สรุปผลการดำเนินงาน

ประชุมเชิงปฏิบัติการ พัฒนาศักยภาพเจ้าหน้าที่ด่านควบคุมโรคฯ ด้านความมั่นคงปลอดภัยของข้อมูลและการจัดการภัยคุกคามทางไซเบอร์ ช่องทางเข้าออกประเทศ

จัดทำโดย

กลุ่มพัฒนาระบบเฝ้าระวังดิจิทัลด่านควบคุมโรคติดต่อระหว่างประเทศ

เอกสารนี้ใช้ประกอบการรายงานผลการดำเนินงาน งบดำเนินงาน (โครงการ)
ภายใต้ผลผลิตที่ 7 กิจกรรมหลักที่ 7.3
ยุทธศาสตร์ที่ 2 การเสริมสร้างความเข้มแข็งของระบบจัดการภาวะฉุกเฉินทางสาธารณสุข

02 591 6514 ต่อ 214
อาคาร 8 ชั้น 3 กรมควบคุมโรค
https://ddc.moph.go.th/idcp/

สรุปประชุมเชิงปฏิบัติการพัฒนาศักยภาพเจ้าหน้าที่ด่านควบคุมโรคฯ ด้านความมั่นคงปลอดภัยของข้อมูลและการจัดการภัยคุกคามทางไซเบอร์ช่องทางเข้าออกประเทศ

ยุทธศาสตร์ที่ 2: การเสริมสร้างความเข้มแข็งของระบบจัดการภาวะฉุกเฉินทางสาธารณสุข

ประเภทงบรายจ่าย: งบดำเนินงาน (โครงการ) **ผลผลิตที่:** 7 **กิจกรรมหลักที่:** 7.3

หลักการและเหตุผล:

กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค ได้ดำเนินการพัฒนาระบบฐานข้อมูลการเฝ้าระวัง คัดกรอง ตรวจตรา เชื่อมโยงข้อมูลผู้เดินทาง และยานพาหนะระหว่างประเทศกับหน่วยงานที่เกี่ยวข้อง อาทิ ตรวจคนเข้าเมือง กรมศุลกากร กรมเจ้าท่า สายการบิน เป็นต้น โดยมุ่งหวังให้บุคลากรด่านควบคุมโรคติดต่อระหว่างประเทศมีทักษะที่ดี มีระบบเฝ้าระวัง ป้องกันควบคุมโรครวดเร็ว แม่นยำ มีการบริการที่ทันสมัยและได้มาตรฐาน และสร้างความปลอดภัยรวมถึงความเชื่อมั่นให้กับประชาชนและผู้เดินทาง

ปัจจุบันการดำเนินงานเฝ้าระวัง คัดกรอง ป้องกัน ตรวจตรา และควบคุมโรคติดต่อระหว่างประเทศได้นำระบบดิจิทัลมาช่วยสนับสนุนการดำเนินงาน จึงได้เพิ่มประสิทธิภาพทรัพยากรเทคโนโลยีสารสนเทศรองรับการทำงานเพื่อการเฝ้าระวัง ป้องกัน และควบคุมโรคติดต่อระหว่างประเทศ ซึ่งมีข้อมูลด้านสุขภาพ ข้อมูลการเดินทาง และข้อมูลส่วนบุคคลของประชาชนและผู้เดินทางนั้น ถือเป็นข้อมูลที่มีความสำคัญและอ่อนไหวเป็นพิเศษ ซึ่งมีแนวโน้มที่จะตกเป็นเป้าหมายของภัยคุกคามทางไซเบอร์ ไม่ว่าจะเป็นการโจมตีระบบฐานข้อมูล การเข้าถึงโดยไม่ได้รับอนุญาต หรือการรั่วไหลของข้อมูลส่วนบุคคล ปรากฏการณ์เหล่านี้อาจส่งผลกระทบอย่างรุนแรงต่อความเชื่อมั่นของผู้เดินทางและนักท่องเที่ยว ระบบการป้องกันควบคุมโรค ภาพลักษณ์ของประเทศ การสร้างความปลอดภัยและความเชื่อมั่นให้กับประชาชนและผู้เดินทาง จึงเป็นสิ่งสำคัญ

การจัดประชุมเชิงปฏิบัติการพัฒนาศักยภาพเจ้าหน้าที่ด่านควบคุมโรคฯ ด้านความมั่นคงปลอดภัยของข้อมูลและการจัดการภัยคุกคามทางไซเบอร์ช่องทางเข้าออกประเทศที่กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรคได้พัฒนาขึ้นนี้ เพื่อให้เจ้าหน้าที่ด่านควบคุมโรคติดต่อระหว่างประเทศที่ถูกกำหนดตามแนวทางกฎอนามัยระหว่างประเทศ (Designated) จำนวน 20 แห่ง และเจ้าหน้าที่หรือผู้ดูแลระบบเทคโนโลยีสารสนเทศ (IT) ของสำนักงานป้องกันควบคุมโรคซึ่งที่มีด่านฯ ในกำกับดูแลมีความเข้มแข็งและสนับสนุนเสริมสร้างสมรรถภาพในการดำเนินงานให้แก่เจ้าหน้าที่ประจำช่องทางฯ ให้มีแนวทางและมาตรการในการเฝ้าระวัง ป้องกัน ควบคุมโรคและเตรียมความพร้อมรองรับภัยคุกคามทางไซเบอร์ และการโจมตีระบบฐานข้อมูลให้มีประสิทธิภาพต่อไป

วัตถุประสงค์:

1. เพื่อให้เจ้าหน้าที่ด่านควบคุมโรคฯ มีทักษะด้านความมั่นคงปลอดภัยของข้อมูลและการจัดการภัยคุกคามทางไซเบอร์ด่านควบคุมโรคติดต่อระหว่างประเทศ
2. เพื่อให้เจ้าหน้าที่ด่านควบคุมโรคฯ วิเคราะห์ ประเมินความเสี่ยงการใช้งานข้อมูลส่วนบุคคลและความปลอดภัยทางไซเบอร์ได้

ระยะเวลาดำเนินโครงการ

ระหว่างวันที่ 22 – 23 ธันวาคม 2568

ณ โรงแรมโอ๊ควู๊ด โฮเทล แอนด์ เรสซิเดนซ์ ศรีราชา อำเภอ ศรีราชา จังหวัดชลบุรี

ผลผลิตและตัวชี้วัดความสำเร็จของโครงการ :

ผลผลิตโครงการ

ลำดับ	ผลผลิตของโครงการ	จำนวน	หน่วยนับ	ผลลัพธ์
1.	รายงานการวิเคราะห์และประเมินความเสี่ยงการใช้งานข้อมูลส่วนบุคคลและความปลอดภัยทางไซเบอร์	1	เรื่อง	1

ตัวชี้วัดความสำเร็จของโครงการ

ลำดับ	ตัวชี้วัดความสำเร็จของโครงการ	จำนวน	หน่วยนับ	ผลลัพธ์
1	ระดับความสำเร็จของเจ้าหน้าที่ด่านควบคุมโรคฯ เข้าร่วมการประชุมเชิงปฏิบัติการพัฒนาศักยภาพเจ้าหน้าที่ด่านควบคุมโรคฯ ด้านความมั่นคงปลอดภัยของข้อมูลและการจัดการภัยคุกคามทางไซเบอร์ช่องทางเข้าออกประเทศ	≥70	ร้อยละ	ร้อยละ 86

วงเงินงบประมาณที่ใช้ 252,325.- บาท (สองแสนห้าหมื่นสองพันสามร้อยยี่สิบห้าบาทถ้วน)

กลุ่มเป้าหมาย: กลุ่มเป้าหมายของโครงการ จำนวน 39 คน จำแนกตามกลุ่มเป้าหมายตามระเบียบค่าใช้จ่ายในการฝึกอบรมฯ ได้แก่

1. ประธานในพิธีเปิดหรือพิธีปิดการประชุมเชิงฯ จำนวน 1 คน
2. วิทยากร จำนวน 5 คน
3. ผู้เข้าร่วมประชุมเชิงฯ จำนวน 33 คน ประกอบด้วย
   - เจ้าหน้าที่ด่านควบคุมโรคติดต่อระหว่างประเทศ จำนวน 17 คน
   - เจ้าหน้าที่สำนักงานป้องกันควบคุมโรคที่ 2,5-6, 8 ,11 และ 12 จำนวน 8 คน
   - เจ้าหน้าที่กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค จำนวน 6 คน
   - เจ้าหน้าที่หรือผู้ดูแลระบบเทคโนโลยีสารสนเทศ (IT) สำนักงานป้องกันควบคุมโรค จำนวน 2 คน

ประโยชน์ที่คาดว่าจะได้รับ

- เจ้าหน้าที่ด่านควบคุมโรคฯ มีทักษะด้านความมั่นคงปลอดภัยของข้อมูลและการจัดการภัยคุกคามทางไซเบอร์ด่านควบคุมโรคติดต่อระหว่างประเทศ สามารถจัดการข้อมูลที่เกี่ยวข้องกับผู้เดินทางและข้อมูลความปลอดภัยต่างๆด้านสุขภาพที่ช่องทางเข้าออกประเทศได้
- เจ้าหน้าที่ด่านควบคุมโรคฯ วิเคราะห์ ประเมินความเสี่ยงการใช้งานข้อมูลส่วนบุคคลและความปลอดภัยทางไซเบอร์ได้

