ตัวชี้วัด 4.18 : ระดับความสำเร็จการขับเคลื่อนระดับความพร้อมรัฐบาลดิจิทัล กรมอนามัย

5. Outcome ผลลัพธ์ของตัวชี้วัดระดับความสำเร็จการขับเคลื่อนระดับความพร้อมรัฐบาลดิจิทัล กรมอนามัย

มีผลลัพธ์ตรงตามเป้าหมายที่กำหนด ระดับความสำเร็จของประเด็นการขับเคลื่อนระดับความพร้อมรัฐบาลดิจิทัล กรมอนามัย 5 ขั้นตอน (รอบที่ 1 : 5 เดือนหลัง)

คะแนน	ประเด็น
0.2	ประเด็นที่ 1
0.4	ประเด็นที่ 1 - 2
0.6	ประเด็นที่ 1 - 3
0.8	ประเด็นที่ 1 - 4
1.0	ประเด็นที่ 1 - 5

ดำเนินงานตามประเด็นการขับเคลื่อนระดับความพร้อมรัฐบาลดิจิทัล กรมอนามัย ครบทั้ง 5 ประเด็น ดังนี้

1. **การดำเนินงานด้านโครงสร้างพื้นฐานความมั่นคงปลอดภัยและมีประสิทธิภาพ (Secure and Efficient Infrastructure)**
2. **การดำเนินงานด้านธรรมาภิบาลข้อมูลภาครัฐ (Data Governance)**
3. **การดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA)**
4. **การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)**
5. **การดำเนินงานด้านเทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ (Digital Technology Practices)**

ประเด็นที่ 1 : การดำเนินงานด้านโครงสร้างพื้นฐานความมั่นคงปลอดภัยและมีประสิทธิภาพ (Secure and Efficient Infrastructure)

กรมอนามัยมีภารกิจสำคัญในการพัฒนาโครงสร้างพื้นฐานให้มีความมั่นคงปลอดภัยและมีประสิทธิภาพ เพื่อสนับสนุนการดำเนินงานด้านสาธารณสุขให้เป็นไปอย่างมีประสิทธิภาพ และรองรับการพัฒนาระบบดิจิทัลขององค์กรให้ทันสมัยและสอดคล้องกับนโยบายของรัฐบาล

1. มาตรการที่ดำเนินการ

- การเสริมสร้างความมั่นคงปลอดภัยของระบบเครือข่าย
- ติดตั้งระบบ Firewall และ Intrusion Detection System (IDS) เพื่อป้องกันภัยคุกคามทางไซเบอร์
- ใช้มาตรการควบคุมการเข้าถึงระบบสารสนเทศผ่านการยืนยันตัวตนแบบสองขั้นตอน (2FA)
- การพัฒนาโครงสร้างพื้นฐานด้านดิจิทัล
- ปรับปรุงระบบ Data Center ให้สามารถรองรับการทำงานของหน่วยงานได้อย่างมีเสถียรภาพ
- ใช้เทคโนโลยี Cloud Computing เพื่อเพิ่มความยืดหยุ่นและประสิทธิภาพของระบบสารสนเทศ

2. มาตรการสำรองข้อมูลและกู้คืนระบบ

- ดำเนินการสำรองข้อมูลอัตโนมัติ (Automated Backup) และจัดทำแผนกู้คืนระบบ (Disaster Recovery Plan) เพื่อรับมือกับสถานการณ์ฉุกเฉิน
- ทดสอบแผนสำรองข้อมูลและแผนกู้คืนระบบเป็นประจำ

3. ผลลัพธ์ที่ได้รับ

- ความมั่นคงปลอดภัยของระบบสารสนเทศได้รับการยกระดับ ลดความเสี่ยงจากภัยคุกคามไซเบอร์
- โครงสร้างพื้นฐานที่ได้รับการพัฒนาทำให้การให้บริการสาธารณสุขมีประสิทธิภาพมากขึ้น
- ระบบเครือข่ายและศูนย์ข้อมูลมีเสถียรภาพ รองรับปริมาณการใช้งานที่เพิ่มขึ้น
- สามารถสำรองข้อมูลและกู้คืนระบบได้อย่างรวดเร็ว ลดผลกระทบจากความล้มเหลวของระบบ

4. แนวทางพัฒนาต่อไป

- ขยายขีดความสามารถของระบบโครงสร้างพื้นฐานให้รองรับการใช้งานที่เพิ่มขึ้น
- พัฒนามาตรการรักษาความปลอดภัยให้สอดคล้องกับมาตรฐานสากล เช่น ISO 27001
- ส่งเสริมการใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) และ Big Data Analytics ในการบริหารจัดการข้อมูลด้านสุขภาพ

โครงสร้างพื้นฐานให้มีความมั่นคงปลอดภัยและมีประสิทธิภาพอย่างต่อเนื่อง ซึ่งช่วยเพิ่มประสิทธิภาพการทำงานของหน่วยงานและส่งเสริมการให้บริการสาธารณสุขที่มีคุณภาพแก่ประชาชน ทั้งนี้ กรมอนามัยจะยังคงมุ่งเน้นการพัฒนาเทคโนโลยีสารสนเทศและระบบความปลอดภัยเพื่อรองรับการเปลี่ยนแปลงในอนาคต

ประเด็นที่ 2 : การดำเนินงานด้านธรรมาภิบาลข้อมูลภาครัฐ (Data Governance)

กรมอนามัยได้ดำเนินการส่งเสริมธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) ตามแนวนโยบายรัฐบาลดิจิทัลและหลักการของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) โดยมีผลการดำเนินงานที่สำคัญ ดังนี้:

1. การจัดตั้งคณะทำงาน

จัดตั้งคำสั่ง คณะกรรมการปฏิรูประบบเทคโนโลยีดิจิทัลและสารสนเทศ กรมอนามัย โดยดำเนินการด้านธรรมาภิบาลข้อมูลกรมอนามัยร่วมด้วย โดยมีผู้บริหารระดับสูงเป็นประธาน และมีผู้แทนจากหน่วยงานต่าง ๆ ร่วมเป็นกรรมการ กำหนดบทบาทหน้าที่ เช่น การกำกับดูแลการจัดการข้อมูล การกำหนดนโยบายและมาตรฐานข้อมูลของกรมอนามัย

สำเนาคู่ฉบับ

คำสั่งกรมอนามัย
ที่ ๙๑๐๙/๒๕๖๗
เรื่อง แต่งตั้งคณะกรรมการปฏิรูประบบเทคโนโลยีดิจิทัลและสารสนเทศกรมอนามัย

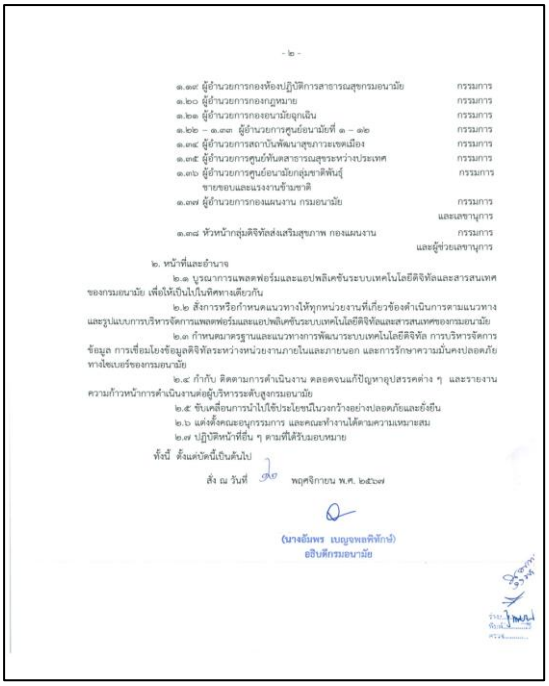
ด้วยสถานการณ์โลกด้านสุขภาพ มีการเปลี่ยนแปลงอย่างรวดเร็วในทุกมิติ แนวโน้มสุขภาพของประชาชนไทยในอนาคตมีความซับซ้อน หน่วยงานที่เกี่ยวข้องในระบบสุขภาพ ต้องเร่งบูรณาการเทคโนโลยีดิจิทัล เพื่อเพิ่มขีดความสามารถในการปรับเปลี่ยนระบบการดูแลสุขภาพคนไทยให้เป็นดิจิทัล ที่ยึดประชาชนเป็นศูนย์กลาง เพื่อเตรียมความพร้อมในการปรับตัวด้านการนำเทคโนโลยีและนวัตกรรมดิจิทัลมาพัฒนาการกิจการส่งเสริมสุขภาพและอนามัยสิ่งแวดล้อม และยกระดับให้ระบบการปฏิบัติงานของกรมอนามัยก้าวสู่ระบบการปฏิบัติงานแบบดิจิทัล ที่สามารถส่งเสริมให้คนไทยมีสุขภาพดีอย่างยั่งยืน

อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ แก้ไขเพิ่มเติม โดยพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ. ๒๕๔๕ อธิบดีกรมอนามัยจึงแต่งตั้งคณะกรรมการปฏิรูประบบเทคโนโลยีดิจิทัลและสารสนเทศกรมอนามัย โดยมีองค์ประกอบ หน้าที่และอำนาจ ดังนี้

๑. องค์ประกอบ

๑.๑	นางอัมพร เบญจพลพิทักษ์ อธิบดีกรมอนามัย	ประธาน
๑.๒	นางนงนุช ภัทรอนันตนท รองอธิบดีกรมอนามัย	รองประธาน
๑.๓	นายปองพล วรปาณี รองอธิบดีกรมอนามัย	รองประธาน
๑.๔	นายธิติ แสวงธรรม รองอธิบดีกรมอนามัย	รองประธาน
๑.๕	รองอธิบดีกรมอนามัย	รองประธาน
๑.๖	ประธานคณะกรรมการผู้ทรงคุณวุฒิ	กรรมการ
๑.๗	ผู้อำนวยการกองคลัง	กรรมการ
๑.๘	ผู้อำนวยการสำนักส่งเสริมสุขภาพ	กรรมการ
๑.๙	ผู้อำนวยการสำนักโภชนาการ	กรรมการ
๑.๑๐	ผู้อำนวยการสำนักอนามัยการเจริญพันธุ์	กรรมการ
๑.๑๑	ผู้อำนวยการกองกิจกรรมทางกายเพื่อสุขภาพ	กรรมการ
๑.๑๒	ผู้อำนวยการสำนักทันตสาธารณสุข	กรรมการ
๑.๑๓	ผู้อำนวยการสำนักอนามัยผู้สูงอายุ	กรรมการ
๑.๑๔	ผู้อำนวยการกองส่งเสริมความรอบรู้และสื่อสารสุขภาพ	กรรมการ
๑.๑๕	ผู้อำนวยการสถาบันเวชศาสตร์วิถีชีวิต	กรรมการ
๑.๑๖	ผู้อำนวยการสำนักอนามัยสิ่งแวดล้อม	กรรมการ
๑.๑๗	ผู้อำนวยการสำนักสุขาภิบาลอาหารและน้ำ	กรรมการ
๑.๑๘	ผู้อำนวยการกองประเมินผลกระทบต่อสุขภาพ	กรรมการ

