ประชุมรับมอบนโยบาย และ มาตรการ การรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงสาธารณสุข

ณ ห้องประชุมการบูร สำนักงานปลัดกระทรวงสาธารณสุข
และผ่านระบบออนไลน์ Cisco WebEx Meeting
วันที่ 12 เมษายน 2566

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงสาธารณสุข

ระเบียบวาระการประชุม

ระเบียบวาระที่ 1

1. เรื่องที่ประธานแจ้งให้ที่ประชุมทราบ

โดย นายโอภาส การย์กวินพงศ์ ปลัดกระทรวงสาธารณสุข

มอบนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงสาธารณสุข

ระเบียบวาระที่ 2

2. เรื่องเพื่อทราบ

2.1 สรุปเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์

โดย นายพงศ์เกษม ไข่มุกด์ รองปลัดกระทรวงสาธารณสุข

ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ประจำกระทรวงสาธารณสุข

2.2 มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์

โดย นายอนันต์ กนกศิลป์ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานปลัดกระทรวงสาธารณสุข

ระเบียบวาระที่ 3

3. เรื่องอื่นๆ (ถ้ามี)

1. เรื่องที่ประธานแจ้งให้ที่ประชุมทราบ

นายโอภาส การย์กวินพงศ์ ปลัดกระทรวงสาธารณสุข

สั่งการ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงสาธารณสุข

ถอดความข้อสั่งการ:

1. **กระทรวงสาธารณสุขให้ความสำคัญกับนโยบายด้านความปลอดภัยทาง Cyber Security ถือเป็นนโยบายเร่งด่วนของกระทรวง** และได้มีข้อสั่งการที่ลงนามโดยรองปลัด นพ.พงศ์เกษม ในฐานะผู้รับผิดชอบในนามของกระทรวงสาธารณสุขไปหลายครั้งแล้ว **ขอให้ผู้บริหารทุกหน่วยงานให้ความสำคัญ และติดตามสถานการณ์ การจัดการอย่างใกล้ชิด** หากมีข้อสงสัยให้ปรึกษามายังหน่วยงานที่เกี่ยวข้อง

2. การ**ทำความเข้าใจกฎหมายที่เกี่ยวข้องในการเก็บข้อมูล ดูแลรักษา รวมถึงเชื่อมโยงกับหน่วยงานภายนอก** อยู่ภายใต้กฎหมายที่สำคัญหลายอย่าง ไม่ว่าจะเป็น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือ กฎหมาย PDPA , พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 หรือ กฎหมาย Cyber Security คือเวลามีกฎหมายอะไรออกมา จะต้องมีกฎหมายลูกหรือภาคปฏิบัติออกมา แต่ก็ต้องยอมรับ เวลากฎหมายฉบับใดฉบับหนึ่งออกมา ภาคปฏิบัติกับกฎหมายลูกส่วนใหญ่จะออกตามมาไม่ทัน ก็เลยทำให้มีปัญหาติดขัดในเชิงการจัดการอยู่หลายประการ แต่**ต้องทำความเข้าใจว่าประเด็นอะไรที่ต้องดำเนินการบ้าง** และได้หารือกับ ผอ.กองกฎหมาย (นายปิยวัฒน์) ว่า**การดำเนินงานด้านไซเบอร์** นอกจากจะมี CIO, มีหน่วยงานด้านไอทีแล้ว ก็**ขอให้มีนิติกรเข้ามาร่วม**ดูด้วย จะได้ปิดจุดโหว่เรื่องของการทำความเข้าใจข้อกฎหมายไปด้วย

3. ให้**เร่งรัดมาตรการปฏิบัติการยกระดับ cyber security ให้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์**ตามแนวทางกับประกาศกระทรวงสาธารณสุขด้านไซเบอร์ปี 2565 ที่ทาง ศทส. ได้ประกาศเป็นแนวทางไว้แล้ว *(**ประกาศกระทรวงสาธารณสุข เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565** ฉบับลงวันที่ 23 มี.ค.65)* หากมีข้อสงสัยให้สอบถามมา และขอ**ให้ ศทส.** เป็นเจ้าภาพใหญ่ ในการลงไป**ติดตามให้ทุกหน่วยงานในสังกัดกระทรวงสาธารณสุขสามารถดำเนินการได้ครบถ้วน**

