Operation Center)



การติดตั้งอุปกรณ์ตรวจจับเฝ้าระวัง Sensor สำหรับเครื่อง Endpoint และ สำหรับ Networkให้กับระบบของ โรงพยาบาลรัฐ

1. **Threat Prevention** สำหรับในระดับเครือข่าย - ทำการติดตั้งอุปกรณ์ป้องกันและตรวจจับภัยคุกคาม (Threat Prevention & Monitoring Sensor)
2. **Threat Prevention** สำหรับในระดับเครื่องปลายทาง – ทำการติดตั้ง Agent Software สำหรับเครื่องปลายทางที่ใช้งานในโรงพยาบาล โดย Agent Software สำหรับเป็น Sensor สามารถป้องกันภัยคุกคามที่เกิดขึ้นบนเครื่องคอมพิวเตอร์ลูกข่าย (Client

การติดตั้งระบบบริหารจัดการ การเฝ้าระวังรักษาความปลอดภัย และตอบสนองภัยคุกคามทางด้านไซเบอร์

1. **Threat Monitoring** – ติดตั้ง Platform ที่ระบบศูนย์กลางโดย
   1.1 ระบบ Firewall Policy Management ที่ติดตั้งมีความสามารถในการบริหารจัดการระบบตรวจหาภัยคุกคามที่เกิดขึ้นใน รพ. ทางด้านเครือข่าย
   1.2 ระบบ XDR Broker ที่ติดตั้งมีความสามารถใช้งานร่วมกับระบบ ML, AI ในการคุกคามที่เกิดขึ้นใน รพ. ทางด้านเครื่องลูกข่าย
2. **Threat Hunting / Threat Incident Response** – ติดตั้ง Platform ที่ศูนย์กลางในการบริหารจัดการผ่านระบบ SOAR เพื่อเชื่อมต่อกับข้อมูลจากแหล่งภัยคุกคาม (Threat Intelligence) ใช้ทำการตรวจสอบตัวบ่งชี้การโจมตี (IOC) ด้วย
3. **ดำเนินการจัดทำ Playbook** บนระบบบริหารการจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response (SOAR) จำนวนไม่น้อยกว่า 2 Playbooks

Flow การแจ้งเหตุการณ์ภัยคุกคามไซเบอร์ ของหน่วยงาน .....

สป. : คุณสุวันต์นา เสมอเนตร
โทร. 025902180 ต่อ 112
Email dpo@moph.go.th
คำสั่ง สป. ที่ 1189/2565 ลว. 25 พ.ค.65

Health Sector Regulator **	Health Sectoral CERT (ศทส.สป.)	CIRT / IT / SOC ของหน่วยงาน	ผู้ประสานงาน DPO ของหน่วยงาน	CEO / CIO / CDO / CISO ของหน่วยงาน	DPO (สป./กรม)	CEO / CIO / CDO / CISO (สป./กรม)
	โทร. 025901169, 025901200, 0830649867 Email health-cirt@moph.go.th Line: @health-cirt https://health-cirt.moph.go.th	พบเหตุ/ได้รับแจ้งเหตุ	ใครบ้าง? ช่องทางติดต่อ?	ใครบ้าง? ช่องทางติดต่อ?	สป. : นพ.อนันต์ กนกศิลป์ ผอ.ศทส. โทร. 025901214 Email anant.k@moph.go.th คำสั่ง สป. ที่ 2986/2563 ลว. 5 พ.ย.63	
	รับแจ้งเหตุ /ตรวจสอบภัยคุกคามไซเบอร์	แจ้ง - ตรวจสอบเหตุการณ์ - แก้ไขเหตุ/หยุดการโจมตี		เสนอ หัวหน้าหน่วยงานรับทราบเหตุ		
		คาดว่าจะเกิดการละเมิดข้อมูลส่วนบุคคล? Yes / No (ดำเนินการต่อ)	ตรวจสอบและจัดทำรายงานตามแบบฟอร์มเสนอหัวหน้าหน่วยงานลงนาม	เสนอ หัวหน้าหน่วยงานลงนาม ภายใน 24 ชั่วโมง	แจ้ง ตรวจสอบรายงานและนำเสนอ CEO ภายใน 24 ชั่วโมง	เสนอ รับทราบเหตุการณ์และลงนามแจ้ง สคส. ภายใน 24 ชั่วโมง
NCSA สกมช	ดำเนินการแก้ไขเหตุการณ์ร่วมกับหน่วยงานที่เกี่ยวข้อง	แจ้ง พิจารณาขอความช่วยเหลือ? Yes / No (ดำเนินการต่อ)				
รับทราบเหตุการณ์และพิจารณาดำเนินการตามอำนาจหน้าที่	แจ้ง	- แก้ไขและป้องกันเหตุเกิดซ้ำ - บันทึกเหตุการณ์และผล - จัดทำรายงานโดยเร็ว		เสนอ หัวหน้าหน่วยงานลงนาม	เสนอ	แจ้ง รับทราบเหตุการณ์และลงนามแจ้ง สกมช. / Regulator

