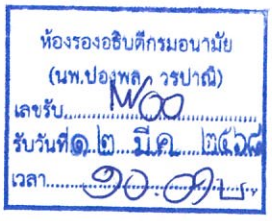


บันทึกข้อความ

ส่วนราชการ กองแผนงาน กลุ่มดิจิทัลเทคโนโลยีและระบบข้อมูล โทร. ๐ ๒๕๙๐ ๔๗๘๗

ที่ สธ ๐๙๐๕.๐๔/๔๒๑ **วันที่** ๑๑ มีนาคม ๒๕๖๘

เรื่อง ขอส่งสรุปการประชุมเชิงปฏิบัติการ เรื่อง "การพัฒนาศักยภาพภาคีเครือข่ายบุคลากรด้านเทคโนโลยีดิจิทัล กรมอนามัย ปี ๒๕๖๘"

เรียน อธิบดีกรมอนามัย

ตามที่กรมอนามัย ได้อนุมัติให้กองแผนงานดำเนินการจัดประชุมเชิงปฏิบัติการ เรื่อง "การพัฒนาศักยภาพภาคีเครือข่ายบุคลากรด้านเทคโนโลยีดิจิทัล กรมอนามัย ปี ๒๕๖๘" ระหว่างวันที่ ๒๔ – ๒๖ กุมภาพันธ์ ๒๕๖๘ ณ บ้านริมแคว แพริมน้ำ รีสอร์ท อำเภอไทรโยค จังหวัดกาญจนบุรี นั้น

ในการนี้ กองแผนงานขอส่งสรุปการประชุมเชิงปฏิบัติการ เรื่อง "การพัฒนาศักยภาพภาคีเครือข่ายบุคลากรด้านเทคโนโลยีดิจิทัล กรมอนามัย ปี ๒๕๖๘" รายละเอียดตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ จะเป็นพระคุณ

(นายนุกูลกิจ พุกาธร)
ผู้อำนวยการกองแผนงาน กรมอนามัย

ทราบ

(นายปองพล วรปาณิ)
รองอธิบดีกรมอนามัย ปฏิบัติราชการแทน
อธิบดีกรมอนามัย
๑๒ มี.ค. ๒๕๖๘

กรมอนามัย
กองแผนงาน

สรุปผลการประชุมเชิงปฏิบัติการ
เรื่อง “การพัฒนาศักยภาพภาคีเครือข่ายบุคลากรด้านเทคโนโลยีดิจิทัลกรมอนามัย ปี ๒๕๖๘”

ระหว่างวันที่ ๒๔ – ๒๖ กุมภาพันธ์ ๒๕๖๘
ณ ห้องประชุมทองกวาว บ้านริมแคว แพริมน้ำ รีสอร์ท อ.ไทรโยค จ.กาญจนบุรี

จัดทำโดย
กลุ่มดิจิทัลส่งเสริมสุขภาพ
กองแผนงาน กรมอนามัย

สรุปผลการประชุมเชิงปฏิบัติการ
เรื่อง "การพัฒนาศักยภาพภาคีเครือข่ายบุคลากรด้านเทคโนโลยีดิจิทัลกรมอนามัย ปี ๒๕๖๘"
ระหว่างวันที่ ๒๔ – ๒๖ กุมภาพันธ์ ๒๕๖๘
ณ ห้องประชุมทองกวาว บ้านริมแคว แพริมน้ำ รีสอร์ท อ.ไทรโยค จ.กาญจนบุรี
****

ประธานเปิดการประชุม :

ดร.นายแพทย์ปองพล วรปาณิ รองอธิบดีกรมอนามัย

ผู้กล่าวรายงานการประชุม :

นายนุกูลกิจ พุกาธร ผู้อำนวยการกองแผนงาน

ผู้เข้าร่วมการประชุม : จำนวน ๕๐ คน ประกอบด้วย

- ผู้บริหารกรมอนามัย
- บุคลากรกรมอนามัยทั้งส่วนกลางและส่วนภูมิภาค
- วิทยากร
- คณะทำงาน
- ผู้สังเกตการณ์