4. ขอให้**ติดตามการยกระดับ cyber security ของหน่วยงาน**ในการประชุม สป. สัญจรครั้งต่อไป ซึ่งจะจัด**ประชุมที่จังหวัดเลย วันที่ 12-13 มิ.ย.66** กำหนดการวันที่ 12 จะไปดูงานด้าน cyber security วันที่ 13 ประชุม สป. ก็จะใช้ระบบเดิมคือการ**จับสลากให้ท่านผู้บริหารได้มาอธิบายว่าหน่วยงานท่านทำเรื่อง cyber security อะไร อย่างไรบ้าง**

2. เรื่องเพื่อทราบ

2.1 สรุปเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์

โดย นายพงศ์เกษม ไข่มุกด์ รองปลัดกระทรวงสาธารณสุข

ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ประจำกระทรวงสาธารณสุข

2. เรื่องเพื่อทราบ

2.2 มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์

โดย นายอนันต์ กนกศิลป์

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานปลัดกระทรวงสาธารณสุข

มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรการเร่งด่วน สำหรับผู้บริหารหน่วยงานพิจารณาสั่งการ

- ติดตั้งอุปกรณ์ป้องกันภัยคุกคามไซเบอร์ เช่น Firewall, Web Application Firewall และ Antivirus เป็นต้น พร้อม**ตั้งค่าให้ถูกต้อง** เหมาะสมกับระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน
- เฝ้าระวังภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง โดยต้อง**จัดให้มีเจ้าหน้าที่ปฏิบัติงานเป็นประจำ**อย่างน้อย 1 คน และต้องสามารถ**ประสานงานกับ Health CERT ได้ตลอดเวลา**
- เว็บไซต์และระบบงาน ควร**ใช้ชื่อโดเมนของกระทรวงสาธารณสุข** (xxxx.moph.goth) เพื่อให้ทีม Health CERT สามารถช่วยค้นหาช่องโหว่ และดูแลแนะนำเบื้องต้นได้
- **จัดทำทะเบียน**ชื่อเว็บไซต์ ชื่อโดเมน และ IP Address ในความดูแล และสำเนาส่ง ศทส.สป.
- **สำรวจและปิด**เว็บไซต์/ระบบงานที่ไม่ได้ใช้งาน

หนังสือด่วนที่สุด
ที่ สธ 0212/ว 8584
ลว. 7 เม.ย. 65

เรื่อง ย้ำเตือนให้ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด

เรียน เลขาธิการคณะกรรมการอาหารและยา/อธิบดีกรมทุกกรม/นายแพทย์สาธารณสุขจังหวัดทุกแห่ง/ผู้อำนวยการสำนักงานเขตสุขภาพที่ ๑ – ๑๓/ผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไป ทุกแห่ง หัวหน้าสำนักงานรัฐมนตรี และผู้อำนวยการหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

ด่วนที่สุด

ที่ สธ ๐๒๑๒/ว ๘๕๘๔

สำนักงานปลัดกระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๗ เมษายน ๒๕๖๖

เรื่อง ย้ำเตือนให้ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด

เรียน เลขาธิการคณะกรรมการอาหารและยา/อธิบดีกรมทุกกรม/นายแพทย์สาธารณสุขจังหวัดทุกแห่ง/ผู้อำนวยการสำนักงานเขตสุขภาพที่ ๑ – ๑๓/ผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไป ทุกแห่ง หัวหน้าสำนักงานรัฐมนตรี และผู้อำนวยการหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

อ้างถึง หนังสือสำนักงานปลัดกระทรวงสาธารณสุข ที่ สธ ๐๒๑๒/ว ๑๙๐๘ ลงวันที่ ๒๖ มกราคม ๒๕๖๖

สิ่งที่ส่งมาด้วย มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ จำนวน ๑ ฉบับ

ตามหนังสือที่อ้างถึง สำนักงานปลัดกระทรวงสาธารณสุข ได้แจ้งมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กรณีการแฝงเว็บไซต์พนันออนไลน์) กระทรวงสาธารณสุข ให้ทุกหน่วยงานดำเนินการตามมาตรการโดยเคร่งครัด นั้น

บัดนี้ยังคงพบช่องโหว่ทางไซเบอร์ของหลายหน่วยงาน ซึ่งเป็นปัจจัยเสี่ยงภัยคุกคามทางไซเบอร์และอาจนำไปสู่การกระทำความผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ สำนักงานปลัดกระทรวงสาธารณสุข จึงขอย้ำเตือนให้ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเคร่งครัด โดยได้จัดทำมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงสาธารณสุข ฉบับที่ ๑ รายละเอียดตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อโปรดทราบและมอบหมายหน่วยงานที่เกี่ยวข้องดำเนินการตามมาตรการฯ โดยเคร่งครัดและต่อเนื่องต่อไปด้วย

