ตัวชี้วัด 4.18 : ระดับความสำเร็จการขับเคลื่อนระดับความพร้อมรัฐบาลดิจิทัล กรมอนามัย

5. Outcome ผลลัพธ์ของตัวชี้วัดระดับความสำเร็จการขับเคลื่อนระดับความพร้อมรัฐบาลดิจิทัล กรมอนามัย
มีผลลัพธ์ตรงตามเป้าหมายที่กำหนด ระดับความสำเร็จของประเด็นการขับเคลื่อนระดับความพร้อมรัฐบาลดิจิทัล กรมอนามัย 5 ขั้นตอน (รอบที่ 1 : 5 เดือนแรก)

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)

กรมอนามัยให้ความสำคัญกับการบริหารจัดการข้อมูลภาครัฐอย่างมีประสิทธิภาพ โปร่งใส และปลอดภัย ตามหลักธรรมาภิบาลข้อมูล (Data Governance) เพื่อให้เกิดการใช้ข้อมูลที่ถูกต้อง เชื่อถือได้ และเป็นประโยชน์ต่อการกำหนดนโยบายด้านสาธารณสุขของประเทศ

1. มาตรการที่ดำเนินการ

- การกำหนดกรอบนโยบายธรรมาภิบาลข้อมูล
- จัดทำแนวทางการบริหารจัดการข้อมูลที่เป็นมาตรฐานและสอดคล้องกับกฎหมายและระเบียบภาครัฐ
- กำหนดบทบาทและความรับผิดชอบของเจ้าหน้าที่ในการดูแลข้อมูล (Data Steward, Data Owner, Data Custodian)

2. การบริหารคุณภาพข้อมูล

- พัฒนาแนวทางการตรวจสอบและปรับปรุงคุณภาพข้อมูลให้มีความถูกต้อง ครบถ้วน และทันสมัย ใช้เทคโนโลยี Data Analytics และ Machine Learning ในการประเมินคุณภาพข้อมูล
- การบริหารความปลอดภัยและการปกป้องข้อมูลส่วนบุคคล
- ดำเนินมาตรการรักษาความปลอดภัยข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)
- จัดทำระบบการเข้าถึงข้อมูลตามระดับสิทธิ์ และใช้เทคโนโลยีการเข้ารหัสข้อมูล (Encryption)
- การบูรณาการข้อมูลและการแลกเปลี่ยนข้อมูลภาครัฐ
- พัฒนาระบบเชื่อมโยงข้อมูลระหว่างหน่วยงานภายในและภายนอกกรมอนามัยผ่านแพลตฟอร์มกลาง
- ใช้มาตรฐาน Open Data เพื่อเพิ่มความสามารถในการเข้าถึงข้อมูลสาธารณะ

3. ผลลัพธ์ที่ได้รับ

- ระบบบริหารจัดการข้อมูลมีความโปร่งใส ตรวจสอบได้ และเป็นไปตามหลักธรรมาภิบาลข้อมูล
- คุณภาพของข้อมูลด้านสาธารณสุขดีขึ้น ลดข้อผิดพลาดในการวิเคราะห์และการตัดสินใจ
- การรักษาความปลอดภัยของข้อมูลเป็นไปตามมาตรฐานสากล ลดความเสี่ยงด้านข้อมูลรั่วไหล
- มีระบบการแลกเปลี่ยนข้อมูลที่รวดเร็วและมีประสิทธิภาพ ช่วยให้การดำเนินงานด้านสาธารณสุขมีความคล่องตัว

4. แนวทางพัฒนาต่อไป

- ยกระดับมาตรฐานธรรมาภิบาลข้อมูลให้เป็นไปตามมาตรฐานสากล เช่น ISO 27001 และ Data Management Maturity Model (DMM)

- พัฒนาศักยภาพบุคลากรด้าน Data Governance และ Data Security ให้มีความเชี่ยวชาญ

- ส่งเสริมการใช้เทคโนโลยี Big Data และ AI ในการวิเคราะห์ข้อมูลเพื่อสนับสนุนการตัดสินใจด้านสาธารณสุข

กรมอนามัยมุ่งมั่นพัฒนาการดำเนินงานด้านธรรมาภิบาลข้อมูลให้มีประสิทธิภาพและปลอดภัย เพื่อให้ข้อมูลที่ได้สามารถนำไปใช้ประโยชน์อย่างสูงสุดในการพัฒนาระบบสาธารณสุขของประเทศ โดยจะยังคงปรับปรุงมาตรการด้านข้อมูลให้ทันสมัยและสอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอยู่เสมอ

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)

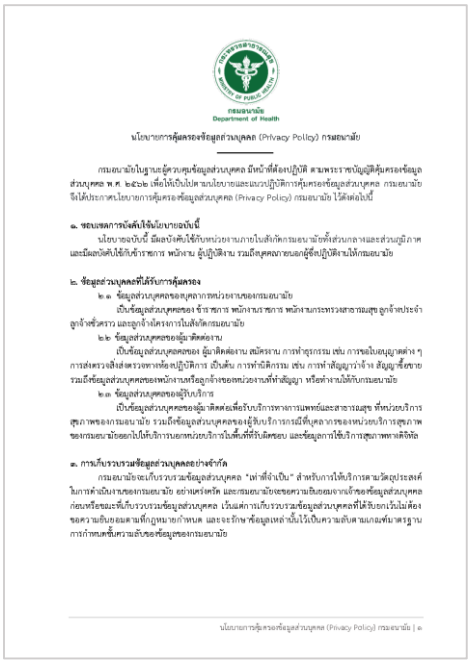
ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้กำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลของกรมอนามัยเป็นไปอย่างมีประสิทธิภาพ สามารถปฏิบัติตามได้อย่างเป็นรูปธรรม นั้น

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 ๒๗ ธันวาคม พ.ศ. ๒๕๖๗

(นางอัมพร เบญจพลพิทักษ์)
อธิบดีกรมอนามัย



นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) กรมอนามัย

กรมอนามัยในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องปฏิบัติ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล กรมอนามัย จึงได้ประกาศนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) กรมอนามัย ไว้ดังต่อไปนี้

๑. ขอบเขตการบังคับใช้นโยบายฉบับนี้

นโยบายฉบับนี้ มีผลบังคับใช้กับหน่วยงานภายในสังกัดกรมอนามัยทั้งส่วนกลางและส่วนภูมิภาค และมีผลบังคับใช้กับเจ้าหน้าที่ หน่วยงาน ผู้ปฏิบัติงาน รวมถึงบุคคลภายนอกผู้ซึ่งปฏิบัติงานให้กรมอนามัย