กองแผนงาน ได้จัดประชุมเชิงปฏิบัติการ เรื่อง "การพัฒนาศักยภาพภาคีเครือข่ายบุคลากรด้านเทคโนโลยีดิจิทัลกรมอนามัย ปี ๒๕๖๘" ระหว่างวันที่ ๒๔ – ๒๖ กุมภาพันธ์ ๒๕๖๘ ณ ห้องประชุมทองกวาว บ้านริมแคว แพริมน้ำ รีสอร์ท อ.ไทรโยค จ.กาญจนบุรี เพื่อเสริมสร้างความมั่นคงในการดำเนินงานและป้องกันภัยคุกคามที่อาจเกิดขึ้นกับข้อมูลและระบบสารสนเทศต่าง ๆ ของกรมอนามัย โดยมีเป้าหมายในการเสริมสร้างความรู้ ความเข้าใจและทักษะที่จำเป็นแก่บุคลากรของกรมอนามัย ในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ

วันที่ ๒๔ กุมภาพันธ์ ๒๕๖๘

๑. การบรรยาย เรื่อง "PDPA กับหน่วยงานภาครัฐ : แนวทางการปฏิบัติตามกฎหมายอย่างมีประสิทธิภาพ" และฝึกปฏิบัติ เรื่อง "สร้าง ROPA ฉบับสมบูรณ์ : แนวทางการจัดทำบันทึกรายการกิจกรรมประมวลผลข้อมูลส่วนบุคคล"

โดย โดย นางสาวอุมารัตน์ โพธิ์ชัย บริษัท โทรคมนาคมแห่งชาติ จำกัด

วัตถุประสงค์ : เพื่อให้ผู้เข้าร่วมอบรมมีความรู้ความเข้าใจเกี่ยวกับหลักการสำคัญของ พระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

เนื้อหา/บทสรุป

กรมอนามัยในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) มีหน้าที่ในการคุ้มครองและรักษาความปลอดภัยของข้อมูลส่วนบุคคล และกำหนดมาตรฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย เพื่อสร้างความเชื่อมั่นให้แก่ประชาชนและภาคธุรกิจ

๑. กฎหมายที่เกี่ยวข้อง

๑.๑ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑.๒ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑.๓ พ.ร.บ. บริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

๑.๔ พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

๑.๕ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ ๒๕๖๐

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ๒๕๖๐ มาตรา ๓๒ กำหนดให้บุคคลมีสิทธิในความเป็นส่วนตัว และได้รับความคุ้มครองจากการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นหลักการสำคัญที่นำไปสู่การตรา พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ เพื่อให้เกิดการคุ้มครองสิทธิของเจ้าของข้อมูลอย่างมีประสิทธิภาพ

๒. การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

PDPA บังคับใช้กับบุคคลหรือนิติบุคคลที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล ไม่ว่าจะอยู่ในรูปแบบอิเล็กทรอนิกส์หรือไม่ก็ตาม โดยผู้อยู่ภายใต้ข้อบังคับตามกฎหมาย ได้แก่

- องค์กรภาครัฐและภาคเอกชน ซึ่งอยู่ในราชอาณาจักร
- ผู้ควบคุมหรือผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งอยู่ในราชอาณาจักร หรือแม้อยู่ต่างประเทศแต่ให้บริการแก่บุคคลในประเทศไทย

๓. ข้อมูลส่วนบุคคล

ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้โดยตรงหรือโดยอ้อม เช่น ชื่อ-นามสกุล เลขประจำตัวประชาชน หมายเลขโทรศัพท์ อีเมล หรือข้อมูลชีวภาพ เป็นต้น