ขอแสดงความนับถือ

(นายพงศ์เกษม ไข่มุกด์)
รองปลัดกระทรวงสาธารณสุข
ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)
ประจำกระทรวงสาธารณสุข

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กลุ่มบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการ
โทร ๐ ๒๕๙๐ ๑๒๐๘, ๐๘ ๗๐๒๗ ๖๖๖๓ (รุ่งนิภา)
โทรสาร ๐ ๒๕๙๐ ๑๒๑๕
อีเมล ict-moph@health.moph.go.th

มีผลบังคับใช้

6 ก.ย. 65

ให้ดำเนินการ ให้มีกระบวนการ

เป้าหมาย คือ การได้รับการรับรองกระบวนงานตามมาตรฐาน

HAIT , HA
ISO/IEC 27001
ISO/IEC 27799

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

เพื่อจัดให้มีประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็วมีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๑๓ วรรคหนึ่ง (๔) และวรรคสอง และมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบมติที่ประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๑/๒๕๖๔ เมื่อวันที่ ๒๕ มิถุนายน ๒๕๖๔ และมติที่ประชุมคณะกรรมการกำกับดูแลด้านความปลอดภัยไซเบอร์ ครั้งที่ ๑/๒๕๖๔ เมื่อวันที่ ๘ มิถุนายน ๒๕๖๔ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้เป็นไปตามแนบท้ายประกาศนี้

มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงสาธารณสุข

ให้ดำเนินการตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสาคัญทางสารสนเทศ พ.ศ. 2564 โดยเคร่งครัด และให้ดำเนินการตามมาตรการ ดังนี้

1) สำรวจเว็บไซต์และระบบงานในความดูแลของหน่วยงาน และจัดทำทะเบียนชื่อเว็บไซต์และชื่อโดเมน และ IP Address เช่น ict-ops-moph.moph.go.th 203.xxx.xxx.xxx เป็นต้น และจัดส่งสำเนาไฟล์ไปยังศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ. อีเมล ictmoph.moph.go.th เพื่อนำไปจัดทำทะเบียนกลางของกระทรวงสาธารณสุข ให้ Health CERT ใช้ในการกำกับดูแลต่อไป

2) ปิดเว็บไซต์และระบบงานที่ไม่ได้ใช้งาน รวมถึงเว็บไซต์และระบบงานที่พบความเสี่ยงทั้งหมดในทันที เพื่อลดความเสี่ยงในการถูกคุกคามทางไซเบอร์จากผู้ไม่หวังดี

3) ดูแล Environments ทั้งหมดที่เกี่ยวข้อง ของเว็บไซต์ และอัปเดตให้ทันสมัย เช่น อัปเดตเวอร์ชั่น และ Patch ของ ระบบปฏิบัติการและซอฟต์แวร์ให้เป็นปัจจุบัน เป็นต้น

มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์

4) ติดตั้งอุปกรณ์ป้องกันภัยคุกคามไซเบอร์ เช่น Firewall, Web Application Firewall และ Antivirus เป็นต้น พร้อมตั้งค่าให้ถูกต้อง เหมาะสมกับระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน

5) เฝ้าระวังภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง โดยต้องจัดให้มีเจ้าหน้าที่ปฏิบัติงานเป็นประจำอย่างน้อย 1 คน และต้องสามารถประสานงานกับ Health CERT ได้ตลอดเวลา

6) ก่อนเผยแพร่ข้อมูลส่วนบุคคลในทุกช่องทางทั้งระบบอินทราเน็ตและอินเทอร์เน็ต จะต้องได้รับความเห็นชอบหรืออนุญาต (อย่างมีหลักฐาน) จากผู้บริหารสูงสุดของหน่วยงาน

7) เว็บไซต์และระบบงาน ควรใช้ชื่อโดเมนของกระทรวงสาธารณสุข (xxxx.moph.goth) โดยแจ้งความประสงค์เป็นหนังสือราชการถึงศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.สธ.