กำหนดการประชุมเชิงปฏิบัติการพัฒนาศักยภาพเจ้าหน้าที่ด่านควบคุมโรคฯ
ด้านความมั่นคงปลอดภัยของข้อมูลและการจัดการภัยคุกคามทางไซเบอร์ช่องทางเข้าออกประเทศ
ระหว่างวันที่ 22 - 23 ธันวาคม 2568
ณ โรงแรมโอ๊ควู้ด โฮเทล แอนด์ เรสซิเดนซ์ ศรีราชา อำเภอ ศรีราชา จังหวัดชลบุรี

วันที่ 22 ธันวาคม 2568	
08.00 -08.15 น.	**ลงทะเบียน** ณ ห้องประชุมมาบตาพุด-แหลมฉบัง
08.15–08.30 น.	**พิธีเปิดการประชุม** โดย นายแพทย์โรม บัวทอง ผู้อำนวยการกองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค **กล่าวรายงาน** โดย นายเทวพร จานนอก หัวหน้ากลุ่มพัฒนาระบบเฝ้าระวังดิจิทัลด่านควบคุมโรคติดต่อระหว่างประเทศ
08.30–09.30 น.	**บรรยาย “แนวทางการดำเนินงานด้านความมั่นคงปลอดภัยของข้อมูลและการจัดการภัยคุกคามทางไซเบอร์ช่องทางเข้าออกประเทศ”** **วิทยากร** นายแพทย์โรม บัวทอง ผู้อำนวยการกองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค
09.30-12.00 น.	**บรรยาย หัวข้อ“หลักการและสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล”** **วิทยากร** นายประพนธ์ กิจอำไพวงศ์ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
12.00–13.00 น.	พักรับประทานอาหารกลางวัน
13.00 –14.30 น.	**บรรยาย หัวข้อ “Cyber Security และ Risk Assessment”** **วิทยากร** นายชัยรัตน์ ปรีชากร นักวิชาการคอมพิวเตอร์ชำนาญการ กองดิจิทัลเพื่อการควบคุมโรค
14.30–16.30 น.	**แบ่งกลุ่มฝึกปฏิบัติ** **“บทบาทหน้าที่ด่านควบคุมโรคติดต่อระหว่างประเทศ ต่อการจัดการความมั่นคงปลอดภัยของข้อมูลที่เกี่ยวข้องกับฐานข้อมูลการเฝ้าระวัง คัดกรอง ตรวจตราของด่านควบคุมโรคติดต่อระหว่างประเทศ”** • **(ร่าง) จัดทำใบบันทึกกิจกรรมการประมวลผล (RoPA)** • **ข้อมูลที่เกี่ยวข้องตามบทบาทหน้าที่ตามกฎหมาย** - พระราชบัญญัติโรคติดต่อ พ.ศ.2558 - กฎอนามัยระหว่างประเทศ - พระราชบัญญัติคนเข้าเมือง พ.ศ.2522 - กฎหมายที่เกี่ยวข้องด้านการเดินทางระหว่างประเทศ **กลุ่มที่ 1 การจัดการข้อมูลในกระบวนการเฝ้าระวัง คัดกรอง ผู้เดินทางจากต่างประเทศ (ห้องอมตะ)** **วิทยากร** นางสาวกรรณิการ์ กาญจนสุวรรณ นักวิชาการสาธารณสุขปฏิบัติการ กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค **กลุ่มที่ 2 การจัดการข้อมูลในกระบวนการตรวจสุขาบาลยานพาหนะ (ห้องอมตะ)** **วิทยากร** นายเทวพร จานนอก นักวิชาการสาธารณสุขชำนาญการ กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค **กลุ่มที่ 3 การจัดการข้อมูลในกระบวนการบันทึกข้อมูลด้านสุขภาพ ด้วยระบบ Quarantine Thailand (ห้องเหมราช)** **วิทยากร** นายกิตติพัทธ์ วรเชษฐ์ นักวิชาการสาธารณสุขชำนาญการ กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค

กำหนดการประชุมเชิงปฏิบัติการพัฒนาศักยภาพเจ้าหน้าที่ด่านควบคุมโรคฯ
ด้านความมั่นคงปลอดภัยของข้อมูลและการจัดการภัยคุกคามทางไซเบอร์ช่องทางเข้าออกประเทศ
ระหว่างวันที่ 22 - 23 ธันวาคม 2568
ณ โรงแรมโอ๊ควู้ด โฮเทล แอนด์ เรสซิเดนซ์ ศรีราชา อำเภอ ศรีราชา จังหวัดชลบุรี

วันที่ 23 ธันวาคม 2568	
09.00-10.30 น.	**บรรยาย หัวข้อ"การจัดทำใบบันทึกกิจกรรมการประมวลผล (RoPA) และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล"** **วิทยากร** นายเทวพร จานนอก นักวิชาการสาธารณสุขชำนาญการ กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค
10.30-12.00 น.	**แบ่งกลุ่มฝึกปฏิบัติ "การจัดทำใบบันทึกกิจกรรมการประมวลผล (RoPA) และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล"** **กลุ่มที่ 1** การจัดการข้อมูลในกระบวนการเฝ้าระวัง คัดกรอง ผู้เดินทางจากต่างประเทศ **วิทยากร** นางสาวกรรณิการ์ กาญจนสุวรรณ นักวิชาการสาธารณสุขปฏิบัติการ กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค **กลุ่มที่ 2** การจัดการข้อมูลในกระบวนการตรวจสุขาบาลยานพาหนะ **วิทยากร** นายเทวพร จานนอก นักวิชาการสาธารณสุขชำนาญการ กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค **กลุ่มที่ 3** การจัดการข้อมูลในกระบวนการบันทึกข้อมูลด้านสุขภาพ ด้วยระบบ Quarantine Thailand **วิทยากร** นายกิตติพัทธ์ วรเชษฐ์ นักวิชาการสาธารณสุขชำนาญการ กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค
12.00-13.00 น.	พักรับประทานอาหารกลางวัน
13.00-14.30 น.	**นำเสนอ "การจัดทำใบบันทึกกิจกรรมการประมวลผล (RoPA) และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล"** **กลุ่มที่ 1** การจัดการข้อมูลในกระบวนการเฝ้าระวัง คัดกรอง ผู้เดินทางจาก **กลุ่มที่ 2** การจัดการข้อมูลในกระบวนการตรวจสุขาบาลยานพาหนะ **กลุ่มที่ 3** การจัดการข้อมูลในกระบวนการบันทึกข้อมูลด้านสุขภาพ ด้วยระบบ Quarantine Thailand
14.30-16.00 น.	**บรรยาย หัวข้อ "แนวทางการจัดการข้อมูลด่านควบคุมโรคติดต่อระหว่างประเทศ เพื่อการปกป้องระบบเฝ้าระวังทางคอมพิวเตอร์ เครือข่าย ซอฟต์แวร์ และข้อมูลจากภัยคุกคามทางดิจิทัล"** **วิทยากร** นายกิตติพัทธ์ วรเชษฐ์ นักวิชาการสาธารณสุขชำนาญการ กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค
16.00-16.30 น.	**สรุป (ร่าง) แนวทางการจัดการข้อมูลด่านควบคุมโรคติดต่อระหว่างประเทศ เพื่อการปกป้องระบบเฝ้าระวังทางคอมพิวเตอร์ เครือข่าย ซอฟต์แวร์ และข้อมูลจากภัยคุกคามทางไซเบอร์** - การจัดการข้อมูล - ตัวอย่าง ROPA ด่านควบคุมโรคฯ - (ร่าง) แนวทางการแจ้งเพื่อปกป้องระบบเฝ้าระวังจากภัยคุกคามทางไซเบอร์

แนวทางการดำเนินงานด้านความมั่นคงปลอดภัยของข้อมูล และการจัดการภัยคุกคามทางไซเบอร์ช่องทางเข้าออกประเทศ

โดย นายแพทย์โรม บัวทอง

พิมพ์เขียวสู่อนาคตดิจิทัล: การเตรียมความพร้อมสู่รัฐบาลดิจิทัล

เน้น "นโยบายการเตรียมความพร้อมสู่รัฐบาลดิจิทัล" ของกองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค ที่มุ่งเน้นการปฏิรูปองค์กรให้ก้าวทันต่อความเปลี่ยนแปลงของเทคโนโลยีและเพิ่มประสิทธิภาพในการให้บริการประชาชนผ่านระบบดิจิทัล

บทสรุปผู้บริหาร

กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค ภายใต้การนำของผู้อำนวยการนายแพทย์โรม บัวทอง ได้กำหนดวิสัยทัศน์ในการยกระดับองค์กรไปสู่การเป็น "องค์กรดิจิทัลที่ขับเคลื่อนด้วยข้อมูลและนวัตกรรม" แผนงานนี้จะดำเนินการเพื่อให้สอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 และแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566 – 2570

สาระสำคัญ

- การบริหารจัดการข้อมูล (Data-Driven)
- การพัฒนาบุคลากร (Digital Workforce)
- การพัฒนาระบบเทคโนโลยีสารสนเทศ (IT Innovation)
- การสร้างความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

โดยมีเป้าหมายเพื่อสร้างระบบการทำงานที่บูรณาการ ลดความซ้ำซ้อน และสร้างความมั่นใจในความปลอดภัยของข้อมูลให้แก่ผู้รับบริการ

สาระสำคัญที่ 1: การพัฒนาองค์กรด้วยข้อมูล (Data-Driven Organization)

มุ่งเน้นการใช้ประโยชน์จากข้อมูลและการประมวลผลข้อมูลสารสนเทศเพื่อเป็นหัวใจสำคัญในการตัดสินใจ