๓.๑ ข้อมูลส่วนบุคคล แบ่งเป็น ๒ ประเภท ดังนี้

- ข้อมูลส่วนบุคคลทั่วไป (General Personal Data)
- ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ตามมาตรา ๒๖ เช่น เชื้อชาติ ศาสนา ข้อมูลสุขภาพ ข้อมูลชีวภาพ เป็นต้น

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

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

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

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

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

๔.๕ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) คือ หน่วยงานของรัฐที่มีหน้าที่กำกับดูแล ให้คำแนะนำ และบังคับใช้กฎหมาย PDPA รวมถึงพิจารณาโทษเมื่อมีการละเมิดข้อมูล

๕. บันทึกข้อตกลงการประมวลผลข้อมูล (DPA : Data Processing Agreement)

DPA คือ ข้อตกลงทางกฎหมายระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล เพื่อกำหนดข้อกำหนดและแนวทางปฏิบัติในการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

๖. วงจรชีวิตของข้อมูล (Data Life Cycle) ประกอบด้วย

- การเก็บรวบรวมข้อมูล
- การจัดเก็บและรักษาข้อมูล
- การใช้ข้อมูล
- การแบ่งปันและถ่ายโอนข้อมูล
- การทำลายข้อมูล

๗. ROPA (Record of Processing Activities)

บันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล เป็นเอกสารที่องค์กรต้องจัดทำและบันทึกไว้ เพื่อแสดงต่อเจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ และเป็นหลักฐานว่าองค์กรปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูล

๗.๑ องค์ประกอบของ RoPA ดังนี้

- ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
- การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม
- การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง
- คำอธิบายเกี่ยวกับมาตราการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)

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

- Privacy Notice: การแจ้งให้เจ้าของข้อมูลทราบถึงวิธีการและเหตุผลในการประมวลผลข้อมูล
- Privacy Policy: นโยบายขององค์กรที่กำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคล

๙. ตกลงการประมวลผลข้อมูล (Data Processing Agreement)

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

วันที่ ๒๕ กุมภาพันธ์ ๒๕๖๘

๒. การบรรยาย เรื่อง การสแกนช่องโหว่ระบบสารสนเทศ ด้วยโปรแกรม Nessus" และฝึกปฏิบัติเรื่อง "VA Scan Report : สร้างรายงานและเสนอแนวทางการแก้ไขช่องโหว่ระบบสารสนเทศของหน่วยงาน"

โดย นายสุทธิรัตน์ ปิ่นสญชัย บริษัท อินฟอร์เมชั่น แอนด์ คอนซัลแตนท์ จำกัด

วัตถุประสงค์ : เพื่อเสริมสร้างความรู้และทักษะให้กับบุคลากรในการสแกนช่องโหว่ของระบบสารสนเทศด้วยโปรแกรม Nessus พร้อมทั้งฝึกปฏิบัติการสร้างรายงาน VA Scan Report และนำเสนอแนวทางการแก้ไขช่องโหว่เพื่อเพิ่มความมั่นคงปลอดภัยของระบบสารสนเทศในหน่วยงานให้เป็นไปตามมาตรฐานที่กำหนด

เนื้อหา/บทสรุป

ปัจจุบันหน่วยงานภาครัฐเป็นเป้าหมายสำคัญของการโจมตีทางไซเบอร์ เนื่องจากมักมีข้อมูลสำคัญ เช่น ข้อมูลประชาชน ข้อมูลทางการเงิน และโครงสร้างพื้นฐานของประเทศ ซึ่งหากถูกโจมตี อาจส่งผลกระทบต่อความมั่นคงของรัฐและประชาชนโดยรวม

๑. ภัยคุกคามทางไซเบอร์ที่มักเกิดขึ้นกับองค์กรภาครัฐ

๑.๑ มัลแวร์เรียกค่าไถ่ (Ransomware)

๑.๒ การป้อนข้อมูลที่เป็นอันตราย (Injection)