8) ตรวจสอบรายการปัจจัยเสี่ยงที่ทำให้เกิดช่องโหว่ทางไซเบอร์ ดังต่อไปนี้ หากพบให้จัดการปิดช่องโหว่ทันทีหรือโดยเร็วที่สุด

8.1) มีการอัปโหลดไฟล์ที่มีความสำคัญขึ้นบนหน้าเว็บไซต์ทั้งภายใต้โดเมน (moph.go.th) และภายนอก (Development Platform ต่างๆ เช่น github) ทำให้ผู้โจมตีใช้ประโยชน์ได้ เช่น ไฟล์ที่ประกอบด้วย Username Password สำหรับเข้าใช้งานระบบ, Source code ของระบบ Token ในการยืนยันตัวตน

มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์

8.2) ขาดการอัปเดตซอฟต์แวร์ที่ใช้งานให้เป็นเวอร์ชันปัจจุบัน

8.3) มี CMS Plugins ที่ไม่ได้ใช้งานแล้วแต่ยังไม่ถอนการติดตั้ง

8.4) ขาดการทำ Data Encryption เพื่อการรับ-ส่งข้อมูลสำคัญทำได้จากคนที่มี Key เท่านั้น

8.5) ไม่มีการปิดกั้นการ exposed ของ website configuration, database configuration, website directory หรือเปิดให้เข้าถึงไฟล์ได้จากอินเทอร์เน็ตโดยไม่มีการตรวจสอบ เช่น เปิดหน้า Index Directory ไว้ ทำให้เห็นไฟล์ต่างๆ

8.6) ไม่ได้กำหนด IP Address ที่จะเข้าถึง Service จากระยะไกลที่มีความอ่อนไหว เช่น Database และ Network Protocol ต่าง ๆ

8.7) ไม่ได้กำหนด Rate-Limitation ในการเข้าถึง Service ว่าหากเกิด Connection failed บ่อยๆ จะต้องถูกปิดกั้น

8.8) ไม่มีการทำตรวจสอบ User Input ทำให้สามารถพัฒนาเป็นช่องโหว่ที่ใช้โจมตีได้ เช่น SQL Injection, XSS Attack

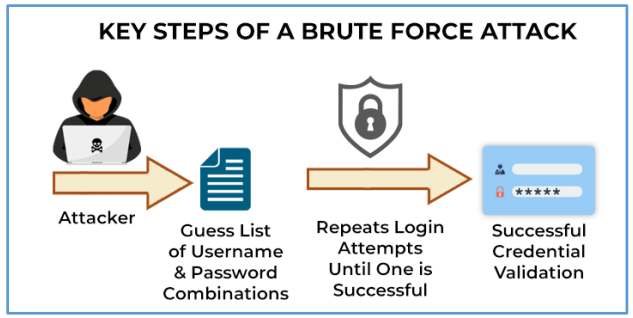
8.9) ไม่มีการปิด Error ที่ระบบตอบกลับ ทำให้ผู้โจมตีตรวจสอบได้ว่า Payload ที่ใช้สามารถทำงานได้หรือไม่

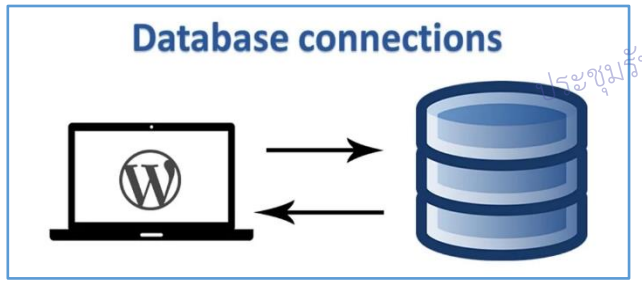
8.10) ปิดให้เชื่อมต่อ Database จากสาธารณะ เช่น เปิด Port 3306 โดยไม่ผ่าน VPN

8.11) มีการแชร์ไฟล์ที่มีข้อมูลส่วนบุคคลในพื้นที่สาธารณะ (Public File Sharing) เช่น google drive , OneDrive โดยไม่เข้ารหัสไฟล์ หรือแชร์เฉพาะบุคคล

8.12) ขาดการตรวจสอบ Username และ Permission บนระบบที่อยู่ภายใต้การดูแลให้ถูกต้อง หากพบความผิดปกติควรแก้ไขโดยทันที