๑.๑๙ ผู้อำนวยการ



- ๒ -

๑.๑๙ ผู้อำนวยการกองห้องปฏิบัติการสาธารณสุขกรมอนามัย	กรรมการ
๑.๒๐ ผู้อำนวยการกองกฎหมาย	กรรมการ
๑.๒๑ ผู้อำนวยการกองอนามัยอุตุนเย็น	กรรมการ
๑.๒๒ – ๑.๓๓ ผู้อำนวยการศูนย์อนามัยที่ ๑ – ๑๒	กรรมการ
๑.๓๔ ผู้อำนวยการสถาบันพัฒนาสุขภาวะเขตเมือง	กรรมการ
๑.๓๕ ผู้อำนวยการศูนย์ทันตสาธารณสุขระหว่างประเทศ	กรรมการ
๑.๓๖ ผู้อำนวยการศูนย์อนามัยกลุ่มชาติพันธุ์ ชายขอบและแรงงานข้ามชาติ	กรรมการ
๑.๓๗ ผู้อำนวยการกองแผนงาน กรมอนามัย	กรรมการ และเลขานุการ
๑.๓๘ หัวหน้ากลุ่มดิจิทัลส่งเสริมสุขภาพ กองแผนงาน	กรรมการ และผู้ช่วยเลขานุการ

๒. หน้าที่และอำนาจ

๒.๑ บูรณาการแพลตฟอร์มและแอปพลิเคชันระบบเทคโนโลยีดิจิทัลและสารสนเทศของกรมอนามัย เพื่อให้เป็นไปในทิศทางเดียวกัน

๒.๒ สั่งการหรือกำหนดแนวทางให้ทุกหน่วยงานที่เกี่ยวข้องดำเนินการตามแนวทางและรูปแบบการบริหารจัดการแพลตฟอร์มและแอปพลิเคชันระบบเทคโนโลยีดิจิทัลและสารสนเทศของกรมอนามัย

๒.๓ กำหนดมาตรฐานและแนวทางการพัฒนาระบบเทคโนโลยีดิจิทัล การบริหารจัดการข้อมูล การเชื่อมโยงข้อมูลดิจิทัลระหว่างหน่วยงานภายในและภายนอก และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกรมอนามัย

๒.๔ กำกับ ติดตามการดำเนินงาน ตลอดจนแก้ปัญหาอุปสรรคต่าง ๆ และรายงานความก้าวหน้าการดำเนินงานต่อผู้บริหารระดับสูงกรมอนามัย

๒.๕ ขับเคลื่อนการนำไปใช้ประโยชน์ในวงกว้างอย่างปลอดภัยและยั่งยืน

๒.๖ แต่งตั้งคณะอนุกรรมการ และคณะทำงานได้ตามความเหมาะสม

๒.๗ ปฏิบัติหน้าที่อื่น ๆ ตามที่ได้รับมอบหมาย

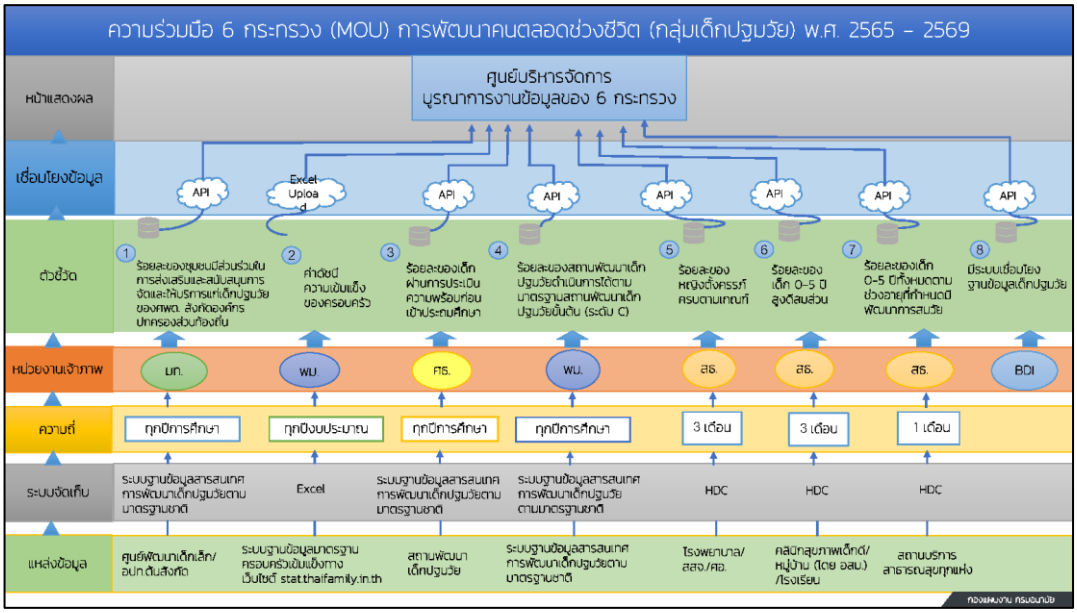
ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑๑ พฤศจิกายน พ.ศ. ๒๕๖๗

(นางอัมพร เบญจพลพิทักษ์)
อธิบดีกรมอนามัย

2. การจัดทำแผนธรรมาภิบาลข้อมูล

จัดทำ “แผนแม่บทธรรมาภิบาลข้อมูล” ของกรมอนามัย เพื่อใช้เป็นกรอบในการบริหารจัดการข้อมูลระบุเป้าหมายด้านคุณภาพข้อมูล การแบ่งปันข้อมูล และการรักษาความมั่นคงปลอดภัยของข้อมูล



ที่มาข้อมูล : กรอบความร่วมมือการเชื่อมโยงข้อมูลกรมอนามัยกับหน่วยงานภาคีเครือข่ายภายนอก

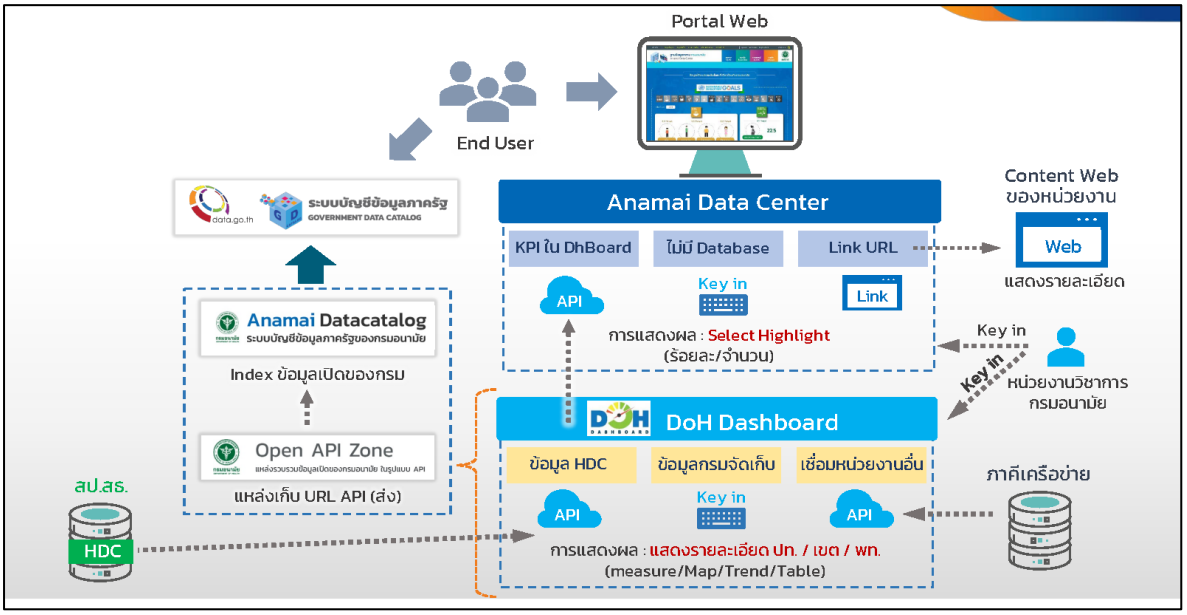
3. การบริหารจัดการข้อมูลและการขึ้นทะเบียนข้อมูล (Data Catalog)

สำรวจและขึ้นทะเบียนชุดข้อมูลหลัก (Master Data) และข้อมูลสำคัญ (Critical Data) ที่อยู่ภายใต้ความรับผิดชอบของกรมจัดทำ Data Catalog เพื่อเป็นฐานข้อมูลกลางในการบริหารจัดการและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

ที่มาข้อมูล : https://datacatalog.anamai.moph.go.th/

4. การกำหนดมาตรฐานและคุณภาพข้อมูล

กำหนดหลักเกณฑ์การตรวจสอบคุณภาพข้อมูล เช่น ความครบถ้วน ความถูกต้อง ความทันสมัยดำเนินการประเมินคุณภาพข้อมูลจากระบบสารสนเทศภายในอย่างสม่ำเสมอ



5. การคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัย ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

จัดให้มีการวางแนวทางการรักษาความปลอดภัยข้อมูลตามกรอบ PDPA และหลัก Cybersecurity

ประกาศกรมอนามัย
เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
และคำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice)

ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้กำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลของกรมอนามัยเป็นไปอย่างมีประสิทธิภาพ สามารถปฏิบัติตามได้อย่างเป็นรูปธรรม นั้น

ฉะนั้น อาศัยอำนาจตามความในมาตรา ๗๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม และมาตรา ๒๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ อธิบดีกรมอนามัยจึงออกประกาศไว้ ดังต่อไปนี้

๑. นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) กรมอนามัย
๒. คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) กรมอนามัย

ประกาศ ณ วันที่ ๒๙ ธันวาคม พ.ศ. ๒๕๖๗

(นางอัมพร เบญจพลพิทักษ์)
อธิบดีกรมอนามัย

กรมอนามัย
Department of Health

คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) กรมอนามัย
(สำหรับการบริการส่งเสริมสุขภาพและอนามัยสิ่งแวดล้อม การแพทย์และสาธารณสุข)

กรมอนามัย ตระหนักและให้ความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของผู้มาติดต่อและใช้บริการของกรมอนามัย (“ท่าน”) โดยกรมจะดูแลและบริหารจัดการข้อมูลส่วนบุคคลของท่านอย่างโปร่งใส เป็นธรรม และเป็นไปตามข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคลรวมถึงกฎหมายอื่นที่เกี่ยวข้อง

โดยประกาศความเป็นส่วนตัวนี้ (“ประกาศ”) จะแจ้งให้ท่านทราบถึงวิธีการที่กรมอนามัยเก็บรวบรวม ใช้ เปิดเผย และปกป้องดูแลข้อมูลส่วนบุคคลของท่าน

กรมอนามัยขอแนะนำให้ท่านอ่านและทำความเข้าใจประกาศนี้ก่อนให้ข้อมูลส่วนบุคคลกับกรมอนามัย หากท่านมีข้อกังวล ข้อสงสัยหรือต้องการสอบถามข้อมูลเพิ่มเติมเกี่ยวกับประกาศนี้ตลอดจนถึงประกาศและนโยบายอื่น ๆ ที่เกี่ยวข้อง โปรดติดต่อกรมอนามัยตามช่องทางการติดต่อที่ปรากฏท้ายประกาศนี้