- **แนวปฏิบัติ**
  - **พัฒนาชุดข้อมูลเปิด (Open Data)** จัดทำตามมาตรฐานบัญชีข้อมูลภาครัฐ (GD Catalog)
  - **วิเคราะห์และใช้ประโยชน์** ประมวลผลข้อมูลสารสนเทศให้เหมาะสมกับกลุ่มเป้าหมาย
  - **การทำงานร่วมกัน** ส่งเสริมการทำงานข้ามสายงานเพื่อบูรณาการข้อมูลเป็นหนึ่งเดียว
  - **คุ้มครองข้อมูล** ปฏิบัติตามนโยบายด้านข้อมูลส่วนบุคคลอย่างเคร่งครัด

สาระสำคัญที่ 2 : การพัฒนาศักยภาพบุคลากรด้านดิจิทัล (Digital Workforce Development)

ตระหนักถึงคุณค่าของบุคลากรและมุ่งพัฒนาไปสู่องค์กรแห่งความรอบรู้ด้านดิจิทัลอย่างเป็นระบบ

- **แนวปฏิบัติ**
  - **ส่งเสริมความก้าวหน้า** สร้างเส้นทางอาชีพในสายงานดิจิทัลให้เป็นรูปธรรม (Promote Career Growth)
  - **การนำเทคโนโลยีมาใช้** เลือกใช้เครื่องมือที่เหมาะสมและเชื่อมโยงข้อมูลเพื่อประสิทธิภาพและความปลอดภัย

สาระสำคัญที่ 3 : การพัฒนาระบบสารสนเทศและนวัตกรรม (IT Systems & Innovation Development)

มุ่งนำระบบสารสนเทศที่มีประสิทธิภาพมาสนับสนุนภารกิจ เพื่อตอบสนองความต้องการของผู้รับบริการและผู้มีส่วนได้ส่วนเสีย

- **แนวปฏิบัติ**
  - **สำรวจและวิเคราะห์** ประเมินความเสี่ยงและความต้องการของระบบอย่างต่อเนื่อง
  - **บูรณาการและลดความซ้ำซ้อน** ยึดหลักการรวมระบบสารสนเทศให้เป็นหนึ่งเดียว
  - **รับฟังความคิดเห็น** มีช่องทางรับ Feedback ทั้งภายในและภายนอกเพื่อปรับปรุงระบบ

สาระสำคัญที่ 4 : การพัฒนาโครงสร้างพื้นฐานและความมั่นคงปลอดภัยไซเบอร์ (Infrastructure & Cybersecurity)

วางรากฐานโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศให้มีความมั่นคง ปลอดภัย และมีประสิทธิภาพสูงตามมาตรฐานสากล

- **แนวปฏิบัติ**
    - **ประเมินและวางแผน** จัดทำแผนพัฒนาและประเมินความเสี่ยงอย่างต่อเนื่อง
    - **สร้างการตระหนักรู้** อบรมบุคลากรให้มีความรู้เรื่องภัยคุกคามไซเบอร์และมีการวัดผลสม่ำเสมอ
    - **ความพร้อมใช้งาน** พัฒนาระบบให้เพียงพอและพร้อมใช้งานตลอดเวลา
    - **ปฏิบัติตามนโยบาย** ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมควบคุมโรค

บทสรุปและความมุ่งมั่นขององค์กร

"นโยบายนี้คือพันธกิจร่วมกันของเราทุกคนในการสร้างอนาคตที่แข็งแกร่งและยั่งยืนให้แก่กองด่านฯ ความสำเร็จจะเกิดขึ้นได้จากความร่วมมือและการลงมือทำของพวกเราทุกคน"

— นายแพทย์โรม บัวทอง

หลักการและสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

โดย นายประพนธ์ กิจอำไพวงศ์
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

บทสรุปสำหรับผู้บริหาร

มุ่งเน้นการทำความเข้าใจในโครงสร้างการกำกับดูแล หลักการสำคัญ และผลกระทบในทางปฏิบัติ การปฏิบัติตาม PDPA โดยมีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) เป็นหน่วยงานกำกับดูแล หลักประเด็นสำคัญที่สุด คือบทลงโทษที่ครอบคลุมทั้งความรับผิดทางแพ่ง อาญา และโทษปรับทางปกครอง ซึ่งอาจสูงถึง 5 ล้านบาท

ดังนั้น กองด่านควบคุมโรคติดต่อระหว่างประเทศ เห็นควรดำเนินการในการประมวลผลข้อมูล, จัดทำประกาศความเป็นส่วนตัว (Privacy Notice), จัดทำบันทึกรายการกิจกรรมการประมวลผล (ROPA) อย่างเป็นระบบซึ่งการประชุมในครั้งนี้มีกิจกรรมนี้และร่วมกันแลกเปลี่ยนเรียนรู้และจัดทำร่วมกัน รวมถึงมาตรการรักษาความมั่นคงปลอดภัย เพื่อป้องกันเหตุละเมิดข้อมูล

โครงสร้างและกลไก

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) มีสถานะเป็นหน่วยงานของรัฐประเภทองค์การมหาชน มีอำนาจในการเรียกบุคคล เอกสาร หรือพยานหลักฐาน และมีอำนาจในการสั่งปรับทางปกครอง

หลักการสำคัญในการประมวลผลข้อมูลส่วนบุคคล

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องเป็นไปตามหลักการที่กฎหมายกำหนด โดยเฉพาะอย่างยิ่งการมีฐานทางกฎหมายรองรับและการปฏิบัติตามหน้าที่ของผู้ควบคุมข้อมูล

ฐานทางกฎหมายในการประมวลผลข้อมูล

Privacy Notice (ประกาศความเป็นส่วนตัว)

เป็นเอกสารสำหรับ สื่อสารภายนอก เพื่อแจ้งให้เจ้าของข้อมูลทราบว่าจะทำอะไรกับข้อมูลของเขา ซึ่งแตกต่างจาก Privacy Policy ที่เป็นนโยบายสำหรับการปฏิบัติงานภายในองค์กร

Privacy Notice ประกอบด้วย

- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล (DC) และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) (ถ้ามี)
- ข้อมูลส่วนบุคคลที่เก็บรวบรวมและวัตถุประสงค์
- ระยะเวลาในการเก็บรวบรวม
- ประเภทของบุคคลหรือหน่วยงานที่อาจได้รับข้อมูล
- สิทธิของเจ้าของข้อมูลส่วนบุคคล
- ผลกระทบกรณีไม่ให้ข้อมูลที่จำเป็นตามกฎหมายหรือสัญญา

ROPA (Record of Processing Activities)

แบบบันทึกรายการกิจกรรมการประมวลผล ซึ่งเป็นเอกสารภายในที่ต้องจัดทำตามมาตรา 39 เพื่อบันทึกรายละเอียดการประมวลผลข้อมูลทั้งหมด และใช้เป็นข้อมูลพื้นฐานในการจัดทำ Privacy Notice

โดย ROPA มีรายละเอียด (ซึ่งจะสอดคล้องกับการแบ่งกลุ่มฝึกปฏิบัติของด่านพรมแดนทางบก ท่าเรือ ท่าอากาศยาน)

- ข้อมูลส่วนบุคคลที่เก็บรวบรวม (ของใคร, ได้มาโดยตรง/โดยอ้อม, เป็นข้อมูลทั่วไป/อ่อนไหว)
- วัตถุประสงค์และฐานทางกฎหมายที่ใช้
- ข้อมูลผู้ควบคุมข้อมูลและ DPO
- ระยะเวลาการเก็บรักษาข้อมูล (ต้องระบุที่มา เช่น อายุความ 10 ปี, พ.ร.บ.บัญชี 5 ปี)
- รายละเอียดการใช้หรือเปิดเผยข้อมูล
- คำอธิบายมาตรการรักษาความมั่นคงปลอดภัย
- ข้อตกลงการประมวลผลข้อมูล (Data Processing Agreement - DPA) กรณีมีการใช้ผู้ประมวลผลข้อมูลส่วนบุคคล (DP) ผู้ควบคุมข้อมูล (DC) ต้องจัดให้มี DPA ซึ่งหากไม่มี DPA จะมีโทษปรับทางปกครอง 3 ล้านบาท โดยกฎหมายกำหนดโทษไว้ที่ DP แต่ DC ก็อาจมีความผิดฐานไม่มีมาตรการรักษาความปลอดภัยที่เหมาะสมได้เช่นกัน

กรณีศึกษาการละเมิดและบทลงโทษ

เพื่อเป็นประโยชน์ต่อการประยุกต์ใช้ในการทำงาน ณ ช่องทางเข้าออกประเทศ

1. โรงพยาบาลเอกชน (กรณีถุงขนมโตเกียว) จ้างบริษัทขนาดเล็กทำลายเวชระเบียนโดยไม่มีการควบคุมตรวจสอบ ทำให้ข้อมูลรั่วไหล และผู้ประมวลผลไม่แจ้งเหตุให้ทราบ
   โทษปรับ โรงพยาบาล (DC) 1,210,000 บาท , บุคคลธรรมดา (DP) 16,940 บาท
2. บริษัทขายเครื่องสำอาง ข้อมูลลูกค้ารั่วไหลไปถึงแก๊งคอลเซ็นเตอร์ โดยไม่มีมาตรการรักษาความมั่นคงปลอดภัย ไม่มีการแจ้งเหตุ และไม่มีมาตรการเยียวยาผู้เสียหาย
   โทษปรับ 2,000,000 บาท
3. บริษัทขายของเล่นสะสม ระบบจองสินค้าถูกแฮกเกอร์เจาะระบบ เนื่องจากบริษัทผู้พัฒนาระบบ (DP) ไม่มีมาตรการรักษาความมั่นคงปลอดภัย และบริษัทขายของเล่น (DC) ไม่มีการตอบสนองต่อเหตุรั่วไหลที่รวดเร็วและไม่มีการเยียวยา
   โทษปรับ บริษัทขายของเล่น (DC) 500,000 บาท , บริษัทผู้พัฒนาระบบ (DP) 3,000,000 บาท

ช่องทางการติดต่อและแหล่งข้อมูลของ สคส.