๑.๓ DDoS (Distributed Denial of Service)

๑.๔ อีเมลและเว็บไซต์ปลอมเพื่อหลอกลวง (Phishing & Spear Phishing)

๑.๕ การโจมตีช่องโหว่ที่ยังไม่มีแพตช์แก้ไข (Zero-Day Attacks)

๒. ความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ในยุคดิจิทัลที่มีการใช้เทคโนโลยีสารสนเทศอย่างแพร่หลาย ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) กลายเป็นประเด็นสำคัญสำหรับทุกองค์กร เนื่องจากภัยคุกคามทางไซเบอร์มีความซับซ้อนและเพิ่มขึ้นอย่างต่อเนื่อง การโจมตีทางไซเบอร์สามารถสร้างความเสียหายต่อข้อมูล ระบบเครือข่าย และทรัพย์สินทางดิจิทัลได้อย่างร้ายแรง ซึ่งอาจส่งผลกระทบต่อชื่อเสียงขององค์กรและการดำเนินธุรกิจ

๒.๑ การรักษาความมั่นคงปลอดภัยทางไซเบอร์มีความสำคัญในหลายด้าน ดังนี้

- ป้องกันข้อมูลรั่วไหล: ช่วยป้องกันการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต เช่น ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน หรือข้อมูลทางธุรกิจ
- ลดความเสี่ยงจากการโจมตี: สามารถลดโอกาสในการถูกโจมตีจากแฮกเกอร์ หรือมัลแวร์ที่พยายามเข้าถึงระบบโดยไม่ได้รับอนุญาต
- สร้างความน่าเชื่อถือให้กับองค์กร: การมีระบบรักษาความปลอดภัยที่ดีช่วยเพิ่มความไว้วางใจจากลูกค้าและพันธมิตรทางธุรกิจ
- ปฏิบัติตามกฎหมายและข้อกำหนด: หลายองค์กรต้องปฏิบัติตามมาตรฐานและกฎหมายด้านความปลอดภัยทางไซเบอร์ เช่น GDPR, ISO ๒๗๐๐๑, NIST

๓. ความรู้เบื้องต้นเกี่ยวกับโปรแกรม Nessus

Nessus เป็นซอฟต์แวร์ที่ใช้สำหรับสแกนและประเมินช่องโหว่ในระบบเครือข่ายและอุปกรณ์ต่างๆ เพื่อช่วยให้องค์กรสามารถตรวจสอบและป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ โปรแกรม Nessus พัฒนาโดยบริษัท Tenable และได้รับการยอมรับในระดับสากลสำหรับการตรวจสอบช่องโหว่ทางไซเบอร์ (Vulnerability Assessment) โดยสามารถตรวจจับจุดอ่อนในระบบ เช่น การตั้งค่าที่ไม่ปลอดภัย, ซอฟต์แวร์ที่ล้าสมัย, การเปิดพอร์ตที่ไม่จำเป็น และการโจมตีที่อาจเกิดขึ้นจากแฮกเกอร์

Nessus มีความสามารถในการสแกนทั้งเครือข่ายภายใน (Internal Network) และเครือข่ายภายนอก (External Network) พร้อมทั้งให้คำแนะนำในการแก้ไขปัญหาเพื่อเสริมสร้างความมั่นคงปลอดภัยของระบบไอที โดยสามารถใช้ได้กับหลายระบบปฏิบัติการ เช่น Windows, Linux และ macOS

๔. ขั้นตอนเตรียมการก่อนการติดตั้งและใช้งานโปรแกรม Nessus

๔.๑ ตรวจสอบความต้องการของระบบ (System Requirements)