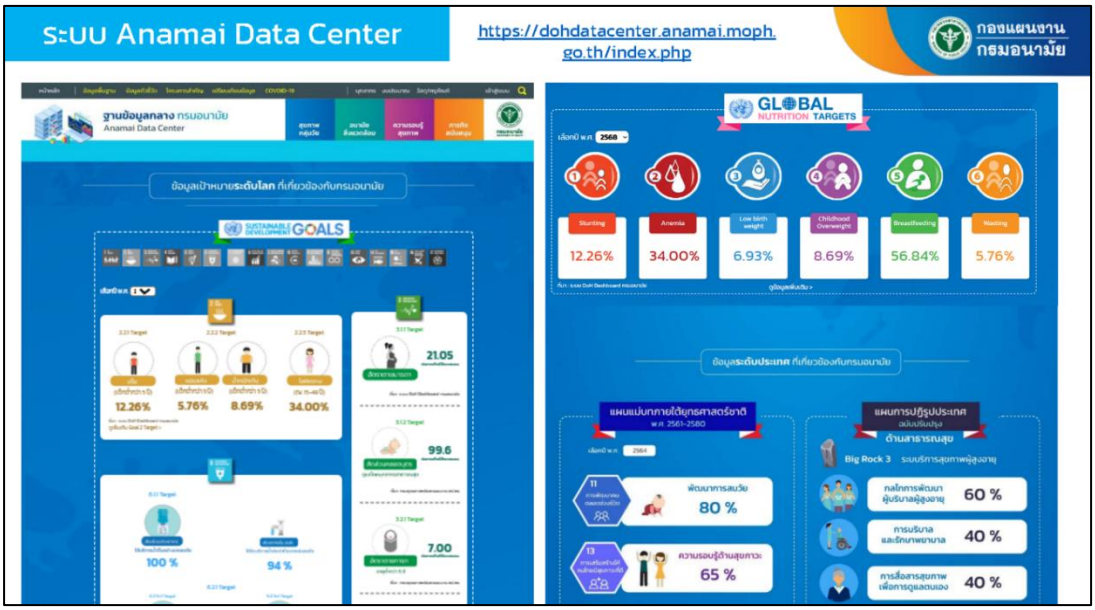
กรมอนามัยในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อให้การประมวลผลข้อมูลส่วนบุคคล เป็นไปตามที่กฎหมายกำหนด ทั้งนี้กรมอนามัยดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของท่าน ดังนี้

๑. การเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูล

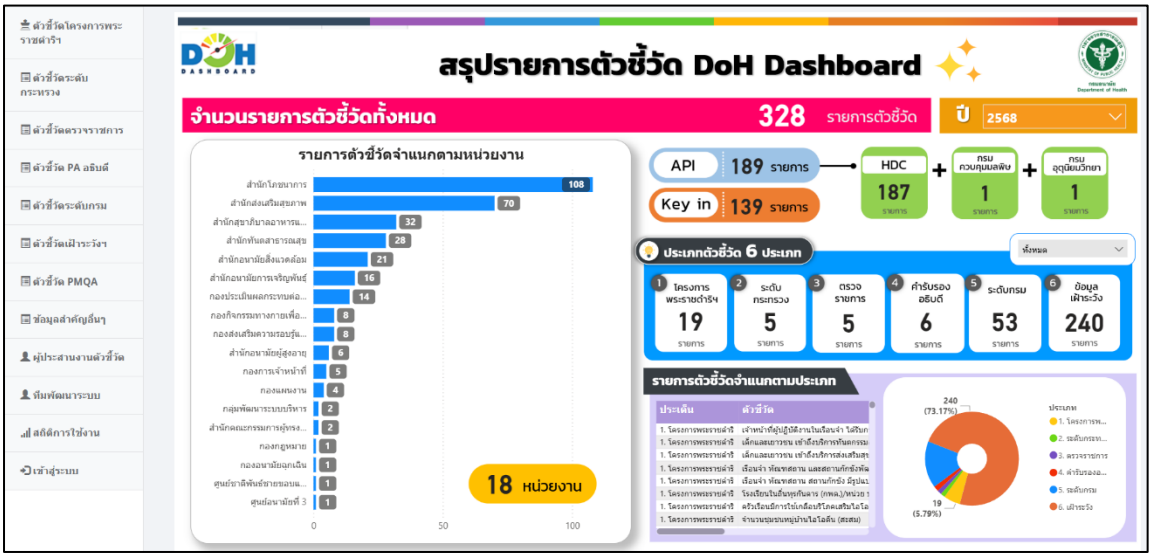
กรมอนามัยจะเก็บรวบรวมข้อมูลส่วนบุคคลและข้อมูลสุขภาพจากเจ้าของข้อมูลโดยตรง และอาจเก็บข้อมูลส่วนบุคคลและข้อมูลสุขภาพทางอ้อมจากข้อมูลที่เจ้าของข้อมูลหรือตัวแทนของเจ้าของข้อมูลให้ไว้กับกรมอนามัย หรือผู้มีส่วนเกี่ยวข้องกับเจ้าของข้อมูล โรงพยาบาลหรือหน่วยงานภายในอื่น ๆ ของกรมอนามัย หน่วยงานพันธมิตร การให้บริการทางโทรศัพท์ บริการทางด้านดิจิทัลต่าง ๆ ของกรมอนามัย รวมถึง การใช้งานเว็บไซต์ การดาวน์โหลดข้อมูลจากแอปพลิเคชันจากแหล่งข้อมูลอื่นใดที่เชื่อถือได้ เช่น สมาคมองค์กรของรัฐ หน่วยงานภาครัฐ องค์กรเอกชน งานสัมมนา งานฝึกอบรม งานออกร้าน ทั้งที่กรมอนามัยจัดขึ้นเองหรือองค์กรภาครัฐ และภาคเอกชนอื่น ๆ รวมไปถึงสื่อสังคมออนไลน์ต่าง ๆ เป็นต้น ทั้งนี้เป็นไปเพื่อประโยชน์ในการให้บริการสุขภาพและเพื่อการดูแลสุขภาพของเจ้าของข้อมูล ตามภารกิจภายใต้อำนาจหน้าที่ของกรมอนามัย

6. การใช้ข้อมูลในการตัดสินใจเชิงนโยบาย

นำข้อมูลสุขภาพที่มีคุณภาพมาสนับสนุนการตัดสินใจด้านนโยบาย เช่น การวิเคราะห์ข้อมูล Open Data, การจัดทำ Dashboard สำหรับผู้บริหาร ส่งเสริมการใช้ข้อมูลเพื่อเพิ่มประสิทธิภาพในการให้บริการประชาชน



ที่มาข้อมูล : https://dohdatacenter.anamai.moph.go.th/index.php



ที่มาข้อมูล : https://dashboard.anamai.moph.go.th/

7. การส่งเสริมวัฒนธรรมข้อมูล (Data Culture)

พัฒนาทักษะให้ความรู้ด้านธรรมาภิบาลข้อมูลแก่บุคลากรของกรมส่งเสริมให้มีการใช้ข้อมูลในการทำงานเชิงรุกและมีความรับผิดชอบต่อข้อมูล ผู้เข้าร่วมการประชุมประกอบด้วยนักวิชาการ ผู้ปฏิบัติงานด้านข้อมูล และบุคลากรที่เกี่ยวข้องจากหน่วยงานส่วนกลางและส่วนภูมิภาคของกรมอนามัย รวมทั้งสิ้น 50 ท่าน โดยมีเป้าหมายเพื่อพัฒนาทักษะด้านการวิเคราะห์ข้อมูลและเสริมสร้างความสามารถในการคาดการณ์สถานการณ์สำคัญ เพื่อใช้ในการสนับสนุนการดำเนินงานของกรมอนามัยในอนาคต

https://planning.anamai.moph.go.th

ภาพข่าวกิจกรรม

ANAMA NEWS

กองแผนงาน Planning Division

ฉบับที่ 006/2567

การประชุมเชิงปฏิบัติการพัฒนาศักยภาพสู่การเป็นนักวิทยาการข้อมูลภาครัฐ (Data Scientist) ด้านการวิเคราะห์ข้อมูลและคาดการณ์สถานการณ์ในประเด็นข้อมูลสำคัญของกรมอนามัย

ณ โรงแรมเซ็นทารา อยุธยา จังหวัดพระนครศรีอยุธยา

กองแผนงาน กรมอนามัย จัดการประชุมเชิงปฏิบัติการพัฒนาศักยภาพสู่การเป็นนักวิทยาการข้อมูลภาครัฐ (Data Scientist) ในด้านการวิเคราะห์ข้อมูลและคาดการณ์สถานการณ์ในประเด็นข้อมูลสำคัญของกรมอนามัย ในวันที่ 23-25 ธันวาคม 2567

โดยมี ดร.นายแพทย์ปองพล วรปาณี รองอธิบดีกรมอนามัย เป็นประธานในพิธีเปิดการประชุมการประชุมครั้งนี้ได้รับเกียรติจาก ดร.ปริสุทธิ์ จิตต์ภักดี ผู้จัดการอบรมและพัฒนาการจัดการข้อมูล สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน) หรือ Big Data Institute (BDI) พร้อมด้วยทีมงาน มาเป็นวิทยากรบรรยายและสอนการใช้เครื่องมือวิเคราะห์ข้อมูลเชิงลึก

ผู้เข้าร่วมการประชุมประกอบด้วยนักวิชาการ ผู้ปฏิบัติงานด้านข้อมูล และบุคลากรที่เกี่ยวข้องจากหน่วยงานส่วนกลางและส่วนภูมิภาคของกรมอนามัย รวมทั้งสิ้น 50 ท่าน โดยมีเป้าหมายเพื่อพัฒนาทักษะด้านการวิเคราะห์ข้อมูลและเสริมสร้างความสามารถในการคาดการณ์สถานการณ์สำคัญ เพื่อใช้ในการสนับสนุนการดำเนินงานของกรมอนามัยในอนาคต

การประชุมครั้งนี้ถือเป็นก้าวสำคัญในการส่งเสริมการพัฒนาศักยภาพบุคลากรของกรมอนามัยให้สามารถใช้ข้อมูลเชิงลึกในการบริหารจัดการและตัดสินใจอย่างมีประสิทธิภาพ รองรับการเปลี่ยนแปลงและความท้าทายที่เกิดขึ้นในยุคดิจิทัล.