- เว็บไซต์ https://www.pdpc.or.th
- ที่อยู่ 120 หมู่ 3 ชั้น 5-7 อาคารรัฐประศาสนภักดี (อาคาร B) ศูนย์ราชการเฉลิมพระเกียรติฯ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
- โทรศัพท์ 02 111 8800
- อีเมล saraban@pdpc.or.th
- Facebook https://www.facebook.com/pdpc.th

Cyber Security และ Risk Assessment

โดย นายชัยรัตน์ ปรีชากร

กองดิจิทัลเพื่อการควบคุมโรค

บทสรุปสำหรับผู้บริหาร

เน้นย้ำว่าความปลอดภัยของข้อมูลผู้ป่วย ผู้เดินทาง ข้อมูลสุขภาพ มีความเชื่อมโยงโดยตรงกับความปลอดภัยในชีวิต ตามหลักการ CIA Triad (Confidentiality, Integrity, Availability) ซึ่งต้องรักษาความลับ ความถูกต้อง ครบถ้วน และความพร้อมใช้งานของข้อมูล และชี้ให้เห็นถึงความสำคัญของการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ซึ่งกำหนดให้ข้อมูลสุขภาพเป็นข้อมูลที่ละเอียดอ่อน และมีบทลงโทษหากเกิดการรั่วไหล การบริหารจัดการความเสี่ยงอย่างเป็นระบบจึงเป็นกระบวนการที่จำเป็นสำหรับหน่วยงานกรมควบคุมโรค เพื่อให้สามารถประเมิน ตอบสนอง และทบทวนความเสี่ยงได้อย่างต่อเนื่องและมีประสิทธิภาพ

หลักการพื้นฐานของความปลอดภัยสารสนเทศ (CIA Triad)

ประกอบด้วย 3 องค์ประกอบหลัก ดังนี้

1. Confidentiality (การรักษาความลับ) การปกป้องข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต ข้อมูลผู้ป่วยต้องถูกเก็บเป็นความลับเพื่อป้องกันการรั่วไหลที่อาจส่งผลกระทบต่อชีวิตและสวัสดิภาพของผู้ป่วย

2. Integrity (ความถูกต้องครบถ้วน) การรับประกันว่าข้อมูลมีความถูกต้องสมบูรณ์และไม่ถูกแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต ข้อมูลทางการแพทย์ที่ผิดพลาดอาจนำไปสู่การวินิจฉัยและการรักษาที่ผิดพลาด ซึ่งเป็นอันตรายอย่างยิ่ง

3. Availability (ความพร้อมใช้) การรับประกันว่าผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและระบบได้เมื่อต้องการ ข้อมูลผู้ป่วยต้องพร้อมใช้งานสำหรับบุคลากรทางการแพทย์ในเวลาที่จำเป็น เพื่อให้การรักษาเป็นไปอย่างต่อเนื่องและทันท่วงที

ภัยคุกคามทางไซเบอร์ที่ต้องตระหนัก

- **Phishing** การหลอกลวงเพื่อขโมยข้อมูลส่วนตัวและรหัสผ่านจากผู้ใช้
- **Ransomware** มัลแวร์ที่เข้ารหัสข้อมูล ทำให้ไม่สามารถเข้าถึงได้จนกว่าจะจ่ายเงินค่าไถ่
- **Data Breach** การรั่วไหลของข้อมูล ซึ่งอาจสร้างความเสียหายต่อความเชื่อมั่นของประชาชนต่อหน่วยงาน
- **SQL Injection** การโจมตีฐานข้อมูลโดยใช้ช่องโหว่ของระบบเพื่อเข้าถึงข้อมูลที่ไม่ควรเปิดเผย
- **Dumpster Diving** การรื้อค้นเอกสารที่ถูกทิ้ง เช่น รายชื่อผู้ป่วย สำเนาบัตรประชาชน หรือใบรายงานผลตรวจ
- **Weak Password** การตั้งรหัสผ่านที่คาดเดาได้ง่าย หรือการใช้รหัสผ่านเดียวกันซ้ำๆ ในหลายระบบ

NIST Cybersecurity Framework

1. Identify (ระบุสินทรัพย์และความเสี่ยง): การทำความเข้าใจและระบุว่าองค์กรมีสินทรัพย์ดิจิทัลที่สำคัญอะไรบ้าง และมีความเสี่ยงใดที่เกี่ยวข้อง เปรียบได้กับ "รู้ว่าเรามีทรัพย์สินสำคัญอะไร"
2. Protect (ป้องกันภัยคุกคาม): การวางมาตรการควบคุมเพื่อป้องกันและจำกัดผลกระทบจากภัยคุกคาม เปรียบได้กับ "การล็อคประตู"
3. Detect (ตรวจพบเหตุผิดปกติ): การพัฒนากลไกเพื่อตรวจจับกิจกรรมหรือเหตุการณ์ที่ผิดปกติทางไซเบอร์ได้อย่างรวดเร็ว เปรียบได้กับ "สัญญาณกันขโมย"
4. Respond (ตอบสนองและควบคุมเหตุการณ์): การกำหนดแผนและกระบวนการเพื่อตอบสนองต่อเหตุการณ์ที่ตรวจพบ เพื่อควบคุมความเสียหาย เปรียบได้กับ "เมื่อโดนแล้วทำอย่างไร"
5. Recover (ฟื้นฟูระบบกลับสู่สภาวะปกติ): การวางแผนเพื่อฟื้นฟูระบบและบริการให้กลับมาทำงานได้ตามปกติหลังเกิดเหตุการณ์ เปรียบได้กับ "การกู้คืนระบบ"

7 กฎเหล็ก (Safe Entry) เพื่อปลอดภัยในการทำงานของเจ้าหน้าที่

1.Accountability (บัญชีใคร บัญชีมัน) ห้ามยืมรหัสผ่านของผู้อื่น หรือจดรหัสผ่านแปะไว้หน้าจอคอมพิวเตอร์

2.Accuracy (ถูกต้องแม่นยำ) ตรวจทานข้อมูลให้ดีก่อนกดบันทึก (Submit) เพื่อป้องกันปัญหาข้อมูลผิดพลาด

3.No Social Media (งดแชร์ข้อมูลหน้างาน) ห้ามส่งภาพหน้าจอที่มีข้อมูลคนไข้ผ่านแอปพลิเคชันสนทนาส่วนตัว (เช่น Line, Messenger) และต้องระมัดระวังการถ่ายภาพในที่ทำงานที่อาจติดภาพหน้าจอคอมพิวเตอร์เป็นพื้นหลัง

4.Storage (เก็บให้ถูกที่) จัดเก็บไฟล์งานบนเซิร์ฟเวอร์กลางของกรมฯ เท่านั้น ห้ามเก็บข้อมูลคนไข้ไว้ในอุปกรณ์ส่วนตัว เช่น Flash Drive หรือบนหน้าจอ Desktop เพื่อป้องกันข้อมูลสูญหายกรณีอุปกรณ์ชำรุดหรือถูกขโมย

5.Secure Disposal (ทำลาย) เอกสารที่มีข้อมูลส่วนบุคคลต้องถูกทำลายผ่านเครื่องทำลายเอกสาร ห้ามนำกระดาษที่มีข้อมูลผู้ป่วยมาใช้ซ้ำ (Reuse)

6.Verification (เช็คก่อนเชื่อ) หากได้รับการติดต่อผ่านแชทหรืออีเมลเพื่อขอข้อมูลลับ/รหัสผ่าน โดยอ้างว่าเป็นผู้บริหารหรือฝ่าย IT ให้โทรศัพท์ยืนยันกับเจ้าของตัวตนโดยตรงก่อนเสมอ เพื่อป้องกันการหลอกลวงสวมรอย

7.Lock & Clear (ลุกแล้วล็อค) กดปุ่ม Windows + L เพื่อล็อคหน้าจอทุกครั้งที่ลุกจากโต๊ะ และเคลียร์เอกสารสำคัญบนโต๊ะเก็บเข้าลิ้นชักให้เรียบร้อยก่อนกลับบ้าน (Clean Desk Policy)

การบริหารจัดการความเสี่ยง (Risk Management)

ความเสี่ยง (Risk) คือ เหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อการบรรลุเป้าหมาย ซึ่งเกิดจากองค์ประกอบ 2 ส่วนคือ ภัยคุกคาม (Threat) เช่น แฮ็กเกอร์, ความประมาทเลินเล่อ และจุดอ่อนที่พบ เช่น รหัสตั้งรหัสผ่านแบบคาดเดาได้ง่าย เช่น "123456" ซึ่งบางระบบเฝ้าระวังด่านฯ ยังพบอยู่บ้าง จึงมี**แนวทางการตอบสนองต่อความเสี่ยง (Risk Response)** มี 4 รูปแบบดังนี้