** Regulator ของ หน่วยบริการสุขภาพ (รพ. ,คลินิก) คือ กรมสนับสนุนบริการสุขภาพ (สบส.)
Regulator ของ หน่วยงานที่ดำเนินการเกี่ยวกับผลิตภัณฑ์สุขภาพ (ยา, เวชภัณฑ์, เครื่องมือแพทย์) คือ อย.
Regulator ของ หน่วยงานที่มีการดำเนินการกับข้อมูลสุขภาพ (Digital health) ยกเว้นหน่วยบริการสุขภาพ คือ สป.(ศทส.)

- คำสั่ง สป. ที่ 1480/2565 เรื่องแต่งตั้งเจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล (ประสาน DPO ระดับจังหวัด/หน่วยงาน)
- แบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ดาวน์โหลดได้ที่ https://pdpa.moph.go.th/

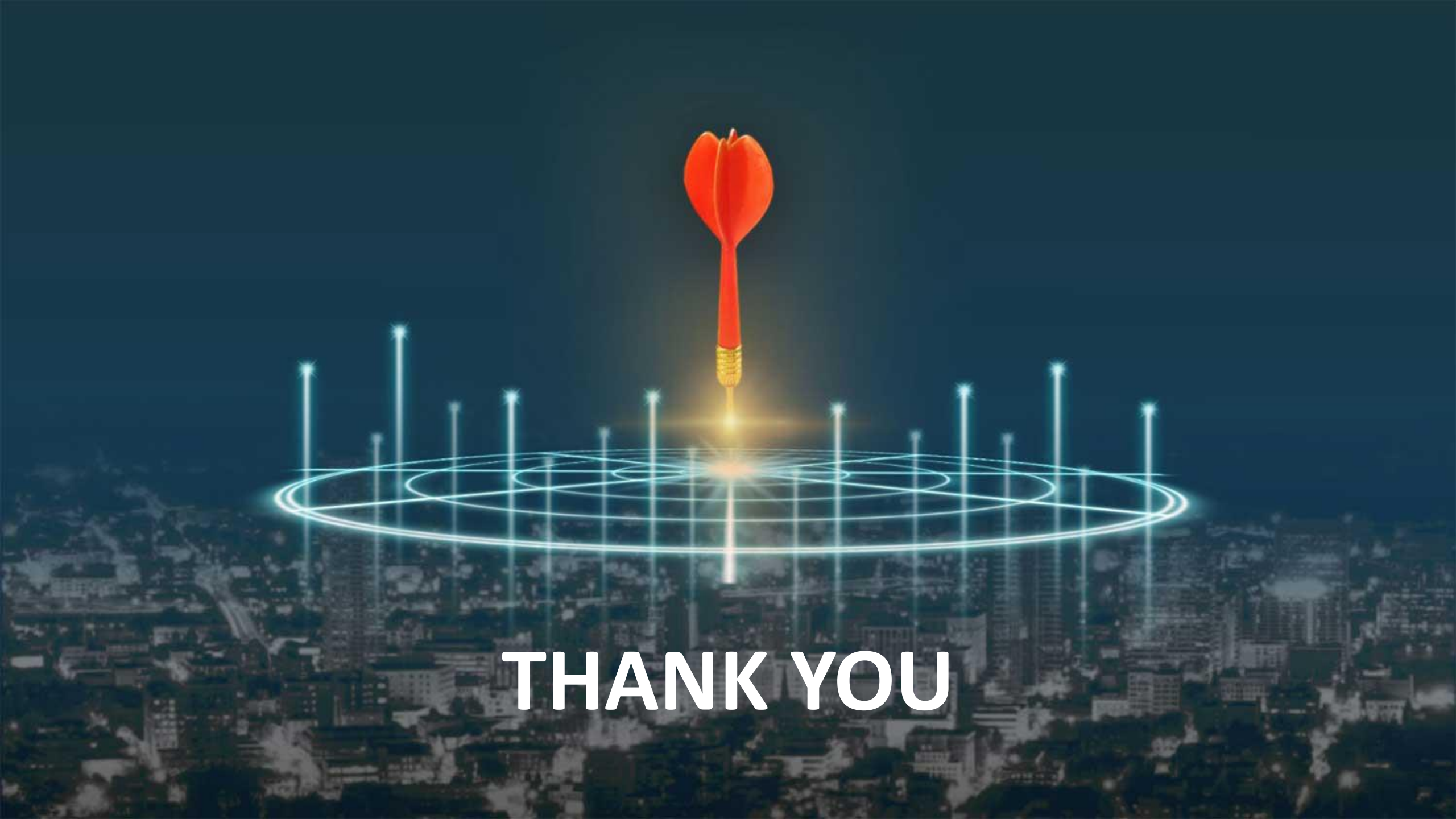
แบบสำรวจผลการดำเนินการติดตั้ง Cyber Security ระบบ HIS ของโรงพยาบาล ในเขตสุขภาพที่ 1

จังหวัด	หน่วยงาน	Login User	Server Security	System control	Generator Backup	Backup Data	Firewall	Anti-virus