๒. ข้อมูลส่วนบุคคลที่ได้รับการคุ้มครอง

๒.๑ ข้อมูลส่วนบุคคลของบุคลากรหน่วยงานของกรมอนามัย

เป็นข้อมูลส่วนบุคคลของ ข้าราชการ พนักงานราชการ พนักงานกระทรวงสาธารณสุข ลูกจ้างประจำ ลูกจ้างชั่วคราว และลูกจ้างโครงการในสังกัดกรมอนามัย

๒.๒ ข้อมูลส่วนบุคคลของผู้มาติดต่องาน

เป็นข้อมูลส่วนบุคคลของ ผู้มาติดต่องาน สมัครงาน การทำธุรกรรม เช่น การขอใบอนุญาตต่าง ๆ การส่งตรวจสิ่งส่งตรวจทางห้องปฏิบัติการ เป็นต้น การทำนิติกรรม เช่น การทำสัญญาว่าจ้าง สัญญาซื้อขาย รวมถึงข้อมูลส่วนบุคคลของหนังงานหรือลูกจ้างของหน่วยงานที่ทำสัญญา หรือทำงานให้กับกรมอนามัย

๒.๓ ข้อมูลส่วนบุคคลของผู้รับบริการ

เป็นข้อมูลส่วนบุคคลของผู้มาติดต่อเพื่อรับบริการทางการแพทย์และสาธารณสุข ที่หน่วยบริการสุขภาพของกรมอนามัย รวมถึงข้อมูลส่วนบุคคลของผู้รับบริการกรณีที่บุคลากรของหน่วยบริการสุขภาพของกรมอนามัยออกไปให้บริการนอกหน่วยบริการในพื้นที่ที่รับผิดชอบ และข้อมูลการใช้บริการสุขภาพทางดิจิทัล

๓. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

กรมอนามัยจะเก็บรวบรวมข้อมูลส่วนบุคคล "เท่าที่จำเป็น" สำหรับการให้บริการตามวัตถุประสงค์ในการดำเนินงานของกรมอนามัย อย่างเคร่งครัด และกรมอนามัยจะขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล เว้นแต่การเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามที่กฎหมายกำหนด และจะรักษาข้อมูลเหล่านั้นไว้เป็นความลับตามมาตรฐานการกำหนดชั้นความลับของข้อมูลของกรมอนามัย

นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) กรมอนามัย | ๑

กรมอนามัย
Department of Health

คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) กรมอนามัย
(สำหรับการบริการส่งเสริมสุขภาพและอนามัยสิ่งแวดล้อม การแพทย์และสาธารณสุข)

กรมอนามัย ตระหนักและให้ความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของผู้มาติดต่อและใช้บริการของกรมอนามัย ("ท่าน") โดยกรมจะดูแลและบริหารจัดการข้อมูลส่วนบุคคลของท่านอย่างโปร่งใส เป็นธรรม และเป็นไปตามข้อกำหนดของกฎหมายคุ้มครองข้อมูลส่วนบุคคลรวมถึงกฎหมายอื่นที่เกี่ยวข้อง

โดยประกาศความเป็นส่วนตัวนี้ ("ประกาศ") จะแจ้งให้ท่านทราบถึงวิธีการที่กรมอนามัยเก็บรวบรวม ใช้ เปิดเผย และปกป้องดูแลข้อมูลส่วนบุคคลของท่าน

กรมอนามัยขอแนะนำให้ท่านอ่านและทำความเข้าใจประกาศนี้โดยเฉพาะข้อมูลส่วนบุคคลที่บกรมอนามัย หากท่านมีข้อกังวล ข้อสงสัยหรือต้องการสอบถามข้อมูลเพิ่มเติมเกี่ยวกับประกาศนี้ตลอดจนถึงประกาศและนโยบายอื่น ๆ ที่เกี่ยวข้อง โปรดติดต่อกรมอนามัยตามช่องทางการติดต่อที่ปรากฏท้ายประกาศนี้

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

๑. การเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูล

กรมอนามัยจะเก็บรวบรวมข้อมูลส่วนบุคคลและข้อมูลสุขภาพจากเจ้าของข้อมูลโดยตรง และอาจเก็บข้อมูลส่วนบุคคลและข้อมูลสุขภาพจากข้อมูลที่เจ้าของข้อมูลหรือตัวแทนของเจ้าของข้อมูลให้ไว้กับกรมอนามัย หรือผู้ให้บริการที่เกี่ยวข้องกับเจ้าของข้อมูล โรงพยาบาลหรือหน่วยงานภายในสังกัด ๆ ของกรมอนามัย หน่วยงานที่มีอำนาจหน้าที่ในการกำกับดูแลหรือบังคับใช้กฎหมายต่างประเทศ ปรึกษาหารือที่เกี่ยวข้องต่าง ๆ ของกรมอนามัย รวมถึง การใช้งานเว็บไซต์ การสวนนิทรรศข้อมูลจากแอปพลิเคชันจากแหล่งข้อมูลอื่นใดที่เชื่อถือได้ เช่น สมาคมองค์การของรัฐ หน่วยงานภาครัฐ องค์กรอกกน งานสัมมนา งานนิทรรบน งานออกร้าน ทั้งที่กรมอนามัยจัดขึ้นเองหรือองค์กรภาครัฐ และภาคเอกชนอื่น ๆ รวมไปถึงสื่อสังคมออนไลน์ต่าง ๆ เป็นต้น ทั้งนี้เป็นไปเพื่อประโยชนในการให้บริการสุขภาพและเพื่อการสุขภาพของเจ้าของข้อมูล ตามการกำหนดไว้อำนาจหน้าที่ของกรมอนามัย

คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice) กรมอนามัย หน้า ๑

3.2 สร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้กับเจ้าหน้าที่ของกรมอนามัย

การจัดประชุมชักซ้อมแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และการกู้คืนข้อมูล มีรายละเอียด ดังนี้

1. สร้างความเข้าใจเกี่ยวกับอันตรายจากการโจมตีทางไซเบอร์ สามารถเกิดขึ้นได้ทุกเมื่อและมีผลกระทบที่หลากหลาย