1.TERMINATE (หลีกเลี่ยง) ให้เลิกใช้ระบบเก่าที่มีช่องโหว่มากเกินกว่าจะแก้ไขได้

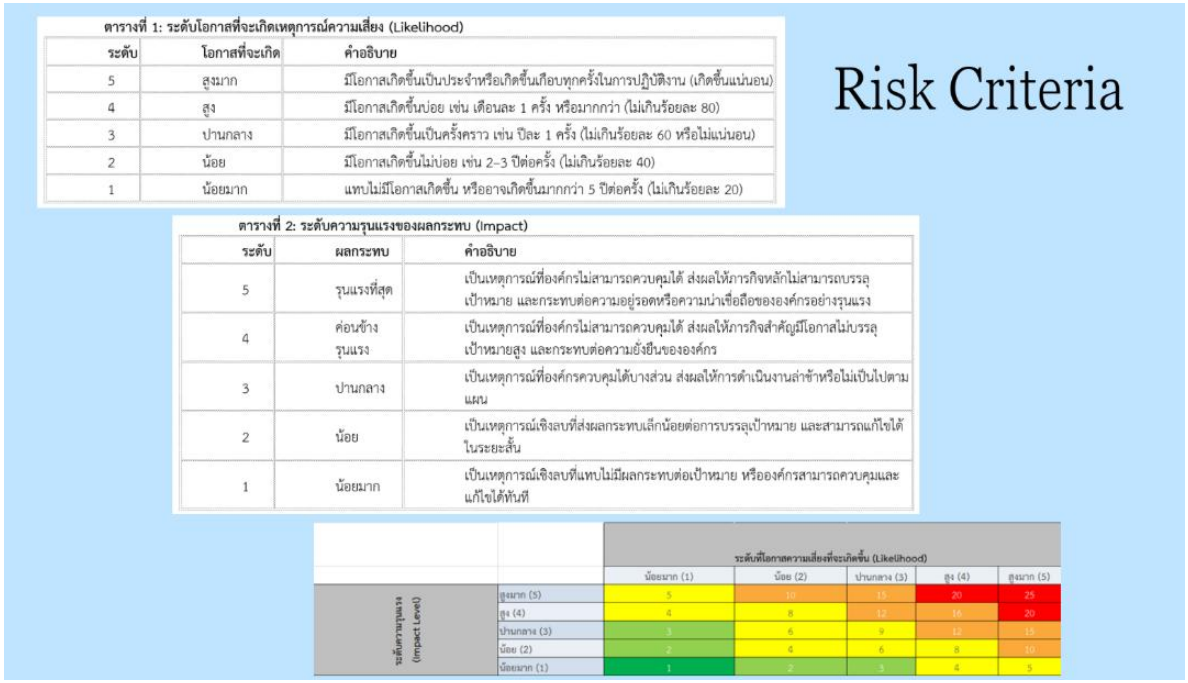
2.TRANSFER (ถ่ายโอน) จ้างผู้ให้บริการคลาวด์ (Cloud Provider) ที่มีมาตรฐานสูงมาดูแล ซึ่งกองด่านฯ วางแผนดำเนินการแล้ว

3.TREAT (ลด) ติดตั้ง Firewall และอบรมพัฒนาทักษะเจ้าหน้าที่เพื่อสร้างความตระหนักรู้

4.TOLERATE (ยอมรับ) ยอมรับความเสี่ยงนั้น หากค่าใช้จ่ายในการป้องกันสูงกว่ามูลค่าของข้อมูลและผลกระทบอยู่ในระดับที่ยอมรับได้

เกณฑ์การประเมินความเสี่ยง

การประเมินความเสี่ยงทำโดยการพิจารณา โอกาสที่จะเกิด (Likelihood) และ ความรุนแรงของผลกระทบ (Impact)



Risk Criteria

ตารางที่ 1: ระดับโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง (Likelihood)

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	มีโอกาสเกิดขึ้นเป็นประจำหรือเกิดขึ้นเกือบทุกครั้งในการปฏิบัติงาน (เกิดขึ้นแน่นอน)
4	สูง	มีโอกาสเกิดขึ้นบ่อย เช่น เดือนละ 1 ครั้ง หรือมากกว่า (ไม่เกินร้อยละ 80)
3	ปานกลาง	มีโอกาสเกิดขึ้นเป็นครั้งคราว เช่น ปีละ 1 ครั้ง (ไม่เกินร้อยละ 60 หรือไม่แน่นอน)
2	น้อย	มีโอกาสเกิดขึ้นไม่บ่อย เช่น 2-3 ปีต่อครั้ง (ไม่เกินร้อยละ 40)
1	น้อยมาก	แทบไม่มีโอกาสเกิดขึ้น หรืออาจเกิดขึ้นมากกว่า 5 ปีต่อครั้ง (ไม่เกินร้อยละ 20)

ตารางที่ 2: ระดับความรุนแรงของผลกระทบ (Impact)

ระดับ	ผลกระทบ	คำอธิบาย
5	รุนแรงที่สุด	เป็นเหตุการณ์ที่องค์กรไม่สามารถควบคุมได้ ส่งผลให้ภารกิจหลักไม่สามารถบรรลุเป้าหมาย และกระทบต่อความอยู่รอดหรือความน่าเชื่อถือขององค์กรอย่างรุนแรง
4	ค่อนข้างรุนแรง	เป็นเหตุการณ์ที่องค์กรไม่สามารถควบคุมได้ ส่งผลให้ภารกิจสำคัญมีโอกาสไม่บรรลุเป้าหมายสูง และกระทบต่อความยั่งยืนขององค์กร
3	ปานกลาง	เป็นเหตุการณ์ที่องค์กรควบคุมได้บางส่วน ส่งผลให้การดำเนินงานล่าช้าหรือไม่เป็นไปตามแผน
2	น้อย	เป็นเหตุการณ์เชิงลบที่ส่งผลกระทบเล็กน้อยต่อการบรรลุเป้าหมาย และสามารถแก้ไขได้ในระยะสั้น
1	น้อยมาก	เป็นเหตุการณ์เชิงลบที่แทบไม่มีผลกระทบต่อเป้าหมาย หรือองค์กรสามารถควบคุมและแก้ไขได้ทันที

ระดับความรุนแรง (Impact Level)	ระดับที่โอกาสความเสี่ยงที่จะเกิดขึ้น (Likelihood)				
	น้อยมาก (1)	น้อย (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
สูงมาก (5)	5	10	15	20	25
สูง (4)	4	8	12	16	20
ปานกลาง (3)	3	6	9	12	15
น้อย (2)	2	4	6	8	10
น้อยมาก (1)	1	2	3	4	5

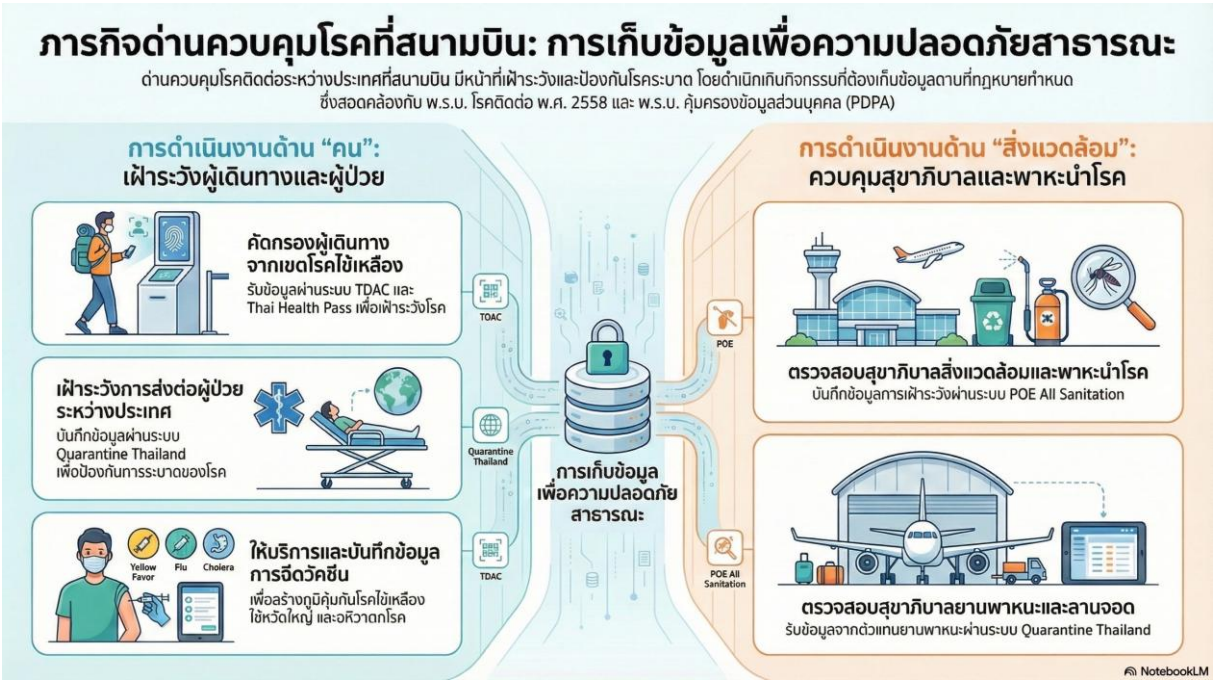
แบ่งกลุ่มฝึกปฏิบัติ
“บทบาทหน้าที่ด่านควบคุมโรคติดต่อระหว่างประเทศ ต่อการจัดการความมั่นคงปลอดภัยของข้อมูลที่เกี่ยวข้องกับฐานข้อมูลการเฝ้าระวัง คัดกรอง ตรวจตราของด่านควบคุมโรคติดต่อระหว่างประเทศ”