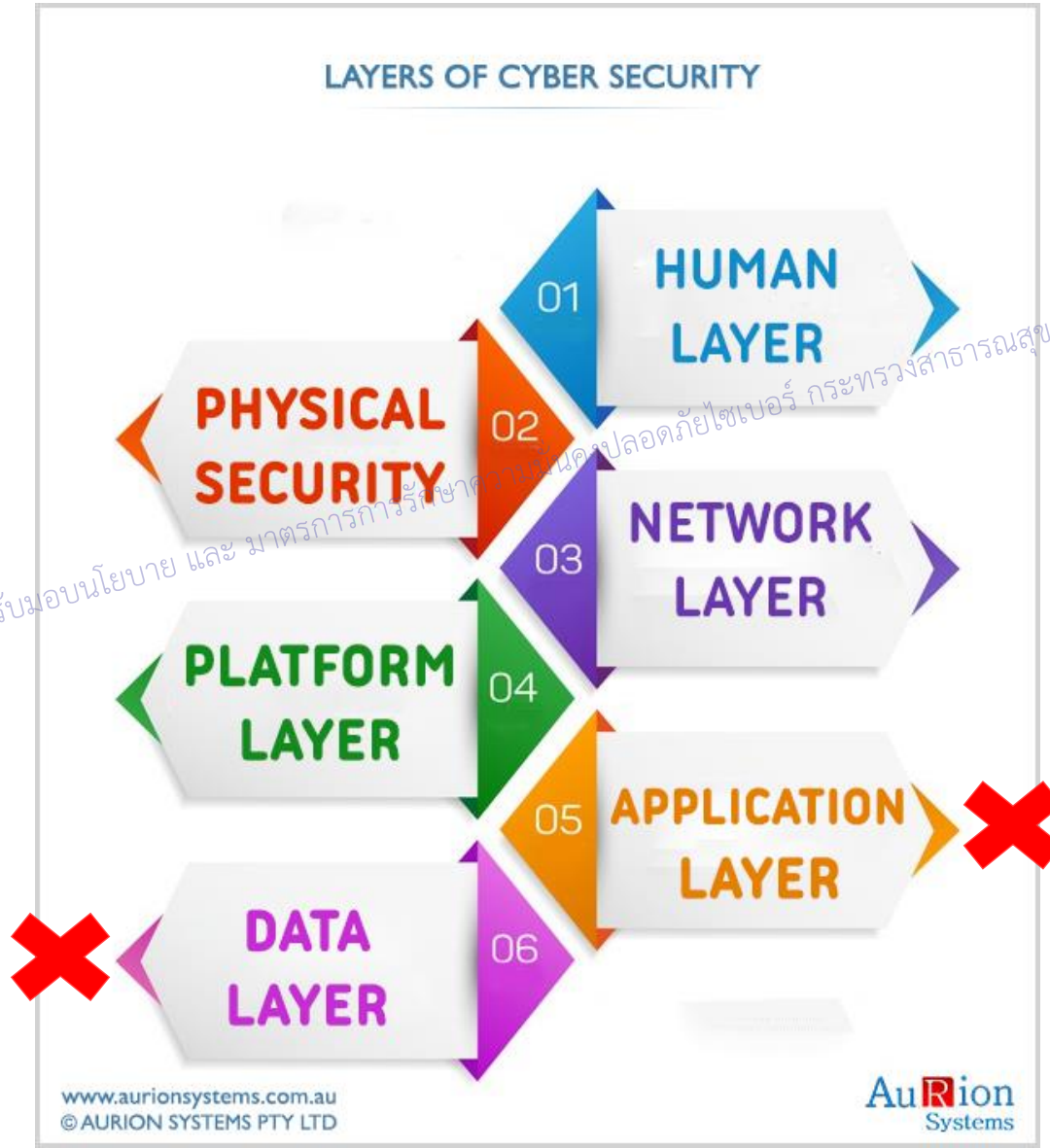
มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์