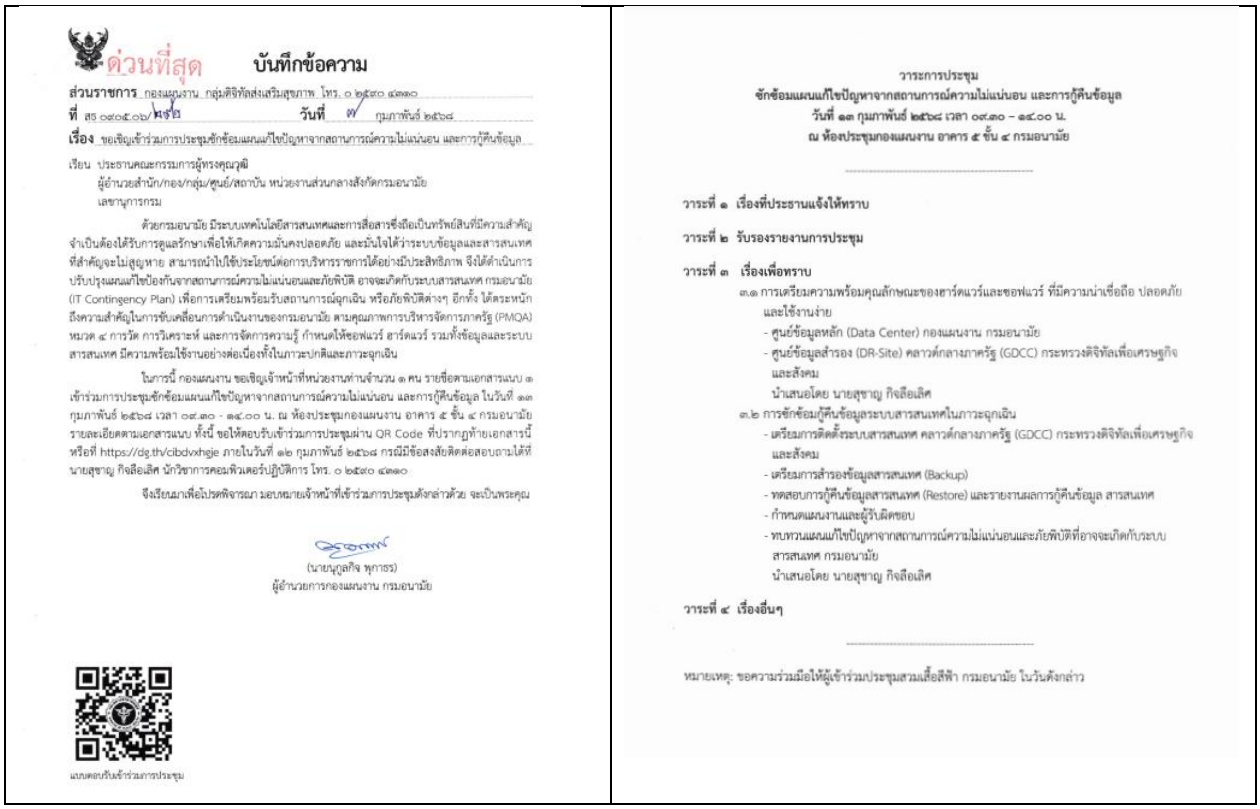
2. การเข้าใจเกี่ยวกับมาตรการป้องกัน โดยอธิบายหรือแสดงให้เห็นถึงมาตรการที่สามารถใช้ป้องกันการโจมตีทางไซเบอร์ เช่น การใช้รหัสผ่านที่ปลอดภัย การป้องกันมัลแวร์ และการอัพเดตซอฟต์แวร์ เป็นต้น

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 ๐๙๐๔.๐๒/ พิเศษ **วันที่** ๗ กุมภาพันธ์ ๒๕๖๘
เรื่อง ขอเชิญเข้าร่วมการประชุมซักซ้อมแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และการกู้คืนข้อมูล

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

ด้วยกรมอนามัย มีระบบเทคโนโลยีสารสนเทศและการสื่อสารซึ่งถือเป็นทรัพย์สินที่มีความสำคัญจำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย และมั่นใจได้ว่าระบบข้อมูลและสารสนเทศที่สำคัญจะไม่สูญหาย สามารถนำไปใช้ประโยชน์ต่อการบริหารราชการได้อย่างมีประสิทธิภาพ จึงได้ดำเนินการปรับปรุงแผนแก้ไขป้องกันจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ 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 พุการธร)
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)

กองแผนงานดำเนินการจัดประชุมเชิงปฏิบัติการขับเคลื่อนการดำเนินงาด้านความมั่นคงปลอดภัยสารสนเทศของกรมอนามัย ระหว่างวันที่ 19 – 20 ธันวาคม 2567 ณ โรงแรมแกรนด์ริชมอนด์ จังหวัดนนทบุรี เพื่อให้ผู้เข้าร่วมตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ สามารถป้องกันภัยคุกคามไซเบอร์ที่จะเกิดขึ้นในอนาคตได้อย่างทันท่วงที และมีแนวทางการดำเนินงานที่ถูกต้องเหมาะสม รวมทั้งมีความรู้และความเข้าใจด้านกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์สำหรับผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศของกรมอนามัย

กรมอนามัยเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญที่ต้องมีมาตรการ Cyber Security ตามมาตรฐานระดับประเทศ ปัจจุบันสถานการณ์ทางเทคโนโลยีมีภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างต่อเนื่อง จำเป็นต้องมีระบบป้องกันที่ทันสมัย ต้องยกระดับการเฝ้าระวังและปฏิบัติตามมาตรฐาน CTAM และ ISO/IEC 27001 การลงทุนด้าน Cyber Security และการพัฒนาบุคลากรเป็นสิ่งสำคัญ

1. กฎหมายและนโยบายด้าน Cyber Security ที่เกี่ยวข้อง

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

- กำหนดให้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานหลักในการกำกับดูแล
- มีหน้าที่ป้องกันภัยคุกคามไซเบอร์ ร่วมมือกับภาครัฐและเอกชน และลดความเสี่ยงทางไซเบอร์

1.2 แผนปฏิบัติการด้าน Cyber Security ของประเทศไทย (2565-2570)

มี 4 ยุทธศาสตร์หลัก: Capacity – เพิ่มขีดความสามารถของประเทศ ,Partnership – บูรณาการความร่วมมือ , Resilience – ป้องกันและฟื้นฟูโครงสร้างพื้นฐาน และ Standard – ยกระดับมาตรฐาน

1.3 หน่วยงานที่เกี่ยวข้อง

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) แบ่งหน่วยงานที่ต้องปฏิบัติตามมาตรการ Cyber Security เป็น 4 กลุ่มหลัก: 1. Regulator – หน่วยงานกำกับดูแล 2. Government – หน่วยงานของรัฐ 3. CII (Critical Information Infrastructure) – หน่วยงานโครงสร้างพื้นฐานสำคัญ และ 4. CERT (Cybersecurity Emergency Response Team) – หน่วยงานรับมือภัยคุกคามไซเบอร์