๔.๒ ลงทะเบียนบัญชี Nessus และดาวน์โหลดซอฟต์แวร์

๔.๓ ตรวจสอบสิทธิ์และการตั้งค่าของระบบ

๔.๔ เตรียมรายการเป้าหมายที่ต้องการสแกน

๕. วิธีการใช้งานโปรแกรม Nessus

๕.๑ ติดตั้ง Nessus

- ดาวน์โหลด Nessus จาก Tenable
- ติดตั้งตามระบบปฏิบัติการที่รองรับ (Windows, Linux, macOS)
- ลงทะเบียนและเปิดใช้งาน License

๕.๒ ตั้งค่า Nessus

- เข้าสู่ระบบผ่านเว็บเบราว์เซอร์ (https://localhost:๘๘๓๔/)
- ตั้งค่าผู้ใช้และการกำหนดสิทธิ์
- อัปเดต Plugin เพื่อให้ Nessus มีฐานข้อมูลช่องโหว่ล่าสุด

๕.๓ สแกนระบบ

- ไปที่ Scans > New Scan
- เลือกประเภทการสแกน เช่น Basic Network Scan
- กำหนด Target (IP/Domain) ที่ต้องการสแกน
- ปรับแต่งค่าต่างๆ (เลือก Policy, ตั้งเวลา ฯลฯ)
- กด Launch เพื่อเริ่มสแกน

๕.๔ วิเคราะห์ผลการสแกน

- เมื่อสแกนเสร็จ ให้เปิดดู Reports
- Nessus จะจัดระดับความร้ายแรงของช่องโหว่เป็น Critical, High, Medium, Low
- คลิกดูรายละเอียดช่องโหว่ และนำไปใช้ในการปรับปรุงระบบ

๕.๕ แก้ไขและปรับปรุงความปลอดภัย

- ใช้คำแนะนำจาก Nessus เพื่ออุดช่องโหว่
- ติดตั้งแพตช์อัปเดตระบบ
- กำหนดค่า Firewall และ Policy ที่เหมาะสม
- สแกนซ้ำเพื่อให้แน่ใจว่าช่องโหว่ถูกแก้ไขแล้ว

วันที่ ๒๖ กุมภาพันธ์ ๒๕๖๘

๓. การอภิปราย เรื่อง "แนวทางการบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย กรมอนามัย"

ผู้อภิปราย นายสมยศ หาญวงศ์ บริษัท อินฟอร์เมชั่น แอนด์ คอนซัลแตนท์ จำกัด

นายนันทนิจ จิตตเกษม บริษัท อินฟอร์เมชั่น แอนด์ คอนซัลแตนท์ จำกัด

ผู้ดำเนินการอภิปราย นางสาวมัณฑนา ควรพินิจ กองแผนงาน

วัตถุประสงค์ : เพื่อกำหนดแนวทางการบริหารจัดการเซิร์ฟเวอร์ของกรมอนามัยให้มีประสิทธิภาพ มั่นคง ปลอดภัย เป็นไปตามมาตรฐานและกฎหมายที่เกี่ยวข้อง รองรับการบูรณาการระบบสารสนเทศและการให้บริการด้านสุขภาพได้อย่างต่อเนื่องและยั่งยืน

เนื้อหา/บทสรุป

เครื่องคอมพิวเตอร์แม่ข่าย (Server) เป็นโครงสร้างพื้นฐานสำคัญในการให้บริการระบบสารสนเทศของกรมอนามัย ซึ่งมีบทบาทในการจัดเก็บ ประมวลผล และเผยแพร่ข้อมูลด้านสาธารณสุข การบริหารจัดการที่มีประสิทธิภาพจะช่วยเพิ่มความเสถียร ความปลอดภัย และประสิทธิภาพของระบบ

๑. ขั้นตอนการดูแลหลังได้รับเครื่อง Server

๑.๑ ติดตั้งอัปเดตและแพตช์

- ทำการติดตั้งอัปเดตและแพตช์ล่าสุด เพื่อแก้ไขข้อบกพร่องและเสริมความปลอดภัยของระบบ