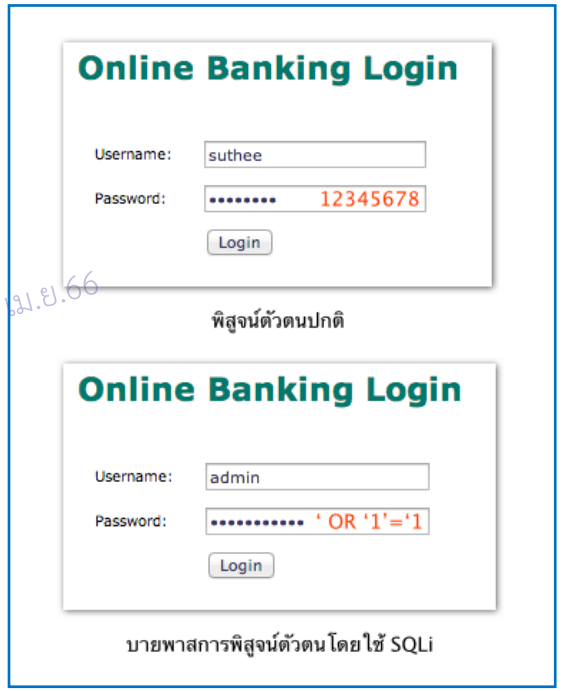




Exposed Data in Public

Public Database Connection

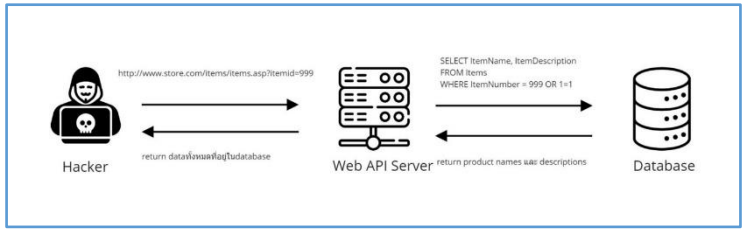




SQL Injection

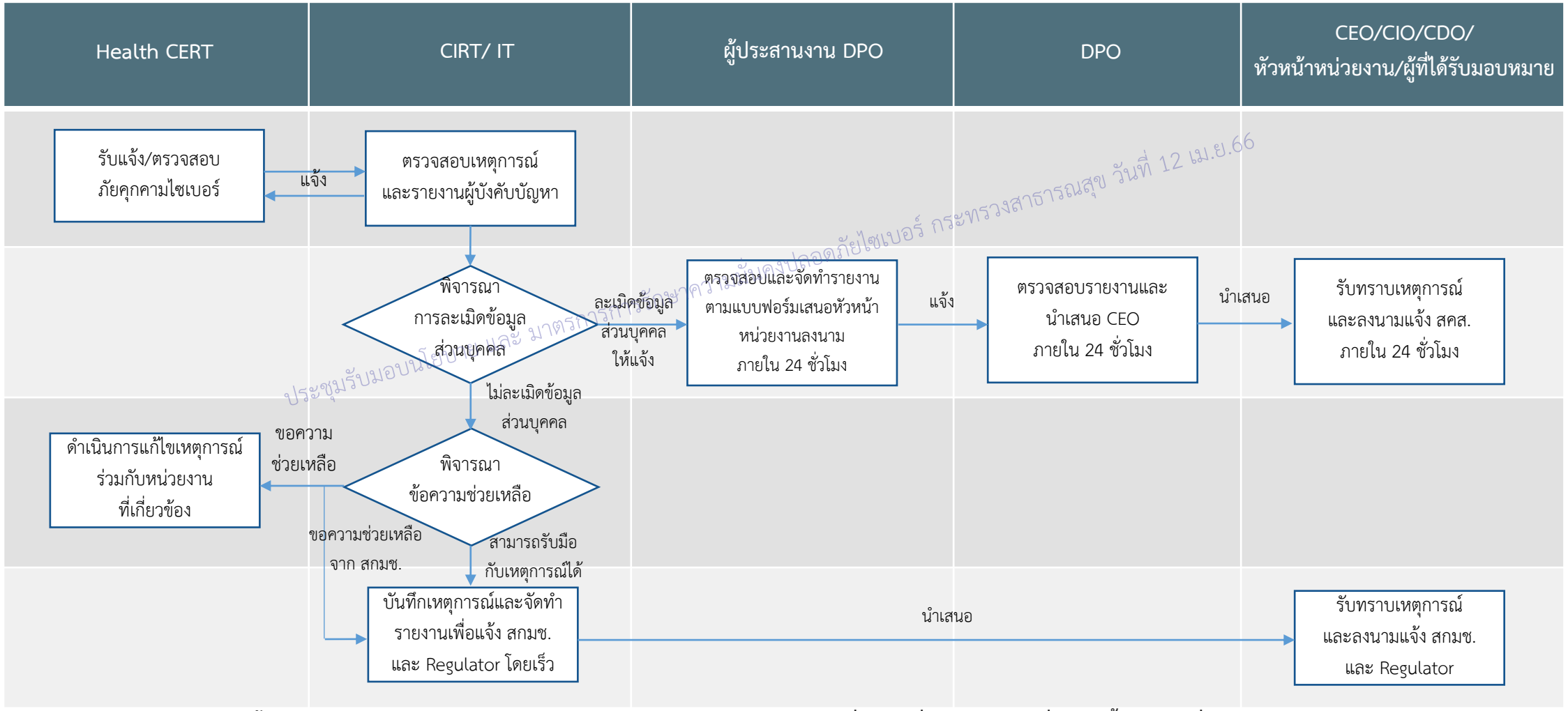
ฝัง Script เวปพนัน

Weak API Security



มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์

Flow การแจ้งเหตุการณ์ภัยคุกคามไซเบอร์



1. คำสั่ง สป. ที่ 1189/2565 เรื่องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
2. คำสั่ง สป. ที่ 1480/2565 เรื่องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ระดับส่วนกลาง)
3. คำสั่ง สป. ที่ 1480/2565 เรื่องแต่งตั้งเจ้าหน้าที่ประสานงานคุ้มครองข้อมูลส่วนบุคคล (ระดับจังหวัด)
4. แบบการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ดาวน์โหลดได้ที่ https://pdpa.moph.go.th/

มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์

ช่องทางติดต่อ Health CERT

- โทรศัพท์ 08 3064 9867, 02 590 1169, 02 5901200
- อีเมล: health-cirt@moph.go.th
- Line Official: @health-cirt
- เว็บไซต์แจ้งเหตุการณ์ไซเบอร์ https://health-cirt.moph.go.th
- เว็บไซต์เผยแพร่ประชาสัมพันธ์ข้อมูลข่าวสารทางไซเบอร์ https://cyber.moph.go.th/

ช่องทางติดต่อ DPO

- โทรศัพท์ 0 2590 2180 ต่อ 112
- อีเมล: dpo@moph.go.th
- เว็บไซต์เผยแพร่ประชาสัมพันธ์ข้อมูลและดาวน์โหลดเอกสารที่เกี่ยวข้องกับ PDPA https://pdpa.moph.go.th/

Line กลุ่มเจ้าหน้าที่ประสานงาน DPO

(PDPA: ข้อมูลส่วนบุคคล)

3. เรื่องอื่นๆ (ถ้ามี)

ขอบคุณครับ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงสาธารณสุข

ข้อมูลสนับสนุน

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงสาธารณสุข

บริหารจัดการข้อมูลส่วนบุคคล
ให้สอดคล้องกับ
พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. 2562

หลักปฏิบัติในการทำงาน

ท ทำทันที
ท ทำต่อเนื่อง
ท ทำและพัฒนา

MCIO = Ministry CIO
DCIO = Department CIO

เพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยไซเบอร์ในทุกมิติ

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

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

ส่งเสริมให้ สธ. เป็น Healthcare Regulator ของประเทศ

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

พัฒนาบุคลากรให้มีทักษะด้านไซเบอร์ และมีความก้าวหน้า

- สนับสนุนงบประมาณฝึกอบรมและสอบใบประกาศนียบัตร
- สนับสนุนค่าตอบแทนการปฏิบัติงานล่วงเวลา

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

ใหม่

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านสาธารณสุข
ปลัด สธ. เป็นประธาน (คำสั่ง สธ. ที่ 452/2564 ณ 20 เม.ย.64)

สำนักงานปลัดกระทรวงสาธารณสุข (โดย ศทส.)
Main Regulator

Health CERT

สกมช.
National CERT

สบส.

อย.

สป. (โดย ศทส.)