กรมอนามัยอยู่ภายใต้หมวด CII เนื่องจากมีข้อมูลด้านสุขภาพที่สำคัญ หากถูกโจมตี อาจส่งผลกระทบต่อความปลอดภัยของประชาชนในวงกว้าง

2. นโยบาย Cyber Security ของกรมอนามัย

2.1 โครงสร้างการบริหารจัดการ Cyber Security

- CIO (Chief Information Officer) – บริหารระบบสารสนเทศ
- CISO (Chief Information Security Officer) – ควบคุมและตรวจสอบมาตรการความมั่นคงปลอดภัย
- CIRT (Cyber Incident Response Team) – ทีมรับมือภัยคุกคามไซเบอร์
- IT Staff – เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศในแต่ละหน่วยงาน

2.2 แนวทางการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของกรมอนามัย

1) ยกระดับมาตรฐานและการเฝ้าระวังภัยคุกคาม
   - แต่งตั้งเจ้าหน้าที่ Cyber Security ประจำหน่วยงาน
   - ลงทุนในซอฟต์แวร์และเครื่องมือเฝ้าระวัง (SIEM, EDR, Firewall)
   - ปฏิบัติตามมาตรฐานสากล เช่น ISO/IEC 27001 และ 27799
2) พัฒนาศักยภาพบุคลากร
   - จัดอบรมและให้สอบใบรับรองด้าน Cyber Security
   - สนับสนุนค่าตอบแทนและค่าล่วงเวลา
3) เพิ่มขีดความสามารถของโครงสร้างพื้นฐาน
   - ลงทุนติดตั้งระบบ Next-Gen Firewall, IDS/IPS
   - ปรับปรุง Data Center และระบบเครือข่าย
   - พัฒนาระบบสำรองข้อมูล

3. สถานการณ์ภัยคุกคามทางไซเบอร์ที่พบในกรมอนามัย (ปี 2566-2567)

3.1 ประเภทของภัยคุกคามที่พบ

- Directory Listing – เปิดเผยรายการไฟล์บนเว็บไซต์
- Password Exposed – รหัสผ่านรั่วไหล
- PDPA Violation – การละเมิดข้อมูลส่วนบุคคล
- SQL Injection – การโจมตีฐานข้อมูล
- Ransomware – อยู่ระหว่างการตรวจสอบ

3.2 สถิติการโจมตี

- พบเหตุการณ์ด้านความมั่นคงปลอดภัยกว่า 2 ล้านครั้ง เฉลี่ยการโจมตี 10,000 ครั้ง/ปี โจมตีสำเร็จไปทั้งสิ้น 32 ครั้ง

ประเภทภัยคุกคาม	รายละเอียด	จำนวนครั้งที่พบ
Directory Listing	ระบบเปิดเผยรายการไฟล์และโฟลเดอร์ที่ไม่ควรถูกเข้าถึง	12 ครั้ง
Password Exposed	รหัสผ่านของผู้ใช้งานรั่วไหลบนอินเทอร์เน็ต	6 ครั้ง
PDPA Violation	มีการเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ตั้งใจ	5 ครั้ง
SQL Injection	การโจมตีฐานข้อมูลเพื่อเข้าถึงหรือขโมยข้อมูล	6 ครั้ง
Web Skimming & Phishing	มีเว็บพนันออนไลน์ฝังอยู่ในหน้าเว็บไซต์ทางการของกรมอนามัย	2 ครั้ง
Ransomware	ถูกเข้ารหัสข้อมูลและเรียกค่าไถ่ (อยู่ระหว่างการตรวจสอบ)	1 ครั้ง

4. แผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

กรมอนามัยใช้ NIST Cybersecurity Framework ในการบริหารจัดการภัยคุกคาม

4.1 มาตรการเชิงรุก (Proactive Measures)

1) Risk Management:

- จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยี
- พัฒนาระบบความต่อเนื่องทางธุรกิจ (BCP)
- ซ้อมแผนรับมือเหตุการณ์ฉุกเฉิน

2) Security Investment:

- ติดตั้ง Next-Gen Firewall, IPS/IDS, XDR
- ลงทุนในระบบเฝ้าระวังภัยคุกคาม เช่น SEIM, EDR, DAST, SAST
- พัฒนาระบบสำรองข้อมูล

3) Governance & Compliance:

- ปฏิบัติตามมาตรฐาน CTAM และกฎหมาย PDPA
- ตรวจสอบและประเมินความเสี่ยงเป็นประจำ

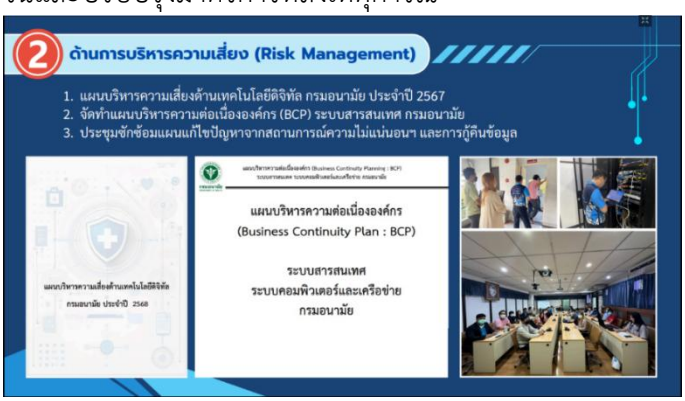
4.2 มาตรการตอบสนอง (Incident Response Measures)

1) การตอบสนอง (Respond):

- ใช้ SIAM (Security Information and Management) ในการจัดการเหตุการณ์
- แจ้งเตือนและรายงานเหตุการณ์ตามข้อกำหนดของกฎหมาย
    - ประสานงานกับ Health CERT และหน่วยงานกำกับดูแล

2) การฟื้นฟู (Recover):

- ใช้ BCP & Disaster Recovery Plan เพื่อกู้คืนระบบ
- กู้คืนข้อมูลจากระบบสำรอง
- ทบทวนและปรับปรุงมาตรการหลังเหตุการณ์



กรมอนามัยต้องเสริมสร้างมาตรการ Cyber Security อย่างเข้มงวด เนื่องจากมีภัยคุกคามเพิ่มขึ้นอย่างต่อเนื่อง การป้องกันที่ดีจะช่วยลดความเสี่ยงและปกป้องข้อมูลสำคัญของประชาชน

2. การบรรยาย เรื่อง “แนวทางการปฏิบัติและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Incident Response)”