ผลผลิตแบ่งกลุ่มฝึกปฏิบัติ กิจกรรมตามบทบาทหน้าที่ของด่านควบคุมโรคติดต่อระหว่างประเทศ ประเภทท่าอากาศยาน

ลำดับ	กิจกรรมตามบทบาทหน้าที่	วัตถุประสงค์ในการเก็บข้อมูล	ฐานกฎหมายที่ใช้เก็บ	ฐานอำนาจตาม PDPA
1	การได้รับข้อมูลผู้เดินทางจากพื้นที่เขตติดโรคไข้เหลืองผ่านระบบ TDAC และดำเนินการลงข้อมูลในระบบ Thai Health Pass	การเฝ้าระวังคัดกรองผู้เดินทางพื้นที่เขตติดโรคไข้เหลือง	พ.ร.บ.โรคติดต่อ พ.ศ.2558 ม.38, ม.39, ม.40	- ฐานหน้าที่ตามกฎหมาย - ฐานประโยชน์สำคัญต่อชีวิต - ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข - ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ
2	การบันทึกข้อมูลการส่งต่อผู้ป่วยจากสายการบินระหว่างประเทศ ด้วยระบบ Quarantine Thailand	การเฝ้าระวังโรคและภัยสุขภาพจากการส่งต่อผู้ป่วยระหว่างประเทศ	พ.ร.บ.โรคติดต่อ พ.ศ.2558 ม.38, ม.39, ม.40 IHR 2005	- ฐานหน้าที่ตามกฎหมาย - ฐานประโยชน์สำคัญต่อชีวิต - ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข - ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ
3	การบันทึกข้อมูลด้านสุขาภิบาลสิ่งแวดล้อมทั่วไปและการเฝ้าระวังพาหะนำโรค ด้วยระบบ Quarantine Thailand (POE All Sanitation)	การเฝ้าระวังสุขาภิบาลสิ่งแวดล้อมทั่วไปและการเฝ้าระวังพาหะนำโรค	พ.ร.บ.โรคติดต่อ พ.ศ.2558 ม.38, ม.39, ม.40 พรบ.การสาธารณสุข พ.ศ. 2535	- ฐานหน้าที่ตามกฎหมาย - ฐานประโยชน์สำคัญต่อชีวิต - ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข - ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ
4	การได้รับข้อมูลจากตัวแทนยานพาหนะผ่านระบบ Quarantine Thailand (POE All Sanitation)	การเฝ้าระวังสุขาภิบาลยานพาหนะและลานจอด	พ.ร.บ.โรคติดต่อ พ.ศ.2558 ม.39, ม.40	- ฐานหน้าที่ตามกฎหมาย - ฐานประโยชน์สำคัญต่อชีวิต

ลำดับ	กิจกรรม ตามบทบาทหน้าที่	วัตถุประสงค์ ในการเก็บข้อมูล	ฐานกฎหมายที่ใช้เก็บ	ฐานอำนาจตาม PDPA
5	การบันทึกข้อมูลผู้รับบริการวัคซีนป้องกันโรค ด้วยระบบ Quarantine Thailand	การเสริมสร้างภูมิกันโรคไข้เหลือง ไข้หวัดใหญ่ และอหิวาตกโรค	พ.ร.บ.โรคติดต่อ พ.ศ.2558 ม.39(5)	- ฐานหน้าที่ตามกฎหมาย - ฐานประโยชน์สำคัญต่อชีวิต - ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะด้านสาธารณสุข - ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญ

การประยุกต์ ใช้ AI ในการนำเสนอผลผลิตแบ่งกลุ่มฝึกปฏิบัติ ประเภทท่าอากาศยาน



ภาพกิจกรรม

ผลผลิตแบ่งกลุ่มฝึกปฏิบัติ กิจกรรมตามบทบาทหน้าที่ของด่านควบคุมโรคติดต่อระหว่างประเทศ ประเภทท่าเรือ

ลำดับ	กิจกรรม ตามบทบาทหน้าที่	วัตถุประสงค์ ในการเก็บข้อมูล	ฐานกฎหมายที่ใช้เก็บ	ฐานอำนาจตาม PDPA
1	เฝ้าระวังคัดกรองผู้เดินทางที่สงสัยป่วย	- เฝ้าระวังอาการตามเอกสารสำแดงทางสุขภาพของผู้เดินทาง หรือใบ ต.8	- พ.ร.บ.โรคติดต่อ พ.ศ.2558 - IHR 2005 - ประกาศกฎกระทรวงสาธารณสุข 2560 - พ.ร.บ.คนเข้าเมือง พ.ศ.2522	- ฐานหน้าที่ตามกฎหมาย
2	การตรวจสุขาภิบาลร้านอาหาร	- เพื่อเฝ้าระวังความปลอดภัยด้านอาหาร - เพื่อจัดทำทะเบียนร้านอาหารและผู้ประกอบการ	- พ.ร.บ.โรคติดต่อ พ.ศ.2558 - IHR 2005 - ประกาศกฎกระทรวงสาธารณสุข 2560	- ฐานหน้าที่ตามกฎหมาย
3	การให้บริการวัคซีน	- เพื่อเฝ้าระวัง ติดตามความครอบคลุมของผู้เดินทาง	- พ.ร.บ.โรคติดต่อ พ.ศ.2558 - IHR 2005 - ประกาศกฎกระทรวงสาธารณสุข 2560	- ฐานหน้าที่ตามกฎหมาย
4	การเฝ้าระวังสุขาภิบาลเรือ	- เพื่อใช้สำหรับเฝ้าระวัง ติดตามผู้เดินทางที่มาจากเขตติดโรค	- พ.ร.บ.โรคติดต่อ พ.ศ.2558 - IHR 2005 - ประกาศกฎกระทรวงสาธารณสุข 2560	- ฐานหน้าที่ตามกฎหมาย
5	บริการทางการแพทย์และการส่งต่อผู้ป่วย	- เพื่อสำหรับการประสานงานติดตามเฝ้าระวังโรคติดต่อ	- พ.ร.บ.โรคติดต่อ พ.ศ.2558 - IHR 2005 - พ.ร.บ.สาธารณสุข พ.ศ.2535	- ฐานหน้าที่ตามกฎหมาย
6	ทะเบียนสื่อสารของคณะทำงานฯประจำช่องทาง	- เพื่อประสานงานสำหรับการตอบโต้ภาวะฉุกเฉิน และการเฝ้าระวังโรค	- พ.ร.บ.โรคติดต่อ พ.ศ.2558 - IHR 2005	- ฐานหน้าที่ตามกฎหมาย
7	รายละเอียดของผู้ต้องกักต่างด้าว	- เพื่อเฝ้าระวังโรค ติดตามของแรงงานต่างด้าว	- พ.ร.บ.คนเข้าเมือง พ.ศ.2522	- ฐานหน้าที่ตามกฎหมาย

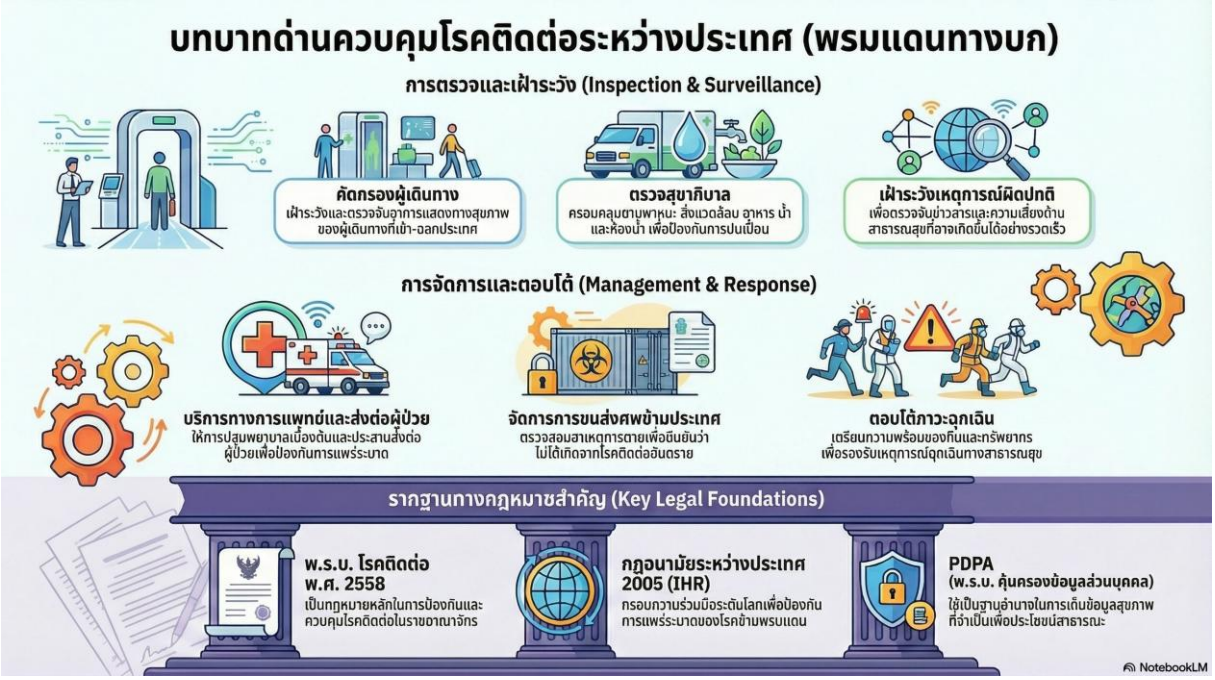
การประยุกต์ ใช้ AI ในการนำเสนอผลผลิตแบ่งกลุ่มฝึกปฏิบัติ ประเภทท่าเรือ