กรมอนามัยส่งเสริมให้คนไทยสุขภาพดี

FIND ME ON FACEBOOK @PlanningDOH

FIND ME ON WEBSITE @กองแผนงาน กรมอนามัย

จัดทำโดย กลุ่มพัฒนาระบบข้อมูล โทร. 0-2590-4301

ประเด็นที่ 3 : การดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

3.1 ดำเนินการจัดประชุมเชิงปฏิบัติการ เรื่อง “การพัฒนาศักยภาพภาคีเครือข่ายบุคลากรด้านเทคโนโลยีดิจิทัลกรมอนามัย ปี 2568” ระหว่างวันที่ 24 – 26 กุมภาพันธ์ 2568 ณ บ้านริมแคว แพริมน้ำ รีสอร์ท อ.ไทรโยค จ.กาญจนบุรี โดยมีการการบรรยาย เรื่อง “PDPA กับหน่วยงานภาครัฐ : แนวทางการปฏิบัติตามกฎหมายอย่างมีประสิทธิภาพ” และ ฝึกปฏิบัติ เรื่อง “สร้าง ROPA ฉบับสมบูรณ์ : แนวทางการจัดทำบันทึกรายการกิจกรรมประมวลผลข้อมูลส่วนบุคคล” วิทยากรจาก บริษัท โทรคมนาคมแห่งชาติ จำกัด ซึ่งมีหน่วยงานสังกัดกรมอนามัยเข้าร่วมรับฟังและฝึกปฏิบัติ มีรายละเอียด ดังนี้

กรมอนามัยในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มีหน้าที่ในการคุ้มครองและรักษาความปลอดภัยของข้อมูลส่วนบุคคล และกำหนดมาตรฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย เพื่อสร้างความเชื่อมั่นให้แก่ประชาชนและภาคธุรกิจ

1. กฎหมายที่เกี่ยวข้อง

1.1 พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.2 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.3 พ.ร.บ. บริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

1.4 พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

1.5 พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ 2560

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 32 กำหนดให้บุคคลมีสิทธิในความเป็นส่วนตัวและได้รับความคุ้มครองจากการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นหลักการสำคัญที่นำไปสู่การตรา พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้เกิดการคุ้มครองสิทธิของเจ้าของข้อมูลอย่างมีประสิทธิภาพ

2. การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

PDPA บังคับใช้กับบุคคลหรือนิติบุคคลที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล ไม่ว่าจะอยู่ในรูปแบบอิเล็กทรอนิกส์หรือไม่ก็ตาม โดยผู้อยู่ภายใต้ข้อบังคับตามกฎหมาย ได้แก่

- องค์กรภาครัฐและภาคเอกชน ซึ่งอยู่ในราชอาณาจักร

- ผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งอยู่ในราชอาณาจักร หรือแม้อยู่ต่างประเทศแต่ให้บริการแก่บุคคลในประเทศไทย

3. ข้อมูลส่วนบุคคล

ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้โดยตรงหรือโดยอ้อม เช่น ชื่อ-นามสกุล เลขประจำตัวประชาชน หมายเลขโทรศัพท์ อีเมล หรือข้อมูลชีวภาพ เป็นต้น

3.1 ข้อมูลส่วนบุคคล แบ่งเป็น 2 ประเภท ดังนี้

- ข้อมูลส่วนบุคคลทั่วไป (General Personal Data)
- ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ตามมาตรา 26 เช่น เชื้อชาติ ศาสนา ข้อมูลสุขภาพ ข้อมูลชีวภาพ เป็นต้น

4. ผู้ที่มีส่วนเกี่ยวข้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) ได้แก่

4.1 เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือ บุคคลที่ข้อมูลส่วนบุคคลของเขาถูกเก็บรวบรวม ใช้ หรือเปิดเผย เช่น ลูกค้า ผู้ป่วย พนักงาน หรือประชาชนทั่วไป

4.2 ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือ หน่วยงานหรือบุคคลที่กำหนดวัตถุประสงค์และวิธีการใช้ข้อมูลส่วนบุคคล เช่น โรงพยาบาล ธนาคาร บริษัทเอกชน หรือหน่วยงานรัฐที่เก็บข้อมูลประชาชน

4.3 ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือ หน่วยงานหรือบุคคลที่ดำเนินการประมวลผลข้อมูลตามคำสั่งของผู้ควบคุมข้อมูล เช่น บริษัทให้บริการคลาวด์ ผู้ให้บริการด้าน IT หรือบริษัทภายนอกที่ช่วยบริหารระบบเงินเดือน

4.4 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer - DPO) คือ บุคคลที่องค์กรแต่งตั้งให้ดูแลและตรวจสอบการปฏิบัติตามกฎหมาย PDPA โดยเฉพาะองค์กรที่เก็บข้อมูลจำนวนมากหรือข้อมูลอ่อนไหว

4.5 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) คือ หน่วยงานของรัฐที่มีหน้าที่กำกับดูแล ให้คำแนะนำ และบังคับใช้กฎหมาย PDPA รวมถึงพิจารณาโทษเมื่อมีการละเมิดข้อมูล

5. บันทึกข้อตกลงการประมวลผลข้อมูล (DPA : Data Processing Agreement)

DPA คือ ข้อตกลงทางกฎหมายระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล เพื่อกำหนดข้อกำหนดและแนวทางปฏิบัติในการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

6. วงจรชีวิตของข้อมูล (Data Life Cycle) ประกอบด้วย

- การเก็บรวบรวมข้อมูล
- การจัดเก็บและรักษาข้อมูล
- การใช้ข้อมูล
- การแบ่งปันและถ่ายโอนข้อมูล
- การทำลายข้อมูล

7. ROPA (Record of Processing Activities)

บันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล เป็นเอกสารที่องค์กรต้องจัดทำและบันทึกไว้ เพื่อ แสดงต่อเจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ และเป็นหลักฐานว่าองค์กรปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูล

7.1 องค์ประกอบของ RoPA ดังนี้

- ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
- การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม
- การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และมาตรา 36 วรรคหนึ่ง
- คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)

8. ประกาศความเป็นส่วนตัว (Privacy Notice) และ นโยบายความเป็นส่วนตัว (Privacy Policy)

- Privacy Notice: การแจ้งให้เจ้าของข้อมูลทราบถึงวิธีการและเหตุผลในการประมวลผลข้อมูล
- Privacy Policy: นโยบายขององค์กรที่กำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคล

9. ตกลงการประมวลผลข้อมูล (Data Processing Agreement)

ข้อตกลงระหว่าง ผู้ควบคุมข้อมูล (Data Controller) และ ผู้ประมวลผลข้อมูล (Data Processor) ที่กำหนดเงื่อนไขการประมวลผลข้อมูลส่วนบุคคล เช่น วัตถุประสงค์ในการใช้ข้อมูล มาตรการรักษาความปลอดภัย การรายงานข้อมูลรั่วไหล และการจัดการสิทธิของเจ้าของข้อมูล ข้อตกลงนี้ช่วยให้การประมวลผลข้อมูลเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น GDPR หรือ PDPA

3.2 ดำเนินการจัดทำนโยบายและมาตรการการปกป้องข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย PDPA และแจ้งเวียนให้ทุกหน่วยงานรับทราบและถือปฏิบัติ

ประกาศกรมอนามัย
เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
และคำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice)

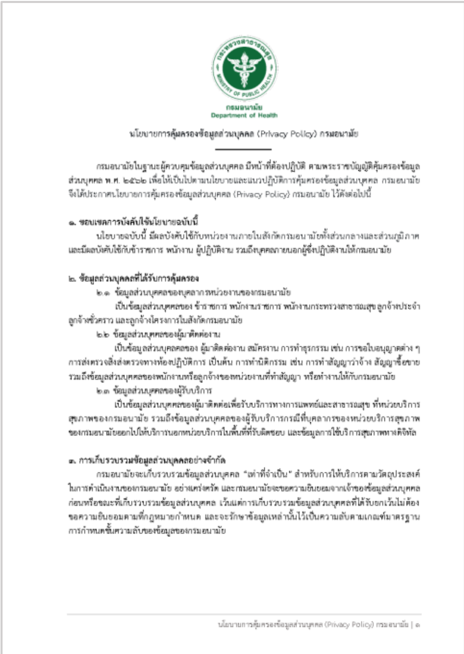
ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้กำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลของกรมอนามัยเป็นไปอย่างมีประสิทธิภาพ สามารถปฏิบัติตามได้อย่างเป็นรูปธรรม นั้น

ฉะนั้น อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม และมาตรา ๒๓ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ อธิบดีกรมอนามัยจึงออกประกาศไว้ ดังต่อไปนี้

๑. นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) กรมอนามัย
๒. คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) กรมอนามัย

ประกาศ ณ วันที่ ๒๑ ธันวาคม พ.ศ. ๒๕๖๗

(นางอัมพร เบญจพลพิทักษ์)
อธิบดีกรมอนามัย



กรมอนามัย
Department of Health
นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) กรมอนามัย

กรมอนามัย
Department of Health
คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) กรมอนามัย

3.2 สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้กับเจ้าหน้าที่ของกรมอนามัย

การจัดประชุมซักซ้อมแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และการกู้คืนข้อมูล มีรายละเอียด ดังนี้

1. สร้างความเข้าใจเกี่ยวกับอันตรายจากการโจมตีทางไซเบอร์ สามารถเกิดขึ้นได้ทุกเมื่อและมีผลกระทบที่หลากหลาย

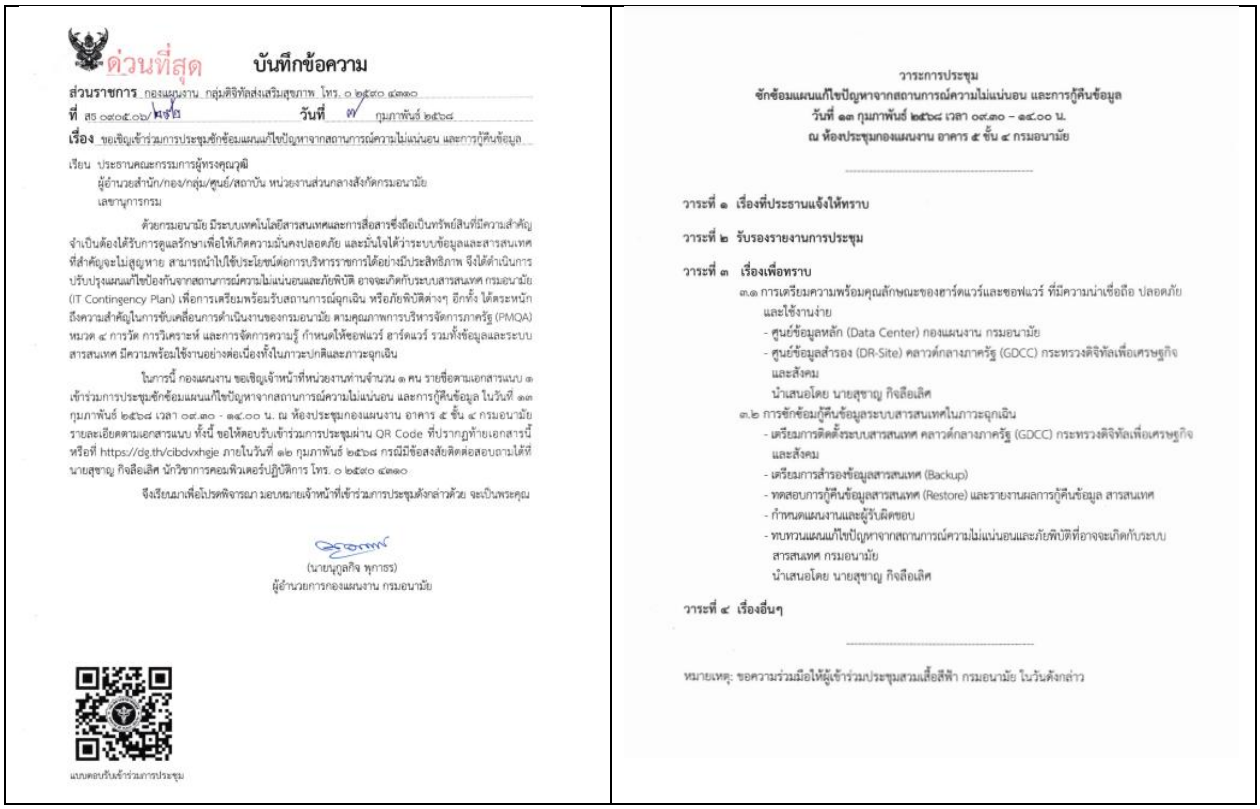
2. การเข้าใจเกี่ยวกับมาตรการป้องกัน โดยอธิบายหรือแสดงให้เห็นถึงมาตรการที่สามารถใช้ป้องกันการโจมตีทางไซเบอร์ เช่น การใช้รหัสผ่านที่ปลอดภัย การป้องกันมัลแวร์ และการอัพเดตซอฟต์แวร์ เป็นต้น