วิทยากรโดย ว่าที่ร้อยตรี ภูวิช ชัยกรเริงเดช ผู้อำนวยการการฝ่ายสืบสวนและตรวจพิสูจน์หลักฐานทางไซเบอร์
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

วัตถุประสงค์ : เพื่อกำหนดแนวทางการปฏิบัติและตอบสนองต่อภัยคุกคามทางไซเบอร์ กรมอนามัย

เนื้อหา/บทสรุป

1. ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงไซเบอร์เป็นกระบวนการสำคัญที่ช่วยให้หน่วยงานสามารถเข้าใจและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยมีเป้าหมายหลักดังนี้:

- ระบุเหตุการณ์ที่อาจเกิดขึ้น ("What Could Go Wrong") ซึ่งมักเป็นผลจากการโจมตีของผู้ไม่หวังดี
- กำหนดระดับของความเสี่ยง เพื่อช่วยให้สามารถจัดสรรทรัพยากรในการป้องกันได้อย่างเหมาะสม
- สร้างวัฒนธรรมหน่วยงานที่ตระหนักถึงความเสี่ยง โดยให้บุคลากรทุกระดับมีส่วนร่วมในการลดความเสี่ยง

2. กรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ หน่วยงานควรมีกระบวนการบริหารความเสี่ยงที่ชัดเจน ประกอบด้วย

- เอกสารแนวทางปฏิบัติ (Policy & Frameworks)
- เกณฑ์การประเมินความเสี่ยงและระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)
- ระบบเฝ้าระวังและติดตามความเสี่ยง (Risk Monitoring & Tracking)
- รวมความเสี่ยงไซเบอร์เป็นส่วนหนึ่งของการบริหารความเสี่ยงหน่วยงาน

3. การกำหนดบริบทและระดับของความเสี่ยง

3.1 การกำหนดบริบทของความเสี่ยง

- หน่วยงานต้องเข้าใจว่าความเสี่ยงไซเบอร์มีผลกระทบต่อการดำเนินงานอย่างไร
- มีการระบุผู้มีส่วนได้เสียที่เกี่ยวข้องทั้งภายในและภายนอก

3.2 การกำหนดความเสี่ยง (Define Risk)

ระดับของความเสี่ยงพิจารณาจาก โอกาสเกิด (Likelihood) และ ผลกระทบ (Impact)

ตามสมการ : Risk = Function (Likelihood, Impact)

3.3 ปัจจัยที่ส่งผลต่อความเสี่ยง

1. เหตุการณ์ภัยคุกคาม (Threat Event) - การกระทำของผู้โจมตีที่อาจส่งผลเสียหายต่อระบบ
2. ช่องโหว่ (Vulnerability) - จุดอ่อนของระบบที่อาจถูกโจมตีได้

3. โอกาสเกิด (Likelihood) - ความเป็นไปได้ที่ภัยคุกคามจะเกิดขึ้น
4. ผลกระทบ (Impact) - ความเสียหายที่อาจเกิดขึ้นหากถูกโจมตีสำเร็จ

3.4 การกำหนดระดับความเสี่ยงที่ยอมรับได้

- สูง (High) ⟶ ต้องแก้ไขทันที เพราะอาจทำให้กิจกรรมต้องหยุดลง
- กลาง (Medium) ⟶ ต้องลดความเสี่ยงภายใน 3-6 เดือน
- ต่ำ (Low) ⟶ อาจยอมรับได้แต่ต้องเฝ้าระวัง

4. การประเมินความเสี่ยงทางไซเบอร์ กระบวนการประเมินความเสี่ยงแบ่งเป็น 3 ขั้นตอน

4.1 การระบุความเสี่ยง (Risk Identification)

- ระบุทรัพย์สินสำคัญ (Identify Assets) เช่น ฐานข้อมูล, ระบบเครือข่าย
- การสร้างแบบจำลองภัยคุกคาม (Threat Modelling)
  - กำหนดขอบเขตของระบบ
  - ระบุภัยคุกคามที่เป็นไปได้
  - สร้างแบบจำลองการโจมตี
- สร้างสถานการณ์ความเสี่ยง (Risk Scenario Construction)
  - ระบุสินทรัพย์ ⟶ ระบุภัยคุกคาม ⟶ ระบุช่องโหว่ ⟶ วิเคราะห์ผลกระทบ

ตัวอย่างสถานการณ์ความเสี่ยง

- การโจมตี SQL Injection เพื่อล้วงข้อมูลเวชระเบียนผู้ป่วย
- พนักงานถูกหลอกให้ทำธุรกรรมผิดพลาด
- ผู้บุกรุกเข้าถึงระบบ SCADA และปิดระบบน้ำประปา
- อีเมลฟิชชิ่ง (Phishing mail) ที่ขโมยข้อมูลบัญชีผู้ใช้

4.2 การวิเคราะห์ความเสี่ยง (Risk Analysis)

- กำหนดโอกาสเกิด (Determine Likelihood)
- กำหนดผลกระทบ (Determine Impact)

4.3 การประเมินความเสี่ยง (Risk Evaluation)

- จัดลำดับความสำคัญของความเสี่ยง
- บันทึกลงทะเบียนความเสี่ยงเพื่อใช้ติดตามและปรับปรุงมาตรการ

5. การตอบสนองต่อความเสี่ยง (Risk Response) หน่วยงานสามารถเลือกแนวทางจัดการความเสี่ยงได้ดังนี้

- ยอมรับ (Accept) ⟶ หากความเสี่ยงต่ำและผลกระทบจำกัด
- หลีกเลี่ยง (Avoid) ⟶ เปลี่ยนแปลงกระบวนการทำงานเพื่อลดความเสี่ยง
- โอนย้าย (Transfer) ⟶ ใช้ประกันภัยหรือให้บุคคลภายนอกรับผิดชอบ
- ลดความเสี่ยง (Mitigate) ⟶ นำมาตรการป้องกันมาใช้ เช่น การเข้ารหัสข้อมูล

6. แผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) แผนการรับมือแบ่งออกเป็น 4 ขั้นตอน

6.1 การเตรียมการ (Preparation)

- จัดตั้ง ทีมรับมือเหตุการณ์ไซเบอร์ (CIRT - Cyber Incident Response Team)
- กำหนดโครงสร้างการรายงานเหตุการณ์
- สร้างแผนสำรองและมาตรการตอบสนอง

6.2 การตรวจจับและวิเคราะห์ (Detection & Analysis)

- ใช้ระบบเฝ้าระวังภัยคุกคาม (SIEM, IDS/IPS)