ภาพกิจกรรม

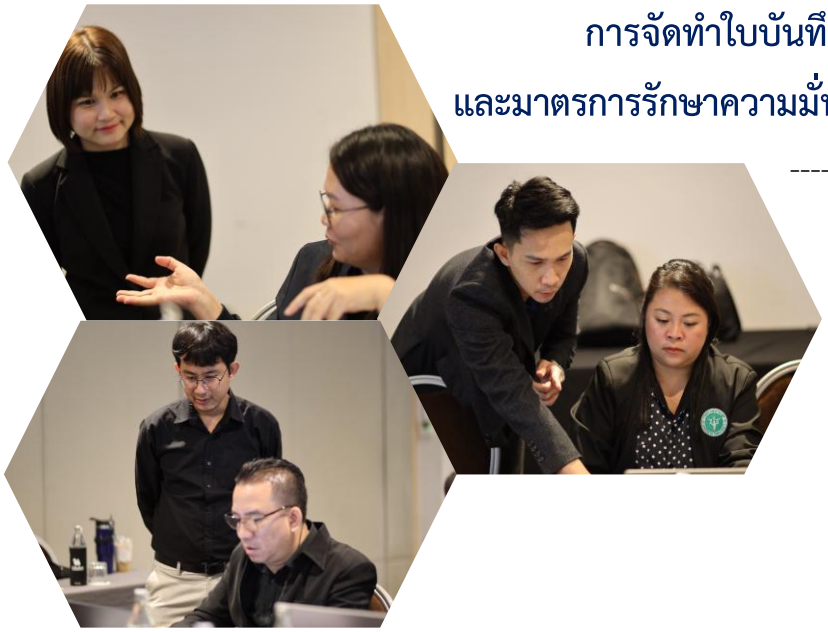
ผลผลิตแบ่งกลุ่มฝึกปฏิบัติ กิจกรรมตามบทบาทหน้าที่ของด่านควบคุมโรคติดต่อระหว่างประเทศ ประเภทพรมแดนทางบก

ลำดับ	กิจกรรมตามบทบาทหน้าที่	วัตถุประสงค์ในการเก็บข้อมูล	ฐานกฎหมายที่ใช้เก็บ	ฐานอำนาจตาม PDPA
1	คัดกรองผู้เดินทาง	การเฝ้าระวังตรวจจับอาการแสดงทางสุขภาพผู้เดินทาง	พ.ร.บ.โรคติดต่อ พ.ศ.2558 พ.ร.บ.คนเข้าเมือง พ.ศ.2522 IHR 2005	ฐานการปฏิบัติ/หน้าที่ตามกฎหมาย ฐานประโยชน์สำคัญต่อชีวิต
2	ตรวจสุขาภิบาลยานพาหนะทางบก	การคัดกรองและการเฝ้าระวังผู้เดินทางเข้าออกระหว่างประเทศ	พ.ร.บ.โรคติดต่อ พ.ศ.2558 IHR 2005	ฐานการปฏิบัติ/หน้าที่ตามกฎหมาย
3	ตรวจสุขาภิบาลสิ่งแวดล้อมและพาหะนำโรค	การเฝ้าระวังโรคที่เกิดจากพาหะนำโรคและการปนเปื้อนในสิ่งแวดล้อม	พ.ร.บ.โรคติดต่อ พ.ศ.2558 IHR 2005	ฐานการปฏิบัติ/หน้าที่ตามกฎหมาย
4	ตรวจสุขาภิบาลอาหาร น้ำ	การเฝ้าระวังโรคที่เกิดจากพาหะนำโรคและการปนเปื้อนทางอาหารและน้ำ	พ.ร.บ.โรคติดต่อ พ.ศ.2558 IHR 2005 พ.ร.บ.สาธารณสุข พ.ศ.2535	ฐานการปฏิบัติ/หน้าที่ตามกฎหมาย
5	ตรวจสุขาภิบาลห้องน้ำ	เพื่อป้องกันเชื้อโรคที่เกิดจากการใช้ส้วมสาธารณะเพื่อให้ผ่านมาตรฐานHAS	พ.ร.บ.โรคติดต่อ พ.ศ.2558 IHR 2005 พ.ร.บ.สาธารณสุข พ.ศ.2535	ฐานการปฏิบัติ/หน้าที่ตามกฎหมาย
6	การส่งต่อผู้ป่วยระหว่างประเทศ	เพื่อให้ผู้ป่วยเข้าถึงบริการรักษาทางการแพทย์และป้องกันการแพร่กระจายทางโรคติดต่อข้ามพรมแดน	พ.ร.บ.โรคติดต่อ พ.ศ.2558 IHR 2005 พ.ร.บ.คนเข้าเมือง พ.ศ.2522 (กรณีเมื่อพบโรคต้องห้าม)	ฐานการปฏิบัติ/หน้าที่ตามกฎหมาย ฐานประโยชน์สำคัญต่อชีวิต
7	การส่งต่อศพระหว่างประเทศ	ตรวจสอบสาเหตุการตายและยืนยันว่าไม่ได้เป็นโรคติดต่อ	พ.ร.บ.โรคติดต่อ พ.ศ.2558 IHR 2005	ฐานการปฏิบัติ/หน้าที่ตามกฎหมาย
8	การบริการทางการแพทย์	เป็นการเฝ้าระวังโรค คัดกรองสุขภาพ และปฐมพยาบาลเบื้องต้น	พ.ร.บ.โรคติดต่อ พ.ศ.2558 IHR 2005	ฐานการปฏิบัติ/หน้าที่ตามกฎหมาย ฐานประโยชน์สำคัญต่อชีวิต
9	การเฝ้าระวังและการรายงานเหตุการณ์ผิดปกติช่องทางระหว่างประเทศ	เพื่อตรวจจับข่าวและเหตุการณ์ที่ผิดปกติ	พ.ร.บ.โรคติดต่อ พ.ศ.2558 IHR 2005	ฐานการปฏิบัติ/หน้าที่ตามกฎหมาย
10	การตอบโต้ภาวะฉุกเฉินระหว่างประเทศ	เป็นการเตรียมความพร้อมเพื่อรองรับเหตุการณ์ฉุกเฉินทางโรคและภัยสุขภาพ	IHR 2005	ฐานการปฏิบัติ/หน้าที่ตามกฎหมาย

การประยุกต์ ใช้ AI ในการนำเสนอผลผลิตแบ่งกลุ่มฝึกปฏิบัติ ประเภทพรมแดนทางบก



ภาพกิจกรรม



การจัดทำใบบันทึกกิจกรรมการประมวลผล (RoPA) และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

โดย นายเทวพร จานนอก

นายกิตติพัทธ์ วรเชษฐ์

นางสาวกรรณิการ์ กาญจนสุวรรณ

กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค

การประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคล เพื่อนำไปประกอบการจัดทำใบบันทึกกิจกรรมการประมวลผล (RoPA) และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของด่านควบคุมโรคติดต่อระหว่างประเทศ

ความเสี่ยง (Risk) คือ เหตุการณ์ที่อาจเกิดขึ้น โดยพิจารณาจาก ความรุนแรงของผลกระทบ (Impact)และความน่าจะเป็นที่จะเกิด (Likelihood)

การบริหารความเสี่ยง การวางแผนกิจกรรมเพื่อควบคุมองค์กรให้ตอบสนองต่อความเสี่ยงนั้นๆ โดยมุ่งเน้นที่การลดความรุนแรงหรือลดโอกาสที่จะเกิดเหตุการณ์

ปัจจัยความเสี่ยง (4 M Risk Factor)

การวิเคราะห์ปัจจัยเสี่ยงครอบคลุม 4 ด้านหลัก ได้แก่:

1. Man ปัจจัยจากตัวบุคคลหรือตำแหน่งงาน
2. Management ปัจจัยจากการบริหารจัดการและคำสั่งปฏิบัติงาน
3. Material ปัจจัยจากวัสดุและอุปกรณ์ที่ใช้ทำงาน
4. Method ปัจจัยจากวิธีการหรือกระบวนการปฏิบัติงาน

เกณฑ์การประเมินระดับความเสี่ยง (Risk Matrix)

ระดับความเสี่ยงเกิดจากการคำนวณคะแนน

"โอกาส (1-5) × ผลกระทบ (1-5)"

โดยมีเกณฑ์ตัดสินดังนี้

- ระดับสูงมาก (17 - 25 คะแนน) ยอมรับไม่ได้ ต้องกำกับดูแลอย่างใกล้ชิด มีมาตรการ
- ระดับสูง (10 - 16 คะแนน) ต้องเฝ้าระวัง
- ระดับปานกลาง (6 - 9 คะแนน) ยอมรับได้ แต่ต้องใช้การควบคุมตามปกติ
- ระดับต่ำ (1 - 5 คะแนน) ไม่ต้องมีมาตรการควบคุมเพิ่มเติม

แนวทางการจัดการข้อมูลด่านควบคุมโรคติดต่อระหว่างประเทศ เพื่อการปกป้องระบบเฝ้าระวังทางคอมพิวเตอร์ เครือข่าย ซอฟต์แวร์ และข้อมูลจากภัยคุกคามทางดิจิทัล