3. สร้างทักษะในการระมัดระวัง โดยแนะนำหรือสอนทักษะเกี่ยวกับการระมัดระวังต่อการละเมิดความปลอดภัยที่อาจเกิดขึ้น เช่น การระวังการส่งอีเมล์แฝง การตรวจสอบลิงก์ก่อนคลิก และการระวังการใช้ข้อมูลส่วนตัว เป็นต้น

4. ส่งเสริมพฤติกรรมที่ปลอดภัย ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ เช่น การสำรวจและรายงานข้อผิดพลาด การส่งรายงานการบุกรุกทางไซเบอร์ และการรายงานการโจมตีที่สำเร็จ เป็นต้น

5. สนับสนุนและการกำกับดูแลผู้ใช้งาน ในการปฏิบัติตามนโยบายและมาตรการที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

6. เผยแพร่ความรู้และข้อมูลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์อย่างต่อเนื่อง ผ่านช่องทางต่าง ๆ เช่น สื่อสังคมออนไลน์ อีเมล์ และการประชาสัมพันธ์ เป็นต้น



ด่วนที่สุด **บันทึกข้อความ**

ส่วนราชการ กองแผนงาน กลุ่มดิจิทัลส่งเสริมสุขภาพ โทร. ๐ ๒๕๙๐ ๔๓๓๐
ที่ สธ ๐๙๐๕.๐๒/ พิเศษ **วันที่** ๗ กุมภาพันธ์ ๒๕๖๘
เรื่อง ขอเชิญเข้าร่วมการประชุมซักซ้อมแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และการกู้คืนข้อมูล

เรียน ประธานคณะกรรมการผู้ทรงคุณวุฒิ
ผู้อำนวยสำนัก/กอง/กลุ่ม/ศูนย์/สถาบัน หน่วยงานส่วนกลางสังกัดกรมอนามัย
เลขานุการกรม

ด้วยกรมอนามัย มีระบบเทคโนโลยีสารสนเทศและการสื่อสารซึ่งถือเป็นทรัพย์สินที่มีความสำคัญจำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย และมั่นใจได้ว่าระบบข้อมูลและสารสนเทศที่สำคัญจะไม่สูญหาย สามารถนำไปใช้ประโยชน์ต่อการบริหารราชการได้อย่างมีประสิทธิภาพ จึงได้ดำเนินการปรับปรุงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ อาจจะเกิดกับระบบสารสนเทศ กรมอนามัย (IT Contingency Plan) เพื่อการเตรียมพร้อมรับสถานการณ์ฉุกเฉิน หรือภัยพิบัติต่างๆ อีกทั้ง ได้ตระหนักถึงความสำคัญในการขับเคลื่อนการดำเนินงานของกรมอนามัย ตามคุณภาพการบริหารจัดการภาครัฐ (PMQA) หมวด ๔ การวัด การวิเคราะห์ และการจัดการความรู้ กำหนดให้ซอฟแวร์ ฮาร์ดแวร์ รวมทั้งข้อมูลและระบบสารสนเทศ มีความพร้อมใช้งานอย่างต่อเนื่องทั้งในภาวะปกติและภาวะฉุกเฉิน

ในการนี้ กองแผนงาน ขอเชิญเจ้าหน้าที่หน่วยงานท่านจำนวน ๑ คน รายชื่อตามเอกสารแนบ ๑ เข้าร่วมการประชุมซักซ้อมแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และการกู้คืนข้อมูล ในวันที่ ๑๓ กุมภาพันธ์ ๒๕๖๘ เวลา ๐๙.๓๐ - ๑๔.๐๐ น. ณ ห้องประชุมกองแผนงาน อาคาร ๕ ชั้น ๔ กรมอนามัย รายละเอียดตามเอกสารแนบ ทั้งนี้ ขอให้ตอบรับเข้าร่วมการประชุมผ่าน QR Code ที่ปรากฏท้ายเอกสารนี้ หรือที่ https://dg.th/cibdvxhgje ภายในวันที่ ๑๑ กุมภาพันธ์ ๒๕๖๘ กรณีมีข้อสงสัยติดต่อสอบถามได้ที่ นายสุชาญ กิจลือเลิศ นักวิชาการคอมพิวเตอร์ปฏิบัติการ โทร. ๐ ๒๕๙๐ ๔๓๓๐

จึงเรียนมาเพื่อโปรดพิจารณา มอบหมายเจ้าหน้าที่เข้าร่วมการประชุมดังกล่าวด้วย จะเป็นพระคุณ

(นายนฤดลกิจ พุกาธร)
ผู้อำนวยการกองแผนงาน กรมอนามัย

แบบตอบรับเข้าร่วมการประชุม

วาระการประชุม
ซักซ้อมแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และการกู้คืนข้อมูล
วันที่ ๑๓ กุมภาพันธ์ ๒๕๖๘ เวลา ๐๙.๓๐ – ๑๔.๐๐ น.
ณ ห้องประชุมกองแผนงาน อาคาร ๕ ชั้น ๔ กรมอนามัย

วาระที่ ๑ เรื่องที่ประธานแจ้งให้ทราบ

วาระที่ ๒ รับรองรายงานการประชุม

วาระที่ ๓ เรื่องเพื่อทราบ
๓.๑ การเตรียมความพร้อมคุณลักษณะของฮาร์ดแวร์และซอฟแวร์ ที่มีความน่าเชื่อถือ ปลอดภัย และใช้งานง่าย
- ศูนย์ข้อมูลหลัก (Data Center) กองแผนงาน กรมอนามัย
- ศูนย์ข้อมูลสำรอง (DR-Site) คลาวด์กลางภาครัฐ (GDCC) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

นำเสนอโดย นายสุชาญ กิจลือเลิศ
๓.๒ การซักซ้อมกู้คืนข้อมูลระบบสารสนเทศในภาวะฉุกเฉิน
- เตรียมการติดตั้งระบบสารสนเทศ คลาวด์กลางภาครัฐ (GDCC) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- เตรียมการสำรองข้อมูลสารสนเทศ (Backup)
- ทดสอบการกู้คืนข้อมูลสารสนเทศ (Restore) และรายงานผลการกู้คืนข้อมูล สารสนเทศ
- กำหนดแผนงานและผู้รับผิดชอบ
- ทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ กรมอนามัย

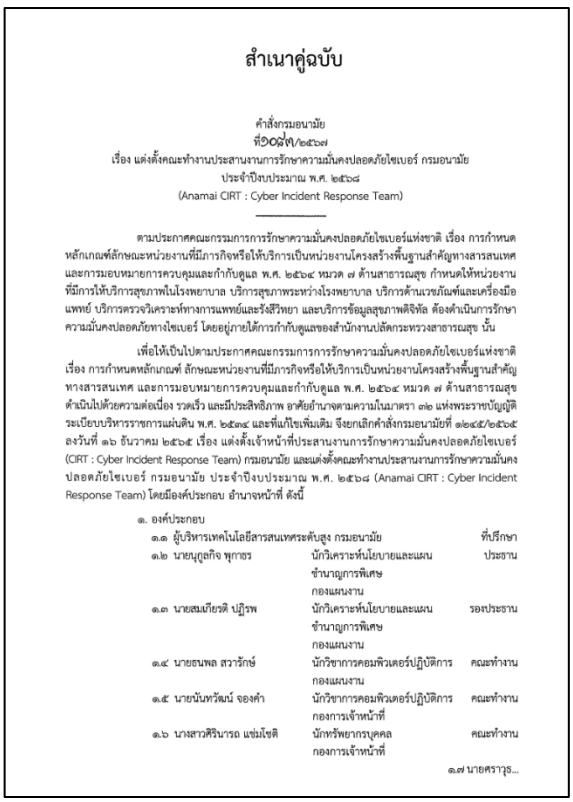
นำเสนอโดย นายสุชาญ กิจลือเลิศ

วาระที่ ๔ เรื่องอื่นๆ

หมายเหตุ: ขอความร่วมมือให้ผู้เข้าร่วมประชุมสวมเสื้อสีฟ้า กรมอนามัย ในวันดังกล่าว

ประเด็นที่ 4 : การดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

1. จัดทำคำสั่งคณะทำงานประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย (CIRT) ปี 2568



สำเนาคู่ฉบับ

คำสั่งกรมอนามัย
ที่๑๐๘๓/๒๕๖๗
เรื่อง แต่งตั้งคณะทำงานประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย
ประจำปีงบประมาณ พ.ศ. ๒๕๖๘
(Anamai CIRT : Cyber Incident Response Team)

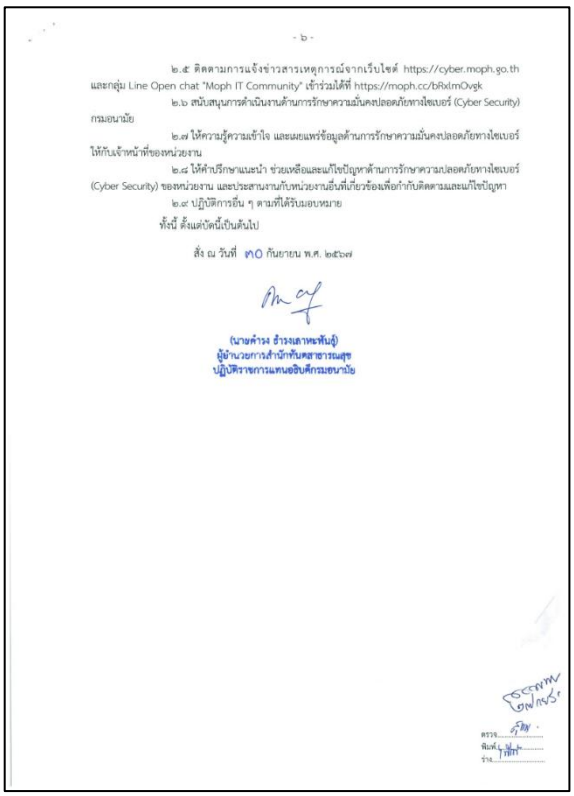
ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๗ ด้านสาธารณสุข กำหนดให้หน่วยงานที่มีการให้บริการสุขภาพในโรงพยาบาล บริการสุขภาพระหว่างโรงพยาบาล บริการด้านเวชภัณฑ์และเครื่องมือแพทย์ บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา และบริการข้อมูลสุขภาพดิจิทัล ต้องดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยอยู่ภายใต้การกำกับดูแลของสำนักงานปลัดกระทรวงสาธารณสุข นั้น

เพื่อให้เป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๗ ด้านสาธารณสุข ดำเนินไปด้วยความต่อเนื่อง รวดเร็ว และมีประสิทธิภาพ อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม จึงยกเลิกคำสั่งกรมอนามัยที่ ๑๒๔๕/๒๕๖๕ ลงวันที่ ๑๖ ธันวาคม ๒๕๖๕ เรื่อง แต่งตั้งเจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (CIRT : Cyber Incident Response Team) กรมอนามัย และแต่งตั้งคณะทำงานประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมอนามัย ประจำปีงบประมาณ พ.ศ. ๒๕๖๘ (Anamai CIRT : Cyber Incident Response Team) โดยมีองค์ประกอบ อำนาจหน้าที่ ดังนี้

๑. องค์ประกอบ

๑.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง กรมอนามัย		ที่ปรึกษา
๑.๒ นายนฤดลกิจ พุกาธร	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กองแผนงาน	ประธาน
๑.๓ นายสมเกียรติ ปฏิรูพ	นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ กองแผนงาน	รองประธาน
๑.๔ นายธนพล สวารักษ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองแผนงาน	คณะทำงาน
๑.๕ นายนันทวัฒน์ จองคำ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ กองการเจ้าหน้าที่	คณะทำงาน
๑.๖ นางสาวศิรินารถ แข่มโชติ	นักทรัพยากรบุคคล กองการเจ้าหน้าที่	คณะทำงาน

๑.๗ นายศราวุธ...