๑.๒ ตั้งค่าระบบความปลอดภัย

- เปิดใช้งาน Firewall
- ตั้งค่ารหัสผ่านที่มีความซับซ้อน และกำหนดนโยบายด้านความปลอดภัย

๑.๓ ตรวจสอบและตั้งค่าการล็อกเหตุการณ์

- เปิดใช้งานระบบบันทึกเหตุการณ์ (Event Logging) เพื่อเก็บข้อมูลกิจกรรมบนเซิร์ฟเวอร์

๑.๔ ติดตั้งซอฟต์แวร์ป้องกันไวรัส

- ติดตั้งซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ เพื่อป้องกันภัยคุกคามทางไซเบอร์

๑.๕ ติดตั้งแอปพลิเคชันที่จำเป็น

- ติดตั้งซอฟต์แวร์และแอปพลิเคชันที่จำเป็นสำหรับการทำงานของเซิร์ฟเวอร์ เช่น ฐานข้อมูล และเว็บเซิร์ฟเวอร์

๑.๖ กำหนดค่า Backup

- ตั้งค่าระบบสำรองข้อมูลอย่างเหมาะสม เพื่อป้องกันการสูญเสียข้อมูลสำคัญ

๑.๗ ตรวจสอบระบบ

- ติดตามสถานะการทำงานของเซิร์ฟเวอร์ และดำเนินการแก้ไขปัญหาที่เกิดขึ้น

๑.๘ บำรุงรักษา

- ดำเนินการบำรุงรักษาระบบอย่างสม่ำเสมอ รวมถึงการอัปเดตซอฟต์แวร์และระบบปฏิบัติการ

๒. การบรรยาย เรื่อง "แนวทางการจัดหาครุภัณฑ์คอมพิวเตอร์ กรมอนามัย"

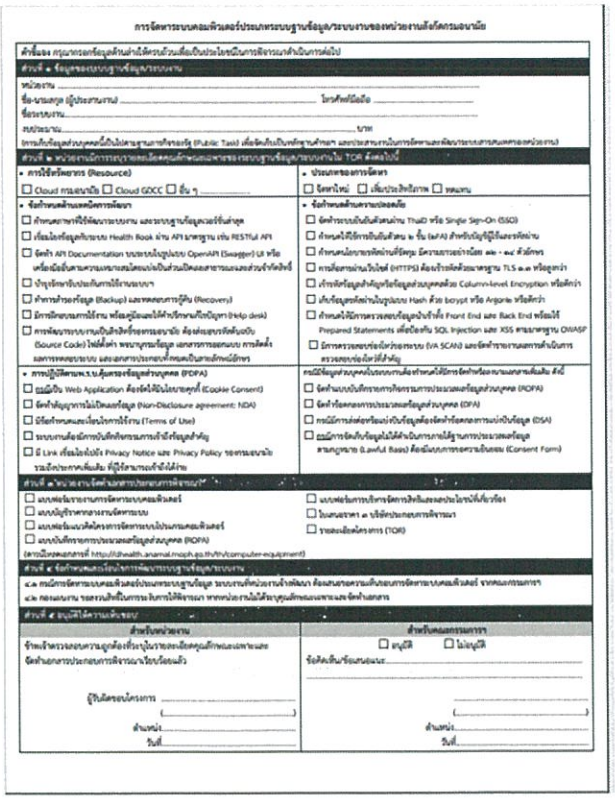
โดย นายสุชาญ กิจลือเลิศ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

วัตถุประสงค์ : เพื่อให้ผู้เข้าร่วมอบรมทราบแนวทางการจัดหาครุภัณฑ์คอมพิวเตอร์ กรมอนามัย

เนื้อหา/บทสรุป

นายสุชาญ กิจลือเลิศ นักวิชาการคอมพิวเตอร์ปฏิบัติการ ได้นำเสนอร่างแบบฟอร์มการจัดหาระบบคอมพิวเตอร์ประเภทระบบฐานข้อมูล/ระบบงาน ให้แก่บุคลากรกรมอนามัย เพื่อให้หน่วยงานที่มีความประสงค์จัดหาระบบคอมพิวเตอร์ประเภทดังกล่าวใช้เป็นแนวทางในการดำเนินการ