สาระสำคัญ

สถานการณ์สมมติที่เกิดขึ้น

- **เหตุการณ์** ตรวจพบข้อมูลชื่อผู้ใช้งานและรหัสผ่าน (Username/Password) ของบุคลากรกรมควบคุมโรคถูกประกาศขายใน Dark Web
- **ผลกระทบ** พบข้อมูลรั่วไหลจำนวน 3,220 รายการ ซึ่งครอบคลุมผู้ใช้งานจาก 33 **หน่วยงาน** ภายในกรม
- **การแจ้งเตือน** ได้รับการประสานงานจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.), สกมช. และสำนักงานปลัดกระทรวงสาธารณสุข

มาตรการตอบโต้และจัดการเหตุการณ์

เมื่อกองดิจิทัลเพื่อการควบคุมโรคได้รับแจ้ง ได้ดำเนินการตามขั้นตอนดังนี้:

- **ตรวจสอบและรายงาน** ตรวจสอบความถูกต้องของข้อมูลและรายงานผู้บังคับบัญชาทันที
- **ประสานงานหน่วยงาน** แจ้งทั้ง 33 หน่วยงานที่ได้รับผลกระทบ พร้อมส่งแนวทางแก้ไขและแบบรายงานภัยคุกคาม
- **ด้านกฎหมายและการคุ้มครองข้อมูล** แจ้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และส่งรายงานการตรวจสอบการโจมตีเบื้องต้นเพื่อดำเนินการในส่วนที่เกี่ยวข้อง
- **การสนับสนุนทางเทคนิค** ประสานการแก้ไขปัญหาและชี้แจงรายละเอียดเพิ่มเติมให้หน่วยงานต่างๆ
- **การสร้างความตระหนักรู้:** จัดอบรมด้าน Cybersecurity Awareness ให้แก่บุคลากร

ข้อเสนอแนะและมาตรการป้องกันสำหรับหน่วยงาน

เพื่อให้เกิดความปลอดภัยอย่างยั่งยืน หน่วยงานควรปฏิบัติตามแนวทางดังนี้:

1. **วิเคราะห์และป้องกัน** หาสาเหตุของปัญหาและเสนอแนวทางป้องกันส่งให้กองดิจิทัลฯ
2. **ลดช่องโหว่** ทบทวนและยกเลิกระบบที่ไม่ใช้งานแล้วเพื่อลดความเสี่ยง
3. **จัดการรหัสผ่าน** เปลี่ยนรหัสผ่านตามมาตรการที่กรมกำหนด
4. **การตรวจสอบ** จัดทำบันทึกการใช้งานระบบ (Accountability Log) และติดตามการเข้าถึงอย่างต่อเนื่อง
5. **ยกระดับมาตรฐาน** ปรับปรุงระบบให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของกรมฯ

ข้อสั่งการเพิ่มเติมสำหรับเจ้าหน้าที่ด่านควบคุมโรค

- **การเปลี่ยนรหัสผ่าน** กำหนดให้เปลี่ยนรหัสผ่านอย่างน้อย **ทุก 6 เดือน**
- **การเฝ้าระวัง** จัดให้มีเจ้าหน้าที่ตรวจสอบความปลอดภัยประจำแต่ละด่านหรือสำนักงาน
- **การพัฒนาทักษะ** เจ้าหน้าที่ทุกคนต้องเข้ารับการอบรมด้าน Cybersecurity

ภาคผนวก

ผลการประเมินความพึงพอใจ

ประชุมเชิงปฏิบัติการพัฒนาศักยภาพเจ้าหน้าที่ด่านควบคุมโรคฯ ด้านความมั่นคงปลอดภัยของข้อมูลและการจัดการภัยคุกคามทางไซเบอร์ช่องทางเข้าออกประเทศ

---

1. ข้อมูลทั่วไป

กลุ่มประชากรผู้ตอบแบบประเมินความพึงพอใจในครั้งนี้ คือ เจ้าหน้าที่ด่านควบคุมโรคติดต่อระหว่างประเทศ เจ้าหน้าที่สำนักงานป้องกันควบคุมโรคที่ 2,5-6, 8 ,11 และ 12 เจ้าหน้าที่กองด่านควบคุมโรคติดต่อระหว่างประเทศและกักกันโรค เจ้าหน้าที่หรือผู้ดูแลระบบเทคโนโลยีสารสนเทศ (IT) สำนักงานป้องกันควบคุมโรค ที่ตอบประเมินความพึงพอใจมา ทั้งหมด 34 คน โดยแบ่งเป็นเพศชาย จำนวน 16 คน คิดเป็นร้อยละ 47.05 เพศหญิง จำนวน 18 คน คิดเป็นร้อยละ 52.95 มีอายุระหว่าง 20 – 30 ปี จำนวน 4 คน คิดเป็นร้อยละ 11.76 รองลงมา คือ อายุ 31 - 40 ปี จำนวน 25 คน คิดเป็นร้อยละ 73.53 และอายุ 41 ปีขึ้นไป จำนวน 5 คน คิดเป็นร้อยละ 14.71 รายละเอียด ดังแสดงในตารางที่ 1

ตารางที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม (N = 34)

ข้อมูลทั่วไป	จำนวน	ร้อยละ
เพศ		
ชาย	16	47.05
หญิง	18	52.95
อายุ (ปี)		
20 – 30 ปี	4	11.76
31 – 40 ปี	25	73.53
41 ปี ขึ้นไป	5	14.70
ตำแหน่ง		
นักวิชาการสาธารณสุข	25	73.53
พยาบาลวิชาชีพ	1	2.94
เจ้าพนักงานสาธารณสุข	2	5.88
นักจัดการงานทั่วไป นักทรัพยากรบุคคล นักวิเคราะห์นโยบายและแผน นักวิชาการเผยแพร่	4	11.76
นักวิชาการคอมพิวเตอร์	2	5.88

หัวข้อ	การแปรผลความพึงพอใจ	ค่าเฉลี่ย	S.D.
ด้านวิทยากร			
1.หลักการและสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	**มากที่สุด**	4.55	0.53
2.Cyber Security และ Risk Assessment	**มากที่สุด**	4.60	0.52
3.บทบาทหน้าที่ด่านควบคุมโรคติดต่อระหว่างประเทศ ต่อการจัดการความมั่นคงปลอดภัยของข้อมูลที่เกี่ยวข้องกับฐานข้อมูลการเฝ้าระวัง คัดกรอง ตรวจตราของด่านควบคุมโรคติดต่อระหว่างประเทศ	**มากที่สุด**	4.63	0.50
4.การจัดทำใบบันทึกกิจกรรมการประมวลผล (RoPA) และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล	**มากที่สุด**	4.66	0.49
ด้านสภาพแวดล้อม			
1.ด้านสถานที่ เวลา และอาหาร	**มากที่สุด**	4.65	0.50
2.ด้านการมีส่วนร่วม	**มากที่สุด**	4.64	0.49
ความพึงพอใจต่อการจัดประชุมภาพรวม	**มากที่สุด**	**4.62**	**0.49**

ผลการวิเคราะห์แบบประเมินความพึงพอใจโดยใช้สถิติเชิงพรรณนา พบว่า ผู้เข้าร่วมประชุมมีความพึงพอใจในระดับมากทุกด้าน แสดงถึงประสิทธิภาพของการดำเนินโครงการใน**ระดับสูง** โดยมีปัจจัยสำคัญดังนี้

- เนื้อหามีความสอดคล้องกับบริบทการปฏิบัติงานจริง
- วิทยากรมีความรู้ ความเชี่ยวชาญ และสามารถถ่ายทอดเนื้อหาได้อย่างชัดเจน
- กระบวนการจัดกิจกรรมเปิดโอกาสให้เจ้าหน้าที่ด่านฯได้แลกเปลี่ยนและมีส่วนร่วม
- การบริหารจัดการด้านสถานที่และสิ่งอำนวยความสะดวกมีความเหมาะสม เดินทางสะดวก

โดยหัวข้อที่ผลประเมินความพึงพอใจของผู้เข้าร่วมประชุมมากที่สุด และได้รับความสำคัญ คือ **บทบาทหน้าที่ด่านควบคุมโรคติดต่อระหว่างประเทศ ต่อการจัดการความมั่นคงปลอดภัยของข้อมูลที่เกี่ยวข้องกับฐานข้อมูลการเฝ้าระวัง คัดกรอง ตรวจตราของด่านควบคุมโรคติดต่อระหว่างประเทศ** ซึ่งเป็นกิจกรรมกลุ่มแบ่งตามบทบาทหน้าที่ทำให้ทราบและเกิดการแลกเปลี่ยนเรียนรู้ตามบริบทด่านฯของตนเอง

ข้อเสนอแนะ

- พัฒนาเนื้อหาและทักษะการปฏิบัติ หรือ Workshop เพิ่มเติม เพื่อเสริมสร้างการประยุกต์ปัญญาประดิษฐ์เพื่อนำมาใช้สนับสนุนการดำเนินงานความมั่นคงปลอดภัยของข้อมูลและการจัดการภัยคุกคามทางไซเบอร์ช่องทางเข้าออกประเทศ
- ควรจัดการประชุมในลักษณะต่อเนื่องเน้นการใช้งานระบบเฝ้าระวังและการจัดการข้อมูลที่ปลอดภัย เพื่อพัฒนาศักยภาพบุคลากรอย่างมีประสิทธิภาพและขยายกลุ่มเป้าหมายให้ครอบคลุมด่านฯอื่นๆ