- ๖ -

๒.๕ ติดตามการแจ้งข่าวสารเหตุการณ์จากเว็บไซต์ https://cyber.moph.go.th และกลุ่ม Line Open chat "Moph IT Community" เข้าร่วมได้ที่ https://moph.cc/bRxlmOvgk
๒.๖ สนับสนุนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) กรมอนามัย
๒.๗ ให้ความรู้ความเข้าใจ และแลกเปลี่ยนข้อมูลด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับเจ้าหน้าที่ของหน่วยงาน
๒.๘ ให้คำปรึกษาแนะนำ ช่วยเหลือและแก้ไขปัญหาด้านการรักษาความปลอดภัยทางไซเบอร์ (Cyber Security) ของหน่วยงาน และประสานงานกับหน่วยงานอื่นที่เกี่ยวข้องเพื่อกำกับติดตามและแก้ไขปัญหา
๒.๙ ปฏิบัติการอื่น ๆ ตามที่ได้รับมอบหมาย

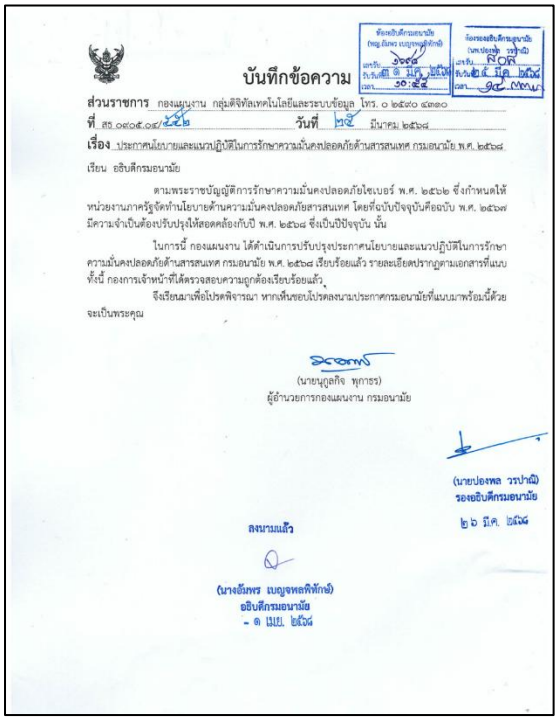
ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๗

(นายคำนวง อำนวยเลาหะพันธุ์)
ผู้อำนวยการสำนักทันตสาธารณสุข
ปฏิบัติราชการแทนอธิบดีกรมอนามัย

ที่มาข้อมูล : คำสั่งกรมอนามัย ที่ 1083/2568 ลงวันที่ 30 กันยายน 2567

2. จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมอนามัย พ.ศ. 2568



บันทึกข้อความ

ส่วนราชการ กองแผนงาน กลุ่มดิจิทัลเทคโนโลยีและระบบข้อมูล โทร. ๐ ๒๕๙๐ ๔๓๓๐

ที่ สธ ๐๔๐๕.๐๔/๕๕๒ วันที่ ๒๕ มีนาคม ๒๕๖๘

เรื่อง ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมอนามัย พ.ศ. ๒๕๖๘

เรียน อธิบดีกรมอนามัย

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งกำหนดให้หน่วยงานภาครัฐจัดทำนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ โดยที่ฉบับปัจจุบันคือฉบับ พ.ศ. ๒๕๖๗ มีความจำเป็นต้องปรับปรุงให้สอดคล้องกับปี พ.ศ. ๒๕๖๘ ซึ่งเป็นปีปัจจุบัน นั้น

ในการนี้ กองแผนงาน ได้ดำเนินการปรับปรุงประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมอนามัย พ.ศ. ๒๕๖๘ เรียบร้อยแล้ว รายละเอียดปรากฏตามเอกสารที่แนบทั้งนี้ กองการเจ้าหน้าที่ได้ตรวจสอบความถูกต้องเรียบร้อยแล้ว

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบโปรดลงนามประกาศกรมอนามัยที่แนบมาพร้อมนี้ด้วย จะเป็นพระคุณ

(นายนฤดลกิจ ทุการ)
ผู้อำนวยการกองแผนงาน กรมอนามัย

(นายปองพล วรปาณี)
รองอธิบดีกรมอนามัย
๒๖ มี.ค. ๒๕๖๘

ลงนามแล้ว

(นางอัมพร เบญจทศพิทักษ์)
อธิบดีกรมอนามัย
- ๑ เม.ย. ๒๕๖๘

ประกาศกรมอนามัย
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมอนามัย พ.ศ. ๒๕๖๘

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมอนามัย เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่กรมอนามัยและหน่วยงานภายในได้สังกัด และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๔๐ และกฎหมายอื่นที่เกี่ยวข้องได้ กรมอนามัยจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๖๙ กรมอนามัยจึงออกประกาศไว้ดังต่อไปนี้

๑. ประกาศนี้เรียกว่า "ประกาศกรมอนามัย เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมอนามัย พ.ศ. ๒๕๖๘ "

๒. ประกาศฉบับนี้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

๓. ให้ยกเลิกประกาศกรมอนามัย เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรมอนามัย ลงวันที่ ๑๓ สิงหาคม ๒๕๖๗

๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอนามัยมีวัตถุประสงค์ดังต่อไปนี้

๔.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของกรมอนามัย ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานสังกัดกรมอนามัยได้รับทราบและถือปฏิบัติตามนโยบายอย่างเคร่งครัด

๔.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับกรมอนามัย ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของกรมอนามัยในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละ ๑ ครั้ง

๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมอนามัยกำหนดประเด็นสำคัญดังต่อไปนี้

๕.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๕.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงกำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติ

ที่มาข้อมูล : ประกาศกรมอนามัย ลงวันที่ 1 เมษายน 2568

3. การจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมอนามัย

ทบทวนการการจัดทำแผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident Response) กรมอนามัย ใช้เป็นแนวทางในการเตรียมความพร้อม เพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยจะระบุขั้นตอนที่จำเป็น ผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ และข้อควรระวังในแต่ละขั้นตอน ซึ่งครอบคลุมตั้งแต่ การเตรียมความพร้อม (Preparation) การตรวจจับ และวิเคราะห์ (Detection & Analysis) การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery) และการดำเนินการภายหลังการรับมือและตอบสนองเสร็จสิ้น (Post Incident Activity) มุ่งหวังให้เป็นประโยชน์ในการนำไปประยุกต์ใช้ให้สามารถดำเนินการได้อย่างมี ประสิทธิภาพ เหมาะสมกับขนาดความซับซ้อน ความเสี่ยง และรูปแบบในการดำเนินงาน โดยมีรายละเอียด ดังนี้

กรมอนามัย
DEPARTMENT OF HEALTH

แผนบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์
(Cybersecurity Incident Response) กรมอนามัย ประจำปี ๒๕๖๘

๑. หลักการและเหตุผล

แผนรับมือภัยคุกคามทางไซเบอร์ใช้เป็นแนวทางในการเตรียมความพร้อม เพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยจะระบุขั้นตอนที่จำเป็น ผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ และข้อควรระวังในแต่ละ ขั้นตอน ซึ่งครอบคลุมตั้งแต่ การเตรียมความพร้อม (Preparation) การตรวจจับ และวิเคราะห์ (Detection & Analysis) การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery) และการดำเนินการภายหลังการรับมือและตอบสนองเสร็จสิ้น (Post Incident Activity) มุ่งหวังให้เป็นประโยชน์ในการนำไปประยุกต์ใช้ให้สามารถดำเนินการได้อย่างมี ประสิทธิภาพ เหมาะสมกับขนาดความซับซ้อน ความเสี่ยง และรูปแบบในการดำเนินงาน

๒. วัตถุประสงค์

เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ให้มีการดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องกับ ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงาน รวมถึงพฤติการณ์ฉวยโอกาส เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์ และหาวิธีการจัดเหตุการณ์ได้ทันท่วงที

๓. แนวทางปฏิบัติในการรับมือเหตุภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นส่งผลกระทบต่อความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานสำคัญที่เป็นประโยชน์สาธารณะ สามารถจำแนกหมวดหมู่ตามประกาศของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แห่งระดับ พ.ศ. ๒๕๖๔ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สรุปได้ดังนี้

๑. เหตุการณ์ฝึกซ้อม และการฝึกอบรมของหน่วยงานเอง (Cyber Training and Exercise)
๒. การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๓. การพยายามรวบรวมข้อมูลของค์กรเพื่อโจมตี (Reconnaissance)
๔. การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๕. การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๖. การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๗. การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๘. การบุกรุกที่ทำให้ไม่สามารถเข้าใช้บริการได้ (Denial of Service)
๙. เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

4. ทบทวนการจัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามทางไซเบอร์

ทบทวนการการจัดทำระบบเฝ้าระวังและแจ้งภัยคุกคามภัยทางไซเบอร์ โดยดำเนินการจัดทำระบบตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เพื่อตอบสนองและยังยั้งต่อภัยคุกคามทางไซเบอร์ โดยมีการจัดเตรียมระบบ/อุปกรณ์ บุคลากร และช่องทางการสื่อสารแจ้งภัยคุกคามทางไซเบอร์ของกรมอนามัย สำหรับป้องกัน ตรวจจับ และเฝ้าระวังการบุกรุกระบบคอมพิวเตอร์และเครือข่าย รวมทั้งหน่วยงานภาครัฐที่กำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานทำหน้าที่ประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, กระทรวงสาธารณสุข โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT) เป็นหน่วยงานทำหน้าที่ประสานงาน เฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์ด้านสาธารณสุข และคณะประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Anamai CIRT) ของกรมอนามัย เป็นต้น โดยมีรายละเอียด ดังนี้

4.1 จัดเตรียมระบบ/อุปกรณ์สำหรับป้องกัน ตรวจจับ และเฝ้าระวังการบุกรุกระบบคอมพิวเตอร์และเครือข่าย จากภัยคุกคามทางไซเบอร์ ดังนี้