- วิเคราะห์รูปแบบการโจมตีเพื่อกำหนดมาตรการตอบโต้

6.3 การระงับและกู้คืนระบบ (Containment, Eradication & Recovery)

- จำกัดขอบเขตของการโจมตีเพื่อลดความเสียหาย
- กู้คืนระบบจากข้อมูลสำรอง
- เก็บหลักฐานเพื่อสืบสวนหาต้นตอของการโจมตี

6.4 การทบทวนหลังเหตุการณ์ (Post-Incident Activity)

- ประเมินผลการตอบสนองและหาแนวทางปรับปรุง
- ปรับมาตรการความปลอดภัยเพื่อป้องกันเหตุการณ์ในอนาคต

7. แหล่งเรียนรู้และพัฒนาทักษะไซเบอร์

- National Cyber Security Agency (NCSA) มีหลักสูตรอบรมและ Certification ฟรี
- เปิดให้บุคลากรทุกระดับสามารถ Upskill & Reskill ด้านไซเบอร์

<u>จากการบรรยายครั้งนี้</u> เน้นความสำคัญของการประเมินความเสี่ยงทางไซเบอร์และการจัดทำแผนรับมือเหตุการณ์ไซเบอร์ที่มีประสิทธิภาพ โดยให้ความสำคัญกับ

- ✓ การวิเคราะห์ความเสี่ยง เพื่อระบุและจัดลำดับความสำคัญของภัยคุกคาม
- ✓ การตอบสนองต่อความเสี่ยง โดยใช้มาตรการป้องกันและลดความเสียหาย
- ✓ การจัดตั้งทีมรับมือเหตุการณ์ไซเบอร์ (CIRT) เพื่อรับมือกับภัยคุกคามในอนาคต

หน่วยงานควรนำแนวทางเหล่านี้ไปปรับใช้เพื่อเพิ่มความปลอดภัยของข้อมูลและระบบสารสนเทศ

3. การบรรยายเรื่อง “การตรวจสอบช่องโหว่เบื้องต้นด้วยโปรแกรม Nessus เพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์กรมอนามัย” และการฝึกปฏิบัติ เรื่อง “การวิเคราะห์และประเมินจุดอ่อน (Vulnerability Assessment) ด้วยโปรแกรม Nessus”

วิทยากรโดย นายพงษ์ศักดิ์ ทองประหยัด System Engineer

นางสาวศรัญญา เจริญผล Product Manager

บริษัท นิช-เอส โซลูชั่น จำกัด

วัตถุประสงค์ : เพื่อสอนการใช้งานการตรวจสอบช่องโหว่เบื้องต้นด้วยโปรแกรม Nessus

1. ความหมายของช่องโหว่ (Vulnerability)

ช่องโหว่คือ จุดอ่อนของระบบ ที่อาจถูกใช้โดยผู้โจมตีเพื่อลดทอนการรักษาความมั่นคงปลอดภัยของข้อมูล โดยมีองค์ประกอบหลัก 3 ส่วน ได้แก่

- ข้อตำหนิของระบบ (Weakness) ที่สามารถถูกโจมตี
- ผู้โจมตีที่สามารถเข้าถึงช่องโหว่นั้น
- เครื่องมือหรือเทคนิคที่ใช้ในการโจมตี

ช่องโหว่เป็นส่วนหนึ่งของ พื้นหน้าของการโจมตี (Attack Surface) ซึ่งหมายถึงจุดที่ระบบเปิดโอกาสให้ถูกโจมตีได้

2. การจัดการช่องโหว่ (Vulnerability Management)

การจัดการช่องโหว่เป็น กระบวนการเชิงวัฏจักร ที่เกี่ยวข้องกับการ

- ระบุ (Identify)
- จำแนก (Categorize)
- เยียวยา (Remediate)
- บรรเทาผลกระทบ (Mitigate)

โดยช่องโหว่บางประเภทอาจไม่ก่อให้เกิดความเสี่ยงเสมอไป เช่น ช่องโหว่ที่กระทบกับสินทรัพย์ที่ไม่มีมูลค่า

3. องค์ประกอบของการโจมตีทางไซเบอร์

1. เติบโตขึ้น – จำนวนช่องโหว่เพิ่มขึ้นอย่างต่อเนื่อง
2. ยืดหยุ่นมากขึ้น – วิธีการโจมตีมีความซับซ้อนและพัฒนาอย่างรวดเร็ว
3. แพร่กระจายในวงกว้างมากขึ้น – มีหลายช่องทางที่สามารถใช้โจมตีได้ เช่น เว็บไซต์หรือเซิร์ฟเวอร์

4. ช่องทางที่อาจถูกโจมตี ดังนี้

1. อุปกรณ์ปลายทาง (Endpoint Devices) – เช่น โน้ตบุ๊กหรือมือถือ
2. โดเมนหน่วยงาน (Domain Enumeration) – ค้นหาโดเมนที่เกี่ยวข้องเพื่อล้วงข้อมูล
3. Web Application / Internal Web – เว็บไซต์และระบบภายในหน่วยงาน
4. Public Cloud – บริการคลาวด์ที่อาจมีการตั้งค่าไม่ปลอดภัย
5. OT/IoT (Operational Technology & Internet of Things) – อุปกรณ์อัจฉริยะ เช่น เครื่องจักรในโรงงาน, เครื่องมือแพทย์
6. Identity Management System – ระบบที่เก็บข้อมูลสำคัญของหน่วยงาน

5. ระบบ Nessus และการใช้งาน

Nessus เป็นระบบตรวจสอบช่องโหว่และการตั้งค่าความปลอดภัยที่ได้รับการยอมรับในระดับสากล ซึ่งช่วยให้สามารถ ตรวจสอบอุปกรณ์ในเครือข่าย วิเคราะห์การตั้งค่าความปลอดภัย ค้นหา Malware และช่องโหว่โดยอัตโนมัติ ปรับแต่งการสแกนและรายงานผล

ข้อดีของ Nessus

- มีทีมวิเคราะห์ข้อมูลจาก Dark Web และ Social Media เพื่อเก็บข้อมูลความเสี่ยง
- รองรับการใช้งานในหลายอุตสาหกรรม

6. ขั้นตอนการตรวจสอบช่องโหว่ของ Nessus (5 ขั้นตอน)