โดยหน่วยงานที่มีความประสงค์จะจัดหาระบบฐานข้อมูลหรือระบบงาน จำเป็นต้องดำเนินการกรอกข้อมูลในแบบฟอร์มดังกล่าว เพื่อเป็นการเตรียมความพร้อมในการพัฒนาระบบงานของหน่วยงาน ทั้งนี้ ข้อมูลที่ได้รับจะถูกนำเสนอให้คณะกรรมการขับเคลื่อนการส่งเสริมสุขภาพและอนามัยสิ่งแวดล้อม กรมอนามัย (กลุ่มที่ ๕: กลุ่มพัฒนาระบบดิจิทัลเพื่อส่งเสริมสุขภาพและอนามัยสิ่งแวดล้อม) และคณะกรรมการจัดหาระบบคอมพิวเตอร์ กรมอนามัย พิจารณาต่อไป



การจัดหาระบบคอมพิวเตอร์ประเภทระบบฐานข้อมูล/ระบบงานของหน่วยงานสังกัดกรมอนามัย

การดำเนินงานต่อไป

๑. ทุกหน่วยงานส่วนกลาง และส่วนภูมิภาค ที่ต้องการจัดหาครุภัณฑ์คอมพิวเตอร์ กรอกข้อมูลในแบบฟอร์มการจัดหาระบบคอมพิวเตอร์ประเภทระบบฐานข้อมูล/ระบบงาน เพื่อเสนอคณะกรรมการขับเคลื่อนการส่งเสริมสุขภาพและอนามัยสิ่งแวดล้อม กรมอนามัย (กลุ่มที่ ๕: กลุ่มพัฒนาระบบดิจิทัล เพื่อส่งเสริมสุขภาพและอนามัยสิ่งแวดล้อม) และคณะกรรมการจัดหาระบบคอมพิวเตอร์ กรมอนามัย พิจารณา

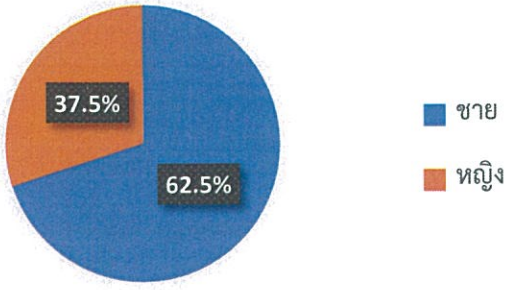
สรุปแบบประเมินความพึงพอใจในการจัดการประชุมเชิงปฏิบัติการ
ขับเคลื่อนการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ ของกรมอนามัย

๑. ข้อมูลทั่วไป

๑.๑ เพศ

- ชาย ๓๖ คน
- หญิง ๑๔ คน

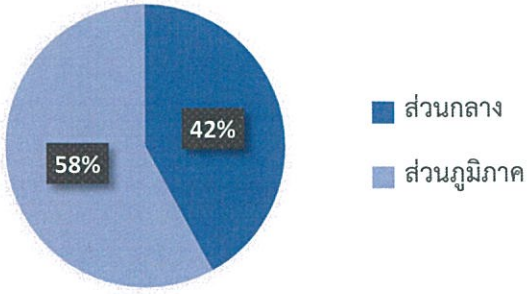
รวม ๕๐ คน



๑.๒ หน่วยงาน

- หน่วยงานส่วนกลาง ๑๒ หน่วยงาน
- หน่วยงานส่วนภูมิภาค ๑๔ หน่วยงาน

รวม ๒๖ หน่วยงาน



๒. ระดับความพึงพอใจต่อการประชุมฯ

๒.๑ ความสอดคล้องของเนื้อหาสาระกับวัตถุประสงค์
- มากที่สุด ร้อยละ ๘๑.๒๕%
- มาก ร้อยละ ๑๘.๗๕%