4.1.1 อุปกรณ์ป้องกันความปลอดภัยด้านเครือข่าย เช่น

- อุปกรณ์ป้องกันเครือข่าย (Firewall)
- อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System : IPS)
- อุปกรณ์ตรวจจับและป้องกันการโจมตีระบบเครือข่ายแบบ (DDoS)
- อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)
- ระบบป้องกันไวรัส (Kaspersky Antivirus Security System)
- อุปกรณ์จัดเก็บ Log File ระบบเครือข่าย

4.1.2 การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ โดยการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น

- เทคโนโลยีการเข้ารหัสข้อมูล (Secure Socket Layer : SSL) โดยการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์
- เครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) โดยสร้างการเชื่อมต่อเครือข่ายส่วนตัวระหว่างอุปกรณ์ต่างๆ ผ่านอินเทอร์เน็ต

4.1.3 ซอฟต์แวร์เฝ้าระวังภัยคุกคามทางไซเบอร์ เช่น PRTG Network Monitor เป็นต้น

- ระบบตรวจสอบสถานะเครือข่าย (PRTG Network Monitoring) โดยมีโปรโตคอลสำหรับมอนิเตอร์อุปกรณ์ (SNMP) และคำสั่งตรวจสอบสถานะการทำงาน UP/Down (Ping)

4.2 จัดเตรียมบุคลากร เพื่อทำหน้าที่ประสานงาน เฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์

- ทีมรับมือ และตอบสนองต่อภัยคุกคามทางไซเบอร์มีหน้าที่รับผิดชอบในการแจ้งข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้กับผู้ที่เกี่ยวข้องทั้งภายใน และภายนอกองค์กร เพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่รับผิดชอบของตนเองตามกำหนดไว้ โดยมีรายละเอียด ดังนี้

ลำดับ	ผู้ที่เกี่ยวข้อง	หน้าที่รับผิดชอบ
1	ผู้แจ้งเหตุ หรือผู้ได้รับผลกระทบ	แจ้งเหตุการณ์หรือรายงานเหตุการณ์ภัยคุกคามที่พบหรือต้องสงสัยว่าอาจจะเกิดเหตุการณ์
2	ผู้รับแจ้งเหตุการณ์ (กองแผนงาน)	รับแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
3	ทีมรับมือ และเฝ้าระวัง (กองแผนงาน) (เจ้าหน้าที่ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์)	1. วิเคราะห์เหตุการณ์ภัยคุกคาม 2. รับมือและตอบสนองต่อเหตุการณ์ภัยคุกคาม 3. ให้คำปรึกษาในการป้องกัน และข้อควรระวังต่าง ๆ เกี่ยวกับเหตุการณ์ภัยคุกคาม 4. เฝ้าระวังและวิเคราะห์การแจ้งเตือนจากอุปกรณ์ตรวจจับ 5. ติดต่อหน่วยงานภายนอกในกรณีที่ไม่สามารถดำเนินการระงับเหตุการณ์ได้
4	ผู้บริหาร	รับผิดชอบกำหนดนโยบาย แนวปฏิบัติ ให้ข้อเสนอแนะ และสนับสนุนงบประมาณในด้านต่าง ๆ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

4.3 ช่องทางการสื่อสารแจ้งภัยคุกคามทางไซเบอร์ของกรมอนามัย เพื่อเป็นช่องทางการรายงานเหตุการณ์ ให้ผู้ได้รับผลกระทบหรือพบเห็นเหตุการณ์ ดังนี้

- จดหมายอิเล็กทรอนิกส์ : cybersec@anamai.mail.go.th
- กลุ่มไลน์ : AnamaiCIRT
- เบอร์ติดต่อ : 0 2590 4310

เว็บไซต์เผยแพร่ข่าวสาร : https://cybersec.anamai.moph.go.th

5. สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้กับเจ้าหน้าที่ของกรมอนามัย

การจัดการฝึกอบรมระบบบริหารเครือข่าย (Network Management System) เพื่อให้เจ้าหน้าที่กรมอนามัยตระหนักถึงภัยคุกคามทางไซเบอร์ และเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 มีรายละเอียด ดังนี้

5.1 สร้างความเข้าใจเกี่ยวกับอันตรายจากการโจมตีทางไซเบอร์

5.2 การเข้าใจเกี่ยวกับมาตรการป้องกันการโจมตีทางไซเบอร์ และทักษะในการระมัดระวังต่อการละเมิดความปลอดภัย

5.3 ส่งเสริมพฤติกรรมที่ปลอดภัยที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

5.4 สนับสนุนและการกำกับดูแลผู้ใช้งานในการปฏิบัติตามนโยบายและมาตรการ

5.5 เผยแพร่ความรู้และข้อมูลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

ด่วนที่สุด **บันทึกข้อความ**

ส่วนราชการ กองแผนงาน กลุ่มดิจิทัลเทคโนโลยีและระบบข้อมูล โทร. ๐ ๒๕๙๐ ๔๓๑๐

ที่ สธ ๐๙๐๕.๐๔/๖๑๔๕๔ **วันที่** ๒๑ กรกฎาคม ๒๕๖๘

เรื่อง ขอเชิญเข้าร่วมการฝึกอบรมระบบบริหารเครือข่าย (Network Management System)

เรียน ประธานคณะกรรมการผู้ทรงคุณวุฒิ
ผู้อำนวยการสำนัก/กอง/ศูนย์/กลุ่ม/สถาบัน ทุกหน่วยงานในสังกัดกรมอนามัย
เลขานุการกรม

ตามที่กรมอนามัยได้จัดทำสัญญากับ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ดำเนินการเช่าเชื่อมโยงเครือข่ายสื่อสารความเร็วสูง โดยในข้อกำหนดการเช่าดังกล่าว กำหนดให้บริษัทสนับสนุนการจัดฝึกอบรมให้กับเจ้าหน้าที่กรมอนามัย เพื่อให้มีความรู้ ความเข้าใจในเทคนิคการบริหารจัดการเครือข่ายอินเทอร์เน็ตที่ทันสมัย และสามารถนำไปประยุกต์ใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ นั้น

ในการนี้ กองแผนงาน ขอเชิญเจ้าหน้าที่ผู้เกี่ยวข้องจากหน่วยงานท่าน จำนวน ๑ คน เข้าร่วมการฝึกอบรมระบบบริหารเครือข่าย (Network Management System) ในวันที่ ๒๕ กรกฎาคม ๒๕๖๘ เวลา ๐๘.๓๐ - ๑๖.๓๐ น. ณ ห้องประชุมชิต ชัยวงศ์ อาคาร ๕ ชั้น ๕ สำนักอนามัยสิ่งแวดล้อม กรมอนามัย และหน่วยงานส่วนภูมิภาคเข้าร่วมประชุมผ่านระบบ Video Conference ที่ https://dg.th/l๔ujqao๙b๒ รายละเอียดดังวาระการประชุมที่แนบ ทั้งนี้ ขอให้ตอบรับเข้าร่วมการประชุมผ่าน QR Code ที่ปรากฏท้ายหนังสือ หรือที่ https://dg.th/vfjum๙aow๕ ภายในวันที่ ๒๔ กรกฎาคม ๒๕๖๘ กรณีมีข้อสงสัยติดต่อสอบถามได้ที่ นายสุชาญ กิจลือเลิศ นักวิชาการคอมพิวเตอร์ปฏิบัติการ โทรศัพท์ ๐ ๒๕๙๐ ๔๓๑๐

จึงเรียนมาโปรดพิจารณามอบหมายเจ้าหน้าที่เข้าร่วมการประชุมตามวัน เวลา และสถานที่ดังกล่าวด้วย จะเป็นพระคุณ

(นายนุกูลกิจ พุกาธร)
ผู้อำนวยการกองแผนงาน กรมอนามัย

แบบฟอร์มตอบรับ
เข้าร่วมการประชุม

Meeting ID: ๙๙๑ ๙๙๗๖ ๗๓๘๕
Passcode: NMs๒๐๒๕

การจัดอบรม เรื่อง "หลักสูตรการฝึกอบรมระบบบริหารเครือข่าย (Network Management System)
วันศุกร์ที่ ๒๕ กรกฎาคม ๒๕๖๘ เวลา ๐๘.๓๐ – ๑๖.๓๐ น.

เวลา	กิจกรรม
๐๘.๓๐ – ๐๙.๐๐ น.	ลงทะเบียนเข้าร่วมการอบรม
๐๙.๐๐ – ๐๙.๓๐ น.	การบรรยายหัวข้อ "หลักสูตรการฝึกอบรมระบบบริหารเครือข่าย (Network Management System) สำหรับผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร" บรรยาย โดยผู้แทน บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
๐๙.๓๐ - ๑๐.๓๐ น.	การบรรยายหัวข้อ "หลักสูตรความรู้เกี่ยวกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Cyber Security)" บรรยาย โดยผู้แทน บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
๑๐.๓๐ - ๑๐.๔๕ น.	พักรับประทานอาหารว่าง
๑๐.๔๕ – ๑๑.๓๐ น.	การบรรยายหัวข้อ "หลักสูตรความรู้เกี่ยวกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Cyber Security)" บรรยาย โดยผู้แทน บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
๑๒.๐๐ - ๑๓.๐๐ น.	รับประทานอาหารกลางวัน
๑๓.๐๐ – ๑๔.๓๐ น.	การบรรยายหัวข้อ "หลักสูตรความรู้ด้านการจัดการความเสี่ยงดิจิทัล (Digital Risk Management)" บรรยาย โดยผู้แทน บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
๑๔.๓๐ – ๑๔.๔๕ น.	พักรับประทานอาหารว่าง
๑๔.๔๕ – ๑๖.๐๐ น.	การบรรยายหัวข้อ "หลักสูตรความรู้ด้านการจัดการความเสี่ยงดิจิทัล (Digital Risk Management)" บรรยาย โดยผู้แทน บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
๑๖.๐๐ – ๑๖.๓๐ น.	การตอบคำถาม และปิดกิจกรรมการอบรม

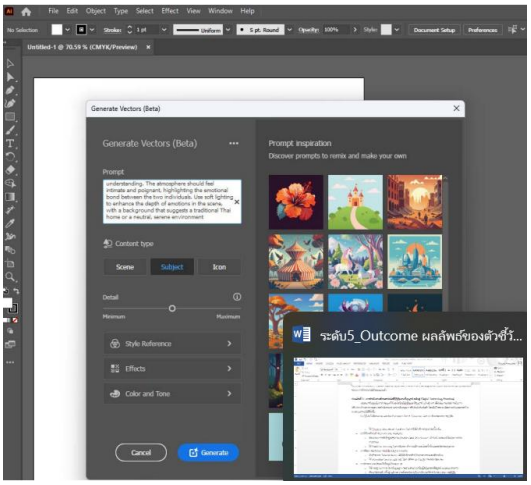
สรุปสาระสำคัญการฝึกอบรมระบบบริหารเครือข่าย (Network Management System)

วัตถุประสงค์ เพื่อถ่ายทอดความรู้และสร้างความเข้าใจเกี่ยวกับระบบบริหารจัดการเครือข่ายอินเทอร์เน็ตและความปลอดภัยของระบบเครือข่าย ให้แก่เจ้าหน้าที่กรมอนามัย และยกระดับการป้องกันภัยคุกคามด้านไซเบอร์ของกรมอนามัยทั้งส่วนกลาง และส่วนภูมิภาค โดยมีผู้เชี่ยวชาญจากบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) เป็นผู้ถ่ายทอดความรู้เชิงเทคนิคและแนวทางปฏิบัติที่มีประสิทธิภาพ