1. Discovery – ตรวจสอบอุปกรณ์ที่ออนไลน์
2. Assessment – สแกนหาช่องโหว่
    - สแกนแบบระบุ User/Pass (Provincial)
    - สแกนแบบไม่ใช้รหัสผ่าน (External Scan)
3. Prioritize – จัดลำดับความรุนแรงของช่องโหว่เป็น 5 ระดับ
    - Critical, High, Medium, Low และ Info
4. Fix – แนะนำวิธีแก้ไข แต่ระบบไม่สามารถปิดช่องโหว่เองได้
5. Measure – สแกนซ้ำเพื่อตรวจสอบว่าช่องโหว่ถูกปิดแล้วหรือไม่

7. การวิเคราะห์และจัดลำดับการแก้ไข

- VPR (Vulnerability Priority Rating): ปรับคะแนนความรุนแรงของช่องโหว่ตามเหตุการณ์และความจำเป็น
- ACR (Asset Criticality Rating): จัดลำดับความสำคัญของช่องโหว่ที่ต้องแก้ไข

8. ฟีเจอร์เด่นของ Nessus

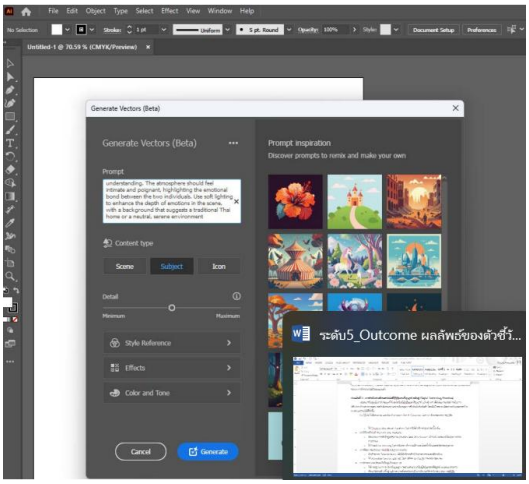
- สรุป 10 อันดับช่องโหว่ที่สำคัญที่สุด
- สามารถสร้างและปรับแต่งรายงานได้หลายรูปแบบ (HTML, CSV, XML)
- Live Results – วิเคราะห์ช่องโหว่แบบอัตโนมัติและแสดงผลทันที
- จัดกลุ่มช่องโหว่ที่คล้ายกัน เพื่อให้แก้ไขได้ง่ายขึ้น

สรุปการใช้งานโปรแกรม Nessus เป็นเครื่องมือที่ช่วยหน่วยงาน วิเคราะห์และจัดการช่องโหว่ได้อย่างมีประสิทธิภาพ ผ่านกระบวนการตรวจสอบ 5 ขั้นตอน และสามารถปรับแต่งการจัดลำดับความสำคัญของช่องโหว่ได้ ซึ่งช่วยให้สามารถปิดจุดอ่อนของระบบได้อย่างรวดเร็วและแม่นยำ

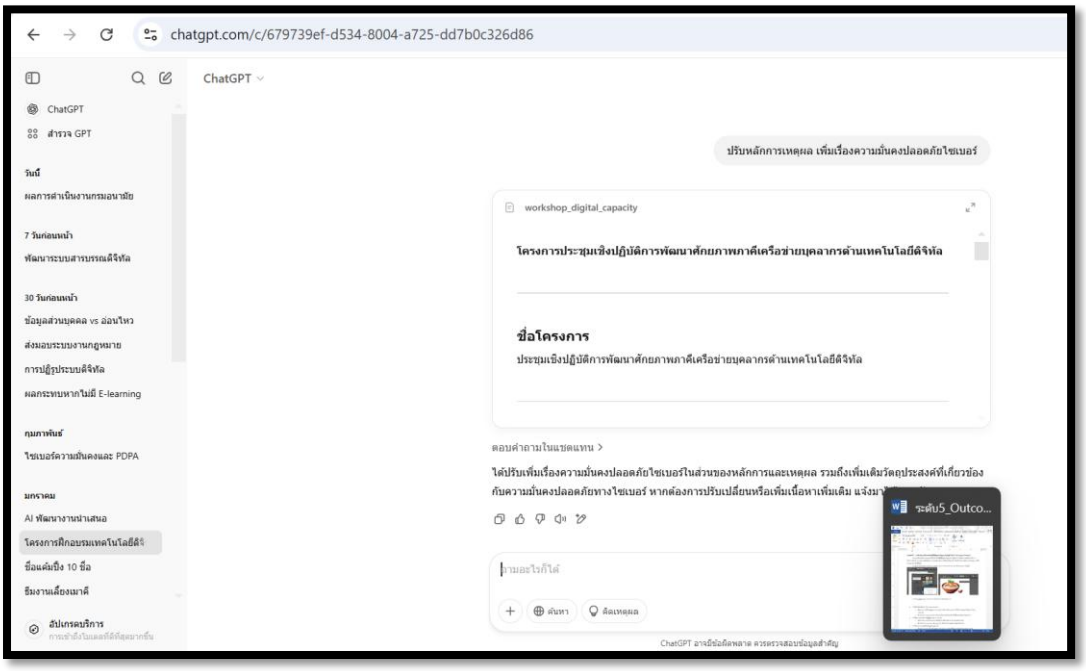
ประเด็นที่ 5 : การดำเนินงานด้านเทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ (Digital Technology Practices)

กรมอนามัยมุ่งเน้นการประยุกต์ใช้เทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ (AI) เพื่อเพิ่มประสิทธิภาพในการให้บริการด้านสาธารณสุข ลดข้อผิดพลาด และสนับสนุนการตัดสินใจที่แม่นยำ โดยมีเป้าหมายเพื่อยกระดับคุณภาพชีวิตของประชาชนให้ดียิ่งขึ้น

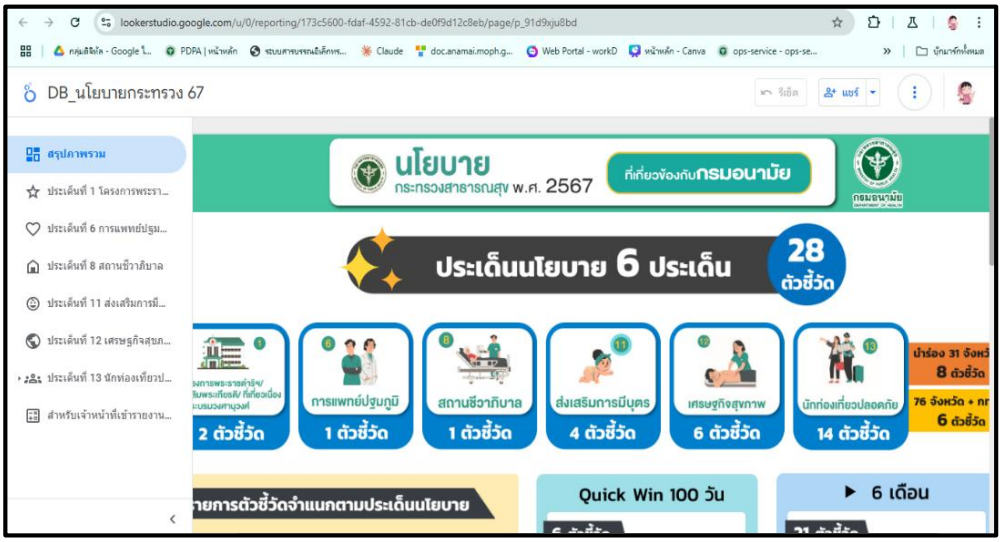
5.1 ใช้ AI ในโปรแกรม Adobe Illustrator ในการ Generate Vector เพื่อประกอบการทำสื่อ