น่าน	โรงพยาบาลน่าน	มี	มี	มี	มี	มี	มี	มี
น่าน	โรงพยาบาลเชียงกลาง	มี	มี	มี	มี	มี	มี	มี
น่าน	โรงพยาบาลท่าวังผา	มี	มี	มี	มี	มี	มี	มี
น่าน	โรงพยาบาลทุ่งช้าง	มี	มี	มี	มี	มี	มี	ไม่มี
น่าน	โรงพยาบาลเฉลิมพระเกียรติ	มี	มี	มี	มี	มี	มี	มี
น่าน	โรงพยาบาลนาน้อย	มี	มี	มี	ไม่มี	มี	มี	ไม่มี
น่าน	โรงพยาบาลนาหมื่น	มี	มี	มี	มี	มี	มี	ไม่มี
น่าน	โรงพยาบาลบ่อเกลือ	มี	มี	ไม่มี	มี	มี	มี	มี
น่าน	โรงพยาบาลบ้านหลวง	มี	มี	มี	มี	มี	มี	มี
น่าน	โรงพยาบาลภูเพียง	มี	มี	ไม่มี	มี	มี	มี	ไม่มี
น่าน	โรงพยาบาลแม่จริม	มี	มี	มี	มี	มี	มี	ไม่มี
น่าน	โรงพยาบาลเวียงสา	มี	มี	มี	มี	มี	มี	ไม่มี
น่าน	โรงพยาบาลสมเด็จพระยุพราชปัว	มี	มี	ไม่มี	ไม่มี	มี	มี	มี
น่าน	โรงพยาบาลสองแคว	มี	มี	ไม่มี	มี	มี	มี	ไม่มี
น่าน	โรงพยาบาลสันติสุข	มี	มี	ไม่มี	มี	มี	มี	ไม่มี