ผู้ประกอบการ
ด้านบริการสุขภาพ

ผู้ประกอบการ
ด้านผลิตภัณฑ์สุขภาพ

ผู้ประกอบการ
ด้านสุขภาพดิจิทัล

Operator ด้านต่างๆ ภาครัฐ ทั้งในและนอกสังกัด สธ. และภาคเอกชน

โรงพยาบาลสังกัด สธ. ทุกแห่ง CIRT SOC

โรงพยาบาลนอกสังกัด สธ. เฉพาะที่เป็น CII CIRT SOC

หน่วยงานที่เป็น CII CIRT SOC

รายงานต่อ Health CERT. เมื่อคาดว่าเกิดเหตุการณ์

คณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพ ระดับจังหวัด

CIO เขตสุขภาพ

คณะทำงานบริหารเทคโนโลยีสารสนเทศและระบบสุขภาพดิจิทัลกระทรวงสาธารณสุข

Auditor
ISO 27001
HA , HAIT

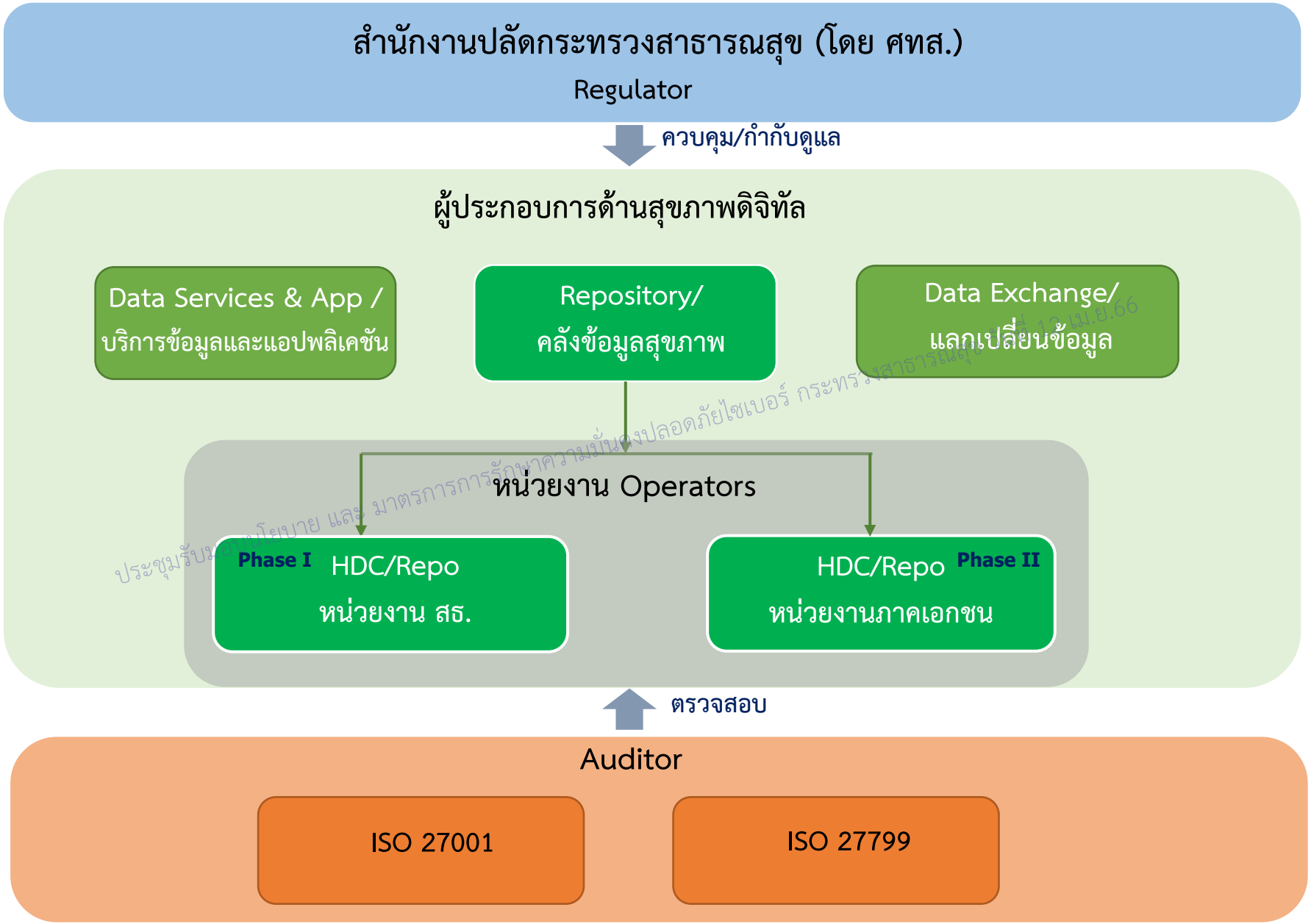
Health CERT = Healthcare Sectorial CERT
(HCERT) หมายถึง ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข
CERT = Cyber Emergency Response Team
CIRT = Cyber Incident Response Team
SOC = Security Operation Center

หมายถึง กำกับดูแล

หมายถึง ให้การสนับสนุน

จำนวน รพ. ที่ผ่านประเมิน HAIT
(Healthcare Accreditation Information Technology)
ระดับ 1 = 17
ระดับ 2 = 6
ระดับ 3 = 9
ระดับ 4 = 0
ระดับ 5 = 0
ระดับ 6 = 0

ICT MOPH Key of Success


สำนักงานปลัดกระทรวงสาธารณสุข (โดย ศทส.)
Regulator
ควบคุม/กำกับดูแล
ผู้ประกอบการด้านสุขภาพดิจิทัล
Data Services & App / บริการข้อมูลและแอปพลิเคชัน
Repository/ คลังข้อมูลสุขภาพ
Data Exchange/ แลกเปลี่ยนข้อมูล
หน่วยงาน Operators
Phase I HDC/Repo หน่วยงาน สธ.
HDC/Repo Phase II หน่วยงานภาคเอกชน
ตรวจสอบ
Auditor
ISO 27001
ISO 27799