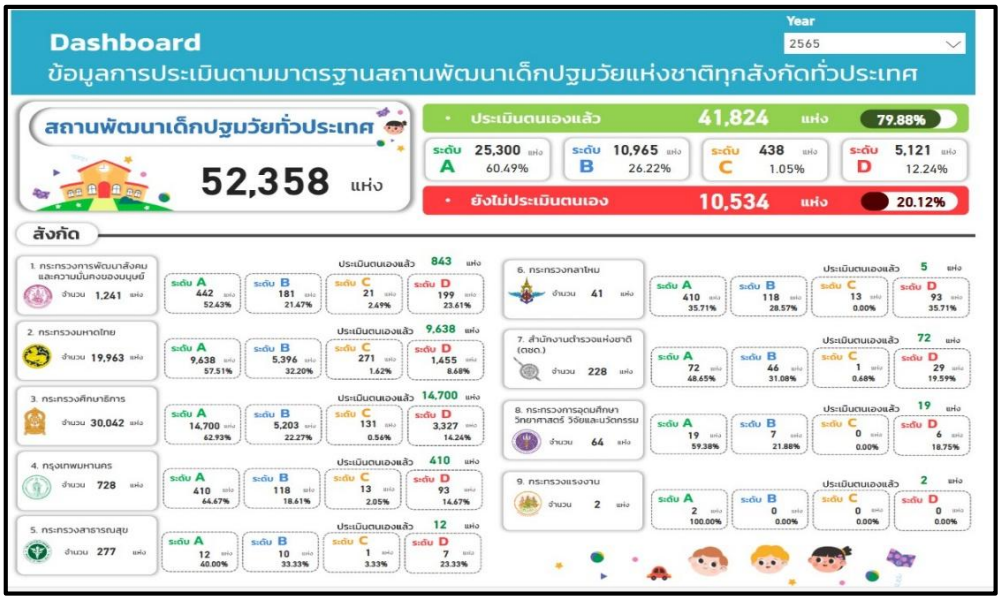


5.2 ใช้ Chatbot และ Virtual Assistant ในการเขียนโครงการฯ



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

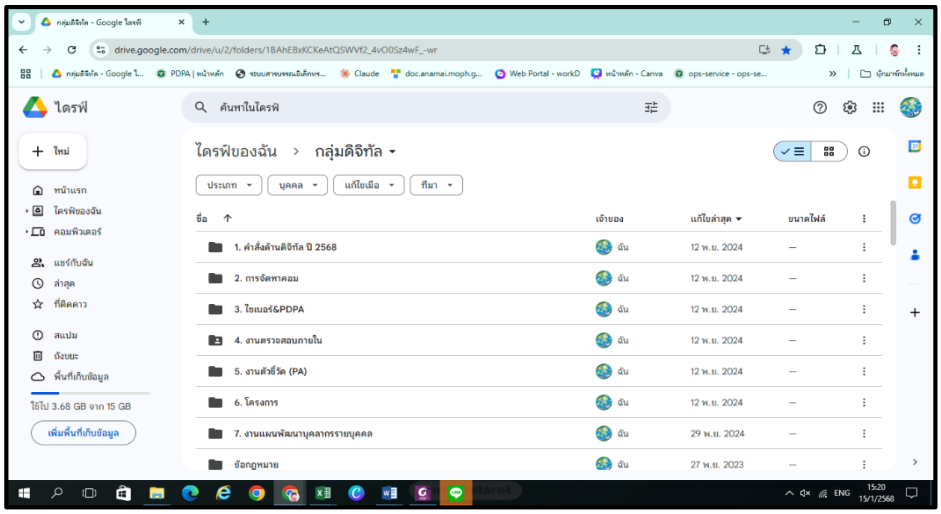


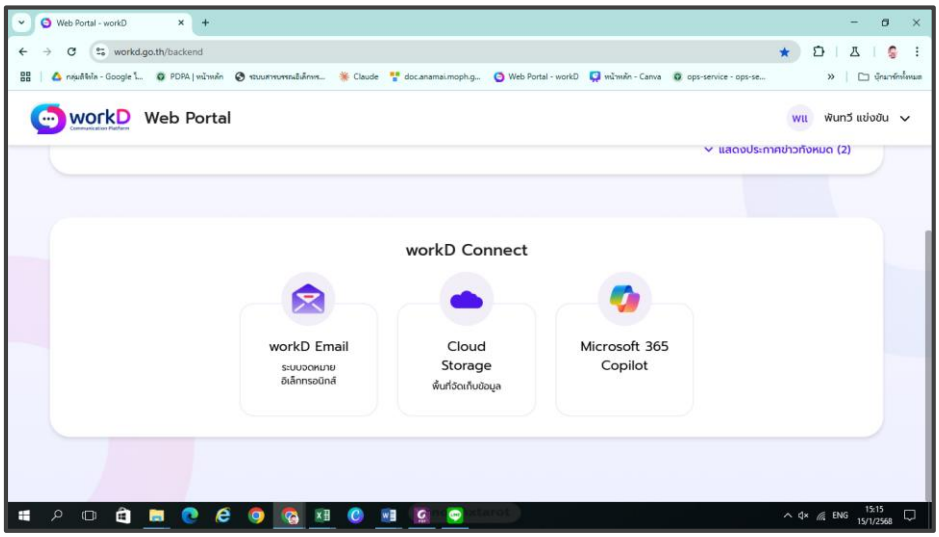


5.4 เทคโนโลยีเพื่อยกระดับประสบการณ์ AR ที่ให้ความรู้ เกี่ยวกับโภชนาการ สำหรับแม่และลูก โดยใช้เทคโนโลยี AR เข้ามาช่วยให้เห็นภาพเสมือนจริงมากยิ่งขึ้น

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