๒.๒ ประโยชน์ของการประชุมฯ ในครั้งนี้ต่อการปฏิบัติงาน
- มากที่สุด ร้อยละ ๘๑.๒๕%
- มาก ร้อยละ ๑๘.๗๕%

๒.๓ สถานที่ในการประชุมฯ เหมาะสมหรือไม่
- มากที่สุด ร้อยละ ๖๕.๖๓%
- มาก ร้อยละ ๒๕%
- ปานกลาง ร้อยละ ๙.๓๘%

๒.๔ ระยะเวลาในการประชุมฯ เหมาะสมหรือไม่
- มากที่สุด ร้อยละ ๖๘.๗๕%
- มาก ร้อยละ ๒๕%
- ปานกลาง ร้อยละ ๓.๑๓%
- น้อยที่สุด ร้อยละ ๓.๑๓%

๒.๕ อาหารและอาหารว่าง มีความเหมาะสมหรือไม่
- มากที่สุด ร้อยละ ๖๘.๗๕%
- มาก ร้อยละ ๒๑.๘๘%
- ปานกลาง ร้อยละ ๙.๓๘%

๒.๖ ความรอบรู้ในเนื้อหาของการประชุมฯ

- มากที่สุด ร้อยละ ๗๕%
- มาก ร้อยละ ๒๕%

๒.๗ เทคนิค/วิธีการ/การถ่ายทอดให้เข้าใจได้ง่าย

- มากที่สุด ร้อยละ ๗๑.๘๘%
- มาก ร้อยละ ๒๘.๑๓%

๒.๘ ความชัดเจนในการบรรยายและการตอบคำถาม

- มากที่สุด ร้อยละ ๖๘.๗๕%
- มาก ร้อยละ ๒๘.๑๓%
- ปานกลาง ร้อยละ ๓.๑๓%

๒.๙ บุคลิกภาพ น้ำเสียง และความเป็นกันเอง

- มากที่สุด ร้อยละ ๖๘.๗๕%
- มาก ร้อยละ ๓๑.๒๕%

๒.๑๐ การรักษาเวลา

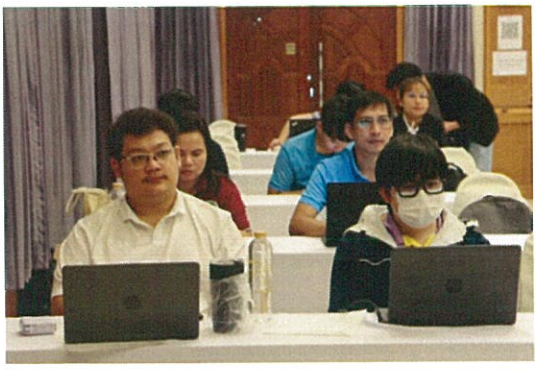
- มากที่สุด ร้อยละ ๗๑.๘๘%
- มาก ร้อยละ ๒๘.๑๓%

ภาคผนวก

- ภาพการประชุม
- เอกสารการประชุม

ภาพประกอบการประชุมเชิงปฏิบัติการ

เรื่อง “การพัฒนาศักยภาพภาคีเครือข่ายบุคลากรด้านเทคโนโลยีดิจิทัลกรม




PDPA กับหน่วยงาน


Vulnerability As:
Tenable Ne
การวิเค


เวลา 15.00 - 15.30
กลุ่มละ 15 นาที
เลือก 1 ในงาน
เพื่อนำเสนอ


ด้านเทคโนโลยีดิจิทัลกรม
24-26 กุมภา


วันที่ 24-26 กุมภา


ดิจิทัลครม
4-26 กุมภา
อ แพริมน้ำ รีส

แสกน QR Code

เอกสารประกอบการประชุม