แบบสอบถามการป้องกันความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล จ.น่าน

รพ.	ได้มีคำสั่งแต่งตั้ง CIRT ประจำแต่ละ รพ.	ได้มีการควบคุมการเข้า - ออกห้องปฏิบัติการระบบเครือข่าย	ได้มีการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ	ได้มีการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ	ได้มีควบคุมการใช้งานคอมพิวเตอร์ส่วนบุคคล (PC)	ได้มีการควบคุมการใช้งานคอมพิวเตอร์ (Notebook)	ได้มีการควบคุมการใช้งาน Internet	ได้มีควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Security)	ได้มีการจัดหาและติดตั้งระบบ software license (windows)	ได้มีการจัดหาและติดตั้งระบบ antivirus สำหรับเครื่องคอมพิวเตอร์	ได้มีการควบคุมการติดตั้งซอฟต์แวร์ในระบบของบริการ	มีการแยก server จาก network client เช่นinternal zone , server zone	ได้มีระบบ firewall จัดการระบบ network	ได้มีระบบการพิสูจน์ตัวตนในการใช้งาน (internet) authentication	ได้มีการอบรม/สร้างความตระหนักรู้ด้าน cyber security ให้แก่	ได้มีการใช้ outsource ตรวจสอบระบบ network
10716 น่าน	ไม่มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	ไม่มี	มี	มี	มี	มี
11173 แม่จริม	ไม่มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	ไม่มี	ไม่มี	มี
11174 บ้านหลวง	มี	มี	มี	มี	มี	มี	มี	มี	ไม่มี	มี	ไม่มี	มี	มี	มี	ไม่มี	ไม่มี
11175 นาน้อย	มี	มี	มี	มี	มี	มี	มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี	มี	ไม่มี	ไม่มี	ไม่มี
11176 ท่าวังผา	มี	มี	มี	มี	มี	มี	มี	มี	ไม่มี	มี	มี	มี	มี	มี	มี	มี
11177 เวียงสา	ไม่มี	มี	มี	มี	มี	มี	มี	มี	ไม่มี	ไม่มี	ไม่มี	ไม่มี	มี	มี	ไม่มี	มี
11178 รพ.ทุ่งช้าง	มี	มี	มี	มี	มี	มี	มี	มี	ไม่มี	ไม่มี	มี	มี	มี	มี	มี	มี
11179 เชียงกลาง	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี
11180 นาหมื่น	ไม่มี	มี	มี	มี	มี	มี	มี	มี	ไม่มี	มี	มี	ไม่มี	มี	มี	มี	มี
11181 สันติสุข	ไม่มี	มี	มี	มี	มี	ไม่มี	มี	มี	ไม่มี	มี	มี	มี	มี	ไม่มี	ไม่มี	ไม่มี
11182 บ่อเกลือ	ไม่มี	มี	มี	มี	ไม่มี	ไม่มี	มี	มี	ไม่มี	ไม่มี	ไม่มี	มี	มี	ไม่มี	มี	ไม่มี
11183 สองแคว	มี	มี	มี	มี	มี	มี	มี	มี	ไม่มี	ไม่มี	มี	ไม่มี	มี	ไม่มี	ไม่มี	ไม่มี
11625 เฉลิมพระเกียรติ	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี	มี
25017 ภูเพียง	ไม่มี	มี	มี	มี	มี	มี	มี	มี	ไม่มี	ไม่มี	มี	มี	มี	ไม่มี	ไม่มี	มี

เอกสารเกี่ยวกับ Cyber Security และ PDPA


THANK YOU