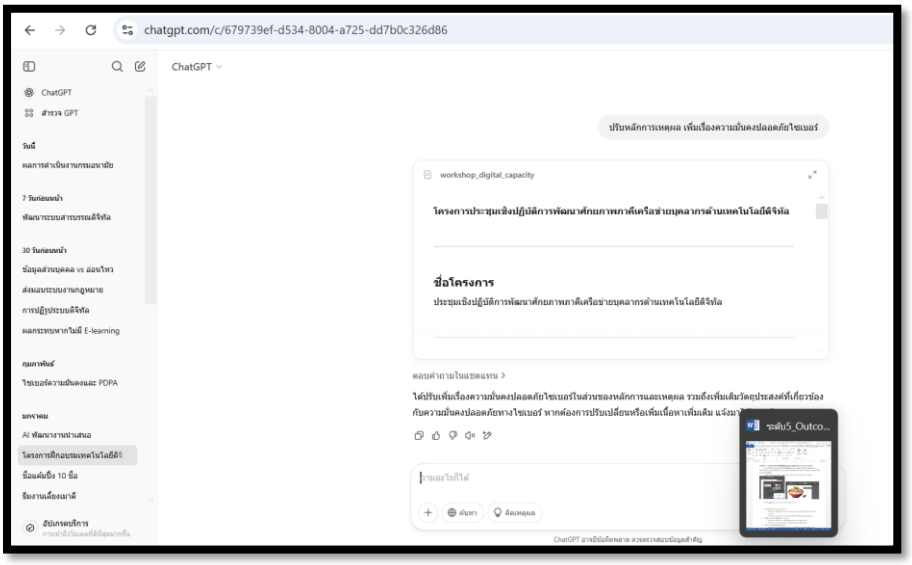
ประเด็นที่ 5 : การดำเนินงานด้านเทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ (Digital Technology Practices)

กรมอนามัยมุ่งเน้นการประยุกต์ใช้เทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ (AI) เพื่อเพิ่มประสิทธิภาพในการให้บริการด้านสาธารณสุข ลดข้อผิดพลาด และสนับสนุนการตัดสินใจที่แม่นยำ โดยมีเป้าหมายเพื่อยกระดับคุณภาพชีวิตของประชาชนให้ดียิ่งขึ้น

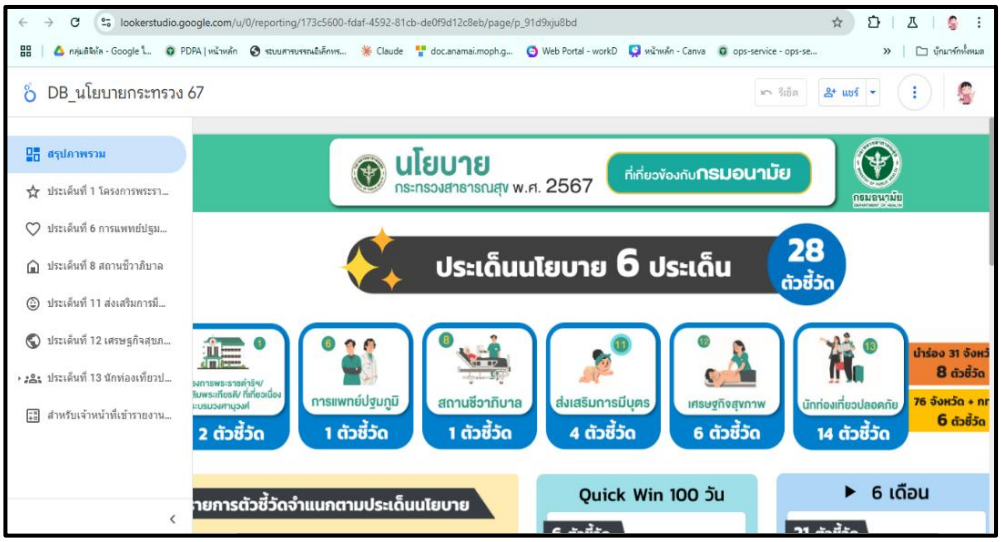
5.1 ใช AI ในโปรแกรม Adobe Illustrator ในการ Generate Vector เพื่อประกอบการทำสื่อ

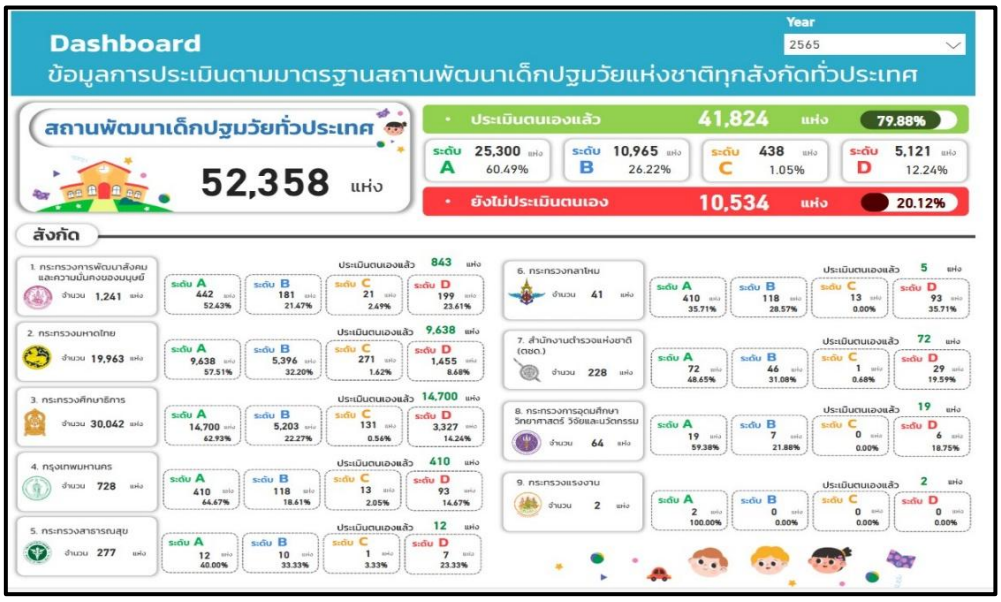


5.2 ใช้ Chatbot และ Virtual Assistant ในการเขียนโครงการฯ



5.3 การใช้เทคโนโลยี Big Data และ Analytics พัฒนาระบบคลังข้อมูลสุขภาพ (Health Data Warehouse) เพื่อวิเคราะห์แนวโน้มสุขภาพของประชาชน เช่น ระบบสมุดสุขภาพ (Health Book), AI อาหารแม่ลูก เป็นต้น

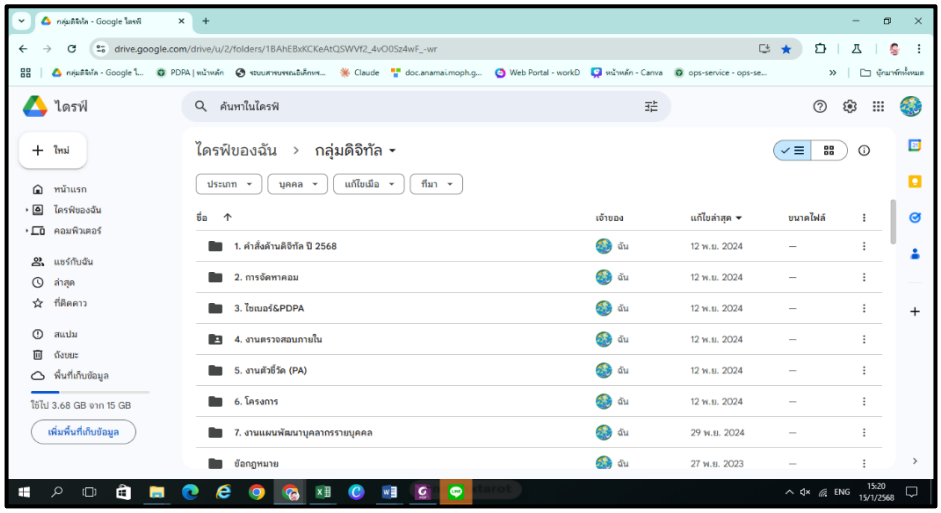


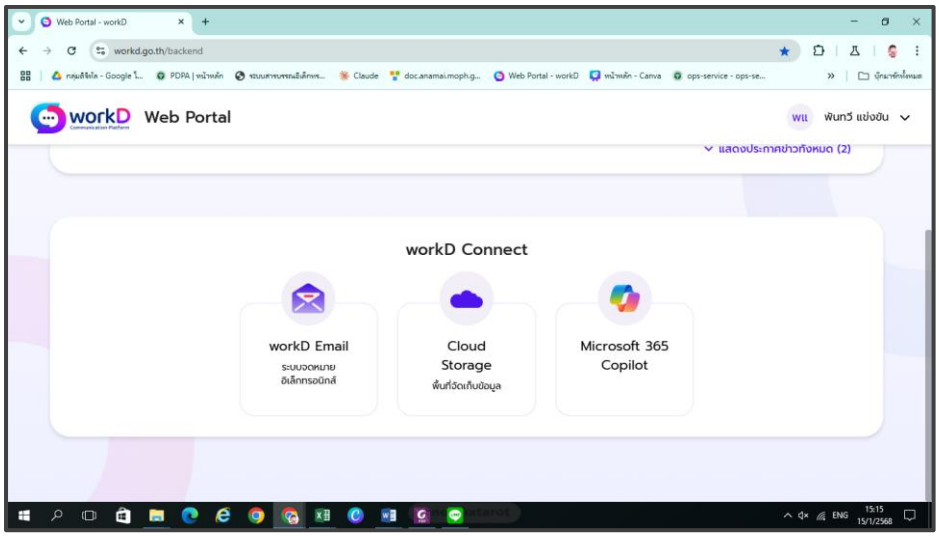


5.4 เทคโนโลยีเพื่อยกระดับประสบการณ์ AR ที่ให้ความรู้ เกี่ยวกับโภชนาการ สำหรับแม่และลูก โดยใช้เทคโนโลยี AR เข้ามาช่วยให้เห็นภาพเสมือนจริงมากยิ่งขึ้น

5.5 เทคโนโลยีการสื่อสารและโทรคมนาคม 5G ประชุมออนไลน์ผ่านเครือข่าย 5G นำมาใช้ภายในหน่วยงาน ช่วยเพิ่มประสิทธิภาพ ในการทำงานจากการรับ-ส่งสัญญาณที่รวดเร็วขึ้นไม่สะดุดและภาพมีความคมชัด เช่น โปรแกรมZoom หรือ Cisco Webex เป็นต้น

5.6 Google Drive และ Google Workspace





กรมอนามัยให้ความสำคัญกับการนำเทคโนโลยีดิจิทัลและปัญญาประดิษฐ์มาใช้ในการพัฒนาระบบสุขภาพ เพื่อเพิ่มประสิทธิภาพและความแม่นยำในการให้บริการประชาชน โดยมีแผนพัฒนาอย่างต่อเนื่องเพื่อรองรับการเปลี่ยนแปลงของเทคโนโลยีในอนาคต